

RECOVERY ACT – SMARTGRID REGIONAL DEMONSTRATION
TRANSMISSION AND DISTRIBUTION (T&D) INFRASTRUCTURE

KCP&L GREEN IMPACT ZONE SMARTGRID DEMONSTRATION

INTERIM TECHNOLOGY PERFORMANCE REPORT



WORK PERFORMED UNDER AGREEMENT

DE-OE0000221

SUBMITTED BY

Kansas City Power & Light Company
A Subsidiary of Great Plains Energy Incorporated
1200 Main St.
Kansas City, MO 64105

PRINCIPAL INVESTIGATOR

Edward T. Hedges, P.E.
Phone: 816-245-3861
Fax: 816-245-3615
ed.hedges@kcpl.com

SUBMITTED TO

U. S. Department of Energy
National Energy Technology Laboratory
Darshan Goswami
darshan.goswami@netl.doe.gov
Version 2.0 - December 31, 2013



DOE ACKNOWLEDGEMENT

This material is based upon work supported by the Department of Energy
under Award Number DE-OE0000221

FEDERAL DISCLAIMER

"This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof."

REPORT APPROVALS


Approved by



 Edward T. Hedges
 Manager of SmartGrid Technology Planning (Principal Investigator)
 Kansas City Power & Light

1-2-2014

 Date



 Bill Menge
 Director of SmartGrid
 Kansas City Power & Light

1-2-2014

 Date

REVISION LOG

Revision	Approval Date	Description
1.0	12/31/2012	Original Interim TPR submittal to DOE
1.1	03/28/2013	Updated with corrected terminology regarding project funding
2.0	12/31/2013	2013 Interim TPR submittal to DOE

ACKNOWLEDGEMENT

The following organizations and individuals, under contract to Kansas City Power & Light (KCP&L), prepared this report:

KCP&L

Kansas City Power & Light Co.
1200 Main St.
Kansas City, MO 64105

- Ed Hedges, Mgr. SmartGrid Tech. Planning
- Bill Menge, Director SmartGrid
- Gail Allen, Sr. Mgr. Customer Solutions
- Vicki Barszczak, Project Mgr. Delivery
- Steve Goeckeler, Sr. Engineer
- Mark Hopkins, Engineer III

Burns & McDonnell

Burns & McDonnell Engineering Co.
9400 Ward Pkwy
Kansas City, MO 64114

- Lucas McIntosh, Consulting Engineer
- Kim Bartak, Consulting Engineer
- Meghan Calabro, Consulting Engineer
- Matt Milligan, Consulting Engineer
- Jesse Teas, Consulting Engineer
- Rahul Chhabra, Consulting Engineer
- Matt Olson, Consulting Engineer

Structure

The Structure Group
12335 Kingsride, #401
Houston, TX 77024

- Andrew Dicker, Consultant
- Preeti Mathema, Consulting Engineer
- Angilberto Hernandez, Consulting Engineer
- Satyaveer, Consulting Engineer

EPRI

942 Corridor Park Blvd
Knoxville, TN 37932

- Brian Green, EPRI Representative

Other contributing authors

- Jim Jones, Independent IT Consultant
- Troy Terrell, Siemens

TABLE OF CONTENTS

1	SCOPE [1]	1
1.1	PROJECT ABSTRACT	1
1.2	PROJECT OVERVIEW	2
1.2.1	<i>Project Objectives</i>	2
1.2.2	<i>Introduction to Kansas City Power & Light Company (KCP&L)</i>	9
1.2.3	<i>Project Location</i>	11
1.2.4	<i>Project Timeline</i>	12
1.2.5	<i>Project Major Milestones</i>	12
1.3	SMARTGRID DEMONSTRATION PROJECT PARTICIPANTS	14
1.3.1	<i>Project Partners</i>	15
1.3.2	<i>Consultants</i>	16
1.3.3	<i>Contractors</i>	17
1.3.4	<i>Vendors</i>	18
1.4	DEMONSTRATION SYSTEMS & TECHNOLOGIES	19
1.4.1	<i>Demonstration Systems Overview</i>	19
1.4.2	<i>SmartMetering</i>	22
1.4.2.1	Advanced Metering Infrastructure (AMI).....	22
1.4.2.2	Meter Data Management (MDM).....	24
1.4.3	<i>SmartEnd-Use</i>	31
1.4.3.1	Customer Web Portal.....	32
1.4.3.2	In-Home Display (IHD).....	33
1.4.3.3	Standalone Programmable Communicating Thermostat (PCT)	34
1.4.3.4	Home Area Network (HAN).....	35
1.4.3.5	Residential Time-of-Use (TOU) Billing Pilot Program	36
1.4.4	<i>SmartSubstation</i>	38
1.4.4.1	Substation Protection Network (SPN) Upgrade	38
1.4.4.2	Distribution Data Concentrator (DDC)	40
1.4.4.3	Human Machine Interface (HMI)	41
1.4.4.4	Generic Object-Oriented Substation Event (GOOSE) [3].....	41
1.4.4.5	Substation Distributed Control and Data Acquisition (DCADA) System	43
1.4.5	<i>SmartDistribution</i>	43
1.4.5.1	Distribution Management System (DMS) User Interface (UI)	45
1.4.5.2	Distribution Supervisory Control and Data Acquisition (D-SCADA).....	46
1.4.5.3	Outage Management System (OMS)	47
1.4.5.4	1 st Responder Functions.....	47
1.4.5.5	Advanced Distribution Automation Field Area Network (FAN).....	50
1.4.5.6	Data Historian (HIS).....	52
1.4.6	<i>SmartGeneration</i>	53
1.4.6.1	Distributed Energy Resources Management (DERM)	53
1.4.6.2	DR Load Curtailment Programs.....	55
1.4.6.3	Battery Energy Storage System (BESS).....	56
1.4.6.4	Distributed Renewable Generation: Solar Photovoltaic	58
1.4.6.5	Vehicle Charge Management System (VCMS).....	59

2	TECHNICAL APPROACH [4]	61
2.1	CROSS-CUTTING PLANS & IMPLEMENTATIONS	61
2.1.1	<i>Interoperability Strategy & Plan [5]</i>	61
2.1.1.1	Interoperability Vision	61
2.1.1.2	Interoperability Strategy	62
2.1.1.3	SmartGrid Demonstration Communication Networks	63
2.1.1.4	Interoperability Plan and Approach	65
2.1.2	<i>Cyber Security Strategy & Plan [11]</i>	77
2.1.2.1	Smart Grid Cyber Security Trends & Challenges	77
2.1.2.2	Cyber Security Strategy & Approach	78
2.1.2.3	Smart Grid Cyber Security Design Considerations	79
2.1.3	<i>Education & Outreach Strategy & Plan [14]</i>	85
2.1.3.1	Introduction	85
2.1.3.2	Education & Outreach Messaging	85
2.1.3.3	Education & Outreach Audiences	86
2.1.3.4	Value Proposition Groups	88
2.1.3.5	Communications Approach	89
2.1.4	<i>Metrics & Benefits [4]</i>	90
2.1.4.1	Project Benefits	90
2.1.4.2	SmartGrid Project Metrics Reporting	90
2.1.4.3	Build Metrics – Measurement of Smart Grid Progress	92
2.1.4.4	Impact Metrics – Measurement of Smart Grid Impacts	94
2.1.4.5	Demonstration Sub-Projects and Expected Benefits	94
2.1.4.6	Smart Grid and Energy Storage Functions and Benefits	95
2.1.4.7	Data Gathering and Benefit Quantification	96
2.1.4.8	Baseline Data for Impact Metrics and Benefits Assessment	98
2.2	SYSTEMS IMPLEMENTATION	100
2.2.1	<i>SmartMetering</i>	101
2.2.1.1	AMI	101
2.2.1.2	MDM	109
2.2.2	<i>SmartEnd-Use</i>	115
2.2.2.1	Home Energy Management Web Portal	115
2.2.2.2	In-Home Display	120
2.2.2.3	Standalone Programmable Communicating Thermostat (PCT)	122
2.2.2.4	Home Area Network	125
2.2.2.5	Time-of-Use Rate	128
2.2.3	<i>SmartSubstation</i>	135
2.2.3.1	Substation Protection Network	136
2.2.3.2	Distribution Data Concentrator	141
2.2.3.3	Human Machine Interface	150
2.2.3.4	GOOSE Messaging	156
2.2.3.5	Substation DCADA	159
2.2.4	<i>SmartDistribution</i>	163
2.2.4.1	DMS UI/CAD	164
2.2.4.2	Distribution-SCADA	174
2.2.4.3	Outage Management System	182
2.2.4.4	1 st Responder Functions	186
2.2.4.5	ADA Field Area Network	192
2.2.4.6	Historical Information System	201
2.2.5	<i>SmartGeneration</i>	204
2.2.5.1	DERM	204
2.2.5.2	DR Load Curtailment	209

2.2.5.3	BESS	214
2.2.5.4	Solar PV	219
2.2.5.5	VCMS.....	222
2.3	IMPLEMENTATION TESTING PLANS.....	224
2.3.1	<i>System Testing</i>	224
2.3.1.1	Environments	225
2.3.1.2	Factory Acceptance Testing (FAT)	227
2.3.1.3	Site Acceptance Testing (SAT)	228
2.3.1.4	Details	229
2.3.2	<i>Integration Testing</i>	230
2.3.2.1	Environment	231
2.3.2.2	Factory Acceptance Testing (FAT)	242
2.3.2.3	Site Acceptance Testing (SAT)	243
2.3.2.4	Details	244
2.3.3	<i>End-to-End Interoperability Testing</i>	246
2.3.3.1	Description	246
2.3.3.2	Interoperability Flows	247
2.3.3.3	Interoperability Test Scripts	248
2.3.4	<i>End-to-End Field Demonstrations</i>	251
2.3.4.1	Description	251
2.3.4.2	Demonstration Flows	252
2.3.4.3	Demonstration Scripts	253
2.4	OPERATIONAL DEMONSTRATION AND TESTING PLANS.....	255
2.4.1	<i>Automated Voltage and VAR Control</i>	256
2.4.1.1	DOE SGCT Function to Benefit Rationale	256
2.4.1.2	Integrated Volt/VAR Management	257
2.4.2	<i>Real-Time Load Transfer</i>	259
2.4.2.1	DOE SGCT Function to Benefit Rationale	260
2.4.2.2	Feeder Load Transfer	260
2.4.3	<i>Automated Feeder and Line Switching</i>	262
2.4.3.1	DOE SGCT Function to Benefit Rationale	262
2.4.3.2	Fault Isolation and Service Restoration.....	263
2.4.4	<i>Automated Islanding and Reconnection</i>	265
2.4.4.1	DOE SGCT Function to Benefit Rationale	265
2.4.4.2	Feeder Islanding with Grid Battery	266
2.4.5	<i>Diagnosis and Notification of Equipment Condition</i>	267
2.4.5.1	DOE SGCT Function to Benefit Rationale	267
2.4.5.2	Substation Protection Automation	268
2.4.5.3	Asset Condition Monitoring	269
2.4.5.4	Substation Hierarchical Control	270
2.4.6	<i>Real-Time Load Measurement and Management</i>	272
2.4.6.1	DOE SGCT Function to Benefit Rationale	272
2.4.6.2	Automated Meter Reading	273
2.4.6.3	Remote Meter Disconnect/Reconnect	275
2.4.6.4	Meter Outage Restoration	276
2.4.6.5	Demand Response Events.....	277
2.4.7	<i>Customer Electricity Use Optimization</i>	279
2.4.7.1	DOE SGCT Function to Benefit Rationale	279
2.4.7.2	Historical Interval Usage Access.....	280
2.4.7.3	In-Home Display.....	282
2.4.7.4	Home Area Network	284
2.4.7.5	Time-of-Use Rate	286

2.4.8	<i>Distributed Production of Electricity</i>	288
2.4.8.1	DOE SGCT Function to Benefit Rationale	288
2.4.8.2	Distributed Roof-Top Solar Generation (DG)	289
2.4.9	<i>Storing Electricity for Later Use</i>	291
2.4.9.1	DOE SGCT Function to Benefit Rationale	291
2.4.9.2	Electric Energy Time Shift	293
2.4.9.3	Electric Supply Capacity	295
2.4.9.4	T&D Upgrade Deferral	297
2.4.9.5	Time-of-Use Energy Cost Management	299
2.4.9.6	Electric Service Reliability	301
2.4.9.7	Renewable Energy Time Shift	303
2.4.9.8	PEV Charging (VCM).....	304
2.5	DATA COLLECTION AND BENEFITS ANALYSIS	306
2.5.1	<i>SmartGrid Computational Tool (SGCT) Analysis [16]</i>	306
2.5.2	<i>Energy Storage Computational Tool (ESCT) Analysis [17]</i>	307
2.5.2.1	Bulk Energy Storage System Analysis	308
2.5.2.2	Premise Energy Storage System Analysis	309
2.5.3	<i>KCP&L Go-Forward Benefit/Cost Analysis of Demonstration Technologies</i>	309
3	RESULTS	311
3.1	INTEROPERABILITY [5]	312
3.1.1	<i>Integration Requirement Planning</i>	312
3.1.2	<i>Integration and Interoperability Requirement Definition</i>	313
3.1.2.1	EPRI-Assisted Use Cases	313
3.1.2.2	KCP&L-Developed Use Cases	314
3.1.2.3	Project Integration/Interface Points	317
3.1.3	<i>SmartGrid Application Integration Architecture Design</i>	318
3.1.3.1	SmartGrid Enterprise Service Bus Framework	318
3.1.4	<i>Interoperability Standards</i>	320
3.1.4.1	Back-Office Systems Integration Standards	320
3.1.4.2	Field Device Communication Standards.....	320
3.1.4.3	In-Home Communication Standards	320
3.2	CYBER SECURITY	321
3.2.1	<i>Risk Assessment [18]</i>	322
3.2.1.1	Scope of Assessment.....	322
3.2.1.2	Risk Quantification	323
3.2.1.3	Risk Assessment Recommendations	325
3.2.2	<i>Risk Mitigation</i>	326
3.2.2.1	Creation of Security Zones and Implementation of Tailored Control Sets.....	326
3.2.2.2	Industry-Suggested Controls	328
3.2.3	<i>Security Requirements Development</i>	329
3.2.4	<i>Application Security Assessment & Implementation</i>	332
3.2.5	<i>Physical Security Assessment & Implementation</i>	333
3.2.6	<i>Network Security Assessment & Implementation</i>	334
3.2.7	<i>Cyber Security Verification</i>	340
3.3	EDUCATION & OUTREACH	343
3.3.1	<i>All KCP&L Customers</i>	345
3.3.1.1	Customer Focused SmartGrid Website	345
3.3.1.2	Advertising	346
3.3.1.3	Energy Fairs.....	346
3.3.1.4	Social Media	347
3.3.1.5	Kansas City Media Briefings	347

3.3.2	<i>SmartGrid Demonstration Project Area Customers</i>	350
3.3.2.1	Direct Mail.....	350
3.3.2.2	SmartGrid Welcome Kit	351
3.3.2.3	SmartGrid DVD.....	351
3.3.2.4	E-mail Outreach	352
3.3.2.5	Automated Customer Notification.....	352
3.3.2.6	Civic Outreach.....	353
3.3.2.7	Consumer Advocate Interaction	356
3.3.3	<i>KCP&L Employees</i>	357
3.3.3.1	Employee Newsletter (The Source).....	357
3.3.3.2	E-Source	357
3.3.3.3	Employee Communications via TV Monitors, e-Mail, and Employee Meetings.....	358
3.3.3.4	Leadership Link Videos.....	358
3.3.3.5	SmartGrid Snippets	358
3.3.3.6	SmartGrid Project Sponsor Team Meetings.....	359
3.3.3.7	Executive Management Briefings.....	359
3.3.4	<i>State Agencies, Legislators and Regulators</i>	360
3.3.4.1	State Regulatory Commission Proceedings.....	360
3.3.4.2	MO and KS SmartGrid Stakeholder Groups.....	361
3.3.4.3	MO and KS Commission Staff.....	363
3.3.5	<i>Electric Utilities and Smart Grid Industry</i>	363
3.3.5.1	EPRI's Smart Grid Demonstration Project Participation.....	363
3.3.5.2	Technical Project Website.....	364
3.3.5.3	Technical Publications.....	365
3.3.5.4	Industry Conferences	365
3.3.5.5	Technical Education	368
3.3.5.6	Local Business and Industry Association Presentations	369
3.3.6	<i>Targeted Education & Outreach Initiatives</i>	370
3.3.6.1	AMI Education & Outreach	370
3.3.6.2	Residential SmartEnd-Use Products.....	370
3.3.6.3	Residential TOU Rates.....	370
3.3.6.4	SmartGrid Demonstration House.....	371
3.3.6.5	SmartGrid Innovation Park.....	373
3.3.7	<i>Project Tours & Field Demonstrations</i>	375
3.3.7.1	SmartGrid Demonstration House Tour	375
3.3.7.2	SmartGrid Innovation Park Tour	377
3.3.7.3	Grid Management Systems Tour	377
3.4	OPERATIONAL TESTING RESULTS	378
3.4.1	<i>Automated Voltage and VAR Control</i>	378
3.4.1.1	Integrated Volt/VAR Management	378
3.4.2	<i>Real-Time Load Transfer</i>	378
3.4.2.1	Feeder Load Transfer (FLT)	378
3.4.3	<i>Automated Feeder and Line Switching</i>	378
3.4.3.1	Fault Isolation and Service Restoration (FISR).....	378
3.4.4	<i>Automated Islanding and Reconnection</i>	378
3.4.4.1	Feeder Islanding with Grid Battery	378
3.4.5	<i>Diagnosis & Notification of Equipment Condition</i>	379
3.4.5.1	Substation Protection Automation	379
3.4.5.2	Asset Condition Monitoring	379
3.4.5.3	Substation Hierarchical Control (DCADA)	379
3.4.6	<i>Real Time Load Measurement & Management</i>	380
3.4.6.1	Automated Meter Reading (AMR)	380

3.4.6.2 Remote Connect/Disconnect 380

3.4.6.3 Outage Restoration 380

3.4.6.4 Demand Response Events (DR) 380

3.4.7 *Customer Electricity Use Optimization (Information)* 381

3.4.7.1 Historical Interval Usage Information (HEMP) 381

3.4.7.2 In-Home Display (IHD) 381

3.4.7.3 Home Area Network (HAN) 381

3.4.7.4 Time-of-Use (TOU) 381

3.4.8 *Distributed Production of Energy* 382

3.4.8.1 Distributed Roof-top Solar Generation (SDG) 382

3.4.9 *Storing Electricity for Later Use* 383

3.4.9.1 Electric Energy Time Shift 383

3.4.9.2 Electric Supply Capacity 383

3.4.9.3 T&D Upgrade Deferral 383

3.4.9.4 Time-of-Use Energy Cost Management 383

3.4.9.5 Electric Service Reliability 383

3.4.9.6 Renewable Energy Time Shift 383

3.4.9.7 PEV Charging (VCM) 383

3.5 METRICS AND BENEFITS ANALYSIS 384

3.5.1 *Build Metrics* 384

3.5.2 *Impact Metrics* 384

3.5.3 *SmartGrid Computational Tool Analysis* 384

3.5.4 *Energy Storage Computational Tool Analysis* 384

3.6 STAKEHOLDER FEEDBACK 385

4 CONCLUSIONS **387**

4.1 PERFORMANCE PROJECTIONS OF ENTERPRISE DEPLOYMENT 387

4.1.1 *Smart Grid Functions* 387

4.1.2 *Energy Storage Functions* 387

4.2 TECHNOLOGY GAPS 388

4.2.1 *Interoperability* 388

4.2.2 *Cyber Security* 388

4.2.3 *Education & Outreach* 388

4.2.4 *SmartMetering* 388

4.2.5 *SmartEnd-Use* 388

4.2.6 *SmartSubstation* 388

4.2.7 *SmartDistribution* 388

4.2.8 *SmartGeneration* 388

4.3 LESSONS LEARNED AND BEST PRACTICES 389

4.3.1 *Interoperability* 389

4.3.2 *Cyber Security* 389

4.3.3 *Education & Outreach* 389

4.3.4 *SmartMetering* 389

4.3.5 *SmartEnd-Use* 389

4.3.6 *SmartSubstation* 389

4.3.7 *SmartDistribution* 389

4.3.8 *SmartGeneration* 389

4.4 PROJECT IMPACT ON KCP&L'S FUTURE PLANS FOR SMART GRID DEPLOYMENT 390

5 CONTACTS **391**

6 REFERENCES **393**

7 ABBREVIATIONS AND ACRONYMS 395

8 APPENDICES 399

APPENDIX A BUILD & IMPACT METRICS..... A-1

APPENDIX B KCP&L SMART GRID USE CASES..... B-1

APPENDIX C KCP&L SMARTGRID MASTER INTERFACE LIST..... C-1

APPENDIX D IEC 61850 COMMUNICATIONS NETWORK D-1

APPENDIX E IEC 61850 SUBSTATION ETHERNET SWITCH TEST RESULTS E-1

APPENDIX F DEVICE POINTS LIST.....F-1

APPENDIX G BESS ACCEPTANCE TEST REPORT.....G-1

APPENDIX H SYSTEM DEPLOYMENT/GO-LIVE TEST STRATEGY..... H-1

APPENDIX I TEST PLAN WORKBOOKS I-1

APPENDIX J END-TO-END INTEROPERABILITY TESTING DOCUMENTATION J-1

APPENDIX K INTEROPERABILITY FIELD DEMONSTRATION SCRIPTS..... K-1

APPENDIX L SMARTGRID INTEROPERABILITY IMPLEMENTED FUTURE

APPENDIX M KCP&L SMARTGRID RISK ASSESSMENT MASTER REPORT..... FUTURE

APPENDIX N CYBER SECURITY CONTROLS MATRIX FUTURE

APPENDIX O AMI AUDIT RESULTS FUTURE

APPENDIX P EDUCATION & OUTREACH COLLATERAL..... FUTURE

APPENDIX Q EPRI SMARTEND-USE ANALYSIS RESULTS FUTURE

APPENDIX R NAVIGANT SMARTEND-USE PROGRAM ANALYSIS RESULTS FUTURE

APPENDIX S CUSTOMER SURVEY RESULTS..... FUTURE

APPENDIX T FINAL BUILD METRICS..... FUTURE

APPENDIX U FINAL IMPACT METRICS..... FUTURE

APPENDIX V RESERVED..... TBD

APPENDIX W RESERVED..... TBD

APPENDIX X RESERVED..... TBD

APPENDIX Y RESERVED..... TBD

APPENDIX Z RESERVED..... TBD

LIST OF TABLES

Table 1-1: Smart Grid Functions by KCP&L Demonstration Sub-Project	7
Table 1-2: Smart Grid Benefits Realized by KCP&L Demonstration Sub-Project	8
Table 1-3: KCP&L's Service Territory Statistics	9
Table 1-4: Major Project Milestones	13
Table 1-5: MDM Events Tracked.....	29
Table 1-6: Outage Restoration Events	30
Table 1-7: Pilot TOU Tariff Details	37
Table 2-1: Domains & Actors in the Smart Grid Conceptual Model	66
Table 2-2: Summary of Applicable Cyber Security Standards.....	80
Table 2-3: Summary of Applicable Cyber Security Frameworks.....	81
Table 2-4: Green Impact Zone Demographic Chart	86
Table 2-5: Smart Grid Benefits for KCP&L's Demonstration Project	91
Table 2-6: Build/Impact Metrics and TPR Reporting Schedule	92
Table 2-7: Applicable Monetary Investment Build Metrics (\$000).....	93
Table 2-8: Smart Grid Functions by KCP&L Demonstration Sub-Project	96
Table 2-9: Smart Grid Benefits Realized by SmartGrid Functions.....	97
Table 2-10: Pilot TOU Rate Details.....	131
Table 2-11: Substation IEDs Installed	138
Table 2-12: Field Devices	194
Table 2-13: Smart Grid PV Systems Installed.....	219
Table 2-14: System Test Books	230
Table 2-15: Devices Deployed in LAB Environment	236
Table 2-16: Devices Deployed in DEMO Environment.....	240
Table 2-17: Integration Test Books.....	245
Table 2-18: Interoperability Testing Documentation	250
Table 2-19: End-to-End Demonstration Scripts	254
Table 2-20: KCP&L Operational Demonstration/Tests	255
Table 2-21: SGCT Function-Benefit Chart for KCP&L Demonstration Project	307
Table 2-22: ESCT Application-Benefit Matrix for KCP&L BESS Analysis	308
Table 2-23: ESCT Application-Benefit Matrix for KCP&L PESS analysis.....	309
Table 3-1: SmartGrid Demonstration Project Use Cases	315
Table 3-2: Smart Grid Systems Included in the KCP&L Risk Assessment	322
Table 3-3: NISTIR-7628 Security Requirements Applicability by System	328
Table 3-4: Master Security Controls	330
Table 3-5: SmartGrid Audience Communication Methods.....	343
Table 3-6: Paid Advertising Initiatives	346
Table 3-7: Schedule of Energy Fairs.....	346
Table 3-8: Kansas City Media Initiatives	348
Table 3-9: Direct Mailing Timeline.....	350
Table 3-10: E-mail Initiatives	352
Table 3-11: Schedule of Events.....	353
Table 3-12: Community Events.....	354
Table 3-13: Schedule of Neighborhood Meetings	354
Table 3-14: Schedule of School Events	355
Table 3-15: The Source Articles	357

LIST OF TABLES CONTINUED

Table 3-16: The E-Source Articles	357
Table 3-17: Other Employee SmartGrid Communications	358
Table 3-18: Leadership Link Videos	358
Table 3-18: Executive Management Briefings	359
Table 3-20: State Agency, Legislator and Regulator Briefings	360
Table 3-21: Stakeholder Project Update Meetings.....	362
Table 3-22: Technical Publications	365
Table 3-23: Industry Conference Presentations	365
Table 3-24: Industry Webinars	368
Table 3-25: Local Business and Industry Association Presentations	369
Table 3-20: Schedule of Demonstration House Tours	375
Table 3-21: Schedule of SmartGrid Innovation Park Events	377

LIST OF FIGURES

Figure 1-1: KCP&L Service Territory Map	10
Figure 1-2: KCP&L Green Impact Zone SmartGrid Demonstration Map	11
Figure 1-3: Project Timeline.....	12
Figure 1-4: Selected Project Partners	14
Figure 1-5: KCP&L Demonstration, a True End-to-End SmartGrid.....	19
Figure 1-6: KCP&L Demonstration, T&D Control Systems Infrastructure.....	20
Figure 1-7: AMI RF Mesh FAN	23
Figure 1-8: Communication Flow from the AHE to the HAN via the FAN	24
Figure 1-9: MDM Integration Overview.....	25
Figure 1-10: MDM Interval VEE Workflow	26
Figure 1-11: Usage Framing for TOU	27
Figure 1-12: MDM Event Handling Overview	28
Figure 1-13: MDM Outage/Restoration Event Handling	29
Figure 1-14: MDM Remote Service Order Handling Overview	30
Figure 1-15: Tendril™ Connect Platform Architecture.....	31
Figure 1-16: Customer Web Portal	32
Figure 1-17: In-Home Display	33
Figure 1-18: Standalone PCT.....	34
Figure 1-19: Home Area Network Devices.....	35
Figure 1-20: KCP&L System Load Profile and TOU Rates.....	36
Figure 1-21: Midtown Substation Protection and Control Network Architecture	39
Figure 1-22: GOOSE Logic Diagram.....	43
Figure 1-23: SmartDistribution Components.....	45
Figure 1-24: HIS Components	52
Figure 1-25: Distributed Energy Management Solution Functional Overview	54

LIST OF FIGURES CONTINUED

Figure 1-26: Demand Response Load Curtailment Architecture	55
Figure 1-27: Grid-Connected Battery.....	57
Figure 1-28: Paseo High School Roof-top Solar PV System.....	58
Figure 1-29: Coulomb CT2021 Charging Station	59
Figure 2-1: KCP&L MPLS-based IP Communication	63
Figure 2-2: KCP&L SmartGrid Demonstration Project Communication Network.....	64
Figure 2-3: KCP&L SmartGrid Interoperability Approach	65
Figure 2-4: Interaction of Actors in Different Smart Grid Domains	67
Figure 2-5: GridWise Interoperability Framework.....	68
Figure 2-6: IntelliGrid SM Architecture Definition Evolution	69
Figure 2-7: IntelliGrid SM Use Case Driven Interoperability Test Plan Development Process	70
Figure 2-8: NIST Smart Grid Logical Interface Reference Model	71
Figure 2-9: NIST Smart Grid Cyber Security Logical Reference Model	72
Figure 2-10: NIST Guiding Principles for Identifying Standards for Implementation	76
Figure 2-11: KCP&L SmartGrid Security Strategy and Approach	79
Figure 2-12: KCP&L GRC Management Framework.....	80
Figure 2-13: KCP&L Risk Management Process	82
Figure 2-14: KCP&L <i>Defense in Depth</i> Security Posture.....	82
Figure 2-15: KCP&L Trust Model.....	84
Figure 2-16: Customer Value Proposition.....	89
Figure 2-17: KCP&L SmartGrid Demonstration Systems Integration.....	100
Figure 2-18: L+G Gridstream AMI Command Center and FAN	101
Figure 2-19: KCP&L SmartGrid Demonstration Project AMI Deployment Timeline	101
Figure 2-20: AMI Head End - L+G Gridstream Command Center	102
Figure 2-21: Installed AMI FAN Infrastructure.....	103
Figure 2-22: KCP&L SmartGrid Demonstration Project AHE Integration	104
Figure 2-23: EnergyIP MDM Application Components	109
Figure 2-24: KCP&L SmartGrid Demonstration Project MDM Integration	112
Figure 2-25: Tendril TM Connect Platform Architecture.....	115
Figure 2-26: Customer Web Portal Data Flows	116
Figure 2-27: KCP&L SmartGrid Demonstration Project HEMP Integration.....	117
Figure 2-28: In-Home Display Communication.....	121
Figure 2-29: Standalone PCT Communication	123
Figure 2-30: Home Area Network Communication	126
Figure 2-31: KCP&L Summer Monthly Average System Load.....	129
Figure 2-32: KCP&L Summer Average Residential Load	129
Figure 2-33: Customer Savings Potential in Various Revenue Neutral Price Options	130
Figure 2-34: Peak Price in Various Revenue Neutral Price Options.....	130
Figure 2-35: KCP&L SmartGrid Demonstration Project TOU Integration	133
Figure 2-36: SmartSubstation Protection and Control Infrastructure	137
Figure 2-37: IEC 61850 Device Template on the SICAM	143
Figure 2-38: DNP3 Device Configuration on the SICAM	144
Figure 2-39: KCP&L SmartGrid Demonstration Project DDC Integration	146
Figure 2-40: HMI One-Line Screenshot.....	152
Figure 2-41: HMI Single Bus Screenshot	152

LIST OF FIGURES CONTINUED

Figure 2-42: HMI Device Diagnostic Screenshot.....	153
Figure 2-43: HMI Alarm List Screenshot	153
Figure 2-44: HMI Event Log Screenshot.....	154
Figure 2-45: HMI Network Overview Screenshot	154
Figure 2-46: KCP&L SmartGrid Demonstration Project HMI Integration.....	155
Figure 2-47: GOOSE Lab Testing Rack Setup.....	157
Figure 2-48: KCP&L SmartGrid Demonstration Project DCADA Integration	160
Figure 2-49: KCP&L SmartGrid Demonstration Project CAD Integration.....	168
Figure 2-50: KCP&L SmartGrid Demonstration Project D-SCADA Integration.....	177
Figure 2-51: KCP&L SmartGrid Demonstration Project OMS Integration.....	184
Figure 2-52: KCP&L SmartGrid Demonstration Project First Responder Integration	189
Figure 2-53: KCP&L Base Mesh Network.....	193
Figure 2-54: KCP&L Final Deployed Mesh Network.....	194
Figure 2-55: Typical Capacitor Bank Installation.....	195
Figure 2-56: Typical Fault Current Indicator Installation	196
Figure 2-57: Typical Recloser Installation	196
Figure 2-58: Battery Installation	197
Figure 2-59: KCP&L SmartGrid Demonstration Project DA Integration.....	198
Figure 2-60: KCP&L SmartGrid Demonstration Project HIS Integration	202
Figure 2-61: KCP&L SmartGrid Demonstration Project DERM Integration.....	207
Figure 2-62: Demand Response Load Curtailment Architecture	209
Figure 2-63: KCP&L SmartGrid Demonstration Project DR Load Curtailment Integration	212
Figure 2-64: Innovation Park and BESS Site Overview.....	214
Figure 2-65: BESS Installation	215
Figure 2-66: KCP&L SmartGrid Demonstration Project BESS Integration.....	216
Figure 2-67: KCP&L SmartGrid Demonstration Project PV Integration	220
Figure 2-68: ChargePoint Map of SmartGrid EVCSs.....	222
Figure 2-69: KCP&L SmartGrid Demonstration Project VCMS Integration	223
Figure 2-70: System Testing.....	225
Figure 2-71: Integration Testing	231
Figure 2-72: SmartGrid LAB Environment Integrated Systems.....	234
Figure 2-73: SmartGrid DEMO Environment Integrated Systems	237
Figure 2-74: Midtown Substation	238
Figure 2-75: Midtown Substation and Distribution Feeders	239
Figure 2-76: SmartEnd-Use Home Configuration	239
Figure 2-77: End-to-End Interoperability Testing	246
Figure 2-78: Interoperability Flows.....	248
Figure 2-79: End-to-End Field Demonstration	251
Figure 2-80: Demonstration Flows	252
Figure 2-81: Demonstration Script	253
Figure 2-82: SGCT Translation of Smart Grid Assets to Monetary Value.....	306
Figure 2-83: System ESCT Methodology for determining the monetary value of an ES deployment	308
Figure 3-1: KCP&L Project vs. NIST SmartGrid Logical Interface Reference Model	312
Figure 3-2: KCP&L SmartGrid Demonstration Systems Interfaces	313
Figure 3-3: KCP&L SmartGrid Systems Integration	317

LIST OF FIGURES CONTINUED

Figure 3-4: KCP&L SmartGrid Master Interface Diagram	318
Figure 3-5: KCP&L SmartGrid ESB Framework Example	319
Figure 3-6: Cyber Security Plan Execution Focus Areas	321
Figure 3-7: Graphical Representation of Relative Vulnerability Ratings.....	323
Figure 3-8: Graphical Representation of Relative Criticality Results	324
Figure 3-9: Risk Rating Categories	325
Figure 3-10: Representation of Smart Grid Applications in Respective Security Zones	327
Figure 3-11: Representation of Control Sets for Inter-Security Zone Communication	327
Figure 3-12: AMI Security Service Domains [19]	331
Figure 3-13: Excerpt from Vendor Cyber Security Survey	332
Figure 3-14: Midtown Substation Network Architecture	336
Figure 3-15: Back Office Network Architecture	337
Figure 3-16: Overall SmartGrid Network Architecture	338
Figure 3-17: <i>www.kcplsmartgrid.com</i> Home Page Screenshot	345
Figure 3-18: Screenshot of SmartGrid News Story	347
Figure 3-19: SmartGrid Welcome Kit	351
Figure 3-20: SmartGrid DVD	351
Figure 3-21: <i>www.kcplsmartgrid.com/industry-resources</i> Page Screenshot	364
Figure 3-21: Rooftop PV Installation on Project Living Proof Demonstration House	372
Figure 3-22: Sunverge Unit Installation at Project Living Proof Demonstration House	372
Figure 3-23: KCP&L's Smart Grid Innovation Park Site Layout	373
Figure 3-24: Battery Energy Storage System (BESS) at SmartGrid Innovation Park	374
Figure 3-25: 5 kW Photovoltaic Array at SmartGrid Innovation Park	374
Figure 3-26: Informational Kiosk at SmartGrid Innovation Park.....	375

1 Scope [1]

This document represents the second interim Technology Performance Report for the Kansas City Power & Light Company (KCP&L) Green Impact Zone SmartGrid Demonstration Project. The KCP&L project is partially funded by DOE Regional Smart Grid Demonstration Project (SGDP) cooperative agreement DE-OE0000221 in the Transmission and Distribution Infrastructure application area.

This interim Technology Performance Report (TPR) summarizes the KCP&L SmartGrid Demonstration Project as of December 31, 2013 and includes summaries of the project design, implementation, operations, and analysis performed as of that date.

1.1 Project Abstract

Kansas City Power & Light (KCP&L) is known for its commitment to community engagement and its ability to bring together diverse stakeholder groups to develop regional energy solutions. In 2007, KCP&L won the Edison Electric Institute's top award for innovation and contribution to the advancement of the electric industry. In addition, KCP&L is the only utility in the U.S. to reach an agreement with the Sierra Club in pursuing renewable energy and energy efficiency projects while building a high-efficiency coal generating station. Recognizing the need for a new approach to electricity generation, transmission, and distribution, KCP&L was awarded a DOE Regional SGDP cooperative agreement to deploy a fully integrated SmartGrid Demonstration in an economically challenged area of Kansas City, Missouri. The project is investing over \$58 million to explore potential benefits to customers and the local grid and provide technology learning and advancement to the entire industry. Of the total investment, the DOE Regional SGDP cooperative agreement is providing approximately \$23.9 million.

For the Demonstration Project, KCP&L is deploying an end-to-end Smart Grid that will include advanced renewable generation; storage resources; leading edge substation and distribution automation and controls; energy management interfaces; and innovative customer programs and rate structures. The Demonstration Project is focused on a subset of the area served by KCP&L's Midtown Substation, impacting approximately 14,000 commercial and residential customers across five square miles.

KCP&L's project complies with the DOE's funding guidelines and introduces commercial innovation with a unique approach to SmartGrid development and demonstration:

- First, this project truly creates a complete, end-to-end Smart Grid – from smart generation to smart end-use; it will deliver improved performance focused on a major substation in an urban location.
- Second, it introduces new technologies, applications, protocols, communications, and business models that will be evaluated, demonstrated, and refined to achieve improved operations, increased energy efficiency, reduced energy delivery costs, and improved environmental performance.
- Third, it involves a best-in-class approach to technology integration, application development, and partnership collaboration, allowing KCP&L to advance the progression of complete smart grid solutions, with interoperability standards, rather than single, packaged applications.
- Finally, KCP&L's SmartGrid Demonstration Project will provide the critical energy infrastructure required to support a targeted urban revitalization effort—Kansas City's Green Impact Zone.

The project introduces new technologies in the substation and the distribution network as well as advanced renewable resources and large-scale energy storage to supply electricity and offset peak electrical demand. Finally, end users will be provided detailed usage information, digital tools, and innovative programs to empower them to optimize energy consumption and bill savings.

The Green Impact Zone (www.greenimpactzone.org) is the vision of Rep. Emanuel Cleaver II (D-MO) and will be a model for urban renewal and sustainability. The City of Kansas City and the Mid-America Regional Council have also taken lead roles in the effort. Through KCP&L's participation, innovators in today's SmartGrid landscape such as Siemens, OATI, Landis+Gyr, Intergraph, EPRI, Tendril, and Exergonix (formerly Kokam America) have signed-on to provide equipment, technical expertise, and in-kind financial support. A key component of the project is enhancing collaboration between public and private stakeholders. KCP&L believes the SmartGrid project will foster an environment for increased employment opportunities, broad economic development, and reinvestment in the area.

By demonstrating an end-to-end solution, KCP&L will be able to test, evaluate, and report on a complete suite of Smart Grid benefits that include greater energy efficiency, reduced cost, improved reliability, more transparent and interactive information, and an improved environmental footprint. KCP&L believes this project will serve as a blueprint for future Smart Grid implementations and will accelerate the realization of the "utility of the future" that safely delivers reliable electricity with greater efficiency, reduced costs, and improved environmental performance.

1.2 Project Overview

1.2.1 Project Objectives

The primary objective of the SmartGrid Demonstration Project is twofold: (a) to demonstrate, test and report on the feasibility of combining, integrating and applying existing and emerging Smart Grid technologies and solutions to build innovative Smart Grid solutions and (b) to demonstrate, measure, and report on the costs, benefits, and business model viability of the demonstrated solutions. The proposed technologies and solutions will be evaluated both individually, and as part of a complete end-to-end integrated Smart Grid system in a defined geographical area. The project will demonstrate certain operational, economic, consumer, and environmental benefits that can be enabled by single Smart Grid technologies and further enhanced by integrated solutions as proposed for this demonstration.

The objectives of individual initiatives are focused on implementing a next-generation, end-to-end Smart Grid that will include Distributed Energy Resources (DER), enhanced customer facing technologies, and a distributed-hierarchical grid control system.

1.2.1.1.1 Interoperability

The KCP&L SmartGrid Demonstration Project interoperability objective is to implement an integrated end-to-end solution that demonstrates interoperability of the key Smart Grid components and incorporates elements of seven (7) of the eight (8) priority areas identified by FERC and NIST in the NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0 (NIST Smart Grid Framework):

- Demand Response and Consumer Energy Efficiency,
- Electric Storage,
- Electric Transportation,
- Advanced Metering Infrastructure,
- Distribution Grid Management,
- Cyber Security, and
- Network Communications.

This demonstration will implement a distribution network management system, substation and distribution automation systems, distributed resource and demand-side management systems, advanced metering infrastructure and customer-based energy management and behind-the-meter

resources and loads. The proposed solution architecture follows the EPRI IntelliGrid Architecture and GridWise Architectural Council recommendations, as well as the NIST Smart Grid Framework.

1.2.1.1.2 Cyber Security

One of the objectives of the KCP&L SmartGrid Demonstration Project (SGDP) is to evaluate and demonstrate end-to-end cyber security and incorporate the appropriate NIST cyber security standards and emerging industry security profiles, namely the NISTIR-7628 and UCAIug Security Profiles for Distribution Management (DM) and Advanced Metering Infrastructure (AMI). Over the course of the project to date, the project team has assessed the applicability of these standards and profiles and has adopted and/or augmented these standards as deemed appropriate.

The project team has taken cyber security considerations into account during each phase of the KCP&L SGDP infrastructure development both from an IT and grid infrastructure perspective. KCP&L has also chosen to implement the SGDP using a private communications architecture wherever practical. By utilizing the Corporate IT Wide Area Network (WAN) and utility-owned Field Area Network (FAN), the communication between KCP&L SmartGrid systems can leverage the vast amount of industry research and development for IP-based technologies. Another benefit of utilizing private networks instead of the public Internet for internal communication is to minimize vulnerability to cyber security attacks.

1.2.1.1.3 Education & Outreach

KCP&L's SmartGrid Demonstration Project and associated partnerships in the Green Impact Zone create a tremendous opportunity for customers, the region and the entire country to understand the value of advanced energy distribution and load management while providing reinvestment in Kansas City's urban core. Successful implementation of the KCP&L SmartGrid Demonstration Project will require a steadfast commitment to effective stakeholder-focused communication.

There are three primary communications objectives for KCP&L's SmartGrid Demonstration Project:

- Educate and engage customers in the project area, including the Green Impact Zone, about how SmartGrid investments will ultimately impact and benefit them, and then influence behavior and encourage participation in energy usage management
- Inform the remainder of KCP&L's customer base about how SmartGrid investments could ultimately impact and benefit them
- Share information with the broader utility industry on the progress and outcome of the project

Just as the Demonstration Project is being deployed in a series of phases, so too is the public education and outreach plan. In 2010, the goal was to create general project awareness and understanding through face-to-face interaction, customer engagement and the introduction of new SmartGrid tools. As the project moved into 2011 and beyond, the communications efforts become even more targeted as customer segments emerge and product adoption increases. At this point, KCP&L will begin to analyze and evaluate customer behaviors, attitudes and channel preferences as well as the messaging mix that is most effective. In addition, the grid focused components of the project will be introduced to customers to help them better understanding the complexity and potential value of these investments and transformations.

1.2.1.1.4 SmartMetering

The primary objective of the SmartMetering sub-project is to develop and demonstrate state-of-the-art integrated advanced metering infrastructure (AMI) and meter data management (MDM) systems that support two-way communication with 14,000 SmartMeters in the Demonstration Project area and that integrate with other enterprise systems such as CIS, DMS, OMS, and DERM. The SmartMetering

infrastructure will provide the technology basis for recording customer and grid data that will be used to measure many SmartGrid benefits.

This new SmartMetering implementation will enable and quantify the following benefits:

- Reduced operating expenses through remote connect/disconnect capabilities
- Improved accuracy and frequency of meter reads
- Improved accuracy of meter inventory and reduction in untracked meters
- Increased success rate of automated reads relative to existing one-way AMR
- Improved outage handling relative to existing AMR technology with increased outage notification success rates and new power restoration messages
- Enables real-time, two-way communication for demand response program control initiation and verification of program participation

The SmartMetering technology will also provide advanced meter-to-HAN communications to facilitate in-home display, home energy management systems, and other consumer facing programs.

1.2.1.1.5 SmartEnd-Use

The primary objective of the KCP&L SmartEnd-Use sub-project is two-fold. This sub-project will achieve a sufficient number of consumers enrolled in a variety of consumer facing programs to 1) support the DERM development and demonstration, and 2) measure, analyze, and evaluate the impact that consumer education, enhanced energy consumption information, energy cost and pricing programs and other consumer based programs have on end-use consumption. We have identified several secondary objectives for the suite of SmartEnd-Use programs expected to be deployed in the Demonstration Area:

- Improve customer satisfaction by increasing awareness and providing cost-saving opportunities
- Improve KCP&L's capacity to serve customers through increased knowledge of customer behavior and usage patterns
- Demonstrate potential to reduce residential peak load profiles and reduce the need for future system capacity expansion by incenting off peak energy usage
- Pilot novel time-of-use (TOU) rate programs designed to incent consumer energy usage reduction during peak periods

By achieving these objectives, we expect to demonstrate how the integration of a broad suite of innovative efficiency and rate programs into a complete SmartGrid solution can enhance the overall benefits of the solution and optimally leverage the additional technical and operational capabilities that are enabled by the pilot investment.

1.2.1.1.6 SmartSubstation

The primary objective of the SmartSubstation sub-project is to develop and demonstrate a fully automated; next-generation distribution SmartSubstation with a local distributed control system based on IEC 61850 protocols.

This new SmartSubstation demonstration will enable and quantify the following expected benefits:

- Improved real-time operating data on critical substation equipment
- Reduced O&M costs of relay maintenance
- Improved reliability through automation

By achieving these objectives, we expect to demonstrate Advanced Distribution Substation Automation with full substation automation with local automation controllers, operator interfaces, and other benefits of integrated intelligent electronic relays such as peer-to-peer communication, intelligent bus throw-over, fault recording, fault location, circuit breaker monitoring and more efficient maintenance.

1.2.1.1.7 SmartDistribution

The primary objective of the SmartDistribution sub-project is to develop and demonstrate a next generation Distribution Management System (DMS) architecture that includes a fully automated, Distributed Control and Data Acquisition (DCADA) SmartSubstation controller that incorporates a Common Information Model (CIM) based model of the local distribution network and performs local grid assessment and control of individual intelligent electronic device (IED) field controls. The DMS and DCADA will provide the operational backbone of the system supporting significant levels of automation on the feeders, complex and automated feeder reconfiguration decisions, and tightly integrated supervision with the Control Centers. The DMS serves as the primary point of integration for the grid facilities and network management functionality including Distribution Supervisory Control and Data Acquisition (D-SCADA) systems, Distribution Network Applications (DNA) systems, Outage Management Systems (OMS), Distributed Energy Resource Management (DERM) systems, Geographic Information Systems (GIS) and other supporting systems.

This new SmartDistribution demonstration will enable and quantify the following benefits:

- Improved service reliability by reducing the frequency and duration of outages
- Reduced frequency of momentary outages
- Reduced operational expenses through automation and remote control
- Reduced maintenance expenses through predictive maintenance strategies

In achieving the above objectives, we expect to demonstrate a family of automatic, distributed “first responder” distribution grid monitoring and control functions:

- Substation and feeder load profile metering at 15 minute intervals
- Circuit outage and faulted section identification and isolation switching
- Substation and feeder VAR management
- Substation and feeder voltage management
- Substation and feeder integrated Volt/VAR Management
- Substation and feeder overload management with Dynamic Voltage Control (DVC) and Conservation Voltage Reduction (CVR)
- Distributed DER monitoring and management
- Substation and feeder overload management with Distributed Energy Resources
- Digital fault recording on breaker relays

We also expect to demonstrate time-synchronized voltage and current from strategic points on the circuits, which will improve the accuracy of capacity planning models and will enable better load balancing and improved decision-making for capacity additions.

1.2.1.1.8 SmartGeneration

The primary objective of the SmartGeneration sub-project is two-fold. The program will develop and demonstrate a next-generation, end-to-end Distributed Energy Resource Management (DERM) system that provides balancing of renewable and variable distributed energy resources (DER) with controllable demand response (DR) as it becomes integrated in the utility grid, coordination with market systems, and provision of pricing signals.

We expect to demonstrate a number of capabilities including:

- The ability to manage and control diverse DERs (e.g. DVC, DG, storage, etc.)
- The ability to manage and control various DR programs effectively
- The ability to manage price-based and voluntary programs with market-based and dynamic tariffs similar to those described under SmartEnd-Use.
- Interoperability with the DMS to monitor distribution grid conditions and leverage DR and DERs to manage distribution grid congestion.

The SmartGeneration sub-project will also implement DR/DER resources and DR programs sufficient in quantity and diversity to support the DERM development and demonstration. This sub-project will include:

- Installation of a variety of roof-top solar systems on a mix of residential and commercial buildings, including one larger scale installation (100 kW)
- Installation of a 1MW grid-connected battery
- Implementation of an AMI-based direct load control (DLC) DR program with installation of up to 1600 standalone residential programmable communicating thermostats (PCTs)
- Implementation of a home energy management program with installation of up to 400 Home Area Networks (HAN) that include a PCT, 120V outlet disconnects, and 240V (water heater, pool pump, etc.) disconnects
- Implementation of DR-enabled publicly accessible plug-in hybrid electric vehicle (PHEV) charging stations to demonstrate smart charging strategies

By achieving these objectives, KCP&L expects to demonstrate advanced capabilities in demand side resource management, including the ability to leverage those resources for operational efficiencies, reduction of environmental impact, and to support wholesale market operations.

In addition to the primary objective, KCP&L expects to evaluate the feasibility to offset fossil-based generation with renewable sources as well as the potential for flexible, alternative business ownership models.

1.2.1.1.9 *SmartGrid Functions*

The DOE has identified a series of Smart Grid Functions [2] that capture the characteristics or capabilities of a Smart Grid. Each of the KCP&L SmartGrid Demonstration Project sub-projects will implement a variety of SmartGrid assets and technologies that enable one or more of these Smart Grid Functions. Table 1-1 below, identifies which sub-project will directly implement or support the implementation of the Smart Grid Functions that will be implemented by the project.

Table 1-1: Smart Grid Functions by KCP&L Demonstration Sub-Project

Smart Grid Functions		Demonstration Sub-Project				
		Smart Metering	Smart End-Use	Smart Substation	Smart Distribution	Smart Generation
D = Direct S = Support						
Smart Grid Functions	Fault Current Limiting					
	Wide Area Monitoring, Visualization, and Control					
	Dynamic Capability Rating					
	Power Flow Control					
	Adaptive Protection					
	Automated Feeder Switching			S	D	
	Automated Islanding and Reconnection			S	S	D
	Automated Voltage and VAR control	S		S	D	
	Diagnosis and Notification of Equipment Condition			D	D	
	Enhanced Fault Protection					
	Real-Time Load Measurement and Management	D	S			D
	Real-Time Load Transfer	S		S	D	
	Customer Electricity Use Optimization	D	D			
	Distributed Production of Electricity					D
	Storing Electricity for Later Use					D

1.2.1.1.10 Smart Grid Benefits

The KCP&L SmartGrid Demonstration Project components, technologies, and Smart Grid functions to be demonstrated were chosen because they have the possibility of providing extensive system benefits, individually, and collectively, they offer an even more effective means for achieving the project objectives. For each of the project components, KCP&L has identified the DOE identified SmartGrid benefits that are anticipated to be observed, quantified, or calculated during the course of the project are summarized in Table 1-2 below.

Table 1-2: Smart Grid Benefits Realized by KCP&L Demonstration Sub-Project

Smart Grid Benefits			Demonstration Sub-Project				
			Smart Metering	Smart End-Use	Smart Substation	Smart Distribution	Smart Generation
D = Direct Benefit I = Indirect Benefit							
Economic	Market Revenue	Arbitrage Revenue*					
		Capacity Revenue*					
		Ancillary Services Revenue*					
	Improved Asset Utilization	Optimized Generator Operation					
		Deferred Gen. Capacity Investments	I	D			D
		Reduced Ancillary Service Cost					
		Reduced Congestion Cost					
	T&D Capital Savings	Deferred Trans. Capacity Investment					
		Deferred Dist. Capacity Investments		D		D	D
		Reduced Equipment Failures			D	D	
	T&D O&M Savings	Reduced Dist. Equip. O&M Cost					
		Reduced Dist. Operations Cost				D	
		Reduced Meter Reading Cost	D				
Reduced Theft	Reduced Electricity Theft	D					
Energy Efficiency	Reduced Electricity Losses	I	I		D	D	
Electricity Cost	Reduced Electricity Cost		D			D	
Reliability	Power Interruptions	Reduced Sustained Outages			D	D	D
		Reduced Major Outages	D		D	D	
		Reduced Restoration Cost	D		D	D	
	Power Quality	Reduced Momentary Outages					
Reduced Sags and Swells							
Environmental	Air Emissions	Reduced carbon dioxide Emissions		I		I	D
		Reduced Emissions		I		I	D
Security	Energy Security	Reduced Oil Usage	D		I	D	
		Reduced Wide-scale Blackouts					

*These benefits are only applicable to energy storage demonstrations.

1.2.2 Introduction to Kansas City Power & Light Company (KCP&L)

The mission of KCP&L, as a leading and trusted energy partner, is to provide safe, reliable power and customer-focused energy solutions that create stakeholder value through operational excellence, innovation, and a diverse, engaged workforce. Our higher purpose is improving life in the communities that we serve.

Great Plains Energy (GPE), a Missouri corporation incorporated in 2001 and headquartered in Kansas City, Missouri, is the holding company for two vertically integrated electric utilities - KCP&L and KCP&L Greater Missouri Operations Company (KCP&L-GMO). Both utilities operate under the brand name KCP&L. KCP&L's service territory encompasses all or portions of 47 counties over approximately 18,000 square miles in western Missouri and eastern Kansas.

1.2.2.1.1 KCP&L Utility Operations

Operating from its headquarters in Kansas City, Missouri, KCP&L has evolved into a full-service energy provider and resource. The company was founded in 1882 and has become one of the Midwest's most affordable energy suppliers because of our leadership in efficient power production and distribution through advanced fuel procurement, power plant technology, and distribution technology.

Our utilities serve over 820,000 customers with approximately 722,000 residential, 96,000 commercial, and 2,800 industrial and bulk power customers. Our utilities, located in Missouri and Kansas, have a combined generation capacity of over 6,100 MWs, 3,000 miles of transmission lines, approximately 17,000 miles of overhead distribution lines and over 7,000 miles of underground distribution lines. Detailed statistics of KCP&L's service territory are shown in Table 1-3.

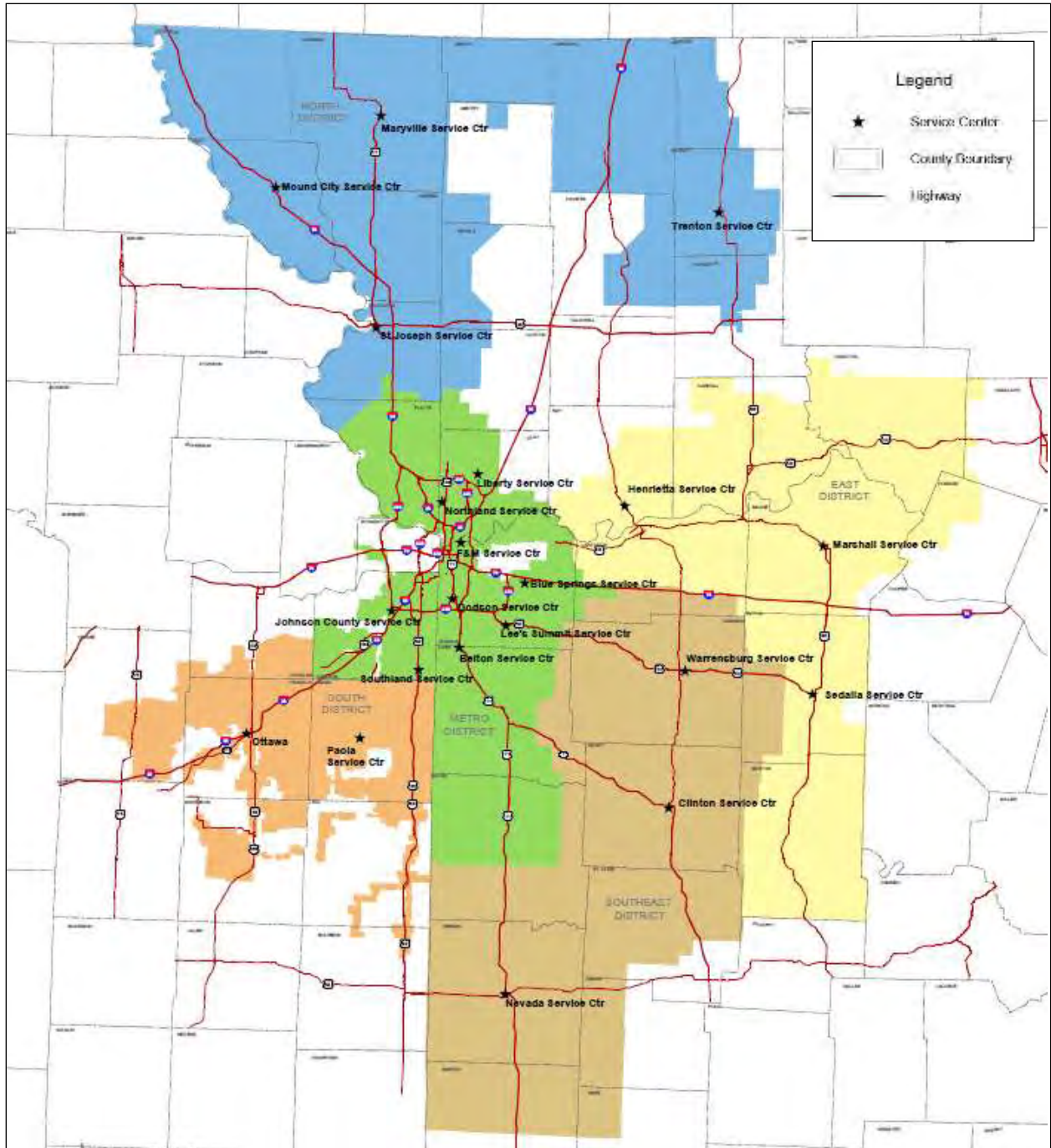
Table 1-3: KCP&L's Service Territory Statistics

KCP&L's Service Territory			
	GPE	KCP&L	KCP&L - GMO
Total number of customers:			
Residential	723,752	450,359	273,393
Commercial	95,801	57,725	38,076
Industrial & Municipal	2,753	2,393	360
Peak load:			
Summer	5,253 MW	3448 MW	1878 MW
Winter	4,115 MW	2670 MW	1568 MW
Total MWh sales:			
Residential	8,647,450	5,202,904	3,444,546
Commercial	10,636,691	7,506,463	3,130,228
Industrial	3,142,761	1,884,401	1,258,360
Bulk Power	5,492,710	5,280,312	212,398
Distribution Assets:			
Total number of substations	316	91	225
Total number of distribution feeders	1382	767	615
Total miles of overhead distribution line	17,000 mi.	11,768 mi.	5,232 mi.
Total miles of underground distribution lines	7,000 mi.	4,502 mi.	2,498 mi.
Total miles of transmission lines	3,000 mi.	1,765 mi.	1,235 mi.

1.2.2.1.2 Service Territory

As shown in Figure 1-1, KCP&L services customers in 47 northwestern Missouri and eastern Kansas counties - a service territory of approximately 18,000 square miles (www.kcpl.com).

Figure 1-1: KCP&L Service Territory Map



1.2.2.1.3 *Regulation and Oversight*

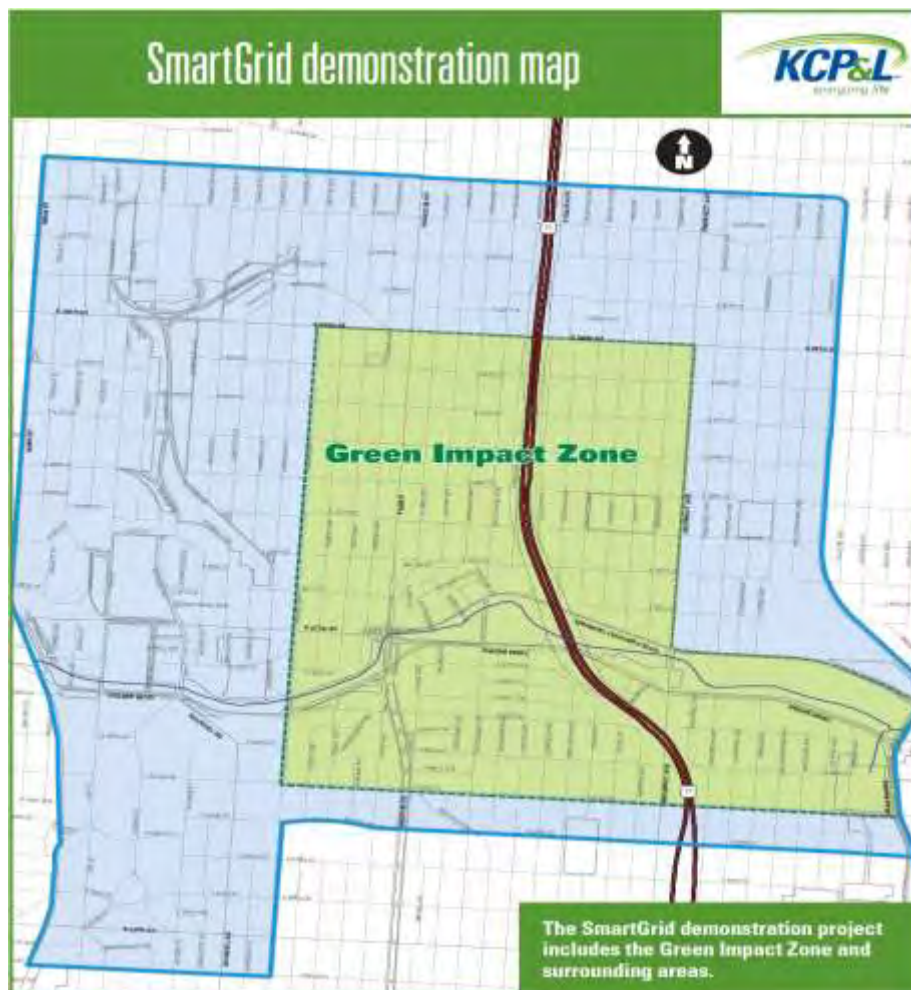
Both utilities are regulated by the Missouri Public Service Commission (MPSC). Kansas City Power & Light is regulated also by the Kansas Corporation Commission (KCC) with respect to retail rates, certain accounting matters, standards of service, and, in certain cases, the issuance of securities, certification of facilities, and service territories.

The utilities are also subject to regulation and oversight by the Federal Energy Regulatory Commission (FERC), North American Electric Reliability Corporation (NERC), and Southwest Power Pool, Inc. (SPP). Kansas City Power & Light has a 47% ownership interest in the Wolf Creek Generating Station (Wolf Creek), which is subject to regulation by the Nuclear Regulatory Commission (NRC), with respect to licensing, operations and safety-related requirements.

1.2.3 Project Location

The Project will deploy Smart Grid technologies on the KCP&L distribution system to the entire Green Impact Zone plus surrounding areas as shown in Figure 1-2. The total SmartGrid Demonstration Project area is approximately five square miles (www.kcplsmartgrid.com).

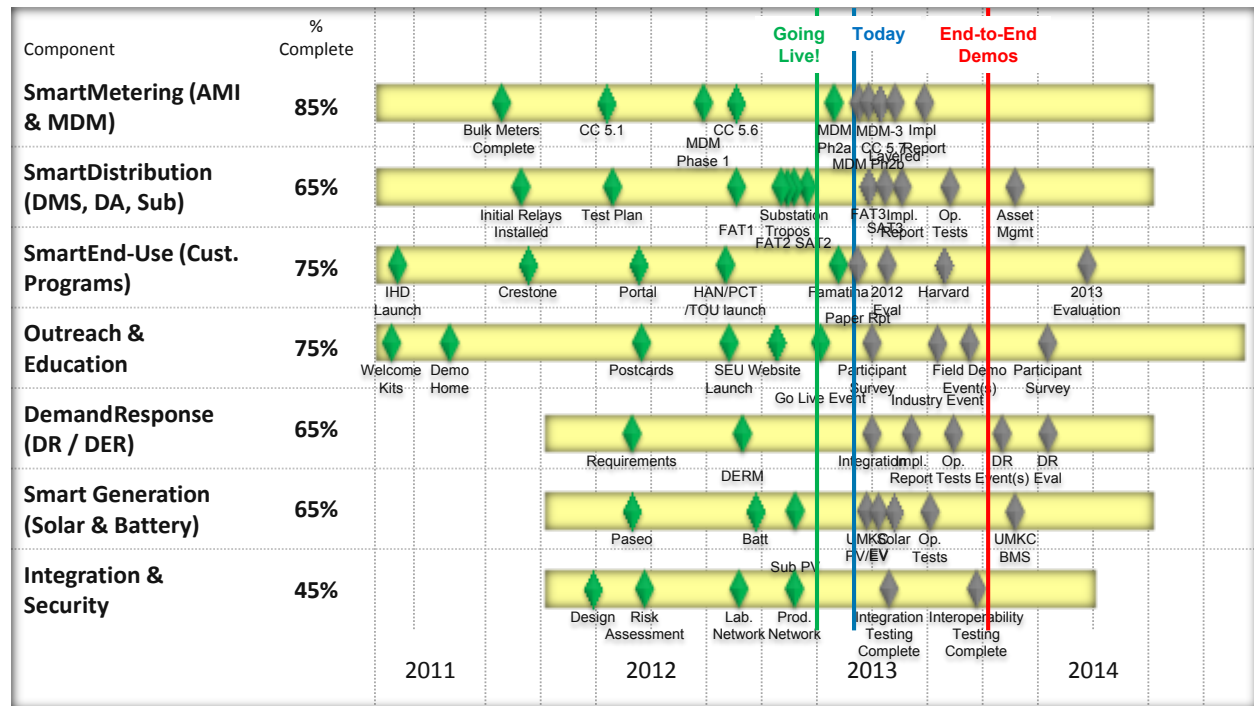
Figure 1-2: KCP&L Green Impact Zone SmartGrid Demonstration Map



1.2.4 Project Timeline

This section includes a condensed schedule of the KCP&L SmartGrid Demonstration Project. The schedule shown in Figure 1-3 includes main subcomponents of the project and shows their relative start and completion dates. Interdependencies between tasks are not shown on this schedule; however, the information is readily available within the Microsoft Project file that has been created for this project.

Figure 1-3: Project Timeline



1.2.5 Project Major Milestones

The master project schedule is aligned with the WBS; key project milestones for the project are listed in Table 1-4. During project performance, KCP&L will report the Milestone Status as part of the required monthly Progress Report as prescribed under the Reporting Requirements Checklist. The Milestone Status will present actual performance in comparison with the Milestone Log, and include:

- the actual status and progress of the project;
- specific progress made toward achieving the project’s milestones; and
- any proposed changes to the project’s schedule required to complete milestones.

The shaded milestones have been published by the DOE as external project milestones.

Table 1-4: Major Project Milestones

Task	Milestone	Planned Completion Date	Revised Completion Date	Actual Completion Date
1	Revised PMP to DOE for Review	10/29/2010		10/29/2010
2	NEPA Compliance obtained	10/28/2010		10/28/2010
3.2	Develop Initial Cyber Security Plan	10/29/2010		10/29/2010
4.4	Develop Benefits & Metrics Reporting Plan (v1.0 Submitted)	12/30/2010		12/30/2010
5.7.1	First Interim Technology Performance Report	12/31/2012		12/31/2012
5.7.2	Second Interim Technology Performance Report	12/31/2013		12/31/2013
6	Public Outreach and Education	06/30/2014		
	SmartGrid Demonstration Home Grand Opening			04/30/2011
	Innovation Park Grand Opening			10/12/2012
8.4	SmartMetering Deployment	03/18/2011		03/18/2011
8.5	SmartMetering System Acceptance	05/13/2011		05/13/2011
9.4	Collect Consumer 15 min Interval Usage Data	01/03/2012		03/31/2012
10.4	SmartSubstation Protection Network Factory Config. & FAT	12/21/2011		05/04/2012
10.7	SmartSubstation Automation Network Factory Config. & FAT	06/14/2012	08/30/2012	08/30/2012
10.10	Commission SmartSubstation (ready for day-to-day operations)	09/30/2012		09/30/2012
11.4	MDM Phase 1 – Implementation	12/30/2011		03/24/2012
12.10	DMS Factory Configuration and FAT	12/21/2011	08/30/2012	08/30/2012
12.14	Commission DMS System (ready for day-to-day operations)	07/10/2012	09/30/2012	09/30/2012
13.2	Design, Construct, & Test SmartDistribution IP FAN	09/30/2012		09/21/2012
13.6	Commission SmartGrid “First Responder” Subsystem	12/21/2011	08/31/2013	08/27/2013
14	Deploy SmartEnd-Use Implementation (14.2-4 & 14.6-9)	12/31/2012		06/30/2012
14.3	Implement Home Energy WEB Portal	12/08/2010		10/20/2010
14.4	Implement Home Energy EMS Web Portal	07/06/2011	07/31/2012	06/28/2012
14.5	Implement Home Energy DER Portal	07/06/2011	06/30/2014	
14.6.5	Launch In-Home Display	10/27/2010		10/27/2010
14.7	Demonstration Home Grand Opening	07/13/2011		04/30/2011
14.8	Launch EMS HAN Devices	04/30/2012		04/30/2012
14.9	Launch TOU Tariff	04/30/2012		05/22/2012
15	SmartGeneration Implementation	06/30/2014		
15.1	Deploy Grid Connected Roof-Top Solar	01/11/2012	09/30/2013	12/15/2013
15.2	Deploy DR (AMI) Thermostats (Available to Customers)			04/30/2012
15.5.16	Commission BESS	07/27/2012		06/28/2012
16	Smart DER/DR Management System Implementation	07/03/2014		
16.5	Implement & Unit Test DR Management Sub-system	06/30/2012	07/30/2012	07/27/2012
17.2	Conduct System-System Integration Testing	06/08/2012	07/31/2013	07/31/2013
17.4	Field Demo Integrated SmartGrid Functionality	12/31/2012	06/30/2013	06/28/2013
18.1	Operate System According to Program Plan & Procedures	10/01/2012		10/01/2012
18	Operate Integrated Solution (complete)	10/31/2014		
20.1.4	Submit Draft Report to DOE for Review	12/31/2014		

1.3 SmartGrid Demonstration Project Participants

KCP&L has developed a ‘distributed’ technical solution model working with a set of best-in-breed vendor participants. The vision for the SmartGrid Demonstration Project is to bring these technical implementation vendors and their capabilities together to develop leading edge, scalable SmartGrid solutions. In selecting participating vendors, KCP&L focused on companies with which we have established relationships, who are leading companies in their respective SmartGrid area, and who share the SmartGrid vision set forth in the Demonstration Project.

To further the cause of SmartGrid technology development, partners that have agreed to contribute in-kind to the effort have been classified and treated as project partners. In addition to these project partners, KCP&L will work closely with selected vendors to ensure a successful deployment of the Demonstration Project. These strategic partners and vendors are shown in Figure 1-4 and described below.

Figure 1-4: Selected Project Partners



1.3.1 Project Partners

In addition to providing equipment, technical expertise, and in-kind financial support, the project vendor partners will provide leadership on the technical and process aspects of the project, including the selection, implementation, and review of emerging technologies, and ensure that the project's vision is brought to bear through the collaboration of the project's partners and stakeholders.

1.3.1.1.1 Electric Power Research Institute (EPRI)

EPRI conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. EPRI will provide technical expertise and advice on defined portions of the project. In addition, they are a member of the five-year EPRI Smart Grid Demonstration Initiative, which is focused on Smart Grid projects that integrate distributed energy resources (www.smartgrid.epri.com). One of the main objectives of this initiative is to identify approaches for interoperability and integration that can be used on a system-wide scale to help standardize the use of DER as part of overall system operations and control. As part of this Initiative, EPRI will support this project in several areas including, but not limited to, cost-benefit analysis efforts, use case documentation per the IntelliGridSM methodology, data analysis and benefits estimation, CO₂ impact assessment and technology transfer.

1.3.1.1.2 eMeter/Siemens

eMeter's EnergyIP MDM solution is the industry's leading platform for real-time Smart Grid data management. Purpose-built for mass market deployment in heterogeneous and evolving technology environments, EnergyIP brings scalability, adaptability and flexibility to the utility enterprise. eMeter/Siemens will implement the EnergyIP product to provide an enterprise level repository of meter and metering data and support the provision of validated, estimated, and edited (VEE'd) AMI data.

1.3.1.1.3 Exergonix

Exergonix will leverage existing lithium polymer battery technology development and manufacturing expertise to develop and deploy a grid-scale energy storage system to supply peak-shaving, demand-management, and restoration capabilities to the KCP&L grid. The installation will function as part of a larger DERM system, controlled remotely and programmed to function automatically in conjunction with other SmartGrid components.

1.3.1.1.4 Intergraph

Intergraph is a strategic partner of Siemens Inc., together leading the industry with a number of active Smart Grid projects. Through the partnership, Intergraph and Siemens provide a Smart Grid Operations Command-and-Control Center that integrates an advanced distribution management system (DMS) with SCADA functionality, outage management, mobile workforce management and electric and communications infrastructure management.

Intergraph has also partnered with eMeter to integrate MDM functionality with their Command-and-Control Center platform. The integration will provide grid operators with consolidated end-to-end network visibility and management capabilities to provide utilities with the full operational benefits of their advanced metering infrastructure (AMI) and smart meter deployments for use in outage detection and response. KCP&L will be implementing Intergraph's Smart Grid Operations Command-and-Control Center integrated with Siemens DMS and eMeter's MDM.

1.3.1.1.5 Landis+Gyr

Landis+Gyr ranks as the worldwide leader in electricity metering with a preeminent position in advanced or "smart metering" systems. In 1994, KCP&L partnered with L+G (then Cellnet) to develop and deploy the first production AMR system in use by a utility. Today, L+G offers the broadest portfolio of products and services in the electricity metering industry including integrated AMM/AMI solutions,

communication systems and software, meters, meter data management, services and financing. KCP&L is again partnering with L+G to deploy a state-of-the-art Gridstream technology, AMI system and RF mesh AMI field area network.

1.3.1.1.6 OATI

Open Access Technology International (OATI) Inc. has been serving the energy industry since 1995 and has had steady growth since its inception. As a sub-recipient, OATI will deploy the Distributed Energy Resource Management (DERM) system component of the Demonstration Project through implementation of its webSmartEnergy application. The webSmartEnergy suites of applications are modular solutions to address the requirements for the emerging SmartGrid. OATI webSmartEnergy products include software and services for Demand Response and Distributed Energy Resources Management, Renewable Management, and Asset Management.

1.3.1.1.7 Siemens

Siemens is a world-wide provider of products and services whose experience spans the entire energy network, including generation, transmission, distribution, and the market. They focus on reliable, efficient, and practical innovation and implementation in each segment. As a sub-recipient, they will focus on providing the distribution network "First Responder" functions and the integration of the Distribution Management System (DMS) with SmartSubstation controllers and Distribution SCADA, as well as integration with the GIS, AMI, MDM and DERM systems.

Siemens plays a dual partner role in that they are both a sub-recipient and a vendor. As a vendor, Siemens will provide the SmartSubstation automation controllers, Distribution SCADA, Distribution Management System (DMS), and a variety of substation and field grid devices and IEDs. Siemens also teamed up with eMeter (and later purchased eMeter) to provide the MDM.

1.3.1.1.8 Tendril

Tendril offers solutions to aid customers in understanding, reducing, and managing energy consumption. Tendril will provide a residential Home Energy Management Portal (HEMP) and Home Area Network (HAN) platform which will provide energy consumers and utilities with an intelligent network of distributed energy resource management tools that will enable consumer and utility control through a single Web-based interface.

1.3.2 Consultants

1.3.2.1.1 Bridge Strategy Group

Bridge Strategy Group is an elite general management consulting firm used by KCP&L on numerous occasions on key strategic assignments. Bridge was retained to temporarily perform the Director of SmartGrid project functions and provide project level consulting services during the initiation phase in the form of guidance, expertise, and project support to the SmartGrid PMO.

1.3.2.1.2 Burns & McDonnell Engineering Company

Founded in 1898, Burns & McDonnell is a 100 percent employee-owned, full-service engineering, architecture, construction, environmental and consulting solutions firm with over 4,000 professionals in more than 30 offices. Burns & McDonnell will provide assistance to KCP&L in the form of skilled staff to augment the Project team.

1.3.2.1.3 IBM

IBM Global Services is the world's largest information technology services provider with professionals servicing customers in 160 countries. They are at the forefront of developing, integrating, and

implementing Smart Grid systems. IBM will provide assistance to KCP&L in the development of the project Interoperability and Cyber Security Plan.

1.3.2.1.4 The Structure Group

The Structure Group is an energy and utility consulting firm specializing in SmartGrid, energy management, risk management and competitive market solutions and will provide assistance to KCP&L in the form of skilled staff to augment the Project team, particularly in the role of IT integration.

1.3.3 Contractors

1.3.3.1.1 AOS

Alexander Open Systems (AOS) specializes in consulting, designing, implementing and supporting Local, Wide Area and Wireless Networking, Communication and Collaboration, Data Center, Physical and Data Security. AOS will provide assistance to KCP&L in the form of skilled staff to augment the IT project team.

1.3.3.1.2 Corix Utilities

KCP&L currently contracts with Corix Utilities to provide manual meter reading services for our non-AMR service territory. Corix has performed over 3,000,000 meter changes, AMR/AMI device installations and retrofits for gas, water and electric utilities since 1995, helping utilities make a smooth transition from traditional meter reading to automation. Corix has been retained to perform a pre-deployment audit of all electric meters in the SmartGrid Demonstration Project area.

1.3.3.1.3 Global Prairie

Global Prairie is an integrated communications and brand management company. Global Prairie will be providing education and outreach enrollment and soliciting volunteers to assist in these efforts.

1.3.3.1.4 MARC

The Mid-America Regional Council (MARC) provides administrative staff and services for the Green Impact Zone. The Green Impact Zone initiative is an effort to concentrate resources — with funding, coordination, and public and private partnerships — in one specific area to demonstrate that a targeted effort can literally transform a community. Plans are underway to make the Green Impact Zone a model for energy efficiency. Neighborhood leaders, the coordinating council, local utilities and other strategic partners intend to develop and implement a highly coordinated initiative to reduce energy and water usage within the zone — and, in the process, reduce utility bills for residents. The initiative will include individual property strategies as well as neighborhood-wide strategies, such as installation of a smart grid and the expansion of solar and other renewable energy sources within the zone.

1.3.3.1.5 Metropolitan Energy Center

The Metropolitan Energy Center's mission, when it was founded, was to assist people in the Kansas City region to manage and control their energy use. This nonprofit organization has evolved to become a catalyst for community partnerships focused on energy efficiency, environmental stewardship and economic improvement. KCP&L has partnered with MEC to integrate our SmartGrid Demonstration Home in their "Project Living Proof" demonstration. More information may be found at <http://www.kcenergy.org/community.htm>.

1.3.3.1.6 NextSource

NextSource is a global labor resource provider. NextSource will provide assistance to KCP&L in the form of on-site personnel in a variety of roles.

1.3.3.1.7 QTI, Inc.

QTI, Inc. offers turnkey solutions for general contracting needs. It is a corporation that provides general construction services along with fiber optic network build outs, underground power distribution and warehouse distribution. QTI, Inc. has been selected to manage the AMI meter deployment with a locally hired and trained workforce.

1.3.4 Vendors

1.3.4.1.1 Cisco

Cisco is the worldwide leader in IP-based networking products and solutions designed to implement truly intelligent information networks. A Cisco® Smart Grid network is a holistic, cross-technology solution that enables utilities and other organizations in the energy industry to build secure, standards-based IP networks to efficiently meet the demands of energy generation, distribution, storage, and consumption. KCP&L will extend our existing Cisco based network to support the SmartGrid Demonstration Project by implementing a new Cisco Smart Grid network as the foundation of the SmartSubstation.

1.3.4.1.2 Milbank

Milbank, headquartered in Kansas City, is an industry leader in the manufacture of electrical meter sockets and has been servicing the electric utility & wholesale distribution industries for over 75 years with innovative, quality engineered products. Milbank will be providing retrofit A-base meter enclosure covers to accommodate the larger physical dimensions of the AMI meters.

1.3.4.1.3 Oracle

Oracle is #1 in the worldwide relational database management systems (RDBMS) software market and holds more market share than its four closest competitors combined. The Oracle RDBMS is an integral foundation for many of the SmartGrid demonstration system components to be implemented.

1.3.4.1.4 Ruggedcom

Ruggedcom designs and manufactures rugged communications equipment for harsh environments such as substations and other outdoor applications. KCP&L will use Ruggedcom network components to implement half of the redundant SmartSubstation IP based protection network.

1.3.4.1.5 Schweitzer Engineering Laboratories (SEL)

SEL makes electric power safer, more reliable, and more economical. To accomplish this mission, they design, manufacture, and support a complete line of products and services for the protection, monitoring, control, automation, and metering of electric power systems. KCP&L will replace existing electromechanical relays with new SEL feeder relays in transforming the Midtown substation to a next generation SmartSubstation.

1.3.4.1.6 SISCO

The SISCO ICCP product is being used to integrate the Intergraph and Siemens products. The ICCP-TASE.2 (IEC60870-6) is the internationally accepted standard for the exchange of real-time data in energy utilities for control center integration.

1.3.4.1.7 Tropos

Tropos provides wireless communications networks for utilities to build and control the Smart Grid. Tropos will provide the wireless, IP-based mesh network for distribution automation.

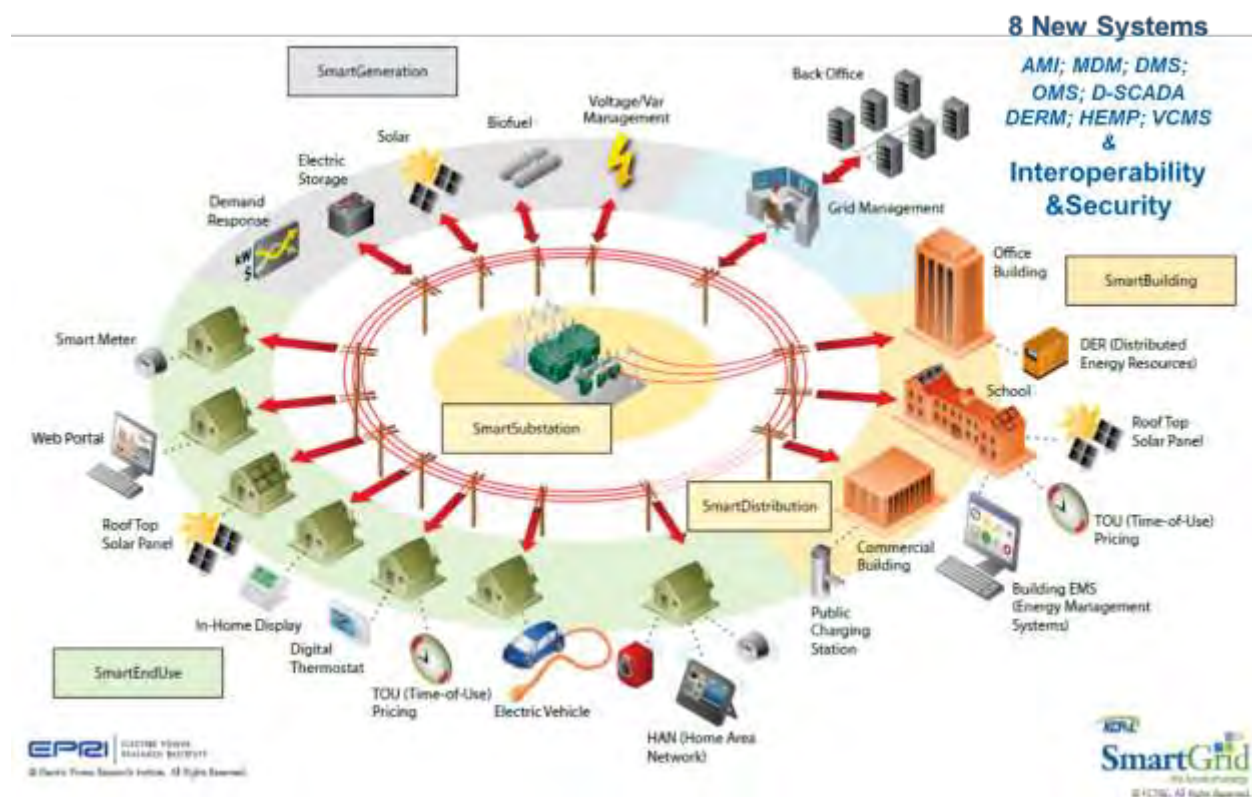
1.4 Demonstration Systems & Technologies

The KCP&L SmartGrid Demonstration Project will demonstrate the value of integrating Smart Grid technology, communications and control systems to manage the distribution system in cooperation with distributed energy resources within a utility's service territory. In particular, we are targeting distributed, edge-of-grid, resources using a comprehensive next generation Smart Grid infrastructure to integrate and manage the distributed grid assets. Not only will the distributed energy resources be aggregated, visible, and available to the energy traders and bulk grid operators, they will also be available to the DMS and distribution operators as a tool to solve local congestion or power quality issues. Ultimately, individual or circuit aggregated resources can be initiated automatically by the distributed substation controller (DCADA) as one of its "First Responder" functions.

1.4.1 Demonstration Systems Overview

The KCP&L SmartGrid Demonstration Project focuses on the Company's Midtown Substation and multiple distribution circuits serving approximately 14,000 customers across 3.75 square miles with total demand of up to approximately 69.5 MVA. Our scope of work, illustrated in Figure 1-5, touches every functional area of the electricity distribution network.

Figure 1-5: KCP&L Demonstration, a True End-to-End SmartGrid

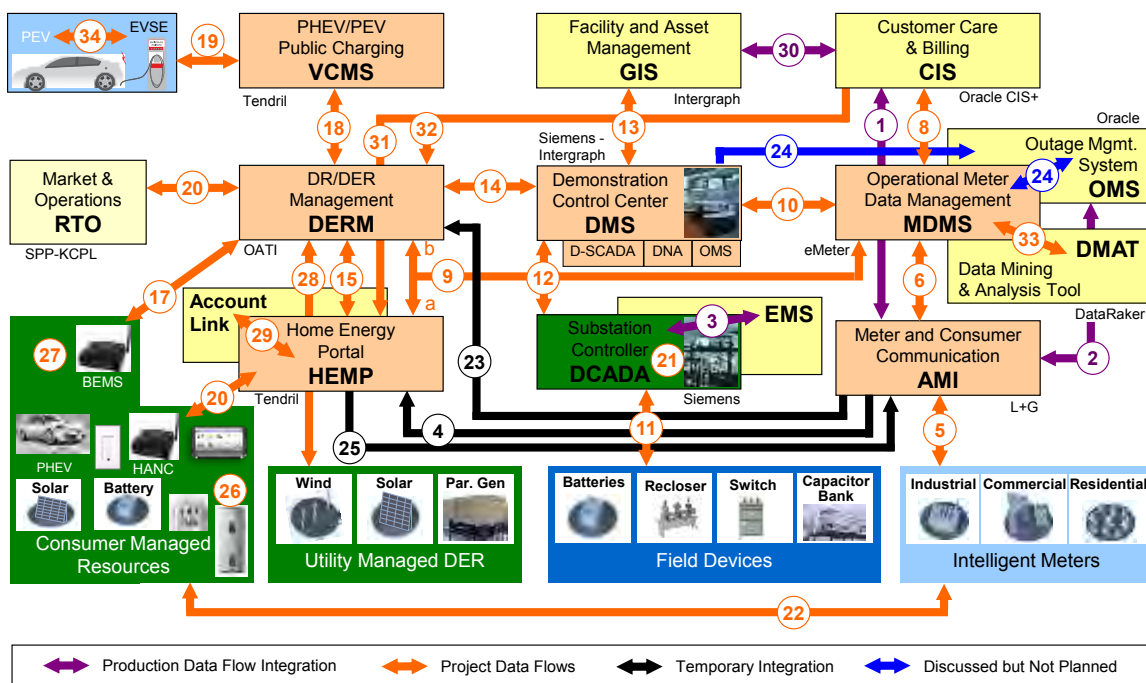


The SmartGrid pilot infrastructure includes a distribution grid control system that consists of five major components as shown in Figure 1-6 below. The grid control infrastructure is a "stand-alone" system for the Demonstration Project, but it is used to control the grid as part of normal day-to-day operations within the Demonstration Project area.

The pilot infrastructure components include:

- **Distribution Management System.** This provides all the necessary systems and applications for the KCP&L Control Center Operators to manage the distribution network reliability, quality of supply, coordinate with substation controllers and field automation, and enhance efficiency of the operations, crew and maintenance staff.
- **Distributed Control and Data Acquisition.** This DCADA includes the SmartSubstation control functions and the automation of reclosers, switches, and capacitor banks to support communication with Smart-Substation™ Controllers for automated feeder reconfiguration.
- **Advanced Metering Infrastructure and Meter Data Management.** This supports two-way communication with electronic meters for consumer billing information, verification of electrical service status, and remote service on-off capabilities.
- **Distributed Energy Resource Management.** This provides balancing of renewable and variable energy sources with controllable demand as it becomes integrated in the utility grid, coordination with market systems, and provision of pricing signals to consumers.
- **Home and Vehicle Energy Management.** This enables customers to make informed consumption decisions and allows consumer managed resources to participate in proactive utility grid management programs.

Figure 1-6: KCP&L Demonstration, T&D Control Systems Infrastructure



As depicted in Figure 1-6, there are four (4) integration points with existing systems; GIS, CIS, OMS, and EMS/SCADA.

- **GIS** – will continue to be the source of facility and network connectivity information.
- **CIS** – will continue to be the source of customer information and will continue to provide billing functions for customers on existing rate structures.
- **OMS** – will continue to be the production system for analysis of customer outage information for manual dispatch. The DMS will process outage calls for automated restoration and demonstration purposes.

- **EMS/SCADA** - will continue to have control authority over the distribution functions for which it currently controls, primarily distribution feeder breakers. DMS will have control authority over all new control functions.

This pilot infrastructure creates the next-generation grid monitoring and control platform that is being used to manage the KCP&L Green Impact Zone SmartGrid Demonstration grid for project duration.

The DMS and DCADA provide the operational backbone of the system supporting significant levels of automation on the feeders, complex and automated feeder reconfiguration decisions, and tightly integrated supervision with the Control Centers. The DMS serves as the primary point of integration for the grid facilities, electrical system load, and real-time substation and feeder information. It includes Distribution Supervisory Control and Data Acquisition (D-SCADA), Distribution Network Analysis (DNA), Outage Management (OMS) and integration with KCP&L's existing Mobile Work Force Management system, Geographic Information System (GIS), and other supporting systems.

The Smart-Substation™ controller establishes an intelligent substation IT infrastructure with the ability to make feeder and substation reconfiguration decisions, control field equipment, verify operations, track local grid capacity, and coordinate with the DMS. This “proactive” management of the distribution grid is a necessary step in preparing for the integration of significant levels of renewable and variable energy resources, controllable demand, and demand response. With the addition of distributed energy resources, the DMS and Smart-Substation™ become essential to managing Volt/VAR conditions, adaptively modifying protection equipment settings, and managing crew safety.

The AMI and MDM provide access, collection, and management of meter asset information and the consumer metering information for billing, consumer awareness and consumer participation in demand management and response programs or the market. They will be deployed to all customers in the KCP&L Green Impact Zone SmartGrid Demonstration Project area, including residential, commercial and industrial consumers. They will collect the customers' 15 minute interval consumption data required to support many of the SmartGrid analyses to be performed and the experimental TOU rates and other EE/DR incentives to be evaluated. Additionally, the MDM will manage the flow of events and other data flows between the legacy CIS and OMS and the demonstration DMS/OMS and DERM systems and provide an avenue for integration with selected Home Area Network (HAN) management systems.

The DERM system provides all the necessary functions to balance distributed energy resources with available dispatchable (“controllable”) demand to make most efficient use of existing energy options while optimizing economic value for consumers in the market. It aggregates distributed energy resources and controllable load groups for dispatch and market participation with group and, potentially, demographic leverage. It assesses balancing within a defined future time period (i.e. 5 minutes) and issues commands to participating resources to adjust their output and/or demand where appropriate. Excess resources can be bid into the market. The system tracks aggregate and individual resource commitments and settles accounts. It uses available load models and network conditions from the DMS as constraints to ensure reliable network operation, request network control changes and verify resource participation. It accepts requests from the DMS to suspend dispatch of energy resources in areas where operational safety conditions are at risk. It will use consumption information from the AMI and MDM systems to verify demand management/response participation. It will track, retain, and report all information necessary to quantify resource and related economic participation.

All these systems assume an underlying standards-based infrastructure of communications, field automation, and end-to-end cyber-security. The demonstration systems are fully integrated using the standards defined by the NIST Smart Grid Interoperability Framework, where applicable, and interface with existing production systems at KCP&L at clearly defined and controlled integration points to maintain the security and integrity of KCP&L enterprise systems. As a whole, the program is verifying a full range of NIST and other standard modeling and information exchange protocols necessary to

implement a functional, cost-effective, secure intelligent grid. The project has helped define, validate, and verify the necessary parameters and potential solution adjustments for KCP&L, and the industry, to plan and implement a system wide roll-out of the successful Smart Grid technologies and processes.

Several fundamental aspects of next generation Smart Grid T&D Infrastructure are being demonstrated and verified in this project, including:

- State-of-the-art multi-transformer, multi-bus distribution substation upgrade
- SmartSubstation with IEC61850 communication protocols over a secure IP Ethernet substation LAN
- Highly-integrated, distributed hierarchal control solution between a centralized DERM system, DMS/SCADA system, a distributed DCADA controller within the SmartSubstation, and individual IED field controls
- Automated “first responder” distributed decision making through intelligent substation controllers and enabled feeder devices
- Dynamic equipment ratings based on field conditions
- Integrated supervision of automation and filtering of field information to improve distribution operations situational awareness
- Integration of distributed and renewable energy resources and controllable demand
- Availability of customer demand response, price signals, and market participation
- Two-way accessibility of the customer meter, availability of current energy usage information, and customer participation in energy programs
- A comprehensive SmartGrid communications infrastructure
- End-to-end cyber security provisions

The following subsections describe the various sub-projects of the Demonstration Project.

1.4.2 SmartMetering

The SmartMetering sub-project deployed a state-of-the-art integrated AMI and MDM. AMI deployment consisted of replacing all customer meters within the Demonstration Project area (approximately 14,000 meters) with communicating SmartMeters and installing an accompanying wireless two-way communication network to enable real-time communications between the meters and the MDM. The MDM stores and manages all meter data reported by the SmartMeters and is integrated with KCP&L’s other systems including the CIS, DMS, OMS, and the DERM.

The SmartMeters lower operating costs, increase the frequency of meter reads, increase the accuracy of meter reads, and facilitate utility-controlled demand response messaging. Customer satisfaction will be improved through remote service connect/disconnect, on-demand meter reading, and increased customer access to usage information. Furthermore, overall system reliability has been increased through enhanced outage/restoration notification.

1.4.2.1 Advanced Metering Infrastructure (AMI)

1.4.2.1.1 AMI Overview

The Landis+Gyr Gridstream SmartGrid communication system and SmartMeters provide the capability for AMI and Home Area Networks (HAN) via a common two-way communication infrastructure. The system supports the acquisition of load profile, time-of-use and demand meter data, and meter and site diagnostic information from the electric meters that perform these measurements. Using meters equipped with these capabilities, the system also supports “under-glass” remote physical disconnect and HAN communication via the ZigBee-standard Smart Energy Profile. SmartMeters also support outage and restoration reporting and real-time on-demand reads.

1.4.2.1.2 AMI Characteristics

The AMI is composed of two main components: Command Center – the AMI Head-End System (AHE) and the Gridstream Wireless Field Area Network (FAN). The AHE is the software and hardware that allows the utility to interact with the AMI and integrate the AMI with other systems within the utility. The FAN is the hardware (collectors, routers, and meters) that enables the utility to receive meter data and send commands to meters.

1.4.2.1.2.1 **Command Center – The AMI Head-End System**

The AHE is the advanced metering software and hardware platform that enables data reporting and system control between itself and the FAN. The scalable system enables KCP&L to remotely program meters, manage remote connects/disconnects, analyze critical peak usage, view load control indices, and perform other critical, day-to-day functional operations. The AHE simultaneously manages the meter data collected from all SmartMeters within the Demonstration Project area, validating each data element, and integrates the data with the MDM. The AHE is compliant with the Multispeak, CIM, and IEC 61968 standards. The AHE utilizes Web Service APIs to interface with other systems and can deliver specific scheduled data extracts to these systems.

1.4.2.1.2.2 **Gridstream Wireless Field Area Network**

The Landis+Gyr Gridstream wireless FAN provides full two-way wireless mesh communication and functionality to electric meters, direct load control devices, advanced distribution automation (ADA) devices and Home Area Network devices enabled with a ZigBee communication module.

Advanced metering and diagnostic information that electric meters provide can be communicated over the network to the Command Center head-end operating system and displayed, reported and interfaced to the MDM, CIS, OMS and other enterprise applications. Figure 1-7 shows a schematic of the Gridstream System for AMI, ADA and Meter-to-HAN Gateway.

Figure 1-7: AMI RF Mesh FAN



1.4.2.1.2.3 Smart Meters

Features of the SmartMeters within the AMI include:

- Full Two-way Mesh Radio AMI Communications
- Variable Output Power
- Auto-registration
- ANSI C12.19 Tables support
- Forward, Reverse, Net, Total Energy
- Voltage/Power Quality Information
- Downloadable Firmware
- Advanced Metering: Demand/TOU/Load Profile
- 5/15/30/60-minute Interval Data Recording
- Data Storage
- Outage and Restoration Notification
- Integrated Service Connect/Disconnect
- Load limiting
- ZigBee Smart Energy Profile HAN Interface
- Reactive Energy & Power Factor (commercial meter only)

1.4.2.1.2.4 HAN Communications via the AMI

The AMI supports HAN applications via the ZigBee-standard Smart Energy Profile using the SmartMeter to manage the HAN. This allows KCP&L to communicate usage information, pricing information, and text messages with ZigBee-compliant in-home devices, such as In-Home Displays (IHDs), Programmable Communicating Thermostats (PCTs) and HAN Gateways.

Figure 1-8: Communication Flow from the AHE to the HAN via the FAN



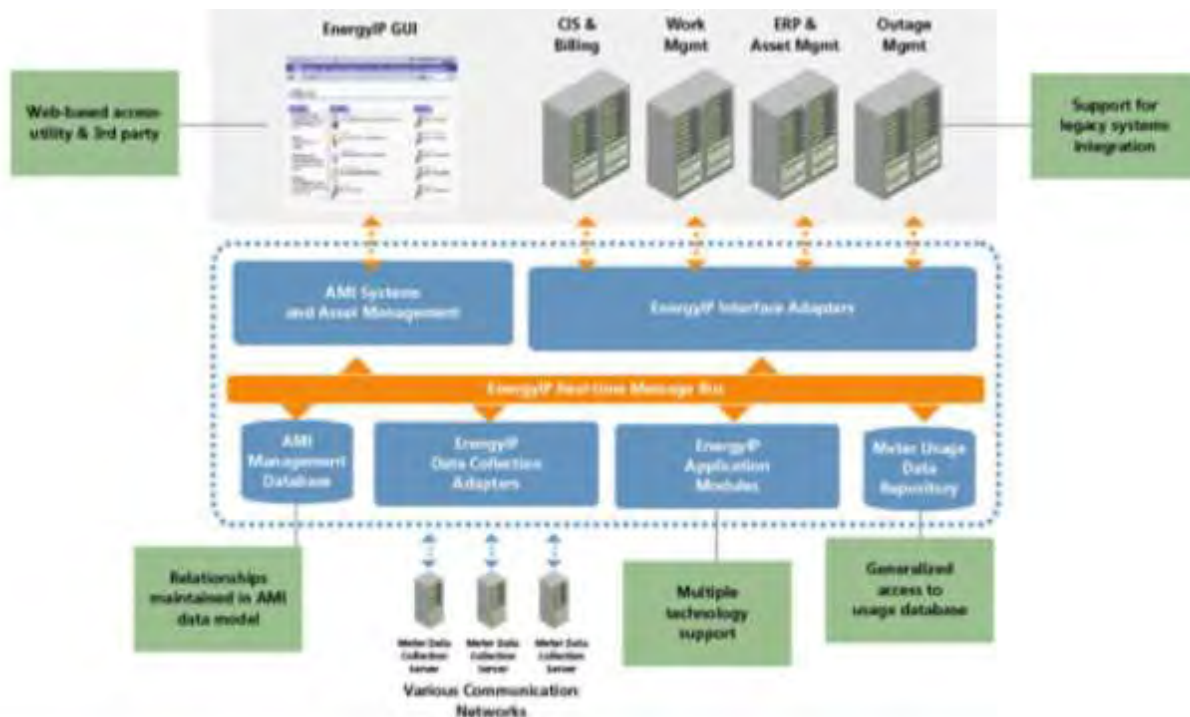
1.4.2.2 Meter Data Management (MDM)

The Meter Data Management System (MDM) provides access, collection, and management capabilities of the consumer metering information for all customers in the KCP&L Green Impact Zone SmartGrid Demonstration Project area, including residential, commercial and industrial consumers. It stores the customers' 15-minute interval consumption data and daily register read data which is then available to support SmartGrid data analytics and billing for the TOU Billing Pilot Program rates launched in 2012. Other EE/DR incentives may be evaluated using this data in the future. Additionally, the MDM manages the work flow of events and other requests between the legacy CIS and AMI infrastructure for Remote Service Order handling as well as integration between the AMI and the demonstration OMS for outage analysis. Future avenues for integration may include the demonstration DMS/OMS systems, DERM system and selected Home Area Network (HAN) management systems.

1.4.2.2.1 *MDM Overview*

The eMeter EnergyIP MDM provides the capability for receiving and storing meter interval and register data from the AMI system. Services such as Validation, Estimation and Editing (VEE) are provided as part of the data storage process to ensure a high level of data completeness and data quality. The EnergyIP platform supports integration with CIS for data synchronization, remote service order processing (i.e. Connects, Disconnects, and On-Demand Reads) and calculation of billing determinants from interval data for use in TOU billing and other advanced billing programs. Additional integration is provided with the AMI infrastructure to capture and manage meter events including outages and restorations generated from the AMI which are then sent downstream to systems, such as the OMS, for further processing.

Figure 1-9: MDM Integration Overview



1.4.2.2.2 *MDM Characteristics*

This section describes the major characteristics of the MDM system which are being leveraged by KCP&L as part of the SmartGrid Demonstration Project.

1.4.2.2.2.1 **AMI Data Store**

The MDM's AMI Management Database is the data store that maintains the complex relationships among the meter, account, premise, service point, communications node, AMI infrastructure, and the application services under the direction of the AMI Systems and Services Manager. The AMI Management Database includes all the AMI systems and services management data, object relationships, and histories. This database contains records for assets, premises, accounts, meters, services, service requests, activities, activity outcomes, and more. This database tracks not only the current status but also the historical relationships.

The EnergyIP Data Synchronization Engine (DSE) will use the FlexSync process to manage the synchronization of data maintained in the AMI Data Store data with the CIS, and other core utility business systems. FlexSync provides incremental, transactional based approach to synchronizing data

and ensures that any changes in data elements or relationships such as meter changes, rate changes, move-in move outs, and other changes to customer premise or service delivery point information are identified and reflected in EnergyIP.

1.4.2.2.2 Meter Usage Data Repository

At the core of the MDM's capabilities is the ability to store large amounts of meter-generated data. The Metered Usage Data Repository (MUDR) is the data store that maintains the meter readings, register reads, interval records, outage and restoration events, and event logs. The MUDR also maintains derived or computed data.

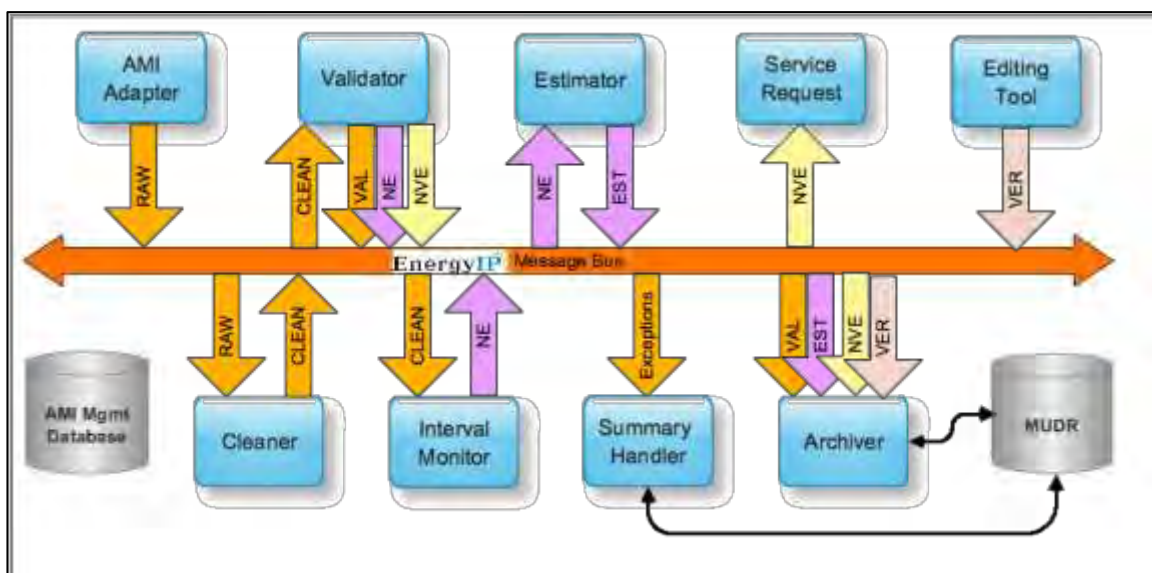
For the KCP&L Demonstration Project, this includes daily register reads and 15-minute interval reads for the 14,000 AMI meters deployed to the Demonstration Project area, or roughly 1.3M interval reads per day to go with 14,000 register reads. Once in the MDM repository, the MDM can provide aggregations of data across various levels including circuit, feeder, substation and transformer. It can also export this VEE'd data for use in downstream systems such as the Data Mining and Analysis Tool (DMAT), Distributed Energy Resource Manager (DERM) and Home Energy Management Platform (HEMP).

The MDM also provides storage for all historical meter read data from the beginning of the SmartGrid Demonstration Project AMI-rollout in October 2010; full history will be retained for the duration of the Demonstration Project for each meter. This is a significant improvement over what would otherwise be available from the AHE or meters themselves.

1.4.2.2.3 Validation, Estimation & Editing

The MDM delivers Validation, Estimation, and Editing (VEE) capabilities that provide estimations for missing intervals, and ensure more reliable, accurate interval data posted to the Meter Usage Data Repository. The Validation module performs validation according to user-configurable rules associated with each data stream; these validations include checks for usage spikes, reverse rotation, etc. Where possible, the Estimation module will follow a defined set of rules to extrapolate and interpolate interval data as well as to estimate register read data when the data is not received from the AMI. There are times when the Validator determines that the interval data needs manual verification and editing and/or

Figure 1-10: MDM Interval VEE Workflow



when the Estimator is unable to provide a valid estimate. For these instances, manual editing via a tabular or graphical view is available within the MDM. In all cases, the MDM also tracks versioning of data when estimation and editing are taking place and provides audit trails for data manipulations.

1.4.2.2.4 Usage Framing

The MDM can support multiple usage framing configurations based on a utility's needs. This "framing" sums up a customer's interval data over a specified period of time into a total usage amount for that period and stores it in the appropriate "bin". For example, KCP&L's Time-of-Use (TOU) Billing Pilot Program has established a framing schedule that, on non-holiday weekdays, sums all 16 of a customer's 15 minute interval values between 3PM-7PM to create a "peak" usage bin and the remaining 80 daily interval values between 12AM-3PM and 7PM-12AM to provide an "off-peak" usage bin. For weekends and holidays, all 96 daily intervals are added to the "off-peak" total. The schedule is further split into summer vs. winter seasons – during the winter, all usage is added to the "off-peak" bin. As the MDM can support multiple framing configurations, when KCP&L considers additional custom programs in the future such as critical peak pricing, EV charging (aka super-off-peak pricing), or simply different TOU schedules, these can all be set up in the MDM for framing into the appropriate usage bins. Each of these framing programs can also be configured to be setup on specific subsets of customers which further enables the utility to deliver advanced billing solutions to its customers.

Figure 1-11: Usage Framing for TOU

Season	ProfileID	Weekday	TOU BIN	Season	ProfileID	Weekend	TOU BIN	Season	ProfileID	Holiday	TOU BIN
Winter	1	00:00-08:00	1	Winter	1	00:00-00:00	1	Winter	1	00:00-00:00	1
		08:00-21:00	3								
		21:00-00:00	1								
Summer	1	00:00-08:00	1	Summer	1	00:00-00:00	1	Summer	1	00:00-00:00	1
		08:00-12:00	3								
		12:00-18:00	2								
		18:00-23:00	3								
		23:00-00:00	1								

1.4.2.2.5 Billing Determinant Calculator

The MDM Billing Determinant Calculator provides the flexibility to compute the billing determinant values based on utility defined formulas. Formulas are built around logical and arithmetic operators, and can contain other billing determinants, constants, and customer functions. In addition to traditional billing, MDM billing determinant calculator can support various advanced billing programs such as TOU billing, critical peak pricing, EV charging rates, etc. as desired by the utility.

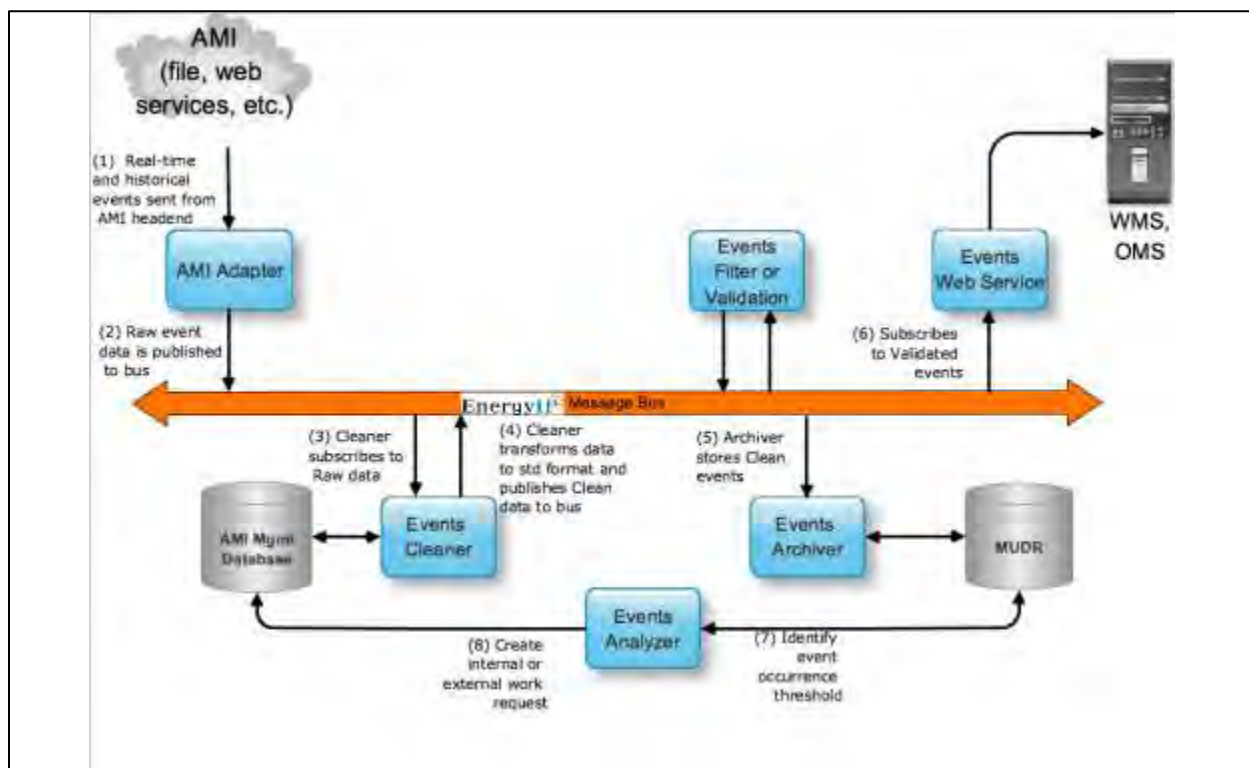
The MDM provides a variety of methods to calculate and deliver billing determinant information to a utility's CIS system. This can be done in a batch format that matches bill cycles / billing routes and delivers a customer's total usage for the month or at various other more customizable levels. The billing determinants can be delivered in both a "Push" method where the MDM produces and delivers a file on a set schedule or in a "Pull" method where the CIS system makes the request for data to the MDM and receives the necessary response back

KCP&L is currently using a modified version of the Pull Billing process to support its TOU Billing Pilot Program. The TOU rate schedule (summer/winter seasons and on-peak/off-peak times) and rate programs (1TOUA for standard customers and 1TOAA for all-electric customers) are set up in the MDM to drive usage framing as noted above. This framed usage is then retrieved via an “off-cycle”, “informational” request to the MDM Pull Billing interface. This type of request supports KCP&L’s daily retrieval of the on-peak/off-peak bin values for TOU customers. These daily usage values are then processed through KCP&L’s SmartGrid middleware which converts them to virtual daily dial values for each TOU bin. These values are then fed into the CIS system when needed for monthly bill cycle processing.

1.4.2.2.6 Meter Event Management

In addition to meter readings and usage information, the MDM also is a repository for meter events such as outages, restorations, alarms (i.e. tampering) and operational activities (i.e. demand resets). MDM provides the capability to interface with the AMI to collect event messages generated directly by the meter for outage, restoration, tamper and diagnostic issues. Service order based events are also tracked and stored in the MDM system for activities including remote connects, remote disconnects and on-demand reads. MDM has the ability to generate reporting on these events as well.

Figure 1-12: MDM Event Handling Overview



With the exception of the outage/restoration events which are described in more detail below, KCP&L is currently capturing and storing event messages in the MDM; future projects may build additional interfaces and reports to utilize this information. Events being tracked in the MDM are listed in Table 1-5.

Table 1-5: MDM Events Tracked

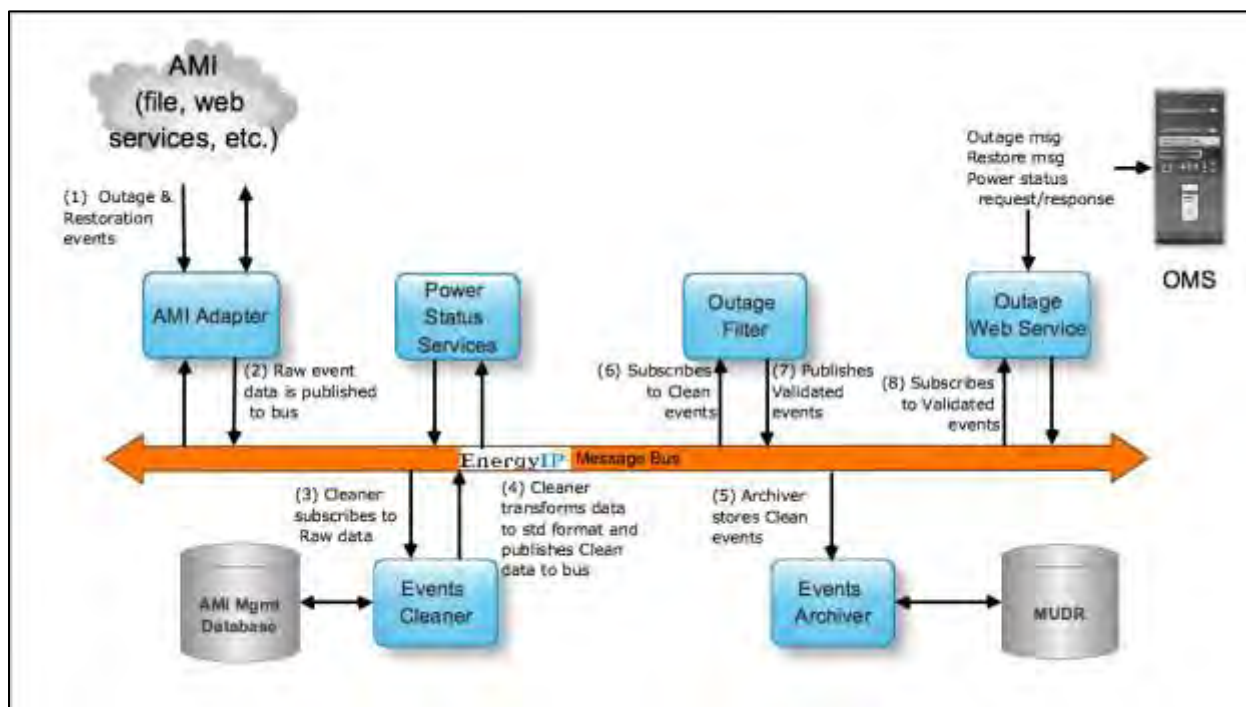
Event Number	Event Description
3.18.1.199	RAM Failure Detected event mapping
3.18.1.220	ROM Failure Detected event mapping
3.2.1.149	Meter Battery Low event mapping
3.21.1.173	Non-volatile Memory Failure Detected event mapping
3.21.1.213	Meter Reprogrammed event mapping
3.21.1.52	Fatal Error
3.21.1.79	Measurement Error Detected event mapping
3.21.1.81	Event Log Cleared event mapping
3.21.1.95	History Log Cleared event mapping
3.21.18.79	Self-Check Error Detected event mapping
3.21.7.79	Meter Configuration Error event mapping
3.33.1.219	Reverse Rotation Detected event mapping
3.33.1.257	Tamper Attempted Suspected event mapping
3.8.1.61	Meter Demand Reset Occurred event mapping

1.4.2.2.7 Outage Event Management

As noted above, the MDM receives outage and restoration events generated from the AMI system. The EnergyIP MDM has a number of additional functionalities that provide outage related information, collectively referred to as the Outage Management Support Module (OMSM). The OMSM delivers outage events received from the AMI system to the utility's Outage Management System (OMS) in an intelligent manner.

Once outage events are received by the MDM, configurable business rules can be applied to filter the raw outage information prior to transmitting it along to the OMS system. These filtering rules include

Figure 1-13: MDM Outage/Restoration Event Handling



managing the time stamps on events that may be transmitted multiple times to prevent the repetitive messages from having to go downstream to the OMS as well as monitoring for de-bouncing scenarios where the outage and restoration come into the MDM in a very short time span. The MDM also provides a bellwether capability as well as critical infrastructure monitoring capability for designated meters; neither of these functions are being used currently by KCP&L in the MDM. The MDM workflow can also provide integration support for Power Status Verification requests made by the OMS system and transmitted down to the AMI through the MDM.

The outage and restoration events configured in the KCP&L MDM are listed in Table 1-6.

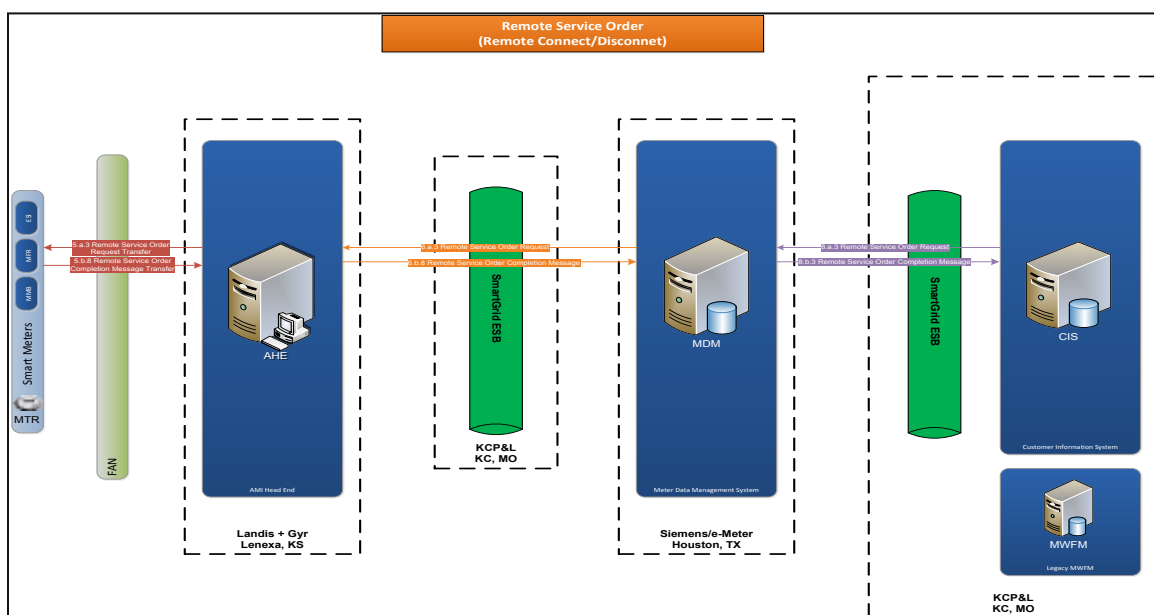
Table 1-6: Outage Restoration Events

Event Number	Event Description
3.26.9.185	Endpoint Power Outage
3.26.9.216	Endpoint Power Restore
3.26.17.185	Primary Power Down
3.26.17.216	Primary Power Restore

1.4.2.2.8 Remote Service Orders

The MDM provides the capability for integration with the CIS and AHE systems to provide workflow management for various service orders, including remote connects, remote disconnects and on-demand reads (ODR). As part of this integration, MDM receives a single order from the CIS and breaks it down into the appropriate components – i.e. disconnect and ODR or reconnect and ODR – to be sent down to the AHE in the appropriate order. As part of the workflow, the MDM will send the initial request (i.e. ODR) to the AHE and then wait for the response prior to sending the second part of the service order (i.e. disconnect) down to the AHE. Once the necessary responses for all messages in the workflow are received from the AHE, the MDM then packages them into a single response that is then sent back to the CIS for processing. In addition to supporting integration with the CIS for these order types, the MDM also supports manual entry (if needed) of these service requests directly in the MDM.

Figure 1-14: MDM Remote Service Order Handling Overview

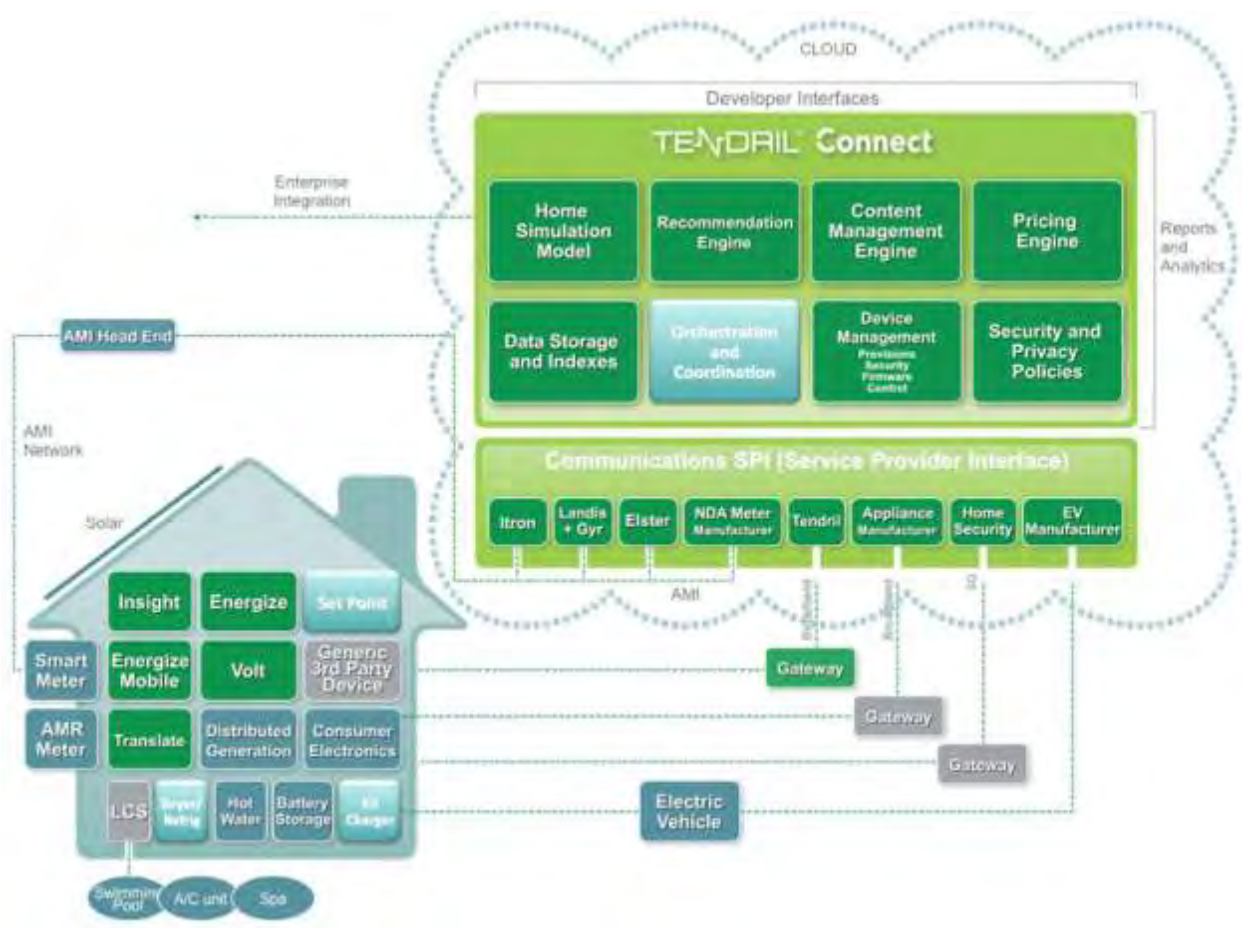


1.4.3 SmartEnd-Use

The SmartEnd-Use sub-project deployed a Home Energy Management Platform (HEMP) and Time-of-Use (TOU) rate plan to increase customer adoption of consumption awareness and management techniques, as well as expand KCP&L's demand management capabilities. Together, the HEMP and TOU rate enable customers to directly manage their energy consumption and associated costs. Furthermore, the HEMP provides KCP&L with demand response assets that can be called on during peak demand times to help increase distribution grid stability and decrease operating costs.

A smart grid contains advanced technology that enables enhanced, two-way communication between a utility and its customers. The HEMP provides KCP&L a means to monitor customer involvement, communicate billing and consumption information to customers, and manage demand response assets. In turn, the HEMP provides customers with information to understand their energy consumption and costs and tools to help manage both. The HEMP enables KCP&L to implement and evaluate several technologies that facilitate both indirect and direct load control by providing customers with energy education tools and in-premise Home Area Network (HAN) devices, thus empowering customers to better manage energy consumption and costs. These tools also serve the added benefit of preparing customers for dynamic pricing as well as a means for utilities to communicate pricing signals and billing information.

Figure 1-15: Tendril™ Connect Platform Architecture



The HEMP is a system that interfaces with other back-office systems to exchange various data, including energy consumption, billing plans, demand response events and information about various in-premise Home Area Network (HAN) devices. The HEMP is composed of two main components: 1) a web-based portal that provides KCP&L with access to manage customer accounts and devices and provides customers with access to their historic energy usage information and tips for managing energy consumption, and 2) the ability to manage the in-premise HAN devices, monitor real-time usage, and set preferences for responses to demand response events and pricing programs. KCP&L uses the Administrative Portal to monitor and manage Customer Portal accounts and HAN devices. The Customer uses the Customer Portal to view their energy consumption, billing plans, and demand response events and manage their in-premise HAN devices.

1.4.3.1 Customer Web Portal

1.4.3.1.1 Customer Web Portal Overview

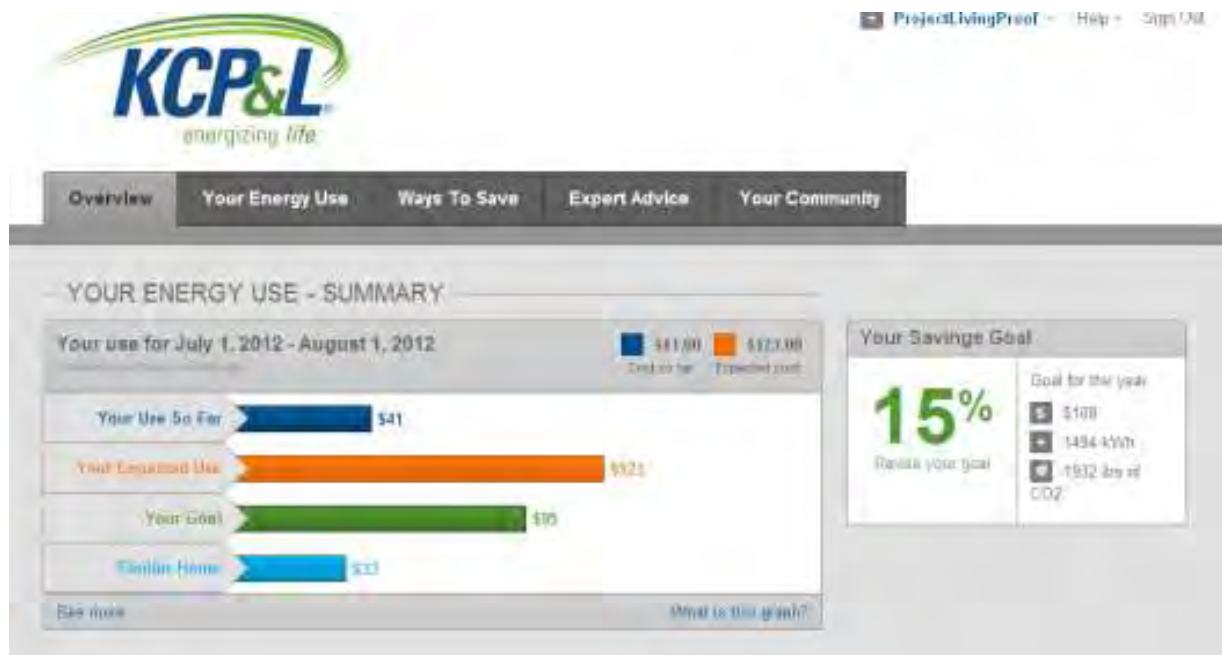
The Customer Web Portal is a full featured informational web portal that is designed to give customers access to their detailed energy usage and help them better understand the impact of their electricity usage on their bills. It also provides additional recommendations and information to encourage them to make decisions that conserve energy, help the environment, and save money.

1.4.3.1.2 Customer Web Portal Characteristics

KCP&L's Customer Web Portal, shown in Figure 1-16, is designed to show a customer how much and when they use electricity each day and help them estimate their bill, including taxes and charges, before they receive it.

Traditionally, electricity customers have used energy without knowing how much money they were spending and when. Now, for example, on a hot summer day customers will be able to see exactly when usage goes up. This information may influence customers to use electricity differently at those times and receiving it in near real-time through in-premise HAN devices facilitates immediate action to manage energy consumption and costs instead of waiting for a monthly bill to see this information.

Figure 1-16: Customer Web Portal



The Customer Web Portal allows customers to:

- See energy usage information in easy-to-understand charts
- Estimate their current monthly bill
- Compare this month's bill against last month's bill
- Evaluate hourly, daily, and monthly electricity usage amounts
- Review yearly billing history
- Compare their usage against other homes in their community
- Receive messages from KCP&L about their usage

1.4.3.2 In-Home Display (IHD)

1.4.3.2.1 IHD Overview

The In-Home Display (IHD) is a portable electronic device that provides real-time energy usage information to customers directly from their meter to increase awareness of electricity usage and help identify opportunities to reduce consumption and save money. The IHD receives information directly from a customer SmartMeter and presents it to them in easy-to-understand screens.

1.4.3.2.2 IHD Characteristics

The IHD communicates with the SmartMeter wirelessly via an IEEE 802.15.4 network running the ZigBee Smart Energy Profile (SEP) 1.0 specification to receive real-time energy consumption data, pricing signals, text messages, and estimated billing information. The IHD does not require an Internet connection.

The IHD, shown in Figure 1-17, provides customers with:

- Current electricity usage information
- Current electricity costs
- Important text messages from KCP&L
- Up-to-date current month usage and estimated billing information

The IHD allows a customer to set a price limit on how much electricity they want to use for the month. It will then visually notify customers with green, yellow, and red backlighting indicating whether they are meeting, nearing, or exceeding that limit. The IHD only receives and displays energy usage information and does not directly affect customer energy consumption; it simply sends warning signals to influence energy consumption in order to meet the customer-imposed limits, thus enabling customers to manage their consumption and costs.

Figure 1-17: In-Home Display



1.4.3.3 Standalone Programmable Communicating Thermostat (PCT)

1.4.3.3.1 Standalone PCT Overview

The Standalone Programmable Communicating Thermostat (PCT) is an electronic device that receives information directly from a customer SmartMeter to allow customers to participate in utility-initiated demand response events. The Standalone PCT provides customers a means to better manage their heating and cooling consumption costs by enabling them to program a weekly heating/cooling schedule, participate in demand response events, and receive real-time pricing signals and text messages from KCP&L.

1.4.3.3.2 Standalone PCT Characteristics

The Standalone PCT communicates with the SmartMeter wirelessly via an IEEE 802.15.4 network running the ZigBee Smart Energy Profile (SEP) 1.0 specification to receive real-time pricing signals, demand response events, and text messages. The Standalone PCT does not require an Internet connection.

The Standalone PCT, shown in Figure 1-18, provides customers with the ability to:

- Receive real-time pricing information
- Receive demand response event information from KCP&L
- Opt-in/out of demand response events at the thermostat
- Program temperature set points for the thermostat
- Receive important text messages from KCP&L

Figure 1-18: Standalone PCT



The Standalone PCT allows customers to set schedules for their heating and cooling needs throughout the week. Customers can set four different temperature set points for both heating and cooling throughout each day of the week. This helps customers better manage their heating/cooling loads when they are away from their homes. The Standalone PCT also includes different temperature modes, such as “Hold” and “Vacation”, which offer customers more flexibility in managing their consumption.

Program participants will have their Standalone PCT enrolled in the SmartGrid demand response program. When a demand response event occurs, customers are notified ahead of time with information about the event start time and duration. By default, customers are opted into each event. However, once customers receive the event, they can opt-out or back in at any time before the event concludes. Customers can make this opt-in/out decision at the Standalone PCT. Event participation is recorded for post-event evaluation and analytics.

1.4.3.4 Home Area Network (HAN)

1.4.3.4.1 HAN Overview

The Home Area Network (HAN) is a suite of electronic devices that receive information directly from a customer SmartMeter to increase customer awareness of electricity usage and help identify opportunities to reduce consumption and save money. The HAN provides customers a means to better manage their heating, cooling, and simple load consumption costs by enabling them to program a weekly heating/cooling schedule, program pricing schedules for each device, participate in demand response events, and receive real-time pricing signals and text messages from KCP&L.

1.4.3.4.2 HAN Characteristics

The HAN communicates with the SmartMeter wirelessly via an IEEE 802.15.4 network running the ZigBee Smart Energy Profile (SEP) 1.0 specification to receive usage information, pricing signals, and text messages. Included in the suite is a gateway device, a PCT and a pair of 120V Load Control Switches (LCSs). An optional 240V LCS may be included for customers with a larger controllable electric load, such as a water heater or pool pump.

The HAN, shown in Figure 1-19, provides customers with the ability to:

- Receive real-time pricing information
- Receive demand response event information from KCP&L
- Opt-in/out of demand response events at the thermostat and load control switches
- Remotely monitor and control the devices via the Customer Web Portal
- Program temperature set points for the thermostat
- Program pricing rules for the load control switches
- Receive important text messages from KCP&L

Figure 1-19: Home Area Network Devices



The gateway within the HAN establishes an IP connection with the Customer Web Portal via the customer supplied internet connection, enabling customers to manage energy consumption in their home using the functionality provided by the HEMP. The gateway device receives real-time usage information directly from the customer SmartMeter. This usage information is passed to the Customer Web Portal to be displayed to the customer. The gateway also transfers control commands from the Customer Web Portal to the PCT and LCSs. This enables customers to remotely manage device schedules and rules, control devices, and manage demand response event participation.

The PCT within the HAN allows customers to set schedules for their heating and cooling needs throughout the week. Customers can set four different temperature set points for both heating and cooling throughout each day of the week. This helps customers better manage their heating/cooling loads when they are away from their homes. The PCT also includes different temperature modes, such as “Hold” and “Vacation”, which offer customers more flexibility in managing their consumption.

The LCSs within the HAN allow customers to set pricing rules for the simple loads attached to the LCSs. This enables the device to respond and operate to changes in electricity rates automatically, thus giving the customers added flexibility to help manage energy consumption and costs. The LCSs also report individual device consumption data to the Customer Web Portal to be displayed to customers. This feature enables customers to better understand the energy consumption and operating costs of individual appliances within their homes.

Program participants will have their PCT and LCSs enrolled in the SmartGrid demand response program. When a demand response event occurs, customers are notified ahead of time with information about the event start time and duration. By default, customers are opted into each event. However, once customers receive the event, they can opt-out or back in at any time before the event concludes. Customers can make this opt-in/out decision at the PCT, the LCSs, or the Customer Web Portal. Event participation is recorded for post-event evaluation and analytics.

In conjunction with new voluntary TOU rate options and the energy management capabilities that the HAN provides, it is expected that the HAN users will reduce their overall kWh usage, shift load to off peak times, and voluntarily allow HAN-connected devices to participate in demand response events.

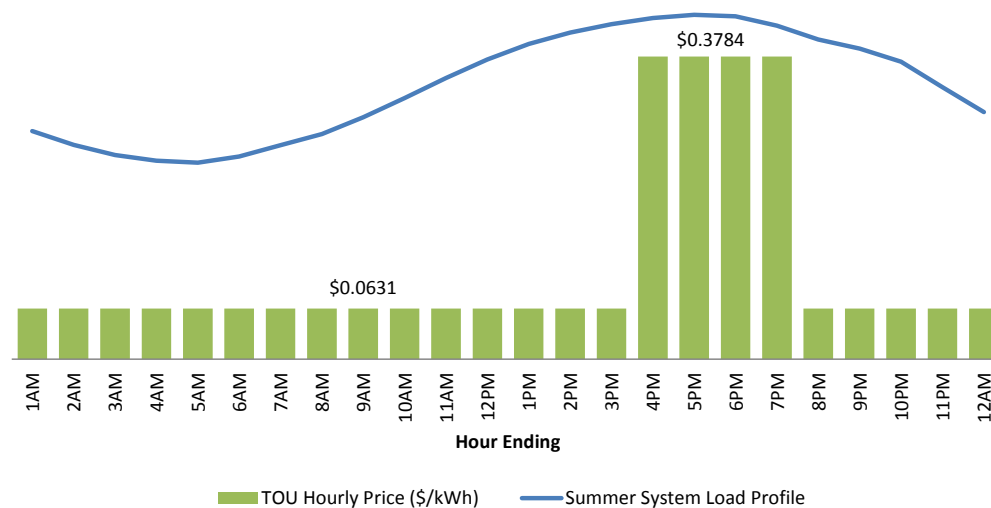
1.4.3.5 Residential Time-of-Use (TOU) Billing Pilot Program

In response to a request from the Missouri Public Service Committee (MPSC) and in conjunction with the KCP&L SmartGrid Demonstration Project that included AMI metering, KCP&L implemented a process by which KCP&L is able to bill a new Missouri time-of-use (TOU) pilot tariff through the CIS system based on usage information collected from AMI meters and stored in the MDM.

The initial pilot tariff went into effect on January 1, 2012 and consists of two daily periods in the summer months: an on-peak period and an off-peak period. Summer on-peak periods occur over a defined hourly range (a four hour period that will start and end on the hour from 3pm-7pm) on summer weekdays and non-holidays. The summer season runs from May 16th to September 15th, inclusive. The tariff expires at the end of the SmartGrid Demonstration Project pilot on December 31, 2014.

Participating customers receive monthly bills that include usage information grouped into the three TOU period categories of peak summer, off-peak summer, and winter usage. They are also able to view TOU cues in the HEMP and IHDs, if they are participating in those programs.

Figure 1-20: KCP&L System Load Profile and TOU Rates



1.4.3.5.1 TOU Overview

While designed to be revenue neutral for KCP&L average residential customers, the pilot TOU tariff provides greater incentive for customers to shift load from peak periods to off-peak periods due to the significant difference between peak and off-peak prices during summer months. Off-peak prices of these tariffs represent a tangible opportunity for customers to shift load and save money on their annual electricity expenses without reducing overall usage.

Successful peak load shifting benefits KCP&L by reducing burdens on inefficient generators and limiting strain on various components of the distribution system resulting in more efficient and more economical delivery of electricity to customers. This project will also provide key inputs to the overall DOE SmartGrid Demonstration Project analyses and reporting.

1.4.3.5.2 TOU Characteristics

Two pilot TOU tariffs offer one summer rate structure: peak period of 3-7pm. Peak periods for both tariffs occur on summer weekdays, excluding holidays. Summer is defined as May 16th through September 15th, inclusive. During the summer season, a flat peak price is applied to all energy used during defined peak hours and a flat off-peak price is applied to energy used at all other times. The customer's standard rate would apply to all energy used in the remainder of the year, considered the winter season. Table 1-7 summarizes tariff details.

Table 1-7: Pilot TOU Tariff Details

Rate Codes	
1TOUA – TOU Rate for Residential Standard Customers currently on 1RS1A rates	
1TOAA – TOU Rate for Residential All-Electric Customers currently on 1RS6A rates	
Schedule	
Peak Rates are charged from 3PM – 7PM Central on non-holiday weekdays (Monday-Friday) during Summer Season; weekends (Saturday-Sunday) and holidays are billed at discounted off-peak rates	
Summer Season: May 16th through September 15th (inclusive)	
Winter Season: September 16th through May 15th (inclusive)	
Holidays observed during Summer Season include Memorial Day, Independence Day and Labor Day	
Pricing	
TOU Summer Peak Price:	\$0.3784/kWh
TOU Summer Off-Peak Price:	\$0.0631/kWh
TOU Winter Price:	Declining Block; same as standard rates
Excluded Customers	
Dual meter customers	
Net metering customers	
Customers w/ Current Transformer greater than 1.0	
Business Rules	
Customer can sign-up anytime during the year; however, the rates will not be affected until the first day of their next billing cycle	
Customer may exit the program anytime; however, they cannot join again during the remainder of the pilot period, which ends on December 31, 2014	
Other Considerations	
Upon request, customer will be made “whole” for the current and previous billing cycles; the current approach would not include making them whole for an entire summer season or to retroactively go back to prior years	
Enrollment occurs at the start of a billing period and customers who elect to exit the program may have their exit backdated to the start of the previous billing period	

1.4.4 SmartSubstation

The Midtown SmartSubstation implementation will consist of new microprocessor based protective relays, a new substation protection and control network, Human Machine Interfaces (HMIs), substation data concentrators, substation controllers, and applications. The SmartSubstation will operate KCP&L's substation with advanced functionality to provide more reliability, efficiency, and security.

Upon completion of the SmartSubstation implementation, KCP&L will be able to demonstrate the following functions:

- Peer-to-peer communication between IEDs via IEC 61850 GOOSE messages
- Controlling the tap changer of the transformers and the smart grid feeder breakers via IEC 61850 MMS messages
- Protection of substation devices, assets and feeders
- Redundant data collection concentration in the substation
- Redundant local HMI
- Cyber security through use of firewall rules and VLANs
- Physical security through electronic access control and NERC-compliant logging tools
- Redundant TCP/IP communication between substation and DMS SCADA system
- Smart applications in the substation that operate in closed-loop mode
- Volt/VAR management using tap changers and capacitor controllers
- Feeder overload management via Dynamic Voltage Control
- Fault management applications performed in conjunction with devices on the feeders (via the substation controller)
- Automated switching procedures to isolate faults on the feeders and provide service restoration
- Relay metering including calculations for real power, reactive power, apparent power, etc.

1.4.4.1 Substation Protection Network (SPN) Upgrade

1.4.4.1.1 SPN Upgrade Overview

This project includes upgrades to protection and control equipment and the deployment of an Ethernet-based substation control network utilizing the IEC 61850 network architecture. This effort requires the Network Services, Substation Protection, and Relay System Protection departments of KCP&L to work together to design, provision, and operate this joint network. The IEC 61850 network should be treated like any other protection and control system, and should only be used for protection and control purposes.

The existing electromechanical relays at Midtown Substation will be replaced with new microprocessor relays (Intelligent Electronic Devices). These IEDs will have communication capabilities utilizing IEC 61850 in the protection and automation system. The IEC 61850 implementation will allow KCP&L to minimize wiring in the substation and provide automation such as interlocks through this digital system.

1.4.4.1.2 SPN Upgrade Characteristics

Substation protection and control networks are deployed in harsh environments and transport critical data. As such, the network and its components have demanding requirements. The network must have high availability and low latency, providing fast, reliable communication between networked devices. Networking equipment deployed in these networks must be environmentally hardened, as it may be deployed in enclosures with limited climate control, requiring the equipment to operate across extreme humidity and temperature ranges. Therefore, a reliable physical architecture for the network is needed along with ruggedized, highly reliable network components.

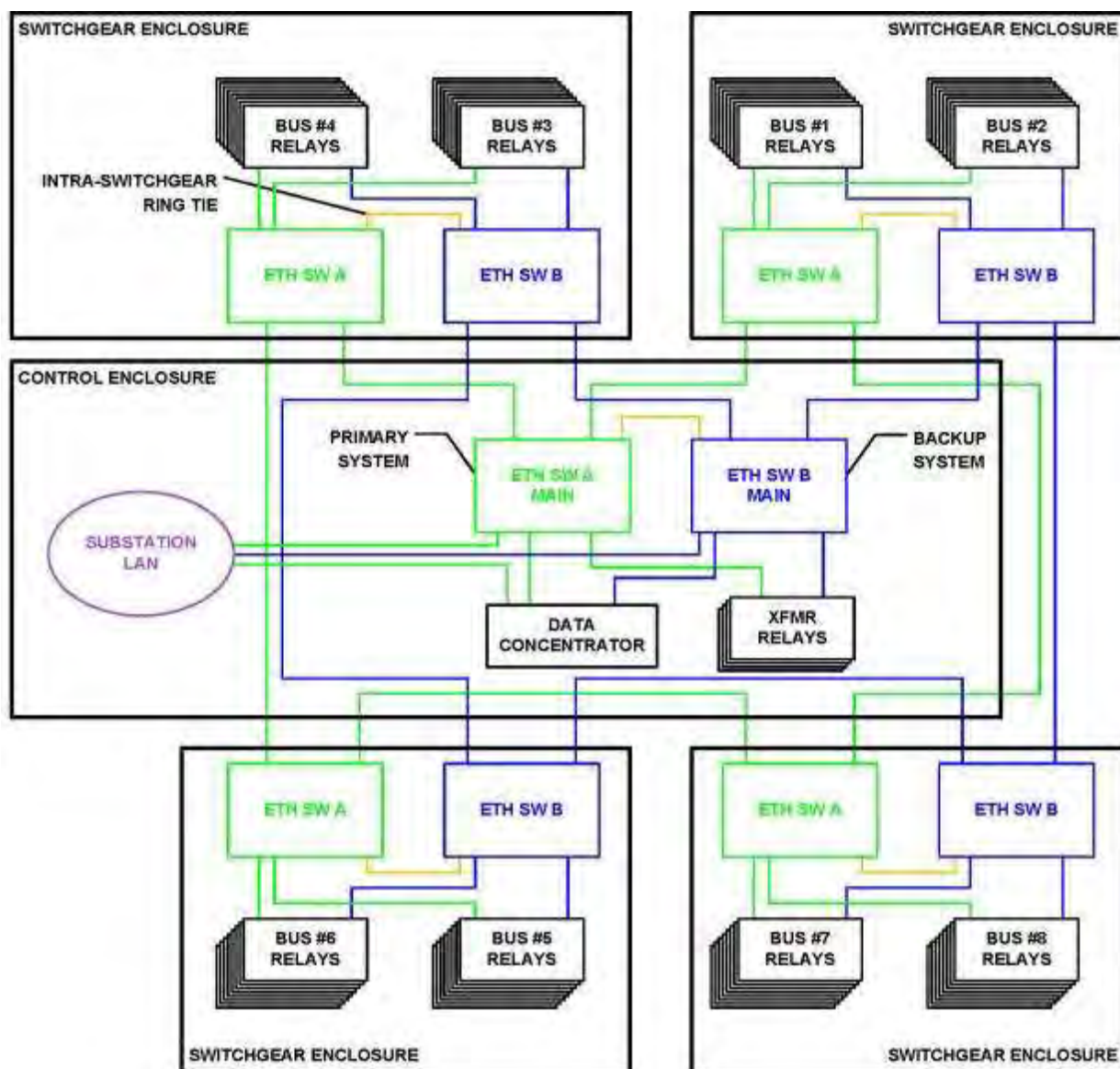
The IEC 61850 Midtown substation control network configuration [2] consists of redundant 1 Gbps Ethernet backbones routed throughout the substation. These backbones will interconnect remote primary and backup Ethernet switches installed in various switchgear enclosures to main Ethernet switches located in the main control enclosure. Protective relays, equipped with redundant Ethernet ports, will connect to the appropriate primary and backup remote switches using 100 Mbps Ethernet.

The Midtown Substation control network topology was chosen to achieve the following:

- Provide high-bandwidth, low-latency communications
- Minimize or eliminate single points of failure for cabling and equipment
- Minimize infrastructure costs

The Midtown substation protection and control network architecture is shown in Figure 1-21.

Figure 1-21: Midtown Substation Protection and Control Network Architecture



The IEC 61850 network was designed as a redundant Ethernet ring architecture. Ring architectures allow for self-healing networks, increasing availability and reliability. The Ethernet switches comprising the network are arranged in rings, providing redundant pathways between two points in the network via the Ethernet backbone. This configuration protects against loss of communication between devices due to failure of a communication link or loss of an intermediate switch. Loss of communication only occurs when there is a failure in the edge switch to which one of the two communicating devices is connected. To further increase reliability, redundant rings can be deployed. This allows devices with redundant Ethernet interfaces to take advantage of a standby Ethernet network, reducing the probability of a loss of station control due to failure of any single piece of network equipment. This redundant ring configuration eliminates single points of failure for all Ethernet hardware when the communication devices are configured in fail-over mode.

Aside from enhanced fault recovery, the additional redundancy can significantly ease maintenance of the network, as any single network device can be completely removed from service without network disruption or loss of station control. Direct connections should be made between primary and backup switches in each control enclosure, providing a local link for traffic in the event any enclosure is isolated from the rest of the network.

1.4.4.2 Distribution Data Concentrator (DDC)

1.4.4.2.1 DDC Overview

Siemens' SICAM PAS (Siemens Integrated Control And Monitoring Power Automation System) acts as the Distribution Data Concentrator (DDC) for the substation and field devices reporting to Midtown. The DDC controls and registers the process data for all the devices in a substation. It is essentially a communication gateway, so that only one data connection to a higher-level system control center is required.

1.4.4.2.2 DDC Characteristics

The SICAM's networking and IT capabilities, interoperable system structure, and integration with existing systems are designed to simplify configuration and commissioning and help to increase the efficiency of operations management. The SICAM is capable of polling for data collection, power monitoring, control automation and system-wide visualization. The over-arching goals of the SICAM are to increase the reliability and availability of KCP&L's systems, leading to a stable power supply.

The SICAM PAS is capable of communicating via the following:

- IEC 61850
- DNP3
- Modbus
- OPC
- Profibus
- TG8979

For KCP&L's Demonstration Project, the SICAM will utilize DNP3 to communicate with the field devices and IEC 61850 to communicate with the substation devices. The 61850 communications in the substation will utilize the manufacturing messaging specification (MMS). The devices will send the SICAM annunciators and metering values. The SICAM will send the devices control messages. Rather than implementing a typical SCADA poll, the devices will be configured to have unsolicited reporting enabled. When one point's instantaneous magnitude crosses a pre-defined deadband threshold, the device will send the SICAM the magnitude of all the points in its 61850 report.

During the pilot, serial communications will be maintained to each relay from the substation remote terminal unit to support dual communications with the relays from the existing energy management system (EMS).

1.4.4.3 Human Machine Interface (HMI)

1.4.4.3.1 HMI Overview

The substation Human Machine Interface (HMI) provides a local view of all of the equipment located inside the fence of the substation. The purpose of the HMI is to give substation personnel a tool for viewing the current status of the equipment within the substation, as well as giving them the potential to operate the smart grid devices from within the substation control house.

1.4.4.3.2 HMI Characteristics

For this project, the Distribution Management System (DMS) only contains information for one substation, but for a system-wide DMS implementation, the DMS would likely provide a higher level of information about devices at all of the substations, and the Substation Distributed Control and Data Acquisition (DCADA) would just be a black box with no graphical user interface. Thus, the HMI would provide this look inside the black box.

Unlike the DMS and the DCADA, the HMI does not contain any information about the field devices. The HMI does, however, provide information about the substation network equipment, which is not displayed in the DMS. Through the HMI, the user will be able to verify whether any substation issues are related to network communications. Each substation device will be connected to a particular network switch and mapped to a specific port. Although the user can't modify any network configurations from the HMI, he will be able to easily determine whether any problems exist on the network prior to engaging the IT personnel at KCP&L.

1.4.4.4 Generic Object-Oriented Substation Event (GOOSE) [3]

1.4.4.4.1 GOOSE Overview

As discussed above, for device to controller communications in the substation, 61850 MMS communications will be used. For peer-to-peer communications, however, the substation IEDs will utilize 61850 Generic Object-Oriented Substation Event (GOOSE) messaging.

1.4.4.4.2 GOOSE Characteristics

For the Demonstration Project, KCP&L will be using GOOSE messaging to implement four functionalities described in the following sections depicted in the GOOSE logic diagram, Figure 1-22.

1.4.4.4.2.1 **Load Transfer**

The load-transfer scheme restores service to customers by automatically closing the tie breaker upon lockout of the transformer. The Midtown Substation design consists of two four-position buses fed from a dual-wound distribution transformer. Tie buses are used for maintenance and emergency backup of station operations when the transformer is removed from operation. The combined load of the two buses can be above the two-hour power rating for the transformer on many of the buses. In the past, a dedicated programmable logic controller (PLC) was used at these locations to calculate the optimal feeder configuration to transfer to the tie bus before the tie breaker was closed. As part of the upgrade, KCP&L wanted this logic to be moved into the relay logic, eliminating the need for the PLC and additional wiring. This objective was achieved through the use of automation logic in a SEL-451 relay, with the real-time event notification capabilities of IEC 61850 GOOSE messaging for inter-relay communications. The feeder relays (SEL-751) were used to publish the individual feeder loads and the

total tie-bus transformer load (SEL-487) using IEC 61850 GOOSE messages. The main relay (SEL-451) subscribes to these analog values along with status messages for bus lockout, which triggers the scheme. The main breaker relay continually computes and publishes the optimal feeder configuration to transfer if a fault occurs, based on each feeder's load and available capacity. When each feeder relay sees the scheme-enabled GOOSE message sent, it opens if it is to be shed before the bus tie breaker is closed. This scheme uses the two-hour overload power rating for the tie bus transformer, which gives the distribution operator two hours to reconfigure distribution feeders, thereby relieving the overload condition while continuing to provide service to customers on the affected bus.

1.4.4.4.2.2 Faster Overcurrent Tripping

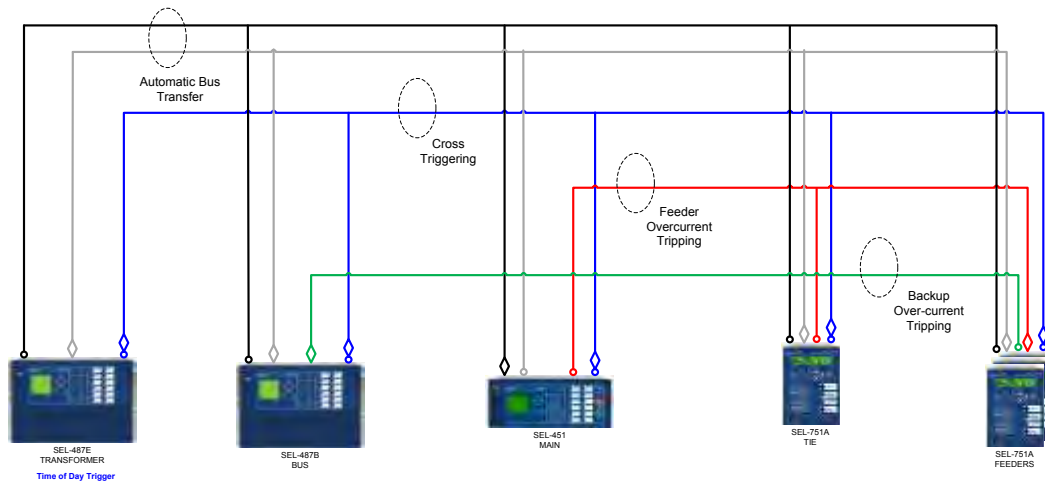
Implementing a communications-based breaker failure scheme instead of relying on time overcurrent values resulted in the faster overcurrent tripping of main and tie breakers upon feeder breaker failure. When a feeder breaker trips, it sends a GOOSE message to the main and tie breakers indicating an operation where a stuck breaker timer is initiated. If a follow-up breaker-open message is not received within this time, the main and tie breakers trip, thereby clearing the fault. This faster overcurrent tripping scheme and subsequent schemes reduce wear on equipment, decreasing the likelihood of equipment failure and improving customer reliability.

1.4.4.4.2.3 Backup Overcurrent Tripping Scheme

Backup overcurrent protection in the bus differential relay provides redundancy to the logic, sensors and wiring in the feeder relays, allowing them to trip a feeder with a reclosing function if the feeder relay fails to detect or clear a fault. The bus differential relay uses its current circuit and sensor to monitor the feeder, and it is programmed to send a GOOSE-based trip message to the feeder relay, clearing the fault if the feeder relay has not already done so. This scheme and the previous scheme could have been implemented using pre-IEC 61850 protection and control designs and techniques, but they were not cost effective to implement. Using the common communications bus reduces the cost of implementing these additional schemes to programming and testing. Once the schemes are initially developed as part of this pilot, they can be used for future projects at a marginal cost.

1.4.4.4.2.4 Cross Triggering

Cross triggering of all devices for every distribution system event and at a specific time each day provides the engineering department with detailed oscillography and event information. This information explains how the protection and control functions performed under fault conditions. Previously, event information was only available from fault recorders, which were not cost-effective for distribution substations. KCP&L's design leverages the power of relays for recording waveforms and IEC 61850 GOOSE messages to cross trigger devices, enabling station-wide awareness that had been impossible in the past. Analyzing this information allows schemes and settings to be optimized, providing customers with more reliable service.

Figure 1-22: GOOSE Logic Diagram

1.4.4.5 Substation Distributed Control and Data Acquisition (DCADA) System

1.4.4.5.1 DCADA Overview

The Substation Distributed Control and Data Acquisition (DCADA) is the brains of the substation. It receives device status updates from the SICAM, and it determines how to respond to activity occurring on the distribution system.

1.4.4.5.2 DCADA Characteristics

The DCADA can perform many of the same applications as the Distribution Management System, but it does so in a closed loop method, and it can only control devices within its area of control. The DCADA can control any devices within Midtown substation or any field devices on Midtown feeders.

The Distribution Network Applications that can be performed by the DCADA include:

- Distribution System Power Flow
- Distribution System State Estimation
- Feeder Load Transfer
- Volt/VAR
- Fault Management

If the substation is running in closed loop mode, then the DCADA makes decisions and sends controls to IEDs without the interaction of an operator. In this mode, the DCADA attempts to resolve any issues that arise using its “First Responder” functionalities. If the DCADA isn’t able to solve the problem with its available tools and applications, then the DCADA transfers control to the DMS, where the operator is alerted of the issue and asked for input to solve the problem.

1.4.5 SmartDistribution

The SmartDistribution sub-project deployed a state-of-the-art Distribution Management System (DMS) and Advanced Distribution Automation (ADA) network. The DMS for this project will only be used for Midtown Substation, but for an enterprise-wide deployment, this DMS would be Central Control for *all* of the distributed intelligent substations and field networks. The DMS monitors and controls the state of distribution network at all times, and serves as the primary point of integration for the facilities, consumer, electrical system, load, distributed energy resource, and real-time substation and feeder information. The DMS includes Distribution Supervisory Control and Data Acquisition (D-SCADA), an

Outage Management System (OMS), and a common graphical user interface for operations. It solves reliability issues through its Distribution Network Analyses (DNA) applications.

Some of the key features of KCP&L's Demonstration Project DMS include:

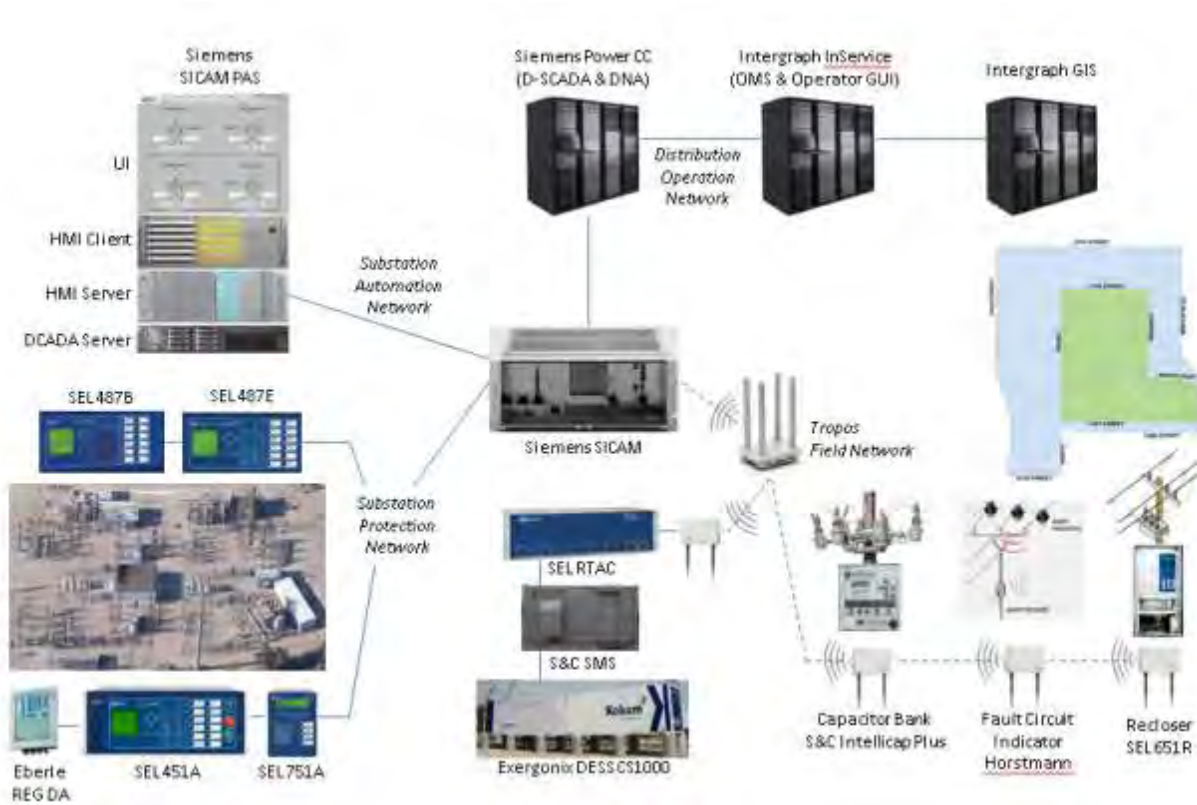
- Provides a single highly efficient user interface for all DMS functions
- Visually correlates and integrates large amounts of field information
- Supports management of outage restoration and mobile work crews
- Utilizes available information from Distribution Automation (DA) and Automated Metering Infrastructure (AMI) sources
- Provides modeling and simulation of Distributed Energy Resources
- Provides modeling and simulation of intelligent field devices and the supporting protection and control schemes
- Incorporates all available feeder and substation measurements and fault indicators
- Establishes a time-smoothed granular feeder load model for more accurate solutions
- Rapidly and accurately determines fault locations and automatically provides isolation and restoration plan options
- Tracks system/feeder load reduction capacity on an on-going basis
- Supports various optimization objectives, including voltage, VAR, loss, and load capacity management
- Establishes a generalized model-based integration platform for simplified integration with other enterprise systems

For the Demonstration Project, Siemens and Intergraph will provide a packaged solution that satisfies all the components of a Distribution Management System. Siemens will be responsible for the D-SCADA and DNA pieces, and Intergraph will provide the OMS and user interface.

The ADA network consists of a Tropos 2.4/5.8 MHz mesh network, capacitor banks, fault current interrupters, and reclosers. The field devices will communicate back to the substation controller and the DMS. The DNA applications will run in open or closed loop at the DMS, and in closed loop at the substation. These applications will respond to any potential network overloads, and will automatically reconfigure the network as needed.

Figure 1-23 shows the components of KCP&L's SmartDistribution implementation.

Figure 1-23: SmartDistribution Components



1.4.5.1 Distribution Management System (DMS) User Interface (UI)

1.4.5.1.1 DMS UI Overview

The DMS user interface (UI) will provide a single comprehensive user environment by which the grid operators will interact with the all DMS components (D-SCADA, OMS, DNA, etc.) and SmartDistribution Functions. The DMS UI will provide a tight integration between DMS components to automate the grid operator's workflow as much as possible and enable efficient transition between major functions.

1.4.5.1.2 DMS UI Characteristics

The DMS UI component of the Demonstration Project DMS is provided by Intergraph's InService system and creates a SmartDistribution operations command and control center that provides the following:

- A common user environment, consolidating multiple control room systems into one user interface to improve situation awareness and reduce human error. The UI allows DMS component applications to be invoked and data/dialogs from these applications to be displayed.
- The geospatial network map display features dynamic colorization and attribute-based symbology that changes with the state of the device. The display can be filtered based on network components or devices related to a particular event.

- From the base map, users will be able to view device statuses, operate switches, turn on and off layers, and view configurable attributes of the facilities. The display can be filtered based on network components or devices related to a particular event.
- The InService UI will provide comprehensive dialog for SCADA Alarms, Crew Status, Pending Jobs, and Work Dispatched.
- The InService system will construct the DMS geospatial electric network model from data imported from the KCP&L GIS.

1.4.5.2 Distribution Supervisory Control and Data Acquisition (D-SCADA)

1.4.5.2.1 D-SCADA Overview

The Distribution Supervisory Control and Data Acquisition (D-SCADA) provides real-time device and automation information to keep the operating model as close as possible to the real conditions in the field. D-SCADA provides all real-time data services and control agent capabilities for the combined Siemens/Intergraph DMS solution.

1.4.5.2.2 D-SCADA Characteristics

The D-SCADA component of the DMS is provided by Siemens for the Demonstration Project. D-SCADA provides interaction capabilities with automated and intelligent distribution system field devices. D-SCADA includes the following:

- Data Acquisition – provides the interface to the system field devices, facilitates the scanning of telemetered data periodically and by exception, transmits control commands, and ensures data integrity
- Network Control Executive – handles switching commands from the OMS and manages their execution
- ICCP Interface – provides the interface that connects D-SCADA to the OMS. It facilitates real-time data transmission and reception, as well as required data point identifier mapping and conversion
- Data Archiving Interface – directs scanned and derived system data to an independent long term archiving system (Siemens HIS)
- Communications Management Display – enables the user to view and change the status of the data acquisition equipment and also displays communications equipment errors and allow the user to view and reset communication error counts
- Configuration Management Tool – monitors the status of key components of the D-SCADA network servers, printers, network interfaces, true time devices, database domains, etc.; it also allows the user to start and stop D-SCADA on individual servers

1.4.5.3 Outage Management System (OMS)

1.4.5.3.1 OMS Overview

The Outage Management System component of the DMS is provided by Intergraph for the Demonstration Project. This component provides the ability to view the current connectivity of the distribution feeders and safely manage day-to-day and emergency restoration work. The OMS provides the basis for all outage information and is uniquely suited for KCP&L's needs, minimizing the integration costs with the existing GIS and Mobile Work Force Management systems. The OMS is integrated at a product level with the Siemens DNA and D-SCADA products to provide a complete solution with "best of breed" product functionality.

1.4.5.3.2 OMS Characteristics

Intergraph's InService model is built upon KCP&L's existing Geographic Information System (GIS) with links to KCP&L's Customer Information System (CIS). Intergraph's base OMS product is capable of analyzing outage notifications from CIS, integrated voice response (IVR), and the automated metering infrastructure (AMI). Using a configurable rules engine, these "calls" are grouped together to predict the correct protection device. Input from SCADA systems and manual input from an operator or dispatcher supplement these predictions.

The major benefits of Intergraph's OMS for KCP&L's implementation include:

- **Increased network reliability** by proactively monitoring the grid for potential problems using distribution analytics and alarming for notification.
- **Reduced time to restore power** by using the trouble analysis engine to pinpoint the most probable outage location

InService's trouble analysis uses the GIS network connectivity model as the baseline configuration, and then processes all transactions to maintain the real-time state of the distribution system. Trouble analysis handles the meter notifications to predict the extent of an outage and the most likely point of failure.

InService's switching procedure management (SPM) works with Siemens' DNA to handle emergency or planned switching orders. SPM will allow KCP&L dispatchers to create, review, and execute switch plans with multiple levels of approval.

1.4.5.4 1st Responder Functions

One of the main objectives of the SmartDistribution sub-project is to implement a family of automatic, distributed "first responder" functionalities. These functionalities are provided by Siemens' Distribution Network Analyses (DNA), and they will be performed centrally by the DMS and locally by the DCADA system in the Midtown Substation. These applications, running on redundant systems, are enhancements to the basic substation automation system. The applications are configurable to their deployment location and the utility's needs.

1.4.5.4.1 1st Responder Function Overview

As part of the project, KCP&L will implement distribution First Responder applications that greatly improve the control of the distribution network, increase supply quality and reliability, ensure optimal use of network equipment, and minimize losses and detection and elimination of overloads at particular points in time.

The First Responder functions are provided through Siemens' Distribution Network Analyses (DNA). The DNA provides tools to simplify and improve the analysis of situations, providing more reliable network status information and supporting the network operation for both unplanned situations and planned activities. DNA uses the CIM-based logical and topological data model of the distribution network of the

real-time database. This data model will be synchronized between the central DMS SCADA system into the substation DCADA system.

For this project, Distribution Network Analyses are composed of the following capabilities:

- Distribution System Power Flow
- Distribution System State Estimator
- Feeder Load Transfer
- Volt/VAR Control
- Fault Management

1.4.5.4.2 1st Responder Function Characteristics

Each DMS and substation controller vendor has its own set of distribution applications, but for this project, KCP&L is utilizing Siemens' Distribution Network Analyses. The DNA provides equipment loading and complex voltage calculations to help the operators understand the voltage and loading of the distribution feeders and individual equipment at any point in time. It also provides a variety of Fault Management and Operations Optimization tools to offload the operations staff and improve efficiency. The DNA applications that are being configured for this demonstration project are detailed below.

1.4.5.4.2.1 Distribution System Power Flow

Distribution System Power Flow (DSPF) calculates voltage magnitude and phase angle for all electrical nodes, active and reactive powers for slack nodes, and reactive power and voltage angles for nodes with PQ/PV generators. It calculates network status (voltage magnitudes and phase angles, line flows, and network losses) under different load conditions and configurations to detect any potential limit violations. The results of DSPF are used for further operational analysis and optimization processes. DSPF is capable of handling both symmetrical balanced and unsymmetrical unbalanced distribution systems. In the real-time context the DSPF can be executed based on a periodic, manual or event triggered conditions.

In DCADA substation operation, the DSPF combines the results of the Distribution System State Estimator (DSSE) and calculates the load flows and voltage conditions during the solution search. It operates in a closed loop mode in the substation.

1.4.5.4.2.2 Distribution System State Estimator

Distribution System State Estimator (DSSE) provides a complete network solution for real-time network conditions for real-time monitoring and further analysis of the network. This solution is based on real-time measured values, scheduled loads, and generations. It provides the statistical estimates of the most probable active and reactive power values of the loads using existing measured values, switching device statuses and initial information on active and reactive customer loads. DSSE results are used to monitor the real-time network operating state. In the real-time mode the DSSE can be executed periodically, manually or triggered by an event.

DSSE application provides the real time status of the electric node voltage vectors as a basis for power flow calculations and the starting point for other subsequent analysis functions (Volt/VAR Control (VVC), Feeder Load Transfer (FLT), and Fault Detection, Isolation and Restoration (FDIR)). DSSE is a closed loop function processing initial load values and minimizing the differences between the measured and calculated values. Upon obtaining the voltage vector solutions, it calculates the flows of active and reactive power on all lines as well as power losses.

1.4.5.4.2.3 Feeder Load Transfer

Feeder Load Transfer (FLT) determines the optimal radial distribution network configuration to mitigate or remove feeder overloads. It removes the feeder overloads by transferring load from overloaded feeders to the feeders with spare capacity. FLT determines switching plans that ensure continuous supply of power to the consumers, and voltage and current levels within technical limits. FLT can be triggered manually to transfer the load from one feeder to another or it can be triggered by Distribution System State Estimator (DSSE).

FLT can be executed in closed loop, open loop or study mode in the DMS Control Center level and in closed loop mode in the substation level. The result of closed loop execution in both DMS and DCADA level is a set of the switching steps that will be performed on remotely controlled “normally open switches” as well as closed switches. The result of executing FLT in open loop mode in DMS level is a list of suggested switch operations that includes both remotely as well as manually controlled switching devices. The solutions presented by FLT will be verified by the Distribution System Power Flow (DSPF) to assure there are no remaining overloads or voltage violations. In the latter case, the FLT will trigger VVC functionality to try to find an optimal solution. In case a solution is not found or any of the switching steps is unsuccessful, a warning will be sent to the dispatcher in the DMS Control Center and the DCADA application part of functions will be disabled.

1.4.5.4.2.4 Volt/VAR Control

A Volt/VAR Control (VVC) function deals with the complexity of the voltage and reactive power control in a modern distribution system. The primary objective of VVC is to satisfy voltage and loading constraints. It is able to work with both balanced and unbalanced distribution systems. It supports the control of transformer on-load tap positions (LTC, voltage controllers) and switchable shunt reactive devices (typically capacitors) to meet the objectives. VVC can be executed to satisfy any of the following 4 objective functions:

- Minimize the sum of power losses
- Minimize the power demand
- Maximize the substation transformer reactive power
- Maximize the difference between energy sales and energy prime cost

1.4.5.4.2.5 Fault Management

Fault Management is a set of DNA applications used for locating distribution network faults and providing fault (or planned outage) isolation and service restoration. Fault Management can be executed in real-time or study context. Fault Management is capable of localizing the faulty area as closely as possible, based on available real-time data from SCADA. The Fault Management set of applications includes Fault Location, Fault Isolation and Service Restoration, Fault Isolation and Immediate Restoration, and Fault Detection and Immediate Restoration.

Fault Location (FLOC) determines the locations of permanent faults through the telemetered information protection devices and fault indicators as well as manually updated information. FLOC is triggered by change in the switch status. It can be operated in open and closed loop mode. Fault Location can be configured to handle either outage and/or non-outage faults. If different faults (independent from each other) trigger different fault detectors, FLOC detects and processes multiple faults in parallel.

Fault Isolation and Service Restoration (FISR) can be used for section isolation due to maintenance work or fault in the system. The isolation function determines a set of switching operations to isolate an area of the network. It can be initiated by the location of the faulty segment or area, or by manual selection for planned outage. Service restoration provides a possible choice of switching procedures to restore service. FISR can be executed in open loop or closed loop mode. In open loop mode, FISR presents the

advisory solutions to the dispatcher and the dispatcher will make a final decision to execute the optimal solution. In closed loop mode, FISR executes the solution calculated. Only if the control step is not successful or not executable, further steps are stopped and a dispatcher is informed.

Fault Isolation and Immediate Restoration is performed to isolate equipment from the rest of the network and immediately restore unaffected and non-faulty de-energized equipment. In addition to switching operations required to isolate the specified equipment, additional switching operations required to energize (from alternate sources) equipment that is de-energized but not outaged are determined. If the selected equipment is energized, fault isolation and immediate restoration can be configured to generate restoration steps before isolation steps.

Fault Detection and Immediate Restoration (FDIR) is a combination of the FLOC and FISR features to locate the fault and isolate the faulted area and immediately restore power to unfaulted but out-of-service customers. FDIR is triggered by FLOC function. FDIR can be executed only in closed loop mode at both substation and DMS Control Center levels. It will select the most feasible isolation and restoration procedure and execute it by sending a control command to the field. This assures minimal outage time. In the event that it cannot find a local solution within its means, it will notify the dispatcher for higher level analysis and supervision.

1.4.5.5 Advanced Distribution Automation Field Area Network (FAN)

The Advanced Distribution Automation (ADA) Field Area Network (FAN) exists to provide monitoring and control capabilities to devices outside of the substation. These devices communicate with both the substation controller and the distribution management system. The substation controller uses the field device information to perform First Responder functionalities in closed-loop mode, and the DMS uses the field device information to perform First Responder functionalities in either open or closed loop. The distribution operator will have access to all of the information about these field devices to assist in planning decisions and resolve network issues.

1.4.5.5.1 ADA FAN Overview

Originally, KCP&L planned to use the AMI network for both metering and distribution automation purposes. This would have reduced equipment, installation, and network management requirements. One of KCP&L's main project goals, however, was to utilize NIST's emerging standards for the smart grid and test out the interoperability between system vendors. For ADA, this meant using Internet Protocol (IP) to communicate to the field devices on the feeders. As a result, KCP&L opted to implement a separate field network for DA.

1.4.5.5.2 ADA FAN Characteristics

The KCP&L Advanced Distribution Automation network will consist of a number of field devices that communicate to the substation controller and to the DMS via an RF mesh network.

1.4.5.5.2.1 Tropos Network

Tropos' GridCom® wireless IP mesh network will extend the KCP&L SmartGrid IP network to reclosers, capacitors and fault indicators in the field, providing direct monitoring and control communications with substation-based distribution automation controllers and the centralized distribution management system. It will help KCP&L optimize energy delivery through active Volt/VAR optimization and feeder load transfers.

The Tropos GridCom® network also paves the way for enhancing power reliability by centrally monitoring fault indicators and automatically configuring around faults, reducing the impact and duration of outages, which is a cause of increasing concern for customers. The network provides the

high-capacity, low-latency and security required to support the applications KCP&L plans to deploy to implement their advanced distribution automation vision for the Demonstration Project.

The Tropos GridCom® network provides high resiliency with multiple redundant communications pathways to ensure that there is no single point of failure. It leverages the 2.4 GHz and 5.8 GHz frequency bands simultaneously and dynamically manages airtime, helping to avoid localized interference on any one frequency band. Dynamic channel selection, adaptive noise immunity and other advanced RF resource management techniques provide added resiliency.

GridCom® is based on a fully distributed architecture. It does not rely on a centralized controller for its operation, removing potential single-points-of-failure and eliminating unnecessary network traffic. GridCom's distributed intelligence performs functions such as network optimization, path selection and routing, and enforcing security and QoS policies.

GridCom® supports centralized management using Tropos Control, a comprehensive and scalable network management system. Tropos Control supports network implementation and optimization plus ongoing management of Key Performance Indicators. Although the network itself operates independently of Tropos Control, Tropos Control is used for alarm management, configuration, provisioning, and performance management.

1.4.5.5.2 Automated Field Devices

KCP&L is utilizing a combination of existing and new devices for this distribution automation deployment. The following devices are planned for installation in the Demonstration Project area:

- **Capacitor bank controllers** - KCP&L already has a number of capacitor banks installed in the Demonstration Project area, so these will be used on the new Tropos network. The old controllers will be replaced with new S&C IntelliCAP PLUS controllers, and a Tropos 1310 router will be connected to the controller. The capacitor bank controllers will communicate with the Tropos router via serial DNP3. Although KCP&L wanted IP communications to all of the controllers, this was not an option from most capacitor bank controller manufacturers. As a result, the communications from the SICAM to the router will be IP based, but the communications from the router to the controller itself will be serial. The capacitor banks used for this project are a combination of standard and VAR controls.
- **Fault current indicators** – KCP&L will be installing Horstmann Fault Current Indicators (FCIs) for the Demonstration Project. Each FCI receiver can communicate with up to twelve FCIs, or four sets of three devices (one device per phase). The quantity of FCIs associated with a particular receiver is based on the number of devices desired in a certain geographic area – the range of the receivers is the limiting factor. KCP&L will only be able to get information *from* these devices; FCIs are not capable of responding to any controls.
- **Recloser controllers** - KCP&L plans to use two different types of reclosers for this distribution automation implementation – the G&W Viper-ST solid dielectric and the Siemens SDR 3212 vacuum reclosers. The recloser controllers are SEL 651R. All of the reclosers and their associated controls are new for this project. The reclosers are being used for three different purposes:
 - Isolation switch – used where the feeder transitions from underground to overhead
 - Mid-circuit recloser – used to segment the feeder into multiple pieces to limit the affected customers in the event of a fault
 - Tie recloser – used to feed a portion or all of a circuit from an adjacent circuit

1.4.5.6 Data Historian (HIS)

1.4.5.6.1 HIS Overview

The Historical Information System (HIS) provides a reliable archive for storing historical data from PowerCC. It can also be used for doing data and event analyses.

1.4.5.6.2 HIS Characteristics

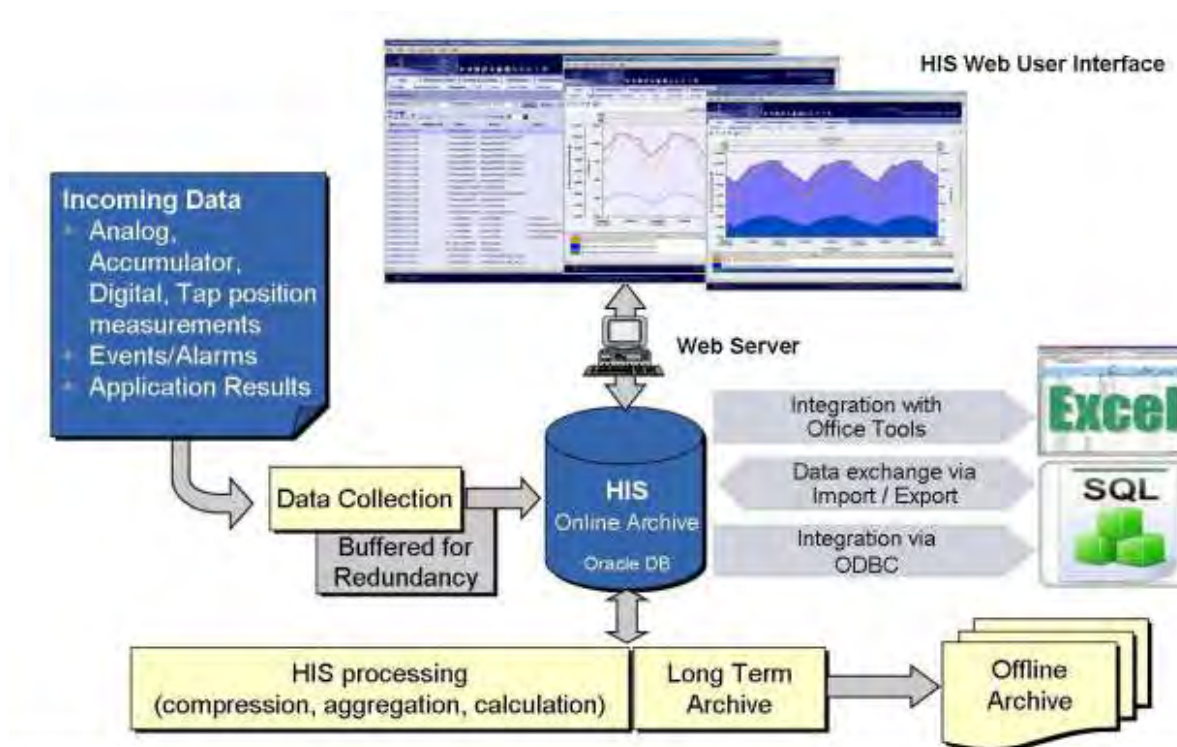
Siemens HIS is designed to store large quantities of real-time data from PowerCC. It archives this data securely, even during periods of system failures and huge data volumes. The storage can be stored periodically or non-periodically. The components of the HIS are shown in Figure 1-24 below.

For KCP&L's implementation, the Historical Information System (HIS) will collect and store analogs, digitals, accumulators, messages, and tap positions. The data is obtained from Siemens PowerCC, and it will be collected both periodically and spontaneously.

The HIS contains a graphical user interface for viewing the data. With this GUI, users can view raw data collected over a specified time range. They can also filter the data by a certain point or a specific event, and they can view a sequence of events for a set of data points over a specified time range.

The HIS web-based user interface follows the look and feel of PowerCC, and it allows the user to view the historical data in multiple formats. The tabular displays and charts can be defined by time range, and the user can filter and sort in a variety of ways to quickly focus on the data point of interest. The data can be printed straight from the HIS or exported to MS Word, MS Excel, CSV, or XML files.

Figure 1-24: HIS Components



The HIS has a calculation engine that can combine values from different data points, and it can perform two types of calculations:

- On-the-fly calculations (executed on-the-fly after they have been started in the UI)
- Persistent calculations (defined based on persistent aggregations)

1.4.6 SmartGeneration

KCP&L will implement a Distributed Energy Resource Management (DERM) system and make use of a variety of distributed energy resources in the project area, including:

- Grid-scale energy storage
- Distributed renewable generation
- Direct load control demand response (DR) programs

Working in concert with other SmartGrid technologies, the DERM and these resources will serve to demonstrate a “virtual power plant” which can dynamically respond to changing system conditions. The net effect of this virtual power plant is to defer the need to build additional fossil-fuel generating resources as well as helping to defer distribution and transmission system upgrades. Benefits of such deferrals flow through to customers in the form of lower costs, increased reliability and reduced environmental impact.

1.4.6.1 Distributed Energy Resources Management (DERM)

The Distributed Energy Resource Management (DERM) system stores and manages all information pertaining to demand response (DR) and distributed energy resources (DER) programs and assets. The DERM must integrate with a number of other KCP&L systems, including the Customer Information System (CIS), Meter Data Management (MDM) system, and Distribution Management System (DMS). In addition to interfacing with these back-end systems, the DERM will communicate with various “control authorities” that oversee particular types of resources.

For this project, the DERM will be used to respond to overload conditions for system reliability purposes. The DERM will help to prevent overloads from occurring, and it will shorten the duration of outages that do occur. The DERM is also capable of being used for economic purposes, but this will not be the focus during the Demonstration Project.

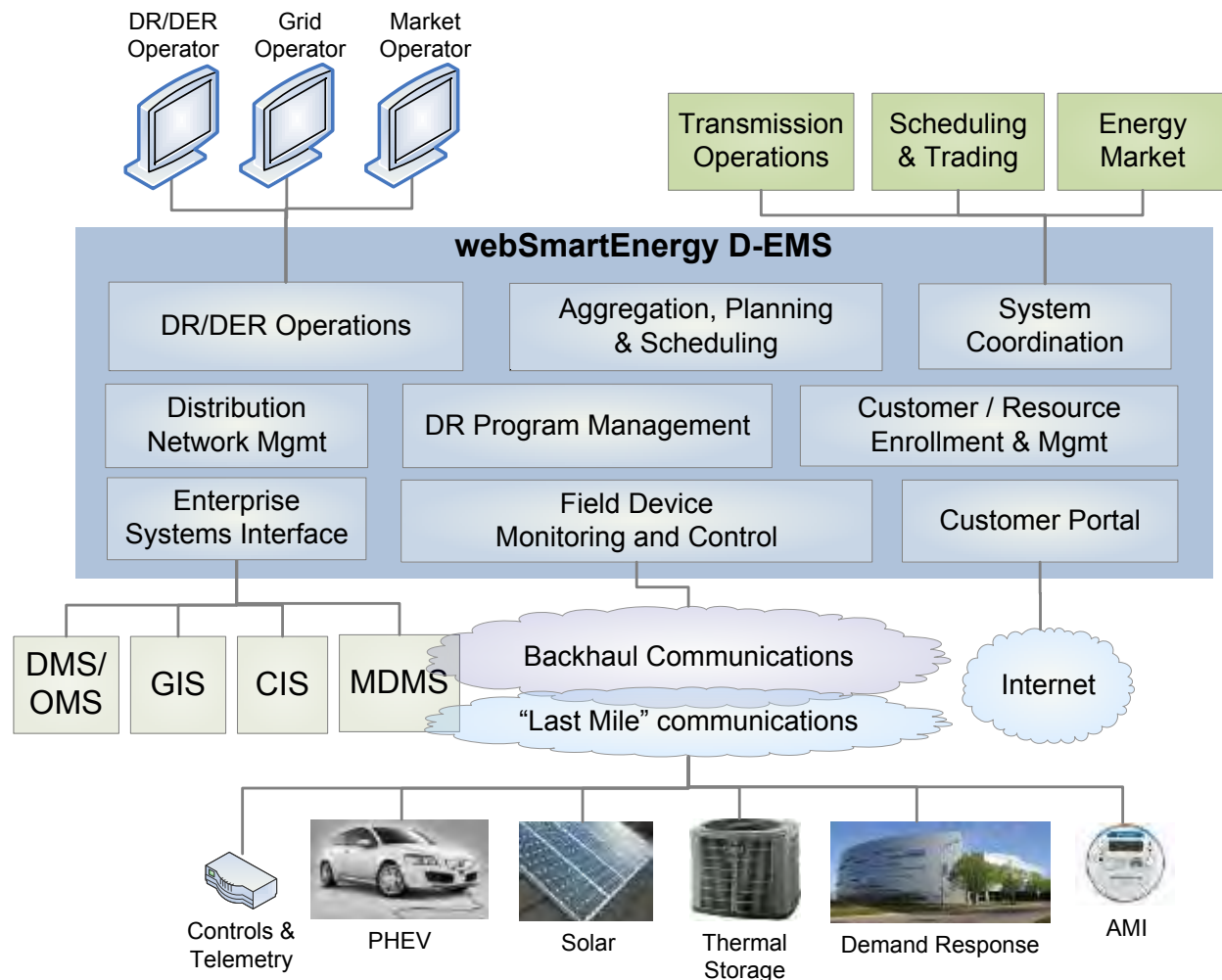
1.4.6.1.1 DERM Overview

For the Demonstration Project, KCP&L will be implementing a DERM system from Open Access Technology International, Inc. (OATI). Their product, called the webSmartEnergy Distributed Energy Management Solution (DEMS) provides full visibility into demand side capabilities, the ability to leverage those capabilities for operational and economic efficiencies, and the ability to aggregate and use those capabilities in support of wholesale market operations. A diagram of the webSmartEnergy DEMS solution appears in Figure 1-25.

1.4.6.1.2 DERM Characteristics

The OATI webSmartEnergy DEMS provides the bridge between advanced metering, DR/DER, variable generation, distribution grid, transmission grid, and wholesale markets. In addition to a full complement of conventional Demand Response capability, webSmartEnergy DEMS provides the capabilities needed to optimally manage distributed energy resources for the support of distribution system load relief, and for the transmission and market operations, (e.g., providing ancillary services and balancing energy to support variable generation). By mapping DR/DER to distribution grid locations, and tracking circuit, feeder, and equipment conditions, webSmartEnergy DEMS provides a unique combination of capabilities for integrated Smart Grid operation while considering limitations imposed by transmission and distribution grids.

For the Demonstration Project, the DERM will be called upon when the DMS needs assistance with a current or projected future overload. The DMS will try to solve the issue using its own resources first, through feeder load transfer or conservation voltage reduction. If these methods do not completely address the overload, then the DMS will call upon the DERM for demand response.

Figure 1-25: Distributed Energy Management Solution Functional Overview

The DERM will store and manage all the information about the various demand response programs and assets for the demonstration project. It will keep track of tariff limitations (for example, KCP&L might only be able to call upon a particular program four times in one month) and any costs associated with calling on each program. It will suggest DR options that address the overloaded feeders and it will prioritize based on these limitations and associated costs.

Once the operator selects the DR to apply to the situation (either using the DERM's recommendation or selecting other options), the DERM schedules the DR event. The DERM won't communicate directly to the end devices participating in the event, however. Instead, the DERM sends DR messages to the "control authorities." For the demonstration project, the DERM will dispatch DR events to the following control authorities:

- Home Energy Management Platform (HEMP) for residential DR
- Vehicle Charge Management System (VCMS) for EV charging stations
- Distribution Management System (DMS) for grid-connected assets, such as the 1MW battery

These control authorities will then send the appropriate DR messages down to the end devices to direct their participation in the scheduled event. These DR interfaces and events are described in additional detail in section 2.2.5.2, Demand Response (DR) Load Curtailment.

1.4.6.2 DR Load Curtailment Programs

1.4.6.2.1 DR Load Curtailment Program Overview

As part of the Demonstration Project, KCP&L will deploy direct load control devices to customers and businesses within the project area and integrate them with back office applications to manage and execute market-driven or reliability-driven demand response events. Direct load control devices will include:

- Residential standalone programmable communicating thermostats (PCT)
- Residential home area network (HAN)-based PCTs
- Residential HAN based load control switches (LCSs)

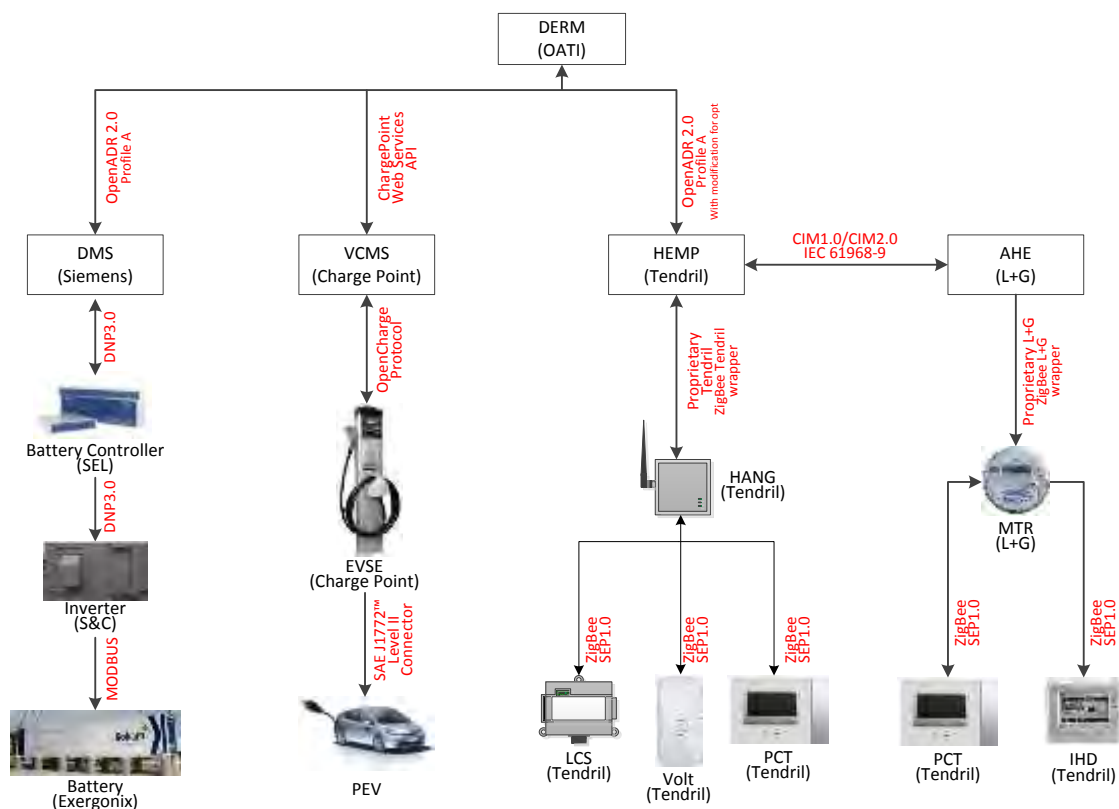
All demand response resources will be engaged through two-way communication between the customer premise and the back office DERM webSmartEnergy application. The DR devices may be aggregated and operated based on grid connectivity (small- or wide-scale) as needed to provide desired locational load relief. The project will assess these DR resources' capabilities for providing emergency "fast DR" and planned DR for day-ahead and hour-ahead grid study case scenarios.

In addition to these residential devices, KCP&L will also utilize the Vehicle Charge Management System (VCMS) for demand response contributions from the ten charge stations associated with the demonstration project. Lastly, the DERM will be able to utilize the grid-connected battery for DR load curtailment.

1.4.6.2.2 DR Load Curtailment Characteristics

Figure 1-26 shows the various systems that the DERM can call upon, along with the message types used for each of the associated interfaces.

Figure 1-26: Demand Response Load Curtailment Architecture



1.4.6.2.2.1 Residential Standalone Programmable Communicating Thermostat (PCT)

The Standalone PCT is an electronic device that receives information directly from a customer SmartMeter wirelessly via an IEEE 802.15.4 network running the ZigBee Smart Energy Profile (SEP) 1.0 specification to receive demand response events, pricing signals, and text messages.

Similar to an existing enterprise-wide program called Energy Optimizer, KCP&L will deploy advanced PCTs to customers in the project zone with SmartMeters in the Demonstration Project area. These ZigBee-based PCTs will be paired with customers' SmartMeters to enable utility-controlled demand response events. Events will be initiated by the DERM and event messages will be delivered to the devices by the AMI network (via the SmartMeter).

When a demand response event occurs, customers are notified ahead of time with information about event start time and duration. By default, customers are opted into each event. However, once customers receive the event, they can opt-out or back in at any time before the event concludes. Event participation is recorded for post-event evaluation and analytics.

1.4.6.2.2.2 Residential HAN DR

Similar to the standalone PCT, KCP&L will deploy HAN PCTs and LCSs as a part of a larger HAN package that includes a HAN gateway, PCT, and two 120 volt control switches. The PCT is identical to the standalone PCT. However, the HAN gateway facilitates two-way communications with utility back office systems over broadband internet connection rather than the AMI network.

1.4.6.2.2.3 Battery Energy Storage System (BESS)

The Battery Energy Storage System (BESS) will be used for a number of standalone applications during the demonstration project, but it will also be used as a resource for demand response purposes. During peak periods of energy use, KCP&L can call on the battery via the DERM and discharge the battery for grid relief.

1.4.6.2.2.4 Vehicle Charge Management System (VCMS)

The Vehicle Charge Management System (VCMS) is the control system for the ten Electric Vehicle Charge Stations (EVCS) that will be deployed within the Demonstration Project area. These stations will be integrated with the DERM and available for use during demand response events. Although they will only provide DR relief if vehicles were using the stations during the time of the event, this interface will still provide a valuable test field.

1.4.6.3 Battery Energy Storage System (BESS)

1.4.6.3.1 BESS Overview

One SmartGeneration component of the Demonstration Project is the evaluation of a 1.0 MW / 1.0 MWh Exergonix lithium polymer battery energy storage system (BESS). This system will be interconnected to the head of a single urban circuit just downstream of the substation bus. It will be integrated with demonstration control systems and will be exercised to demonstrate its capability to offer direct grid support via the following applications:

- Energy time shifting
- Net circuit load peak shaving
- Volt/VAR support
- Circuit Islanding

In addition to demonstrating these applications, KCP&L aims to appraise the battery system's technical performance with regards to roundtrip AC efficiency.

1.4.6.3.2 BESS Characteristics

KCP&L partnered with Exergonix (www.exergonix.com) to provide and install the BESS. The Exergonix BESS consists of over 5,000 Kokam Superior Lithium Polymer Battery (SLPB) pouch cells that are coordinated by a unique battery management system. The battery system is driven by a PureWave Storage Management System (SMS) from S&C Electric (this may also be referred to as the Power Conditioning System or PCS).

1.4.6.3.2.1 Battery Technology

The patented SLPB technology is proven, is already in production in the U.S., and is being used in numerous applications around the world. The SLPB cell design increases energy density to as high as 200 Wh/Kg in high energy cell configurations and power densities as high as 2400 W/Kg can be achieved with minimum optimization on a high power cell design. The Kokam SLPB meets all performance standards of the U.S. Advanced Battery Consortium (USABC). The SLPB cells are expected to provide extended run time, 10+ years of operational life (up to 10,000 cycles), reduced need for complex cooling systems, and safe operation over a wide range of temperatures.

Figure 1-27: Grid-Connected Battery



1.4.6.3.2.2 Power Conditioning System (PCS)

The S&C Electric PureWave SMS manages charge and discharge of the battery subsystem and converts AC grid power to DC battery power. It consists of a control system and a four quadrant bi-directional inverter, rated at ± 1.0 MW / 1.25 MVA. The SMS converts nominal battery voltages ($460 V_{DC} - 800 V_{DC}$) into 3-phase 60 Hz, $480 V_{AC}$, $\pm 10\%$. It can operate at temperatures between -40°C and $+40^{\circ}\text{C}$ and altitudes up to 1,000 meters without de-rating. It is connected to a $480 V_{AC}$ transformer via a wye-delta configuration to step-up voltage to a 13.2-kV MV distribution circuit. This PureWave SMS is specially equipped with remote control protocols for islanding purposes, a feature that is not included in the standard commercial product offering. The 800 V DC-to-DC converter can step down voltage and utilize a UPS to provide 30-minutes of backup auxiliary power to all internal controls needed during islanding events. At the conclusion of islanding events, the SMS can sync the battery with a recloser to automate seamless grid reconnect.

1.4.6.4 Distributed Renewable Generation: Solar Photovoltaic

1.4.6.4.1 Solar PV Overview

KCP&L will install approximately 180 kW of diverse solar photovoltaic (PV) systems on both residential and commercial properties throughout the pilot project area.

The implementation of these PV systems within the pilot project area will enable KCP&L to assess:

- The impacts of intermittent distributed generation on circuit voltage and power quality
- Monitoring of renewable generation and tracking against RPS requirements
- Building a database of PV type/installation generation performance in the KC metro area
- The potential for reverse power flows due to distributed generation
- The feasibility of aggregating, managing and potentially dispatching a high penetration of utility owned distributed PV systems and capacity
- The feasibility of owning and operating numerous distributed generation on the system

1.4.6.4.2 Solar PV Characteristics

The PV systems, with the exception of those installed on utility property, will be established through a lease agreement in which KCP&L will lease roof-top space but will own and maintain the PV system for a multi-year contract period.

Each system will be designed and specified independently based on available southern facing roof space. A variety of PV technologies and installation methods will be sought. Each system will be directly grid connected and metered independently for tracking purposes.

Figure 1-28: Paseo High School Roof-top Solar PV System



1.4.6.5 Vehicle Charge Management System (VCMS)

1.4.6.5.1 VCMS Overview

The Vehicle Charge Management System (VCMS) is deploying an integrated network of electric vehicle charging stations for the SmartGrid Demonstration Project. A total of ten Electric Vehicle Charging Stations (EVCSs) will be deployed within the Demonstration Project area. The VCMS and EVCSs will provide customers the convenience of public charging, while also providing KCP&L with further demand response resources and capabilities. The VCMS will be integrated with the DERM and will serve as the “control authority” for each EVCS during demand response events.

1.4.6.5.2 VCMS Characteristics

The VCMS and EVCSs for the SmartGrid project are being supplied by LilyPad EV, a Kansas City-based licensed ChargePoint supplier. Each EVCS consists of a dual port, level 2 (240V) Coulomb CT2021 Charging Station with SAE J1772 standard connectors (Figure 1-29). Each EVCS is equipped with a cellular modem enabling two-way communications with the ChargePoint web platform. This will allow customers to locate and reserve individual EVCS using web mapping applications. Also, KCP&L will be able to monitor and manage each EVCS via the ChargePoint web platform.

Figure 1-29: Coulomb CT2021 Charging Station



Station summaries, including usage and inventory reports, reservation schedules, and audit reports, will be readily available through the platform. KCP&L will also be able to manage access control, station provisioning, station alarms, and peak load configurations.

As part of the SmartGrid Demonstration Project interoperability efforts, KCP&L is implementing demand response integration between the VCMS and the DERM using APIs developed by ChargePoint. To help meet the SmartGrid Demonstration Project cyber security goals, HTTPS and SSL protocols will be utilized for all API transactions between the VCMS and DERM. These APIs support the project goals of implementing cutting-edge industry interoperability standards. These APIs are capable of providing DERM (or other systems) with EVCS information, scheduling and reservation capabilities, demand management, and usage analysis. Utilizing this integration, the DERM will be able to execute demand response events on the VCMS and EVCS. Events can be performed on the entire population of EVCSs on an emergency or scheduled basis.

This page intentionally blank.

2 Technical Approach [4]

The KCP&L SmartGrid Demonstration has been explicitly designed to be a complete end-to-end SmartGrid demonstration program in a geographically defined area of Kansas City. By focusing on the circuits and distribution feeders surrounding its Midtown Substation, the Company will be able to assess the potential benefits of a SmartGrid solution from SmartGeneration through to SmartEnd-Use in a regionally unique, controlled “laboratory” environment. The goals of this demonstration are in sync with those of the DOE Smart Grid Demonstration Initiative – to quantify Smart Grid costs, benefits and cost-effectiveness as well as verify Smart Grid technology viability, and validate new Smart Grid business models, at a scale that can be readily adapted and replicated around the country.

2.1 Cross-cutting Plans & Implementations

During Phase 1 of the Demonstration Project the KCP&L Project Team developed and published a series of cross-cutting project plans that include:

- SmartGrid Interoperability Plan
- SmartGrid Cyber Security Plan
- Education & Outreach Plan
- Metrics & Benefits Reporting Plan

The following subsections provide an overview of the significant elements of each of these plans.

2.1.1 Interoperability Strategy & Plan [5]

The KCP&L project team developed and published a “SmartGrid Interoperability Plan” that detailed a strategy and approach for system interoperability for the KCP&L SmartGrid Demonstration Project. The following subsections provide an overview of the significant elements of the Interoperability plan developed for the project.

2.1.1.1 Interoperability Vision

Federal and industry requirements for interoperability and security are critical to a successful integrated Smart Grid solution and they are a key focal point for this project. Inherent in any approach to integration and interoperability are the challenges posed by the heterogeneous nature of the grid components; as each component varies in ability to securely and accurately communicate in the overall Smart Grid solution.

KCP&L’s vision calls for many emerging technologies to be integrated into the Transmission and Distribution networks, ultimately, achieving interoperability with and between legacy environments. The planned demonstration project poses challenges due to immature and emerging Smart Grid standards, the high level of interoperability involved across distributed platforms, and the need to carefully protect customer and system control information across a highly distributed network reaching outside of utility boundaries and onto customer premises. Given the heterogeneous nature of combining legacy components and products of numerous vendors, the project must anticipate and mitigate several challenges.

These challenges include:

- Communicating with legacy systems and devices
- Communicating between open standard and proprietary components
- Identifying failure and upgrading and maintaining components so that overall system operation is highly reliable
- Supporting interacting parties' anticipated response to failure scenarios, particularly loss of communications

2.1.1.2 Interoperability Strategy

To make effective progress for this project and deliver customer and operational benefits, KCP&L envisions an approach to maximizing interoperability that takes aggressive action despite market and standards uncertainties, and that provides a measured means to carefully protect operational reliability, cyber security, and long-term investments. The structured, evolutionary approach described in this document preserves investments, yet provides the flexibility needed for orderly integration of emerging frameworks, methods and standards. Key aspects of KCP&L's strategy for managing interoperability risks include:

- Product selection with consideration of emerging standards for distribution grid management (e.g., IEC 61968 and IEC 61850)
- Open and modular architectural approaches that emphasize vendor-independent integration mechanisms (e.g., Service-Oriented Architecture)
- Investment in ongoing integration test-bed capability to provide for agile component integration, interoperability testing and means for managing technical and security risks through hands-on application and integration of new technologies
- Continued collaboration with public/private industry consortia and special interest groups (such as SGIP, EPRI, IEC, IEEE, UCAIug and the GridWise Alliance) toward the refinement of interoperability standards
- Ongoing and regular review of current implementation and architecture versus current industry standards and emerging integration models

However, using a standard, even an open standard, is not a panacea. As technology changes over time, standards go through life cycle phases, both in commercial adoption and technical maturity. Today's new standard is tomorrow's legacy specification. Also, there is no shortage of standards within the complicated landscape of interface specifications in electric power, manufacturing, buildings automation, and information technology in general.

Throughout the project development life cycle, KCP&L will identify, analyze, and develop mitigation approaches to the various risks encountered in the project. This will be accomplished through periodic reviews, implemented to ensure the successful completion of one stage of the project's life cycle prior to progressing to a subsequent stage. During these reviews, adherence to standards, buy-in from stakeholders and resolution of issues will be accomplished. Evidence of completion will be accomplished through documentation of required artifacts for each life cycle stage.

2.1.1.2.1 Strategic Interoperability Directions

This section describes important strategic directions of KCP&L that are intended to enable increased interoperability. These technologies and the accompanying business processes will be implemented as needed for the demonstration project; however, they represent important steps towards a broader integration of the demonstration systems.

2.1.1.2.1.1 Application Interface Interoperability

Initially, integration with legacy production systems will be achieved primarily through file transfers. However, ultimately, web services deployed in a Service-Oriented Architecture will be used to achieve interoperability between proprietary protocols and will be used to create open interfaces between legacy and new systems and applications. Through the use of open standards, such as web services and the protocols and standards defined by W3C and OASIS consortia, along with mechanisms for guaranteed delivery of transactions and resilient network architecture, KCP&L will deploy a Smart Grid ecosystem (system of systems) that is highly available, easily upgraded, interoperable, and that is capable of maintaining transactional integrity despite losses of communication between system components.

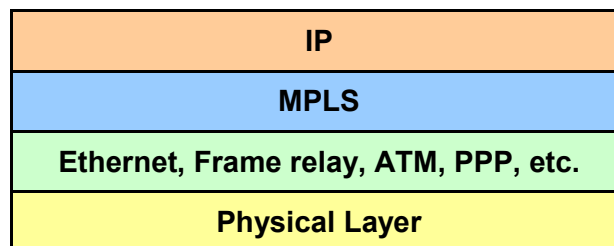
Web services are a set of emerging standards that enable interoperable integration between heterogeneous IT processes and systems. Web services provide a common standard mechanism for interoperable integration among disparate systems, and the key to their utility is their standardization. This common mechanism for delivering a "service" makes them ideal for implementing a Service-Oriented Architecture (SOA).

Besides using the common Web transports, Web services also require a common language for the data exchanged – Extensible Markup Language (XML). XML is simply the “scaffolding” for the actual exchange. For the Web services protocols to be interoperable across diverse systems and suitable for Smart Grid applications, standards bodies, such as W3C, OASIS, and WS-I must formally standardize these protocols. KCP&L continues to implement these standards and contribute to the SOA standards adoption process with other utilities through participation in user groups and standards bodies.

2.1.1.2.1.2 Interoperability of Communications Networks

With respect to the underlying communications network, KCP&L is implementing increasingly meshed approaches with redundant communications paths and traffic prioritization features (Figure 2-1). In part, this is being accomplished through adoption of Multi-Protocol Label Switching (MPLS) as specified by the Internet Engineering Task Force (IETF).

Figure 2-1: KCP&L MPLS-based IP Communication



MPLS is a highly scalable and protocol agnostic data-carrying mechanism that can encapsulate legacy routing protocols. MPLS offers enhanced security and robust communication failover capabilities. In addition, the protocol allows segmentation, prioritization and optimization of specific traffic, such as control and market information.

2.1.1.3 SmartGrid Demonstration Communication Networks

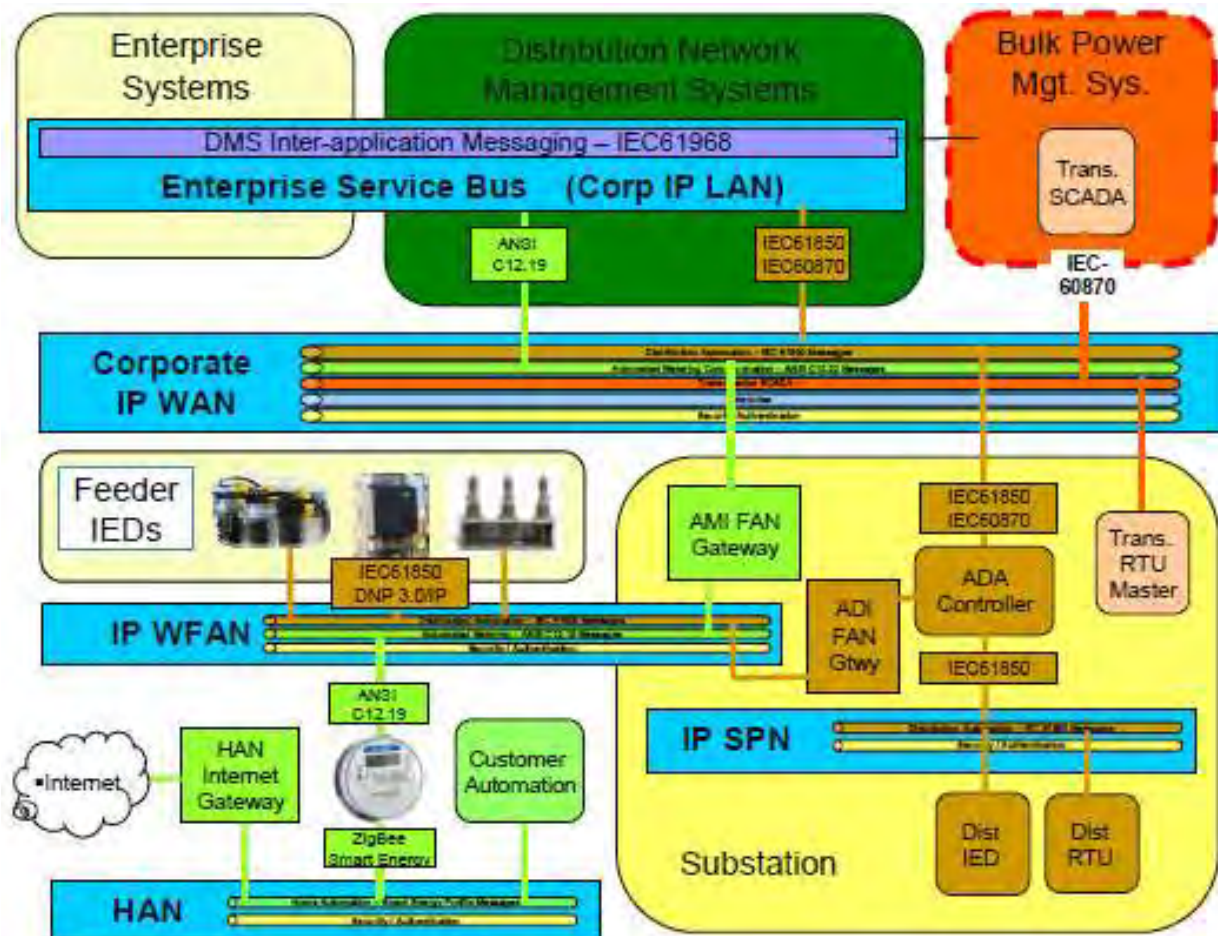
The public Internet is a very powerful, all-pervasive medium. It can provide very inexpensive means to exchange information with a variety of other entities. The Internet is being used by some utilities for exchanging sensitive market information, retrieving power system data, and even issuing some control commands to generators. Despite standard security measures, such as security certificates, a number of vulnerabilities still exist.

KCP&L has chosen to implement its SmartGrid Demonstration Project using private communications media wherever practical. By using the corporate IT WAN and a utility-owned FAN, the KCP&L SmartGrid pilot solution can still leverage the vast amount of research and development into Internet Protocols (IP) and technologies. They will just be implemented over a private Intranet instead of the public Internet to minimize the exposure to cyber security risks. The communications and information networks proposed to support the deployment of the SmartGrid Demonstration Project are depicted in Figure 2-2.

The far reaching and complex nature of the Smart Grid dictates that no single communications technology or security policy can be developed to implement and properly secure the Smart Grid. The hierarchical nature of the technologies that will be implemented to create the SmartGrid Communication Network provides for security “check-points” between control and network layers that may have different security requirements. Therefore, it is a natural extension for the Security Architecture to be constructed around Security Domains.

A Security Domain represents a set of resources (e.g. network, computational, and physical) that share a common set of security requirements and risk assessments. For example, within the 'bulk power system' there are two distinct Security Domains: NERC-CIP and non NERC-CIP. While having different security requirements, all Security Domains will be secured and managed through a consistent set of security policies and processes. Secure connectivity, data encryption, firewall protection, intrusion detection, access logging, change control and the audit reports associated with these applications will likely be required for all SmartGrid security domains.

Figure 2-2: KCP&L SmartGrid Demonstration Project Communication Network

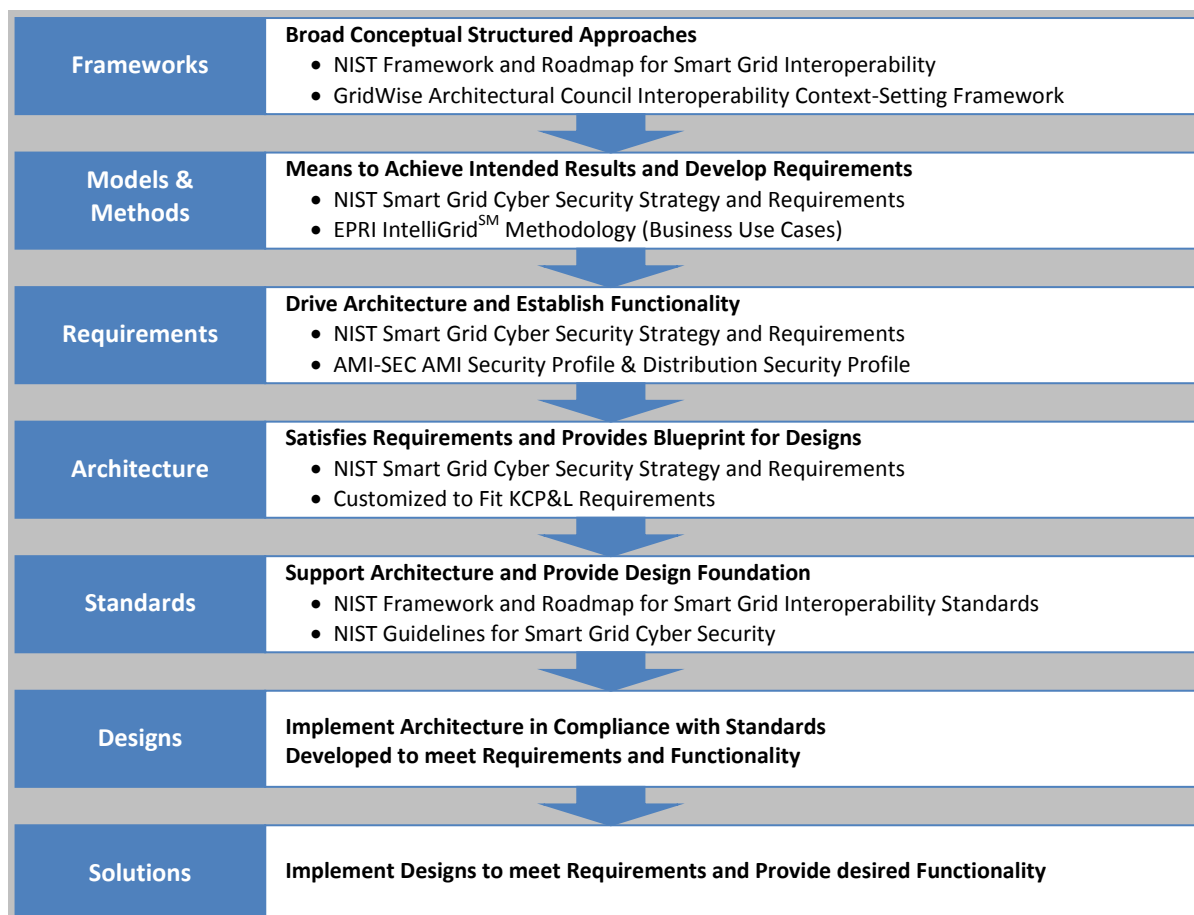


2.1.1.4 Interoperability Plan and Approach

To meet the interoperability challenges associated with ensuring interoperability across the SmartGrid Demonstration Project, KCP&L will use a structured approach as outlined in Figure 2-3. This involves adoption of industry frameworks for interoperability from the GridWise Alliance, the National Institute of Standards and Technology (NIST) and the International Electrotechnical Commission (IEC).

The frameworks, and their associated models and methods will be used to derive architectures that satisfy requirements for interoperability. The architectures will be implemented as blueprints for designs. These components together comprise the KCP&L solution for Smart Grid and, when applied throughout the system life-cycle will ensure that the solution meets KCP&L's business requirements, achieves intended legal and regulatory objectives, operates securely and efficiently, enables reliability and agility, and can be easily integrated within the larger electric grid.

Figure 2-3: KCP&L SmartGrid Interoperability Approach



2.1.1.4.1 Frameworks

A solution framework captures key domains and their interactions in order to enable discussions between partners as to how their contributions address the overall solution. It is used to communicate within the electricity system to compare, align, and harmonize solutions and processes as well as with the management of other critical infrastructure. With the support of the context-setting framework, opportunities and hindrances to interoperability can be debated and prioritized for resolution. Cross-cutting issues, such as cyber security and privacy, are areas that need to be addressed in all aspects of the model and agreed upon to achieve interoperation. They usually are relevant to more than one interoperability category of the framework. The framework makes no architectural or technical

recommendations. However, architectures will be derived from the framework and designs developed based on the architectural blueprints.

2.1.1.4.1.1 NIST SmartGrid Framework [6]

This KCP&L solution framework will be aligned with the NIST Special Publication 1108R2 - NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2. This document identifies guiding principles for the adoption of standards for the Smart Grid and the Smart Grid domains to which interfaces and standards apply. It also identifies standards for consideration and incorporation into Smart Grid architectures and solution designs. Applicable standards will be incorporated into the KCP&L demonstration project.

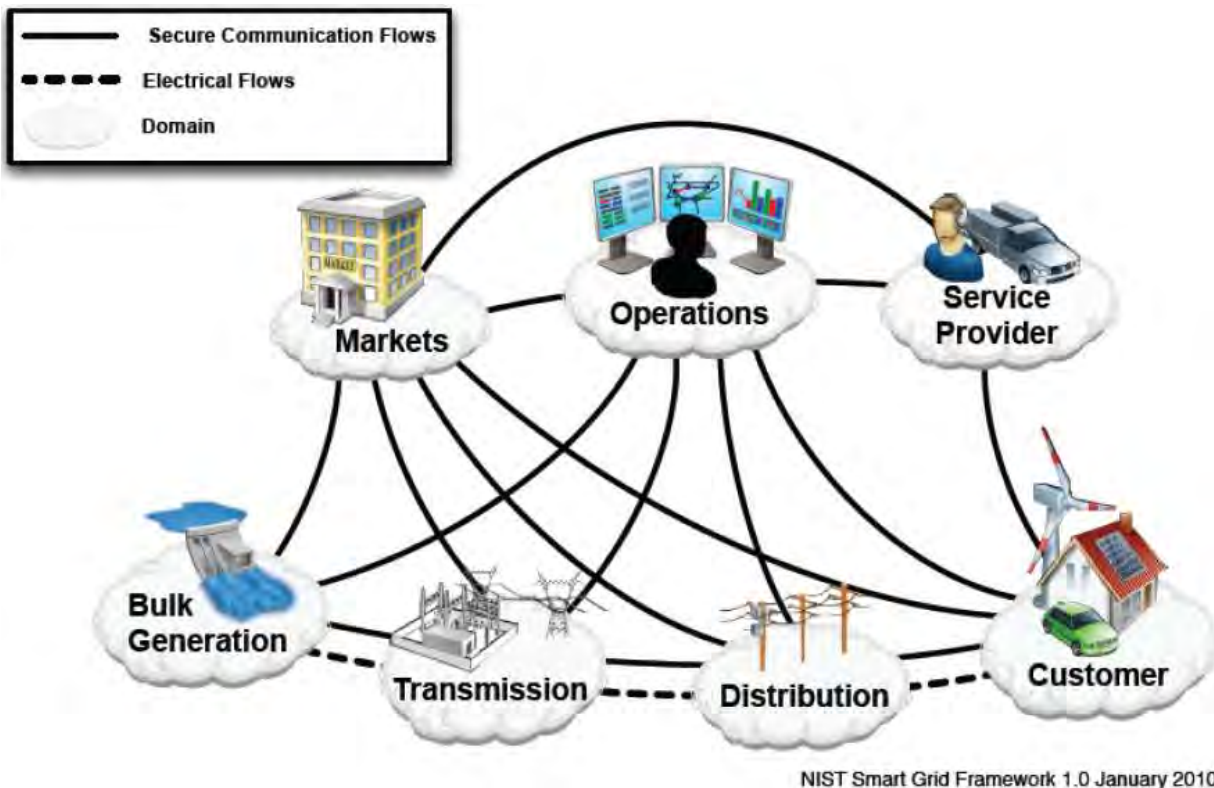
The Smart Grid is a complex system of systems for which a common understanding of its major building blocks and how they interrelate must be broadly shared. NIST has developed a conceptual model to facilitate this shared view. This model provides a means to analyze Use Cases, identify interfaces for which interoperability standards are needed, and facilitate development of a cyber security strategy. For this purpose, NIST adopted a model that divides the Smart Grid into seven domains (described in Table 2-1 and shown in Figure 2-4).

Each domain—and its sub-domains—encompass Smart Grid actors and applications. Actors include devices, systems, or programs that make decisions and exchange information necessary for performing applications: smart meters, solar generators, and control systems represent examples of devices and systems. Applications, on the other hand, are tasks performed by one or more actors within a domain. For example, corresponding applications may be home automation, solar energy generation and energy storage, and energy management. The *NIST Framework and Roadmap for Smart Grid Interoperability Standards* describes the seven Smart Grid domains in more detail.

Table 2-1: Domains & Actors in the Smart Grid Conceptual Model

Domain	Actors in the Domain
Customers	The end users of electricity. May also generate, store, and manage the use of energy. Traditionally, three customer types are discussed, each with its own domain: residential, commercial, and industrial.
Markets	The operators and participants in electricity markets.
Service Providers	The organizations providing services to electrical customers and utilities.
Operations	The managers of the movement of electricity.
Bulk Generation	The generators of electricity in bulk quantities. May also store energy for later distribution.
Transmission	The carriers of bulk electricity over long distances. May also store and generate electricity.
Distribution	The distributors of electricity to and from customers. May also store and generate electricity.

In general, actors in the same domain have similar objectives. In order to enable Smart Grid functionality, the actors in a particular domain often interact with actors in other domains, as shown in Figure 2-4. However, communications within the same domain may not necessarily have similar characteristics and requirements. Moreover, particular domains also may contain components of other domains. For instance, the ten Independent System Operators and Regional Transmission Organizations (ISOs/RTOs) in North America have actors in both the Markets and Operations domains. Similarly, a distribution utility is not entirely contained within the Distribution domain—it is likely to contain actors in the Operations domain, such as a distribution management system, and in the Customer domain, such as meters.

Figure 2-4: Interaction of Actors in Different Smart Grid Domains

Underlying the conceptual model is a legal and regulatory framework that includes policies and requirements that apply to various actors and applications and to their interactions. Regulations, adopted by the Federal Energy Regulatory Commission at the federal level and by public utility commissions at the state and local levels, govern many aspects of the Smart Grid.

2.1.1.4.1.2 GridWise Architecture Council Interoperability Framework [7]

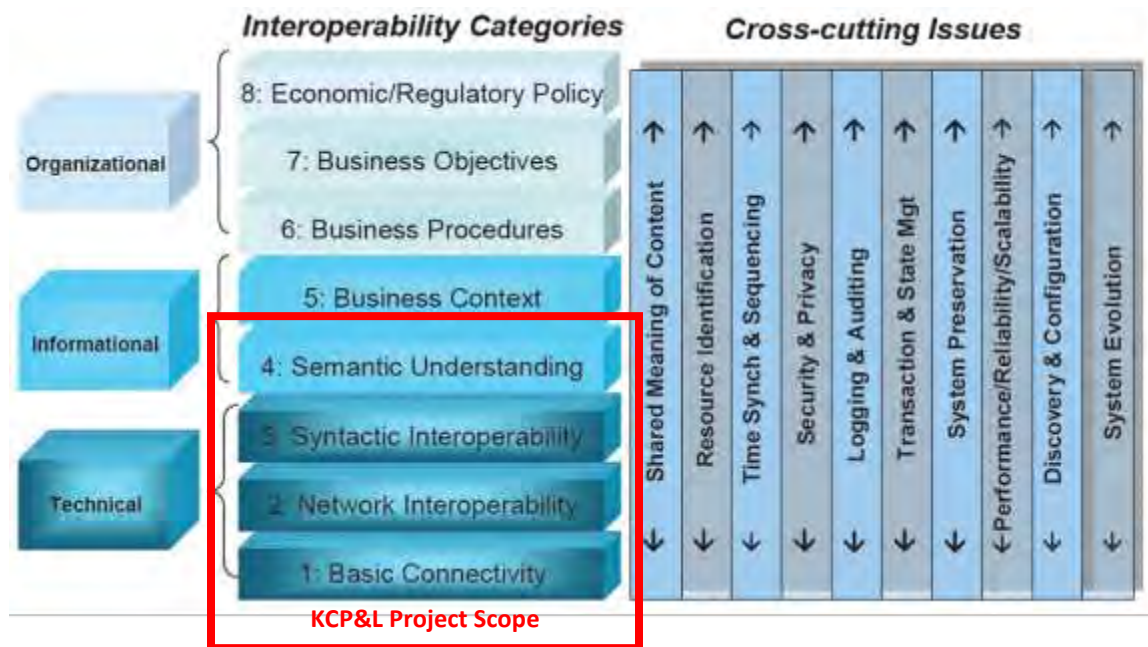
KCP&L will utilize the GridWise Architecture Council's (GWAC) Interoperability Context-Setting Framework to align the solution, make appropriate interoperability decisions, and deliver the anticipated results to the stakeholder community.

The GridWise interoperability context-setting framework identifies eight interoperability categories that are relevant to the mission of systems integration and interoperation in the electrical end-use, generation, transmission, and distribution industries. The major aspects for discussing interoperability fall into three categories: technical, informational, and organizational. The organizational categories emphasize the pragmatic aspects of interoperation. They represent the policy and business drivers for interactions. The informational categories emphasize the semantic aspects of interoperation. They focus on what information is being exchanged and its meaning. The technical categories emphasize the syntax or format of the information. They focus on how information is represented within a message exchange and on the communication medium.

Figure 2-5 depicts these categories of interoperability. The framework pertains to an electricity plus information infrastructure. At the organizational layers, the pragmatic drivers revolve around the management of electricity. At the technical layers, the communications network and syntax issues are information technology oriented. In the middle, we transform information technology into knowledge that supports the organization aspects of the electricity-related business. The material in the *GridWise Interoperability Context-Setting Framework* describes each subcategory. Each layer typically depends

upon, and is enabled by, the layer below it. The KCP&L SmartGrid Demonstration Project will focus on the four (4) lower layers of the GridWise Architecture Council (GWAC) Stack as anchor points for the interoperability testing and demonstration.

Figure 2-5: GridWise Interoperability Framework



2.1.1.4.2 Methods and Models

As a member of EPRI's five-year Smart Grid demonstration project, our system integration and interoperability requirements definition and design will also be coordinated through EPRI's formalized smart grid demonstration project. We will leverage EPRI's IntelliGridSM methodology to support the technical foundation for a smart power grid that links electricity with communications and computer control. The IntelliGridSM Architecture is an open-standard, requirements-based approach for integrating data networks and equipment that enables interoperability between products and systems.

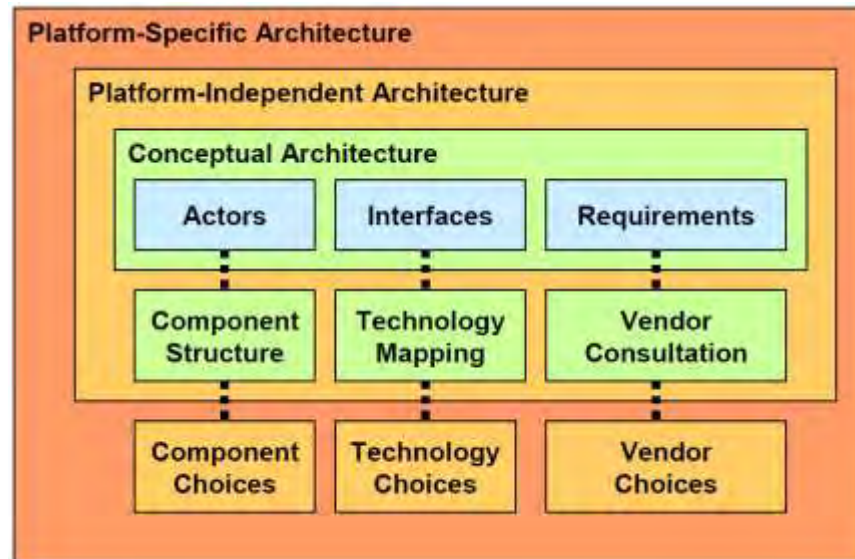
2.1.1.4.2.1 EPRI IntelliGrid Methodology [8]

EPRI's IntelliGridSM methodology provides tools and recommendations for standards and technologies when implementing systems such as advanced metering, distribution automation, and demand response and also provides an independent, unbiased approach for testing technologies and vendor products. The IntelliGridSM methodology was developed at EPRI over a six year period and turned over to the International Electrotechnical Commission (IEC). EPRI has applied this methodology to help a number of utilities (FirstEnergy, Salt River Project, Alliant Energy, Duke Energy, Southern Company, and TVA) with specific roadmaps for smart grid development and deployment in addition to working with industry members of the IntelliGridSM research program to continually advance the interoperability standards and methods for the industry.

The IntelliGridSM methodology starts with a conceptual architecture and then moves to development of a platform-independent architecture that provides a basis for integrating actual applications. The ultimate goal is architecture with vendor specific aspects with the ability to plug-in many different vendor applications as a result of industry standard interfaces. Legacy systems and technology is integrated via appropriate gateways and translators. Figure 2-6 illustrates the concept of designing an architecture that starts with a conceptual architecture and then moves to development of a platform-

independent architecture that provides a basis for integrating actual applications. The requirements developed in this project help provide the basis for the architecture design. For instance, the architecture should support new technologies like substation video and infrared camera data.

Figure 2-6: IntelliGridSM Architecture Definition Evolution



IntelliGridSM methodology defines an Environment as a logical grouping of power system requirements that could be addressed by a similar set of distributed computing technologies. Within a particular environment, the information exchanges used to perform power system operational functions have very similar architectural requirements, including their:

- Configuration requirements
- Quality of service requirements
- Security requirements
- Data management requirements

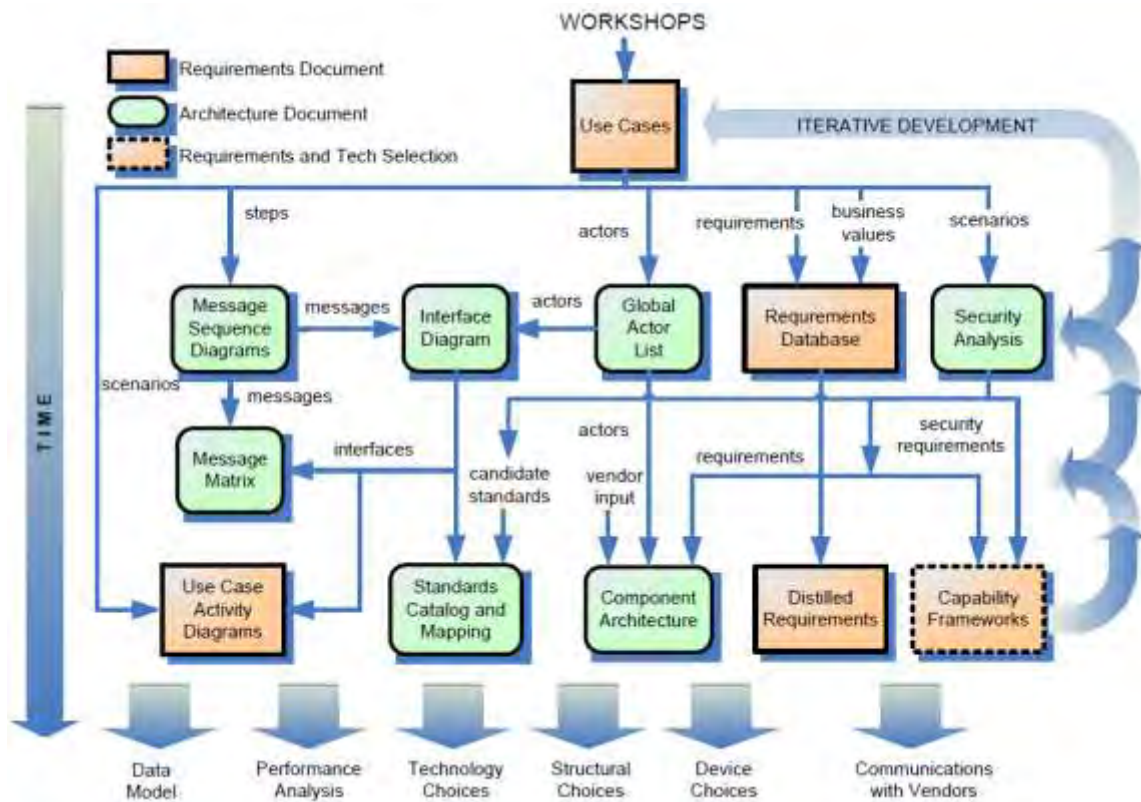
The IntelliGridSM methodology results in both a plan for the integrated information infrastructure and a study of the requirements and principles required to make particular automation projects work. In basic terms, the IntelliGridSM architecture is a set of high level concepts that are used to design a technology independent architecture as well as identify and recommend standard technologies, and best practices. These high level concepts include:

- The use of object models and modeling services to give standardized names to data, and to describe their relationships, formats, and interactions in standardized ways
- The development of security policies and the implementation of security technologies where needed, not only to prevent security attacks and inadvertent mistakes, but also to handle recovery from inevitable failures
- The inclusion of network and system management to monitor and control the information infrastructure in a manner similar to the monitoring and control of the power system
- Reduction in stranded assets from systems that can integrate
- Ability to incrementally build upon first steps; and then scale up massively
- Reduced development costs by building on components of IntelliGridSM architecture systems engineering
- Robustness achieved from structured approaches to systems management
- Architecture is necessary to consistently and adequately secure the energy industry

The Smart Grid infrastructure is defined by the applications and technologies that are built on it. This is at the heart of the “Use Case process” that is used to define the requirements for the Smart Grid. Use Cases define the applications in a way that can be used to determine the specific requirements for communications infrastructure, new technologies, and information integration. From the Use Cases, thorough and effective test plans may be developed as described in Figure 2-7.

The results of the Use Case analysis will be compared against the existing and emerging technologies, standards and best practices of the industry. The focus will be on what technologies best enable building the new architecture on top of what exists now and what will emerge in the future. The recommended technologies, standards and best practices pertaining to the creation, storage, exchange and usage of various forms of power system information will be evaluated and rated.

Figure 2-7: IntelliGridSM Use Case Driven Interoperability Test Plan Development Process



2.1.1.4.2.2 NIST SmartGrid Interface Reference Model [6]

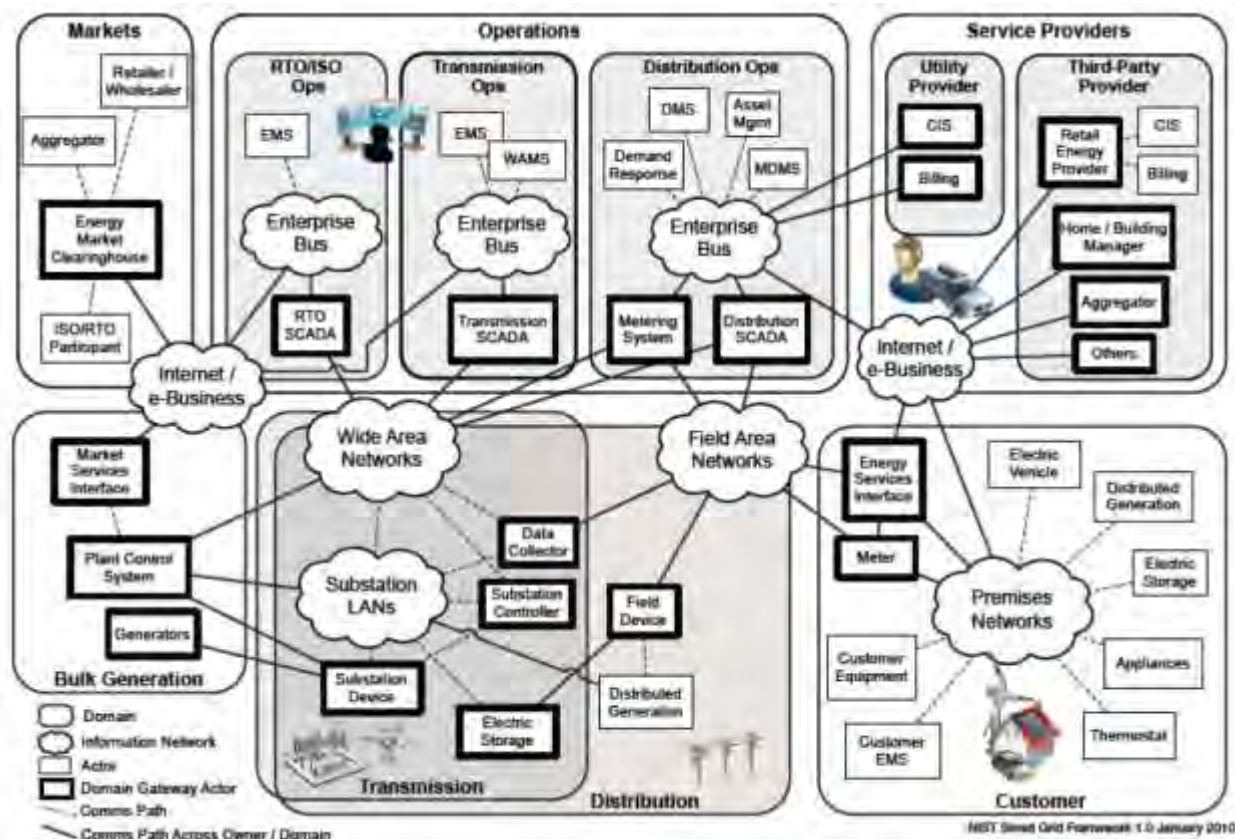
The Smart Grid is a complex system of systems for which a common understanding of its major building blocks and how they interrelate must be broadly shared. The Smart Grid will ultimately require hundreds of standards, specifications, and requirements. Some are needed more urgently than others. To prioritize its work, NIST chose to focus initially on standards needed to address the priorities identified in the Federal Energy Regulatory Commission (FERC) Policy Statement, plus additional areas identified by NIST. The eight priority areas were:

- Demand Response and Consumer Energy Efficiency
- Wide-Area Situational Awareness
- Energy Storage
- Electric Transportation
- Advanced Metering Infrastructure
- Distribution Grid Management

- Cyber Security
- Network Communications

NIST, with the assistance of EPRI and using the IntelliGridSM methodology, developed a conceptual architectural reference model illustrated in Figure 2-8 to facilitate this shared view. This model identifies interfaces among domains and actors. The model provides a means to analyze Use Cases, identify interfaces for which interoperability standards are needed, and facilitate development of a cyber security strategy.

Figure 2-8: NIST Smart Grid Logical Interface Reference Model



2.1.1.4.2.3 NIST/SGIP Smart Grid Cyber Security Logical Reference Model [9]

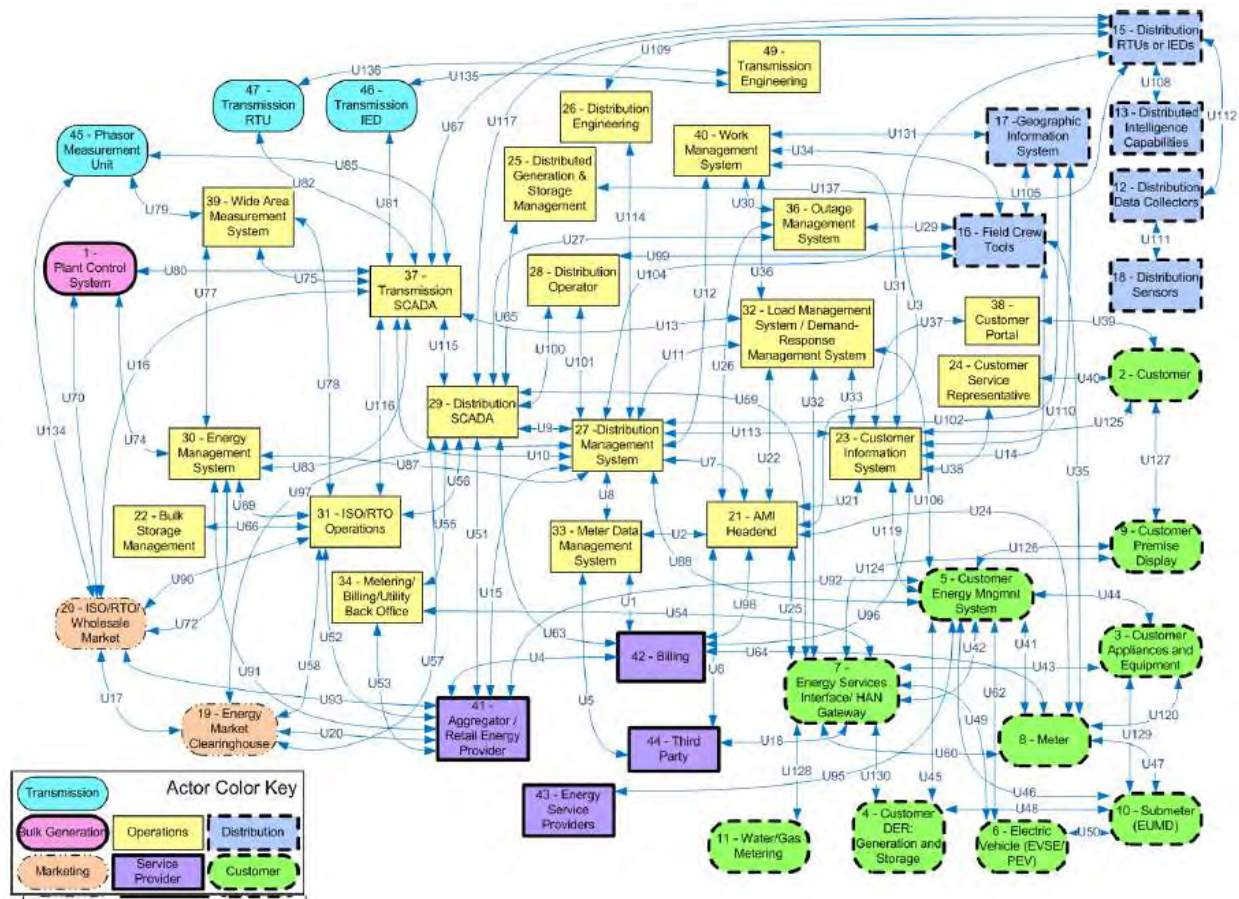
The SGIP Cyber Security Working Group (CSWG) developed a logical reference model of the Smart Grid, including all the major domains—service providers, customer, transmission, distribution, bulk generation, markets, and operations—that are part of the NIST conceptual model. In the future, the NIST conceptual model and the logical reference model included in this report will be used by the SGIP Architecture Committee (SGAC) to develop a single Smart Grid architecture that will be used by the CSWG to revise the logical security architecture included in this report.

Communications among actors in the same domain may have similar characteristics and requirements. Domains may contain subdomains. An actor is a device, computer system, software program, or the individual or organization that participates in the Smart Grid. Actors have the capability to make decisions and to exchange information with other actors. Organizations may have actors in more than one domain. The actors illustrated in this case are representative examples and do not encompass all the actors in the Smart Grid. Each of the actors may exist in several different varieties and may contain many other actors within them.

The logical reference model represents a blending of the initial set of Use Cases, requirements that were developed at the NIST Smart Grid workshops, the initial NIST Smart Grid Interoperability Roadmap, and the logical interface diagrams for the six FERC and NIST priority areas: electric transportation, electric storage, advanced metering infrastructure (AMI), wide area situational awareness (WASA), distribution grid management, and customer premises.

The logical reference model is a work in progress and will be subject to revision and further development. Additional underlying detail as well as additional Smart Grid functions will be needed to enable more detailed analysis of required security functions. Figure 2-9 illustrates, at a high level, the diversity of systems as well as a first representation of associations between systems and components of the Smart Grid.

Figure 2-9: NIST Smart Grid Cyber Security Logical Reference Model



2.1.1.4.3 Requirements

Requirements define what the Smart Grid is and does. Requirements that drive and specify the functions and how they are applied are foundational to the realization of the Smart Grid. The following are some of the key characteristics of effective requirements:

- Industry policies and rules of governance are well developed, mature, and can be consistently applied
- Requirements are well-developed by domain experts and well documented following mature systems-engineering principles
- Requirements define support for applications and are well developed enough to support their management and cyber security as well

2.1.1.4.3.1 KCP&L Application Use Cases

The Use Case process is a mature, industry-accepted practice for describing system behavior as requests are made from it. Use Cases provide a “who does what in what order” analysis. Use Cases are a means to an end, in that they drive requirements which are rational, comprehensive, and defensible.

The IntelliGridSM methodology assists in developing Use Cases in a systematic manner, all with the goal of identifying and documenting all significant requirements.

The steps to define a Use Case include:

1. **Review the Scope of the Use Case.** Identify known assumptions, constraints, and business rules for the Use Case.
2. **List the Actors.** What goals do they want to accomplish? What information will they generate/consume?
3. **Identify the Scenario Pre-Conditions and Assumptions.** What must happen before the scenario can start? What conditions can we assume to exist, or be true, at the start of the scenario?
4. **Identify the Scenario Post-Conditions.** What must happen after the scenario is complete? What is the observable state or status after the implementation of the Use Case?
5. **Identify the Steps for the Scenario.** As each step is defined, identify requirements for that step to occur.
6. **Define Information Exchanged and Requirements for the Steps.** What information is exchanged and between who? What is required for the step to occur (Functional)? What type of targets, behavior, and performance measures must be reached for that requirement (Nonfunctional)?
7. **Identify Alternate Scenarios.** What happens when things go wrong?
8. **Check if We’re Done.** Did the primary actor reach its goal?

The KCP&L SmartGrid Demonstration Project team has identified more than 90 use cases to cover the breadth of the KCP&L SmartGrid demonstration project. The use cases have been organized into the following groupings:

- Network Communications
- Advanced Metering Infrastructure
- Meter Data Management
- Home Area Network
- SmartEnd-Use
- Demand Response Management
- Distribution Substation Automation
- First Responder
- Distribution Management System
- Plug-in Electric Vehicle Charging

The identified Use Cases are by no means a comprehensive listing of Smart Grid Use Cases. As the Smart Grid develops, additional Use Cases will be needed to support new and evolving functions and technologies. KCP&L fully expects that this listing of Use Cases will change slightly through the detailed project design process.

The KCP&L project team acknowledges the prior works of many individuals that form the basis of the Use Cases developed specifically for our project. Prior works by EPRI, SCE, AEP, and the OpenHAN organization provided a foundation for the majority of this work product.

2.1.1.4.3.2 Industry Requirement Profiles

Detailed requirements will be determined by using the method and models mentioned in the preceding section, analyzing KCP&L's business objectives for the demonstration, and using the following industry reference documents:

- NIST NISTR 7628 – Smart Grid Cyber Security Strategy and Requirements
- UtilityAMI AMI Enterprise System Requirements Specification v1.0
- UCAIug (ASAP-SG) Security Profile for Distribution Management (draft)
- UCAIug (ASAP-SG) Security Profile for Third Party Data Access (draft)
- UCAIug (ASAP-SG) Security Profile for Advanced Metering Infrastructure v2.0
- UCAIug (OpenHAN) Home Area Network System Requirements Specification v2.0

2.1.1.4.4 Architecture and Design [10]

It is difficult for organizations and industries to change. Many strategic initiatives end in failure because the required changes are viewed in isolation rather than in relation to the complete infrastructure. When building reference model architectures, there are three key architecture types:

- Conceptual – Services (e.g. Outage Detection Service)
- Logical – Components (e.g. Outage Management System)
- Physical – Implementations (e.g. OMS)

Developing a conceptual SmartGrid architecture model based on goals and requirements will further enhance an organization's ability to be effective in the implementation of core strategy and vision.

The National Institute of Standards and Technology (NIST) Smart Grid Interoperability Panel (SGIP) Smart Grid Architecture Committee (SGAC) is responsible for creating and refining a Smart Grid conceptual architecture reference model. On July 16, 2010, the SGAC approved a plan to develop a generic Smart Grid conceptual architecture by January 2011. The process for developing a generic Smart Grid conceptual architecture will be based on three key process tasks:

- Developing grid architecture goals from national energy goals and national policy documents
- Developing a formalized list of requirements relating to and mapped to each of the accepted grid architecture goals
- Developing a list of energy services based on the list of accepted requirements

The final deliverable of a generic Smart Grid conceptual architecture will allow grid participants to develop their own internal logical and physical architectures.

The systems architecture and designs developed for the KCP&L SmartGrid Demonstration Project will satisfy the requirements developed through the processes outlined in the preceding section. It will leverage existing industry reference architectures and architectural artifacts, such as those developed by GWAC, NIST, and UCAIug.

The demonstration project architecture and systems design will also leverage the IEC 61968 series for Application Integration at Electric Utilities, the IEC 61850 series for Communication Networks and Systems in Substations, and other emerging standards discussed in the next section.

The KCP&L project team is participating in the NIST/SGIP sponsored SmartGrid Conceptual Architecture Model development efforts and as this architectural reference emerges, it will be considered for adoption into the KCP&L SmartGrid Demonstration Project system architecture.

2.1.1.4.5 Standards

This SmartGrid Demonstration Project architecture and standards to be implemented are closely aligned with the *NIST Special Publication 1108 - NIST Framework and Roadmap for Smart Grid Interoperability*

Standards. This document identifies guiding principles for the adoption of standards for the Smart Grid and the Smart Grid domains to which interfaces and standards apply. It also identifies standards for consideration and incorporation into Smart Grid architectures and solution designs.

Additionally, in the NIST Framework, NIST recommends some criteria for adoption of standards. Generally, these involve openness and accessibility. NIST believes that Smart Grid interoperability standards should be open. The term “open” standard as used by NIST means that a standard is “developed and maintained through a collaborative, consensus-driven process that is open to participation by all relevant and materially affected parties and not dominated or under the control of a single organization or group of organizations, and readily and reasonably available to all for Smart Grid applications”. In addition, NIST states that Smart Grid interoperability standards should be developed and implemented internationally, wherever practical. Figure 2-10 summarizes the NIST criteria for standards adoption to achieve interoperability which have been adopted by KCP&L.

2.1.1.4.6 Summary

This section presented a strategy, approach, models and methods for achieving interoperability between components of the KCP&L SmartGrid Demonstration Project.

Adoption of the applicable standards, and the other aspects of the frameworks described in this section will ensure that interoperability is appropriately aligned with business objectives including integration with other market participants.

Additionally, not all standards considered may ultimately be adopted. However, each will be considered for adoption along with other emerging standards and guidelines using the structured approach outlined in this document and incorporated into vendor agreements and procurement language as appropriate. Adopting the NIST and GWAC Interoperability frameworks, along with the EPRI methods, will ensure that interoperability is a primary consideration throughout the lifecycle of the KCP&L SmartGrid solution, and that the appropriate artifacts are documented.

Figure 2-10: NIST Guiding Principles for Identifying Standards for Implementation

For *Release 2.0*, a standard, specification, or guideline is evaluated on whether it:

- Is well-established and widely acknowledged as important to the Smart Grid.
- Is an open, stable, and mature industry-level standard developed in a consensus process from a standards development organization (SDO).
- Enables the transition of the legacy power grid to the Smart Grid.
- Has, or is expected to have, significant implementations, adoption, and use.
- Is supported by an SDO or standards- or specification-setting organization (SSO) such as a users group to ensure that it is regularly revised and improved to meet changing requirements and that there is a strategy for continued relevance.
- Is developed and adopted internationally, wherever practical.
- Is integrated and harmonized, or there is a plan to integrate and harmonize it with complementing standards across the utility enterprise through the use of an industry architecture that documents key points of interoperability and interfaces.
- Enables one or more of the framework characteristics as defined by EISA* or enables one or more of the six chief characteristics of the envisioned Smart Grid.[†]
- Addresses, or is likely to address, anticipated Smart Grid requirements identified through the NIST workshops and other stakeholder engagement.
- Is applicable to one of the priority areas identified by FERC[‡] and NIST:
 - Demand Response and Consumer Energy Efficiency;
 - Wide Area Situational Awareness;
 - Electric Storage;
 - Electric Transportation;
 - Advanced Metering Infrastructure;
 - Distribution Grid Management;
 - Cybersecurity; and
 - Network Communications.
- Focuses on the semantic understanding layer of the GWAC stack,^{*} which has been identified as most critical to Smart Grid interoperability.
- Is openly available under fair, reasonable, and non-discriminatory terms.
- Has associated conformance tests or a strategy for achieving them.
- Accommodates legacy implementations.
- Allows for additional functionality and innovation through:
 - *Symmetry* – facilitates bidirectional flows of energy and information.
 - *Transparency* – supports a transparent and auditable chain of transactions.
 - *Composition* – facilitates building of complex interfaces from simpler ones.
 - *Extensibility* – enables adding new functions or modifying existing ones.
 - *Loose coupling* – helps to create a flexible platform that can support valid bilateral and multilateral transactions without elaborate prearrangement.**
 - *Layered systems* – separates functions, with each layer providing services to the layer above and receiving services from the layer below.
 - *Shallow integration* – does not require detailed mutual information to interact with other managed or configured components.

* GridWise Architecture Council, GridWise Interoperability Context-Setting Framework, March 2008.

** While loose coupling is desirable for general applications, tight coupling often will be required for critical infrastructure controls.

2.1.2 Cyber Security Strategy & Plan [11]

The KCP&L project team developed and published a “SmartGrid Cyber Security Plan” that detailed a strategy and approach for implementing cyber security in the KCP&L SmartGrid Demonstration Project (SGDP). The following subsections provide an overview of the significant elements of the cyber security plan developed for the project.

The cyber security strategy and approach is intended to have broad applicability beyond the SGDP including future development of the portions of the SGDP that ultimately extend into production systems.

The terms ‘cyber security’ and ‘cyber infrastructure’ are used throughout this document. The following definitions are used in the U.S. National Infrastructure Protection Plan (NIPP) and are included to ensure a common understanding:

- **Cyber Security:** The protection required to ensure confidentiality, integrity and availability of the electronic information communication system
- **Cyber Infrastructure:** Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example, computer systems, control systems (e.g., SCADA), networks, including the Internet and cyber services (e.g., managed security services), are all part of cyber infrastructure.

2.1.2.1 Smart Grid Cyber Security Trends & Challenges

Cyber security for the electric grid is evolving in response to several accelerating trends:

- Increasing scrutiny of regulators, customers, shareholders and external entities due to a heightened awareness of the potential for a catastrophic failure or attack on the nation’s critical infrastructure
- Emerging threats to the security of the grid by terrorist nation-states, countries and criminal organizations who may target the electric grid with increasingly sophisticated methods of attack
- Increasing dependence on “smart” networked, IP-enabled devices to monitor and control the grid and decreasing reliance on serial devices communicating over closed networks
- Moving from proprietary systems requiring special expertise known only to a few individuals with specialized skills towards cost and efficiency advantages gained through the use of open operating systems, application platforms and communications protocols
- Increasing use of efficiencies to be gained through using wireless communication and public communications networks, often using non-proprietary technologies and protocols
- Increasing the degree of the distributed electric grid within generation and markets, and the evolution of domains such as distributed generation assets that are not under the direct ownership and control of the utility

The factors noted above contribute to several challenges when considering an approach to securing the grid:

- Cyber security mechanisms must be employed throughout the system life cycle and end-to-end to secure all of the potential attack points in the grid. These attack points are increasing in number. Also, the risk of compromise has increased due to both intentional

and unintentional traditional IT-oriented threats, which increasingly have the potential to affect control systems within the grid.

- Reliability and availability of the grid remain primary considerations, and security controls must not degrade grid reliability and availability.
- Utilities, vendors and standards bodies have been slow to respond to security challenges and incorporate cyber security mechanisms into their products, partially because of these challenges, shifting business requirements and changing regulatory landscapes.
- Mechanisms to detect anomalous behavior within the grid indicating that a cyber-attack on control systems is underway are immature, and some standard operating procedures and disaster scenarios do not adequately account for responses to cyber events.

2.1.2.2 Cyber Security Strategy & Approach

The challenges outlined in the preceding section will be met through the development of a cyber-security controls framework, design, architecture, and infrastructure that ensures that technologies, policies, processes and procedures result in adherence to existing cyber security regulations, evolving Smart Grid security requirements and KCP&L's business requirements. This will be accomplished by adoption of the NIST/EPRI security framework (NIST SP 1108R2: NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 2.0 February 2012 and NISTIR-7628: Guidelines for Smart Grid Cyber Security – August 2010) and other frameworks, subject to KCP&L's business requirements and SGDP budget considerations. Implementing the controls identified in the framework consists of the following activities to provide end-to-end security:

- Perform a comprehensive risk assessment [12] and adopt a risk management strategy to ensure risk-based decision making throughout the system's life cycle
 - Categorize the interfaces according to the framework (i.e., the types of domains that are involved in particular use cases)
 - Identify and analyze all logical interfaces to determine the risks to confidentiality, integrity and availability exposed through them
- Determine cyber security requirements
- Select appropriate controls and technical countermeasures to mitigate the risks and rationalize these in a cyber-security architecture
- Develop and deploy a cyber-security governance, risk management and compliance process and tools tailored for the KCP&L operations environment and project budget
- Implement the countermeasures and controls, leveraging existing cyber security infrastructure capabilities to the extent possible according to an integrated secure systems design
- Test and validate whether the deployed cyber security infrastructure is providing the expected security assurance
- Develop plans to remediate cyber security gaps and address residual risks
- Develop and implement cyber security criteria in procurement language and device vendor selection in accordance with best practices
- Monitor the ongoing development of Smart Grid cyber security standards and requirements for incorporation into KCP&L's strategic plans

The overall cyber security strategy examines both domain-specific and common requirements when developing a mitigation strategy to ensure interoperability of solutions across different parts of the infrastructure. Implementation of a cyber-security strategy requires the development of an overall cyber security risk management framework for the Smart Grid. This framework is based on existing risk management approaches developed by KCP&L and other best practice organizations.

Figure 2-11: KCP&L SmartGrid Security Strategy and Approach

This risk-driven approach to cyber security, depicted in Figure 2-11 above, along with architectural discipline imposed through governance and compliance assessment frameworks will ensure that security expenditures are aligned with business objectives and project budgets. In conjunction with the cyber security architecture, security design objectives will be identified for authentication, access control, logging and auditing, data confidentiality, data integrity and non-repudiation, Service-Oriented Architecture (SOA) and messaging security.

Once the conceptual architecture is completed, high-level and detailed designs will be completed for the cyber security infrastructure. The designs will be documented, refined and validated against the architecture through use cases and scenarios. The risk assessment will be updated if new risks are discovered and additional controls and countermeasures will be deployed using risk mitigation methods within the risk management process.

Well-defined processes, methods, and software solutions are designed to assist and automate the implementation of risk and compliance management processes. Therefore, the solution involves identifying and customizing tools to meet the specific requirements of KCP&L and integrating these tools and methods into a comprehensive solution applicable to the operations environment. The infrastructure will be deployed in a manner consistent with the Government, Risk, and Compliance (GRC) framework shown in Figure 2-12.

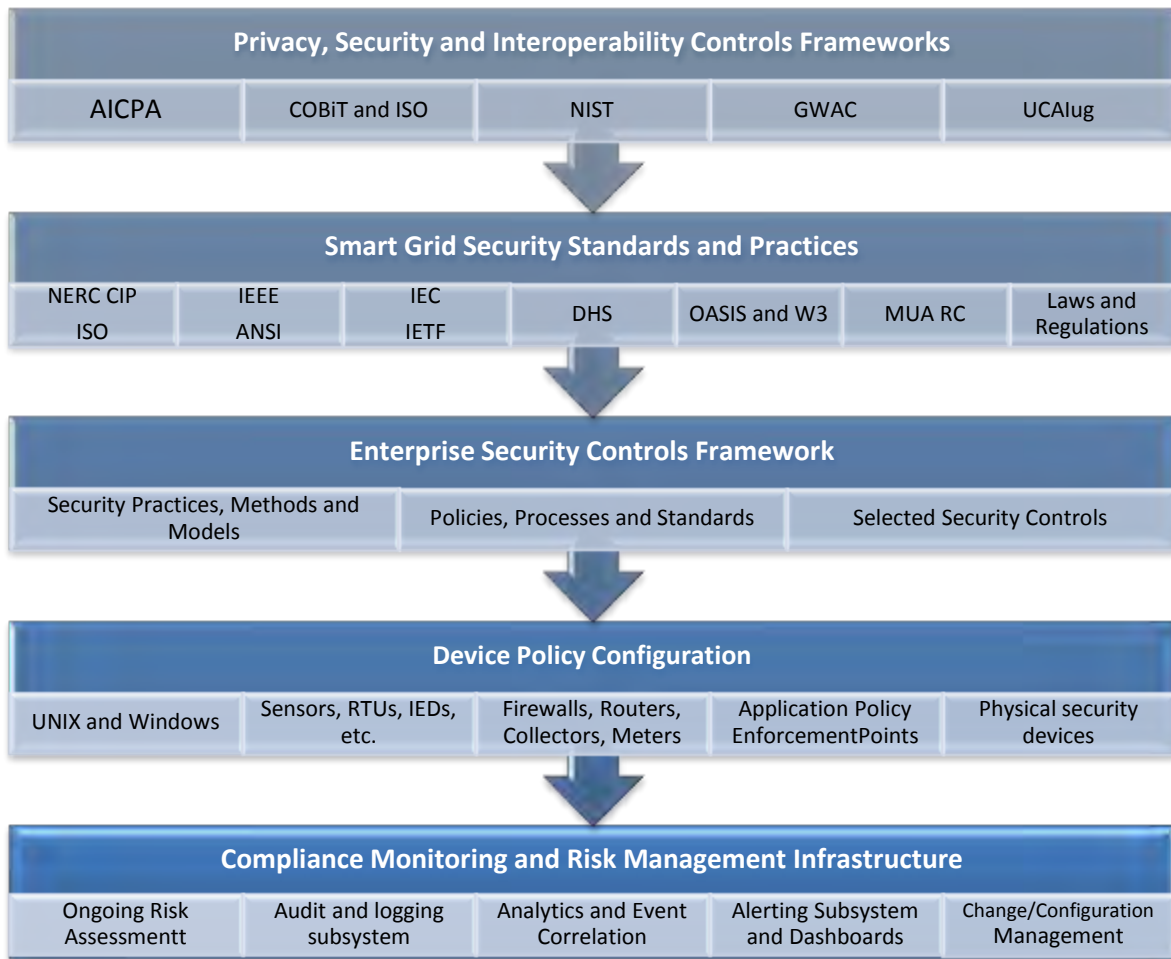
2.1.2.3 Smart Grid Cyber Security Design Considerations

2.1.2.3.1 Cyber Security Standards

In addition to being required by regulatory and compliance audit agencies, security policies, procedures and guidelines form the basis of a risk management program. They express management's intent with regard to the cyber security program and compliance with applicable laws and regulations, assign roles and responsibilities and define who is accountable for cyber security activities. The increasing interoperability of traditional IT systems and control systems, along with increased scrutiny of security controls by external agencies, makes the establishment and maintenance of a standards-based cyber security policy framework an essential component of the security program.

KCP&L has a policy framework that aligns security policies to IT and business policies. These policies will be analyzed for their relevance to the Smart Grid. Cyber security policies applicable to the operations environment will be reviewed and updates to reflect the requirements of Smart Grid operations and compliance with emerging standards will be identified. Gaps in the policy framework will be identified.

Figure 2-12: KCP&L GRC Management Framework



The standards and frameworks listed in Table 2-2 and Table 2-3 are relevant to Smart Grid cyber security best practices with particular emphasis on:

- NERC - Critical Infrastructure Protection (CIP) Version 3.0
- NISTIR-7628 Guidelines for Smart Grid Cyber Security – August 2010

Table 2-2: Summary of Applicable Cyber Security Standards

Standards	Description	Date
NISTIR-7628	Guidelines for Smart Grid Cyber Security	August 2010
NERC - CIP	Critical Infrastructure Protection (CIP) v3.0	Various
NIST SP 800-30	Guide for Conducting Risk Assessments Rev. 1	September 2012
NIST SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations Rev. 4	April 2013

Table 2-3: Summary of Applicable Cyber Security Frameworks

Frameworks	Description	Date
NIST SP 1108R2	NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 2.0	February 2012
UCAlug	Security Profile for AMI v2.1	October 2012
UCAlug	Security Profile for DM v1.0	February 2012
UCAlug	Security Profile for OpenADR v0.03	March 2012
UCAlug	Security Profile for Substation Automation v0.15	September 2012

Controls implementing these standards where required or where warranted based on best practices from other evolving Smart Grid standards will be expressed in cyber security policies, procedures and guidelines as appropriate. Compliance will be assessed through use of the GRC framework. The framework will ensure that:

- policies, procedures and guidelines will be documented in a central repository
- the policy maintenance life cycle will include regular review and incorporation of relevant standards
- compliance is assessed periodically
- exceptions will be documented and associated workflows created
- audit readiness is maintained

2.1.2.3.2 Risk Management

The KCP&L risk management framework defines the processes for combining impact, vulnerability, and threat information to produce an assessment of risk to the KCP&L SmartGrid and to its domains and sub-domains, such as businesses and customer premises. Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated impacts. Because the Smart Grid includes systems and components from the IT, telecommunications, and energy sectors, the risk management framework will be applied on an asset, system, and network basis, as applicable. The goal is to ensure that a comprehensive assessment of the systems and components of the KCP&L SGDP is completed. The framework will make use of the NIST/EPRI cyber security framework as a reference construct to ensure that applicable requirements are incorporated.

The risks of operating a system cannot be completely eliminated. After the implementation of controls, residual risks will be tracked and subject to the further assessment activities to determine methods of reducing the residual risk to acceptable levels. The risk assessment is used as input into the KCP&L Risk Management Process, which includes methods and activities that result in risk mitigation or acceptance. The Risk Management Process is depicted in Figure 2-13 below.

Following the risk assessment, the next step is to select and tailor the cyber security and business requirements. These requirements will drive a security architecture, which will be integrated with the systems architecture, NIST and other industry reference architectures. Integration with the NIST/EPRI reference architecture [6] [13] and other security standards will help ensure interoperability of components.

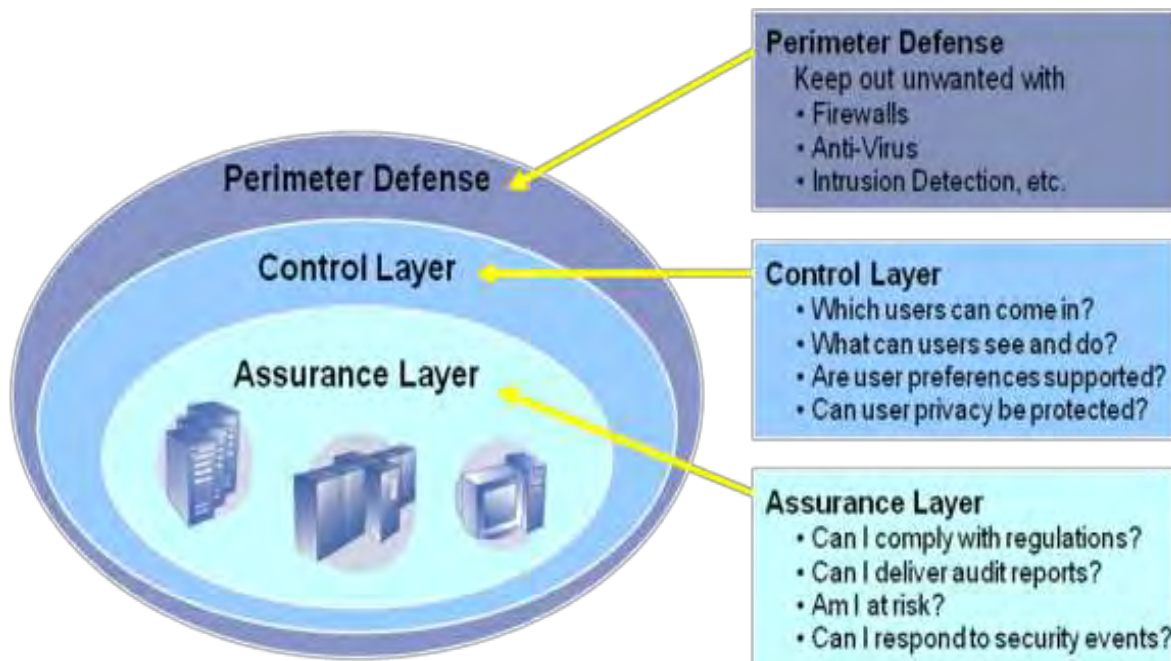
Figure 2-13: KCP&L Risk Management Process



2.1.2.3.3 *Defense in Depth*

Defense in depth is the layering of security controls in such a way that the damage of an exploit is minimized. An attacker must circumvent multiple controls to exploit vulnerabilities or gain unauthorized access. Security mechanisms are also layered in such a way as to limit the damage resulting from a compromise. A medieval castle with its moats, walls and other defenses is an example of a defense in depth security stance. A well-defended castle does not rely on a single defense to protect the most valuable assets, but on multiple layers. The security architecture, as illustrated in Figure 2-14 below provides for layers of security to form a defense in depth cyber security posture.

Figure 2-14: KCP&L *Defense in Depth* Security Posture



The architecture may include the following components to achieve a layered defense that complies with laws and regulations and meets KCP&L's business and budget requirements:

Perimeter Security:

- Protocol-level firewalls
- Intrusion detection (network and host-based)
- Application-level firewalls
- Wireless and endpoint security
- Physical security of cyber assets

Control Layer:

- Identity and access management
- Application security
- Compliance monitoring

Assurance Layer:

- Cyber security governance, risk and compliance management
- Cyber security policy development
- Cyber security testing
- Cyber security incident response

2.1.2.3.4 Trust Model

One important aspect of the Smart Grid that has not been sufficiently addressed by the industry is the development of a trust model for the Smart Grid. This section describes the method that KCP&L will use to develop a solution architecture that implements a trustworthy design.

Trust is defined as the measure of confidence that can be placed in the predictable occurrence of an anticipated event or an expected outcome of a process or activity. For business activities that rely on IT, trust is dependent on both the nature of the agreement between the participants and the correct and reliable operation of the IT solution.

An objective of a trust model for the KCP&L SGDP is to implement mechanisms and strategies for trustworthiness of systems protecting the confidentiality, integrity and availability of information between actors (requesters and consumers of information) and domains by ensuring accountability for actions. In a distributed information system, the ultimate concern of a trust model should be the information itself, rather than the sources that supply the information. A good trust model facilitates this type of interaction without hindering the more traditional approach to trustworthiness – i.e., interacting only with trusted sources of information.

The implementation of a trust model for the Smart Grid has many complex dimensions:

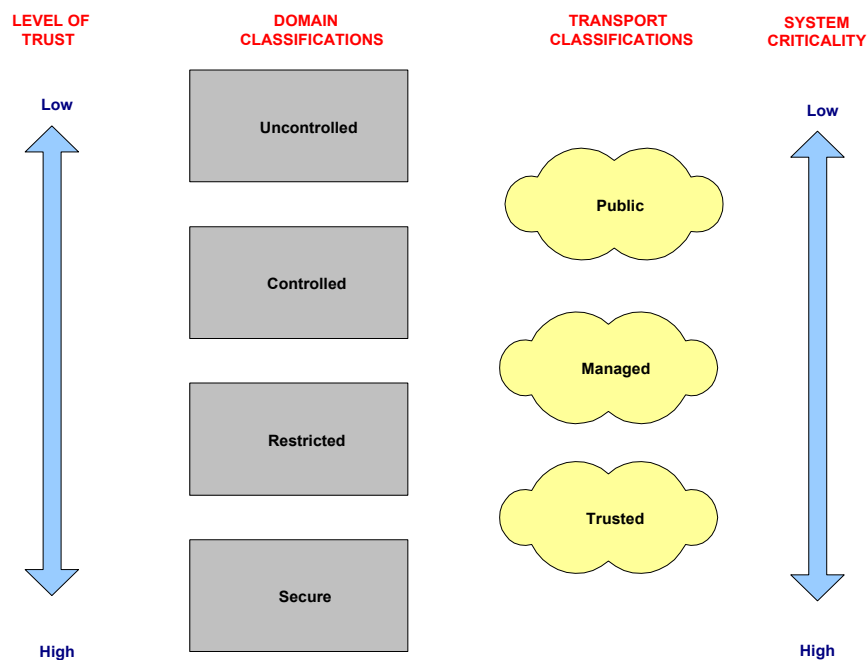
- Control systems with interfaces between them are often in different organizations, and therefore, the chain of trust between them is more important
- By definition, market operations are across organizational boundaries, thus posing trust issues
- The implementation of a model that enables network and systems architecture and facilitates effective communication among the various business entities without inadvertent or unauthorized sharing of trade secrets, business strategies or operational data and activities, while enabling sharing of fine-grained energy data and other information between organizations (and units within organizations) to realize the advantages of Smart Grid technology

- The management of large amounts of privacy-sensitive data in an efficient and responsible manner while complying with regulations regardless of the current state and location of data
- Trust of event or systems data
- Trust relationships between field devices and security policy enforcement points
- Trust within mesh networks, between leaf mesh nodes and gateways, and between mesh and non-mesh networks and interconnected mesh networks having different trust models
- The establishment of a user trust model for administration of keys, passwords and other sensitive data that does not create an undesirable amount of dependence on IT personnel and avoids an actor becoming a single point of failure

The activities undertaken using the secure architecture method will result in development of a conceptual trust model for the KCP&L SGDP.

Once the KCP&L solution architecture has been defined and mapped to the NIST framework, the architecture will be decomposed into its component domains. Figure 2-15 provides an example of semantics associated with varying trust levels of different domains and includes the security zones and the interfaces between them.

Figure 2-15: KCP&L Trust Model



Different semantics than those shown above may be used in the KCP&L SmartGrid trust model, however the process of applying the trust model will be the same. Different security levels that depend on the design of the network and systems architecture, security infrastructure and how trusted the overall system and its elements are will be assigned. This model will help put the choice of technologies and architectural decisions within a security context and guide the choice of security solutions.

One realistic expectation of the usefulness of the trust model, assured by application of this method, is that designers and integrators of IT solutions will enlist all reasonable measures to achieve the correct and reliable operation of IT solutions throughout the design, development, and deployment phases of the solution life cycle.

2.1.3 Education & Outreach Strategy & Plan [14]

The KCP&L project team developed and published a “SmartGrid Education & Outreach Plan” that detailed a strategy and approach for conducting SmartGrid Education and Outreach elements for the KCP&L SmartGrid Demonstration Project. The following subsections provide an overview of the significant elements of the education and outreach plan developed for the project.

2.1.3.1 Introduction

There are numerous examples from other utilities around the country that demonstrate that the overall success of a Smart Grid project is closely tied to the overall success of the utility’s public education and outreach plan. In the case of the Kansas City Power & Light Company (KCP&L) Green Impact Zone SmartGrid Demonstration Project (Demonstration Project), the geographic boundaries and demographic mix of the customer base present a unique set of communications challenges and opportunities. In response, KCP&L has developed a highly targeted, multi-phased public education and outreach effort that will drive awareness and understanding of SmartGrid as well as encourage product acceptance and adoption. KCP&L is working in close collaboration with its vendor partners and a wide range of community groups, most notably, Kansas City’s Green Impact Zone, an initiative led by U.S. Rep. Emanuel Cleaver II to focus federal stimulus dollars on a 150-square block geographic area in Kansas City’s urban core. In addition, although the current SmartGrid pilot project is limited to only 14,000 KCP&L customers, there is the much broader audience of approximately 800,000 customers across the company’s service territory. The success and lessons learned over the next five years will help determine the likelihood and plan for future deployment.

2.1.3.2 Education & Outreach Messaging

2.1.3.2.1 SmartGrid Demonstration Project Messages

The key Demonstration Project messages that support KCP&L’s SmartGrid communications objectives include:

- SmartGrid will provide customers with enhanced energy information and tools, helping them manage usage and control costs.
- SmartGrid will improve system reliability, energy efficiency and air quality.
- The SmartGrid Demonstration Project will allow KCP&L to obtain valuable customer feedback, leading to system-wide improvements for the entire customer base.
- Through KCP&L’s testing, evaluating and reporting, the SmartGrid Demonstration Project will serve as a blueprint for future Smart Grid implementations, and it will accelerate the realization of the “utility of the future.”
- SmartGrid will utilize advanced technology, including renewable generation, storage resources, cutting-edge substation and distribution automation and control, energy management interfaces, and innovative customer programs and rate structures.

2.1.3.2.2 Industry-wide Smart Grid Messages

The overarching messages above were crafted to support and enhance these broader Smart Grid objectives, as articulated by “Seven Principal Characteristics of the Modern Grid,” outlined in The NETL Modern Grid Initiative:

- **Self-heals:** The modern grid will perform continuous self-assessments to detect, analyze, respond to, and as needed, restore grid components or network sections.
- **Motivates and includes the consumer:** The active participation of consumers in electricity markets brings tangible benefits to both the grid and the environment, while reducing the cost of delivered electricity.

- **Resists attack:** Security requires a system-wide solution that will reduce physical and cyber vulnerabilities and recover rapidly from disruptions.
- **Provides power quality for 21st century needs:** The modern grid will provide the quality of power desired by today’s users, as reflected in emerging industry standards. These demands and standards will drive the grid.
- **Accommodates all generation and storage options:** The modern grid will seamlessly integrate many types of electrical generation and storage systems with a simplified interconnection process analogous to “plug-and-play.”
- **Enables markets:** This characteristic is particularly important because open-access markets expose and shed inefficiencies. The modern grid will enable more market participation through increased generation paths, more efficient aggregated demand response initiatives and the placement of energy storage and resources within a more reliable distribution system.
- **Optimizes assets and operates efficiently:** The modern grid’s assets and its maintenance will be managed in concert to deliver desired functionality at minimum cost.

2.1.3.3 Education & Outreach Audiences

Throughout the duration of this project, KCP&L needs to communicate its key messages to a number of audiences, including:

- SmartGrid Demonstration Area Customers (14,000)
- All KCP&L Customers (800,000)
- KCP&L Employees (3,600)
- State Agencies, Legislators and Regulators
- Utilities and Smart Grid Industry

Within each key audience group, KCP&L has identified a number of key stakeholder groups that are also targets for education and outreach. In some cases, these groups and organizations are the vehicle to reach the target audiences, and in other cases they are intended to serve as advocates and supporters for the SmartGrid project.

2.1.3.3.1 SmartGrid Demonstration Area Customers

KCP&L’s SmartGrid Demonstration Project has unique customer demographics and geographic area – in and around the Green Impact Zone. This may be one of the only projects of its kind to be focused on the urban core with such a high percentage of low-to-moderate income residents. This presents a number of unique communications and education challenges that KCP&L will address.

Table 2-4: Green Impact Zone Demographic Chart

Metric	SmartGrid Demonstration Area	Green Impact Zone
Population	19,960	8,374
Population in Poverty	23%	31%
KCP&L Customer Accounts	11,265	2,897
Median Household Income	\$28,000	\$22,000
Ethnicity: White, non-Hispanic	38%	7%
Ethnicity: Black, non-Hispanic	52%	89%
Ethnicity: Hispanic	5%	2%
Age: < 25 years	37%	43%
Age: 25-39 years	25%	20%
Age: 40-59 years	24%	22%
Age: > 60 years	14%	15%
Average Monthly Electric Bill	\$85.10	\$87.01

Within this audience group, the key stakeholders include:

- Individual Customers
- Neighborhood Groups
- Schools
- Community Leaders
- Elected Officials
- Green Impact Zone Partners

2.1.3.3.2 All KCP&L Customers

While customers living within the Demonstration Project area will be the first affected by SmartGrid initiatives, what KCP&L learns from the project will eventually impact all KCP&L customers. As such, outreach to the entirety of KCP&L's customer base will be an important part of SmartGrid communications.

Within this audience group, the key stakeholders include:

- Residential Customers
- Commercial Customers
- Industrial Customers

2.1.3.3.3 KCP&L Employees

As media coverage of and interest in the project in the broader service territory increases, KCP&L employees will be asked by friends, family and neighbors about SmartGrid. The 3,600 KCP&L employees can be utilized as SmartGrid ambassadors, but KCP&L will need to provide them with ongoing communications in order to make them effective.

Within this audience group, the key stakeholders include:

- Customer Care Departments
- Engineering and Operating Departments
- KCP&L Employees Living in the Project Demonstration Area

2.1.3.3.4 State Agencies, Legislators and Regulators

The individuals in this audience are charged with representing the community. They include elected or appointed individuals, who are especially sensitive to activities that may affect their constituents. Educating this audience is critical to ensuring continued support for SmartGrid, as these individuals will want to be informed so that they can answer any questions raised.

Within this audience group, the key stakeholders include:

- Missouri Public Service Commission & Staff
- Kansas Corporation Commission & Staff
- Missouri Office of Public Counsel
- Elected Officials

2.1.3.3.5 Utilities and Smart Grid Industry

One of the main goals of this project is to serve as a blueprint for future integrated Smart Grid demonstrations and implementations throughout the country. The project seeks to define, validate and verify the necessary parameters and potential solution adjustments for KCP&L, and the industry, to plan and implement a system-wide roll-out of the successful Smart Grid technologies and processes. In order to do this, KCP&L will need to effectively communicate and share knowledge with other utilities and the Smart Grid industry as a whole.

Within this audience group, the key stakeholders include:

- Department of Energy
- National Energy Technology Laboratory
- National Institute of Standards & Technology
- Smart Grid Interoperability Panel
- Professional Associations (IEEE, NSPE, etc.)
- Labor Organizations (IBEW)

2.1.3.4 Value Proposition Groups

The key, high-level messages outlined above will be tailored for each of the audience groups outlined above and focused on the appropriate value proposition area.

2.1.3.4.1 The Consumer

Individual residential consumers are primarily interested in what the Smart Grid will do for them as individuals. The consumer value proposition answers the question, “What’s in it for me?” Some of the consumer benefits include the following:

- **Information:** Smart Grid products will provide customers more information about their energy usage and help them learn which end-use devices and behaviors influence their consumption pattern the most.
- **Choice:** Customers will be offered products and services not previously available to them, and they will be able to decide which they want to use. Some of the new opportunities include consumer-owned generation and storage resources.
- **Control:** New Smart Grid products and tools will give customers the ability to manage their electricity use, which can help them save money on their monthly electric bills.
- **Convenience:** The new technologies will enable KCP&L to provide faster customer service: meter alerts of outages, remote service connect/reconnection and 15 minute interval data to help respond to customer inquiries.
- **Reliability:** The updated system will manage the grid to prevent outages and restore service more quickly when outages do occur.

2.1.3.4.2 The Utility

The utility value proposition answers the question, “What’s in it for KCP&L?” It must be noted that direct utility benefits are also indirect consumer benefits, as utility savings are used to reduce the upward pressure on rates. The Smart Grid is expected to provide benefits in a number of utility operational areas, some of which include:

- Improved reliability by enabling distribution automation as well as access to real-time operating data on critical substation equipment
- Reduced energy delivery cost through increased automation and ability to predict and proactively address maintenance strategies
- Improved customer satisfaction
- Improved carbon footprint

2.1.3.4.3 Society

The societal value proposition answers the question, “What’s in it for us?” The Smart Grid is expected to provide benefits in a number of societal areas, some of which include:

- Downward pressure on electricity prices
- Improved reliability, reducing losses that impact consumers and society
- Increased grid robustness, improving grid security

- Reduced emissions
- New jobs and growth in our gross domestic product
- Transformation of the transportation sector leading to a reduction in the U.S. dependence on foreign oil

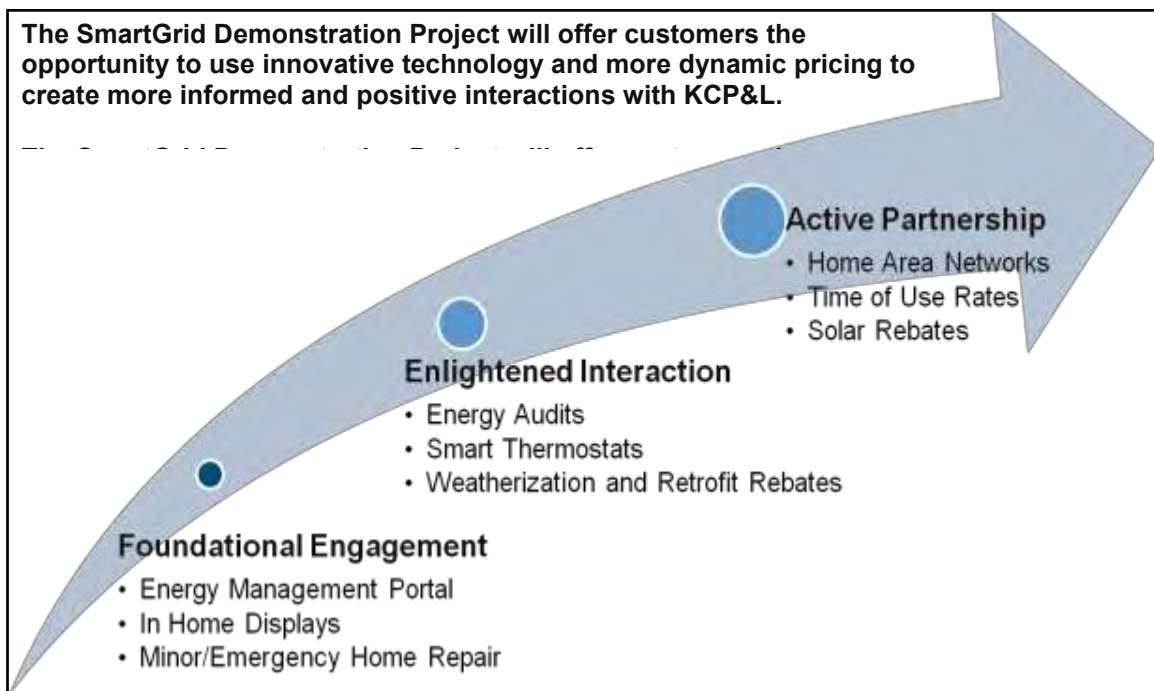
2.1.3.5 Communications Approach

KCP&L intends to educate and engage consumers through a highly targeted, integrated marketing campaign consisting of a variety of tactics across a range of channels for optimal impact. Strategic considerations include:

- Frequent and proactive customer communication, well ahead of customer impacts
- Engagement of key leaders and company ambassadors
- Regular face-to-face communication with customers
- Opportunities for customers to “touch and feel” improvements and products
- Pairing of KCP&L representatives with neighborhood groups and other key organizations
- Cultivation of third-party key leader support

As KCP&L progresses with its Demonstration Project, customers are given the opportunity to move along a continuum tied to value proposition (Figure 2-16). SmartGrid gives them the opportunity to use innovative technology to create a more informed and effective interaction with KCP&L.

Figure 2-16: Customer Value Proposition



2.1.4 Metrics & Benefits [4]

At the beginning of the project, the KCP&L project team developed and published a “SmartGrid Metrics & Benefits Reporting Plan” that set forth the objectives, expected benefits, key asset deployment milestones, Build and Impact Metrics, associated data collection, aggregation and analysis methods, monetary investments, baseline data methodologies, market place innovation, and collaboration/interaction with the DOE necessary to accomplish KCP&L’s fully integrated SmartGrid Demonstration Project. The following sections provide a summary the plan along with plan adjustments that have been made in response to DOE guidance and to incorporate the DOE Smart Grid Computational Tool (SGCT) analysis techniques.

2.1.4.1 Project Benefits

KCP&L’s Demonstration Project is designed as a means to test and evaluate a potential step change improvement in KCP&L’s electricity distribution system. Specifically, we are designing a system with a communication architecture that will facilitate automated system monitoring and control with open-source systems that will allow the integration of technologies and components from multiple vendors in a best-of-breed system of solutions — including a new architecture and system that will enable an interoperable, secure network of components.

We expect this Demonstration Project to identify significant potential grid performance improvements as a result of the technologies and solutions considered. Substation and distributed feeder line automation systems can significantly reduce O&M costs, improve reliability, and enhance the environmental footprint through automated fault location detection, automated switch operation, improved voltage control and regulation, improved Outage Management System communications, enabled two-way end-user communication and information flow, and the integration of distributed energy resources; allowing for a greater role of renewable energy generation into grid operations.

Smart Grid technologies are distinguished by how they improve the performance of the electric system. Each is associated with, or enables, Smart Grid and Energy Storage Functions that change in some (or several) aspects of the physical operation of the system that reduces utility costs, confers identifiable benefits to consumers or society, or all three. Evaluation of an individual smart grid or energy storage function requires establishing linkages between the deployment and operation of the technology and the impacts that are anticipated to result. When multiple technologies are deployed together we will, to the extent practical, isolate and assign the observed impacts to the individual technology.

The benefits will be evaluated using the DOE-specified four major benefit categories: (1) Economic, (2) Reliability, (3) Environmental, and (4) Security. Table 2-5 indicates the benefits KCP&L anticipates will be observed during the course of the project for each of the individual technologies that will be implemented. These technology/benefit linkages manifest KCP&L’s initial project design objectives. These technologies were chosen because they have the possibility of providing extensive system benefits, individually, and collectively, they offer an even more effective means for achieving the Smart Grid objectives.

2.1.4.2 SmartGrid Project Metrics Reporting

The Department of Energy (DOE) requires all Smart Grid Demonstration Projects (SGDP) to report baseline, build, impact, and other metrics, along with Technology Performance Reports (TPR). KCP&L will report all applicable Build and Impact Metrics and TPRs for the KCP&L Green Impact Zone SmartGrid Demonstration according to the schedule shown in Table 2-6. Metrics reports will be submitted 30 days after the completion of a reporting period. For example, the first Build Metrics report is designated for Q2 of 2011; it will be submitted on or before July 30, 2011. Interim TPRs will be submitted annually before the end of calendar years 2012 and 2013. The Final TPR, as part of the project Final Technical Report is due April 30, 2015 (90 days after the contract completion date).

Table 2-5: Smart Grid Benefits for KCP&L's Demonstration Project

Benefit Category	Benefit	Beneficiary	Provided by Project?	Remarks / Estimates
Economic	Arbitrage Revenue*	Consumer	NO	
	Capacity Revenue*	Consumer	NO	
	Ancillary Service *	Consumer	NO	
	Optimized Generator Operation	Utility	MAYBE	The impact of demand response may not impact the generation profile, but KCP&L will investigate if there are benefits.
	Deferred Generation Capacity Investments	Utility	MAYBE	Information will be collected for these benefits however it has not been determined if these benefits will be demonstrated. Benefits will be highly dependent upon the number of customers enrolling in demand response or dynamic pricing programs.
	Reduced Ancillary Service Cost	Utility	MAYBE	
	Reduced Congestion Cost	Utility	MAYBE	
	Deferred Transmission Capacity Investments	Utility	MAYBE	Analysis will be performed by the KCP&L planning group to determine if the peak demand and energy conservation benefits will offset the need for proposed transmission and substation projects.
	Deferred Distribution Capacity Investments	Utility	YES	The 2yr Project operational/monitoring is relatively short period to measure technology upgrade impacts on these benefit categories.
	Reduced Equipment Failures	Utility	YES	
	Reduced Distribution Equipment Maintenance Cost	Utility	YES	
	Reduced Distribution Operations Cost	Utility	YES	
	Reduced Meter Reading Cost	Utility	YES	
	Reduced Electricity Theft	Utility	YES	
	Reduced Electricity Losses	Utility	YES	
Reduced Electricity Cost	Consumer	YES		
Reduced Electricity Cost*	Utility	YES	Based on cycling operation of grid connected battery	
Reliability	Reduced Sustained Outages	Consumer	YES	
	Reduced Major Outages	Consumer	MAYBE	Based on asset monitoring and FLISR
	Reduced Restoration Cost	Utility	YES	
	Reduced Momentary Outages	Consumer	MAYBE	PQ will be monitored, but it has not been determined if the proposed corrective action plan will reduce the number of momentary outages.
	Reduced Sags and Swells	Consumer	YES	
Environmental	Reduced carbon dioxide Emissions	Society	YES	
	Reduced SO _x , NO _x , and PM-10 Emissions	Society	YES	
Energy Security	Reduced Oil Usage	Society	YES	
	Reduced Wide-scale Blackouts	Society	NO	Demonstration project does not include any wide-area or transmission SmartGrid components.

Table 2-6: Build/Impact Metrics and TPR Reporting Schedule

Report	2011				2012				2013				2014			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Build Metrics		X	X	X	X	X	X	X	X	X	X	X				
Impact Metrics			X		X		X		X		X		X		X	
Interim TPR								X				X				
Final TPR/Tech*																X

*The Final TPR, part of the Final Technical Report, will be submitted on April 30, 2015 (90 days after contract completion)

This section describes the Baseline, Build and Impact Metrics that KCP&L will report to the DOE. The metrics apply to the total project supported by the DOE and KCP&L cost-shared funds. Baseline, Build, and Impact Metrics are detailed in Appendix A Each table lists the metrics which are applicable to this project, indicates the measurement units associated with the metric, and any notes.

2.1.4.3 Build Metrics – Measurement of Smart Grid Progress

KCP&L will report both project and system Build Metrics throughout the project for those Build Metrics listed. Project Build Metrics pertain to only those assets deployed by and funded by this Project. System Build Metrics pertain to all assets deployed on the KCP&L system, including Project assets. For example, if 20,000 smart meters were deployed as part of this Project and 10,000 smart meters were deployed by KCP&L outside of this Project, then the Project Build Metric reported would be 20,000 and the System Build Metric reported would be 30,000.

The DOE developed a framework for reporting project Build metrics that organizes the reporting into five categories: Monetary Investments; Electricity Infrastructure Assets; Policies and Programs; Job Creation; and Marketplace Innovation. The following subsections present the build metrics that will be reported for the KCP&L Demonstration Project.

2.1.4.3.1 Electricity Infrastructure Asset Metrics

The Baseline and Build Metrics KCP&L will report for the Distribution infrastructure assets funded by the ARRA and cost share are contained in Appendix A. KCP&L will report the system metrics for the applicable Smart Grid assets that are already in place or will be deployed using non-grant funding during the reporting period. Baseline and Build Metrics will be reported for the following assets classifications deployed in the KCP&L Green Impact Zone SmartGrid Demonstration project:

- AMI Assets
- Customer Systems Assets
- Electric Distribution Assets
- Distributed Energy Resources

2.1.4.3.2 Policies and Programs

The Baseline and Build Metrics KCP&L will report for KCP&L's pricing programs funded by the ARRA and cost share are contained in Appendix A. KCP&L will report the system metrics for the applicable Smart Grid programs that are already in place or will be deployed using non-grant funding during the reporting period. Baseline and Build Metrics will be reported in the following tables:

- KCP&L's Pricing Programs

2.1.4.3.3 Job Creation Reporting

KCP&L will track and report the number and types of jobs by labor category and SGDP project classification, quarterly. In coordination with the DOE, jobs created and retained will be reported using the appropriate DOE full-time equivalents (FTEs) calculation, resulting from both ARRA funding as well as KCP&L's cost-share funds.

2.1.4.3.4 Monetary Investment Reporting

KCP&L will report funds that have been expended for the deployment of the SmartGrid Demonstration Project, quarterly. The report will include the DOE grants and the cost share of all recipients. KCP&L will report investments related to the cumulative 'installed cost of equipment' once the assets are deployed and considered utility assets. Investments metrics that will be reported by KCP&L are highlighted in Table 2-7 below. Financial analysts will utilize the KCP&L Financials System to determine or estimate the monetary investments related to the installation of equipment. KCP&L expects to develop estimates for project management and oversight related to equipment installation, testing, and commissioning, and apply those estimates to each category of investments as assets are installed.

Table 2-7: Applicable Monetary Investment Build Metrics (\$000)

AMI				Customer Systems					
Monetary Investment	AMI Back Office Systems	Communication Equipment	AMI Smart Meters	Customer Back Office Systems	Customer Web Portals	In Home Display	Smart Appliances	Programmable Controllable Thermostats	Participating Load Control Device
ARRA	-	-	-	-	-	-	-	-	-
Cost Share	-	-	-	-	-	-	-	-	-
Total	-	-	-	-	-	-	-	-	-
Other Assets and Costs that do not align with the categories listed above:									
Electric Distribution									
Monetary Investment	Back Office Systems	Distribution Management System	Communications Equipment / SCADA	Feeder Monitor / Indicator	Substation Monitor	Automated Feeder Switches	Capacitor Automation Equipment	Regulator Automation Equipment	Fault Current Limiter
ARRA	-	-	-	-	-	-	-	-	-
Cost Share	-	-	-	-	-	-	-	-	-
Total	-	-	-	-	-	-	-	-	-
Other Assets and Costs that do not align with the categories listed above:									
Electric Distribution – Distributed Energy Resources (DER)									
Monetary Investment	DER Interface / Control Systems	Communication Equipment	DER / DG Interconnection Equipment	Distributed Generation (DG)	Renewable DER	Stationary Electricity Storage	Plug-in Electric Vehicles	Plug-in Electric Charge Stations	
ARRA	-	-	-	-	-	-	-	-	
Cost Share	-	-	-	-	-	-	-	-	
Total	-	-	-	-	-	-	-	-	
Other Assets and Costs that do not align with the categories listed above:									

2.1.4.3.5 Market Place Innovation Reporting

Based upon the review of the project proposal and discussions with the DOE, KCP&L does not believe the Marketplace Innovation Build Metric pertains to this Demonstration Project. Marketplace Innovation will not be tracked and reported, but the Demonstration Project will potentially create additional markets and opportunities that KCP&L and our project partners can pursue.

- The customer facing SmartGrid technologies demonstrated will open the door to an abundance of new products and services that will better allow customers to monitor and manage their energy consumption.
- The next-generation grid management technologies and interoperability demonstrated will provide new SmartGrid products and services that project partners can take to the market furthering the ability of utilities to more economically evolve a more robust SmartGrid.

2.1.4.4 Impact Metrics – Measurement of Smart Grid Impacts

In order to measure, evaluate, and report the performance of Smart Grid technologies implemented through this project, KCP&L will prepare and submit Impact Metrics Reports semi-annually, in accordance with the schedule in Table 2-6. Impact Metrics will consist of measured or calculated characteristics of the functioning Smart Grid system throughout the project contractual period. These metrics will enable trending and evaluation of technologies on an aggregate level by the DOE. Impact Metrics to be reported are described A.2 according to the following classifications.

- AMI and Customer Systems
- Electric Distribution Systems
- Battery Energy Storage System (BESS)

Depending on the Impact Metric to be reported and the availability of data, KCP&L will report either a directly-observed project Impact Metric on project-only assets or will report system level impacts. Since this project affects only a small portion of the KCP&L service territory and customers, noticeable impacts are not expected at the system level. However, system level data may be used to estimate project level metrics.

2.1.4.5 Demonstration Sub-Projects and Expected Benefits

The KCP&L Demonstration Project includes various Smart Grid technologies that will be integrated and operated through advanced automation and interfacing of back office systems. The primary project objective is to demonstrate interoperability of these diverse systems and capabilities. As permitted, the KCP&L Demonstration Project will evaluate the performance of and benefits from the implementation of each individual sub-projects.

The SmartSubstation sub-project is intended to enable the following benefits:

- Improved real-time operating data on critical substation equipment will be provided that will lower operating costs and improve reliability
- O&M cost of relay maintenance will be reduced
- Distribution automation will be enabled through the substation controller which leads to reduced outage time and improved reliability to the consumer

The SmartDistribution sub-project implementation is intended to enable the following benefits:

- Improved service reliability by reducing the frequency and duration of sustained outages
- Reduced frequency of momentary outages
- Reduced operational expenses as many functions will occur automatically without human intervention or be performed remotely without a field crew
- Reduced maintenance expenses by providing rich data to enable predictive and proactive maintenance strategies

The SmartGeneration sub-project is intended to enable the following benefits:

- Improve general or localized reliability through grid-connected storage and load management
- Demand reduction on circuits equipped with DER/Solar/Battery

The Smart DR/DER Management sub-project is intended to enable the following benefits:

- Reduce customer load during DR events through DERM execution of DR devices and programs
- Reduced circuit/feeder load through select execution of demand response
- Defer investments in generation and transmission/distribution assets

The SmartMetering sub-project is intended to enable the following benefits:

- Improved frequency of meter reads and flexibility of read scheduling by enabling customers to select dates for turn on/turn off requests without associated field visits
- Improved accuracy of meter inventory and reduction in untracked meters
- Increased percentage of automated reads and reduced amount of stale reading within the existing automated one-way meter reading system
- Increased percentage of near real-time outage notifications and power restoration that would be supplied by a two-way metering system
- Ability to monitor power quality at the customer service entrance
- Provided real-time, two-way communication for Demand Response (DR) program control initiation and verification of program participation

The SmartEnd-Use sub-project is intended to enable the following benefits:

- Reduced peak demand
- Reduced energy consumption
- Improved customer engagement and participation in DR programs

2.1.4.6 Smart Grid and Energy Storage Functions and Benefits

The KCP&L Demonstration Project has been divided into five sub-projects to demonstrate the expected benefits described in the previous section. Details of each sub-project are described above in Section 2.1.4.5. During Phase 2 (Project Administration and Detailed Design) of the project, the KCP&L SmartGrid Demonstration Team performed a detailed review of the Demonstration Project technologies being implemented and identified the DOE defined SmartGrid and Energy Storage Functions that will be demonstrated within the scope of the project. Table 2-8 lists the Smart Grid Functions to be demonstrated and analyzed by sub-project.

Table 2-8: Smart Grid Functions by KCP&L Demonstration Sub-Project

Smart Grid Functions		Demonstration Sub-Project				
		Smart Metering	Smart End-Use	Smart Substation	Smart Distribution	Smart Generation
D = Direct S = Support						
Smart Grid Functions	Fault Current Limiting					
	Wide Area Monitoring, Visualization, and Control					
	Dynamic Capability Rating					
	Power Flow Control					
	Adaptive Protection					
	Automated Feeder Switching			S	D	
	Automated Islanding and Reconnection			S	S	D
	Automated Voltage and VAR control			D	D	
	Diagnosis and Notification of Equipment Condition			D	D	
	Enhanced Fault Protection					
	Real-Time Load Measurement and Management	D				
	Real-Time Load Transfer				D	
	Customer Electricity Use Optimization	D	D			
	Distributed Production of Electricity					D
	Storing Electricity for Later Use					D

Each Demonstration Project sub-project will support one or more SmartGrid or Energy Storage Function and in many cases a SmartGrid or Energy Storage function will require the integration of technologies multiple sub-projects. Operational Test Plans have been developed for each applicable SmartGrid and Energy Storage functions are described in section 2.4 later in this document. These Operational Test Plans establish linkages between the deployment of the technologies and changes in the performance of the electric system and detail the operational testing steps, data to be collected, anticipated benefits, and outline the analysis to be performed.

Smart Grid benefits identified in Table 2-5 are realized by each Smart Grid Function according to the matrix presented in Table 2-9 below.

2.1.4.7 Data Gathering and Benefit Quantification

Impact metric reporting and benefit quantification for the Demonstration Project will be accomplished through a variety of different tools and methods. This Project is diverse and will implement numerous Smart Grid technologies and applications that will need to be evaluated in different ways. Benefits associated with changes to how energy is used on the KCP&L system will be evaluated through the capture and analysis of detailed interval usage data for all customers, circuits/feeders, and necessary equipment within the project area. Benefits associated with operational efficiency will be evaluated through detailed operational and automated event tracking contained within the various systems to be implemented.

Table 2-9: Smart Grid Benefits Realized by SmartGrid Functions

Smart Grid Benefits		Smart Grid Function								
		Automated Voltage & VAR Control	Real-Time Load Transfer	Automated Feeder & Line Switching	Automated Islanding & Reconnection	Diagnosis & Notification of Equipment Condition	Real-Time Load Measurement & Management	Customer Electricity Use Optimization	Distributed Production of Electricity	Storing Electricity for Later Use
D = Direct Benefit I = Indirect Benefit										
Economic	Arbitrage Revenue*									
	Capacity Revenue*									
	Ancillary Services Revenue*									
	Optimized Generator Operation									
	Deferred Gen. Capacity Investments							D	D	D
	Reduced Ancillary Service Cost									
	Reduced Congestion Cost									
	Deferred Trans. Capacity Investments									
	Deferred Dist. Capacity Investments		D				I	D	D	D
	Reduced Equipment Failures					I				
	Reduced Dist. Equip. O&M Cost									
	Reduced Distribution Operations Cost			D						
	Reduced Meter Reading Cost						D			
	Reduced Electricity Theft						D			
	Reduced Electricity Losses	D	D				I	I	D	D
Reduced Electricity Cost							D	D	D	
Reliability	Reduced Sustained Outages			D	D	I	D		I	D
	Reduced Major Outages		D		D		D			
	Reduced Restoration Cost			D		I	D			
	Reduced Momentary Outages									
	Reduced Sags and Swells									
Environmental	Reduced carbon dioxide Emissions	I	I	I			I	I	I	I
	Reduced Emissions (SO _x , NO _x , PM-2.5)	I	I	I			I	I	I	I
Energy Security	Reduced Oil Usage			D			D		I	
	Reduced Wide-scale Blackouts									

*These benefits are only applicable to energy storage demonstrations.

Interval and historical daily meter data for circuits and customers within the SmartGrid Demonstration area will be accessed through KCP&L's DMAT, DataRaker. This web-based database will enable filtration and selection of relevant meter data that may then be extracted and aggregated for load profile generation. All accounts within the Project area will be tagged with relevant demographic information for efficient and accurate filtration. Load profile generation, weather normalization, and comparative analysis will be accomplished through the use of computational spreadsheet software such as Microsoft Excel.

Operational metrics such as the tracking of events for specific incidents on specific equipment will be recorded by the appropriate management system:

- Manual activities executed will be tracked by the Mobile Workforce Management System
- Automated substation and distribution circuit activities executed will be tracked by the DMS/DCADA
- Various equipment failures and subsequent automated actions will be tracked by the DMS/DCADA
- Outages tracked by the OMS
- Compliance in DR events will be tracked by the HEMP
- AMI performance by the AMI Head-end and MDM system
- Grid-connected battery performance will be tracked through AMI metering, the inverter and switchgear control system, and the battery data acquisition system (DAS)

Usage and operational data will be gathered in accordance with the Operational Test Plans in Section 2.4 for each Smart Grid Function. KCP&L will then report data and impact metrics to the DOE as required. In addition, KCP&L will attempt to quantify benefits associated with each Smart Grid Function in accordance with section 2.5. Benefit quantification will be focused on assessing the potential impact of each Smart Grid Function on the KCP&L system. For example, KCP&L will attempt to quantify the amount of demand reduction that is achieved by each demand response technology deployed by comparing the hourly load profiles of each group during demand response events with weather-adjusted hourly load profiles of the same group from a previous day. Impacts to overall energy usage will be quantified through comparisons of daily, monthly, and annual load profiles of participant groups with those of control groups for the same time period. Impacts to operations and reliability will be quantified by comparing numbers of experienced events to forecasted events based on historical data. System average costs will then be applied to events reduced or increased.

2.1.4.8 Baseline Data for Impact Metrics and Benefits Assessment

The KCP&L Green Impact Zone SmartGrid Demonstration will demonstrate many diverse Smart Grid technologies. Each application of those technologies will provide different benefits which will need to be compared to appropriate baseline data. Therefore, multiple baseline development methodologies will be required for of each impact metric within the project.

2.1.4.8.1 Historical Baseline Data

KCP&L will collect and report historical usage and system performance data on customers and assets within the Project area:

- Historical usage data will consist of daily kWh readings, beginning February, 2010, as collected by the KCP&L AMR system for all customers within the Demonstration Project area. Additionally, KCP&L has initiated 15 minute interval usage reading on approximately 6,000 customers within the project area, the maximum allowed by the system, beginning July, 2010.
- AMI and interval metering will be near fully deployed by March, 2011, providing additional interval data on all customers within the Demonstration Project area prior to the project observation period scheduled to begin in July, 2012.
- System performance data on the assets affected by Smart Grid technology deployment will consist of five years of operational statistics such as SAIDI, SAIFI, MAIFI, CAIDI, and known incidents and outage events.

Interval data for all customers within the Demonstration Project area will be collected through the AMI system throughout the duration of the project and will be reported to the DOE at each reporting milestone (semi-annually) in the form of hourly usage data grouped by customer class and sub-class. In some cases, this data may be utilized to generate historical baselines by which to compare project usage data.

2.1.4.8.2 Baseline Methodology for Automated Operations

Some Smart Grid applications will automate operational activities that were previously accomplished manually. For these applications, baseline data will consist of a forecast of estimated manual activities that KCP&L expects would have occurred on the applicable assets if Smart Grid technologies were not implemented. These forecasted estimations will be based on historical manual activity information available within KCP&L's historical records, specific to the relevant assets within the project area. Actual automated and manual actions that occur within the project area and during the project period will be recorded and compared to these baselines.

2.1.4.8.3 Baseline Methodology for Reduced Event Occurrence

Some Smart Grid applications will reduce distribution system equipment failures through monitoring and automated switching. For these applications, baseline data will consist of a forecast of estimated failure events that KCP&L expects would have occurred on the applicable assets if Smart Grid technologies were not implemented. These forecasted estimations will be based on historical failure event information available within KCP&L's historical records and outage management system, specific to the relevant assets within the project area. Actual monitoring and subsequent avoidance activities will be recorded and compared to these baselines.

2.1.4.8.4 Baseline Methodology for Changes to Energy Consumption

Some Smart Grid applications will reduce overall energy consumption on the system or enable enhanced customer information that will empower customers to control and conserve energy consumption. These impacts occur continuously and are not isolated to discrete events. For these applications, baseline data will consist of hourly, daily, and monthly load profiles for control groups of similar customers that do not have access to or choose not to participate in the relevant Smart Grid technology and information. Control group load profiles will cover the entire project duration and the data will be acquired through the existing AMR and newly deployed AMI and MDM systems that KCP&L is implementing as part of this project for all customers within the project area. Impacts of these energy conservation applications will be contained in required periodic reports to the DOE under the customer hourly load metrics for various customer classes and sub-classes.

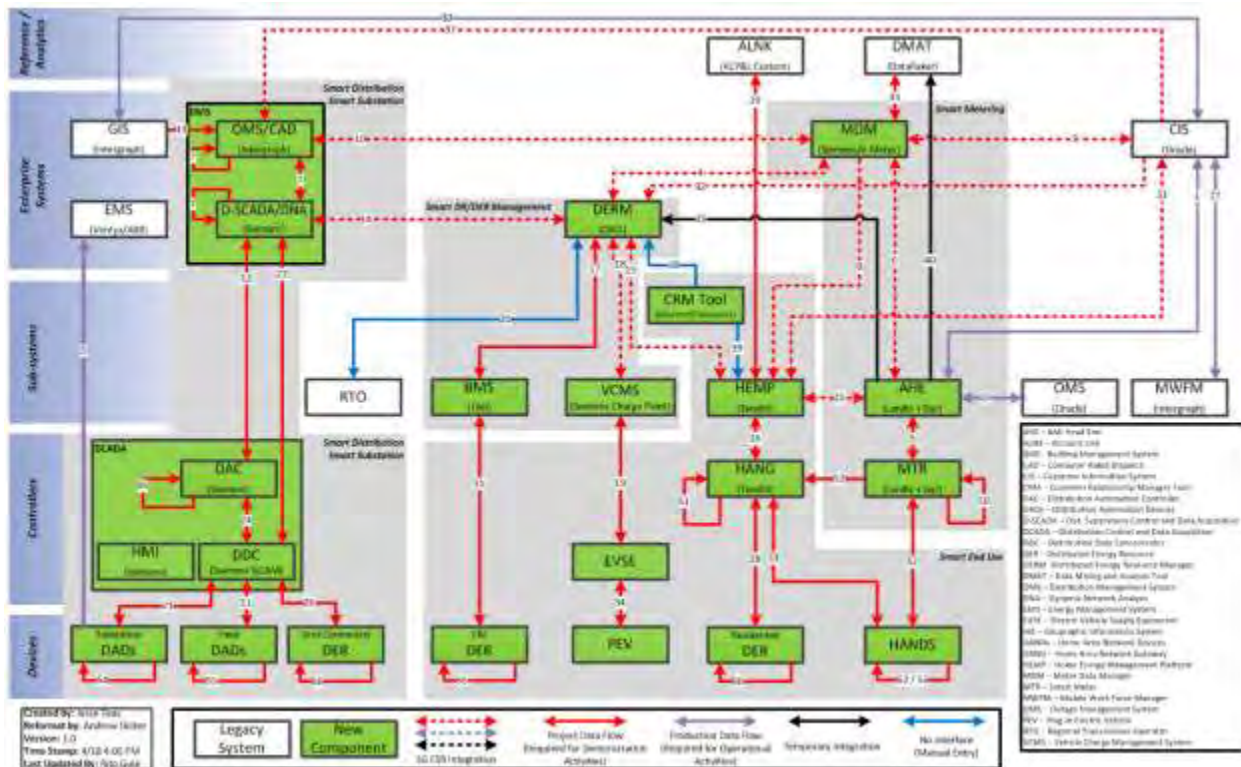
2.1.4.8.5 Baseline Methodology for Demand Response Events

Other Smart Grid applications will reduce system peak load and energy consumption during scheduled and discrete events to accomplish temporary system, circuit, or customer demand reduction. Demand reductions may be executed for either economic value (sold into capacity markets) or to improve system performance and reliability (relieve distribution system congestion). For these applications, event baseline data for evaluation will consist of weather-normalized hourly load profiles for applicable equipment and event participants from either a previous similar day or from a proxy day or a control group. Baseline load profiles will be calculated as hourly average load for applicable equipment, assets, and groups of Smart Grid technology participants for each demand reduction event. Actual average load profiles for day of an event will be compared to the baseline load profiles. Demand response impact analysis results for events associated with this project will be summarized in technical performance reports to the DOE.

2.2 Systems Implementation

The KCP&L SmartGrid Demonstration project is based on deploying an integrated end-to-end solution, illustrated in Figure 2-17 below, that demonstrates interoperability across the five (5) SmartGrid sub-project components that included eight (8) major new back office distribution control, systems (AMI, MDM, HEMP, DMS, OMS, D-SCADA, DERM, & VCMS), five (5) existing legacy back-office systems (CIS, ALNK, DMAT, GIS, & EMS) and numerous substation and field automation controllers. The implementation of these systems is summarized in the following sections.

Figure 2-17: KCP&L SmartGrid Demonstration Systems Integration



The implementation of the Demonstration Project systems was carried out using a disciplined project management approach, through a collaborative effort between leadership and cross-functional and individual sub-project implementation teams. The SmartGrid Demonstration Leadership was provided by members of a Partner Leadership Team, Program Director, and members of the KCP&L Executive Advisory Team. The KCP&L SmartGrid Demonstration Project Management Plan [16] [17] [18] [19] that was approved by the DOE and revised annually by the project PMO staff.

Each cross-functional and sub-project had an assigned lead that reported to the Program Management Director. Each sub-project implementation team was required to utilize a disciplined project management approach to provide integration into the overall program management responsibilities and deliverables. The Program Director provided project management requirements, guidance, and oversight and had overall responsibility for the direction and performance of the project. The Program Management Director, PMO staff, and Implementation Team Leads provided periodic updates to the Partner Leadership Team and the KCP&L Executive Advisory Team.

2.2.1 SmartMetering

The SmartMetering sub-project deployed a state-of-the-art integrated AMI and MDM solution. The following subsections summarize these system implementations.

2.2.1.1 AMI

Figure 2-18 illustrates the Landis+Gyr Gridstream AMI system and FAN infrastructure components implemented as part of the SmartMetering sub-project.

Figure 2-18: L+G Gridstream AMI Command Center and FAN



2.2.1.1.1 Build

The KCP&L Demonstration AMI System was deployed over an approximately nine month period beginning in October, 2010 and ending in June, 2011. The implementation consisted of the deployment of smart meters to all customers within the project area, installation of an AMI Head-End (Command Center) to manage information traffic and meter endpoint registration, the deployment of a wireless communication network to connect meter endpoints to the AMI Head-End, and the integration of the AMI Head-End to KCP&L back office systems.

The KCP&L Demonstration AMI System network and endpoints were deployed over approximately a nine month period with additional project planning and software maintenance activities stretching the entire project out to approximately two years as is shown in Figure 2-19.

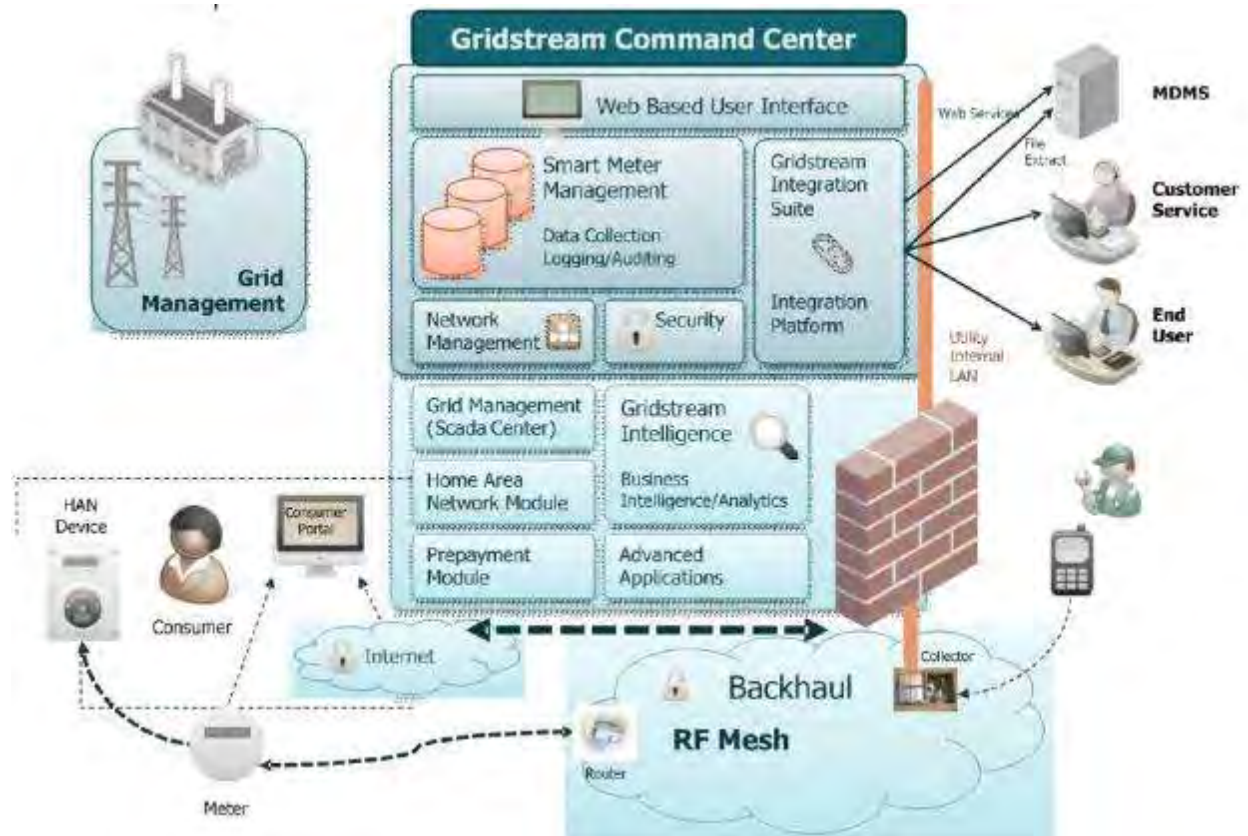
Figure 2-19: KCP&L SmartGrid Demonstration Project AMI Deployment Timeline

Task Name	Start	Finish	2010			2011				2012				
			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
SmartMetering Implementation	Mon 2/1/10	Fri 3/30/12	[Green bar spanning from Q1 2010 to Q4 2011]											
SmartMeter Partner Project Management	Mon 2/1/10	Mon 1/31/11	[Green bar spanning from Q1 2010 to Q4 2010]											
SmartMetering Project Planning	Tue 3/2/10	Fri 12/30/11	[Green bar spanning from Q1 2010 to Q4 2011]											
SmartMetering Project Design/Development	Mon 3/1/10	Mon 10/31/11	[Green bar spanning from Q1 2010 to Q4 2011]											
SmartMetering Deployment	Tue 6/1/10	Fri 3/18/11	[Green bar spanning from Q2 2010 to Q3 2010]											
SmartMetering System Acceptance	Mon 12/27/10	Fri 3/30/12	[Green bar spanning from Q4 2010 to Q4 2011]											
Prepare SmartMetering Implementation Report	Wed 6/1/11	Fri 11/11/11	[Green bar spanning from Q2 2011 to Q3 2011]											
Command Center (AMI Headend) Upgrades	Mon 5/16/11	Fri 10/21/11	[Green bar spanning from Q3 2011 to Q4 2011]											

2.2.1.1.1.1 Hosted AMI Head-End Solution

KCP&L chose to implement the Gridstream AMI Head-End system, Figure 2-20, as a managed-service and hosted-platform, with Landis+Gyr hosting the backend servers and systems and capturing meter reads to meet contractual performance criteria.

Figure 2-20: AMI Head End - L+G Gridstream Command Center



For the demonstration development/lab environment, KCP&L implemented the Gridstream AMI head-end internally within the KCP&L internal systems development infrastructure to facilitate the application, web, and external integration needs of the lab AHE and other systems.

An AMI lab was built-out in KCP&L facilities featuring AMI collectors, routers, and over 25 meters associated to development CIS accounts to emulate real-life customer meters. This lab was used to test all aspects of AMI from a project-perspective, including system-to-system integration, AHE-to-SmartMeter testing, and SmartMeter-to-HAN device testing.

2.2.1.1.1.2 AMI RF Network Build-Out

KCP&L used internal construction crews, assisted by L+G personnel, to deploy the communications network. Collectors, illustrated in Figure 2-21, were installed at the Midtown substation in the Demonstration Project area and on a transmission pole near the future site of a new substation just north of the area. One collector communicates via a fiber-based network and the other via a wireless network. Landis+Gyr provided an optimized network installation guide for the routers within the FAN. Routers were installed on distribution feeder poles where possible.

Figure 2-21 Installed AMI FAN Infrastructure

2.2.1.1.1.3 AMI Meter Exchange

SmartMeter installers for the project were hired through a third party from the Demonstration Project area. This was in line with KCP&L's commitment to hire and train local labor as the overarching theme of the Green Impact Zone. These employees were given training on basic electricity, proper residential metering configuration, meter exchange procedures, workplace safety, and customer service. KCP&L journeymen meter technicians deployed all 3-phase meters in the Demonstration Project area due to their expertise and high level of safety awareness.

Meter reading routes were selected for the determined project geographic area. Prior to implementation, KCP&L conducted a route audit to check for safety concerns, determine accessibility issues, identify non-standard and A-base meter enclosures, and identify potential customer concerns. During KCP&L's previous Automated Meter Reading (AMR) deployment, A-base meter sockets were used to retrofit many legacy meter types housed within meter enclosures. Minor safety issues (e.g. meter seals missing, diversion issues, etc.) were identified and corrected prior to beginning the installation of SmartMeters.

Through pre-deployment testing, KCP&L Measurement Technology staff determined that the greater physical depth of the SmartMeter would not allow the meter enclosure cover to close properly on many of these installations. KCP&L contracted with Milbank, a local Kansas City meter socket manufacturer, to design and construct modified covers for those legacy meter enclosures.

Meters were installed according to sequential routes established by KCP&L. Installers used hand held computer devices to record old meter numbers and readings, latitude/longitude of each smart meter service point, and a picture of both the old and new meters. All new meter identification information was captured and data was uploaded and sent to KCP&L electronically at the end of each day of installation. This helped ensure data transfer was accurate and the pictures assisted in investigations and resolutions of issues that arose.

2.2.1.1.2 Integration

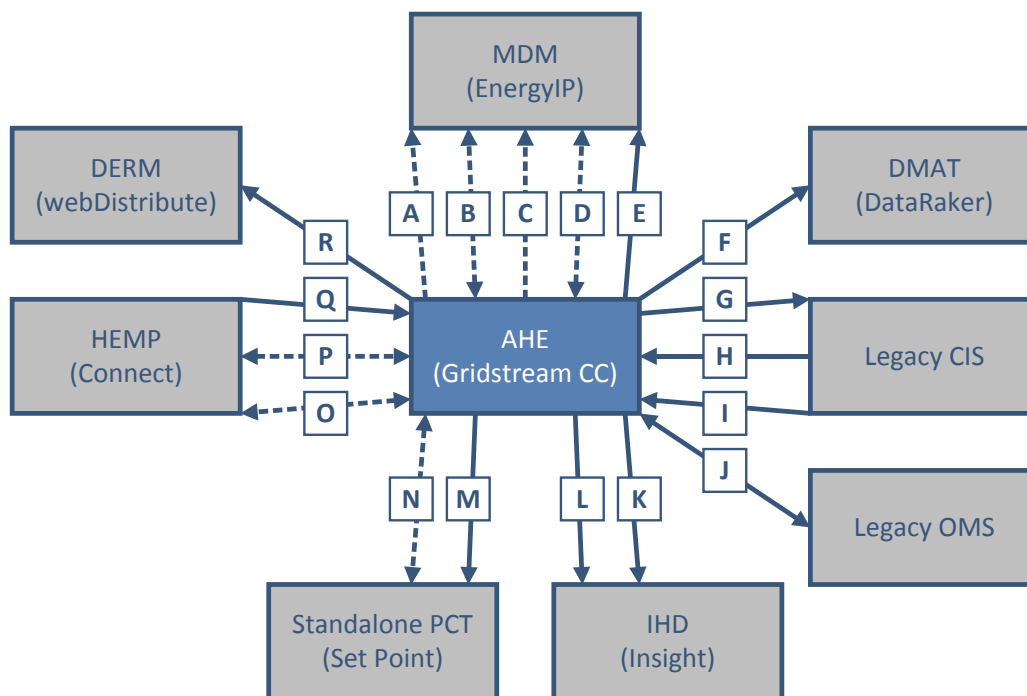
KCP&L utilized use case development to define the AMI system functionality and system-to-system integration requirements early on in the design process. These use cases help define scenarios to be addressed and the systems that are involved, the standards used for the interfaces between systems, and the message formats and payloads required for these interfaces to achieve these scenarios successfully.

KCP&L chose a two-phase approach to the AMI integration implementation. The first phase included point-to-point interfaces between the AHE, the Legacy CIS, the Legacy OMS, and the HEMP to ensure a quick, but functional initial system stand-up. This first phase utilized existing legacy interfaces that were already being used by the Legacy AMR system in an effort to reduce impact on KCP&L Production systems and processes, such as billing in the Legacy CIS and outage/restoration analysis in the Legacy OMS.

The second phase focused on standing-up new SmartGrid interfaces between the AHE and other SmartGrid systems, including the MDM, HEMP, and DERM, utilizing an ESB approach for message routing and transformations. This approach is an alternative to point-to-point interfaces and provides KCP&L greater flexibility in control of message routing and system interfaces by bringing all transactions in-house and removing direct interfaces between systems.

An overview of AHE system-to-system interfaces and applicable messages is illustrated in Figure 2-22.

Figure 2-22: KCP&L SmartGrid Demonstration Project AHE Integration



The integration touch points for the AMI are as follows:

- A. 'Outage/Restoration Event' notification initiated from SmartMeters to MDM and sent from MDM to OMS. This is an IEC 61968 CIM-formatted event message used to notify MDM (and OMS) of an outage or restoration event occurring at a SmartMeter.
- B. 'Power Status Verification' request-reply initiated from OMS to MDM and sent from MDM to AHE in the form of an 'On-Demand Read' request-reply. This is an IEC 61968 CIM-formatted request-reply used to verify power status (On, Unknown, or Service Disconnected) at a target SmartMeter.
- C. 'General Event' notification initiated from AHE to MDM. This is an IEC 61968 CIM-formatted event message used to notify MDM of various MDM-supported events (using the corresponding CIP 4-part IDs) that occur within the AMI system. MDM can then log these events and/or route them to other subscribing systems.
- D. 'Remote Service Order' request-reply messages, including On-Demand Read and Remote Service Connect/Disconnect, initiated from CIS to MDM and sent from MDM to AHE. These are IEC 61968 CIM-formatted request-reply messages used to get on-demand reads and execute remote service connect/disconnects on eligible target SmartMeters.
- E. 'Daily Register and Interval Read' data initiated from AHE to MDM. This is California Metering Exchange Protocol (CMEP)-formatted data sent hourly to be stored in the meter usage data repository and used for TOU billing determinants.
- F. 'Daily Register and Interval Read' data initiated from AHE to DMAT. This is California Metering Exchange Protocol (CMEP)-formatted data sent daily to be used for load research.
- G. 'Daily Register and Interval Read' data initiated from AHE to CIS via a middleware database. This is California Metering Exchange Protocol (CMEP)-formatted data sent daily to be used for billing determinants.
- H. 'Database Maintenance (DBMAINT)' process messages and integration calls initiated from the CIS DBMAINT process. This DBMAINT process is used to keep CIS and AHE in-sync for customer records, service connectivity, and meter deployment/exchange purposes.
- I. 'Estimated Bill True-Up' and 'Consumption Pricing' messages initiated from CIS to AHE. These daily notifications are used to update estimated bill true-up information on customer IHDs and consumption pricing information on customer IHDs and Standalone PCTs.
- J. 'Power Outage Analysis (POA)' messages initiated from AHE to Legacy OMS and 'Restoration Verification Analysis (RVA)' messages initiated from Legacy OMS to AHE. These are Multispeak-formatted messages used for outage and restoration analysis within Legacy OMS.
- K. 'Estimated Bill True-Up' messages initiated from AHE to IHDs. These "tunnel text messages" are ZigBee Smart Energy Profile (SEP) 1.0-formatted messages sent daily to update customer IHDs with up-to-date estimated billing information.
- L. 'Consumption Pricing' messages initiated from AHE to IHDs. These "tunnel text messages" are ZigBee Smart Energy Profile (SEP) 1.0-formatted messages sent daily to update customer IHDs with real-time per-kWh consumption pricing information.
- M. 'Consumption Pricing' messages initiated from AHE to Standalone PCTs. These "tunnel text messages" are ZigBee Smart Energy Profile (SEP) 1.0-formatted messages sent daily to update customer IHDs with real-time per-kWh consumption pricing information.
- N. 'Demand Response Event' requests initiated from AHE to AMI-based DR assets (Standalone PCTs for this project) via SmartMeters, and 'Event Opt-Out/Opt-In' replies initiated from AMI-based DR assets to AHE via SmartMeters. These are ZigBee Smart

Energy Profile (SEP) 1.0 -formatted request-reply messages used to notify AMI-based DR assets of creation, modification, or cancellation of impending DR events and to notify AHE of AMI-based DR asset event participation status.

- O. 'Get Device Info' request-reply initiated from HEMP to AHE. This is an IEC 61968 CIM-formatted request-reply used to gather HAN device information for AMI-based DR assets (Standalone PCTs).
- P. 'Demand Response Event' request initiated from HEMP to AHE, and 'Event Opt-Out/Opt-In' reply initiated from AMI-based DR assets (Standalone PCTs for this project) to HEMP. These are IEC 61968 CIM-formatted request-reply messages used to notify AMI-based DR assets of creation, modification, or cancellation of impending DR events and to notify HEMP of AMI-based DR asset event participation status.
- Q. 'Consumption Pricing' and 'Billing True-Up' messages initiated from HEMP to AHE. These "tunnel text messages" are sent daily to update customer IHDs with real-time per-kWh consumption pricing information and up-to-date estimated billing information.
- R. 'Daily Register and Interval Read' data initiated from AHE to DERM. This is California Metering Exchange Protocol (CMEP)-formatted data sent daily to be used for customer load profile baselines within DERM.

2.2.1.1.3 Post-Implementation Operational Issues

Throughout the SmartGrid Demonstration Project, numerous upgrades to the AMI system and SmartMeters were executed to add support for project-necessary functionalities and increase overall performance of the AMI system as a whole. The upgrades were performed on an as-needed basis, with careful planning and scheduling in an effort to reduce impacts on AMI performance and system-to-system interfaces, and were first tested in the Development environment to verify the upgrades prior to moving them to Production.

- **Command Center 5.0 Upgrade** – As the first major functionality-based upgraded, the move to Command Center 5.0 included many key components that are functionality cornerstones of AMI portion of the SmartGrid Demonstration Project. Security improvements implemented core security requirements for the AMI implementation including security configuration tokens, RF traffic encryption keys, and AMI system security modes with varying degrees of security. The upgrade added support for CIM-compliant meter event messages to further simplify system-to-system integration. Furthermore, CIM-based interfaces for on-demand meter reading, meter disconnect/reconnect, and bulk meter reading were added to the AMI system integration core. This upgrade was performed in the summer of 2011.
- **Command Center 5.1 Upgrade** – Primarily, the Command Center 5.1 upgrade added the much-needed benefit RF broadcast commands. This functionality allows for commands, meter programs, and firmware upgrades to be sent to large groups of meter based on meter type, firmware versions, and other criteria, as opposed to the having to leverage commands sent to meters one-by-one or to predefined groups of meters. This significantly reduced the time and manual effort required to execute meter program updates and firmware upgrades to large groups of SmartMeters.
- Added support for new peripheral software aimed to improve performance and integration with other SmartGrid systems. Additionally, performance-tuning within the back-end server software and RF collector, router, and endpoint firmware helped improve latency issues that were seen on previous releases. This upgrade was performed in the fall of 2011.
- **Command Center 5.6 Upgrade** – On the performance side, the Command Center 5.6 added support for Oracle 11g to improve load balancing and database performance. Also,

the memory utilization within the SmartMeter was improved which helped mitigate potential storage, processing, and communications issues.

- On the end-use side, the improved utilization of memory within the SmartMeter also corrected an issue seen when multiple demand response replies were sent from HAN devices in a short period of time. Support for the Smart Energy Profile 1.1 stack was added enabling the use of added features in SEP 1.1. An interface for third-party DR event processing was also added to enable the AHE to receive DR event requests from external systems and send DR event response back to the requesting systems. This upgrade was performed in the summer of 2012.
- **Command Center 5.7 Upgrade** – The Command Center 5.7 upgrade brought about additional performance enhancements. These enhancements have the added benefit of improving the AMI system scalability, if needed in the future. This upgraded included RF mesh improvements for more efficient network routing and improved outage and restoration reporting. It also included full 64-bit server support on the back-end to improve memory utilization and message queuing from field collectors.
- The upgrade also added support for more CIM-based event messages and updated 4-part IDs for CIM 2.0 compliance. Additionally, CIM-based support was added for Power Status Verification using a modified on-demand read request-reply that can be issued to SmartMeters regardless of the SmartMeter’s last-known status in the AHE. This upgrade was performed in the spring of 2013.
- **Command Center 6.0 Upgrade** – The decision to upgrade to Command Center 6.0 was primarily driven by the needs of KCP&L’s AMR/AMI Refresh Project that ultimately is an expansion of the AMI system that has been implemented as a part of the SmartGrid Demonstration Project. To facilitate a smooth transition from the Legacy KCP&L AMR system to the newly implemented AMI system, KCP&L is deploying AMR-AMI concentrator node into the AMI RF mesh that will route both AMR and AMI traffic accordingly during the three-year AMR-AMI meter exchange process. This AMR-AMI routing capability is a new functionality for the Gridstream RF mesh, and Command Center 6.0 adds necessary layered-routing support for these new AMR-AMI concentrator nodes.
- In addition, the strict security requirements defined for the SmartGrid Demonstration Project include added security and encryption features that are not included in the Legacy AMR system. Thus, Command Center 6.0 adds the capability to provide both strict security and encryption on the AMI-side while maintaining the more relaxed security on the AMR-side in the new AMR-AMI concentrator nodes. This upgrade was performed in the winter of 2013-2014.

2.2.1.1.4 Lessons Learned

Throughout the build, integration, and daily operation of the AMI system, numerous considerations were realized and should be noted for future implementations. These Lessons Learned are as follows:

- KCP&L had a very successful deployment in terms of customer reaction and satisfaction due to strong and deliberate education effort through grassroots communication paths (goal of 10 touch points prior to installation) and a “white glove” installation approach for GIZ (3300 meters) that included a welcome packet, a knock on the door, and an IHD offer. For the entire SmartGrid Demonstration Project area, each installation included a door knock to inform the customer of their smart meter installation occurrence and to ensure safety of the installer, the customer, and the home. Also, KCP&L met with concerned and

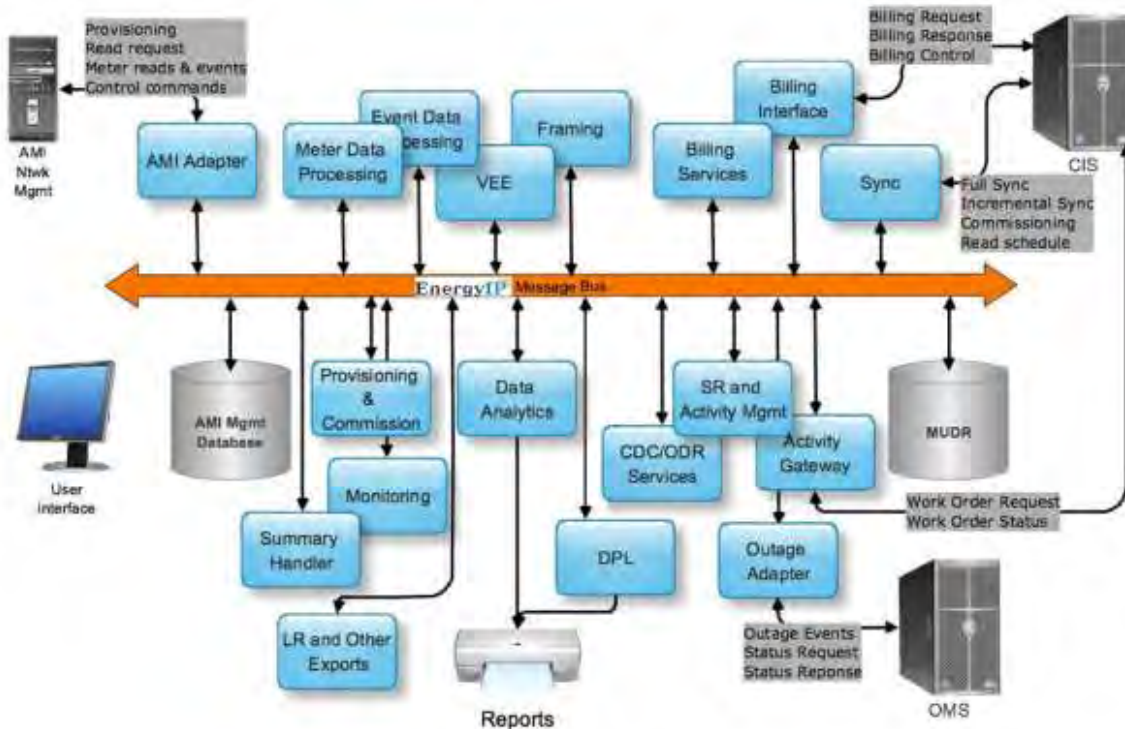
objecting AMI customers face-to-face to discuss their concerns. This helped ensure a full deployment of AMI meters to all service points within the project area.

- The choice to select a relatively unskilled workforce resulted in time delays, quality sacrifices, and a reduction in quality and consistency of customer interactions. Additionally, there was a high turnover of that unskilled workforce. Positively, this selection resulted in significant goodwill due to local job creation and local knowledge of the installers.
- A pre-implementation meter audit to identify safety, theft, and non-standard situations was effective and necessary but could have been executed more robustly with increased detail and more organization. This ancillary information could have significantly improved the efficiency of the installation process. For example, non-A-based cans were not accurately identified resulting in wasted trips to premises by installers. FOCUS AX meters cannot be installed in these cans resulting in KCP&L needed to decide if/how to replace cans which are technically owned by the customer.
- The IHD offering in conjunction with meter installation resulted in goodwill but created some technical and user challenges. For example, device installation codes need to be correlated with the proper meter IDs to ensure communications between the IHD and the meter. This requires strict attention to detail when recording codes and meter IDs. Also, the meter-to-device associations need to be made in a timely manner and could have benefited from a more hands-on provisioning process instead of relying on the customer to contact KCP&L support to finish the device pair process.
- Selection of a current vendor partner for AMI resulted in beneficial treatments such as ensured meter quantities despite industry shortage (supply/demand), pre-established relationships with open communications, a local project manager that could react to issues quickly, and meter-to-cash executed very successfully due to vendor knowledge of KCP&L systems, metering, and billing processes.
- Installation of AMI communications hardware, such as collectors and routers, on utility electric service assets helped ensure the hardware received power most or all of the time. Devices were not installed on light poles, as light poles are the last priority for outage restoration.
- Installers used handheld digital devices to capture bar codes of old and new meters at each premise to enable accurate and immediate tracking of installation progress and issues. Unskilled workers struggled to use these devices properly at times, but the devices were still an extreme improvement over manual paper or spreadsheet tracking.
- Expedited timeline and non-sequential deployment process resulted in some oversights regarding software quality assurance and version control issues that resulted in inadvertent disconnects on a small set of customers.
- The importance of clear and frequent communications between the utility and the AMI vendor and the SmartEnd-Use vendors cannot be underestimated. Technology and device references, including device installation codes, must be consistent or robustly mapped between vendors. Discrepancies often led to some confusion with the implementation of IHDs and other HAN devices. Full disclosure of issues between the vendors regarding technology and schedule risks provided increased confidence and more efficient issue resolution.
- System software and meter firmware upgrades must be highly-coordinated to ensure timely delivery and thorough completion of all upgrades.

2.2.1.2 MDM

Figure 2-23 illustrates the complex nature of the Siemens eMeter MDM implemented as part of the SmartMetering sub-project.

Figure 2-23: EnergyIP MDM Application Components



2.2.1.2.1 Build

The KCP&L Meter Data Management (MDM) system was deployed during Q1 2012 using the eMeter EnergyIP 7.2 software platform hosted by Siemens at their Customer Pilot Hosting Environment (CPHE) in Houston, TX. Initial interfaces were built between the MDM and KCP&L's internal CIS system and SmartGrid Middleware to deliver service point information and meter read data to the MDM. Additional interfaces were added following the initial launch to provide interactive two-way capabilities for Time-of-Use billing, remote service order processing, outage/restoration events and other meter events involving MDM, CIS, the AHE and Enterprise Service Bus (ESB). All meter read data (15 minute intervals and daily register reads) from the beginning of the AMI rollout in October 2010 is stored in the MDM system.

2.2.1.2.1.1 Phase 1 – Initial Launch

The MDM was implemented jointly by KCP&L and Siemens in three major phases, each comprised of several sub-projects. Phase 1 consisted of the initial launch of the system and key interfaces as well as the load of all historical meter read data from October 2010 through March 2012; this phase completed in March 2012. The MDM work necessary to support TOU billing was completed as part of this phase.

Preliminary scoping workshops were conducted in mid-2011 with development and configuration beginning in earnest in September. A key element was the stand-up of Siemens Customer Pilot Hosting Environment in Houston; this was the first time that eMeter or Siemens had implemented an eMeter installation in a Software-As-A-Service (SaaS) model. This included an internal Siemens-only Development environment as well as Test and Production environments that are connected to the corresponding KCP&L systems.

Basic configuration of the MDM included Validation, Estimation and Editing (VEE) settings, the various meter data services that process information within the MDM, all of the field values necessary to operate, configuration of the system calendar (bill cycles, holidays, etc.), user setup and security configuration. The TOU rates, calendar and usage framing setup work was also performed during this initial round of configuration activity.

KCP&L and Siemens implemented a number of core interfaces during this initial phase. They included the “FlexSync” interface to transmit incremental changes in service point information from CIS to MDM to keep the two systems in-sync with CIS acting as the system of record. KCP&L was the first customer to implement the “FlexSync” method instead of the traditional “batch” synchronization method that would send a full set of service point information for all customers on a regularly scheduled basis.

Meter reads are being sent to the MDM from the AHE via a secure file transfer process that transmits the register read file once daily with all 14,000 reads; the 15-minute interval reads are sent on an hourly basis to the MDM with approximately ¼ of the meters sending four hour blocks of intervals every hour which results in roughly 56,000 reads being sent every hour from AHE to MDM in the SmartGrid Demonstration Zone.

The final interface delivered during this phase was the “Pull Billing” interface that KCP&L is using to retrieve daily framed usage totals to be used in billing TOU customers. The “Pull Billing” interface uses the standard MDM interface in a non-traditional manner by pulling daily “Off-Cycle, Informational” reads instead of the standard monthly billing determinants; these daily totals are then fed through KCP&L’s SmartGrid middleware where they are converted into virtual daily dial reads that can be used by the legacy CIS system for billing the TOU customers.

The final component of Phase 1 involved loading both service delivery point information and meter read data to the MDM system. Using the FlexSync process, KCP&L loaded approximately 14,000 records that included customer, account, service delivery point, premise and meter data to establish the appropriate and corresponding information within the MDM. All relationship records between these various data sets were loaded as of January 2012 and did not include any historical changes – i.e. move-ins/outs, meter exchanges, etc. that may have occurred from the beginning of the SmartGrid Demonstration Project and AMI roll-out in October 2010. Once these service delivery points’ records were fully loaded, KCP&L and Siemens then loaded the set of historical AMI data from October 2010 onward. By the time this load was completed in March 2012, approximately 5.8M historical daily register reads and 550M historical 15-minute interval reads had been loaded into the MDM. The ability to load this was aided by Landis+Gyr’s willingness to retain the data longer than would typically be held during the gap between AMI roll-out and MDM stand-up and by Siemens flexibility in developing a load process; per the vendors, an MDM is typically implemented at the start of an AMI roll-out so that the data can begin loading from the onset.

2.2.1.2.1.2 Phase 2 – ESB Integration

The second phase of the MDM implementation took place over the middle and latter part of 2012. This phase focused on improving the security of the end-to-end system by moving the MDM and its interfaces to a VPN tunnel, as well as adding integration of the MDM with the ESB to allow KCP&L to take advantage of the various workflow, service order, and event management capabilities provided by the MDM. This phase completed in November 2012.

While preliminary workshops occurred in February 2012, work began in earnest in the April/May 2012 timeframe with a preliminary security assessment as well as a set of detailed Joint Design Sessions (JDS) that were hosted by KCP&L and included participation from the Siemens delivery team and Siemens/eMeter architects, as well as technical and project management support from Landis+Gyr and Intergraph.

Integration with the KCP&L SmartGrid ESB was one of the main development activities for both KCP&L and Siemens during Phase 2 of the MDM Implementation. The KCP&L ESB development provided interfaces between the MDM and CIS, OMS, AHE. Collectively, these interfaces support three different business processes. Siemens supported this integration work by implementing the eMeter L+G 5.1 Adapter (IEC61968-9 Version 1 compliant) which faces the AHE and supports receipt of outage, restoration and general meter event messages and the handling of remote connect/disconnect and on-demand read commands. Between CIS and MDM, to support the transmission of remote connect, remote disconnect, and on-demand read commands from CIS to the AHE, Siemens developed the "CIM2AG" adapter (IEC61968-9 Version 2 compliant) for transmitting messages between the EnergyIP Activity Gateway and KCP&L's ESB. Between OMS and MDM, Siemens developed the "OMS2CIM" adapter (IEC61968-9 Version 2 compliant) which currently supports transmission of Outage/Restoration events via the ESB to OMS. Configuration of the MDM was also performed by Siemens to support the necessary workflow for translation and management of the remote service orders as well as the outage and restoration events. General meter events (non-outage, non-restoration) are simply logged in the MDM for future analysis.

2.2.1.2.1.3 Phase 3 – Wrap-Up

The final phase of the MDM Implementation was completed in July 2013. Major elements completed in this phase can be broadly grouped into two categories: Functionality and Operational Support.

The category of "Functionality" includes both internal MDM configuration as well as some additional interface work between the MDM, ESB and other KCP&L SmartGrid Systems. The eMeter L+G Adapter was upgraded from the originally implemented 5.1 Adapter to the newer 5.7 Adapter; this enabled support for the Power Status Verification (PSV) interface between the OMS system and AMI infrastructure and also resolved outstanding defects in the original 5.1 adapter that KCP&L had identified. The PSV project enables the OMS system to send a PSV request message via the ESB to MDM where it is translated to the appropriate message type and then sent on to the AMI system for response. MDM provides workflow management for this process.

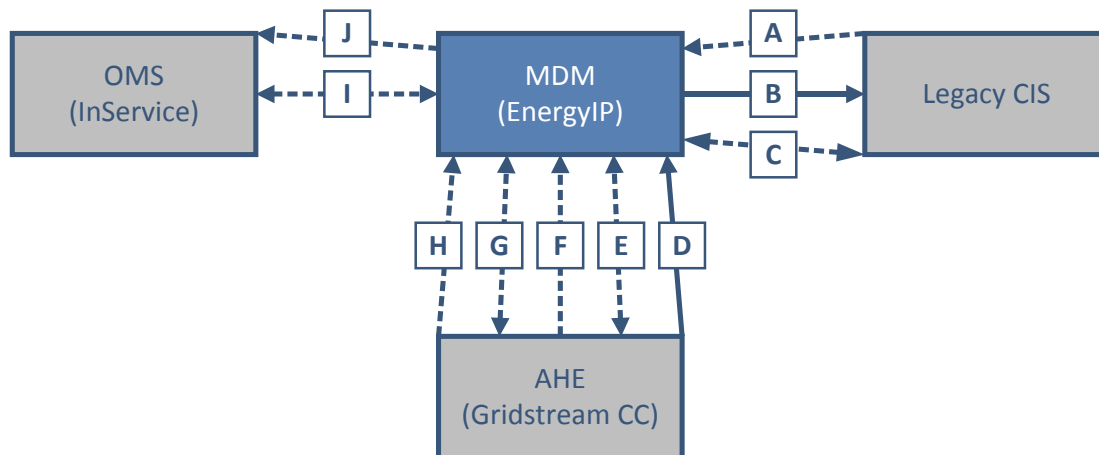
Interval data is at the core of two additional work packages – the aggregation of interval data for load research by KCP&L as well as the delivery of post-VEE'd interval data from MDM to downstream systems such as the HEMP, DMAT and DERM. Configuration to deliver both of these outputs was performed in the MDM. While testing the delivery of post-VEE'd data process, it was discovered that historical gap filling and the re-VEE of data caused data synchronization problems for many of the downstream systems and would cause adverse impacts to some of the existing downstream workflows, therefore KCP&L decided not to move forward with delivering this post-VEE'd data to downstream systems.

A final set of functionality expanded the remote service order capability delivered in phase 2 to include remote disconnects and reconnects related to non-payment by customers; the majority of this work was performed in the CIS system to identify these customers whereas MDM re-used the existing workflow and support testing.

2.2.1.2.2 *Integration*

An overview of MDM system-to-system interfaces and applicable messages is illustrated in Figure 2-24.

Figure 2-24: KCP&L SmartGrid Demonstration Project MDM Integration



The integration touch points for the MDM are as follows:

- A. 'Customer Information' data initiated from CIS to MDM. Also known as "FlexSync", this incremental data is used to keep CIS and AHE in-sync for customer records, service connectivity, and meter deployment/exchange purposes.
- B. 'Billing Determinant' data initiated from MDM to CIS. This data is requested daily by CIS and is used to update CIS with proper billing determinant information for TOU customers including summer on-peak, summer off-peak, and winter off-peak consumption data.
- C. 'Remote Service Order' request-reply messages initiated from CIS to MDM. This consists of a single IEC 61968 CIM-formatted service order request from CIS to MDM and a single IEC 61968 CIM-formatted service order reply from MDM to CIS once the service order has been executed between MDM and AHE. See Item E. below.
- D. 'Daily Register and Interval Read' data initiated from AHE to MDM. This is California Metering Exchange Protocol (CMEP)-formatted data sent hourly to be store in the meter usage data repository and used for TOU billing determinants.
- E. 'Remote Service Order' request-reply messages, including On-Demand Read and Remote Service Connect/Disconnect, initiated from CIS to MDM and sent from MDM to AHE. These are IEC 61968 CIM-formatted request-reply messages used to get on-demand reads and execute remote service connect/disconnects on eligible target SmartMeters. See Item C. above.
- F. 'General Event' notification initiated from AHE to MDM. This is an IEC 61968 CIM-formatted event message used to notify MDM of various MDM-supported events (using the corresponding CIP 4-part IDs) that occur within the AMI system. MDM can then log these events and/or route them to other subscribing systems.
- G. 'Power Status Verification' request-reply initiated from MDM to AHE in the form of an 'On-Demand Read' request-reply. This is an IEC 61968 CIM-formatted request-reply used to verify power status (On, Unknown, or Service Disconnected) at a target SmartMeter. See Item I. below.
- H. 'Outage/Restoration Event' notification initiated from SmartMeters to MDM. This is an IEC 61968 CIM-formatted event message used to notify MDM of an outage or restoration event occurring at a SmartMeter.

- I. 'Power Status Verification' request-reply initiated from OMS to MDM. This is an ESB-translated request-reply used to verify power status (On, Unknown, or Service Disconnected) at a target SmartMeter. See Item G. above.
- J. 'Outage/Restoration Event' notification initiated from MDM to OMS. This is used to notify OMS of an outage or restoration event occurring at a SmartMeter.

2.2.1.2.3 Post-Implementation Operational Issues

Following the standup, integration, and preliminary testing of the MDM system, numerous post-implementation operational issues needed to be mitigated and considered. These issues included the following:

- VPN connection has periods of instability; there is not a redundant connection, so when the tunnel is down, the MDM system is inaccessible. For future off-site hosting, redundant connection should be implemented similar to what was done with the L+G MPLS connection.
- Siemens has experienced several power outage and connectivity issues with their hosting solution. While the solution was only built to support this as a "demonstration", it underscores the need for a robust hosting solution including redundant power supplies and redundant lines of communication.
- The MDM system appears to have a "race" condition within its order processing when handling Remote Service Orders. The MDM receives an "asynchronous" response for On-Demand Reads from the AHE and has to do two things with this data. (1) MDM writes the read value to an internal table; (2) MDM updates the status of the open order which triggers the response message to KCP&L's CIS+ system. There does not appear to be anything internal within the MDM that forces #1 to happen prior to #2, so the CIS regularly receives a response that does not have a meter read value included. Upon investigation, the read value can be seen in MDM, hence the belief by KCP&L that a "race" condition is occurring. Siemens has been unable to identify or resolve this issue.
- Daylight savings time (both "spring forward" and "fall back") has caused issues with system processing on both the KCP&L side as well as the MDM side.
 - The MDM product required a bug fix to resolve an issue on the "fall back" date where it wouldn't allow the load of a file with 100 intervals instead of the regular 96. This was resolved in 1Q 2013 and ran successfully in November 2013.
 - The MDM product doesn't handle the "standard" CMEP format file on the "spring forward" date which sends a file with only 92 intervals. Since MDM is expecting 96 intervals, it estimates the missing 4 intervals. L+G has an "enhanced" CMEP format, however the Siemens MDM does not accept that format with its current adapter. This was handled manually by KCP&L team members for 2013 and the same approach will be used to handle this in 2014.
 - KCP&L interface sends a date/time stamp on pull billing requests for TOU; KCP&L development resources were unable to successfully deploy a working fix to modify the "UTC" value sent over on the days when the daylight savings time change occurs, so the requests had to be manually resubmitted. The manual workaround will be used to support the remaining DST changes.
- KCP&L primarily used contract resources to implement the interfaces to MDM. Once these resources rolled off, the internal team members were left to support solutions that were not within their primary area of expertise and which were not the KCP&L target state solution. This has made it more difficult to troubleshoot issues.

To be updated in future releases of this report.

2.2.1.2.4 Lessons Learned

Throughout the build, integration, and daily operation of the MDM system, numerous considerations were realized and should be noted for future implementations. These Lessons Learned are as follows:

- Industry standards were not readily available from our vendors to support interoperability; in every case (MDM, OMS, and AHE), KCP&L was required to have either KCP&L, project vendors, or both perform custom development work to support these standards, despite the claim that the vendor systems were supposed to be standards compliant.
- For future off-site hosting, a redundant connection should be implemented similar to what was done with the L+G MPLS connection.
- Future hosted solutions should be installed and maintained at a traditional industry standard data center which provides a robust hosting solution including redundant power supplies and redundant lines of communication.
- Per feedback from Siemens as part of this project, as well as other MDM vendors, an MDM solution is more commonly deployed prior to or at the beginning of an AMI rollout which eliminates the need for a historical data load.
- The legacy CIS+ system was unable to accept billing determinants from the MDM. KCP&L had to build a custom process to load MDM generated billing determinants into the CIS+ system to support TOU billing. This MDM-CIS integration point is a key benefit that will be delivered by the new target state systems.
- For future systems that will be implemented by 3rd party system integrators or contract resources, it is imperative that an effective knowledge transfer and system training plan be put into place to ensure that the KCP&L team members will be able to fully support the system once the external resources have rolled off the project.
- Future MDM systems need enhanced workflow management internal to their systems to prevent issues such as the RSO “race” condition from occurring.
- Due to this being a “demo” project, KCP&L business users have not been actively using the MDM system and have only used their existing legacy CIS+ systems to view meter read data. This has left the IT team as the only active user of the system for troubleshooting and support of order processing. For future installations, it will be imperative to get business teams such as Billing Services, Customer Care and Meter Technology engaged in actively using and supporting MDM activities.

To be updated in future releases of this report.

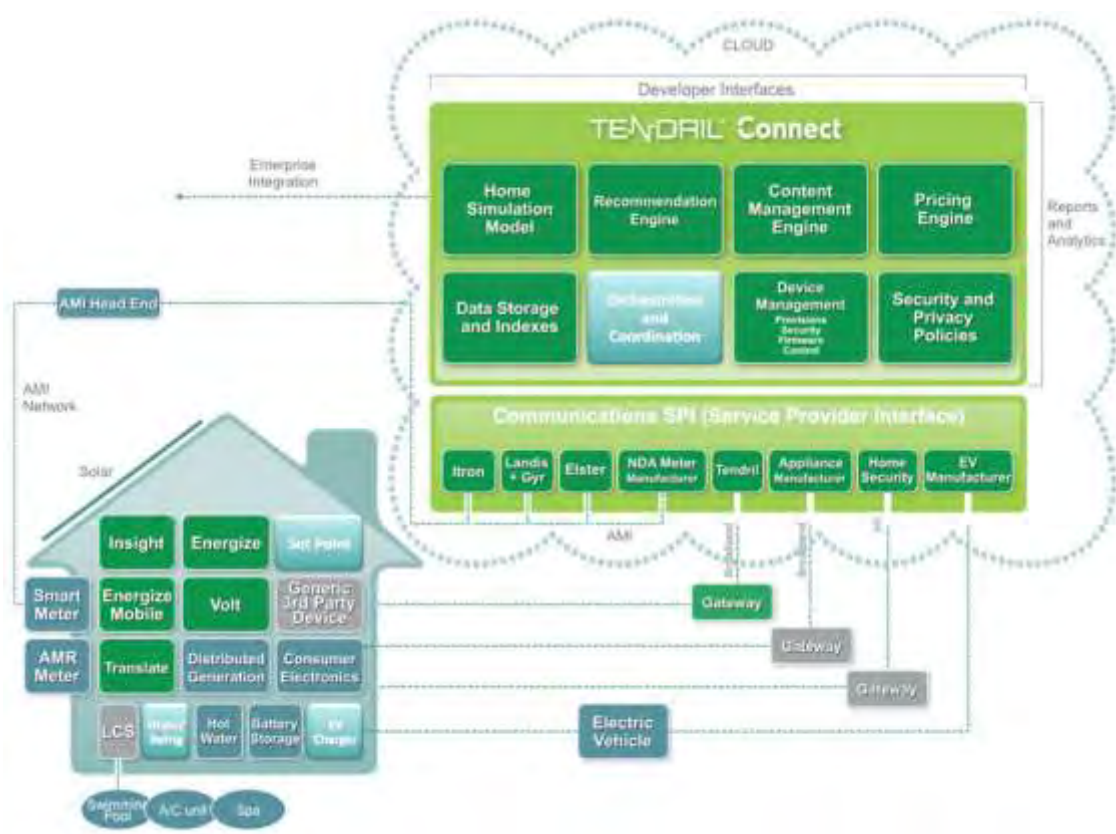
2.2.2 SmartEnd-Use

The SmartEnd-Use sub-project deployed a state-of-the-art Home Energy Management Portal (HEMP) with optional In-Home Displays, Stand-alone PCTs, complete HAN implementations, and TOU pricing programs. The following subsections summarize these Smart-End Use component deployments.

2.2.2.1 Home Energy Management Web Portal

The Customer Home Energy Management Web Portal (HEMP) program was rolled-out to KCP&L customers in October 2010, coinciding with the AMI implementation and IHD deployments. KCP&L chose to implement Tendril's Connect platform to provide customers with both a web-based portal and in-home devices.

Figure 2-25: Tendril™ Connect Platform Architecture



2.2.2.1.1 Build

KCP&L chose to implement the HEMP system as a managed-service and hosted-platform, with Tendril in charge of hosting the backend servers and systems and capturing meter reads to meet contractual performance criteria.

For the development environment, Tendril stood-up a hosted back-end platform cloned from the production system. The hosted development environment interfaced with the development DERM and AHE. Over 25 meters in the AMI lab were associated to development HEMP accounts to emulate real-life customer meters. These development environments and interfaces were used to test all HEMP requirements, including system-to-system integration and HAN device testing.

Integration with the customer AccountLink was completed to enable Single Sign-On (SSO) access to the portal for customers. Secure account sign-on is managed by an interface between HEMP and AccountLink that utilizes Security Assertion Markup Language (SAML).

2.2.2.1.1.1 Energy Usage Information

Historical AMR usage meter reads were loaded into the HEMP up-front to give customers immediate access to up to two years of historical usage information. Integration was completed with the AHE to populate the portal with accurate customer usage. Day-behind meter reads are passed from the AHE through MQ Broker interfaces to the HEMP on a daily basis. The data is then offset by a fixed value equal to the customer's last AMR read to provide a seamless transition between AMR data and AMI data. Customers with a HAN configuration receive real-time meter reads in their portal from the HAN Gateway pulling real-time meter reads from the SmartMeter and sending them to the portal via the Internet.

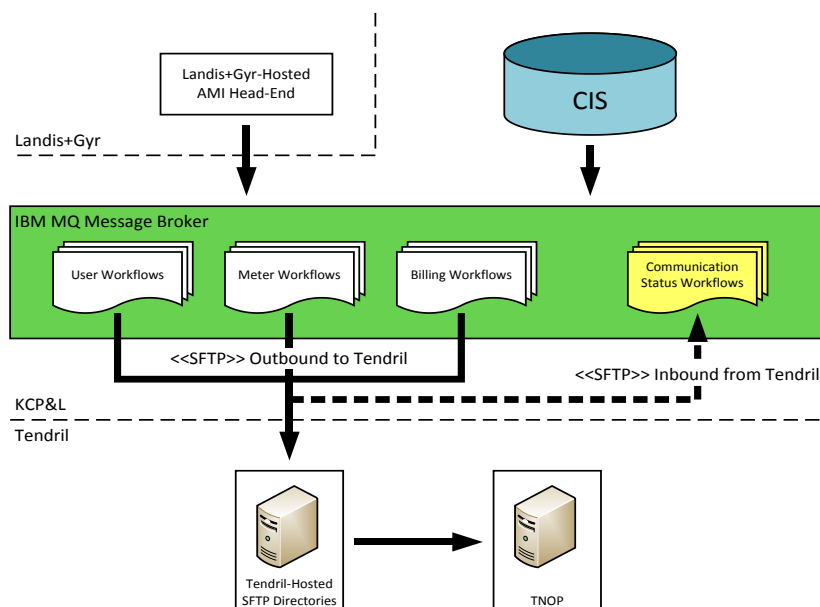
2.2.2.1.1.2 Billing Information (Estimated Billing True-Ups)

Integration was completed with the CIS to populate the portal with accurate customer historical and estimated billing information. A special process was created to estimate the customer billing information with accurate taxes and fees based on the customer's current rate. The bill estimate provides an end-of-bill-cycle projected bill based on usage-to-date in a given billing cycle. Historical billing information and daily estimated bill "true-ups" (including taxes and fees) are created by the CIS and passed through an MQ Broker interface to HEMP to be displayed in the portal. Upon receipt of successful estimated bill "true-up" messages to HEMP, CIS pulls the "true-up" back from Tendril to be sent to customer IHDs on a daily basis by use of a "tunnel text message". The tunnel text message provides a means of getting custom data into the IHD via the built-in ZigBee text messaging mechanism by use of special characters within the message for the device to interpret appropriately.

2.2.2.1.1.3 Pricing Signals

Integration was completed with the CIS to populate the portal with accurate customer pricing information. Pricing signals based on customer rates are created by the CIS and passed through an MQ Broker interface to HEMP to be displayed in the portal. Upon receipt of successful pricing signals, CIS pulls the pricing message back from Tendril to be sent to IHD via the AHE and SmartMeter using the ZigBee SEP 1.0 "publish price" command. A special event pricing signal was required to support TOU rates. Sent on a daily basis, TOU event pricing signals are sent to trigger a peak-price change from 3 – 7 PM.

Figure 2-26: Customer Web Portal Data Flows



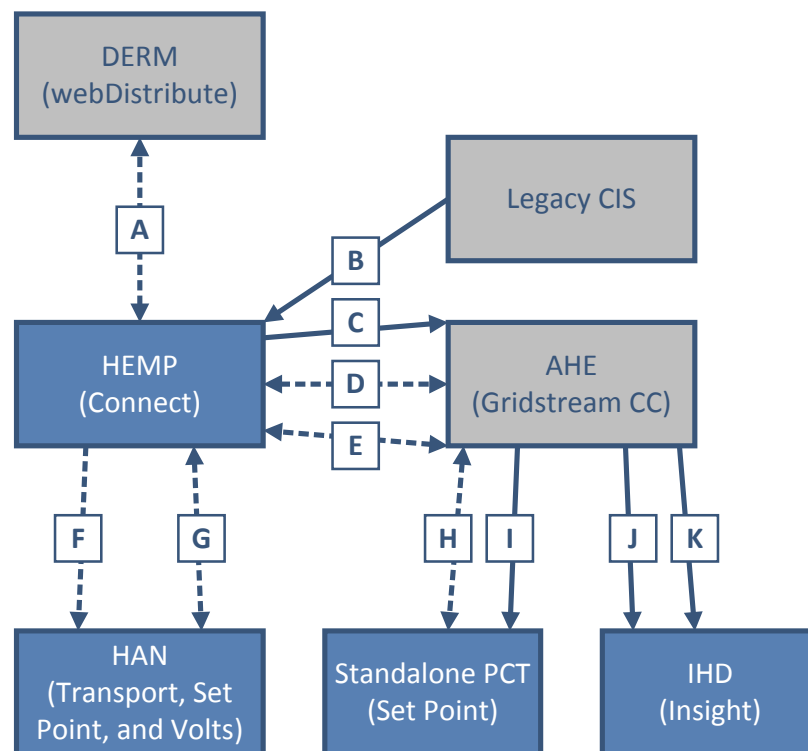
2.2.2.1.1.4 Demand Response Events

Integration was completed with the DERM to receive OpenADR-based demand response events. Demand response events are received into an OpenADR adapter at HEMP, where they are routed based on the target asset(s) (HAN vs. Standalone PCT). For messages directed to HANs, HEMP sends the demand response events directly to the HAN gateway via the Internet and receives event participation messages from the HAN via the same interface. For messages directed to Standalone PCTs, integration was completed with the AHE to allow demand response events and event participation messages to be sent between the two systems. The AHE manages the interface and messaging between the AHE and the Standalone PCTs.

2.2.2.1.2 Integration

An overview of HEMP system-to-system interfaces and applicable messages is illustrated in Figure 2-27.

Figure 2-27: KCP&L SmartGrid Demonstration Project HEMP Integration



The integration touch points for the HEMP are as follows:

- 'Demand Response Event' request initiated from DERM to HEMP, and 'Event Opt-Out/Opt-In' reply initiated from HEMP (for both HANs and Standalone PCTs) to DERM. These are OpenADR-formatted request-reply messages used to notify HEMP of creation, modification, or cancellation of impending DR events and to notify DERM of DR assets' event participation status.
- 'Consumption Pricing' and 'Billing True-Up' messages initiated from CIS to HEMP. These messages are sent daily to update the customer portal and IHDs with real-time per-kWh consumption pricing information and up-to-date estimated billing information.
- 'Consumption Pricing' and 'Billing True-Up' messages initiated from HEMP to AHE. These "tunnel text messages" are sent daily to update customer IHDs with real-time per-kWh consumption pricing information and up-to-date estimated billing information.

- D. 'Get Device Info' request-reply initiated from HEMP to AHE. This is an IEC 61968 CIM-formatted request-reply used to gather HAN device information for AMI-based DR assets (Standalone PCTs).
- E. 'Demand Response Event' request initiated from HEMP to AHE, and 'Event Opt-Out/Opt-In' reply initiated from AMI-based DR assets (Standalone PCTs for this project) to HEMP. These are IEC 61968 CIM-formatted request-reply messages used to notify AMI-based DR assets of creation, modification, or cancellation of impending DR events and to notify HEMP of AMI-based DR assets' event participation status.
- F. 'Device Control' signals initiated from HEMP to HAN devices via the Internet. These are ZigBee Smart Energy Profile (SEP) 1.0-formatted request messages triggered by customer actions in the portal and used to control HAN devices including changing PCT temperature set point and turning LCS devices on/off.
- G. 'Demand Response Event' requests initiated from HEMP to HAN DR assets via the Internet, and 'Event Opt-Out/Opt-In' replies initiated from HAN DR assets to HEMP via the Internet. These are ZigBee Smart Energy Profile (SEP) 1.0-formatted request-reply messages used to notify HAN DR assets of creation, modification, or cancellation of impending DR events and to notify HEMP of HAN DR asset event participation status.
- H. 'Demand Response Event' requests initiated from AHE to AMI-based DR assets (Standalone PCTs for this project) via SmartMeters, and 'Event Opt-Out/Opt-In' replies initiated from AMI-based DR assets to AHE via SmartMeters. These are ZigBee Smart Energy Profile (SEP) 1.0-formatted request-reply messages used to notify AMI-based DR assets of creation, modification, or cancellation of impending DR events and to notify AHE of AMI-based DR asset event participation status.
- I. 'Consumption Pricing' messages initiated from AHE to Standalone PCTs. These "tunnel text messages" are ZigBee Smart Energy Profile (SEP) 1.0-formatted messages sent daily to update customer Standalone PCTs with real-time per-kWh consumption pricing information.
- J. 'Estimated Bill True-Up' messages initiated from AHE to IHDs. These "tunnel text messages" are ZigBee Smart Energy Profile (SEP) 1.0-formatted messages sent daily to update customer IHDs with up-to-date estimated billing information.
- K. 'Consumption Pricing' messages initiated from AHE to IHDs. These "tunnel text messages" are ZigBee Smart Energy Profile (SEP) 1.0-formatted messages sent daily to update customer IHDs with real-time per-kWh consumption pricing information.

2.2.2.1.3 Post-Implementation Operational Issues

Following the standup, integration, and preliminary testing of the HEMP, numerous post-implementation operational issues needed to be mitigated and considered. These issues included the following:

- As part of the initial stand-up, KCP&L decided to add the last pre-exchange AMR meter read to the new AMI meter reads (all of which started at '0' kWh). This was done to give customers immediate access to their historical usage data with a seamless transition between AMR data and AMI data that started at '0' kWh. However, this eventually caused issues for customers who had meter exchanges performed (due to meter issues) because additional offsets were not tracked and added for AMI meters that were exchanged. This discontinuity in the meter data led to meter data "spikes" due to the change in the order of data magnitude. See next item.
- Tendril's platform was designed to utilize register reads, as opposed to interval reads. This caused issues in the case of meter exchanges because the new meter reads would be on a

different order of magnitude from the previous meter (for example, the previous meter register reads could be “30,000 kWh”, while the new meter register read would be “0 kWh”). These abrupt order of magnitude changes in meter read data would cause data “spikes” in the customer presentation in the portal. This resulted in inaccurate representations of usage and cost at the time of the meter exchange. This issue would not present itself in an environment that utilized interval reads as the interval reads would remain at a relatively steady magnitude regardless of the register read magnitude.

- Tendril’s platform did not initially support block rate pricing. The short-term fix for this involved manually send price updates to Tendril’s platform – this was fixed by manually sending pricing information to the Tendril platform to pick up any rate changes that may have gone into effect on the previous day (i.e. customer moved into the next usage block of the rate on the previous day). This issue was resolved in the long-term when Tendril included support for block rates in the first platform upgrade.
- Customer portal accounts in the HEMP platform were each given a unique ID comprised of a concatenation of customer Account ID and Service Point ID. This meant that each customer account was associated to a specific customer at a specific location, instead of being associated to a specific customer. This means that new accounts had to be created every time a customer moved to a new residence, thus resulting in the loss of historical usage data from the customer’s new account.
- KCP&L undertook two major HEMP platform upgrades during the project to support required project functionality and maintain technical support from Tendril. These upgrades required extensive testing of bugs and fixes. The time required for testing was initially underestimated and required additional resources than expected.
- Numerous issues arose with the device installation process of the IHD program. One issue was the device IDs not being communicated properly to the AHE during the device provisioning process. Another issue was that KCP&L was unable to verify whether or not the IHDs were plugged-in by the customer after delivery during the “white glove” process. Most of these issues were mitigated during the Standalone PCT and HAN installations due to the fact that these devices required in-home installation and verification by a trained workforce. Installers were able to correctly verify device IDs and successfully complete device provisioning to the Smart Meter while in the customer’s home.
- Meter exchanges caused issues with HAN device association in that the device(s) would stay associated with the old meter that was exchanged. In order to get the same device provisioned to the new meter, the device(s) needed to be manually cleaned from the AMI database whenever meters were exchanged. This reallocated the device(s) within the AHE database to be provisioned to the new meter.

2.2.2.1.4 Lessons Learned

Throughout the build, integration, and daily operation of the HEMP system, numerous considerations were realized and should be noted for future implementations. These Lessons Learned are as follows:

- Interval data is much more desirable than register reads due to the issues that register reads can cause. With interval reads, data presentation has no dependence on the relationship between reads over time. However, processing register reads can cause issues in the event of meter exchanges, as significant changes in the order of magnitude between two consecutive reads can cause abnormalities in data presentation.
- Loading two years of historical AMR data and creating a process to offset customers new AMI data by a fixed value equal to their last AMR read had benefits up-front in that it allowed customers access to their historical consumption data with a seamless transition between AMR data and AMI data. However, this caused data presentation issues any time

a customer had a meter exchange in that the offset only account for the last AMR read and did not account for the last AMI read of any interim AMI meters.

- Due to the fact that customer HEMP IDs were associated to a specific customer at a specific location, historical customer usage data did not carry over when customers would move to new locations in the Project Area. High turnover in the Project Area led to an exorbitant number of unused accounts that were not deleted after the customers moved out.
- ZigBee SEP 2.0 was not completed during the product development and deployment cycles, so all functionality was limited to functionality available in SEP 1.x. Certain functionalities that exist in Legacy KCP&L thermostat programs (i.e. Energy Optimizer) are not supported by SEP 1.x, such as HVAC cycling, so these functionalities were not available or implemented as a part of this project.
- The OpenADR 2.0 Profile A standard was implemented for the DR interface between HEMP and DERM. This was the first OpenADR integration that Tendril had been involved with, thus Tendril had to develop a special OpenADR appliance to handle OpenADR-formatted DR messaging between HEMP and DERM.
- A special bill-estimation tool needed to be created to generate accurate billing true-ups that included taxes and fees. This was required due to varying customer fees across different customer rates. This tool helped deliver accurate estimated billing information to customers on a daily-basis. This estimated-billing information includes price-to-date as well as projected end-of-month costs based on usage-to-date in the current billing cycle.
- Tendril's platform does not currently support net metering. Negative usage data (-kWh) was not displayed properly in the portal. Thus, customers with net metering did not have the same experience as non-net metered customers.
- A sufficient lab environment was not created early on in the project to give KCP&L and Tendril an accurate representation of the KCP&L implementation. This made it difficult to replicate the customer environment for troubleshooting issues. This was resolved in the middle of the project when robust lab was built-out including a HEMP system cloned from Production, an AMI infrastructure, and numerous HAN devices spanning all three HAN device programs.

2.2.2.2 In-Home Display

The IHD was rolled out to KCP&L customers in October 2010, coinciding with the AMI and Customer Web Portal deployments. Integration was completed with the AHE, CIS, and SmartMeters to populate the IHDs with accurate real-time usage information, real-time pricing information, day-behind customer usage information and estimated billing information.

2.2.2.2.1 Build

The IHD core capabilities are part of Tendril's a commercially available, productized software solution which can be configured to the needs of a given utility. By pursuing this "off-the-shelf" philosophy to the maximum degree possible, limited design and development was required. The following sections provide a summary of the development and configurations that were required to implement and deploy the desired IHD functionality.

2.2.2.2.1.1 **AMI Backhaul and HAN Management**

The IHD is provisioned to the SmartMeter-managed HAN. The HAN is a ZigBee network supporting SEP 1.x. The IHD receives real-time usage information directly from the SmartMeter. Daily estimated bill "true-up" messages and pricing information are sent to the IHD via the AMI network and through the

SmartMeter. Device management (provisioning, de-provisioning, etc.) is performed within the AHE by customer service representatives within KCP&L.

2.2.2.2.1.2 Energy Usage Information

The IHD receives real-time demand (kW) and consumption (kWh) data directly from the SmartMeter. The IHD processes this information, along with pricing signals from the SmartMeter, to give customers an accurate real-time estimate of cost and consumption for the present day as well the previous day.

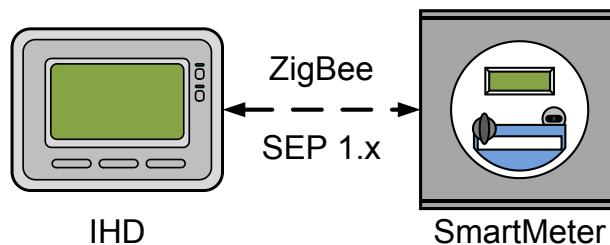
2.2.2.2.1.3 Billing Information (true-up)

A special process was created to estimate the customer billing information with accurate taxes and fees based on the customer's current rate. The bill estimate provides an end-of-bill-cycle projected bill based on usage-to-date in a given billing cycle. Estimated bill "true-up" messages are sent to customer IHDs on a daily basis by use of a "tunnel text message". The tunnel text message provides a means of getting custom data into the IHD via the built-in ZigBee text messaging mechanism by use of special characters within the message for the device to interpret appropriately.

2.2.2.2.1.4 Pricing Signals

Pricing signals based on customer rates are created by the CIS and passed through an MQ Broker interface to the AHE. Pricing signals are sent to the IHD via the AMI network through the SmartMeter using the ZigBee SEP 1.0 "publish price" command. Customers can then see their real-time energy price and accumulated daily costs. A special event pricing signal was required to support TOU rates. Sent on a daily basis, TOU event pricing signals are sent to trigger a peak-price change from 3 – 7 PM.

Figure 2-28: In-Home Display Communication



2.2.2.2.2 Post-Implementation Operational Issues

Following the initial integration, testing and deployment of the IHDs, numerous post-implementation operational issues needed to be considered and mitigated. These issues included the following:

- During the IHD program deployment, an issue was found in the IHD firmware that modified the IHD screen contrast rendering the screen unreadable. This issue was resolved by returning the current inventory of IHDs to Tendril and receiving a new shipment of IHDs on a newer firmware version containing a fix for this bug. As for the IHDs that were already deployed, these were replaced one-by-one as the affected customers contacted KCP&L to report the issue.
- While not an IHD issue directly, a bug with the ZigBee chip in the meter caused a modification to the price pushing process for the IHD where the ZigBee chip had to be reset for pricing changes to take effect on the IHD. This was temporarily remedied with a workaround that involved sending multiple commands to the meter to reset the chip and send the price. Long term, this was remedied with a firmware upgrade to the meter.
- Furthermore, since the Tendril platform did not initially support block rates, including the KCP&L standard residential declining-block rate, pricing changes were not automatically

triggered to the IHDs when the customer moved into a new usage block within the rate. The short-term fix for this issue involved sending the correct price to the IHD on a daily basis, in order to pick up any rate changes that may have gone into effect on the previous day (i.e. customer moved into the next usage block of the rate on the previous day). This issue was resolved in the long-term when Tendril included support for block rates in the first platform upgrade.

- Prior to the first HEMP platform upgrade, Tendril frequently encountered issues when processing estimated bill “true-up” messages. Consequently, CIS was never notified of a successful “true-up” receipt at HEMP and was unable to pull the “true-up” message back from HEMP. This broke the defined “true-up” process and resulted in “true-up” messages not getting sent to customer IHDs.

2.2.2.2.3 Lessons Learned

Throughout the deployment and daily operation of the IHDs, numerous considerations were realized and should be noted for future implementations. These Lessons Learned are as follows:

- A special “tunnel text message” was implemented to support getting estimated billing information into the IHD. This message contained unique identifiers to enable it to “tunnel” into the IHD and was required to update the billing information within the IHD.
- Tendril’s IHD does not currently support net metering. Negative usage data (-kWh) was not displayed properly on the IHDs. Thus, customers with net metering did not have the same experience as non-net metered customers.
- The IHD offering in conjunction with meter installation resulted in goodwill but created some technical and user challenges. For example, device installation codes need to be correlated with the proper meter IDs to ensure communications between the IHD and the meter. This requires strict attention to detail when recording codes and meter IDs. Also, the meter-to-device associations need to be made in a timely manner and could have benefited from a more hands-on provisioning process instead of relying on the customer to contact KCP&L support to finish the device pair process. Despite the convenience of having a device delivered to them through the “door knock” initiative, many customers did not utilize their IHDs. KCP&L saw better customer engagement on the Standalone PCT and HAN programs, as these programs involved devices that customers already use on a daily basis (thermostats, water heaters, etc.). Furthermore, device reliability and persistent connectivity issues negatively affected on-going customer participation. After deploying over 1,100 IHDs, the project currently has rough 700 operational IHDs that are still communicating with the SmartMeter.

2.2.2.3 Standalone Programmable Communicating Thermostat (PCT)

The Standalone PCT program was rolled-out to KCP&L customers in June 2012. Along with the built-in programmable schedule, the Standalone PCT supports pricing signals and demand response events via communications with the SmartMeter. Integration was completed with the AHE, CIS, and SmartMeters to populate the Standalone PCTs with real-time pricing information to enable customers to make energy and cost conserving decisions when programming the temperature set point and programmable schedule.

2.2.2.3.1 Build

The PCT core capabilities are part of Tendril’s a commercially available, productized software solution which can be configured to the needs of a given utility. By pursuing this “off-the-shelf” philosophy to the maximum degree possible, limited design and development was required. The following sections

provide a summary of the development and configurations that were required to implement and deploy the desired PCT functionality.

2.2.2.3.1.1 AMI Backhaul and HAN Management

The Standalone PCT is provisioned to the SmartMeter-managed HAN. The HAN is a ZigBee network supporting SEP 1.x. DR event messages and pricing information are sent to the Standalone PCT via the AMI network and through the SmartMeter. Prior to provisioning the Standalone PCT to a customer's SmartMeter, the customer's Customer Web Portal account is configured to support the PCT. Device management (provisioning, de-provisioning, etc.) is performed within the AHE by customer service representatives within KCP&L.

2.2.2.3.1.2 Programmable Schedule

The Standalone PCT contains a built-in programmable schedule that allows the customer to choose when and how to change their thermostat set point at multiple times throughout the day. The customer can select the set point and time to change it for four different time slots on each day of the week. The customer can also select the 'mode' for the thermostat to operate under, with the options of Schedule (follows the customer-programmed schedule), Hold (holds the set point at a fixed value), and Vacation (adjusts the set point for a selected window of time).

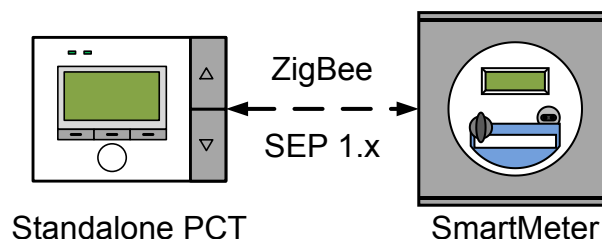
2.2.2.3.1.3 Pricing Signals

Pricing signals based on customers rates are created by the CIS and passed through an MQ Broker interface to the AHE. Pricing signals are sent to the Standalone PCT via the AMI network through the SmartMeter using the ZigBee SEP 1.0 "publish price" command. Customers can then see their real-time energy price. A special event pricing signal was required to support TOU rates. Sent on a daily basis, TOU event pricing signals are sent to trigger a peak-price change from 3 – 7 PM.

2.2.2.3.1.4 Demand Response Events

The Standalone PCT also supports demand response functionality. Through integration between the DERM, HEMP, and AHE, the Standalone PCTs can receive demand response events to help reduce, level, or shift load during peak demand periods. The DERM can forecast demand on the distribution grid and call on the Standalone PCTs for load reduction, if necessary. A message is sent from the DERM to the HEMP to identify the Standalone PCT customers needed to meet the load reduction requirements. The HEMP then routes the demand response messages to the AHE. The AHE passes the demand response events to the Standalone PCTs via the SmartMeters prior to or at the start time of the event, depending on the event parameters. Once received at the Standalone PCT, the customer is automatically opted into event participation with the option to opt out of the event at any time prior to the end of the event. This opt-out/in decision can be made directly at the device. Customer event participation information is then passed to the DERM via the AHE and HEMP to be used for post-event analysis and future demand response forecasting.

Figure 2-29: Standalone PCT Communication



2.2.2.3.2 Post-Implementation Operational Issues

Following the initial integration, testing and deployment of the Standalone PCTs, numerous post-implementation operational issues needed to be considered and mitigated. These issues included the following:

- The initial shipment of Standalone PCTs had to be returned to Tendril because they did not meet project requirements, with the primary issue being that they were not SEP 1.1-certified. These devices were returned to Tendril and replaced with Tendril's newer model PCT that met project requirements for Standards and DR integration.
- Standards-based DR integration between Tendril and L+G did not exist out of the box. Tendril and L+G worked together to develop CIM-based DR integration between the HEMP and the AHE. This additional work led to delays in the deployment schedule of the Standalone PCT. Due to the SEP 1.x compliance of both the SmartMeter and the Standalone PCT, no integration development was required between the two devices.

To be updated in future releases of this report.

2.2.2.3.3 Lessons Learned

Throughout the deployment and daily operation of the Standalone PCTs, numerous considerations were realized and should be noted for future implementations. These Lessons Learned are as follows:

- The number of compatible HVAC systems was lower than expected among customers in the project demonstration zone, thus customer enrollment and participation in the Standalone PCT program turned out to be lower than initially anticipated. Many homes either had non-central heating/cooling (e.g. window air-conditioner) or had systems that were not compatible with Tendril's thermostat. In some instances, KCP&L utilized an "add-a-wire" kit to enable compatibility between the Tendril thermostat and the customer's 4-wire HVAC system. Often times, a customer would be interested in signing up for the Standalone PCT program, but would be disqualified during the pre-installation screening or at the in-home visit due to these incompatibilities.

To be updated in future releases of this report.

2.2.2.4 Home Area Network

The HAN program was rolled-out to KCP&L customers in February 2012. The HAN was initially available to a small set of “friends and family” to verify functionality. Once these “friends and family” HANs were installed and verified, customers within the demonstration project were then able to enroll in the HAN program based on a set of prequalification criteria (broadband internet connectivity, HVAC type, presence of a 240V load, etc.). Integration was completed with the CIS to send pricing information to the HAN via the HEMP to populate the HAN PCT devices with real-time pricing information to enable customers to make energy and cost conserving decisions when programming the temperature set point and programmable schedule.

2.2.2.4.1 Build

The HAN core capabilities are part of Tendril’s a commercially available, productized software solution which can be configured to the needs of a given utility. By pursuing this “off-the-shelf” philosophy to the maximum degree possible, limited design and development was required. The following sections provide a summary of the development and configurations that were required to implement and deploy the desired HAN functionality.

2.2.2.4.1.1 **Broadband Backhaul and HAN Management**

The HAN consists of a broadband-connected HAN gateway that interfaces directly with the HEMP servers, one or two PCTs depending on the customer’s HVAC configuration and compatibility, two 120V Load Control Switches (LCS), and an optional 240V LCS if the customer has a compatible load (e.g. pool pump, electric water heater, etc.).

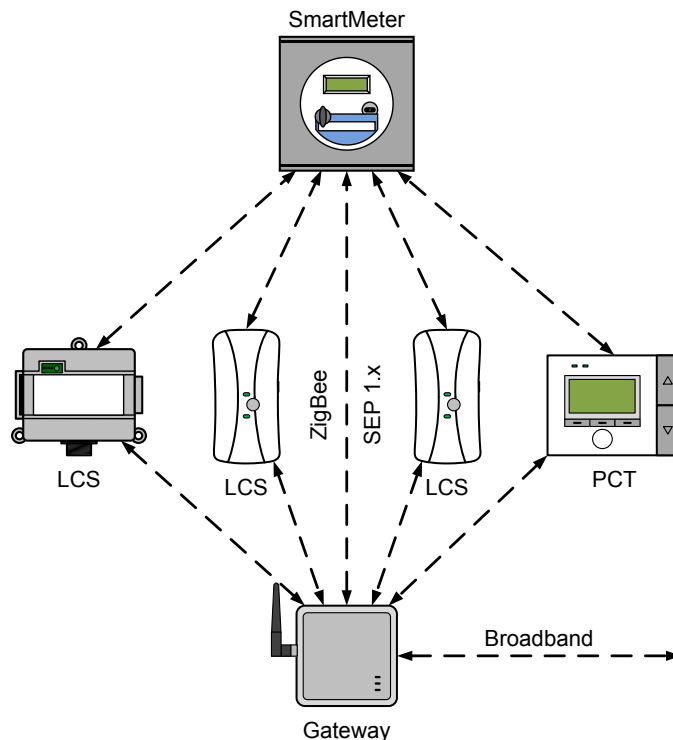
The HAN is provisioned to the SmartMeter-managed HAN. The HAN is a ZigBee network supporting SEP 1.x. DR event messages and pricing information are sent to the HAN via a broadband-connection from Tendril servers to the HAN gateway. Prior to provisioning the devices to the customer’s SmartMeter, the customer’s Customer Web Portal account is configured to support the HAN devices. Device management (provisioning, de-provisioning, etc.) is performed within the AHE by customer service representatives within KCP&L. Once the devices are provisioned to the SmartMeter, they are registered within the Customer Web Portal using the device MAC Address. Once registered within the Customer Web Portal, the customer can then access and control the devices, including changing temperature set point, PCT schedule, and pricing rules for the PCT and LCSs within the HAN.

2.2.2.4.1.2 **Programmable Schedule**

The PCT contains a built-in programmable schedule that allows the customer to choose when and how to change their thermostat set point at multiple times throughout the day. The customer can select the set point and time to change it for four different time slots on each day of the week. The customer can also select the ‘mode’ for the thermostat to operate under, with the options of Schedule (follows the customer-programmed schedule), Hold (holds the set point at a fixed value), and Vacation (adjusts the set point for a selected window of time).

2.2.2.4.1.3 **Pricing Signals**

CIS was configured to send pricing signals to the HEMP based on the customers’ rate codes. These pricing signals are pulled from the HEMP by the HAN gateway rather than through the metering network and are displayed on the PCT. Customers are able to see real-time pricing information on the screen of the PCT to make energy conserving decisions when programming the temperature set point and schedule. TOU pricing signals are managed within the HEMP based on rate information sent from CIS. TOU peak/off-peak pricing signals are sent to HAN devices via the HAN gateway at 3 PM (peak) and 7 PM (off-peak).

Figure 2-30: Home Area Network Communication

2.2.2.4.1.4 Demand Response Events

The HAN also supports demand response functionality. Through integration between the DERM and the HEMP, the HAN can receive demand response events to help reduce, level, or shift load during peak demand periods. The DERM can forecast demand on the distribution grid and call on the HANs for load reduction, if necessary. A message is sent from the DERM to the HEMP to identify the HAN customers needed to meet the load reduction requirements. The HEMP then routes the demand response messages to the HAN gateways via the broadband connection. The HAN gateway passes the demand response events to the PCT(s) and LCSs prior to or at the start time of the event, depending on the event parameters. Once received at the PCT(s) and LCSs, the customer is automatically opted into event participation with the option to opt out of the event at any time prior to the end of the event. This opt-out/in decision can be made directly at the PCT(s) and LCSs or via the Customer Web Portal. Customer event participation information is then passed to the DERM via the HEMP to be used for post-event analysis and future demand response forecasting.

2.2.2.4.2 Post-Implementation Operational Issues

Following the initial integration, testing and deployment of the HANs, numerous post-implementation operational issues needed to be considered and mitigated. These issues included the following:

- Device Firmware had to be upgraded on all HAN devices during the second HEMP platform upgrade to fix various bugs and functionality issues. This was performed via the broadband connection, and this had no impact from a customer point-of-view. Also, due to issues with the HAN inventory PCTs having a higher rate of provisioning issues on their older firmware version, a decision was made during the HAN deployment to use PCTs from the Standalone PCT inventory, as they were on a newer firmware version.
- A successful HAN installation process requires a carefully planned set of coordinated steps between the device installer and the customer service representatives performing the device provisioning to the SmartMeter. The majority of issues encountered during the

device installation process were due to the steps not being completely in the correct order. When the process was not followed properly, issues would arise with devices joining improperly or not joining the network at all. Typically, this required resetting the SmartMeter HAN and restarting the provisioning process again. Occasionally, the devices had to be replaced all together.

To be updated in future releases of this report.

2.2.2.4.3 Lessons Learned

Throughout the deployment and daily operation of the HANs, numerous considerations were realized and should be noted for future implementations. These Lessons Learned are as follows:

- Broadband internet access was lower than expected among customers in the project demonstration zone, thus customer enrollment and participation in the HAN program turned out to be lower than initially anticipated.
- The number of compatible HVAC systems was lower than expected among customers in the project demonstration zone, thus customer enrollment and participation in the HAN program turned out to be lower than initially anticipated. Many homes either had non-central heating/cooling (e.g. window air-conditioner) or had systems that were not compatible with Tendril's thermostat. In some instances, KCP&L utilized an "add-a-wire" kit to enable compatibility between the Tendril thermostat and the customer's 4-wire HVAC system. Often times, a customer would be interested in signing up for the HAN program, but would be disqualified during the pre-installation screening or at the in-home visit due to these incompatibilities.

To be updated in future releases of this report.

2.2.2.5 Time-of-Use Rate

One of the objectives of the KCP&L Smart Grid Demonstration Project was to leverage pilot smart grid technologies to evaluate the effectiveness of dynamic pricing programs on customer usage patterns. As a result, KCP&L designed and implemented an aggressive residential pilot time-of-use (TOU) rate and offered it to all qualifying residential customers within the project area.

2.2.2.5.1 Build

Following regulatory approval in December 2011, KCP&L's TOU Pilot tariff went into effect on January 1, 2012. The systems interfaces and configurations were deployed during May/June 2012 and the first customers were enrolled effective with their bills at the beginning of June 2012. Over the course of this initial Summer Season, a total of 68 customers enrolled. Four of the customers have since exited the program with two customers moving out and two customers withdrawing as they had determined it wasn't the right fit for them.

System implementation included the following components:

- CIS - Rate and measuring component setup in CIS
- MDM - Configuration of the TOU calendar and rates
- SmartGrid Middleware - Deployment of the Pull Billing Interface and the TOU Register Read Calculator
- HEMP – interface and rate changes to transmit TOU data to the Tendril back-office systems as well as the price push to the meter via the AHE

The project also developed an enrollment/cancellation process jointly with the SmartGrid Support Team and Billing Services. Several training sessions were held with these teams to introduce the overall TOU program including the rate structure, customer benefits and business support processes. Ongoing customer support is provided on a day-to-day basis by the SmartGrid Support Team. The IT team is engaged in production operational support of the various system interfaces to ensure that they are transferring and processing the necessary meter read and billing data correctly. The Billing Services team has roughly a five to seven day window of time each month when the SmartGrid Bill Cycles (3-7) are billed; during this timeframe, they review the bills for errors and also manually add the TOU bin detail to the bills for printing.

2.2.2.5.1.1 **Tariff Design and Details**

In designing a pilot dynamic pricing program, the project team established the following primary objectives:

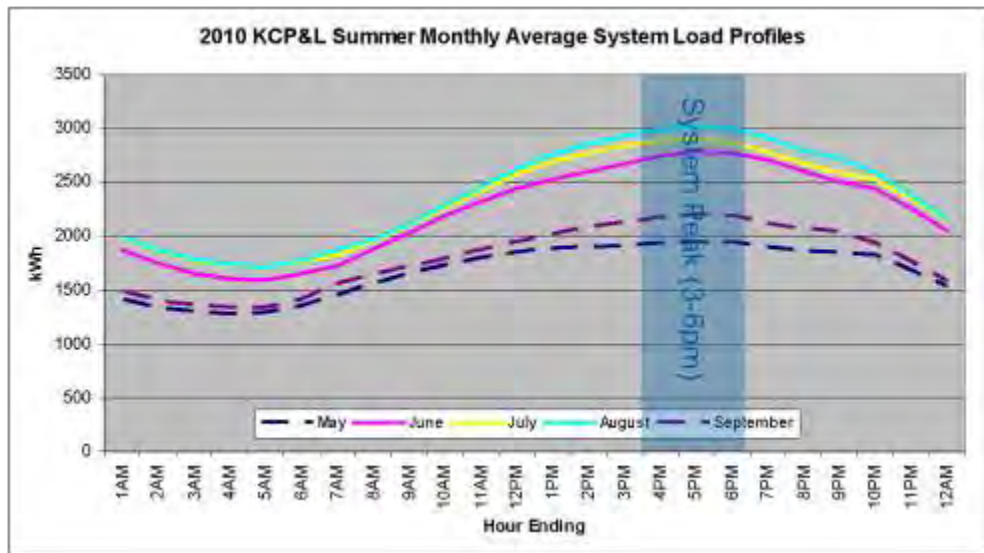
- Evaluate the effectiveness of smart grid technology to enable dynamic rate implementation
- Inform and educate KCP&L customers on the time-varying costs to supply electricity
- Use aggressive rate design to provide valuable learning to KCP&L and the industry with regards to customer behavior and response to price signals
- Implement a simple rate structure that could easily be understood by customers and that could be billed through KCP&L's legacy billing system without major modification
- Utilize effective rate design to provide load reduction during both the KCP&L system and typical residential customer peak load periods

In accordance with the stated objectives above, customer historical preference, the size of the eligible customer pool and some technical limitations with the existing KCP&L billing system, the project team settled on a simple yet aggressive TOU rate structure. This rate consists of two distinct pricing periods, a relatively short peak price period with a noticeably increased price and a discounted price the remainder of the day, effective on non-holiday weekdays throughout the summer months.

Once the general structure of the rate was established, the project team collaborated with various departments to analyze relevant data and develop an effective revenue neutral rate design that met the stated objectives.

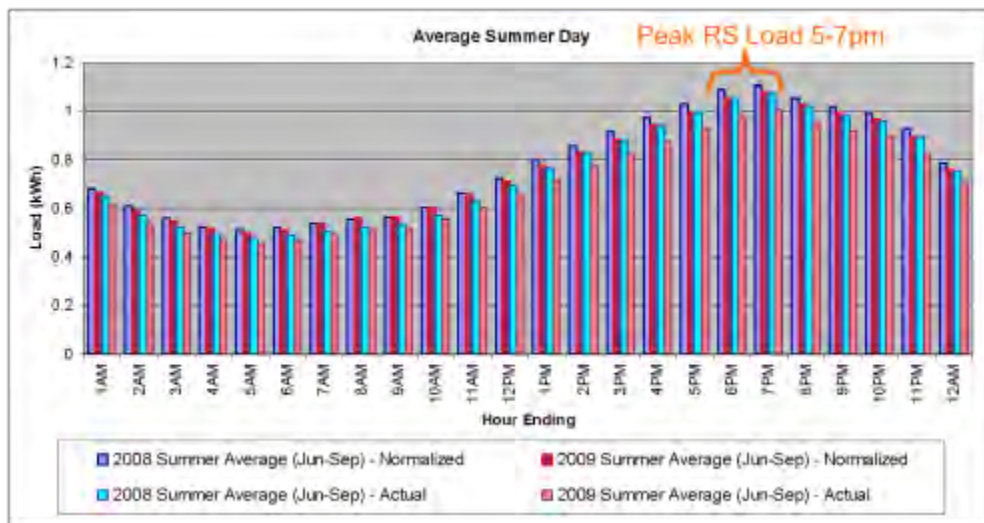
The first step was to investigate historical average daily summer system load profiles. As shown in Figure 2-31, the KCP&L system summer load profile is elevated yet relatively flat with a broad peak period centered on the 4:00-5:00 pm hour. The data shown consist of average monthly weekday hourly load for the aggregate KCP&L system.

Figure 2-31: KCP&L Summer Monthly Average System Load



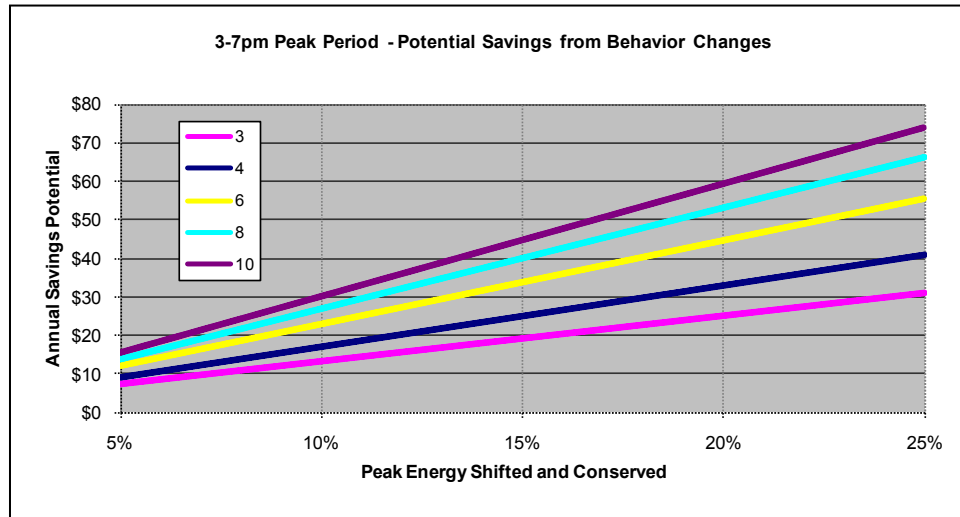
The second step was to investigate historical average residential load profiles. Figure 2-32 summarizes typical summer residential load profiles for customers in and around the project area. Peak residential loads occur later in the day, centered on the 5:00-7:00 pm hours. As a result from assessing both system and residential load profiles, the project team settled on a four hour peak period from 3:00-7:00 pm.

Figure 2-32: KCP&L Summer Average Residential Load



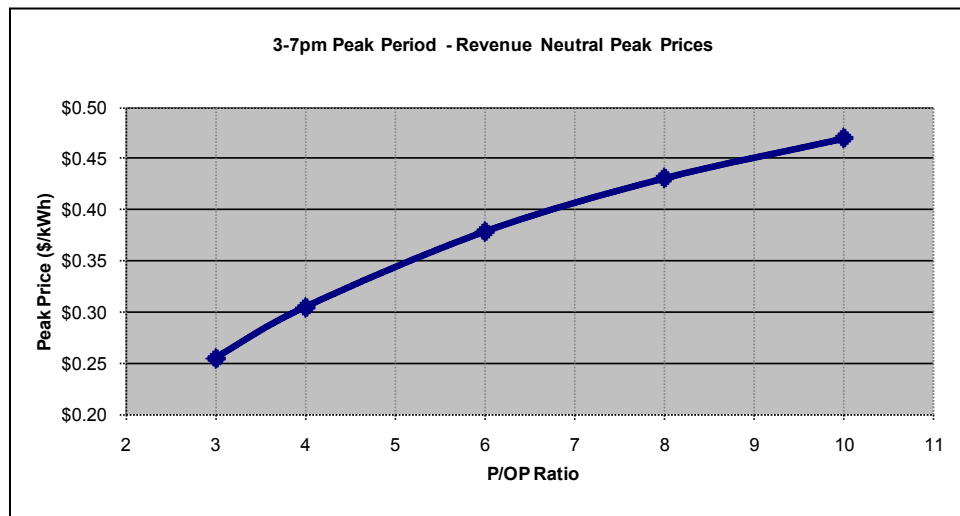
Next, the project team evaluated numerous revenue neutral price options within the determined rate structure to investigate price risk versus customer savings potential. Figure 2-33 summarizes the potential customer savings associated with the amount of peak energy shifted for five targeted peak-to-off-peak price ratios (3x, 4x, 6x, 8x, and 10x).

Figure 2-33: Customer Savings Potential in Various Revenue Neutral Price Options



While price ratios of 8x and 10x offer the most savings potential to customers, Figure 2-34 shows they require aggressive peak prices of over \$0.40/kWh in order to maintain revenue neutrality in this rate structure. Therefore, the project team settled on a 6x price ratio which still offers an unprecedented regional rate option expected to provide valuable customer response learning.

Figure 2-34: Peak Price in Various Revenue Neutral Price Options



A revenue neutral TOU rate with 6x price ratio and four hour peak period from 3:00-7:00 pm resulted in peak price of \$0.3784/kWh and off-peak price of \$0.0631/kWh which represents a significant discount relative to the typical standard rate price of approximately \$0.12/kWh from which participating customers would be switching. Additionally, an off-peak period of twenty hours offers significant flexibility and energy shifting potential to maximize this discounted off-peak price. A summary of these rate details is shown in Table 2-10.

Table 2-10: Pilot TOU Rate Details

Peak Period:	3:00 – 7:00 pm
Peak/Off-Peak Price Ratio:	6x
Summer Peak Price:	\$0.3784/kWh
Summer Off-Peak Price:	\$0.0631/kWh
Winter Rates:	Declining Block
Summer Dates:	May 16 – Sept 15
Customer Charge:	\$9.00/mo.

Along with the rate structure and pricing described above, the following business rules were determined by KCP&L and the project team:

- Voluntary TOU rates only affect summer pricing. During winter, customers revert back to standard winter rates equivalent to standard flat rate
- TOU rate is available to both standard and all-electric customers
- Customers with dual meters are not eligible
- The TOU rate will expire at the end of the Demonstration Project, December 31, 2014
- Customers may sign-up anytime throughout the year; however, the rates will not be affected until the first day of their next billing cycle
- Customers may exit the program at any time; however, they cannot re-join at a later time
- Upon request, KCP&L will credit customers for losses incurred by the pilot TOU rate relative to standard rate treatment for the current and previous billing cycles only

2.2.2.5.1.2 AMI Capture of Meter Read Interval Data

A foundational element of KCP&L's TOU program is the ability of the Landis+Gyr AMI meters to collect and transmit 15-minute interval data that includes date and timestamp information. On a typical day, the meter will capture 96 15-minute intervals with the initial interval running from 12:00:01AM – 12:15:00AM and the final daily interval running from 11:45:01PM – 12:00:00AM. These intervals are transmitted on a regular basis to downstream systems, including the MDM, for further processing. The AMI meters are all set up generically to collect this 15-minute interval data along with the regular daily register read value; a custom metrology solution was not required for TOU due to KCP&L's leveraging of the capabilities of the MDM and SmartGrid Middleware as outlined below.

2.2.2.5.1.3 MDM Usage of Meter Read Interval Data

The 15-minute interval data collected by the AMI system is stored in the eMeter EnergyIP MDM hosted by Siemens. The MDM provides two major capabilities that are critical for TOU: usage framing and billing determinant generation.

Usage framing sums up a customer's interval data over a specified period of time into a total usage amount for that period and stores it in the appropriate "bin". During the Summer Season, on non-holiday weekdays, the MDM sums all 16 of a customer's 15-minute interval values between 3PM-7PM to create a "peak" usage bin and the remaining 80 daily interval values between 12AM-3PM and 7PM-12AM to provide an "off-peak" usage bin. For weekends and holidays, all 96 daily intervals are added to the "off-peak" total. During the winter, all usage is added to the "off-peak" bin.

KCP&L also uses the MDM to deliver billing determinant information to the CIS using a modified version of the MDM's "Pull Billing" method where the CIS makes the request for data to the MDM and receives the necessary response back. Framed usage is retrieved on a daily basis via an "off-cycle", "informational" request to the MDM Pull Billing interface and is returned in "peak" and "off-peak" bin values.

2.2.2.5.1.4 KCP&L SmartGrid Middleware (incl. TOU Register Read Calculator)

KCP&L's legacy CIS currently receives register read values from a variety of metering systems including both AMR and AMI to bill customers. To support integration of these multiple systems, KCP&L has deployed a custom, in-house middleware solution that collects and stores daily register read values from all meters across the territory and normalizes the data to feed to CIS. For integration of the SmartGrid AMI meters, KCP&L added a SmartGrid specific component to the middleware which in turn required an additional enhancement to support TOU billing: the TOU Register Read Calculator.

The TOU Register Read Calculator translates the daily peak and off-peak usage values retrieved from the MDM into a daily dial read, effectively creating a virtual dial for each of the TOU bins: summer on-peak, summer off-peak and winter off-peak. These register read values are then fed into the CIS following the normal meter billing process when needed for monthly bill cycle processing. In addition to the translation from usage values to register values, the calculator provides some additional important capabilities. It provides error tracking and reporting capabilities for use by the IT team and AMI Analyst. It converts AMI- and MDM-provided decimal values to integer values for the CIS; the AMI and MDM systems provide values with up to four decimal places – i.e. 12345.1234. It also supports the accounting requirement that the sum of the TOU kWh bin values match the billed kWh value; this true-up capability is critical due to the decimal-to-integer translation necessary as well as any decimal/integer gap that may occur on a customer's initial enrollment.

2.2.2.5.1.5 CIS/Billing Updates

Additional CIS coding was not required to support TOU billing. Existing system capabilities were leveraged to enable the setup of the virtual register dials noted above in the CIS for billing without requiring a physical meter exchange. During the enrollment process, the meter is temporarily deactivated from the customer account during which time it has the three TOU measuring components for summer peak (SKP), summer off-peak (SKO) and winter off-peak (WKH) added and activated on the customer's meter. Once these measuring components are added, the meter is reactivated on the customer account and once the customer is moved to the 1TOUA/1TOAA rate, including an initial install read, they are then active on the TOU Billing Pilot Program.

2.2.2.5.1.6 TOU Tendril

To aid customers in more effectively participating in the TOU program, various cues are provided to participants who are users of the HEMP and/or KCP&L provided IHDs. Upon enrollment, KCP&L pushes a rate change via the existing MQ interface to the Tendril back-office system that supports the HEMP which causes the Portal to display their 1TOUA/1TOAA rate instead of the previous 1RS1A/1RS6A rate. It also changes the pricing information in the Portal to reflect the TOU prices (outlined in the Tariff section above). The rate change on the customer record also triggers the Portal to display the appropriate TOU pricing based on the season and time of day.

A similar solution was implemented to ensure that the correct pricing amount was pushed out to the AMI meters for display on the IHD. The existing TTM (Tunnel Text Message) interface that pushes customer pricing details out to the meters was updated to send the TOU Summer Peak pricing as a "pricing event" to the meter so that the peak rate will display on the IHD from 3PM-7PM and then revert back to the off-peak price once the TOU period ends each day.

2.2.2.5.1.7 Customer Printed Bill

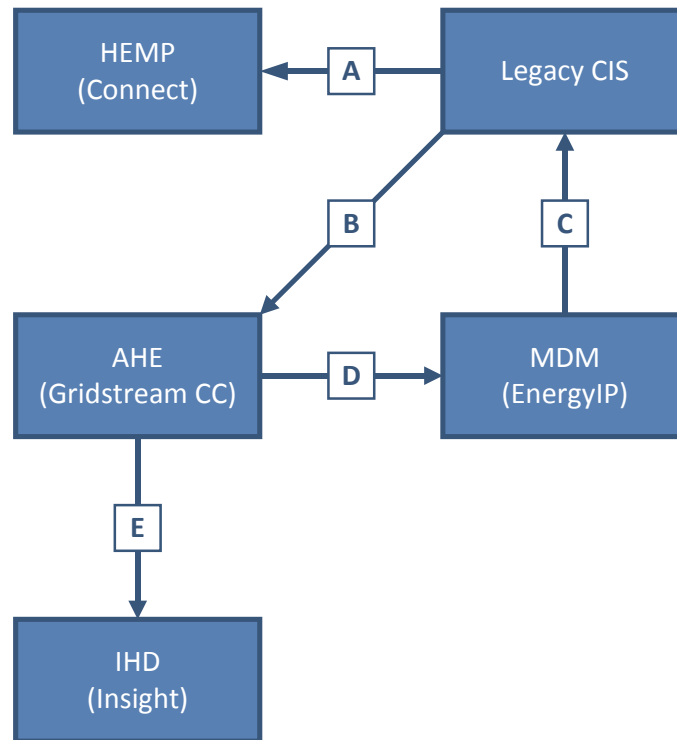
The final visual cue provided to the customer is the billing detail received on their monthly printed (or PDF) bill. At the present time, this is being added manually by the Billing Services team through use of Adobe Writer to edit each monthly customer bill and to add the three lines displaying their register dial

values and usage totals for each of the three TOU bins. This is expected to be automated as part of KCP&L's upcoming OneBillPrint Project.

2.2.2.5.2 *Integration*

An overview of TOU system-to-system interfaces and applicable messages is illustrated in Figure 2-35.

Figure 2-35: KCP&L SmartGrid Demonstration Project TOU Integration



The integration touch points for the TOU implementation are as follows:

- A. 'Consumption Pricing' messages containing 1TOUA/1TOAA rate information pulled from CIS and sent to HEMP via a REST call executed by MQ Broker. These messages are sent once a customer enrolls in the TOU program to update the customer portal with real-time per-kWh consumption pricing information.
- B. 'Consumption Event Pricing' messages initiated from CIS to AHE. These "event pricing" commands are sent daily to update per-kWh consumption pricing information on customer IHDs during the TOU peak hours.
- C. 'Billing Determinant' data initiated from MDM to CIS. This data is requested daily by CIS using MDM's "Pull Billing" interface and is used to update CIS with proper billing determinant information for TOU customers including summer on-peak, summer off-peak, and winter off-peak consumption data.
- D. 'Daily Register and Interval Read' data initiated from AHE to MDM. This is California Metering Exchange Protocol (CMEP)-formatted data sent hourly to be stored in the meter usage data repository and used for TOU billing determinants.
- E. 'Consumption Event Pricing' messages containing 1TOUA/1TOAA rate information initiated from AHE to IHDs. These messages are ZigBee Smart Energy Profile (SEP) 1.0-formatted "event pricing" messages sent daily to the IHD via the AMI network through the SmartMeter using the ZigBee SEP 1.0 "publish price" command to update customer IHDs with real-time per-kWh consumption pricing information during the TOU peak hours.

2.2.2.5.3 Post-Implementation Operational Issues

Following the initial integration, testing and deployment of the TOU program, numerous post-implementation operational issues needed to be considered and mitigated. These issues included the following:

- A special, daily “event” pricing had to be set up to create a pricing event from 3-7 PM on the IHDs to display the correct price during TOU peak hours. This was needed because KCP&L chose not to use the TOU-specific registers within the SmartMeter because this would have required special programming for each individual TOU customer meter. The “event” pricing required a special pricing signal to be sent to the SmartMeters during overnight hours, so that all SmartMeters would be ready to push the pricing event to their IHDs during peak hours.
- The FlexSync interface from CIS+ to MDM has frequent errors in synchronizing customers; this sometimes impacts TOU enrollments by not updating the MDM in a timely manner to trigger the TOU usage framing; this also has caused delays in meter exchanges for TOU customers being processed properly which leads to gaps in usage; it’s expected that with a new MDM/new CIS+ platform that are more tightly integrated this will be less of an issue.
- The custom Pull Billing interface that was written to support our legacy CIS+ system experiences request failures that require constant monitoring and frequent manual submission of the requests to correct errors in the TOU usage being presented to CIS+; it’s expected that with a new MDM / new CIS+ platform that are more tightly integrated this will be less of an issue.
- There have been several instances where meters have stopped reporting intervals or all reads; this has sometimes taken 1-2 months to correct in the field which then results in significant manual effort to recreate/estimate the missing TOU reads and feed them through the MDM and TOU Calculator processes.

To be updated in future releases of this report.

2.2.2.5.4 Lessons Learned

Throughout the build, implementation, and daily operation of the TOU program, numerous considerations were realized and should be noted for future implementations. These Lessons Learned are as follows:

- An additional enhancement was required within the SmartGrid middleware interface to CIS to support TOU billing. This TOU Register Read Calculator was required to convert usage data into register reads and feed the TOU data into CIS in a tolerable format for billing purposes.
- Overall, enrollment in the TOU program was higher than anticipated. TOU enrollment exceeded enrollment for both the Standalone PCT and HAN programs. As of October 2013, TOU enrollment was 131 customers.
- Legacy CIS+ system was less capable in supporting a billing program such as TOU that required customized inputs; the ability to provide this capability “out of the box” is being noted as a requirement and business case benefit for KCP&L’s upcoming CIS+ replacement.
- Tight integration between the MDM and CIS systems was identified as a key business requirement for the selection of a new enterprise MDM platform as KCP&L expects to use the new MDM to support billing of ALL customers and not just the TOU customers; this was driven in part by our experience with the SmartGrid TOU program.

To be updated in future releases of this report

2.2.3 SmartSubstation

The SmartSubstation sub-project deployed a state-of-the art distribution SmartSubstation with an IEC 61850 substation protection network, a distribution data concentrator, human machine interface, GOOSE messaging, and distributed control and data acquisition components.

These various components were initially planned for simultaneous deployment. However, as the project progressed and KCP&L further assimilated the scope and complexity of this overall project, questions arose regarding the feasibility of the original intent to conduct one comprehensive configuration and test effort for all SmartSubstation functions. An analysis was performed to better understand the critical interdependencies between systems to ensure successful testing and deployment. The result of this analysis showed that complexity in the related systems would benefit from increased focus on narrower definitions of scope. To this end, and as pursued with each component system below, it was decided to break the configuration and deployment of the overall SmartSubstation into four phases. Each of the phases of work would include configuration and testing as applicable to the given system.

- **Phase 1 – Substation Device Monitoring:** All substation devices to be automated through the project (breakers, differentials, tap changers, etc.) were configured and installed at KCP&L's Midtown Substation as part of the Substation Protection Network. In parallel, preliminary efforts were conducted to deploy the Distribution Data Concentrator (SICAM) to establish preliminary communications for remote monitoring of substation device point changes. Point-to-point monitoring-only checkouts were conducted on all points for all substation devices to ensure proper communications from the devices.
- **Phase 2 – Substation Device Control:** End-state networking and configurations for the Substation Protection Network were deployed and stabilized. Point-to-point monitor and control checkouts were conducted on all points for all substation devices to ensure proper communications to / from the devices through to the Distribution Data Concentrator (SICAM). Human Machine Interface (HMI) capabilities were configured, tested, and deployed to the substation control house.
- **Phase 3 – Substation DCADA:** Activities highly synchronized with SmartDistribution, once the advanced application algorithms were proven out via centralized 1st Responder test efforts in the DMS, the algorithms were ported to the DCADA for autonomous substation control. Further controlled tests were performed to gain confidence in the system and establish initial configurations for automatic operation (particularly with VVC).
- **Phase 4 – Substation GOOSE Messaging:** Initial configuration efforts for GOOSE were pursued throughout earlier phases, but deployment and real-world testing of the protection schemes were pursued independently upon a stabilized base of previously deployed capabilities.

Another key takeaway from the initial implementation analysis was the need to establish and maintain several integrated environments to ensure that functionality was safely segregated for forthcoming development and testing efforts. Due to the complexity of integrating systems within each of these environments, the effort to set these up was commenced early to ensure their readiness as needed.

- **VENDOR Environment:** The first and most basic environment was the VENDOR environment. The UI/CAD, D-SCADA, and SICAM DDC applications were installed on KCP&L owned servers that were sent to the Siemens facility for initial configuration. In addition, sample substation controllers were also provided for vendor use. All hardware was extensively used to establish initial configurations and ensure they were working under controlled conditions.
- **LAB Environment:** The second and more complex environment was the LAB environment. It was initially setup to augment the VENDOR environment, as sample field devices were setup and connected to a LAB dedicated network which was interfaced with the servers of

the VENDOR environment for preliminary tests. Later in the project lifecycle, the sample substation devices were transferred back to KCP&L's facility and additional KCP&L procured servers were then setup in the LAB to establish a standalone environment; the connection to the VENDOR environment was severed. By that point, the LAB also had integration with numerous other systems to more robustly mimic DEMO and was used to test out preliminary integration configurations.

- **DEMO Environment:** The final and most complex environment was the DEMO environment. This was KCPL's real-world environment where the systems were supported by redundant servers, configured for full integration with other systems, and connected to all of KCPL's Smart Grid devices deployed to the substation and certain highly automated distribution feeders. Redundant HMI, DCADA, and SICAM DDC servers were deployed in the Midtown substation Battery Control Enclosure for this environment. As these devices result in real-time, real-world distribution network changes, special care was taken to ensure that no negative consequences resulted from our efforts when testing in the DEMO environment.

The following subsections summarize these SmartSubstation component deployments.

2.2.3.1 Substation Protection Network

The Midtown Substation Protection Network is an Ethernet-based substation control network utilizing the IEC 61850 network architecture. Because substation protection and control networks are deployed in harsh environments and transport critical data, the network was designed to have high availability and low latency, providing fast, reliable communication between networked devices. Additionally, the networking equipment is environmentally hardened, as it is expected to operate across extreme humidity and temperature ranges.

2.2.3.1.1 Build

The high level network architecture was shown in Figure 1-21, Midtown Substation Protection and Control Network Architecture. In general, the IEC 61850 network consists of redundant 1 Gbps Ethernet backbones routed throughout the substation. These backbones interconnect remote primary and backup Ethernet switches installed in various switchgear enclosures to main Ethernet switches located in the main control enclosure. Protective relays, equipped with redundant Ethernet ports, connect to the appropriate primary and backup remote switches using 100 Mbps Ethernet. The following sections provide a summary of the tasks performed to implement and deploy the substation protection network.

2.2.3.1.1.1 **Network Design**

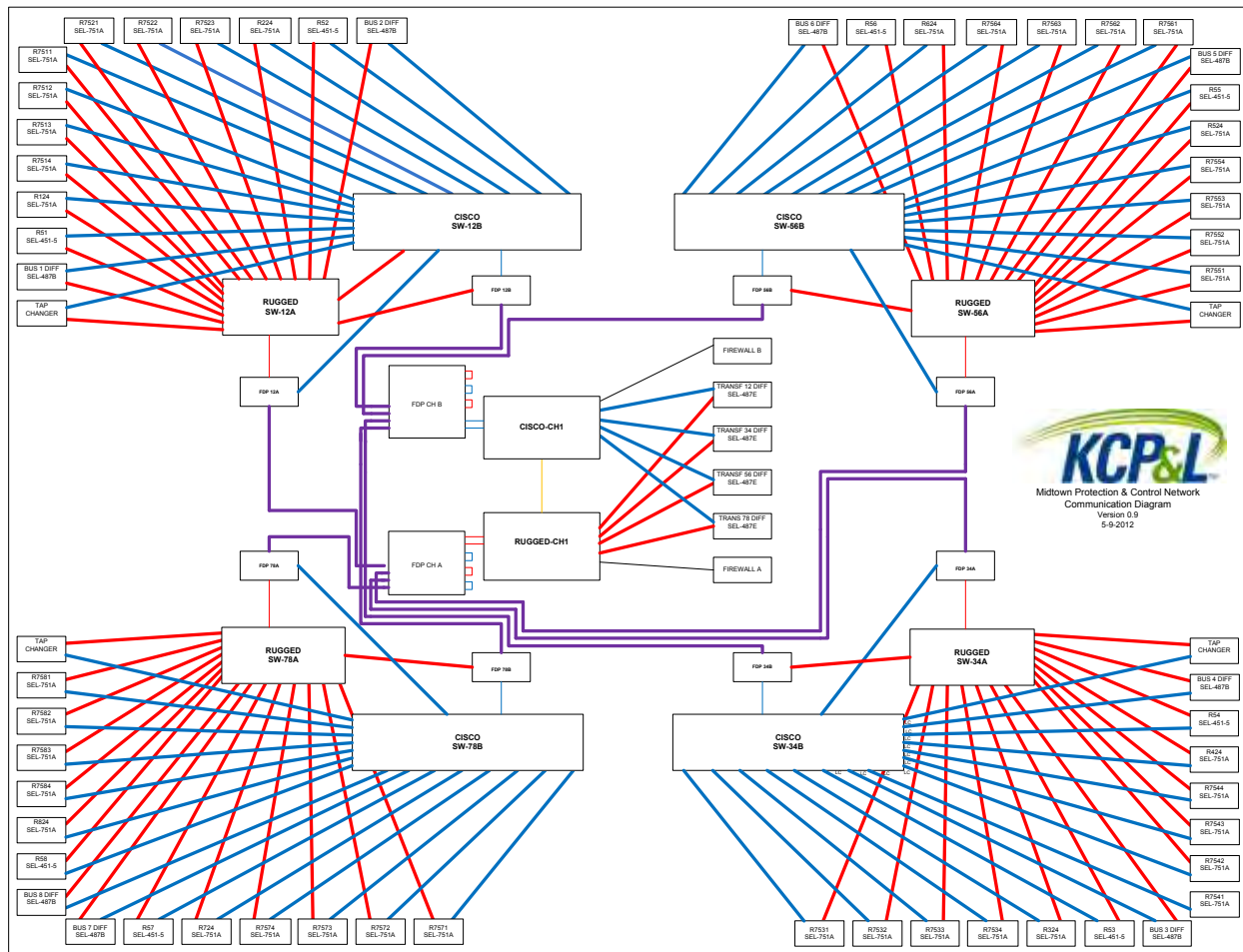
The IEC 61850 network was designed as a redundant Ethernet ring architecture. Ring architectures allow for self-healing networks, increasing availability and reliability. The Ethernet switches comprising the network are arranged in rings, providing redundant pathways between two points in the network via the Ethernet backbone. This configuration protects against loss of communication between devices due to failure of a communication link or loss of an intermediate switch. Loss of communication only occurs when there is a failure in the edge switch to which one of the two communicating devices is connected. To further increase reliability, redundant rings were deployed. This allows devices with redundant Ethernet interfaces to take advantage of a standby Ethernet network, reducing the probability of a loss of station control due to failure of any single piece of network equipment. This redundant ring configuration eliminates single points of failure for all Ethernet hardware when the communication devices are configured in fail-over mode. Figure 2-36 provides an overview of the substation protection and control network that was implemented. The complete IEC 61850 Communications Network design document is included in this report as Appendix D.

2.2.3.1.1.2 Lab Testing

Ethernet switch testing was conducted in a lab environment to verify the configuration and performance of a multi-vendor, IEC 61850 LAN. Cisco CGS 2520 and RuggedCom 2100 Ethernet switches were selected by KCP&L for the Midtown Substation 61850 LAN trial. This section provides a summary of the network lab testing that was performed. The complete IEC Switch Test Results document is included in this report as Appendix E.

The topology KCP&L selected for the Midtown Substation 61850 LAN trial was tested in three parts: the Cisco ring, the RuggedCom ring, and the combined rings. There were two types of tests run on the network to determine network convergence following two types of failures that can occur on an Ethernet LAN: port failures and link failures.

Figure 2-36: SmartSubstation Protection and Control Infrastructure



The primary purpose of the inter-vendor testing was to determine the performance of using the proprietary Layer 2 loop-reduction protocols offered by each vendor. In addition to the industry-standard IEEE 802.1w, Rapid Spanning Tree Protocol (RSTP), each vendor offers a proprietary algorithm with faster than RSTP performance. Cisco offers Resilient Ethernet Protocol (REP), which is designed to interoperate with RSTP. RuggedCom offers Enhanced Rapid Spanning Tree Protocol (eRSTP), which is designed as an extension of RSTP and offers backwards compatibility with RSTP.

Throughout the testing, intra-vendor performance was mostly consistent with each of the vendors. There was a reproducible anomaly with specific failure scenarios with REP in the Cisco ring. Other

convergence times in the Cisco ring were in the sub 50 ms range. Cisco RSTP convergence was very consistent with repair times, but the convergence times were never under 50 ms, and typically more than 100 ms. Additionally there was difficulty configuring REP to interoperate with RSTP in an intra-vendor setup, so there was no testing conducted in an inter-vendor configuration.

Cisco showed consistently better times when failing a single relay port by approximately 120 ms on average with an SEL-451. There were no other relays available for comparison so this could be an issue with the SEL-451 specifically.

The RuggedCom implementation of eRSTP is very consistent with convergence and repair times and was across every test that was run on the RuggedCom and combined rings. Both convergence and repair times on each test were within 1 ms of every other respective convergence and repair time for each configuration.

VLAN configuration had to be adapted, and an extra VLAN was added to accommodate the way Cisco handles tagged traffic going into a trunk port with a native VLAN. Although the workaround poses no operational issues, the difference in the way each manufacturer handles both tagged and untagged packets on a trunk port caused some issues during the initial configuration.

2.2.3.1.1.3 IED Replacement

KCP&L began replacing the Midtown IEDs in February 2011. The devices were replaced in a systematic manner, one switchgear or transformer at a time. Devices associated with five switchgear were replaced in 2011, three switchgear were replaced in 2012, and all four transformers were replaced in 2012. Sixty three total IEDs were installed in the Midtown Substation, as described in Table 2-11.

Table 2-11: Substation IEDs Installed

IED	Model	Monitor/Control	Quantity
Bus Main Breakers	SEL-451-5	Monitor Only	8
Tie Breakers	SEL-751A	Monitor Only	8
Transformer Differential Relays	SEL-487E	Monitor Only	4
Bus Differential Relays	SEL-487B	Monitor Only	8
Feeder Breakers*	SEL-751A	Monitor Only	20
Feeder Breakers*	SEL-751A	Control	11
Load Tap Changers	Eberle REG-DA	Control	4
*11 of the 31 circuits in Midtown Substation feed the Green Impact Zone, or the project area. The feeder breakers for these circuits have monitor and control capabilities, whereas the non-smart grid feeders can only be monitored.			

The point of demarcation between KCP&L's existing transmission EMS and the demonstration project DMS is the substation feeder breaker. Both systems have monitor and control capabilities of these devices. The feeder breakers will continue to send data to the existing Midtown RTU, but the 11 smart grid feeder breakers will also send information to the new substation data concentrator, the SICAM. In order to avoid having controls come from both the EMS and the DMS, a control authority selector has been added to the EMS so that the distribution operators can toggle control between the two systems.

Although the Midtown substation devices have the necessary IEC 61850 Configured IED Description (CID) files loaded, the IEC 61850 GOOSE messaging hasn't been activated as of yet. Currently, the devices are communicating via 61850 MMS messaging to the SICAM, but they won't perform the peer-to-peer GOOSE communications until a multi-bus test can be conducted.

2.2.3.1.1.4 Fiber Installation

The fiber installation occurred during April and May of 2012. The Midtown Substation physical infrastructure is laid out in a star configuration with one cable trench for each bay in the ring bus. These trenches extend from the control enclosure, which is in the center of the substation, out to each switchgear enclosure. Two twelve-fiber, single-mode fiber optic cables were installed between each switchgear enclosure and the main control enclosure. Fiber distribution panels (FDPs) were installed in each switch location, as well as within the control enclosure. At Midtown Substation, it was impractical to install new conduit directly between each switchgear enclosure to create a truly physical ring, so the Ethernet switches were connected in a ring by patching in the FDPs located in the control enclosure. These new fiber optic cables were installed in the existing cable trench with other control cable.

2.2.3.1.1.5 Switch Installation

The network switches were also installed in April-May 2012. As part of the pilot, the Midtown Substation was retrofitted with a redundant Ethernet communications network with hardware from two switch vendors (RuggedCom and Cisco) for protection operation. Using two vendors allowed KCP&L to evaluate the products simultaneously to determine which was best suited for substation protection and control networks. Each vendor's equipment was used to build a ring in the substation, and each relay has an interface connected to both rings. The rings are interconnected at two points for redundancy. The core ring was built using gigabit fiber connections. The relays each have two 100-Mbps Ethernet interfaces used in a hot standby configuration. Each vendor has its own proprietary protocol for blocking loops from forming in the Ethernet network while recovering from a link failure in less than 50 msec. In between the rings, rapid spanning tree protocol was used to provide failover in less than 250 msec.

2.2.3.1.1.6 Production Testing

After the network was physically installed, the Network Services team conducted testing on the production network. The testing occurred in October, 2012, and it included the following tests:

- Verify Baseline Control House L2 Traffic Flow
- Verify Baseline Battery Control House L2 Traffic Flow
- Verify Baseline Cisco Switch House L2 Traffic Flow
- Verify Baseline RuggedCom Switch House L2 Traffic Flow
- RuggedCom eRSTP Devices interact with Cisco MST Devices via RSTP
- Control House Link Failure 1
- Control House Link Failure 2
- Battery Control House Link Failure
- Cisco Switch House Link Failure 1
- Cisco Switch House Link Failure 2
- RuggedCom Switch House Link Failure 1
- RuggedCom Switch House Link Failure 2
- RuggedCom Switch House Link Failure 3

All test cases passed, and upon completion, the substation protection network was put into service.

2.2.3.1.2 Post-Implementation Operational Issues

For the most part, the substation protection network has functioned smoothly thus far. We have only encountered two post-implementation operational issues with this portion of the project.

2.2.3.1.2.1 RuggedCom Switch Replacement

Although the RuggedCom and Cisco rings were functioning sufficiently, the KCP&L team decided to move forward with a RuggedCom replacement. From the outset of the SPN design, one of the major

reasons for using two vendors for the initial implementation was so that KCP&L could evaluate multiple manufacturers. After a year of operation using this mixed-vendor network, KCP&L's Network Services group recommended a change to the production network. They suggested replacing the RuggedCom switches with Cisco switches for the following reasons:

- **No “accounting” function on RuggedCom switches:** There is a networking standard called AAA which stands for Authentication, Authorization, and Accounting. The RuggedCom switches can perform the Authentication and Authorization pieces of AAA, but not the Accounting function. The Cisco switches can perform all three functions of AAA and are currently passing NERC/CIP audits in the KCP&L production environments. Accounting in the network environment provides logs of any user activities performed on the switch by users that have been authenticated and authorized. These logs provide evidence that is used to fulfill a NERC/CIP requirement.
- **Banners:** Login banners are presented to anyone attempting to connect to the management interfaces of the network devices to notify any potential users that they are responsible for what they do when logging in to a KCP&L device and that unauthorized access is prohibited. KCP&L's current standard is to present a banner prior to login and also after login. The RuggedCom switches do not allow for a login banner to be presented prior to login, but rather only after a user has logged in to the device. This lack of functionality would require an exception to be filed if the substation were to fall under the purview of current NERC/CIP standards.
- **Workflow and Procedures:** Since the protection hardware is located in the switchgear buildings at the substation, the Network Services team cannot install or replace the physical switch hardware. This process can be straight forward and simple with the Cisco hardware, but the RuggedCom hardware requires a more highly coordinated effort between Network Services and the KCP&L relay technicians.
 - **Cisco:** Spare hardware can consist of one switch, many SFPs (small form-factor pluggable), and many memory cards. The memory cards can be labeled to match the names of the switches. When a switch replacement is required, the relay technician simply inserts the appropriate memory card into the spare switch that contains the proper configuration for the switch that is being replaced. The process is simple enough that the relay technicians won't need direct assistance from the Network Services team. The Cisco switches also use SFPs (port adapters) to generate the optical signals for each independent connection to the IEDs. The independent, field replaceable units can be replaced without swapping out the entire switch. Additionally, the SFPs are hot swappable and can be replaced without powering down the switch.
 - **RuggedCom:** Spare hardware would consist of spare switches stored at Network Services' location, so that Network Services has physical access to them for initial configuration. The spare switch would require configuration by the Network Services team through the use of TFTP (trivial file transfer protocol), and the configuration would vary depending on which switch needs to be replaced. Then, the switch would be delivered to the relay technician for installation. In the event of a single access port failure, the complete switch would need to be replaced.
 - **Reliability:** Running two switch vendors in the same substation environment presents concerns about multiple protocols being used in a single implementation. When both vendors are used, Reliable Ethernet Protocol (REP), Enhanced Rapid Spanning Tree (eRSTP), and Rapid Per VLAN Spanning Tree (RPVST) protocols are all utilized. When the entire network utilizes Cisco equipment, then only REP is used.

2.2.3.1.2.2 Compromised Fibers:

The other post-operational issue pertaining to the substation protection network has been a few compromised fibers. In 2013, a fiber connected to tap changer 5/6 failed and the communications didn't switch over to the other ring. This was a fortunate issue, as KCP&L didn't realize that the tap changers weren't properly set up to have redundancy. After resolving the issue with the fiber, KCP&L also worked to configure the tap changers to function in a redundant mode.

During HMI retesting in November 2013, the fiber between switches SW-34A and SW-56A was deemed problematic. KCP&L is currently in the process of investigating this issue in order to determine the proper resolution.

2.2.3.1.3 Lessons Learned

Throughout the build, implementation, and daily operation of the SPN, numerous considerations were realized and should be noted for future implementations. These Lessons Learned are as follows:

- **Pros and Cons of Multi-Vendor SPN** – KCP&L learned a lot on this portion of the project in regards to a multi-vendor implementation of the redundant network. In general, KCP&L learned that it is feasible to design, construct, and run a multi-vendor substation protection network, but there are certainly drawbacks to this approach. As described in the sections above, the hybrid approach yields uncertainty in regards to functionality and failover time. Testing out the proposed network architecture in a lab environment was critical prior to deployment of the networking equipment in the production environment.
- **Ownership of the SPN** – As KCP&L designed, tested, and built the Midtown Substation SPN, it became obvious that this type of project was outside of any one department's normal set of tasks. The Substation Protection and Relay System Protection groups are very familiar with the IEDs, but they have minimal experience with local area networks. The Network Services personnel are well-versed with the actual network, but they typically have minimal experience with the IEDs, and they usually don't have access to the substations.

From KCP&L's research and discussions with other utilities, it seems as though this issue is one that many utilities are currently facing. Some utilities are having the Network Services team take ownership of the IEC 61850 network, and some are adding this to the Substation or Relay System Protection team. Meanwhile, other utilities are creating a third, hybrid group that specifically addresses this mix of skill sets. For the demonstration project, KCP&L has chosen to tackle this new domain with a coordinated effort between the Network Services, Substation Protection, and Relay System Protection groups.

To be updated in future releases of this report

2.2.3.2 Distribution Data Concentrator

Siemens' SICAM PAS was deployed as the Distribution Data Concentrator (DDC) or communications gateway for the substation relays and field devices reporting through the Midtown substation.

2.2.3.2.1 Build

The SICAM is one of Siemens commercially available utility products. By pursuing this "off-the-shelf" philosophy to the maximum degree possible, limited design and development efforts are required and the Demonstration Project is provided the opportunity to evaluate the capabilities of existing products and technologies in meeting the emerging Smart Grid requirements. The following sections provide a summary of the development and configurations that were required to implement and deploy the desired DDC functionality.

2.2.3.2.1.1 Training

Training on the SICAM occurred from August 13, 2012 through August 16, 2012. This training was conducted by Siemens and it covered the basics of the system – loading devices, creating templates, mapping points to other interfaces, and basic troubleshooting. Additional training on the SICAM continued through the SICAM go-live and after it became operational.

2.2.3.2.1.2 Hardware Installation

KCP&L chose to implement redundancy for most of the critical systems in this project. The Distribution Data Concentrator is certainly considered a critical piece of hardware, so two SICAMs were rack-mounted in the Battery Control Enclosure, right next to Midtown Substation.

2.2.3.2.1.3 Substation Device Point Configuration

The process of loading the substation devices into the SICAM was a long and detailed endeavor. Once KCP&L chose all of the devices for use in Midtown substation, they determined the data points that were desired for each substation device type. They started with the default maps (what is published by default by each device) and then added some additional data points to their list as desired. A complete listing of data and control points configured for each substation device are contained in Appendix F.

Next, the project team used SEL Architect (the relay vendor's configuration tool) to create the Configured IED Description (CID) files. These files define the logical nodes for each device. These logical nodes are essentially groupings of data points for functional purposes. When a device reports or is polled, if one of these nodes is read, all of the associated data points in that node are also sent back to the concentrator. In addition to the logical nodes, the CID files also have reporting capabilities (frequency, integrity poll, whether or not they're buffered), deadband definitions for analog values, data types, how data formatting. Lastly, the CID files include the IP address of the device.

In terms of naming the points, IEC61850 has format that must be followed, so the points names were basically determined by default once the team determined the data to be sent from the device to the SICAM. The team also used the 61850 names for the ICCP naming, which is discussed further in the DMS UI/CAD and Distribution-SCADA Implementation sections.

Once the CID files for each device were created, the team loaded each one into the SICAM. Upon completion of each CID file load, the SICAM creates a device template. The device templates contain the information necessary to build the communication interface from the device to the SICAM. The SICAM then uses this template to build the device mapping, which contains the information necessary to build the communication interface from the SICAM to the DMS/DCADA/HMI. The team didn't have to select any points for alarming at the SICAM; rather, the SICAM is just a pass through for the alarms to get to I/Dispatcher.

Once the template and mapping is complete, the team selected the data points that they wanted to see on the 61850 client interface. This interface is used to determine what points are shown in the SICAM's Value Viewer, which is essentially the SICAM's GUI. Not all the points that are sent from the device to the SICAM need to be included in this interface – it can be just a subset of the original points transferred. Similarly, the team chose the subset of data points for the 61850 server interface. These points are sent to any upstream systems, such as the DMS, the DCADA, and the HMI.

The screenshot in Figure 2-37 shows some of the information that is brought in when a CID file is loaded on the SICAM for an IEC61850 device.

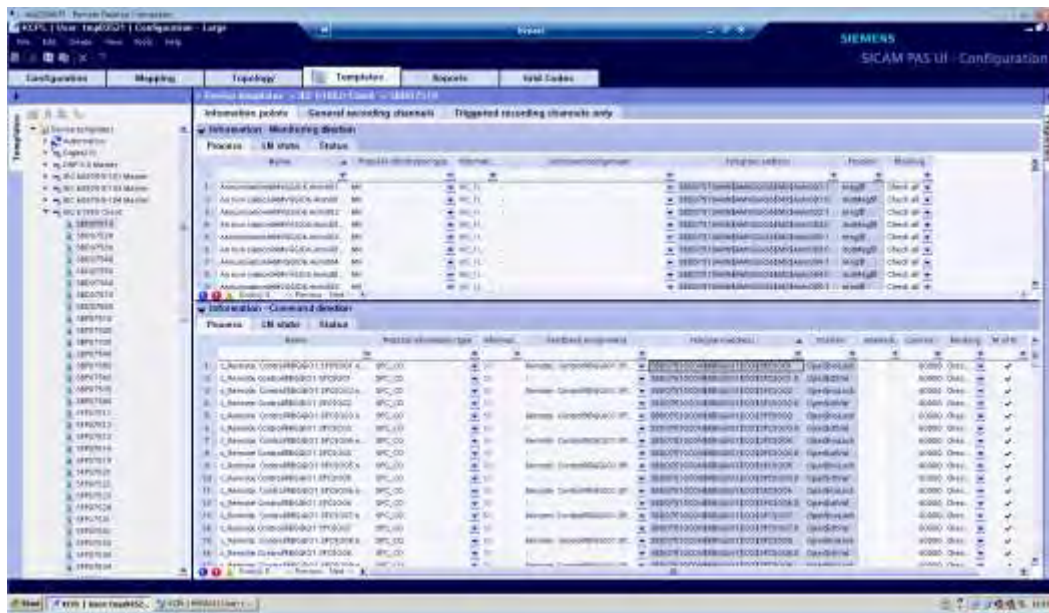
2.2.3.2.1.4 Field Device Point Configuration

The process of loading the field devices into the SICAM differs a bit from the substation devices. For the DNP3 field devices, no file is loaded on the SICAM; rather, the configuration information is all stored within the relay settings file on the device.

Similar to the substation process, the KCP&L team started by determining the desired devices for use in the field network, and then they determined the type of data that they wanted from each device type. The relay group then created the settings files for each device, including the DNP point set list as well as the protection settings. A complete listing of data and control points configured for each field device are contained in Appendix F.

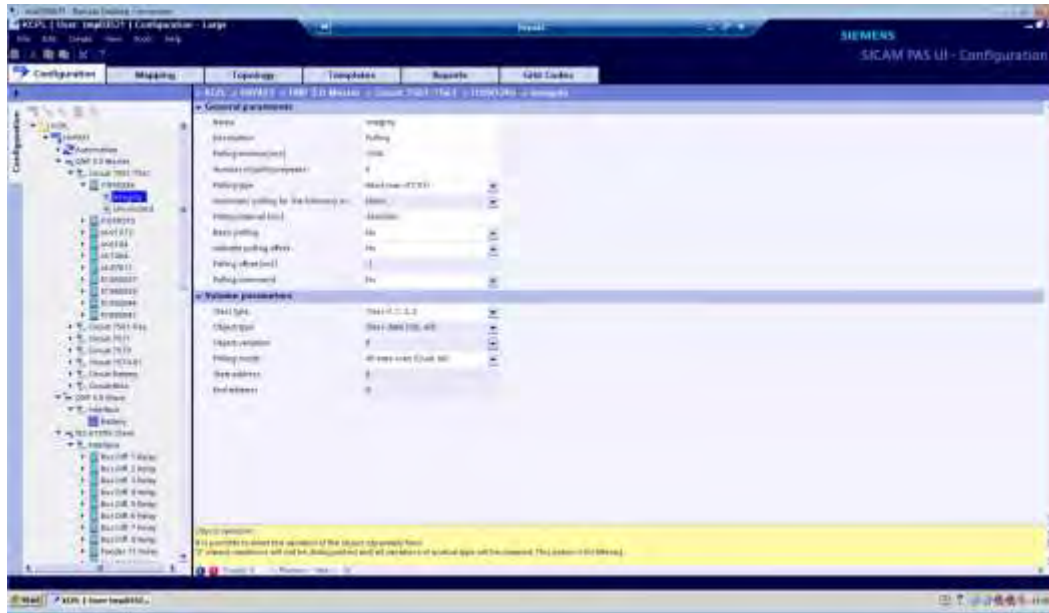
In terms of naming for the DNP3 field devices, the team tried to make the names as 61850-like as possible. Since the long-term goal was to use 61850 for communications to these field devices, the team wanted to make this as easy as possible later on. In some cases, the 61850 names weren't possible, but the team worked to get the names as close as possible. The team used the 61850 names for the ICCP naming, which is discussed further in the DMS UI/CAD and Distribution-SCADA Implementation sections.

Figure 2-37: IEC 61850 Device Template on the SICAM



For the DNP field devices, the project team had to manually build the templates in the SICAM. To do this, they selected a subset of points, and then they matched those points between the settings file on the device and the points selected in the SICAM. DNP addresses and communications settings (IP address and port) need to match for this to function properly. For the mapping step, the SICAM basically uses the template that was created, but then the user has to select the points that are desired for Value Viewer as well as for upstream propagation. For the DNP devices, these interfaces are called DNP Master (these are the points displayed in SICAM Value Viewer) and DNP Slave (these are the points that are sent to upstream systems such as the DMS/DCADA/HMI). The team didn't have to select any points for alarming at the SICAM; rather, the SICAM is just a pass through for the alarms to get to I/Dispatcher.

The screenshot in Figure 2-38 shows some of the configuration that is needed when mapping a DNP3 field device.

Figure 2-38: DNP3 Device Configuration on the SICAM

2.2.3.2.1.5 Demonstration SICAM Implementation

For the Kansas City long-term environment, there were two SICAM implementations – the demonstration system implementation and the development system implementation. To begin the demonstration system implementation, Siemens first created the initial SICAM database through the points lists provided to them by KCP&L. They first programmed the IEC61850 and DNP3 devices to communicate to the SICAM through the IEC61850 Client and DNP3 Slave protocols on the SICAM server. Once the communication from SICAM to device was built, Siemens mapped the signal data to DMS and DCADA through the IEC61850 Server protocol, and to the HMI through its HMI interface.

Once the initial configuration was complete, Siemens invited KCP&L to their regional office in Minneapolis, MN to perform Factory Acceptance Testing (FAT). KCP&L performed FAT testing based on material provided by Siemens as well as additional test material developed by KCP&L. Upon completion of the FAT, KCP&L provided Siemens with a list of variances rated in severity; the more severe needing to be resolved prior to Site Acceptance Testing (SAT). Siemens worked to resolve the critical variances and deploy/test them. Eventually, the servers were shipped from Minneapolis to Kansas City. KCP&L then invited Siemens onsite for SAT testing. KCP&L conducted testing through the materials provided by Siemens, materials created by KCP&L, and any variances that were created in the FAT. Post SAT, Siemens worked to continue resolving variances through “Go-Live”.

2.2.3.2.1.6 Development SICAM Implementation

The implementation of development SICAM was dependent on a working model in the demonstration instance. The database from the demonstration SICAM was migrated on to the development SICAM, so that the development SICAM was an exact copy of the demonstration instance. KCP&L then altered the communication settings within the development SICAM to allow it to communicate over the development network to other development servers and devices. The end result was a working development SICAM that communicated IEC61850, DNP3, and Siemens proprietary protocols data on an isolated Smart Grid environment.

2.2.3.2.1.7 Point-to-Point Checkouts

The substation device point-to-point checkout was conducted by four groups: KCP&L Relay, KCP&L Dispatch, KCP&L Smart Grid, and Siemens. KCP&L's Relay group was on-site to create any binary status events, monitor any analog data, and provide feedback on any device controls. KCP&L's Dispatch was responsible for clearing up any devices that were in service to prevent any consumer outages. KCP&L Smart Grid and Siemens were on-site to verify data was being sent correctly to and from the SICAM server. These groups all worked together to create any binary event, to execute any control, and to monitor all analog changes at substation relays. Point-to-point checkouts were conducted on every device that was deployed in Midtown substation.

The field device point-to-point checkout was conducted by five groups: KCP&L Relay, KCPL Linemen, KCP&L EMS, KCP&L Smart Grid, and Siemens. KCP&L's Relay group was on-site to create any binary status events, monitor any analog data, and provide feedback on any device controls. KCP&L EMS was responsible for clearing up any devices that were in service to prevent any consumer outages. KCP&L Smart Grid and Siemens were on-site to verify data was being sent correctly to and from the SICAM server. These groups all worked together to create any binary event, to execute any control, and to monitor all analog changes at substation relays. Point-to-point checkouts were conducted on several devices of each type, and the controls were tested on every recloser.

2.2.3.2.1.8 Adding Devices to SICAM

In the ideal scenario, all the substation and field devices for a DDC implementation would be known up front, and everything would be added once and then done. This is far from reality, though. For the most part, the substation devices are done once and finalized, but if another IEC61850 device needs to be added, this process is dependent on the device's CID file. The SICAM imports the CID file and then builds the device profile. Device signals will need to be mapped in the IEC61850 Client interface in order to be visible on the SICAM server, in the HMI interface to be visible on the HMI, and in the IEC61850 server to be visible on the DCADA and DMS.

Adding field devices to the SICAM is a much more common task, since field device deployments are rarely done all at once. DNP3 field devices in the SICAM are created through a user build process. This process starts by building a predefined template that will assign points to the SICAM through specific DNP addressing. Then the devices are added to the SICAM, and its communication and reporting parameters are defined. The predefined template is also selected during the device creation. Device signals will need to be mapped in the DNP Slave interface in order to be visible on the SICAM server and in the DNP Master to be visible on the DCADA and DMS.

2.2.3.2.1.9 Adding Points to Device Profiles

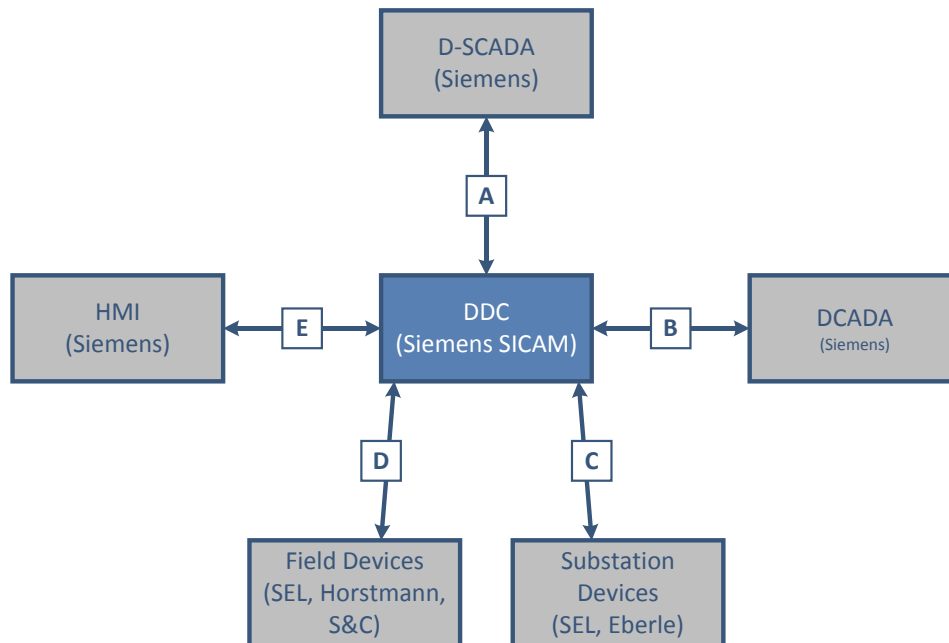
Adding additional points to a substation or field device profile is a bit tedious. Adding points to a substation device requires the creation of a new CID file that includes the additional point. The SICAM then updates the CID process on that specific device. The only further modification is to map the new points to any IEC61850 Client, IEC61850 Server, or HMI interface for visibility on the SICAM, DMS, DCADA, or HMI.

Adding field device points is a very involved process on the SICAM. This process requires building a new predefined template that adds the new point, while being careful not to eliminate any existing signals. The SICAM is incapable of having devices merely switch templates; rather, the addition of any new point requires the deletion of the device and re-adding of the device to implement the new profile. These points will need to be remapped on the DNP Slave and Master to guarantee visibility on the SICAM, DCADA, and DMS servers.

2.2.3.2.2 *Integration*

An overview of DDC system-to-system interfaces and applicable messages is illustrated in Figure 2-39.

Figure 2-39: KCP&L SmartGrid Demonstration Project DDC Integration



The integration touch points for the DDC are as follows:

- A. DDC/D-SCADA Monitor and Control Propagation: A bi-directional interface allowing for substation and field device point monitoring details to be provided by the DDC to D-SCADA so that it has all updated information for use by the DMS. The interface also allows for any controls resulting from DMS functionality to be transmitted to DDC for further propagation to devices in the substation or the field. All data exchanges in this interface are transmitted via IEC 61850.
- B. DDC/DCADA Monitor and Control Propagation: A bi-directional interface allowing for substation and field device point monitoring details to be provided by the DDC to DCADA so that it has all updated information for use by the substation controller. The interface also allows for any controls resulting from closed loop DCADA functionality to be transmitted to the DDC for further propagation to devices in the substation or the field. All data exchanges in this interface are transmitted via IEC 61850.
- C. DDC/Substation Devices Monitor and Control Propagation: A bi-directional interface allowing for substation device point monitoring details to be provided by the substation device (bus main breakers, tie breakers, transformer differential relays, bus differential relays, feeder breakers, or load tap changers) to the DDC so that it has all updated substation information for use by the DDC and other upstream systems. This communication occurs in real time as device status changes, and it also occurs on regular intervals via predefined integrity polls initiated by the DDC. The interface also allows for any controls resulting from DDC functionality to be transmitted to the substation device. All data exchanges in this interface are transmitted via IEC 61850.
- D. DDC/Field Devices Monitor and Control Propagation: A bi-directional interface allowing for field device point monitoring details to be provided by the field device (capacitor bank, fault current indicator, recloser, or battery) to the DDC so that it has all updated field

device information for use by the DDC and other upstream systems. This communication occurs in real time as device status changes, and it also occurs on regular intervals via predefined integrity polls initiated by the DDC. The interface also allows for any controls resulting from DDC functionality to be transmitted to the field device. All data exchanges in this interface are transmitted via the Tropos network using DNP3.0.

- E. DDC/HMI Monitor and Control Propagation: A bi-directional interface allowing for substation device point monitoring details to be provided by the DDC to the HMI so that it has all updated substation information for use by the HMI GUI. The interface also allows for any controls resulting from HMI functionality to be transmitted to the DDC for further propagation to devices in the substation. All data exchanges in this interface are transmitted via a proprietary Siemens protocol.

2.2.3.2.3 Post-Implementation Operational Issues

Following the initial implementation, testing and deployment of the DDC, numerous post-implementation operational issues arose that needed to be considered and mitigated. These issues included the following:

- **Deadbands** – One of the first issues that arose had to do with device deadbands. Rather than polling the substation and field devices periodically for updates, KCP&L wanted the devices to report by exception. Report-by-exception could potentially limit the amount of unnecessary data that flows into the SICAM, as data is only sent when an event occurs. For the binary and counter values, this is simple – the devices just report to the SICAM any time a status changes. For the analog values, however, the reporting frequency isn't as straight forward. The substation and field device analog values fluctuate in real time, but the SICAM doesn't need to be notified of every miniscule change. If every change was sent upstream, then the devices would be constantly transmitting updates. Instead, each device is configured with deadbands for all of the analog points. For the 61850 devices, when one analog reached a deadband, the device would send all the data points within that 61850 report. With KCP&L's initial deadbands, the devices were sending 61850 reports many times each second, and the SICAM processor became overloaded. After some analysis, the project team assigned new, wider deadbands to the analogs. For the substation devices, this required updated CID files, and for the field devices, this required updated settings files. These modifications worked well, and the frequency of transmitted updates to the SICAM became much more manageable.

If KCP&L implemented 61850 in other substations at some point in the future, they would likely consider setting a deadband on only one type of analog in the 61850 report dataset. For example, they might set deadbands on all of the current values, so that only changes to the system current would trigger data transfer. Understanding 61850 reporting was critical to this realization.

- **Point Limit** –Another issue that the team ran into was a point limit on the SICAM. Originally, KCP&L planned to bring back a lot of data for the substation and field devices that wasn't necessarily needed by any of the DNA applications. The thought was that the devices were capable of sending all of this data, and that perhaps engineering would be able to utilize it for various purposes. The team didn't experience any issues after the substation devices were deployed, but as KCP&L and Siemens started to plot out the field device deployment, the team was informed that there is a 10,000 point limit to an individual SICAM. So the total number of binary, counter, and analog points for all of the substation and field devices needed to be less than 10,000. As a result of this hardware limitation, the team went back to the substation and field device profiles and reevaluated

which data was still desired. The points list and templates were revised, and the “final” configuration with all the field devices was brought sufficiently below 10,000 points.

- **Cascading Failures** – In the original configuration, the SICAM had one “interface” to all the substation devices (the IEC 61850 interface) and one interface to all the field devices (the DNP3.0 interface). When the project team started to deploy the field devices, issues began to occur with the SICAM’s DNP interface. After doing some monitoring, the team was able to pin down the specific problem. When the SICAM lost communications to a particular device (mostly due to the wireless network performance), it would continue to try to reestablish communications with that device. It would expend so much processing power on this single, problematic device, that it would lose communications with the other devices in that interface. As a result, the entire interface and the communications to all the field devices went down, including the devices that had good communication. In order to address this issue, Siemens directed the KCP&L team to change a few time out parameters to better accommodate the wireless communications to the field devices. Siemens also helped the team to split up the interfaces into smaller groups. The revised SICAM contained a number of interfaces, each with no more than seven devices. The devices were split into interfaces based on the feeders that they are associated with. This helped the issue a lot, and it also allowed the team to more easily determine which field devices had problematic communications.
- **Server Redundancy** – The last major issue that the team experienced with the SICAM occurred when the SICAM was running in redundant mode. As described above, the long-term design configuration was to have two SICAMs up and running at all times so that if one piece of hardware failed, there would be a seamless transition to the other SICAM. Unfortunately, during periods of extended device outages, when communications with a single device are lost, the SICAMs begin to fail back and forth. Each SICAM is looking to the other one to bring up the connection to the problematic device, and they basically get stuck in the middle. During these times, the team is able to ping and telnet to the problematic device from either SICAM, but no connection is shown in SICAM. So the communications path is back up at this point, but the SICAMs have bounced back and forth enough that they get stuck in the process. When this occurs, the communications path to the problematic device needs to be stopped and restarted. The other approach that the team took to solve this problem was to focus on some of the problematic field devices and improve the communications to them via the wireless network. Focusing on the root of the problem eliminated the server redundancy issue.

To be updated in future releases of this report

2.2.3.2.4 Lessons Learned

Throughout the build and stabilization of the DDC (SICAM) system, numerous considerations were realized and should be noted for future deployments of this sort. These Lessons Learned are as follows:

- One of the major lessons learned on this project had to do with the interfaces to the field devices. Most data concentrators on the market today were designed for use in the substation, where there is a physical connection from the concentrator to each device. This is the case for the substation devices at Midtown, but the field devices utilize a wireless network to communicate to the SICAM. As a result, the project team experienced many issues with the SICAM to field device communications. Since wireless networks don’t guarantee 100% uptime and availability, there are times when the SICAM polls the field devices and the communications fail. The way that the SICAM continues to poll that

problematic device, and how this impacts the other, non-problematic devices, isn't conducive for field devices. Siemens and the project team spent a lot of time troubleshooting issues with the DNP3.0 interface, and they tweaked a lot of configurations in order to make the system perform sufficiently for the wireless network. For larger, system-wide deployments, using a traditional wired concentrator might not be feasible. In the future, vendors will likely need to design new concentrators that are built with wireless communications networks in mind.

- Another lesson that KCP&L learned from the SICAM implementation was that the substation data concentrator can be used in several different ways. Although the SICAM is capable of performing arithmetic functions, it wasn't configured as such for the KCP&L project. For the demonstration implementation, the SICAM was used solely as a concentrator. It received updates from the substation and field devices, and it sent the data upstream to the DMS, DCADA, and HMI. If KCP&L was to use the SICAM in the future, they would likely reconsider the implementation of this system. Since it is capable of performing calculations, KCP&L would probably limit the number of points reported back from each device. A smaller number of points would be sent to the SICAM, and then the SICAM could calculate the remaining points with that information. For example, instead of bringing back all the points associated with voltage, current, and power, the device would just send the voltage and current data and the SICAM would calculate the power values.
- KCP&L learned a lot about IEC61850 and how to use it for substation communications. One lesson that was learned the hard way was that the CID files loaded on the device itself need to match the CID files loaded on the SICAM exactly. If they somehow get out of synch, connection to the device is lost, as seen by the SICAM. There were several instances where the relay technicians went out to the devices to do firmware updates, and the existing CID files were accidentally dumped or replaced in the process. Determining a proper versioning method for the CID files would be critical for a multi-substation implementation.
- The last lesson learned through the SICAM implementation had to do with manufacturer specific 61850 implementations. By design, the 61850 standard is very flexible, and it was intended to meet many needs. While this can be a positive, it also leaves much room for interpretation, and vendors have interpreted the standard in different ways. Configuration tools for IEC 61850 are still in their infancy, and the industry has a long ways to go to fully configure a 61850 station. Currently a vendor-specific tool is the best way to do this configuration, since the vendors have interpreted the standard in such different ways. This can be problematic if the implementation uses multiple IED or system vendors, though. One example problem is due to 61850 being self-descriptive. This means that the device will tell you what points and services it offers. In theory, this is a great feature of 61850, but unfortunately the SICAM doesn't take advantage of this feature. Rather, it requires the 61850 configuration file from each IED be manually loaded into the master configuration. Another issue that the team encountered on the demonstration project had to do with analogs. Specific firmware versions on SEL relays defined analogs differently – some were defined as full complex values, but others were defined as two values (an angle and a magnitude). SEL devices aren't consistent in the way they do this, and SICAM only supports one of these methods (angle and magnitude).

To be updated in future releases of this report

2.2.3.3 Human Machine Interface

The substation Human Machine Interface (HMI) provides a local view of all of the equipment located inside the fence of the substation. The purpose of the HMI is to give substation personnel a tool for viewing the current status of the equipment within the substation, as well as giving them the potential to operate the smart grid devices from within the substation control house. Unlike the DMS and the DCADA, the HMI does not contain any information about the field devices. The HMI does, however, provide information about the substation network equipment, which is not displayed in the DMS.

2.2.3.3.1 Build

The SICAM PAS HMI is one of Siemens commercially available utility products. By pursuing this “off-the-shelf” philosophy to the maximum degree possible, limited design and development efforts are required and the Demonstration Project is provided the opportunity to evaluate the capabilities of existing products and technologies in meeting the emerging Smart Grid requirements. The following sections provide a summary of the development and configurations that were required to implement and deploy the desired HMI functionality.

2.2.3.3.1.1 **Training**

Work on the Human Machine Interface (HMI) began with some preliminary training. Training for the Siemens SICAM and HMI was conducted jointly in August, 2012. Participants learned about how to use the HMI, but didn’t learn much about initial GUI creation and configuration.

2.2.3.3.1.2 **Initial HMI Configuration**

KCP&L provided Siemens with the Midtown substation one-lines and network configuration diagrams, and Siemens began to create the Midtown HMI GUI. KCP&L also worked with Siemens to determine the event list and alarm list that they wanted to be used with the HMI. The alarm list for the HMI was created to as a subset of the DMS alarm list (which was determined while creating the signal list).

Siemens showed KCP&L their initial version of the HMI, and the KCP&L team provided feedback based on the needs of the relay technicians. KCP&L also requested modifications to some of the data points displayed on the HMI GUI. Siemens made the modifications to the HMI and prepared it for the Factory Acceptance Test (FAT).

2.2.3.3.1.3 **Factory Acceptance Test (FAT)**

The KCP&L team traveled to Minnesota for the HMI, SICAM, and DMS Factory Acceptance Test (FAT) from August 20 through August 31, 2012. During FAT, the team tested out the functionality of the HMI and the interface to the SICAM in Siemens’ Minnesota environment. As a reminder, the HMI only displays the substation devices – no field device information is shown in the HMI GUI. For the FAT, only one HMI was used, so the team wasn’t able to do any testing pertaining to redundancy.

Throughout the FAT, the KCP&L team tracked variances and prioritized them by severity. Upon completion of the FAT, they constructed a list of several modifications that they wanted to see prior to the Site Acceptance Test, in addition to several “enhancements” that might be added at a later date. Siemens made the necessary modifications and then sent the test HMI to Kansas City for deployment in the production environment.

2.2.3.3.1.4 Production Configuration and Site Acceptance Test

The production HMI configurations consist of the following:

- Two servers located in the Midtown battery control enclosure – these are to be used by the smart grid team
- One client located in the Midtown battery control enclosure – this is to be used by the smart grid team for demonstration purposes
- One client located in the Midtown substation control house – this is to be used by the relay technicians

Like many other systems in the Demonstration Project, the HMIs were configured to be redundant in the production environment. Unlike the other systems in the project, however, there are no HMIs in the development environment.

Upon configuration of all the HMI clients and servers in the production environment, Site Acceptance Testing (SAT) commenced. SAT for the HMI ran from September 17 through October 5, 2012 (though targeted test and variance remediation continued on sporadically for some time). For the HMI, SAT consisted of a point-to-point checkout of every substation device. It also included network testing, as well as checks of the event and alarm lists. The issues discovered during the point-to-point checkouts were all resolved immediately. The network issues were much more significant, however, as the HMI network GUI had been built from an outdated network diagram with old port mappings.

Before modifying the networking screen of the HMI, Siemens provided some HMI “retraining,” this time focusing on how to create, configure, and alter screens in the GUI. Armed with this knowledge, KCP&L was able to resolve the port mapping issues and rebuild the network screen of the HMI. The network information now displayed on the HMI allows the user to verify whether any substation issues are related to network communications. Each substation device will be connected to a particular network switch and mapped to a specific port. Although the user can’t modify any network configurations from the HMI, he will be able to easily determine whether any problems exist on the network prior to engaging the IT personnel at KCP&L.

2.2.3.3.1.5 Modifications per RuggedCom Switch-Out

As described in section 2.2.3.1.2, during the fall of 2013, KCP&L decided to replace the RuggedCom switches in Midtown substation with Cisco switches. Upon completion of this work, the HMI no longer painted an accurate picture of the Midtown substation networking equipment. KCP&L worked with Siemens to modify the SNMP and completely update the port mapping for these new switches. Once this was done, the team conducted yet another port-to-port checkout to verify the updated mapping.

Screenshots of the current HMI GUI are shown below in Figure 2-40 through Figure 2-45.

Figure 2-40: HMI One-Line Screenshot

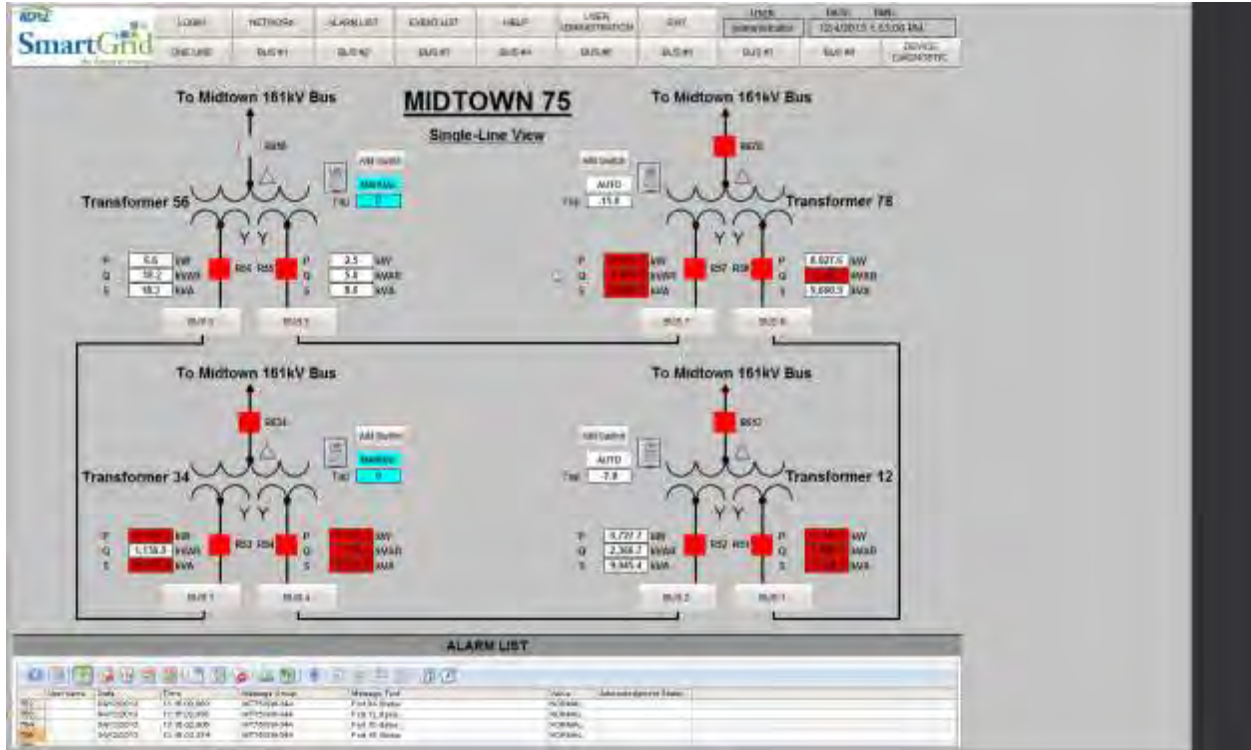


Figure 2-41: HMI Single Bus Screenshot

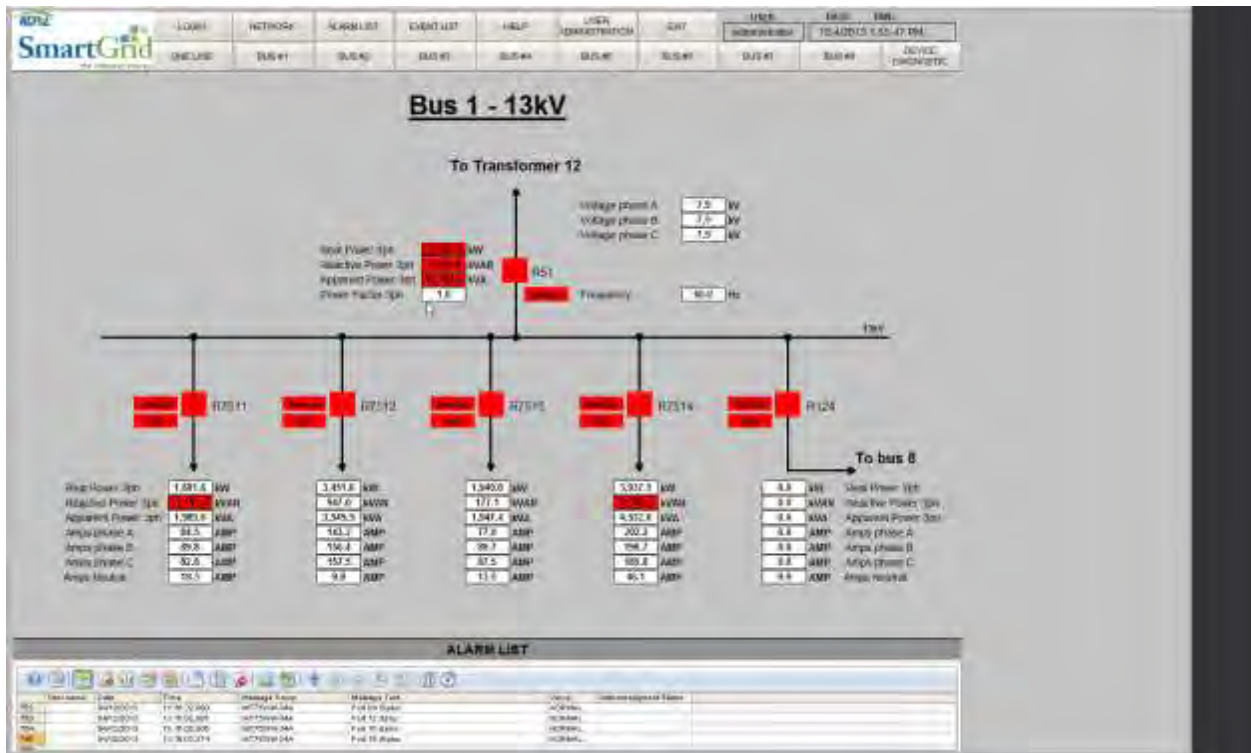


Figure 2-42: HMI Device Diagnostic Screenshot



Figure 2-43: HMI Alarm List Screenshot

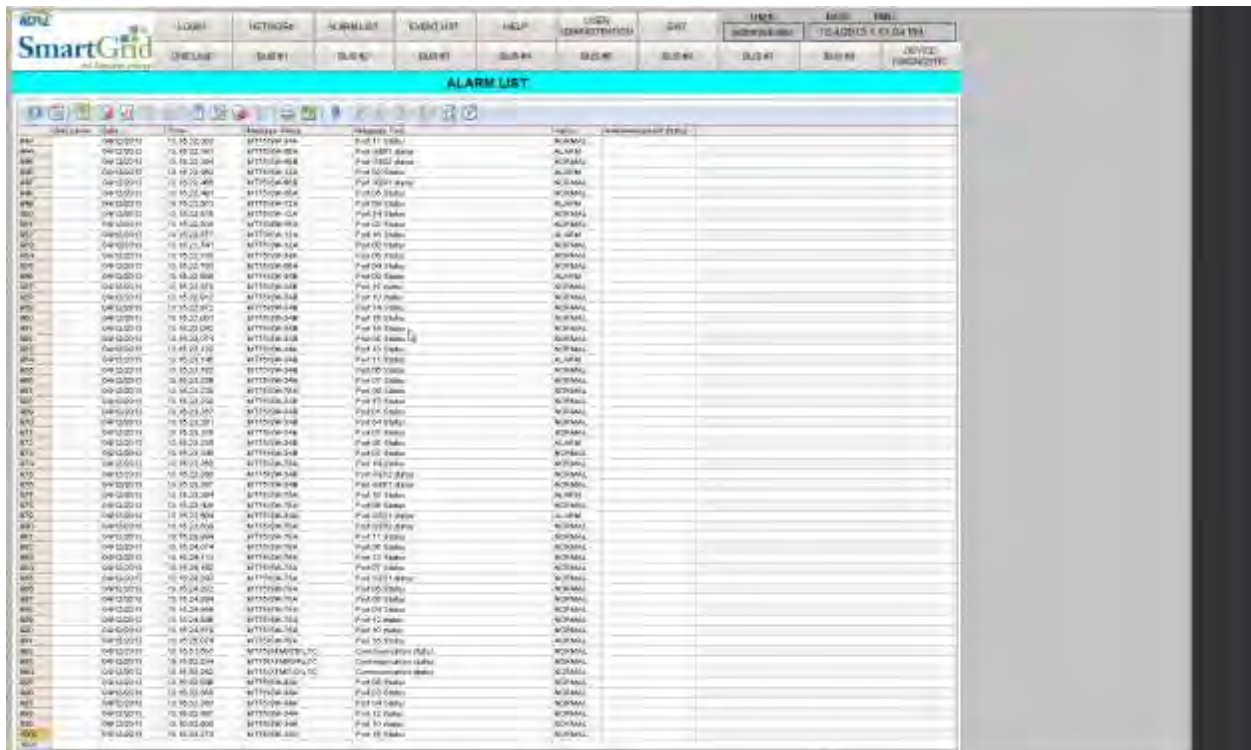
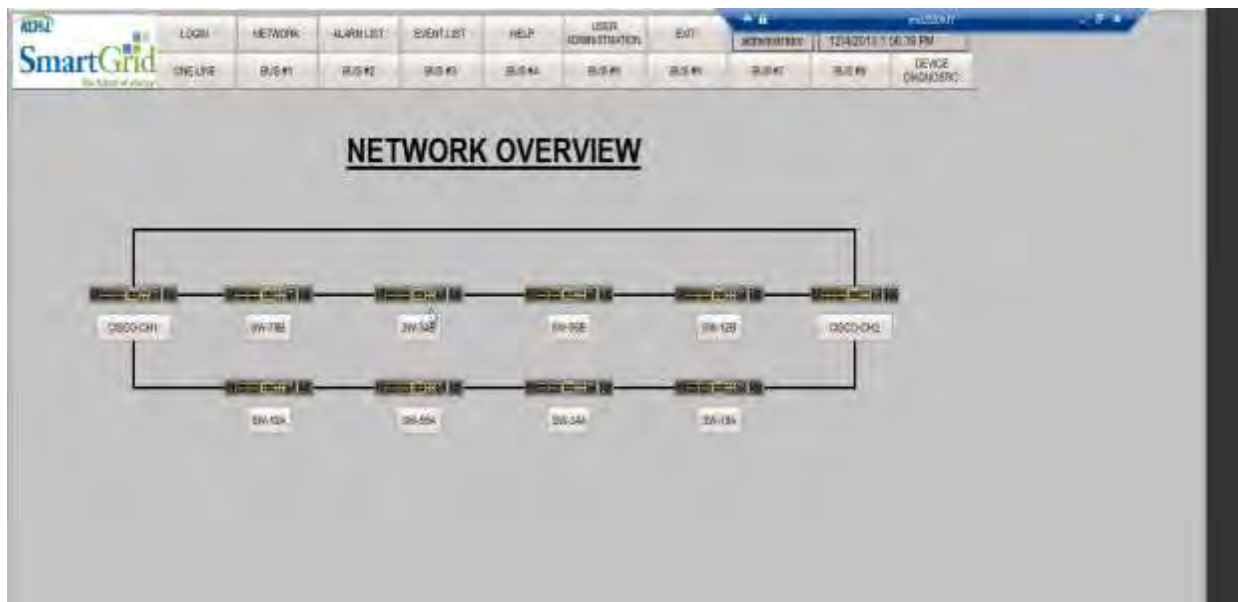


Figure 2-44: HMI Event Log Screenshot

ID	Time	Location	Description	Status
884	09-22-09 11:45:00	BT1009-000	Fail 11 Status	Normal
885	09-22-09 11:45:00	BT1009-000	Fail 10 Status	Normal
886	09-22-09 11:45:00	BT1009-000	Fail 09 Status	Normal
887	09-22-09 11:45:00	BT1009-000	Fail 08 Status	Normal
888	09-22-09 11:45:00	BT1009-000	Fail 07 Status	Normal
889	09-22-09 11:45:00	BT1009-000	Fail 06 Status	Normal
890	09-22-09 11:45:00	BT1009-000	Fail 05 Status	Normal
891	09-22-09 11:45:00	BT1009-000	Fail 04 Status	Normal
892	09-22-09 11:45:00	BT1009-000	Fail 03 Status	Normal
893	09-22-09 11:45:00	BT1009-000	Fail 02 Status	Normal
894	09-22-09 11:45:00	BT1009-000	Fail 01 Status	Normal
895	09-22-09 11:45:00	BT1009-000	Fail 00 Status	Normal
896	09-22-09 11:45:00	BT1009-000	Fail 00 Status	Normal
897	09-22-09 11:45:00	BT1009-000	Fail 00 Status	Normal
898	09-22-09 11:45:00	BT1009-000	Fail 00 Status	Normal
899	09-22-09 11:45:00	BT1009-000	Fail 00 Status	Normal
900	09-22-09 11:45:00	BT1009-000	Fail 00 Status	Normal

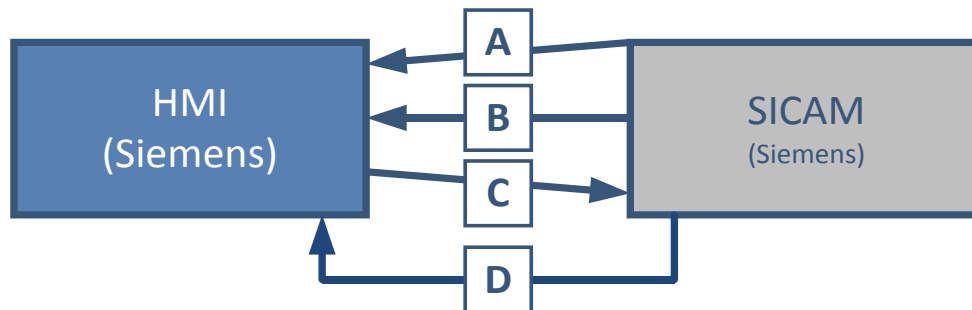
Figure 2-45: HMI Network Overview Screenshot



2.2.3.3.2 Integration

An overview of HMI system-to-system interfaces and applicable messages is illustrated in Figure 2-46.

Figure 2-46: KCP&L SmartGrid Demonstration Project HMI Integration



The integration touch points for the HMI are as follows:

- A. 'Substation Device Status/Analog Update' notification initiated from substation devices to SICAM and sent from SICAM to HMI. (Reminder that field device data doesn't get passed to the SICAM – only substation device data.) This is an IEC 61850 status message used to notify SICAM (and HMI) of an updated analog or status at a substation device.
- B. 'Substation Device Event / Alarm' notification initiated from substation devices to SICAM and sent from SICAM to HMI. (Reminder that field device data doesn't get passed to the SICAM – only substation device data.) This is an IEC 61850 event or alarm message used to notify SICAM (and HMI) of an event that has occurred or an alarm that has been activated.
- C. 'Substation Device Control' message initiated from the HMI and sent to the SICAM and then on to the substation device. This is an IEC 61850 control message.
- D. 'Network Device Status' message initiated from one of the substation network switches and sent to the SICAM and then on to the HMI. This is an SNMP message used to notify SICAM (and HMI) of the status of a particular network switch.

2.2.3.3.3 Post-Implementation Operational Issues

Following the initial testing and deployment of the HMI, several post-implementation operational issues needed to be considered and mitigated. Since devices are rarely added or removed from a substation, the HMI isn't likely to undergo many post-operational modifications. The post implementation issues experienced by the project included the following:

- **RuggedCom Switch Replacement** – For KCP&L's implementation, the main post-operational HMI issue was the replacement of the RuggedCom switches with Cisco switches. Since the network switches and their statuses are displayed on the HMI, the switch replacement forced the KCP&L team to re-work the network screens. Since the Cisco switches use different ports than the RuggedCom switches, re-mapping wasn't a simple exercise. The switches each had to be failed over in order to generate and record the updated port mappings.
- **Mapping and Display Modifications** – In addition to the logical re-mapping described above, KCP&L also worked with Siemens to rework the graphical user interface of the HMI to accurately display the final as-built state of the Midtown substation network.

To be updated in future releases of this report

2.2.3.3.4 Lessons Learned

Throughout the build, implementation, and daily operation of the HMI, numerous considerations were realized and should be noted for future implementations. These Lessons Learned are as follows:

- While minor changes such as GUI text modifications are simple on the HMI, creation and significant modification of the HMI display isn't very intuitive. It requires a comprehensive understanding of the GUI layers that wasn't easily attainable without advanced training.
- Sorting events and alarms on the HMI GUI can be a bit confusing. This topic generated discussion during training classes, and KCP&L made sure to train the end users specifically on this component of the GUI.
- The "finished" HMI will be very useful for both the smart grid project team as well as the system end user – the relay techs. By using the HMI at Midtown substation, the techs will be able to see the status of all substation devices in one place, rather than walking around to each relay to troubleshoot or test.

To be updated in future releases of this report.

2.2.3.4 GOOSE Messaging

For peer-to-peer communications in the substation, the IEDs will utilize 61850 Generic Object-Oriented Substation Event (GOOSE) messaging.

2.2.3.4.1 Build

The following discussion provides a summary of the development and configurations that were required to implement and deploy the desired GOOSE functionality.

2.2.3.4.1.1 **Scheme Logic Design**

The Midtown substation GOOSE implementation began in 2010, when KCP&L started to think about what GOOSE schemes they wanted to implement. After several meetings, the KCP&L substation group decided on four schemes for the project:

- Automatic load transfer upon transformer lockout
- Faster clearing of the bus upon feeder breaker failure
- Backup overcurrent protection in the bus differential relay
- Cross triggering of all devices for distribution system event

After developing the initial logic for these schemes, the team loaded the logic onto the lab substation devices to ensure that they could support it. They wanted to ensure that the logic wouldn't overload the devices, as the devices are limited with how much logic they can process. Unfortunately, these limits aren't fixed values, so the only way to determine whether the devices can support the logic is to actually test it out.

2.2.3.4.1.2 **CID File Creation and Initial Deployment**

After doing some preliminary testing, the team made modifications as needed. Relay technicians then deployed the CID files to the substation devices, with the GOOSE schemes disabled. This allowed the team to begin testing out substation device communications with the SICAM via the IEC61850 MMS messaging, without having the GOOSE work fully tested and finalized.

2.2.3.4.1.3 **Scheme Lab Testing and Modifications**

In 2013, KCP&L came back to the GOOSE work and began in-depth testing. They started by reviewing the logic theoretically – looking at the logic flow diagrams and communications diagrams. Next, they went through the logic code for each scheme, line by line. They ensured that everyone was on the same page

with each step of the logic scheme. Then, they tried breaking the code by using various inputs. They looked at each shed possibility, and they tested each one with different fail bits and trigger bits. Three of the schemes held up well to this logic testing, but the bus transfer scheme required several attempts.

Next, the team mocked everything up in the Burns & McDonnell Smart Grid Lab. Their setup included the following:

- (6) SEL 751A feeder/tie breakers
- SEL 451-5 bus main breaker
- SEL 487E transformer differential
- SEL 487B bus differential
- SLE 3530 (RTAC) for automation control and to act as the far site
- Garrettcom Magnum 6k32f switch
- Computers to run SEL AcSElerator, SEL Architect, AX-S4, VM-Ware
- Manta test set for current and voltage inputs
- Test blades

Figure 2-47 below shows the test rack that was used for the 61850 GOOSE testing in the Burns & McDonnell Smart Grid Lab.

Figure 2-47: GOOSE Lab Testing Rack Setup



The testing team used test kits to provide the necessary voltage and current inputs, and they monitored the status of everything using 61850 on a temporary HMI. As they tested various scenarios, they made any necessary changes to complete the 61850 logic schemes.

2.2.3.4.1.4 GOOSE Activation and Production Testing

There are two settings pertaining to IEC61850 that are stored in the relay settings files. The “Enable IEC 61850 Protocol” setting in the relay settings file has been enabled for a while now – this allows the substation relays to communicate to the SICAM using IEC61850 MMS messages. The second setting pertaining to IEC61850 has not been enabled as of yet. In December of 2013, the relay technicians will return to all of the substation devices to make a few changes in order to “activate” the GOOSE logic. First, they will need to import the modified CID file. Second, they will need to set the “Enable IEC 61850 GOOSE” setting in the relay settings file.

After much discussion, KCP&L decided to do the GOOSE activation and testing in a more incremental manner to avoid major disruption to the Midtown feeders. Due to the highly automated nature of the GOOSE schemes, KCP&L has chosen to activate only one scheme in this first round of production GOOSE testing – the cross triggering of all devices for distribution system events. This will allow KCP&L to gain confidence with the GOOSE schemes, without requiring any outages to test. The event reporting scheme will run anytime an “event” occurs, but since this scheme is simply reporting of statuses of all the substation devices, no devices will open or close as a result. The other schemes would all require significant planning to avoid major customer outages during testing – especially the bus throw-over scheme.

2.2.3.4.2 Integration

For the GOOSE component of the demonstration, there isn’t really any system-to-system integration, since GOOSE isn’t a “system.” Rather, GOOSE is a mechanism for transferring event data over entire substation networks. The GOOSE messages travel between the substation devices over the Midtown substation protection network described in earlier sections (Overall SPN scope in 1.4.4.1 and SPN Implementation in [2]).

2.2.3.4.3 Post-Implementation Operational Issues

Since the GOOSE schemes haven’t been activated yet, the KCP&L team hasn’t experienced any post-implementation operational issues to this point.

To be completed in future releases of this report.

2.2.3.4.4 Lessons Learned

Throughout the development of the GOOSE schemes, a few considerations were realized and should be noted for future deployments of this sort. These Lessons Learned are as follows:

- One of the lessons learned from GOOSE had to do with deadbands. While deadbands were addressed in-depth in the DDC section, they were also important for GOOSE messages. For the transfer scheme, the logic is sending analogs. The team had to double check all the multipliers and deadbands to ensure that the devices weren't sending GOOSE updates too frequently.
- Another lesson learned was in regards to vendor interoperability of the IEC61850 standard. KCP&L used all SEL relays, so this wasn't a big problem for the demonstration implementation, but it became obvious throughout the design/testing/build of the GOOSE component that things would have been much more complex had we utilized relays from multiple vendors. Taking advantage of the flexibility in the IEC 61850 standard, vendors have implemented the GOOSE protocol somewhat differently. For example, the standard specifies four identifying characteristics for each GOOSE message. Certain vendors will only use two of these characteristics for identification, while other vendors might use three characteristics, which may or may not overlap. Moving forward, utilities need to push the vendors to standardize on their GOOSE implementations.

To be updated in future releases of this report.

2.2.3.5 Substation DCADA

The Substation Distributed Control and Data Acquisition (DCADA) is the brains of the substation. It receives device status updates from the SICAM, and it determines how to respond to activity occurring on the distribution system.

The DCADA can perform many of the same applications as the Distribution Management System, but it does so in a closed loop method, and it can only control devices within its area of control. For the demonstration project, the DMS and DCADA will be monitoring and controlling the same set of devices, since the Midtown substation (and its associated substation and field devices) is the only substation that is part of the project.

2.2.3.5.1 Build

KCP&L's DCADA implementation efforts were launched by assembling a team of highly skilled individuals that would pursue and support the deployment of these advanced applications. To familiarize themselves with the goals of the project, the team began by reviewing previously created Use Cases to understand new processes and anticipated system functions. These Use Case documents were finalized where possible and provided to Siemens to establish their baseline understanding of what KCPL hoped to achieve with the system implementation. Where clarifications were required, they were addressed during the Siemens Design / Configuration Workshops.

In parallel to KCPL's preliminary use case familiarization efforts, Siemens began establishing its project team to perform the installation. The DCADA core capabilities and interfaces are part of a commercially available, productized software implementation which can be configured to the needs of a given customer. By pursuing this "off-the-shelf" philosophy to the maximum degree possible, limited custom design was required. However, the systems did require configuration to accommodate KCP&L's distribution system. In this context, Siemens began identifying key staff and subject matter experts who would be performing the configuration. As there were relatively few implementations of this product,

staff began familiarizing themselves with the configuration elements required and documenting questions to be answered in preparation of the actual configuration efforts.

2.2.3.5.1.1 DCADA Testing

The DCADA system has been the lowest priority system, as its functionality mirrors that of the DMS, but it runs in an environment with less opportunity for user control. As a result, KCP&L's overall strategy was to start by testing out the DNA applications in the open loop mode at the DMS, then move to closed loop testing at the DMS, and then finally conduct closed loop testing at the DCADA.

The DCADA implementation was part of KCP&L's Phase 3 DMS work. This phase of implementation and testing focused on the First Responder (or DNA) applications. The goals of this phase were to progressively validate and stabilize DNA results based on required D-SCADA inputs.

The KCP&L team performed DNA and DCADA Factory Acceptance Test (FAT) from KCP&L's facilities and accessed the Minnesota based systems for testing from February 4 through February 15, 2013. During FAT, the team tested out the functionality of the DCADA and the interface to the SICAM and DMS in Siemens' Minnesota environment.

Throughout the FAT, the KCP&L team tracked variances and prioritized them by severity. Upon completion of the FAT, they constructed a list of several modifications that they wanted to see prior to the Site Acceptance Test (SAT), in addition to several "enhancements" that might be added at a later date. Siemens made the necessary modifications and then sent the DCADA to Kansas City for deployment in the production environment.

Once the DCADA servers were deployed in the KCP&L lab and demonstration environments, the Site Acceptance Testing began. The first pass of DCADA SAT testing occurred between 10/10/2013 and 10/22/2013. It included tests covering all of the First Responder applications: State Estimation, Power Flow, Volt-VAR Control, Feeder Load Transfer, Fault Location, and Fault Isolation and Service Restoration. All of this testing was done on the lab DCADA instance. To learn more about the First Responder applications above, refer to the pertinent scope section (specifically 1.4.5.4).

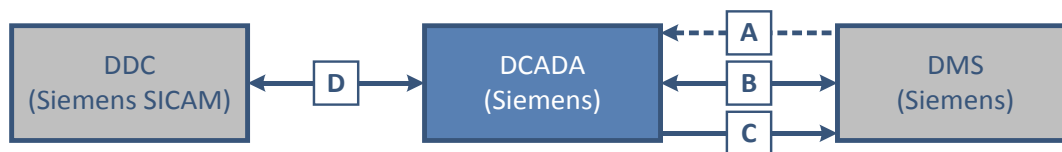
2.2.3.5.1.2 Closed Loop Operation

Currently, the DCADA is receiving substation and field data updates from the SICAM, but it is not used as the control engine for closed loop applications. KCP&L is planning to gain confidence in the systems using a "crawl, walk, run" philosophy. So even though the DCADA hardware has been tested in the lab environment and deployed in the production environment, KCP&L won't be testing in production for a while. Use of the DCADA requires a good deal of system trust, as it has to happen in a closed loop format.

2.2.3.5.2 Integration

An overview of DCADA system-to-system interfaces and applicable messages is illustrated in Figure 2-48.

Figure 2-48: KCP&L SmartGrid Demonstration Project DCADA Integration



The integration touch points for the DCADA are as follows:

- A. DMS / DCADA Model Synchronization: A uni-directional interface allowing for data model updates to be propagated from the DMS to the DCADA as required to stay synchronized as

changes are activated from IMM. All data exchanges in this interface are transmitted via proprietary protocols.

- B. DCADA / DMS SCADA Data and Mastership Synchronization: A bi-directional interface allowing for the following data to be provided by the DMS to the DCADA (if the DMS is in control), or from the DCADA to the DMS (if the DCADA is in control).
- Tags (markers)
 - Jumpers, cuts, and grounds
 - Control actions

This interface also allows for the transmission of delegated control permissions to be exchanged between DMS and DCADA to ensure synchronization of SCADA mastership. All data exchanges in this interface are transmitted via propriety protocols.

- C. DCADA / DMS Alarms: A uni-directional interface allowing for the transfer of SCADA and application alarms from the DCADA to the DMS (if the DCADA is active in closed loop). Example conditions that would generate alarms include:
- DCADA application failed to reach a solution
 - Control was transferred from DCADA to DMS
 - Link between DMS and DCADA is broken
 - An applications running at the DCADA doesn't converge or finishes with violations
 - First Responder application running at the DCADA can't complete operations due to device control being disabled

All data exchanges in this interface are transmitted via propriety protocols.

- D. DCADA / DDC Monitor and Control for Field Values: A bi-directional interface allowing for DCADA point monitoring details to be provided by the DDC (SICAM) so that it has all updated information for propagation to other systems. The interface also allows for any controls resulting from upstream closed-loop DNA applications to be transmitted to the DDC (SICAM) for further propagation to devices in the field. All data exchanges in this interface are automatically transmitted via 61850 protocols.

2.2.3.5.3 Post-Implementation Operational Issues

Since KCP&L hasn't really used the DCADA in a closed-loop mode yet, there haven't been opportunities to identify post-implementation operational Issues. So far, testing of the system in a controlled environment has been positive.

To be completed in future releases of this report.

2.2.3.5.4 Lessons Learned

Throughout the build, implementation, and daily operation of the HMI, numerous considerations were realized and should be noted for future implementations. These Lessons Learned are as follows:

- The major lesson learned so far in regards to the DCADA has to do with system limitations. When the team received training on the Siemens DCADA, they learned about the closed loop capabilities and limitations. In general, the First Responder functionalities need to be activated en masse. For example, if one First Responder function is running in closed loop mode on the Siemens DCADA, then all First Responder functions have to be running in

closed loop mode on the DCADA. The system can't handle having one First Responder application running on the DMS and another running on the DCADA. Instead, the user has to shift to the closed-loop DCADA functionality for everything. Additionally, there is no way to run certain network segments (for example, a particular feeder) in closed loop. Rather, if one feeder is running a First Responder function in closed loop mode, then all feeders need to be running that function in closed loop mode.

- While the team understands the complexities associated with splitting up the First Responder functions by network topology or centralized/substation controllers, it would be very beneficial to be able to do so. As KCP&L gains confidence in a particular First Responder application, for example, they could choose to run that application in closed loop mode on the DCADA, yet continue to run the others from the DMS.

To be updated in future releases of this report.

2.2.4 SmartDistribution

The SmartDistribution sub-project deployed a state-of-the-art DMS with integrated UI/CAD, OMS, D-SCADA, DNA 1st Responder applications, and Historian components to manage numerous field devices and sensors across a wireless mesh IP network. KCP&L selected the Siemens-Intergraph DMS as it was a pre-integrated, commercially available DMS solution. By pursuing this “off-the-shelf” philosophy to the maximum degree possible, limited design and development efforts were required and the Demonstration Project is provided the opportunity to evaluate the capabilities of existing products and technologies in meeting the emerging Smart Grid requirements. The following subsections summarize the SmartDistribution component deployments.

As the project progressed and KCP&L further assimilated the scope and complexity of this overall project, questions arose regarding the feasibility of the original intent to conduct one comprehensive configuration and test effort for DMS functions. An analysis was performed to better understand the critical interdependencies between systems to ensure successful testing and deployment. The result of this analysis showed that complexity in the related systems would benefit from increased focus on narrower definitions of scope. The D-SCADA capabilities are a critical pre-requisite for CAD, First Responder, and DERM functions. Without stability of D-SCADA and downstream device communications, no data points would be transmitted allowing these functions to perform. As a result, the KCP&L team decided to break the configuration and deployment of the overall DMS into three phases; D-SCADA capabilities were broken into two logical components and scheduled first to provide maximum stability for later First Responder efforts. Each of the phases of work would include vendor configuration, Factory Acceptance Test (FAT), and then conclude with KCP&L installation and Site Acceptance Test (SAT).

- **Phase 1 – Substation Device Monitoring:** All substation devices to be automated through the project (breakers, differentials, tap changers, etc.) were configured and installed at KCP&L’s Midtown Substation. In parallel, preliminary efforts were conducted to deploy the D-SCADA system to all environments and establish preliminary communications for remote monitoring of substation device point changes. Point-to-point monitoring-only checkouts were conducted on all points for all substation devices to ensure proper communications from the device through to the CAD.
- **Phase 2 – Substation Device Control & Field Device Monitoring / Control:** All field devices to be automated through the project (reclosers, fault indicators, capacitor banks, 1MWh battery) were configured and installed along selected highly automated circuits. With all devices fully installed and D-SCADA further stabilized, communications for field device monitoring were established and control capability enablement for all devices (both substation and field) were planned, tested, and activated. Point-to-point monitor and control checkouts were conducted on all points for all substation and field devices to ensure proper communications to / from the devices through to the CAD.
- **Phase 3 – First Responder Applications:** Finally, the team enabled the configured DNA applications. They progressively validated and stabilized results based on required D-SCADA inputs. They commenced efforts with State Estimation and Power Flow; advanced to Volt-VAR Control, Feeder Load Transfer, Fault Location, Fault Isolation and Service Restoration. Once confidence in the above capabilities was established and the applications configured to maximum performance and user comfort in CAD, efforts could continue to advance on closed loop functionality and validation of these capabilities when delegated to the DCADA authority through the Control UI functionality in the CAD. Outage Restoration and Power Status Verification efforts and DERM integrations was also pursued during this final phase.

Another key takeaway from the initial implementation analysis was the need to establish and maintain several integrated environments to ensure that functionality was safely segregated for forthcoming development and testing efforts. Due to the complexity of integrating systems within each of these environments, the effort to set these up was commenced early to ensure their readiness as needed.

- **VENDOR Environment:** The first and most basic environment was the VENDOR environment. The UI/CAD, OMS, D-SCADA, DNA, DCADA, and SICAM DDC applications were installed on KCP&L owned servers that were sent to the Siemens facility for initial configuration. In addition, sample substation controllers were also provided for vendor use. All hardware was extensively used to establish initial configurations and ensure they were working under controlled conditions.
- **LAB Environment:** The second and more complex environment was the LAB environment. It was initially setup to augment the VENDOR environment, as sample field devices were setup and connected to a LAB dedicated network which was interfaced with the servers of the VENDOR environment for preliminary tests. Later in the project lifecycle, the sample substation devices were transferred back to KCP&L's facility and additional KCP&L procured servers were then setup in the LAB to establish a standalone environment; the connection to the VENDOR environment was severed. By that point, the LAB also had integration with numerous other systems to more robustly mimic DEMO and was used to test out preliminary integration configurations.
- **DEMO Environment:** The final and most complex environment was the DEMO environment. This was KCP&L's real-world environment where the systems were supported by redundant servers, configured for full integration with other systems, and connected to all of KCP&L's Smart Grid devices deployed to the substation and certain highly automated distribution feeders. As these devices would result in real-time, real-world distribution network changes, special care was taken to ensure that no negative consequences resulted from our efforts when testing in the DEMO environment

2.2.4.1 DMS UI/CAD

The Intergraph DMS UI/CAD component establishes a platform by which the Distribution Grid Operators can access all important information relating to customer and network operations from a single user interface. . The following sections provide a summary of the development and configurations that were required to implement and deploy the desired DMS UI/CAD functionality.

2.2.4.1.1 Build

KCP&L's Integrated UI, also known as Computer Aided Dispatch (CAD) or more specifically Intergraph's InService (I/Dispatcher module), implementation efforts were launched by assembling a team of highly skilled individuals that would pursue and support the deployment of these advanced systems. The goal was to upgrade and integrate the primary control room systems so that Distribution Operations users could access all important information relating to customer and network operations from a single user interface. To familiarize themselves with the goals of the project, the team began by reviewing previously created Use Cases to understand new processes and anticipated system functions. These Use Case documents were finalized where possible and provided to Intergraph to establish their baseline understanding of what KCP&L hoped to achieve with the system implementation. The use cases served as a solid foundation of understanding for newer team members. Where clarifications were required, they were addressed during the Design/Configuration Workshops.

In parallel to KCP&L's preliminary use case familiarization efforts, Intergraph began establishing its project team to perform the installation. The I/Dispatcher core capabilities and interfaces are part of a commercially available, productized software implementation which can be configured to the needs of a given customer. By pursuing this "off-the-shelf" philosophy to the maximum degree possible, limited

custom design was required. However, the systems did require configuration to accommodate KCP&L's distribution system. With this in mind, Intergraph created a System Configuration Diagram based on discussions with KCP&L to better understand the system configuration and requirements. Intergraph then developed a detailed plan which outlined the time required to meet these requirements and configure the system per KCP&L's needs. As there were relatively few implementations of this integrated DMS solution, staff began familiarizing themselves with the key configuration elements required and documenting questions to be answered in preparation of the actual configuration efforts.

2.2.4.1.1.1 Collaborative Design Sessions

After the preliminary familiarization efforts conducted by KCP&L and Intergraph, several workshops were conducted to expedite the configuration effort. The First Responder and Facility Migration Design workshop was conducted to review the details of First Responder data required and KCP&L's existing mapping technologies. The DMS InService Integration Design workshop (focused on D-SCADA integration) was held in which Siemens, Intergraph, and KCP&L jointly participated in this workshop to ensure that all parties were in agreement about the design and configurations to be pursued. Specifically, analysis was performed on the CAD and how it would work with Siemens' D-SCADA (PowerCC) via productized integration. A key element of the workshop was a detailed matrix outlining the data points required from each device to support proper algorithmic processing in the First Responder (DNA) applications; this formed the basis for follow-on signal list definition efforts. To this end, a foundational understanding of the overall model build process was also established. All parties were keenly aware that the signal list definition was central to forward project momentum and that numerous iterations of a model build would be required for stability and full device inclusion through the integrated D-SCADA. At the close of the workshop, KCP&L had a better understanding of what additional data requirements needed to be compiled and provided as it became available. Siemens and Intergraph left with a better defined set of requirements that they could use to begin their efforts.

During the InService Integration workshop there were also several discussions regarding the AMI, CIS, and how both integrate with the OMS and CAD. There were additional discussions on accessing data from the CIS in a format as required by Intergraph and the usage of MQ interface for AMI and MDM communications. KCP&L and Intergraph had substantial discussion on alarming and the required applications that would generate alarms on the Integrated UI from the native InService systems and the various other systems that would be integrated with the CAD. The DNA applications that were to be incorporated into the UI and their data requirements were also discussed and determined. Finally, all involved parties worked on technical specifications to ensure coordinated development of the interfaces to develop the standards-based messages that would be used to exchange the agreed upon information.

KCP&L concluded the workshop series with the recognition that a detailed signal list was required to configure specific points applicable to specific devices. KCP&L started by detailing those points required by Siemens for the First Responder applications to run. However, KCP&L found there to be many additional data points that could be brought back from each of the devices to the data concentrator. These additional points and resulting analytic possibilities were determined to possibly increase situational awareness for operators and were considered for display to the user. KCP&L conducted numerous discussions to establish internal agreement on the set of points that might be useful for operational activities outside of the DNA applications and provided these finalized signal lists to Intergraph and Siemens for their configuration efforts.

2.2.4.1.1.2 System and Interface Configuration

After establishing requirements, configuration considerations, environmental parameters, and a schedule fully recognizes and accommodates dependencies, then development and configuration efforts could begin in earnest. Both Phases 1 and 2 followed the same configuration approach. Intergraph consolidated all configuration data provided along with all requirements and began working

independently in the VENDOR environment. Numerous iterations of configuration and isolated testing were performed to establish preliminary functionality. As conditions warranted, Intergraph coordinated joint working sessions with Siemens to work through integration efforts with the D-SCADA system (also co-located in the VENDOR environment). For Phase 3 scope, additional working sessions were conducted with another Siemens team responsible for the First Responder capabilities to ensure proprietary integration with that system was working as expected. Later, as the preliminary configurations were coming together, KCP&L facilitated daily working sessions between KCP&L, Siemens, and Intergraph to ensure a comprehensive and synchronized understanding of the deployment in some of its most nuanced ways. Shared-desktop technology (WebEx) was used extensively to enable these conversations between remote participants by allowing everyone to see the same system function, defect, or configuration process.

2.2.4.1.1.3 Data Model Migration

While numerous configuration efforts were vital pre-requisites to a functional system, a particularly laborious component was the model build process. The data model leveraged signal list definitions and data from CAD (Intergraph's I/Dispatcher) to ensure that point data is fully synchronized between the systems and the real world devices resulting in a virtual network model. Leveraging proprietary scripts, CAD (I/Dispatcher) would extract this key data and compile it into a format which would be staged on the server. D-SCADA would then transfer the staged data for load into its internal databases. Initial efforts were performed in the VENDOR environment and numerous iterations were conducted. These iterations served the dual purpose of ensuring a quality automation process (in anticipation of numerous data model migrations supporting ongoing device deployment) as well as overall data quality (to validate properly synchronized between devices allowing for end-to-end communications). The KCP&L project team worked diligently with Siemens and Intergraph to understand the data model propagation as well as the behind-the-scenes implications of various configurations. Of particular challenge for this functionality, was the significant manual effort expended to ensure that the D-SCADA could properly synchronize communications with the CAD (I/Dispatcher) and the DDC (SICAM). The CAD referenced points by their ICCP name and the DDC referenced points by their 61850 name or 61850-like name for the DNP field devices. The D-SCADA was then a repository for what the team nicknamed the 'Marriage File' which was the central configuration that mapped the ICCP point names with their corresponding 61850 point names to support cross-platform connectivity. Through many iterations, these configurations were stabilized, but it consumed far more time than initially planned.

2.2.4.1.1.4 Training

The KCP&L team learned a tremendous amount during the workshops and joint configuration sessions. However, formalized training was still deemed very important to allow KCP&L users to prepare for formalized testing efforts and ultimately successful operation of the system. Sessions were conducted in-person and numerous training manuals were available to aid the process. In addition, given the previously established successes with WebEx, KCP&L leveraged this technology in a two-fold manner: 1) many training sessions were broadcast via WebEx which allowed targeted vendor subject matter experts to augment materials presented by the official trainer and 2) training was recorded allowing for ease of referencing back to better understand an explanation or sequence of events. The following table outlines training sessions conducted for Consolidated UI functionality.

Training Course	Dates
I/Dispatcher Training (Intergraph)	07/31/2012 through 08/02/2012
Tester Training (Intergraph and Siemens)	08/13/2012 through 08/14/2012
Alarm Configuration (Intergraph)	10/8/2012
Switch Planning (Intergraph)	10/9/2012 through 10/10/2012

2.2.4.1.1.5 Testing

As outlined above, the more advanced training sessions provided an opportunity for in-depth reviews of functionality to learn how the system is operated. In addition, due to the significantly advanced configuration by this time, the training sessions in the VENDOR environment also provided an opportunity for KCP&L's testing team to select a subset of tests from the formalized test books and review their workability during the training sessions. Additionally, Siemens and Intergraph performed an extensive "Pre-FAT" test where they internally verified that all functionality listed in the test books were working as expected. Formal testing efforts commenced with the Phase 1 Factory Acceptance Testing (FAT) where KCP&L staff travelled to Siemens facility and watched a demonstration of the CAD capabilities along with the D-SCADA with the timestamp generated from a device going through the DDC, D-SCADA and displayed on the CAD. The highest criticality defects were immediately rectified and the servers were sent to KCP&L for installation to the Midtown Substation (DEMO Environment). The system was stabilized and a robust Site Acceptance Testing (SAT) was performed to ensure that the systems were able to properly transmit device monitoring signals between servers.

Later, as configuration progressed, Phase 2 FAT was performed but deviated slightly as required by the defined scope. Specifically, substation devices remained at the Siemens facility and this time testing ensured appropriate monitor and control capabilities. Field devices were tested differently, as the devices remained in KCP&L facilities (LAB Environment). The field devices were connected to a WAN and then they communicated with SICAM, D-SCADA, and CAD in the Siemens facility. This testing required some portion of the test team to remain at KCP&L to verify synchronization with the test efforts being conducted at Siemens. Again, the highest criticality defects were immediately rectified and additional servers were then sent to KCP&L for installation to the Midtown Substation (DEMO Environment). The system was again stabilized and a robust SAT was performed to ensure that the systems were able to properly transmit monitoring and control signals to/from substation and field devices. Throughout the FAT and SAT for both phases, where needed, defects were documented and logged with a tag corresponding to the appropriate testing effort.

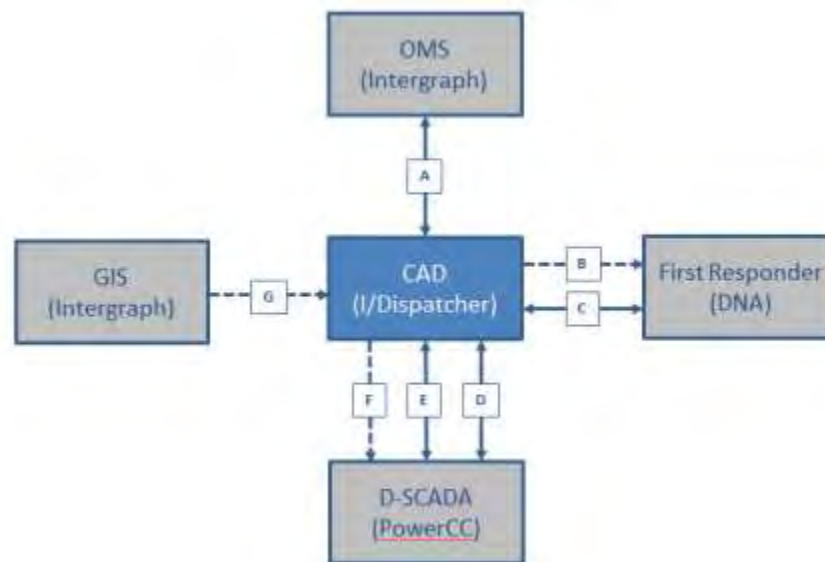
Finally, during Phase 3, the display capabilities of the Consolidated UI were pushed to new territories with the added functionality of displaying algorithmic results from Siemens DNA. Using new screens and new interfaces, a pre-FAT testing effort was again pursued, but this time as a joint weekly session between Siemens, Intergraph, and KCP&L to review the capabilities. Each week a different advanced application was reviewed which allowed all teams properly focus on the nuances of the particular capability. Having resolved many initial defects, FAT was conducted in the VENDOR environment and went rather smoothly based on the time invested during pre-FAT. At that point, all configurations were migrated to the DEMO environment where the comprehensive and fully integrated system could be tested as part of Site Acceptance Testing (SAT).

All testing efforts resulted in numerous defects being documented where functionality deviated from established requirements. Intergraph worked to remediate these defects as soon as they were discovered and continued working to remediate throughout 2013; as variances were fixed, new service packs would be compiled on a regular schedule and installed to KCPL's LAB and DEMO environments for re-testing.

2.2.4.1.2 Integration

An overview of UI/CAD system-to-system interfaces and applicable messages is illustrated in Figure 2-49.

Figure 2-49: KCP&L SmartGrid Demonstration Project CAD Integration



The CAD (I/Dispatcher) is the core point of convergence in the DMS where pertinent data is aggregated and displayed to the end-user to take action. This special integrated UI is the command and control center with a common user environment. It consolidates multiple control room systems into one user interface to improve situational awareness and reduce human error. The Integrated UI will provide comprehensive dialog for SCADA Alarms, Crew Status, Pending Jobs, and Work Dispatched. The UI analyzes and displays data to the user as applicable from the various other component systems of the DMS which are integrated with it. The integration touch points for UI are as follows:

- A. OMS/CAD Proprietary Integration: A bi-directional interface that allows outage information, crew data, new / pending jobs, and outage aggregations / predictions to be sent from the OMS to the CAD for the user to view and take appropriate action. This interface also allows the user to access meter data from the MDM, send meter pings, and receive power status verification messages from the meter through the OMS. All data exchanges are automatically transmitted through Intergraph's proprietary technology.
- B. DNA/CAD Data Model Propagation: As part of the overall network and data model propagation process from GIS to the DMS suite of systems to have an updated data model across all systems, the key details of the network model are prepared in CAD and then transferred to DNA. This process is performed on an ad-hoc and largely manual basis.
- C. DNA/CAD UI Integration: A bi-directional interface allowing for DNA algorithmic results and recommendations to be forwarded on for display to the user. The interface also allows user selections and configurations to be passed from the CAD User Interface to DNA. All data exchanges in this interface are via Message Queues (MQ).
- D. D-SCADA/CAD Alarm & Tag Propagation: A bi-directional interface allowing alarm and tag configurations to be sent from CAD to the D-SCADA for enforcement. The interface also allows for any alarm / tag violation notifications to be transmitted to CAD for a user to view and take appropriate action. All data exchanges in this interface are automatically transmitted via Message Queues (MQ).

- E. D-SCADA / CAD Monitor and Control Propagation: A bi-directional interface allowing for D-SCADA point monitoring details to be provided to CAD so that it has all updated information for user display. The interface also allows for any controls resulting from user selections to be transmitted to D-SCADA for further propagation to devices in the field. All data exchanges in this interface are automatically transmitted via ICCP. Numerous configurations were required on custom XML files to support end-to-end communications with devices.
- F. D-SCADA / CAD Data Model Propagation: As part of the overall network and data model propagation process from GIS to the DMS suite of systems, the key details of enabled devices, their correlated signal list configuration, and the broader network connectivity model are prepared in CAD and then transferred to the D-SCADA (IMM subcomponent). This process is performed on an ad-hoc and largely manual basis using Oracle SQL.
- G. GIS/CAD Data Model Propagation: This is the first step in the overall network and data model propagation from GIS to the DMS Suite of Systems. This one way interface compiles pertinent GIS data and packages it for consumption by CAD where it is further augmented to achieve a broader network model. This process is performed on an ad-hoc and largely manual basis using Oracle SQL and other proprietary tools.

2.2.4.1.3 Post-Implementation Operational Issues

Following the standup, integration, and preliminary testing of the CAD system, numerous post-implementation operational issues needed to be mitigated and considered. These issues are as follows:

- **Productized Integration** – At the inception of this demonstration project, deployment plans were based on the premise of a commercially mature, productized integration of the CAD capabilities with the First Responder (DNA), D-SCADA, OMS and GIS capabilities. However, this productized integration had only been deployed at one other site, which resulted in a larger stabilization effort in KCP&L’s demonstration environment. This continued into the post-operational period, where very specific real-world situations conspired to result in system instability situations. Many of these situations could have been avoided had this system been deployed and fully tested in an enterprise operational context prior to implementation at KCP&L.
- **Software Updates** – Upon installation of the system at KCP&L, efforts were commenced to stabilize the system, perform Site Acceptance Testing (SAT), and begin operating the system as situational opportunities arose. Throughout this period, numerous system deficiencies were discovered, and updates were proactively provided by the software vendor. These necessitated configuration fixes and/or service packs to be delivered by the software vendor. These fixes were delivered by the software vendor together for the OMS and CAD as they are closely integrated with each other. A list of all the service packs installed by KCP&L is listed below:

Build No.	Date	Content
A	4-1-2012	Initial Consolidated UI Installation for Phase 1 SAT
B	9-15-2012	Reinstallation of Consolidated UI with numerous fixes to accommodate advances for Phase 2 SAT
11	2-28-2013	Reinstallation of Consolidated UI with numerous fixes to accommodate advances for Phase 3 SAT
12	4-30-2013	Core UI variances needed to enable stability and advance SAT
13	6-30-2013	Core UI variances needed to enable stability and advance SAT
14	8-30-2013	Remaining high-priority variances to complete SAT
14A	9-16-2013	Fix for SCADA values blank in Feature Information Window
15	11-12-2013	Miscellaneous defect fixes to further stabilize system

- **Network Model Data Migrations** – During initial configuration and build efforts, only a subset of planned, end-state devices and their corresponding points were captured in the data model. This was done to reflect the limited number of deployed devices at configuration inception, but also to limit the complexity of model connectivity while establishing process stability. However, in our preliminary configuration and test environments, many of the attempted data migrations with this limited data set took significant time and effort to implement and stabilize. When the system was transferred to KCP&L, it maintained this subset of devices and due to the known challenges with the data migration process, incremental data migrations were not pursued for some time. This allowed time to complete device deployments in the field as well as setup and conduct numerous additional test data migrations in our LAB environment prior to conducting a data migration in our DEMO environment. In retrospect, the lack of a complete data model was a hindrance requiring certain workarounds, but it was still preferable to the potentially long time periods of environment inaccessibility waiting for the data migration to re-stabilize.
- **Tuning and Configurations** – As the system was installed and stabilized at KCP&L, the Integrated UI (CAD) required several iterations of tuning and configuration to achieve a reasonable level of stability. Due to time constraints for implementation, several glyphs, job tables, meter data, and device locations were not initially “polished”, but these items were prioritized and refined as needed. Furthermore, each functional alarm in InService had to be manually configured InService; a tedious process which was pursued as staff availability allowed. Finally, numerous switch statuses on the CAD database had to be maintained during data migrations as point changes during this time could result in data synchronization issues.
- **Device Connectivity and Directionality** – When migrated from the GIS, the map data and network data model did not meet the DNA model requirements with respect to connectivity and flow of power. While the level of detail was sufficient for legacy applications, the required detail for DMS applications was more nuanced by orders of magnitude. As such, the migration process required multiple iterations to ensure appropriate connectivity in the distribution infrastructure. During subsequent testing with complete integration, it was further realized that the connectivity and directionality of power readings from reclosers were necessary for the First Responder Applications to properly function and analyze data. As the Integrated UI was the core integration point from where the data model was transmitted to the rest of the system, the data model in CAD had to be modified to include device directionality from the GIS and properly display it for end-user consumption.
- **Signal Point List Updates are Not Dynamic**– As the project progressed, at several stages additional devices were added or deleted on to the system. At other times, data points on existing devices were modified based on new learnings and better understanding of data requirements for the system. In all cases, the Signal Points List for these devices was managed in the InService database and migrated onto the rest of the systems as part of the data migration process. This process was laborious as each point change for an existing or new device had to be manually entered into the Signal Point List tables without any templates or options to replicate existing device configurations. The availability of standard device templates for signal lists and the ability to copy existing points list to new devices would have made the process much more dynamic and less prone to error.
- **Field Device Communications Instability** – Consolidated UI (CAD) capabilities were ultimately dependent on the quality of SICAM and further downstream field device / substation data. While there were a handful of issues expressly tied to CAD’s own ability

to consistently display all current data from each field device, a majority of issues were due to these other systems and evidenced themselves in CAD indirectly. As discussed in greater detail in the SICAM and Tropos build sections, significant effort was put forth to stabilize the communications channels to field devices and ensure robust transmission of real-time data. At times where instability was significant, KCP&L's ability to have full monitor and control capability was limited and focus was shifted back to SICAM / Tropos stabilization.

To be updated in future releases of this report.

2.2.4.1.4 Lessons Learned

Throughout the build and stabilization of the Integrated UI system, numerous considerations were realized and should be noted for future deployments of this sort. These Lessons Learned are as follows:

- **UI Maturity and Analytics Presentation** – The Integrated UI used for the DMS integrates several control room systems and applications into a single user interface as discussed above. This concept is relatively new and it is understood to be a still evolving representation and is yet to reach its zenith, but greater usage and feedback shall continually help improve its usability. Navigation of multiple windows and pop ups could be made more efficient for users. Analytics data from DNA applications and other systems could be shown in a more informative manner, particularly, with other presentation tools and styles such as graphs, charts, and device hover data to improve situational awareness for the user. Over the period of implementation, there have been several improvements based on KCP&L feedback and the user interface is already en route to evolving into a more ideal DMS UI.
- **Quality of Real Time Values** – During the implementation, it was observed that the user has access to view all the data points from the field on the integrated UI but is unable to determine the quality or currency of this data. The data points are reported to the system from the field only by exception or periodically. If a device has stopped communicating with the system, then CAD displays the last value reported by D-SCADA (good or bad) to the user without a quality or time stamp. The user cannot directly verify the quality (good, bad, telemetered, non-telemetered, entered etc.) of the data currently being shown in CAD from within the application. To ensure progress, the testers and users at KCP&L have been directly using the D-SCADA application and monitoring the DDC System for establishing the quality of an analog, but from the perspective of an enterprise-wide deployment this would be less than ideal.
- **Initial Signal List Points Definition** – In order to configure the points lists and tables in UI/CAD, it was necessary to conduct an analysis of points to be captured for each group of devices (e.g. reclosers or cap banks in aggregate). To support First Responder capabilities, a relatively small subset of available points were required. However, considerations from groups such as asset management, engineering, and operations all provided input on how data could be used. As such, the decision was made to have the D-SCADA bring back and manage a large number of points available from every connected device and send them to UI/CAD via ICCP. Unfortunately, this volume of data stretched our technology to its limits resulting in numerous challenges to ensure stability through the integrated solution. While more of an issue for some other systems in KCP&L's implementation, as applicable to UI/CAD, the large number of displayed points became unwieldy from an operational perspective. The UI/CAD display needs to incorporate an ICCP point priority filtering capability to allow the grid operator to control the number of points actively displayed.

- **Communication Protocols and Naming Conventions** – The ICCP protocol was used for transmitting control and monitoring data between the integrated UI (CAD) and the D-SCADA system. The 61850 protocol was used to transmit control and monitoring data to the substation and field device from the D-SCADA. Each of these protocols had different naming conventions and the data points from the same device had to be assigned different names when moving from one system to another. This difference in name required the creation of a ‘marriage’ file placed in the DMS that aligned the different names for the same data point. The data migration process and SCADA list modification was in itself a complicated process which de-stabilized the system for substantial amounts of time. Further support of the marriage file with several names for the same data point created further data management issues. In the future, continuing evolution of technology and further adoption of standards should help to make implementations simpler.
- **Incremental Device Communications Configurations** – Where the prior note highlights the challenges in defining points applicable to an entire class of field device (e.g. reclosers or cap banks), KCP&L also encountered challenges when establishing communications to a single incremental device being installed. The points lists would be defined, but the configurations and corresponding synchronization between systems was highly manual. This required significant coordination and attention to detail progressively verifying harmonization at each step of the communication pathway to ensure proper spelling of points and cross-mapping DNP names with 61850 names. These efforts to enable substation and field device communications were a notable contrast to the deployment of incremental AMI meters in the field. In the same way that meters would self-identify and propagate communication point capabilities, other distribution devices would benefit from these same capabilities through to all systems with which they communicate.
- **Incremental Network Model Management** – In addition to the two previous considerations and as mentioned as a post-operational issue, the installation of a new network data model had significant timing considerations and complexity as it was an all-or-nothing implementation. While this step was vital to allow enabled D-SCADA capabilities to be geospatially displayed on the Consolidated UI, the team was hesitant about deploying any new field devices or circuits into the maps because the entire network model needed to be re-deployed. The result of which was significant system downtime to install and re-stabilize the system. In this context, an incremental network management migration capability would have significantly greater value to a real-time system like the Consolidated UI as it would allow the system to maintain its functionality for vast portions of the service territory while only a small, targeted section is having its underlying connectivity details updated.
- **ICCP & MQ Connectivity Failure Awareness** – As the central device status display and control broker in the integrated solution, the CAD heavily uses ICCP and MQ protocols to transmit and receive data from the D-SCADA. Independently, any singular interface has relatively high reliability and stability. Unfortunately, given the vast integration of this project, the small instabilities incumbent in each interface conspire with each other and multiply to a general state of frequent communication instability across the entire platform. From a user perspective, the systems only reactively show that end-to-end communications are not working. Upon notification to the project support team, a more detailed investigation is conducted to resolve. However, each instance of communication failure erodes user confidence in the system’s ability to reliably perform when it matters. As a result, it has become apparent that as operations become more reliant on highly integrated systems such as this, it is vital to have additional capabilities serving as an IT

Network Operations Center. It is envisioned that this function would proactively monitor system communications and ensure consistently higher levels of platform-wide communications and system stability.

- **Cross-Platform Time Synchronization** – Building on the communication stability challenges mentioned previously, a complicating factor in the diagnosis was the general synchronization of time stamps across all devices and systems. A synchronized time stamp is very important in this type of diagnostic to see when certain signals depart one system and arrive at another. In a context of multiple communications from different devices all being recorded in communications logs, if one system is off by even a couple seconds, then the analysis of different data exchanges is complicated by crisscrossed message streams. The KCP&L time synchronization effort was particularly challenged because different systems used multiple time-synch mechanisms: Substation devices from satellite clock, servers derived from network time, field devices synched to SICAM. KCP&L's current enterprise configuration doesn't have a strict requirement for synchronized data as the end-state use of this information is more forgiving in its application. However, this legacy challenge became of greater concern with the advanced applications of the DMS as its algorithms have an increased reliance on timely and synchronized inputs to achieve expected results. Significant effort was put forth to achieve synchronization throughout our demonstration footprint and additional efforts would be required to establish the importance of this throughout KCP&L's culture if it were to be expanded enterprise wide.
- **Hierarchical Controls** – The overall DMS System has several modes of controlling the field devices such as Complete User Control, Open Loop Control, and Closed Loop Control. Furthermore, considerations of Centralized Control (from the control center) and Distributed Control (from the DCADA located at the substation) pervade this implementation. The user or operator is the supreme authority for deciding who is in control: a user or an autonomous system. The user can assign control to an application and take it away at will. The Control UI application hosted on the entire system is utilized to transfer control. The Control UI can transfer control between user and DNA at a higher level but is disconnected from the internal workings of DNA. If DNA relinquishes control then neither the DNA nor the user can control the devices until the user assigns the control back in Control UI. Also the user loses control when DNA is assigned control unless he assigns it back on Control UI. This process works but is cumbersome and not operator friendly. With an anticipated future where multiple systems integrate together forming a single DMS, there is a need for a single hierarchical control system that interacts with all systems yet still gives complete authority to operator at needed times.

To be updated in future releases of this report.

2.2.4.2 Distribution-SCADA

The Siemens D-SCADA component provides real-time device and automation information to keep the operating model as close as possible to the real conditions in the field. D-SCADA provides all real-time data services and control agent capabilities for the combined Siemens/Intergraph DMS solution. The following sections provide a summary of the development and configurations that were required to implement and deploy the desired D-SCADA functionality.

2.2.4.2.1 Build

KCP&L's D-SCADA (PowerCC) implementation efforts were launched by assembling a team of highly skilled individuals that would pursue and support the deployment of these advanced applications. To familiarize themselves with the goals of the project, the team began by reviewing previously created Use Cases to understand new processes and anticipated system functions. These Use Case documents were finalized where possible and provided to Siemens to establish their baseline understanding of what KCP&L hoped to achieve with the system implementation. Where clarifications were required, they were addressed during the Design / Configuration Workshops.

In parallel to KCP&L's preliminary use case familiarization efforts, Siemens began establishing its project team to perform the installation. The D-SCADA core capabilities and interfaces are part of a commercially available, productized software implementation which can be configured to the needs of a given customer. By pursuing this "off-the-shelf" philosophy to the maximum degree possible, limited custom design was required. However, the systems did require configuration to accommodate KCP&L's distribution system. In this context, Siemens began identifying key staff and subject matter experts who would be performing the configuration. As there were relatively few implementations of this product, staff began familiarizing themselves with the configuration elements required and documenting questions to be answered in preparation of the actual configuration efforts.

2.2.4.2.1.1 Collaborative Design Sessions

After the preliminary familiarization efforts conducted by KCP&L and Siemens, a workshop was conducted to expedite the configuration effort. Siemens, Intergraph, and KCP&L jointly participated in this workshop to ensure that all parties were in agreement about the design and configurations to be pursued. Specifically, analysis was performed on Intergraph's Computer Aided Dispatch (CAD) application (I/Dispatcher) and how it would work with Siemens' D-SCADA (PowerCC) via productized integration. A key element of the workshop was a detailed matrix outlining the data points required from each device to support proper algorithmic processing in the First Responder (DNA) applications; this formed the basis for follow-on signal list definition efforts. To this end, a foundational understanding of the overall model build process was also established. All parties were keenly aware that the signal list definition was central to forward project momentum and that numerous iterations of a model build would be required for stability and full device inclusion through the integrated D-SCADA. At the close of the workshop, KCP&L had a better understanding of what additional data requirements needed to be compiled and provided as it became available. Siemens left with a better defined set of requirements that they could use to begin their efforts.

The DMS/DERM interface, however, differed from the productized solution in that it is a custom interface between Siemens and OATI for this demonstration project. In order to design the message exchanges for this interface, KCP&L, Siemens, and OATI met for several days to create additional use cases for the possible scenarios. The main scenarios that were detailed included:

- Initialization between DMS and DERM – used the first time a new database is applied or after one of the systems has been restarted
- Feeder load management – also called "studycase," this is an exchange between the DMS and the DERM done in a planning mode

- Feeder load shed – also called “emergency,” this is an exchange between the DMS and the DERM done in real time when an overload has occurred

Upon completion of the DMS/DERM use cases, all parties worked on technical specifications for these interfaces to develop the standards-based messages that would be used to exchange the agreed upon information.

KCP&L concluded the series of workshops with the recognition that a detailed signal list was required to configure specific points applicable to specific devices. KCP&L started by detailing those points required by Siemens for the First Responder applications to run. However, KCP&L found there to be hundreds of additional data points that could be brought back from each of the devices to the data concentrator. KCP&L conducted numerous discussions to establish internal agreement on the set of points that might be useful for operational activities outside of the DNA applications and provided these signal lists to Siemens for their configuration efforts.

2.2.4.2.1.2 System and Interface Configuration

After establishing requirements, configuration considerations, environmental parameters, and a schedule that recognizes and accommodates dependencies, then development and configuration efforts could begin in earnest. Both Phases 1 and 2 followed the same configuration approach. Siemens consolidated all configuration data provided along with all requirements and began working independently in the VENDOR environment. Numerous iterations of configuration and isolated testing were performed to establish preliminary functionality. As conditions warranted, Siemens coordinated joint working sessions with Intergraph to work through integration efforts with the CAD system (also co-located in the VENDOR environment). Additional working sessions were conducted with another Siemens team responsible for the First Responder capabilities to ensure proprietary integration with that system was working as expected. Later, as the preliminary configurations were coming together, KCP&L facilitated daily working sessions between KCP&L, Siemens, and Intergraph to ensure a comprehensive and synchronized understanding of the deployment in some of its most nuanced ways. Shared-desktop technology was used extensively to enable these conversations between remote participants by allowing everyone to see the same system function, defect, or configuration process.

2.2.4.2.1.3 Data Model Migration

While numerous configuration efforts were vital pre-requisites to a functional system, a particularly laborious component was the model build process. The data model leveraged signal list definitions and data from CAD (Intergraph’s I/Dispatcher) to ensure that point data is fully synchronized between the systems and the real world devices resulting in a virtual network model. Levering proprietary scripts, CAD (I/Dispatcher) would extract this key data and compile it into a format which would be staged on the server. D-SCADA would then transfer the staged data for load into its internal databases. Initial efforts were performed in the VENDOR environment and numerous iterations were conducted. These iterations served the dual purpose of ensuring a quality automation process (in anticipation of numerous data model migrations supporting ongoing field device deployments) as well as overall data quality (to validate properly synchronized data between devices allowing for end-to-end communications). Upon stabilization of the base model build, efforts then commenced to support the model migration to the DERM and progressed similarly; the model was extracted from D-SCADA, staged for DERM consumption, transferred and loaded to DERM, and repeated as necessary. The KCP&L project team worked diligently with Siemens, Intergraph, and OATI to understand the data model propagation as well as the behind-the-scenes implications of various configurations. Of particular challenge for this functionality was the significant manual effort expended to ensure that the D-SCADA could properly synchronize communications with the CAD (I/Dispatcher) and the DDC (SICAM). The CAD referenced points by their ICCP name and the DDC referenced points by their 61850 name. The D-SCADA was then a repository for what the team nicknamed the “Marriage File” which was the central configuration that

mapped the ICCP point names with their corresponding 61850 point names to support cross-platform connectivity. Through many iterations, these configurations were stabilized, but it consumed far more time than initially planned.

2.2.4.2.1.4 Training

The KCP&L team learned a tremendous amount during the workshops and joint configuration sessions. However, formalized training was still deemed very important to allow KCP&L users to prepare for formalized testing efforts and ultimately successful operation of the system. Sessions were conducted in-person and numerous training manuals were available to aid the process. In addition, given the previously established successes with WebEx, we leveraged this technology in a two-fold manner: 1) many training sessions were broadcast via WebEx which allowed targeted vendor subject matter experts to augment materials presented by the official trainer and 2) training was recorded allowing for ease of referencing back to better understand an explanation or sequence of events. The following table outlines training sessions conducted for D-SCADA functionality.

Training Course	Dates
I/Dispatcher Training (Intergraph)	07/31/2012 through 08/02/2012
Tester Training (Siemens)	08/13/2012 through 08/14/2012

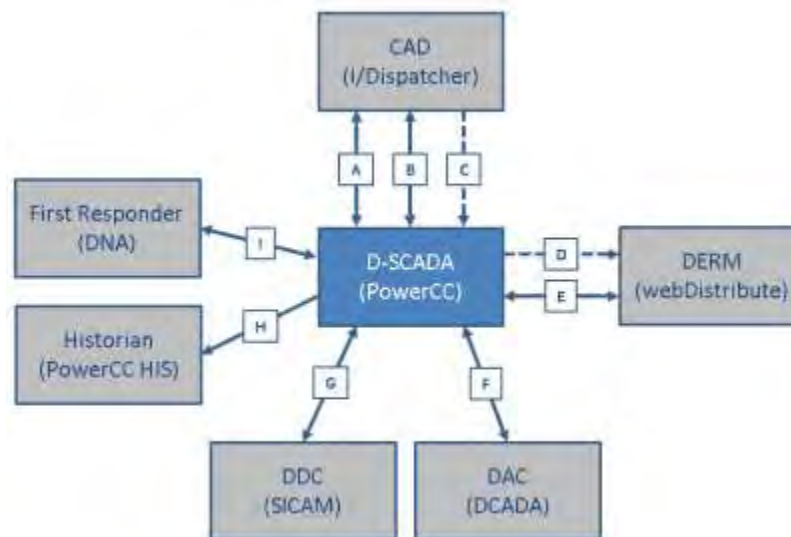
2.2.4.2.1.5 Testing

As outlined above, the more advanced training sessions provided an opportunity for in-depth reviews of functionality to learn how the system is operated. In addition, due to the significantly advanced configuration by this time, the training sessions in the VENDOR environment also provided an opportunity for KCP&L's testing team to select a subset of tests from the formalized test books to ensure the accuracy of the configuration. Additionally, Siemens performed an extensive "Pre-FAT" test where they internally verified that all functionality listed in the test books was working as expected. Formal testing efforts commenced with the Phase 1 Factory Acceptance Testing (FAT) where KCP&L staff travelled to the Siemens facility and watched a demonstration of the D-SCADA capabilities originating with substation device value changes through SICAM and D-SCADA and culminating with a display in the CAD. The highest criticality defects were immediately rectified and the servers were sent to KCP&L for installation to the Midtown Substation (DEMO Environment). The system was stabilized and a robust Site Acceptance Testing (SAT) was performed to ensure that the systems were able to properly transmit device monitoring signals between servers. Later, as configuration progressed, Phase 2 FAT was performed but deviated slightly as required by the defined scope. Specifically, substation devices remained at the Siemens facility and this time testing ensured appropriate monitor and control capabilities. Field devices were tested differently, as the devices remained in KCP&L facilities (LAB Environment). The field devices were connected to a WAN and then they communicated with SICAM and D-SCADA in the Siemens facility. This testing required some portion of the test team to remain at KCP&L to verify synchronization with the test efforts being conducted at Siemens. Again, the highest criticality defects were immediately rectified and additional servers were then sent to KCP&L for installation to the Midtown Substation (DEMO Environment). The system was again stabilized and a robust SAT was performed to ensure that the systems were able to properly transmit monitoring and control signals to/from substation and field devices. With stabilized communications in both environments, efforts shifted to testing communications with the DERM. See section 2.2.5.1.1 for details about the DMS/DERM integration and testing efforts. Throughout the FAT and SAT for both phases, where needed, defects were documented and logged with a tag corresponding to the appropriate testing effort.

2.2.4.2.2 *Integration*

An overview of D-SCADA system-to-system interfaces is illustrated in Figure 2-50.

Figure 2-50: KCP&L SmartGrid Demonstration Project D-SCADA Integration



The D-SCADA capabilities are central to many functions of the larger integrated system. In particular, it is a specialized system managing real-time data and acts as the central broker ensuring that necessary data is appropriately exchanged between different DMS components. The integration touch points for the D-SCADA applications are as follows:

- A. D-SCADA/CAD Alarm & Tag Propagation: A bi-directional interface allowing alarm and tag configurations to be sent from CAD to the D-SCADA for enforcement. The interface also allows for any alarm / tag violation notifications to be transmitted from D-SCADA to CAD for a user to view and take appropriate action. All data exchanges in this interface are automatically transmitted via Message Queues (MQ).
- B. D-SCADA/CAD Monitor and Control Propagation: A bi-directional interface allowing for D-SCADA point monitoring details to be provided to CAD so that it has all updated information for user display. The interface also allows for any controls resulting from user selections to be transmitted to D-SCADA for further propagation to devices in the field. All data exchanges in this interface are automatically transmitted via ICCP. Numerous configurations were required on custom XML files to support end-to-end communications with devices.
- C. D-SCADA/CAD Data Model Propagation: As part of the overall network and data model propagation process from GIS to the DMS suite of systems, the key details of enabled devices, their correlated signal list configuration, and the broader network connectivity model are prepared in CAD and then transferred to the D-SCADA (IMM subcomponent). This process is performed on an ad-hoc and largely manual basis using Oracle SQL.
- D. D-SCADA/DERM Data Model Propagation: In addition to the overall network and data model propagation process from GIS to the DMS suite of systems, the DERM system must have its data model synchronized with D-SCADA to make accurate calculations of its own. The network connectivity model and associated loads are transferred from the DMS to the DERM using a manual CIM RDF export. Generation of the CIM RDF file is done in the Information Model Management (IMM) and then exported via file transfer to OATI. This

process is performed whenever a new data model is taken from the GIS, and it requires massaging from OATI to ensure that it's properly digested by the DERM.

- E. D-SCADA / DERM Dynamic Data Exchange: In addition to the static model data that's exchanged between the DMS and the DERM, the two systems also exchange a number of dynamic messages on an as-needed basis. The DERM sends and receives Web services messages, whereas the DMS sends and receives JMS (Java Messaging Service) messages, so adapters within KCP&L's Enterprise Service Bus (ESB) serve as translators between the two systems. The dynamic data exchanged between the DMS and the DERM can be categorized by the following interfaces:
- Network Topology Interface – Upon initial synchronization of the two databases, the DERM is notified about each switch state change.
 - Distribution Power Flow (DPF) Interface – The DPF interface allows the DERM to query DPF results from the DMS. For scheduled DERM events, the DERM needs calculated overloads on an hourly basis. The DPF interface generates the data and makes it available to DERM. Additionally, violations are published to the DERM in real time.
 - Study Case Interface – When study cases are created in the DMS, a study case needs to be created in the DERM, as well. This interface provides the messages to do so.
 - Demand Response (DR) Event Interface – DR events affect power flow results, so DERM needs an interface for publishing DR events to the DMS.
 - Battery Interface – The DMS is used as the control authority for the battery, so this interface is used to dispatch DR events for this purpose.
- F. D-SCADA / DAC Data Model and Delegated Control Propagation: A bi-directional interface allowing for data model updates to be propagated to the DAC as required to stay synchronized during real-time changes (particularly for cut / jumper updates). The interface also allows for transmission of delegated control permissions to be exchanged between systems to ensure synchronization of SCADA mastership. All data exchanges in this interface are automatically transmitted via proprietary protocols.
- G. D-SCADA / DDC Monitor and Control Propagation: A bi-directional interface allowing for D-SCADA point monitoring details to be provided by the DDC (SICAM) so that it has all updated information for propagation to other systems. The interface also allows for any controls resulting from upstream user selections to be transmitted to the DDC (SICAM) for further propagation to devices in the field. All data exchanges in this interface are automatically transmitted via 61850 protocols.
- H. D-SCADA / HIS Data Archival via Oracle: A one-way interface allowing for D-SCADA point monitoring details to be provided to the Historian so that it has all updated points list details for each configured device. This archive then provides the basis for analysis of all DMS capabilities through the demonstration period. All data exchanges in this interface are automatically transmitted using Oracle SQL.
- I. D-SCADA / DNA Monitor & Control Propagation: A bi-directional interface allowing for D-SCADA point monitoring details to be provided to DNA so that it has all updated information for algorithmic processing. The interface also allows for any controls resulting from algorithmic processing to be transmitted from DNA to D-SCADA for further propagation to devices in the field. All data exchanges in this interface are via Siemens proprietary technology.

2.2.4.2.3 Post-Implementation Operational Issues

Following the standup, integration, and preliminary testing of the D-SCADA (PowerCC) system, numerous post-implementation operational issues needed to be mitigated and considered. These issues included the following:

- **Productized Integration** – At the inception of this demonstration project, deployment plans were based on the premise of a commercially mature, productized integration of the D-SCADA capabilities with the First Responder (DNA), CAD (I/Dispatcher), DAC (DCADA), and DDC (SICAM) capabilities. However, this productized integration had only been deployed at one other site, which resulted in a larger stabilization effort in KCP&L’s real-world environment. This continued into the post-operational period, where very specific real-world situations conspired to result in system instability situations. Many of these situations could have been avoided had this system been deployed and fully tested in an enterprise operational context prior to implementation at KCP&L.
- **Software Updates** – Upon installation of the system at KCP&L, efforts were commenced to stabilize the system, perform Site Acceptance Testing (SAT), and begin operating the system as situational opportunities arose. Throughout this period, numerous system deficiencies were discovered which necessitated fixes to be delivered by the software vendor. Due to the co-mingled architectural nature of the DMS sub-systems, these fixes were delivered and installed as part of several subsequent “builds”. Efforts were initially pursued to deploy updates frequently, but were scaled back due to the complexity of regression testing functionality, completing deployment to all servers and UIs, and then re-establishing stability. A list of builds installed by KCP&L is listed below:

Build No.	Date	Content
80	2-19-2013	Initial DNA KCP&L site installation
90	3-14-2013	Core D-SCADA variances needed to enable DNA functionality
93	4-17-2013	Core D-SCADA variances needed to enable DNA functionality
100	5-30-2013	Core DSSE / DSPF stability variances; preliminary HIS configuration
105	7-26-2013	Prioritized DSSE, DSPF, VVC variances
108	8-22-2013	DMS / DERM heartbeat & battery functionality
116	10-7-2013	Comprehensive delivery of all DSSE, DSPF, and VVC variances
121	11-27-2013	Comprehensive delivery of all outstanding variances

- **Network Model Data Migrations** – During initial configuration and build efforts, only a subset of planned, end-state devices and their corresponding points were captured in the data model. This was done to reflect the limited number of deployed devices at configuration inception, but also to limit the complexity of model connectivity while establishing process stability. However, in our preliminary configuration and test environments, many of the attempted data migrations with this limited data set took significant time and effort to implement and stabilize. When the system was transferred to KCP&L, it maintained this subset of devices and due to the known challenges with the data migration process, incremental data migrations were not pursued for some time. This allowed time to complete device deployments in the field as well as setup and conduct numerous additional test data migrations in our LAB environment prior to conducting a data migration in our DEMO environment. In retrospect, the lack of a complete data model was a hindrance requiring certain workarounds, but it was still preferable to the potentially long time periods of environment inaccessibility waiting for the data migration to re-stabilize.
- **Field Device Communications Instability** – D-SCADA (PowerCC) capabilities are dependent on the quality of SICAM and further downstream field device / substation data. While there were a handful of issues expressly tied to the core D-SCADA capabilities, a majority of issues were due to these other systems and evidenced themselves in D-SCADA. As discussed in greater detail in the SICAM and Tropos build sections, significant effort was put forth to stabilize the communications channels to field devices and ensure robust

transmission of real-time data. At times where instability was significant, KCP&L's ability to have full monitor and control capability was limited and focus was shifted back to SICAM / Tropos stabilization.

To be updated in future releases of this report.

2.2.4.2.4 Lessons Learned

Throughout the build and stabilization of the D-SCADA (PowerCC) system, numerous considerations were realized and should be noted for future deployments of this sort. These Lessons Learned are as follows:

- **Systems require greater modularity** – As mentioned as a post-operational issue, in many cases when a defect fix was delivered it required a fully compiled build to be installed. The project team came to consider this functionality as “Project-ware” instead of “software” recognizing the high level configuration (verging on customization) that seemed to be required to deliver a fix. It would be envisioned that in a more mature software package, core functions would be deliverable and upgradeable in a more compartmentalized fashion, not requiring a full re-installation of the entire integrated software suite (as was required in our First Responder / D-SCADA implementation).
- **Initial Signal List Points Definition** – In order to configure the D-SCADA it was necessary to conduct an analysis of points to be captured for each group of devices (e.g. reclosers or cap banks in aggregate). To support First Responder capabilities, a relatively small subset of available points were required. However, considerations from groups such as asset management, engineering, and operations all provided input on how data could be used. As such, the decision was made to have the D-SCADA bring back and manage a large number of points available from every connected. Unfortunately, this volume of data stretched the DDC and field communication technologies to its limits resulting in numerous challenges to ensure stability through the integrated solution. In retrospect, upon discovery that calculated values are less straining on the infrastructure than device communications, one key approach would have been to review the points list and define a subset of points to be calculated in the DDC instead of telemetered.
- **Incremental Device Communications Configurations** – Where the note above highlights the challenges in defining points applicable to an entire class of field devices (e.g. reclosers or capacitor banks), KCP&L also encountered challenges when establishing communications to a single incremental device being installed. While KCP&L typically knows all of the substation devices that will be in use for the long-term, field devices are deployed in a much more incremental manner. For these incremental field device deployments, the points lists would be defined, but the configurations and corresponding synchronization between systems was highly manual. This required significant coordination and attention to detail, progressively verifying harmonization at each step of the communication pathway to ensure proper spelling of points and cross-mapping DNP names with 61850 names. These efforts to enable substation and field device communications were a notable contrast to the deployment of incremental AMI meters in the field. In the same way that meters would self-identify and propagate communication point capabilities, other distribution devices would benefit from these same capabilities.
- **Incremental Network Model Management** – In addition to the two previous considerations and as mentioned as a post-operational issue, the installation of a new network data model had significant timing considerations and complexity as it was an all-

or-nothing implementation. While this step was vital to allow enabled D-SCADA capabilities to be geospatially displayed on the UI of the OMS component, the team was hesitant about deploying any details about new field devices or circuits because the *entire* network model needed to be re-deployed resulting in significant system downtime to install and re-stabilize. In this context, an incremental network management migration capability would have significantly greater value to a real-time system like the D-SCADA as it would allow the system to maintain its functionality for vast portions of the service territory while only a small, targeted section is having its underlying connectivity details updated.

- **ICCP & MQ Connectivity Failure Awareness** – As the central device status and control broker in the integrated solution, the D-SCADA heavily uses ICCP and MQ protocols to transmit data to other systems. Independently, any singular interface has relatively high reliability and stability. Unfortunately, given the vast integration of this project, the small instabilities incumbent in each interface conspire with each other and multiply to a general state of frequent communication instability across the entire platform. From a user perspective, the systems only reactively show that end-to-end communications are not working. Upon notification to the project support team, a more detailed investigation is conducted to pinpoint and resolve. However, each instance of communication failure erodes user confidence in the system’s ability to reliably perform when it matters. As a result, it has become apparent that as operations become more reliant on highly integrated systems such as this, it is vital to have additional capabilities serving as an IT Network Operations Center. It is envisioned that this function would proactively monitor system communications and ensure consistently higher levels of platform-wide communications and system stability.
- **Cross-Platform Time Synchronization** – Building on the communication stability challenges mentioned previously, a complicating factor in the diagnosis of issues was the general synchronization of time stamps across all devices and systems. A synchronized time stamp is very important in this type of diagnostic to see when certain signals depart one system and arrive at another. In a context of multiple communications from different devices all being recorded in communications logs, if one system is off by even a couple seconds, then the analysis of different data exchanges is complicated by crisscrossed message streams. The KCP&L time synchronization effort was particularly challenged because different systems used multiple time synch mechanisms: Substation devices from satellite clock, servers derived from network time, field devices synched to SICAM. KCP&’s current enterprise configuration doesn’t have a strict requirement for synchronized data as the end-state use of this information is more forgiving in its application. However, this legacy challenge became of greater concern with the advanced applications of the DMS as its algorithms have an increased reliance on timely and synchronized inputs to achieve expected results. Significant effort was put forth to achieve synchronization throughout our demonstration footprint and additional efforts would be required to establish the importance of this throughout KCP&’s culture if it were to be expanded enterprise wide.

To be updated in future releases of this report.

2.2.4.3 Outage Management System

The Intergraph Outage Management System (OMS) is the basis for all outage information and provides the ability to view that status of all grid outages and to safely manage day-to-day and emergency restoration work. The following sections provide a summary of the development and configurations that were required to implement and deploy the desired OMS functionality.

2.2.4.3.1 Build

KCP&L's Outage Management System (OMS) implementation efforts were launched by assembling a team of highly skilled individuals that would pursue and support the deployment of these advanced systems. The goal was to upgrade and integrate the legacy control room system into a broader Distribution Management System so that Distribution Operations users could access all important information relating to customer and network outages from a single user interface. To familiarize themselves with the goals of the project, the team began by reviewing previously created Use Cases to understand new processes and anticipated system functions. These Use Case documents were finalized where possible and provided to Intergraph to establish their baseline understanding of what KCP&L hoped to achieve with the system implementation. The use cases served as a solid foundation of understanding for newer team members. Where clarifications were required, they were addressed during the Design / Configuration Workshops.

In parallel to KCP&L's preliminary use case familiarization efforts, Intergraph began establishing its project team to perform the installation. The OMS's core capabilities and interfaces are part of a commercially available, productized software implementation which can be configured to the needs of a given customer. By pursuing this "off-the-shelf" philosophy to the maximum degree possible, limited custom design was required. However, the systems did require configuration to accommodate KCP&L's distribution system. With this in mind, Intergraph created a System Configuration Diagram based on discussions with KCP&L to better understand the system configuration and requirements. Intergraph then developed a detailed plan which outlined the time required to meet these requirements and configure the system per KCP&L's needs. As there were relatively few implementations of this integrated DMS solution, staff began familiarizing themselves with the key configuration elements required and documenting questions to be answered in preparation of the actual configuration efforts.

2.2.4.3.1.1 **Collaborative Design Sessions**

After the preliminary familiarization efforts conducted by KCP&L and Intergraph, several workshops were conducted to expedite the configuration effort. The First Responder and Facility Migration Design workshop was conducted to review the details of First Responder data required and KCP&L's existing mapping technologies. The DMS InService Integration Design workshop (focused on D-SCADA integration) was held in which Siemens, Intergraph, and KCP&L jointly participated in this workshop to ensure that all parties were in agreement about the design and configurations to be pursued. Specifically, analysis was performed on the CAD and how it would work with Siemens' D-SCADA (PowerCC) via productized integration. To this end, a foundational understanding of the overall model build process was also established. At the close of the workshop, KCP&L had a better understanding of what additional data requirements needed to be compiled and provided as it became available. Siemens and Intergraph left with a better defined set of requirements that they could use to begin their efforts.

During the InService Integration workshop there were also several discussions regarding the AMI, CIS, and how both integrate with the OMS and CAD. There were additional discussions on accessing data from the CIS in a format as required by Intergraph and the usage of MQ interface for AMI and MDM communications. KCP&L and Intergraph had substantial discussion on alarming and the required applications that would generate alarms on the Integrated UI from the native InService systems and the various other systems that would be integrated with the CAD. The DNA applications that were to be incorporated into the UI and their data requirements were also discussed and determined. Finally, all

involved parties worked on technical specifications to ensure coordinated development of the interfaces to develop the standards-based messages that would be used to exchange the agreed upon information.

2.2.4.3.1.2 System and Interface Configuration

After establishing requirements, configuration considerations, environmental parameters, and a schedule fully recognizes and accommodates dependencies, then development and configuration efforts could begin in earnest. Due to its integrated nature, the OMS was installed alongside the CAD during earlier phases even though it was only minimally used. Both Phases 1 and 2 followed the same configuration approach. Intergraph consolidated all configuration data provided along with all requirements and began working independently in the VENDOR environment. Numerous iterations of configuration and isolated testing were performed to establish preliminary functionality. As conditions warranted, Intergraph coordinated joint working sessions with Siemens to work through integration efforts with the D-SCADA system (also co-located in the VENDOR environment). For Phase 3 scope, significantly greater effort was expended to ensure that the Outage Restoration and Power Status Verification functions were working in addition to the core outage prediction and management capabilities. Later, as the preliminary configurations were coming together, KCP&L facilitated daily working sessions between KCP&L, Siemens, and Intergraph to ensure a comprehensive and synchronized understanding of the deployment in some of its most nuanced ways. Shared-desktop technology (WebEx) was used extensively to enable these conversations between remote participants by allowing everyone to see the same system function, defect, or configuration process.

2.2.4.3.1.3 Data Model Migration

While numerous configuration efforts were vital pre-requisites to a functional system, a particularly laborious component was the model build process. The data model leveraged signal list definitions and data from CAD (Intergraph's I/Dispatcher) to ensure that point data is fully synchronized between the systems and the real world devices resulting in a virtual network model. These migrations would ultimately result in a data model that the OMS could use for its algorithms. Initial efforts were performed in the VENDOR environment and numerous iterations were conducted. These iterations served the dual purpose of ensuring a quality automation process (in anticipation of numerous data model migrations supporting ongoing device deployment) as well as overall data quality (to validate properly synchronized between devices allowing for end-to-end communications). The KCP&L project team worked diligently with Siemens and Intergraph to understand the data model propagation as well as the behind-the-scenes implications of various configurations.

2.2.4.3.1.4 Training

The KCP&L team learned a tremendous amount during the workshops and joint configuration sessions. However, formalized training was still deemed very important to allow KCP&L users to prepare for formalized testing efforts and ultimately successful operation of the system. Sessions were conducted in-person and numerous training manuals were available to aid the process. In addition, given the previously established successes with WebEx, KCP&L leveraged this technology in a two-fold manner: 1) many training sessions were broadcast via WebEx which allowed targeted vendor subject matter experts to augment materials presented by the official trainer and 2) training was recorded allowing for ease of referencing back to better understand an explanation or sequence of events. The following table outlines training sessions conducted for OMS functionality:

Training Course	Dates
I/Dispatcher Training (Intergraph)	07/31/2012 through 08/02/2012
Tester Training (Intergraph and Siemens)	08/13/2012 through 08/14/2012
Alarm Configuration (Intergraph)	10/8/2012
Switch Planning (Intergraph)	10/9/2012 through 10/10/2012

2.2.4.3.1.5 Testing

As outlined above, the more advanced training sessions provided an opportunity for in-depth reviews of functionality to learn how the system is operated. In addition, due to the significantly advanced configuration by this time, the training sessions in the VENDOR environment also provided an opportunity for KCP&L's testing team to select a subset of tests from the formalized test books and review their workability during the training sessions. Additionally, Siemens and Intergraph performed an extensive "Pre-FAT" test where they internally verified that all functionality listed in the test books were working as expected. During more formalized testing, the core outage management capabilities were reviewed with particular attention paid to the integration efforts to support the Outage Restoration and Power Status Verification data flows. Due to the complexities of this interface in particular, testing advanced in a more ad-hoc manner whereby SME's were convened to execute tests only when identified dependencies were resolved.

All testing efforts resulted in numerous defects being documented where functionality deviated from established requirements. Intergraph worked to remediate these defects as soon as they were discovered and continued working to remediate throughout 2013; as variances were fixed, new service packs would be compiled on a regular schedule and installed to KCPL's LAB and DEMO environments for re-testing.

2.2.4.3.2 Integration

An overview of OMS system-to-system interfaces and applicable messages is illustrated in Figure 2-51.

Figure 2-51: KCP&L SmartGrid Demonstration Project OMS Integration



The OMS (Intergraph) is the component of the overall DMS that manages the various outages, crews, new and pending jobs, and outage predictions. Meter outage, restoration data, and power status verification data are accessed on the Integrated UI, but this data is transmitted from the OMS, through the OMS. The OMS is capable of analyzing outage notifications from CIS, integrated voice response (IVR), and the automated metering infrastructure (AMI) to provide outage notifications and pin-point troubled areas using the trouble analysis service. The CAD is the core system with the network model and base data from which the OMS performs its numerous functions. The OMS has a integration points with the CAD and the MDM systems as follows:

- A. OMS / CAD Proprietary Integration: A bi-directional interface that allows outage information, crew data, new / pending jobs, and outage aggregations / predictions to be sent from the OMS to the CAD for the user to view and take appropriate action. This interface also allows the user to access meter data from the MDM, send meter pings, and receive power status verification messages from the meter through the OMS. All data exchanges are automatically transmitted through Intergraph's proprietary technology.
- B. OMS / MDM Outage Restoration and PSV Propagation: A bi-directional interface allowing for meter outage and restoration data to be sent between the MDM and the OMS. Data from automated metering (AMI) systems can provide early identification of outages, assist in determining outage extents, and be used to verify power restoration to customers involved in outages. This interface also allows for Power Status Verification (PSV) Requests and Responses to be sent and received between the OMS and MDM. All data exchanges in this interface are via the KCPL ESB using Message Queues (MQ).

2.2.4.3.3 Post-Implementation Operational Issues

Following the standup, integration, and preliminary testing of the OMS system, numerous post-implementation operational issues needed to be mitigated and considered. These issues are as follows:

- **Software Updates** – Upon installation of the system at KCP&L, efforts were commenced to stabilize the system, perform Site Acceptance Testing (SAT), and begin operating the system as situational opportunities arose. Throughout this period, numerous system deficiencies were discovered, and updates were proactively provided by the software vendor. These necessitated configuration fixes and/or service packs to be delivered by the software vendor. These fixes were delivered by the software vendor together for the OMS and CAD as they are closely integrated with each other. A list of all the service packs installed by KCP&L is listed below:

Build No.	Date	Content
A	4-1-2012	Initial Consolidated UI Installation for Phase 1 SAT
B	9-15-2012	Reinstallation of Consolidated UI with numerous fixes to accommodate advances for Phase 2 SAT
11	2-28-2013	Reinstallation of Consolidated UI with numerous fixes to accommodate advances for Phase 3 SAT
12	4-30-2013	Core UI variances needed to enable stability and advance SAT
13	6-30-2013	Core UI variances needed to enable stability and advance SAT
14	8-30-2013	Remaining high-priority variances to complete SAT
14A	9-16-2013	Fix for SCADA values blank in Feature Information Window
15	11-12-2013	Miscellaneous defect fixes to further stabilize system

- **Outage/Restoration and PSV Data Issues**– During initial configuration and testing at the KCP&L site it was observed that the Outage and Restoration data, PSV requests, and responses were not being picked from the ESB by the OMS application. Subsequently, numerous configuration changes were incorporated into the OMS to better enable the data transfer. These changes were then thoroughly tested on site with regular improvements and continuous vendor involvement. The meter outage/restoration data is crucial for the OMS to manage outages, escalate criticality, perform analysis to determine the probable source of an outage, and finally, PSV data to ensure restoration of power to all impacted customers.

To be updated in future releases of this report.

2.2.4.3.4 Lessons Learned

Throughout the build and stabilization of the OMS system, numerous considerations were realized and should be noted for future deployments of this sort. These Lessons Learned are as follows:

- **Incremental Network Model Management** – In addition to the two previous considerations and as mentioned as a post-operational issue, the installation of a new network data model had significant timing considerations and complexity as it was an all-or-nothing implementation. While this step was vital to allow enabled D-SCADA capabilities to be geospatially displayed on the Consolidated UI, the team was hesitant about deploying any new field devices or circuits into the maps because the entire network model needed to be re-deployed. The result of which was significant system downtime to install and re-stabilize the system. In this context, an incremental network management migration capability would have significantly greater value to a real-time system like the OMS as it would allow the system to maintain its functionality for vast portions of the service territory while only a small, targeted section is having its underlying connectivity details updated.

To be updated in future releases of this report.

2.2.4.4 1st Responder Functions

The Siemens DNA applications provide the DMS 1st Responder Functions for the combined Intergraph/Siemens DMS. The 1st Responder Functions improve the operation of the distribution network by performing real-time analysis, automate control, and optimize the performance of the grid. The following sections provide a summary of the development and configurations that were required to implement and deploy the desired 1st Responder functionality.

2.2.4.4.1 Build

KCP&L's First Responder (DNA) implementation efforts were launched by assembling a team of highly skilled individuals that would pursue and support the deployment of these advanced applications. To familiarize themselves with the goals of the project, the team began by reviewing previously created Use Cases to understand new processes and anticipated system functions. In so doing, the team was able to better advocate for how the systems should be configured in later workshops. Unlike some other systems, the First Responder use cases were somewhat higher level as there were relatively few interoperability touch points, but they served as a solid foundation of understanding for newer team members.

In parallel to KCP&L's preliminary use case familiarization efforts, Siemens began establishing its project team to perform the installation. The First Responder core capabilities and interfaces are part of a commercially available, productized software implementation which can be configured to the needs of a given customer. In this context, Siemens began identifying key staff and subject matter experts who would be performing the configuration. As there were relatively few implementations of this product, staff began familiarizing themselves with the key configuration elements required and documenting questions to be answered in preparation of the actual configuration efforts.

2.2.4.4.1.1 Collaborative Design Sessions

After the preliminary familiarization efforts conducted by KCP&L and Siemens, a number of workshops were conducted to ensure a common understanding for what configurations would be performed and how the system would operate. The workshop series started with a discourse addressing various capabilities, modes of operation, and established the context for the system's functionality. As the workshops progressed, a detailed matrix was produced outlining the data points required from each device to support proper algorithmic processing. Further discussions were conducted to define the constructs and requirements from upstream processes to ensure that connectivity in the network model would be sufficient for state estimation and power flow calculations. Based on these discussions, KCP&L had a better understanding of what additional data requirements needed to be compiled and provided as it became available. Siemens left with a better defined set of requirements that they could use to begin their efforts.

2.2.4.4.1.2 System and Interface Configuration

After establishing requirements, configuration considerations, environmental parameters, and a schedule that fully recognizes and accommodates dependencies, then development and configuration efforts could begin in earnest. Siemens consolidated all configuration data provided along with all requirements and began working independently in the VENDOR environment. Numerous iterations of configuration and isolated testing were performed to establish preliminary functionality. As conditions warranted, Siemens coordinated joint working sessions with Intergraph to work through integration efforts with the CAD system (also co-located in the VENDOR environment). Additional working sessions were conducted with another Siemens team responsible for the D-SCADA capabilities to ensure proprietary integration with that system was working as expected. Later, as Phases 1 and 2 of the DMS deployment stabilized and the final First Responder configurations were coming together, KCP&L facilitated daily working sessions between KCP&L, Siemens, and Intergraph to ensure a comprehensive and synchronized understanding of the deployment in some of its most nuanced ways. Shared-desktop technology (WebEx) was used extensively to enable these conversations between remote participants by allowing everyone to see the same system function, defect, or configuration process.

2.2.4.4.1.3 Data Model Migration

While numerous configuration efforts were vital pre-requisites to a functional system, a particularly laborious component was the model build process. The Network Model establishes connectivity between all field devices, their respective circuits, and ultimately the originating substation. Any disconnects or anomalies in this model result in de-energized "islands" of circuitry that confuse the system. Furthermore, the network model leverages signal list configurations and data from CAD (Intergraph's I/Dispatcher) to ensure that this virtual representation of the real world yields maximally legitimate algorithmic results. Levering proprietary scripts, I/Dispatcher would extract this key data and compile it into a format which could be transferred and loaded into the First Responder applications. Initial efforts were performed in the VENDOR environment and numerous iterations were conducted to ensure a stable network model for all devices and all points on each device. As the network model stabilized and configurations were reviewed in LAB and DEMO environments, increasingly nuanced problems began to evidence themselves. In one instance, reclosers were fully integrated into the model, but the secondary terminals of the current transformer were juxtaposed with respect to the primary and secondary side of the recloser, thus resulting in negative current calculations. This hadn't previously evidenced itself as a problem in GIS or DSCADA capabilities given their limited sophistication, but caused significant issues in the DMS. In another instance, many of the individual circuit spans in GIS were very short in length, but this proved highly problematic for legacy EMS power flow algorithms that formed the basis of our DMS as they were designed to apply impedance configurations against spans in

multiples of 1000 feet. To resolve, the spans needed to be aggregated into “Super-spans” so that the algorithms would run as needed.

2.2.4.4.1.4 Training

The KCP&L team learned a tremendous amount during the workshops and joint configuration sessions. However, formalized training was still deemed very important to allow KCP&L users to prepare for testing efforts and ultimately successful operation of the system. Sessions were conducted in-person and numerous training manuals were available to aid the process. In addition, given the previously established successes with WebEx, we leveraged this technology in a two-fold manner: 1) all training sessions were broadcast via WebEx which allowed targeted vendor subject matter experts to augment materials presented by the official trainer and 2) training was recorded allowing for ease of referencing back to better understand an explanation or sequence of events. The following table outlines training sessions conducted for First Responder functionality.

Training Course	Dates
Tester Training (Siemens)	08/13/2012 through 08/14/2012
Distribution Network Analyses (Siemens)	10/29/2012 through 11/01/2012
Pre-FAT Demo and Training: State Estimation	December 13, 2012
Pre-FAT Demo and Training: Power Flow	December 20, 2012
Pre-FAT Demo and Training: Volt/VAR Control	January 03, 2013
Pre-FAT Demo and Training: Feeder Load Transfer	January 10, 2013
Pre-FAT Demo and Training: Fault Location & Restoration	January 17, 2013

2.2.4.4.1.5 Testing

As outlined above, the more advanced training sessions provided an opportunity for in-depth reviews of functionality to learn how the system is operated. In addition, due to the significantly advanced configuration by this time, the training sessions in the VENDOR environment also provided an opportunity for KCP&L’s testing team to select a subset of tests from the formalized test books to ensure the accuracy of the configuration. Where needed, defects were documented and logged as part of this “Pre-FAT” testing effort. Unlike Phases 1 and 2 which focused on the D-SCADA and required the KCP&L test team to be physically present at the Siemens facility for several weeks, Phase 3 First Responder Factory Acceptance Testing (FAT) went much smoother. By conducting pre-FAT tests, Siemens was able to align its configurations with an evolved understanding of what KCP&L expected during the formal FAT and had time to update the system in advance. Following execution of all formal FAT tests, KCP&L decided it was ready to migrate the First Responder functionality to its Kansas City-based LAB and DEMO environments in the Spring of 2013. Numerous procedural mechanisms were implemented to stabilize the system and ensure its preliminary integration with the other systems in the environments. Site Acceptance Testing (SAT) commenced opportunistically through Late Spring 2013 and continued with considerable rigor throughout the Summer. All testing efforts resulted in numerous defects being documented where functionality deviated from established requirements. Siemens worked to remediate these defects as soon as they were discovered and continued working to remediate throughout 2013; as variances were fixed, new builds would be compiled and installed to KCP&L’s LAB and DEMO environments for re-testing.

2.2.4.4.2 Integration

An overview of First Responder system-to-system interfaces and applicable messages is illustrated in Figure 2-52.

Figure 2-52: KCP&L SmartGrid Demonstration Project First Responder Integration



The First Responder (DNA) capabilities are designed to function independently from the largely integrated system. While it does leverage information from these other systems, much of this information is processed and filtered by the D-SCADA. The integration touch points for the First Responder (DNA) applications are as follows:

- A. DNA / CAD Data Model Propagation: As part of the overall network and data model propagation process from GIS to the DMS suite of systems, the key details of the network model are prepared in CAD and then transferred to DNA. This process is performed on an ad-hoc and largely manual basis using Oracle SQL.
- B. DNA / CAD UI Integration: A bi-directional interface allowing for DNA algorithmic results and recommendations to be forwarded on for display to the user. The interface also allows user selections and configurations to be passed from the CAD User Interface to DNA. All data exchanges in this interface are via Message Queues (MQ).
- C. DNA / DSCADA Monitor & Control Propagation: A bi-directional interface allowing for D-SCADA point monitoring details to be provided to DNA so that it has all updated information for algorithmic processing. The interface also allows for any controls resulting from algorithmic processing to be transmitted to D-SCADA for further propagation to devices in the field. All data exchanges in this interface are via Siemens proprietary technology.

2.2.4.4.3 Post-Implementation Operational Issues

Following the standup, integration, and preliminary testing of the First Responder (DNA) system, numerous post-implementation operational issues needed to be mitigated and considered. These issues included the following:

- **Productized Integration** – At inception of this demonstration project, deployment plans were based on the premise of a commercially mature, productized integration of the First Responder (DNA) capabilities with the D-SCADA and CAD capabilities. However, this productized integration had only been deployed at one other site, which resulted in a larger stabilization effort in KCP&L’s real-world environment. This continued into the post-operational period, where very specific real-world situations conspired to result in system instability situations. Many of these situations could have been avoided had this system been deployed and fully tested in an enterprise operational context prior to implementation at KCP&L.
- **Software Updates** – Upon installation of the system at KCP&L, efforts were commenced to stabilize the system, perform Site Acceptance Testing (SAT), and begin operating the system as situational opportunities arose. Throughout this period there were numerous system deficiencies discovered which necessitated fixes to be delivered by the software vendor. Due to the co-mingled architectural nature of the DNA and D-SCADA capabilities,

these fixes were delivered and installed as part of several subsequent “builds”. Efforts were initially pursued to deploy updates frequently, but were scaled back due to the complexity of regression testing functionality, completing deployment to all servers and UIs, and then re-establishing stability. A list of builds installed by KCP&L is listed below:

Build No.	Date	Content
80	2-19-2013	Initial DNA KCP&L Site Installation
90	3-14-2013	Core D-SCADA variances needed to enable DNA functionality
93	4-17-2013	Core D-SCADA variances needed to enable DNA functionality
100	5-30-2013	Core DSSE / DSPF Stability variances; preliminary HIS configuration
105	7-26-2013	Prioritized DSSE, DSPF, VVC variances
108	8-22-2013	DMS / DERM Heartbeat & Battery functionality
116	10-7-2013	Comprehensive delivery of all DSSE, DSPF, and VVC variances
121	11-27-2013	Comprehensive delivery of all outstanding variances

- Network Model Data Migrations** – During initial configuration and build efforts, only a subset of planned, end-state devices were captured in network model. This was done to reflect the limited number of deployed devices at configuration inception, but also to limit the complexity of model connectivity while establishing process stability. However, in our preliminary configuration and test environments, many of the attempted data migrations with this limited data set took significant time and effort to implement and stabilize. When the system was transferred to KCP&L, it maintained this subset of devices and due to the known challenges with the data migration process, incremental data migrations were not pursued for some time. This allowed time to complete device deployments in the field as well as setup and conduct numerous additional test data migrations in our LAB environment prior to conducting a data migration in our DEMO environment. In retrospect, the lack of a complete data model was a hindrance requiring certain workarounds, but it was still preferable to the potentially long time periods of environment inaccessibility waiting for the data migration to re-stabilize.
- Field Device Communications Instability** – First Responder (DNA) algorithms are firstly dependent on the quality of downstream SCADA data. As discussed in greater detail in the D-SCADA and particularly the SICAM build sections, significant effort was put forth to stabilize the communications channels to field devices and ensure robust transmission of real-time data. At times where instability was significant, KCP&L’s ability to test and operate the First Responder capabilities was limited and focus was shifted back to D-SCADA stabilization.
- DSSE / DSPF Tuning** – State estimation (DSSE) and Power Flow (DSPF) algorithms are dependent on a mix of real world SCADA data (recloser, breaker data) as well as historical models (loads per transformer, weather adjustments). While the SCADA data is used directly, in some cases load model data initially used resulted in some algorithmic results being significantly different from real world values (as confirmed by other SCADA or field crew readings). To improve the results, analysis of the algorithms and load models were conducted and tweaked as necessary to achieve more reasonable results.

To be updated in future releases of this report.

2.2.4.4.4 Lessons Learned

Throughout the build and stabilization of the First Responder (DNA) system, numerous considerations were realized and should be noted for future deployments of this sort. These Lessons Learned are as follows:

- **Systems require greater modularity** – As mentioned as a post-operational issue, in many cases when a defect fix was delivered it required a fully compiled build to be installed. The project team came to consider this functionality as “Project-ware” instead of “software” recognizing the high level customization that seemed to be required to deliver a fix. It would be envisioned that in a more mature software package, core functions would be deliverable and upgradeable in a more compartmentalized fashion not requiring a full re-installation of the entire integrated software suite (as was required in our First Responder / D-SCADA implementation).
- **Incremental Network Model Management** – As mentioned as a post-operational issue, the installation of a new network data model had significant timing considerations and complexity as it was an all-or-nothing implementation. The team was hesitant about deploying any details about new field devices or circuits because the *entire* network model needed to be re-deployed. In this context, an incremental network management migration would have significantly greater value to a real-time system like the First Responder capabilities as it would allow the system to maintain its functionality for vast segments of the service territory while only a small, targeted section is having its underlying connectivity details updated.
- **LAB Environment Benefits** – For other Smart Grid system deployments, there have been discussions of the benefits of the integrated LAB environment; particularly for the D-SCADA and SICAM systems as KCP&L was able to test end-to-end communications. However, while the LAB environment was leveraged for a subset of First Responder tests, it was generally not as beneficial for a majority of DNA testing. Specifically, the First Responder applications require a significant quantity of frequently updated data from devices in the field. In a production environment, legitimate devices continually provide this data. However, in the lab environment, it proved to be challenging to simulate or compile enough data to truly simulate an entire distribution footprint.
- **Telepresence Benefits** – Collaboration between KCP&L and its vendor partner were challenged due to geographic dispersion. A vital mitigation strategy was extensive use of shared-desktop technology (WebEx) to allow remote access to systems and support mutually-viewed sessions for trouble analysis. Of particular note, KCP&L was able to better prepare for its Phase 3 First Responder FAT by conducting numerous weekly sessions to verify the basic anticipated functionality. In so doing, travel was minimized and team members were able to participate very effectively from their respective local offices. Furthermore, ad-hoc training sessions were able to be conducted via this technology which enabled the vendor’s subject matter experts to engage and explain concepts more efficiently than traditional methods. Frequently, KCP&L was able to record these digital sessions and found them to be incredibly valuable reference material upon questions arising or to transition new team members to the project. The recordings proved so valuable, that in the future, KCP&L would be interested to include language in vendor contracts to establish a baseline understanding that these assets will be created through the course of project pursuits.

To be updated in future releases of this report.

2.2.4.5 ADA Field Area Network

The Tropos wireless IP mesh was deployed as the foundation for the ADA Field Area Network (FAN). The ADA FAN provides the monitoring and control communications infrastructure to devices outside the substation. The following sections provide a summary of the development and configurations that were required to implement and deploy the desired ADA FAN functionality.

2.2.4.5.1 Build

Work on the Tropos network began in February 2012. As the KCP&L team began getting comfortable with the technology, several Tropos engineers came on site to perform a field survey of the project territory. With the help of KCP&L engineers, they determined the acceptable mounting assets for the network gateways and the base mesh nodes. They also spent some time training the KCP&L field crews on the mounting and installation process for both types of routers.

From a networking perspective, Tropos also worked with KCP&L's Network Services group to determine a strategy for integrating this new RF mesh network into KCP&L's IP infrastructure. They chose not to add the Tropos network to the KCP&L corporate network; rather, it is located within the new, isolated Smart Grid network that Network Services designed and implemented as part of the demonstration project. Tropos worked with Network Services to consider the total quantity of nodes for the smart grid implementation, and based on this, they crafted the initial design. This design called for two take-out points: one at Midtown substation (to backhaul the south half of the network) and the other from a tower at 801 Charlotte (to backhaul the north half of the network). Network Services reserved IP address space for both the Tropos mesh network itself, as well as the wired client interfaces. This translated to two IP addresses for each 1310 router (1 wireless IP for the 2.4GHz radio and 1 wired interface to the connected field device) and three IP addresses for each 6320 router (same as the 1310, plus a wireless interface for the 5.8GHz radio).

Another initial design discussion revolved around the IP-enabled field devices and how to terminate all of the associated VPN tunnels within the smart grid network. In the end, the Network Services team chose to use a dedicated Cisco router to terminate all the VPN tunnels that are used for communication to and from the IP devices – the FCIs, reclosers, and RTAC. The capacitor banks differed – the serial devices don't utilize VPN tunnels for communications.

2.2.4.5.1.1 **Lab Implementation**

The next step in the ADA network implementation was to set up a lab instance of the Tropos mesh network. KCP&L wanted to test out the capabilities of the network in a controlled environment, so routers, gateways, and field devices were set up in a lab at KCP&L. The lab was set up to mimic the production environment as closely as possible. As such, Network Services used this environment extensively to ensure that their designs and configurations would work as expected with the new technology. In its final state, the lab consists of the following routers and field devices:

- (1) 6320 gateway
- (2) 1310 routers connected to capacitor bank controllers
- (1) 1310 router connected to an FCI receiver
- (1) 1310 router connected to an RTAC
- (1) 1310 router connected to a recloser controller

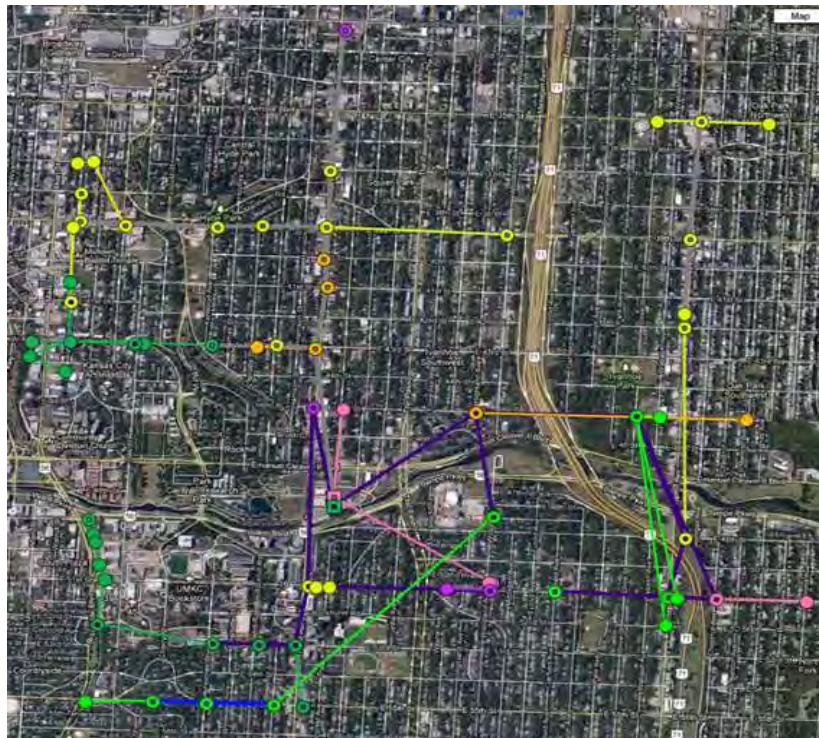
2.2.4.5.1.2 Base Mesh Deployment

After getting comfortable with the lab network and determining the over-arching network design, KCP&L field crews began deploying the base mesh 6320 and 1310 devices in the field. The key elements of the base mesh included:

- Tropos Infrastructure Gateways (6320s) - two at 801 Charlotte and two at Midtown Substation
- Tropos Infrastructure Nodes (6320s)
- Tropos Edge Routers (1310s)

After completing a first pass at the base mesh, Tropos and KCP&L worked together to optimize the network. As a result, several nodes were relocated, and several were added to the network. These changes greatly improved network performance, and at the completion of the base mesh build-out in December 2012, all nodes had at least a 92% ping success rate. The base mesh network is shown below in Figure 2-53.

Figure 2-53: KCP&L Base Mesh Network



2.2.4.5.1.3 Field Device and Edge Router Deployment

After all of the Tropos base mesh nodes were deployed, the remainder of the field devices were installed, along with their respective Tropos routers. KCP&L deployed most of the capacitor banks first, mostly because the controllers were available, and the capacitors were already in the network model. The SEL 651R was a new device, and it wasn't readily available for installation in the production environment at the beginning of 2013. Once they became available, the reclosers were deployed on the highly automated smart grid feeders that were to be used for testing – feeders 7551 and 7561. The FCIs were deployed on these feeders next, finalizing the field device deployments on the prioritized feeders so that the team could start to test the First Responder functions.

After deploying the field devices to the prioritized feeders, KCP&L worked on the reclosers for the non-prioritized feeders. The production RTAC and its associated router were installed at the Midtown substation battery control enclosure during the first quarter of 2013. The FCIs were deployed to the production network last.

Upon deployment of the routers and field devices, point-to-point checkouts were conducted.

Normally, KCP&L would not have utilized reclosers to perform all of these functions; rather, they would have used a combination of switches and reclosers. For this project, however, they decided to use reclosers for isolation, mid-circuit, and tie functions. This decision was made for two reasons. First, the cost difference between reclosers and switches has decreased dramatically. There isn't as much incentive to utilize switches even when full recloser functionality isn't required. Second, KCP&L wanted to test the use of field device profiles. The same device will be used to perform three separate functions, and this will be implemented through the use of DNP profiles.

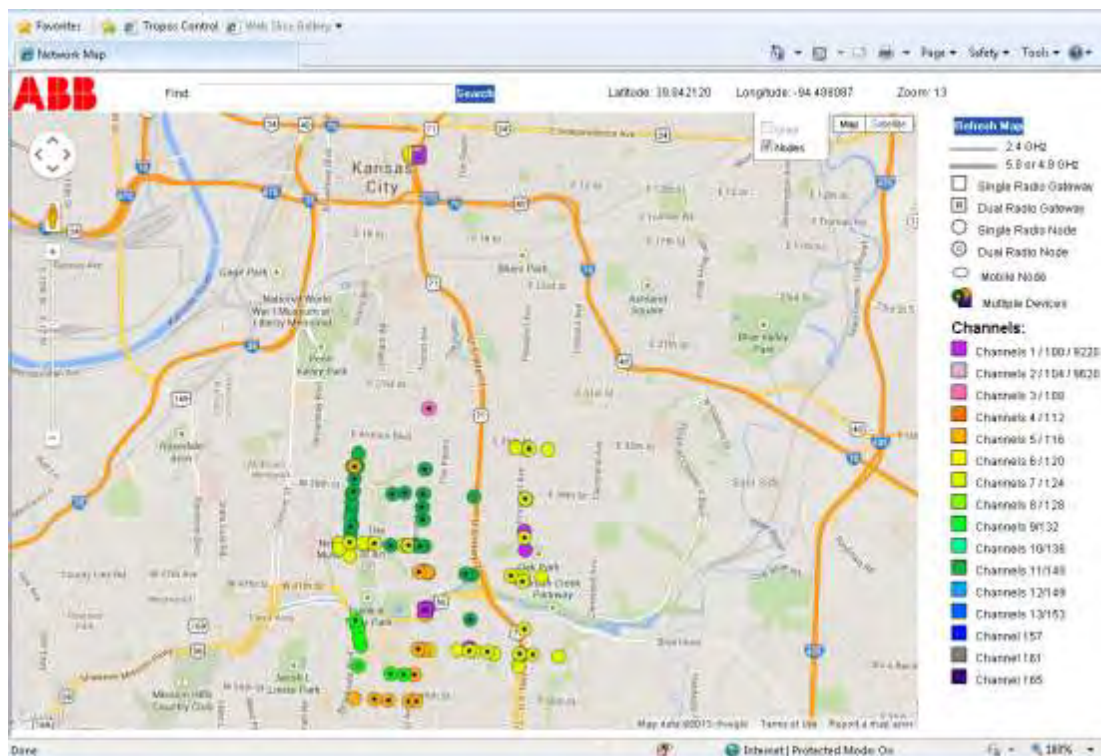
The field device and router deployment was finalized in Q4 of 2013. Upon completion of the ADA deployment, the field devices described in Table 2-12 were installed for the demonstration project.

Table 2-12: Field Devices

Field Device	Vendor/Model	Quantity
Capacitor bank controllers	S&C IntelliCAP PLUS	29
Fault circuit indicator receivers	Horstmann	12
Recloser controllers	SEL 651R	20
Grid-connected battery controller	SEL 3530-4	1

The final deployed Tropos network map is shown below in Figure 2-54. The various colors on the map represent different communications channels that the routers are currently communicating over.

Figure 2-54: KCP&L Final Deployed Mesh Network



2.2.4.5.1.4 Capacitor Bank Deployment Specifics

The capacitor banks themselves were GE Capacitor Racks, and they had been in use prior to the demonstration project. The controllers were new for the project, and KCP&L chose to use the S&C IntelliCAP Plus.

The pictures below detail the capacitor bank installations. The picture on left shows the controller within its enclosure. The picture on the right shows the actual field installation. The controller enclosure is shown in the bottom right corner of the picture (about 8-10 feet above the ground). The Tropos 1310 router is mounted on the arm that extends out from the pole about 2/3 of the way up. The actual cap bank itself is located near the top of the pole.

The capacitor bank is the only field device in the demonstration project that utilizes serial communication to and from the Tropos 1310 router. The interface between the Tropos router and the DDC uses DNP3 for communications.

Figure 2-55: Typical Capacitor Bank Installation



2.2.4.5.1.5 Fault Current Indicator Deployment Specifics

The fault current indicators used in the demonstration project were Horstmann Smart Navigators, and the controllers for the sets of FCIs were Horstmann Smart Receivers. The FCIs provide magnitude of fault and fault direction. Each receiver can communicate with up to twelve Navigators. The receiver utilizes 2.4GHz RF to communicate with FCIs, and the Tropos router automatically adjusts what channel it is communicating on to avoid interference. The range of communication between the receiver and its associated FCIs is approximately 100 feet line-of-sight.

The pictures below detail the FCI installations. The picture on left shows one of the Smart Navigators, the picture in the middle shows the inside of the Smart Receiver enclosure, and the picture on the right shows the actual field installation. The receiver is shown attached to the pole (about 8-10 feet above the ground), the Tropos 1310 router is mounted on the arm that extends out from the pole about 2/3 of the way up, and one of the Smart Navigators is attached to the distribution line.

The FCI is an IP-enabled device and it communicates to the DDC with DNP3.

Figure 2-56: Typical Fault Current Indicator Installation



Figure 2-57: Typical Recloser Installation



2.2.4.5.1.6 Recloser Deployment Specifics

KCP&L used two different types of reclosers for the demonstration project: the G&W Viper – ST Triple Option Vacuum, and the Siemens SDR Triple-Single Vacuum. The recloser controller was the SEL 651R-2. The SEL 651R-2 was chosen because it can support 61850-MMS messages. KCP&L ultimately decided to utilize DNP3 in order to retain consistency throughout the DA deployment; however, the 651R-2 enables KCP&L to demonstrate MMS messaging down the road.

The pictures in Figure 2-57 above detail the recloser installation. The picture on the left shows the controller inside its enclosure with the battery backup. The picture on the right shows the actual field installation. The controller enclosure is mounted about 8-10 feet above the ground. The Tropos 1310 router is mounted on the arm that extends out from the pole about 2/3 of the way up. The recloser itself is near that top of the picture.

2.2.4.5.1.7 Battery RTAC Deployment Specifics

For the grid-connected battery, KCP&L used an Exergonix DESS CS1000. The inverter was an S&C SMS, and the controller was an SEL 3530-4, also known as an RTAC (Real Time Automation Controller). The RTAC was added between the substation controller and the S&C SMS because it supports IP communication and both 61850-MMS messages and DNP3 protocol. The RTAC also enabled the battery to be utilized as a field device. In a real-world application, a battery would most likely reside in a rural location. By utilizing the DA network for communication, it allows KCP&L to demonstrate this architecture. The RTAC also allowed for dynamic operation of the battery, since the inverter can only operate based upon static parameters. Lastly, the RTAC enabled development of battery controller algorithms.

The pictures below show the DESS (top) and the RTAC (bottom).

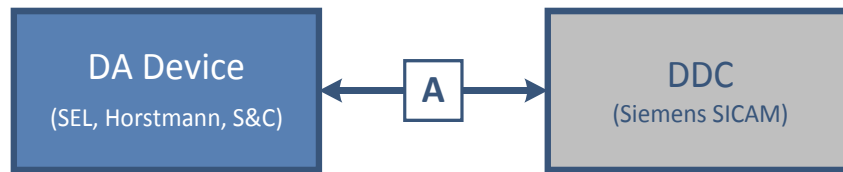
Figure 2-58: Battery Installation



2.2.4.5.2 *Integration*

The Distribution Automation Field Area Network isn't a "system" per se, but it does enable communications between field devices the data concentrator, the SICAM. An overview of the DA device communications and applicable messages is illustrated in Figure 2-59.

Figure 2-59: KCP&L SmartGrid Demonstration Project DA Integration



The integration touch points for the ADA FAN are as follows:

- A. DDC / Field Devices Monitor and Control Propagation: A bi-directional interface allowing for field device point monitoring details to be provided by the field device (capacitor bank, fault current indicator, recloser, or battery) to the DDC so that it has all updated field device information for use by the DDC and other upstream systems. This communication occurs in real time as device status changes, and it also occurs on regular intervals via predefined integrity polls initiated by the DDC. The interface also allows for any controls resulting from DDC functionality to be transmitted to the field device. All data exchanges in this interface are transmitted via the Tropos network using DNP3.0.

2.2.4.5.3 *Post-Implementation Operational Issues*

Following the construction, start-up, and preliminary testing of the ADA FAN, numerous post-implementation operational issues needed to be mitigated and considered. These issues are as follows:

- **Tropos Firmware Updates** – After the initial deployment of the Tropos routers, KCP&L had to conduct several firmware updates. In general, when a new version of firmware came out, Tropos alerted KCP&L and explained the modifications in the updated version. Next, the Network Services team would test out the firmware update in the lab to make sure that everything went smoothly. After a thorough test out, the firmware would be deployed to all of the production routers. This process was fairly simple, as the new firmware can be pushed to all of the devices simultaneously from the Tropos Control GUI. KCP&L has performed XX firmware updates to date, and 2-3 are expected (based on release schedules) for 2014.
- Although the push to the routers usually goes smoothly, KCP&L has had some trouble getting the devices to re-mesh with the network. A handful of devices have required local power cycling of the device in order to re-mesh. This hasn't been a major issue, but it would be more significant in a full-scale deployment.
- **VPN Tunnels** – Occasionally, the router VPN tunnels get dropped and they don't automatically get rebuilt. KCP&L is currently working with Tropos to determine if this is due to some sort of configuration on the Tropos router, or is this due to something on the Cisco router (the router that's terminating the VPN connection). The VPN tunnels are expected to go down occasionally, but they should rebuild themselves – after a certain amount of time, the radio is supposed to request to build the VPN tunnel again. This process is currently taking a lot longer than it should.
- **Poor Signal Quality** – The most common post-operational issue that the KCP&L team has dealt with is poor router signal quality. This is due to all kinds of environmental factors, such as varying tree cover during different seasons, noise on the network from non-

Tropos communications, or weather events. In addition to these environmental variables, the growing Tropos network also had a significant impact on the signal quality of each router. As field devices were deployed and their associated Tropos nodes were added to the network, KCP&L was able to watch to see how the network paths changed and updated themselves to adjust to different routing options.

- Although the Tropos routing algorithms are proprietary, there were certain strategies that Tropos helped the KCP&L team to implement in order to address specific signal quality issues. Some examples of these strategies include:
 - Forcing routers to specific channels temporarily to force certain paths (that are better quality)
 - Configuring 6320 routers to choose the 5.8GHz frequency instead of the 2.4GHz frequency in order to boost stability of the base mesh
 - Moving base mesh nodes to “better” locations in order to provide better signal quality or to reduce the hop count
 - Swapping out 1310 routers with 6320 routers in order to extend the 5.8GHz frequency to a corner area of the Tropos network
- **Power Supplies** – Another post-operational issue that KCP&L encountered had to do with power to the Tropos routers. The routers attached to capacitor banks and FCIs are all powered off the field device controller, so they didn’t require an external power supply to the radios. The base mesh nodes all utilize Power over Ethernet (PoE) devices to supply the input voltage. The substation battery also uses a PoE device, as the RTAC (which is used for battery control) can’t power the associated Tropos router. The reclosers were originally deployed without external power supplies, but KCP&L started to notice issues with these devices. Upon further investigation, they realized that the voltage supplied by the recloser controllers was on the low edge of what the Tropos router would tolerate. As a result, KCP&L chose to deploy PoEs for the recloser routers, and this resolved the problems.
- **On-Going Monitoring and Troubleshooting** – The largest post-operational work that KCP&L has conducted in relation to the DA network is general monitoring and troubleshooting. As the router and field device deployment progressed, KCP&L started doing daily checks of the SICAM. This would alert the team if interfaces to particular devices were problematic, and then the team would use Tropos Control to further investigate the connections to these devices.
- The daily SICAM checks provided the team with an instantaneous snapshot of the status of connections from the SICAM to all field devices, but they were only useful if there was an issue at the particular moment when the user logged into the SICAM. As a result of this shortcoming, KCP&L also found it necessary to do weekly in-depth checks of each router. The Tropos Control router checks provided a history of each router health, and they included logging each router’s uptime, the current path quality, and the number of hops from that router. The router uptime helped the team to discover any issues that might have been missed during the daily SICAM checks. Investigating the problem nodes in this manner helped KCP&L to uncover router reboots that may have occurred over the past week. These reboots were traced back to power issues (leading to the deployment of PoEs on the recloser routers), mechanical issues, or wiring issues with the relays themselves.
- **Gateway Placement** - The last post-operational issue pertaining to the Tropos network involved the gateways. In the original design, KCP&L deployed redundant gateways at the northern end of the network and at the southern end of the network. Unfortunately the northern location was dependent on a point-to-point link between the northernmost base

mesh node and the gateway location, and there were a lot of noise issues there due to other devices installed at that tower. The noise caused significant interference issues with the point-to-point link, so KCP&L ended up disabling the gateway components of the northern 6320s gateways. This basically disabled the capability for downstream nodes to mesh with these 6320s, so all router traffic was forced to the southern gateway. This is obviously not an ideal setup, but it has worked sufficiently well for the small geographic area of the demonstration project, and KCP&L still has redundant gateways at the south location. For a larger deployment, KCP&L would definitely need multiple gateway locations.

To be updated in future releases of this report.

2.2.4.5.4 Lessons Learned

Throughout the build and stabilization of the ADA network, numerous considerations were realized and should be noted for future deployments of this sort. These Lessons Learned are as follows:

- **Maximize Takeout Points** – One of the major lessons learned on this component of the project was that takeout points are extremely important. In order for the mesh network to perform as well as possible, it is critical to have as many takeout points as possible. This will decrease the hop count and decrease the burden on any single set of gateways.
- **Communications Tuning** – Another lesson learned is that despite the proprietary nature of most mesh network routing algorithms, there are always ways to do manual intervention to prioritize certain parameters over others. KCP&L worked with Tropos on several occasions to overcome certain features of their routing algorithm that were problematic in the demonstration project implementation.
- **Latency / Time Requirements** – One of the major themes of the DA deployment was that the use of wireless network technology for DA means that the data concentrator needs to support less than ideal communications quality. Latency and timing are two major factors that will not mimic the traditional wired solution, and these cannot break the concentrator.
- **Device & Radio Placement** – KCP&L learned about the importance of carefully thinking through all the details associated with each router deployment, especially pertaining to router power. Being on the edge of the voltage requirements was problematic for KCP&L, and the team ended up adding power supplies in order to boost input voltage to necessary levels for the routers.

To be updated in future releases of this report.

2.2.4.6 Historical Information System

The Siemens Historical Information System (HIS) component provides a reliable archive of historical real-time D-SCADA data. The following sections provide a summary of the development and configurations that were required to implement and deploy the desired HIS functionality.

2.2.4.6.1 Build

KCP&L's DMS Historian was not initially included in the original scope for the KCP&L SmartGrid project. However, as the project progressed, investigations were conducted on the in-scope systems and the team determined that default archival capabilities of the DMS systems would be insufficient to produce the analytics required for the later stages of this reporting document. Therefore, a dedicated Historian Application was pursued as it became clear that an archival technology would be required for troubleshooting and reporting in the future.

2.2.4.6.1.1 Design

Internal discussions were conducted to determine available alternatives and the team quickly narrowed in on a bolt-on module available for Siemens's PowerCC product known as the Historical Information System (HIS) module. A remote demonstration of HIS capabilities was conducted in Winter 2013 to understand the functionality and known limitations of the system. The team quickly determined that this capability was best for KCP&L's needs and outlined the high level requirements – mainly that the HIS would be configured to store all the data points for all device types. With the goal of reconstructing a particular day's operations, the requirements were later flushed out to include the following real-time information:

- All Analog values
- All Accumulator values
- All Digital values (status information, device operations)
- All Tap positions
- All Messages (alarms, user logons, system status, connection, power flow)

2.2.4.6.1.2 Configuration

Siemens pursued preliminary configurations of HIS in the VENDOR environments to enable capturing of analogs, accumulators, and digitals. Throughout, there were numerous questions that came up where KCP&L provided guidance. Of particular note, the technical environment resulted in the largest number of questions regarding database sizing, integration with the server cluster, and appropriate database privileges configurations allowing for data recording.

2.2.4.6.1.3 Training

The KCPL team learned a tremendous amount during the preliminary demonstration session. However, formalized training was still deemed very important to allow KCPL users to prepare for formalized testing efforts and ultimately successful operation of the system. A session was conducted via WebEx and numerous training manuals were available to aid the process. In addition, given the previously established successes with WebEx on other systems, we leveraged this technology to record the session for ease of referencing back to better understand an explanation or sequence of events. While doing so, some preliminary defects were identified as applicable to the KCPL configuration. The following table outlines training sessions conducted for HIS functionality.

Training Course	Dates
HIS Functionality Demonstration (Siemens)	01/24/2013
HIS Tester Training and Operation (Siemens)	10/07/2013

2.2.4.6.1.4 Implementation

Unlike other systems of the DMS which were tested in VENDOR environments prior to implementation in DEMO environments, for expediency and minimal anticipated risks, the HIS was deployed to KCP&L systems when deemed ready by Siemens. A code release containing only incremental HIS capabilities was provided and installed. Numerous data base changes were required and implemented to ensure the new functions worked as expected. Siemens worked closely with KCP&Ls database administrators to ensure these configurations were implemented properly. Final configuration changes were implemented to enable the new HIS module to commence archival capabilities.

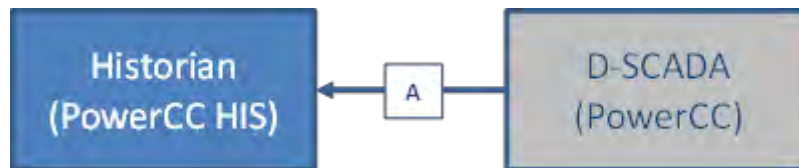
2.2.4.6.1.5 Testing

As with other systems, Siemens provided a standard test book for review by the test team. As the KCP&L test team went through the test book, tests were added and removed as necessary to ensure appropriate coverage and confidence in HIS archival capabilities. Based on an understanding of these functions, the previously mentioned training was pursued with a supplemental agenda outlining certain functions which KCP&L requested to be demonstrated during the session. With the necessary tools to autonomously perform testing, the KCP&L team pursued a more formalized and rigorous testing effort by executing the test scripts documented in the test book. As identified, defects were documented in a tool provided by Siemens and tracked to resolution.

2.2.4.6.2 Integration

An overview of HIS system-to-system interfaces and applicable messages is illustrated in.

Figure 2-60: KCP&L SmartGrid Demonstration Project HIS Integration



The HIS functions enable a significant amount of KCP&L's reporting capabilities. In particular, its integration with D-SCADA is vital to ensure that all real-time data is syphoned and archived as required. The integration touch point for the HIS is as follows:

- A. D-SCADA / HIS Data Propagation: 'Real-Time' data points from all devices are sent from D-SCADA (PowerCC) to HIS for data collection and storage. All data exchanges in this interface are automatically performed using Oracle SQL.

2.2.4.6.3 Post-Implementation Operational Issues

Following the standup, integration, and preliminary testing of the HIS system, few Post-Implementation Operational Issues needed to be mitigated and considered. These issues included the following:

- **Software Updates** – Upon installation of the system at KCP&L, efforts were commenced to stabilize the system, perform Site Acceptance Testing (SAT), and begin operating the system as situational opportunities arose. Throughout this period, several system deficiencies were discovered which necessitated fixes to be delivered by the software vendor. Some of these were corrected by changing some configurations. However, due to the co-mingled architectural nature of the DMS sub-systems, some other fixes were delivered and installed as part of several subsequent "builds". A list of builds including HIS functional for KCP&L is listed below:

Build No.	Date	Content
100	5-30-2013	Preliminary HIS configuration (and other DMS functions)
121	11-27-2013	Misc. HIS defect fixes (and other DMS functions)

- **Integrated System Stabilization** – While not an issue of the HIS directly, other systems in the DMS suite did experience some issues achieving stability. To this end, the HIS was very helpful by providing significantly expanded logging of data and message types. In turn, this was used to help better understand the context of real-time network traffic as a potential basis for underlying stability issues.

To be updated in future releases of this report.

2.2.4.6.4 Lessons Learned

Throughout the build and stabilization of the HIS system, numerous considerations were realized and should be noted for future deployments of this sort. These Lessons Learned are as follows:

- **Archival Capacity** – KCP&L scaled its archival database to 300GB, but in an enterprise deployment, significantly larger capabilities could easily be required. Our archive was based on a limited deployment of substation and Distribution Automation (DA) devices (approx. 120 total). Each device had approximately 50-100 points. Each point was recorded to the archive upon status/value change or no more frequently than once every four seconds (whichever occurred less frequently). KCP&L is currently on track to fill this archival DB after one year of recording. Based on configurations for how much data is captured, size of SCADA deployment, and requirements for maintained capabilities, business processes for later consumption of this historical data should be contemplated to size appropriately.
- **Data Revisions** – The HIS offers the capability to revise data that has been previously recorded; but care should be taken when granting permissions to do so. Depending on system usage, it may or may not be mission critical to be able to modify historic real-time DMS/D-SCADA data. Testing at KCP&L showed that these capabilities could have benefited from additional access restrictions which were possible, but not pursued in the demonstration timeframe.
- **Subsequent Build Coordination** – Deployment of incremental software compilations (or builds) must be coordinated with the project team and Siemens to ensure timely delivery and minimal impact to the system.

To be updated in future releases of this report.

2.2.5 SmartGeneration

The SmartGeneration sub-project deployed a state-of-the art Distributed Energy Resource Management (DERM) system to manage several types of distributed energy resources including DR load curtailment programs, grid connected bulk energy storage system, grid connected distributed solar generation, and electric vehicle charging stations. The following subsections summarize these SmartGeneration component deployments.

2.2.5.1 DERM

The OATI WebSmartEnergy DEMS project was implemented to provide the DERM project component. The DERM system stores and manages all information pertaining to demand response and distributed energy resource programs and assets. The DERM system also communicates DR and DER control events to various ‘control authorities’ that manage particular types of resources. The following sections provide a summary of the development and configurations that were required to implement and deploy the desired DERM functionality.

2.2.5.1.1 Build

The DERM implementation began in 2011. The first step in this process was to familiarize KCP&L personnel with the capabilities of the system. OATI project members came to KCP&L for a workshop where they demonstrated the overall system, and then they walked through the components planned for the KCP&L project.

2.2.5.1.1.1 **DERM Base Functionality FAT**

KCP&L and OATI conducted a Factory Acceptance Test covering the base functionality of the DERM from May 22, 2012 through May 25, 2012. Two KCP&L engineers traveled to Minnesota for this testing, and they also received training on the base system functionality at this time. Throughout the testing, variances were logged and prioritized. The major variances discovered during the FAT were all resolved the month following the testing.

2.2.5.1.1.2 **DMS Interface Design**

In parallel with standing up the DERM base functionality, KCP&L also went to work designing the interface between the DMS and the DERM. These two systems are tightly coupled, and they require real time synchronizations in order for the DERM to function properly. Since this was a completely new, custom interface, it required lots of face-to-face time between Siemens, OATI, and KCP&L. In order to design the message exchanges for this interface, KCP&L, Siemens, and OATI met for several days to create use cases for the possible scenarios. The main scenarios that were detailed included:

- Initialization between DMS and DERM – used the first time a new database is applied or after one of the systems has been restarted
- Feeder load management – also called “studycase,” this is an exchange between the DMS and the DERM done in a planning mode
- Feeder load shed – also called “emergency,” this is an exchange between the DMS and the DERM done in real time when an overload has occurred

Upon completion of the DMS/DERM use cases, all parties worked on technical specifications for these interfaces to develop the standards-based messages that would be used to exchange the agreed upon information.

OATI and Siemens went through several phases of interface testing, lasting through the first half of 2013. They started by doing simple message exchange testing – sending content to each other via email and manually loading it into their respective systems. Once the vendors agreed on message content, they began sending their messages through the KCP&L Enterprise Service Bus, which had been designed

to translate and route the messages appropriately. The OATI system sent and received Web Services messages, and the Siemens system utilized JMS messages. After testing through the ESB, they conducted automated testing, where the message exchanges were triggered from various system events. Finally, Siemens and OATI were able to run through entire use case scenarios and test out the sequence of message flows with internal DMS or DERM applications being triggered as designed.

2.2.5.1.1.3 OpenADR Development

The next major work effort for the DERM component of the project was the DERM/HEMP interface design. KCP&L directed OATI and Tendril (the HEMP vendor) to utilize OpenADR 2.0, profile A, for this interface. KCP&L, OATI, and Tendril all became members of the OpenADR Alliance and became engaged in the OpenADR 2.0 development process. Since the A profile was still under development when the design of the interface was underway, KCP&L agreed to have OATI and Tendril design around a particular working draft. Additionally, KCP&L allowed several modifications to the A profile implementation to facilitate the opt-out functionality that was desired for the project.

OATI and Tendril utilized the following OpenADR messages for the DERM/HEMP interface:

- oadrDistributeEvent to schedule events from the DERM to the HEMP
- oadrCreatedEvent message to confirm events from the HEMP to the DERM

Upon completion of the interface, OATI and Tendril conducted point to point testing of the DR messages. After that, they conducted testing via the KCP&L ESB. Finally, they tested out the end-to-end DR scenarios between the DERM and the HAN devices. The details of the demand response events between the DERM and the HEMP are outlined in Section 2.2.5.2 DR Load Curtailment.

2.2.5.1.1.4 Additional Environment

The DERM differs from most of the other systems deployed in the demonstration project, as it is hosted by the vendor instead of managed and maintained by KCP&L. Originally, KCP&L planned to utilize a single instance of the DERM, hosted by OATI in Minnesota. In January 2013, however, as the DMS implementation progressed, the team started to consider the benefits of an additional DERM environment. Since most of the other systems would have two instances, trying to utilize a single DERM for development and production purposes would be complicated. As a result, KCP&L decided to move forward with the configuration and implementation of a second instance of OATI's webDistribute. Upon completion of this system setup, KCP&L connected the development DERM to KCP&L development servers and the development ESB, and they connected the demonstration DERM to its respective demonstration servers and ESB. This was incredibly beneficial to test out various interfaces and environments since so much of the project was divided into various phases.

2.2.5.1.1.5 Battery Interface Development

Early on in the project, KCP&L came up with the concept of "control authorities." The DERM would schedule demand response events, but the control authorities were the systems that actually send the control messages to the end devices that would be utilized for responding to demand response events. KCP&L chose to use the DMS as the control authority for grid-connected resources, such as the battery.

After KCP&L made this decision, Siemens and OATI went to work to design the interface between the DERM and the DMS. OpenADR 2.0 messages were used, and the vendors designed and tested this interface in a similar manner to the major DERM/DMS described above.

2.2.5.1.1.6 ChargePoint Interface Development

The last interface developed from the DERM to a control authority was to the Electric Vehicle Charge System. The ChargePoint system was used as the control system for the ten charging stations deployed in the smart grid project. KCP&L considered using OpenADR 2.0 messages for this interface, but instead

they chose to use the existing ChargePoint API. KCP&L also allowed the communications between these systems to be point-to-point rather than traveling through KCP&L's ESB.

2.2.5.1.1.7 Customer Enrollment and Program Creation

While KCP&L and OATI were working on the interfaces to the various control authorities, they also began the process of loading the customer enrollment information into the system and creating the various demand response programs in the DERM. The customer enrollment information links service point identification (SPID) to any residential home area network (HAN) devices, such as programmable communicating thermostats (PCTs) or load control switches (LCSs). This information is important so that the DERM knows which assets can be called on for a particular portion of the network. For example, if the DERM received word from the DMS that there was an overload on feeder 7551, then the DERM would be able to dispatch DR to all the devices on that particular feeder.

In addition to the enrollment information, KCP&L also worked with OATI to begin creating the DR programs in the DERM. A single device can be enrolled in multiple programs, so for example the smart grid thermostats could be enrolled in both the SG Thermostats program as well as the SG HAN program. Here are the programs that have currently been created in the DERM:

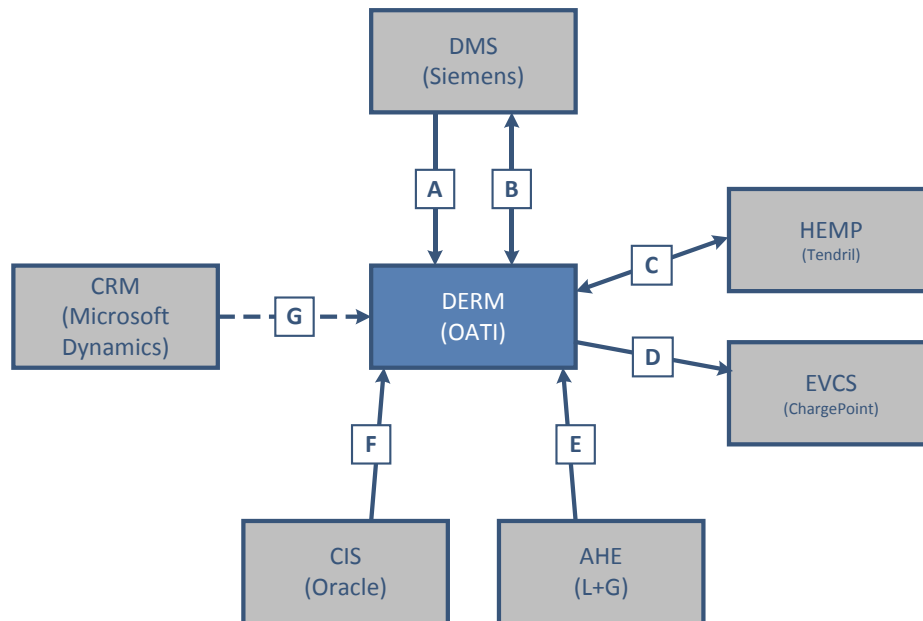
- Test thermostats (only has a few test thermostats enrolled – this was used for testing out DR events in the production environment in a very controlled manner)
- Test load control switches (only has a few test load control switches enrolled – this was used for testing out DR events in the production environment in a very controlled manner)
- SG Thermostats (includes all of the thermostats that were added as part of the smart grid demonstration project)
- SG Load Control Switches (includes all of the load control switches that were added as part of the smart grid demonstration project)
- SG HAN (includes all devices that were deployed as part of a smart grid HAN)
- Battery (only has a single asset – the 1MW-Hr battery located outside Midtown substation)
- ChargePoint (includes the ten electric vehicle charging stations that are part of the ChargePoint interface)
- MPOWER (an existing program for commercial and industrial customers – not part of the smart grid project tariffs, but can be used by the DERM at a later date if desired)
- Optimizer (an existing thermostat program for residential customers – not part of the smart grid project tariffs, but can be used by the DERM at a later date if desired)

2.2.5.1.2 Integration

An overview of DERM system-to-system interfaces and applicable messages is illustrated in Figure 2-61.

The DERM system interfaces with many other KCP&L systems, both for synchronized network models and customer/program enrollment, and for dispatching DR events to various control authorities. The integration touch points for the DERM are as follows:

- A. DMS / DERM Data Model Propagation: The DERM system must synchronize its data model with the D-SCADA to make accurate calculations of its own. The network connectivity model and associated loads are transferred from the DMS to the DERM using a manual CIM RDF export. Generation of the CIM RDF file is done in the Information Model Management (IMM) and then exported via file transfer to OATI. This process is performed whenever a new data model is taken from the GIS, and it requires massaging from OATI to ensure that it's properly digested by the DERM.

Figure 2-61: KCP&L SmartGrid Demonstration Project DERM Integration

- B. **DMS / DERM Dynamic Data Exchange:** In addition to the static model data that's exchanged between the DMS and the DERM, the two systems also exchange a number of dynamic messages on an as-needed basis. The DERM sends and receives Web services messages, whereas the DMS sends and receives JMS (Java Messaging Service) messages, so adapters within KCP&L's Enterprise Service Bus (ESB) serve as translators between the two systems. The dynamic data exchanged between the DMS and the DERM can be categorized by the following interfaces:
- Network Topology Interface – Upon initial synchronization of the two databases, the DERM is notified about each switch state change.
 - Distribution Power Flow (DPF) Interface – The DPF interface allows the DERM to query DPF results from the DMS. For scheduled DERM events, the DERM needs calculated overloads on an hourly basis. The DPF interface generates the data and makes it available to DERM. Additionally, violations are published to the DERM in real time.
 - Study Case Interface – When study cases are created in the DMS, a study case needs to be created in the DERM, as well. This interface provides the messages to do so.
 - Demand Response (DR) Event Interface – DR events affect power flow results, so DERM needs an interface for publishing DR events to the DMS.
 - Battery Interface – The DMS is used as the control authority for the battery, so this interface is used to dispatch DR events for this purpose.
- C. **DERM / HEMP DR Messaging:** This interface includes both the 'Demand Response Event' request initiated from DERM to HEMP, and 'Event Opt-Out/Opt-In' reply initiated from HEMP (for both HANs and Standalone PCTs) to DERM. These are OpenADR-formatted request-reply messages used to notify HEMP of creation, modification, or cancellation of impending DR events and to notify DERM of DR assets' event participation status.
- D. **DERM / EVCS DR Propagation:** A uni-directional interface used to dispatch DR events from the DERM to the ChargePoint EVCS system. All data exchanges in this interface are transmitted via Web Services using ChargePoint's existing API.

- E. AHE / DERM Metering Data: A uni-directional interface from the AMI Head-End (AHE) to the DERM on a daily basis with the previous day's metering interval data. The DERM needs this information to create and update customer baselines. These daily batch files are transferred from the AHE to the DERM via an sftp server.
- F. CIS / DERM Service Point Data: A uni-directional interface from the CIS Server to the DERM on a weekly basis. This transfer is used to link service point identification (SPID) to any residential home area network (HAN) devices, such as programmable communicating thermostats (PCTs) or load control switches (LCSs). This information is important so that the DERM knows which assets can be called on for a particular portion of the network. These weekly files are transferred from KCP&L's CIS Server to the DERM via an sftp server.
- G. Customer Enrollment Data: A uni-directional interface from a combination of data from the CRM, HEMP, and AHE. This file needs significant manual work currently, but the long-term goal is for this process to be automated and sent on a weekly basis. This transfer is used to inform the DERM of DR program enrollment information so that the DERM can link HAN devices with the programs that they're associated with, and to map DR capabilities with distribution transformers. These Excel files are currently transferred via email from KCP&L to OATI for manual loading into the DERM.

2.2.5.1.3 Post-Implementation Operational Issues

The only post-operational issue to date has been the addition of a "heartbeat" message between the DERM and the DMS. This additional message was designed to give KCP&L system operators an alarm on the DMS system summary if the communications path between the two systems was severed for any reason.

To be Completed in future releases of this report.

2.2.5.1.4 Lessons Learned

Throughout the build of DERM, numerous considerations were realized and should be noted for future deployments of this sort. These Lessons Learned are as follows:

- One of the lessons learned with the DERM / DMS integration was that the model propagation between systems is not a trivial feat. Even though the two vendors agreed upon a common version of the CIM data model, there were still issues and tweaks with each model propagation.
- Another lesson learned (in multiple implementations on the demonstration project) was that the standards creation process can be slow and tedious. In order to utilize OpenADR 2.0, KCP&L had to pick a working draft version of the profile and implement to that version. Waiting for the "completed" profile would have been detrimental to the project schedule, so this wasn't an option.
- The last lesson learned from the DERM implementation was that having access to system logs can be extremely helpful during development and integration of a new system. The webDistribute logs are available to the DERM user, and they were very beneficial while testing out the interfaces to all of the control authorities.

To be updated in future releases of this report.

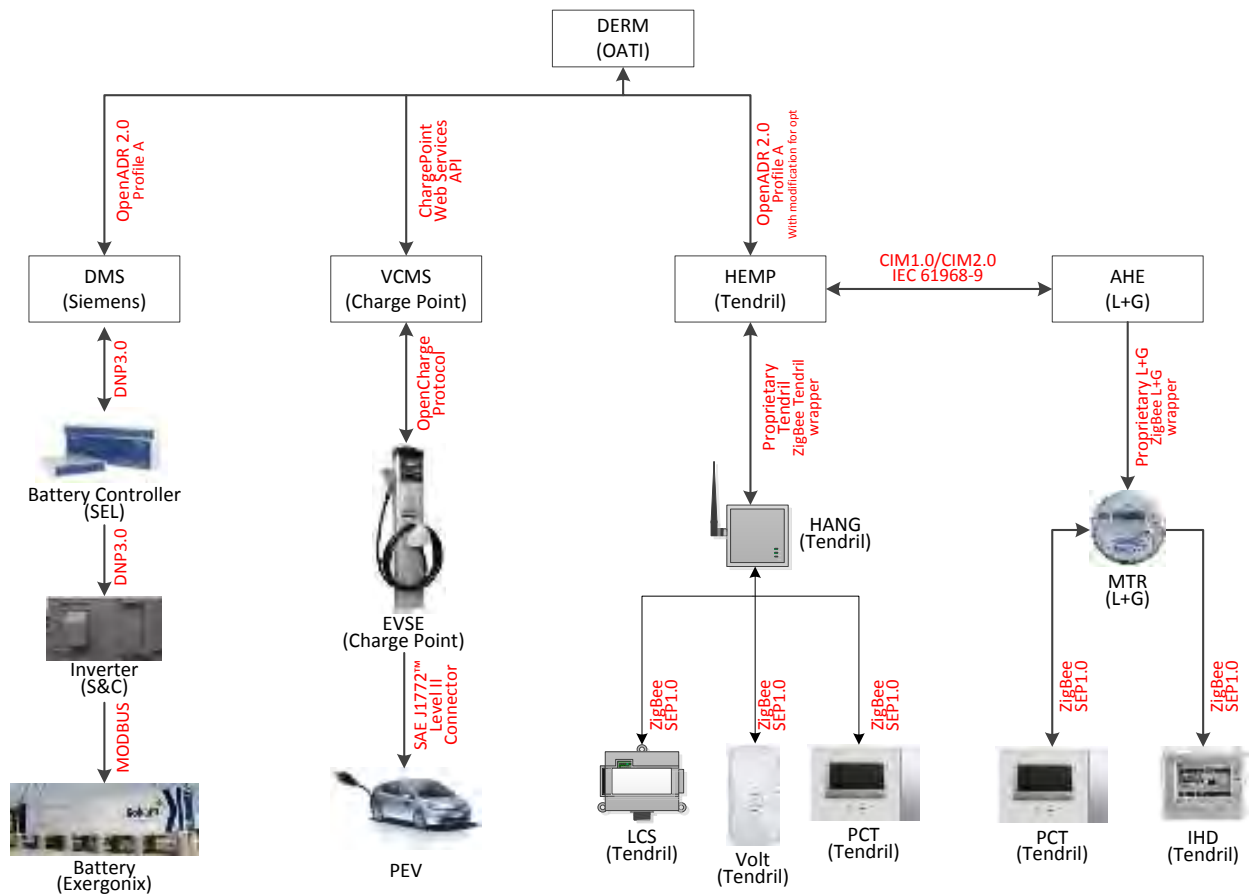
2.2.5.2 DR Load Curtailment

The following sections provide a summary of the development and configurations that were required to implement and deploy the SmartGeneration DR Load Curtailment functionality.

2.2.5.2.1 Build

The demand response (DR) load curtailment programs developed for the demonstration project all required deployment and configuration of DR resources and messaging infrastructure. The development and testing for each program varied depending on the environments available and the messaging standards used. The DR load curtailment integration architecture implemented is illustrated in Figure 2-62.

Figure 2-62: Demand Response Load Curtailment Architecture



2.2.5.2.1.1 Residential Standalone Programmable Communicating Thermostat (PCT)

The Standalone PCT is described in detail in section 2.2.2.3. Through integration between the DERM, HEMP, and AHE, the Standalone PCTs can receive demand response events to help reduce, level, or shift load during peak demand periods. The DERM can forecast demand on the distribution grid and call on the Standalone PCTs for load reduction, if necessary. A message is sent from the DERM to the HEMP to identify the Standalone PCT customers needed to meet the load reduction requirements. The HEMP then routes the demand response messages to the AHE. The AHE passes the demand response events to the Standalone PCTs via the SmartMeters prior to or at the start time of the event, depending on the event parameters. Once received at the Standalone PCT, the customer is automatically opted into event participation with the option to opt out of the event at any time prior to the end of the event. This opt-out/in decision can be made directly at the device. Customer event participation information is then passed to the DERM via the AHE and HEMP to be used for post-event analysis and future demand response forecasting.

In order to test the DR events to the standalone PCTs, KCP&L utilized the development DERM, HEMP, and AHE systems. Messages were triggered manually in the DERM and propagated from system to system, through the development ESB, to the PCTs in the lab environment. Testing in this environment allowed KCP&L to work out issues with firmware versions, messaging structure, and ESB routing, which ensured that no customers would be impacted throughout the intense testing period.

Now that testing in the development environment is complete, KCP&L plans to continue testing in the demonstration environment prior to the summer 2014 demand response season. In order to do this without impacting customers, test events will be sent to the demo house and the Midtown substation battery control enclosure. This will allow the team to verify the DR messaging infrastructure in a safe environment.

2.2.5.2.1.2 Residential Home Area Network (HAN)

The Home Area Network is described in detail in section 0. Through integration between the DERM and the HEMP, the HAN can receive demand response events to help reduce, level, or shift load during peak demand periods. The DERM can forecast demand on the distribution grid and call on the HANs for load reduction, if necessary. A message is sent from the DERM to the HEMP to identify the HAN customers needed to meet the load reduction requirements. The HEMP then routes the demand response messages to the HAN gateways via the broadband connection. The HAN gateway passes the demand response events to the PCTs and LCSs prior to or at the start time of the event, depending on the event parameters. Once received at the PCTs and LCSs, the customer is automatically opted into event participation with the option to opt out of the event at any time prior to the end of the event. This opt-out/in decision can be made directly at the PCTs and LCSs or via the Customer Web Portal. Customer event participation information is then passed to the DERM via the HEMP to be used for post-event analysis and future demand response forecasting.

In order to test the DR events to the HANs, KCP&L utilized the development DERM and HEMP systems. Messages were triggered manually in the DERM and propagated from system to system, through the development ESB, to the HANs, PCTs, and LCSs in the lab environment. Testing in this environment allowed KCP&L to work out issues with firmware versions, messaging structure, and ESB routing, which ensured that no customers would be impacted throughout the intense testing period.

Now that testing in the development environment is complete, KCP&L plans to continue testing in the demonstration environment prior to the summer 2014 demand response season. In order to do this without impacting customers, test events will be sent to the demo house and the Midtown substation battery control enclosure. This will allow the team to verify the DR messaging infrastructure in a safe environment.

2.2.5.2.1.3 Battery Energy Storage System (BESS)

The Battery Energy Storage System (BESS) is described in detail in section 2.2.5.3. Through integration between the DERM and the DMS, the BESS can receive demand response events to help reduce, level, or shift load during peak demand periods. The DERM can forecast demand on the distribution grid and call on the battery to discharge, if necessary. One of the underlying assumptions with this interface is that anytime the battery is placed in DERM mode, the battery is fully charged. This way, the DERM has the potential to discharge the entire battery. Additionally, when the battery is in DERM mode, it cannot be used for other schemes. To utilize the battery for DR, a message is sent from the DERM to the DMS to identify the amount of battery discharge needed to meet the load reduction requirements. The DMS then routes the shed load message to the SICAM, which passes the setpoints on to the Real Time Automation Controller (RTAC). The RTAC then sends the DR battery shed load message on to the inverter, which finally sends the event instructions to the battery itself. The battery will begin to discharge at the rate specified at the designated start time, for the specified duration.

In order to test the DR events to the battery, KCP&L utilized the development DERM and DMS systems. Messages were triggered manually in the DERM and propagated through the ESB to the DMS in the development environment. From the DMS, the setpoints were routed to the SICAM, and then on to the RTAC. In the development environment, KCP&L had no way to verify the last stages of the message propagation; rather, they had to assume that the RTAC logic would properly discharge the battery.

Now that testing in the development environment is complete, KCP&L plans to begin testing in the demonstration environment. Successful DERM battery tests will depend on successful RTAC to inverter to battery tests in the demonstration environment. This demonstration environment testing is planned for early 2014.

2.2.5.2.1.4 Vehicle Charge Management System (VCMS)

The Vehicle Charge Management System (VCMS) is described in detail in section 2.2.5.5. Through integration between the DERM and the ChargePoint system, charging stations can receive demand response events to help reduce, level, or shift load during peak demand periods. The DERM can forecast demand on the distribution grid and call on specific charging stations to stop charging vehicles, if necessary. To utilize the charging stations for DR, a message is sent from the DERM to the ChargePoint system to indicate which charge stations should be turned off at a particular time. Although the DR events to the charging stations won't likely result in much load reduction, KCP&L wants to develop and test out this interface to demonstrate the possibilities for a larger, full-scale VCMS implementation.

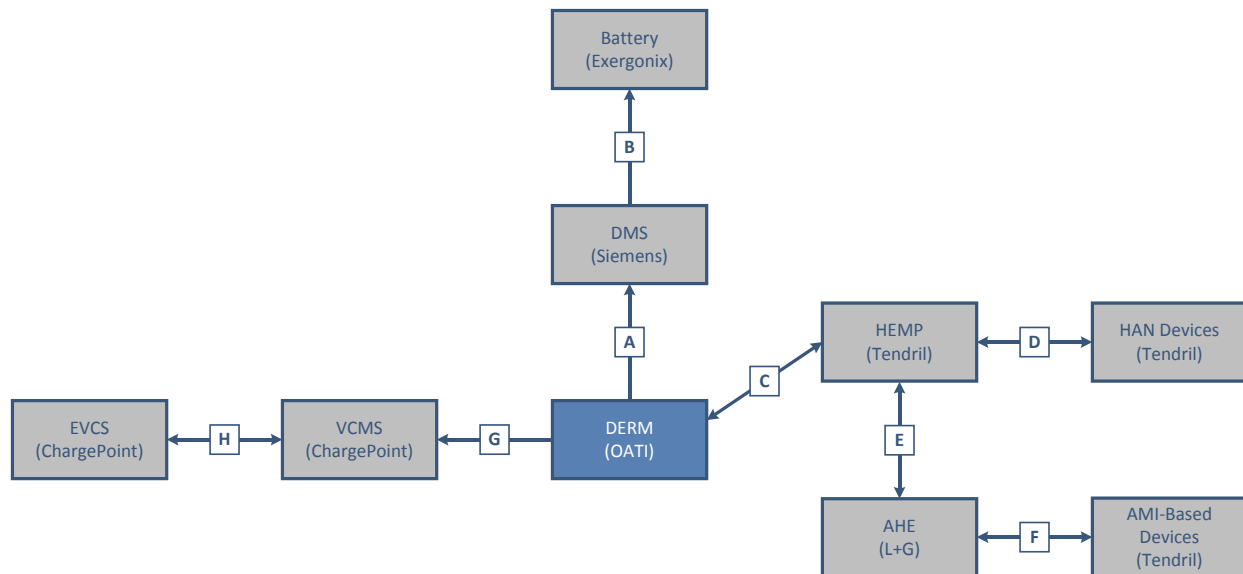
Unlike the other control authorities, the interface from the DERM to the VCMS is a point-to-point interface. This made testing a lot less complicated, as the traffic didn't need to be routed through the KCP&L ESB. OATI and ChargePoint developed a point-to-point interface via the Internet utilizing ChargePoint's existing API function calls. In order to test DR events to the charging stations, KCP&L simply added the charging stations to the DERM and triggered events to specific stations. Since there isn't a development VCMS, the testing was done to an actual production charge station. KCP&L was able to verify that the messages propagated from the DERM to the VCMS via the ChargePoint web UI. Tests were also verified by looking at the screen located at the charging station to see how it changed during DR events.

The next test for the VCMS DR events will include sending an event while an EV is actually plugged into the station. Finally, all of the charging stations will be added to the DERM, and KCP&L will verify that the DERM selects the proper stations for participation in a DR event based on overloads in a particular area of the network.

2.2.5.2.2 *Integration*

An overview of system-to-system interfaces relevant to DR Load Curtailment and applicable messages is illustrated in Figure 2-63.

Figure 2-63: KCP&L SmartGrid Demonstration Project DR Load Curtailment Integration



The Demand Response Load Curtailment programs require many system-to-system and system-to-device interfaces. These integration touch points are as follows:

- A. 'Demand Response Event' request initiated from DERM to DMS. These are OpenADR-formatted request messages sent via the KCP&L ESB and used to notify the DMS of creation, modification, or cancellation of impending DR events to the battery.
- B. 'Demand Response Event' requests initiated from DMS to the battery via the Real Time Automation Controller (RTAC) and the Inverter. These events are DNP3.0 between the DMS to the RTAC and down to the Inverter, and they are Modbus from the inverter to the battery itself. They consist of three set points: kW discharge rate, start time, and duration.
- C. 'Demand Response Event' request initiated from DERM to HEMP, and 'Event Opt-Out/Opt-In' reply initiated from HEMP (for both HANs and Standalone PCTs) to DERM. These are OpenADR-formatted request-reply messages used to notify HEMP of creation, modification, or cancellation of impending DR events and to notify DERM of DR assets' event participation status.
- D. 'Demand Response Event' requests initiated from HEMP to HAN DR assets via the Internet, and 'Event Opt-Out/Opt-In' replies initiated from HAN DR assets to HEMP via the Internet. These are ZigBee Smart Energy Profile (SEP) 1.0-formatted request-reply messages used to notify HAN DR assets of creation, modification, or cancellation of impending DR events and to notify HEMP of HAN DR asset event participation status.
- E. 'Demand Response Event' request initiated from HEMP to AHE, and 'Event Opt-Out/Opt-In' reply initiated from AMI-based DR assets (Standalone PCTs for this project) to HEMP. These are IEC 61968 CIM-formatted request-reply messages used to notify AMI-based DR assets of creation, modification, or cancellation of impending DR events and to notify HEMP of AMI-based DR assets' event participation status.
- F. 'Demand Response Event' requests initiated from AHE to AMI-based DR assets (Standalone PCTs for this project) via SmartMeters, and 'Event Opt-Out/Opt-In' replies

initiated from AMI-based DR assets to AHE via SmartMeters. These are ZigBee Smart Energy Profile (SEP) 1.0-formatted request-reply messages used to notify AMI-based DR assets of creation, modification, or cancellation of impending DR events and to notify AHE of AMI-based DR asset event participation status.

- G. 'Demand Response Event' request initiated from DERM to VCMS. These messages are sent via the Internet (not through KCP&L's ESB), and they utilize ChargePoint's existing API. They are used to notify the VCMS of creation, modification, or cancellation of impending DR events to the charge station infrastructure.
- H. 'Demand Response Event' requests initiated from VCMS to the Electric Vehicle Charge Station (EVCS), and 'Charge Station Status' messages about the real time status of charging stations sent from the EVCS to the VCMS for display on the ChargePoint GUI. Messages in this interface are passed via the Internet using the OpenCharge Protocol.

2.2.5.2.3 Post-Implementation Operational Issues

Since the DR events haven't been exercised in the demonstration environment yet, there are no Post-Implementation Operational Issues to report on at this time. As DR events are dispatched throughout 2014, KCP&L will keep track of issues that occur and summarize findings.

To be completed in future releases of this report.

2.2.5.2.4 Lessons Learned

Throughout the build, implementation, and daily operation of the DR Load Curtailment programs, numerous considerations were realized and should be noted for future implementations. These Lessons Learned are as follows:

- Testing demand response flows in multiple environments was challenging. Originally, KCP&L only utilized a single instance of the DERM, but this led to issues when testing out various flows, as the DERM could only dispatch DR messages to a single instance of the ESB, either development or production. With a single instance of the DERM, KCP&L had to orchestrate consistent phasing between development and demonstration environments in the DERM, DMS, HEMP, AHE, and ESB. Configuring an additional DERM made it feasible to test residential flows in the demonstration environment while testing battery flows in the development environment, for example.

To be updated in future releases of this report.

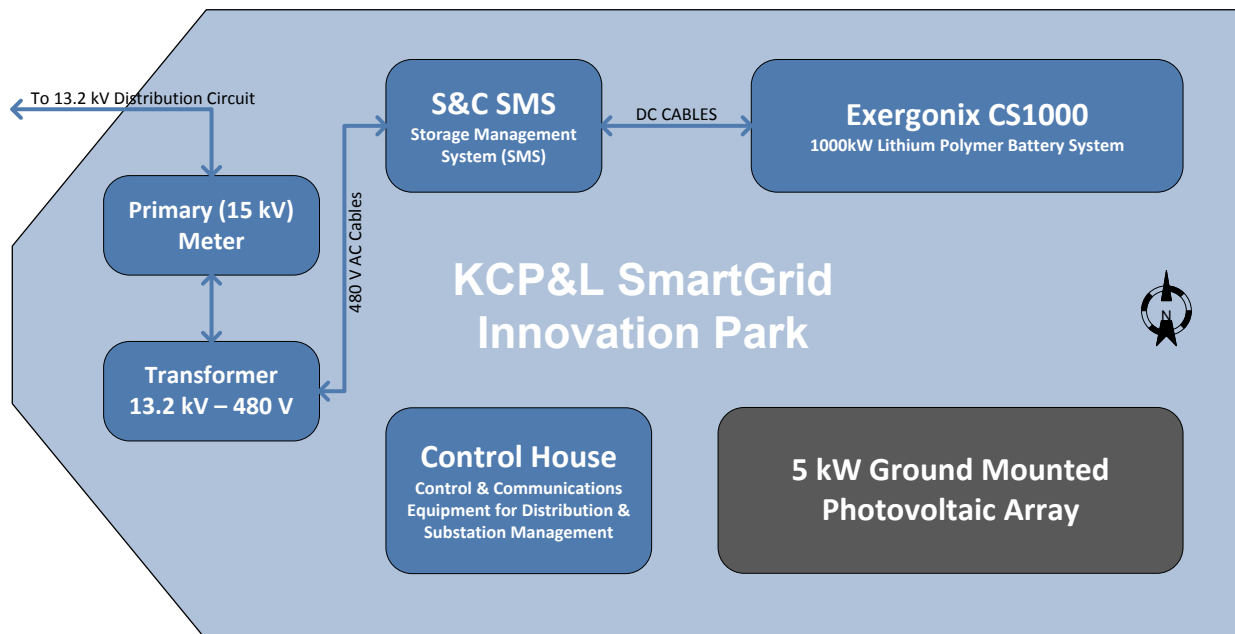
2.2.5.3 BESS

As part of the KCP&L Smart Grid Demonstration Project, a 1.0 MW, 1.0 MWh lithium-polymer grid-connected Battery Energy Storage System (BESS) manufactured by Exergonix was installed adjacent to the Midtown substation. This system includes a 1.25 MVA Storage Management System (SMS), power converter, manufactured by S&C Electric. The following sections provide a summary of the development and configurations that were required to implement and deploy the SmartGeneration DR Load Curtailment functionality.

2.2.5.3.1 Build

Figure 2-64 provides a schematic of the energy storage project's layout at KCP&L's SmartGrid Innovation Park. The site includes the BESS, SMS, smart grid pilot control house equipment, step-up transformer (13.2kV-480V), and associated metering and monitoring equipment. It also includes a 5.0 kW ground-mounted PV array that is grid-connected to the same circuit as the battery through the control house transformer (13.2kV-110V).

Figure 2-64: Innovation Park and BESS Site Overview



2.2.5.3.1.1 Battery Testing and Installation

KCP&L broke ground on the project site in early February 2012 and the BESS arrived in March 2012 after successful completion of factory testing. The battery unit was tested by Exergonix in Korea, while the SMS and a scaled-down version of the battery were factory tested together in Wisconsin at an S&C facility. Interconnection of the SMS and production battery unit occurred on-site in June 2012. The site was completed and unveiled at the opening of the SmartGrid Innovation Park in October 2012. The completed battery system installation is shown in Figure 2-65. The battery enclosure is wrapped in educational content to facilitate community awareness and engagement.

Figure 2-65: BESS Installation

2.2.5.3.1.2 Battery Automation Controller (BAC)

Remote and advanced operation of the BESS through SCADA integration with the DMS is accomplished through the utilization of a custom programmed SCADA controller, the Battery Automation Controller (BAC). The BAC receives control settings from distribution operators or from the DERM via the DMS/DDC. In addition, real-time load data from relays within the substation are provided to the BAC from the DMS/DDC to enable load following storage operations.

2.2.5.3.1.3 Distribution Operation

The battery can be controlled via three means – the distribution operators, the DERM, and locally. Distribution operators may initiate charge/discharge/reactive events within the BESS through the DMS interface. The operator can set various system-level settings through binary and analog points as well as define events through additional analog points. The BAC receives these binary and analog points, processes them, and sends the corresponding SCADA commands to the SMS as required in order to execute the programmed event.

The BAC enables three charge modes, five discharge modes, and four reactive modes:

- Charge Modes:
 - Fixed Charge – specified kW and duration
 - Load Following Charge Feeder – calculated kW based on current feeder load to maintain specified net feeder load
 - DERM Fixed Charge – specified kW and duration
- Discharge Modes:
 - Fixed Discharge – specified kW and duration
 - Load Following Discharge Feeder – calculated kW based on current feeder load to maintain specified net feeder load
 - Load Following Discharge Buss – calculated kW based on current bus load to maintain specified net bus load
 - Load Following Discharge Transformer – calculated kW based on current transformer load to maintain specified net transformer load
 - DERM Fixed Discharge – specified kW and duration

- Reactive Modes:
 - Fixed VAR – specified kVAR and duration
 - Load Following VAR Feeder – calculated kVAR based on current feeder power factor to maintain specified net feeder power factor
 - Load Following VAR Bus – calculated kVAR based on current bus power factor to maintain specified net bus power factor
 - Load Following VAR Transformer – calculated kVAR based on current transformer power factor to maintain specified net transformer power factor

2.2.5.3.1.4 DERM Operation

The BESS is also a controllable Distributed Energy Resource that the DERM may define and engage in a DR event. The DERM sends event information to the DMS via an OpenADR message. The DMS then checks to ensure the BAC is in DERM mode and then automatically sets the corresponding analog points in the BAC which then sends corresponding SCADA commands to the SMS. The DERM only engages the BESS in Fixed Discharge mode as executed by the BAC.

2.2.5.3.1.5 Local Operation

The BESS may also be programmed to charge/discharge on a daily schedule via the local HMI interface in the SMS. One charge event and up to two discharge events may be programmed to occur each day. Each event is based on twenty custom programmable profiles. Each profile is defined by four time/amplitude points (trapezoidal).

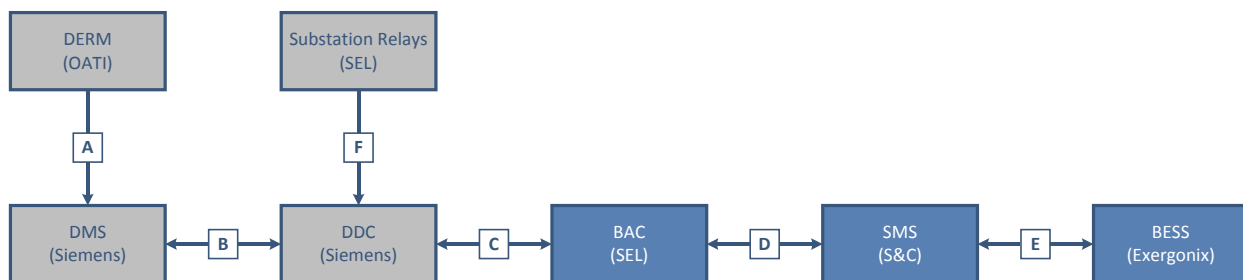
2.2.5.3.1.6 Remote Access

In addition to the three primary operations, KCP&L also enabled remote access to the HMIs of both the SMS and the BESS through secure corporate network connection on direct fiber. This remote access facilitates health monitoring, troubleshooting and emergency control.

2.2.5.3.2 Integration

An overview of system-to-system interfaces relevant to the BESS and applicable messages is illustrated in Figure 2-66.

Figure 2-66: KCP&L SmartGrid Demonstration Project BESS Integration



The BESS control functions require many system-to-system and system-to-device interfaces. These integration touch points are as follows:

- A. 'Demand Response Event' request initiated from DERM to DMS. These are OpenADR-formatted request messages sent via the KCP&L ESB and used to notify the DMS of creation, modification, or cancellation of impending DR events to the battery. Upon receipt of the DR event messages at the DMS, the messages are converted to control signals.

- B. 'Battery Control Signals' sent from the DMS to the DDC and 'Battery Status Updates' sent from the DDC to the DMS for display on the GUI. These messages are IEC61850 messages, and they consist of various setpoints, controls, indicators, and analogs.
- C. 'Battery Control Signals' sent from the DDC to the BAC and 'Battery Status Updates' sent from the BAC to the DDC for upstream propagation back to the DMS. These messages are DNP3.0 messages transmitted via the Tropos wireless mesh network, and they consist of various setpoints, controls, indicators, and analogs.
- D. 'Battery Control Signals' sent from the BAC to the SMS and 'Battery Status Updates' sent from the SMS to the BAC for upstream propagation back to the DMS. These messages are DNP3.0 messages, and they consist of various setpoints, controls, indicators, and analogs.
- E. 'Battery Control Signals' sent from the SMS to the BESS and 'Battery Status Updates' sent from the BESS to the SMS for upstream propagation back to the DMS. These messages are Modbus messages, and they consist of various setpoints, controls, indicators, and analogs.
- F. 'Real Time Load Data' sent from substation relays to the DDC and on to the BAC. This data consists of IEC61850 MMS messages, and it enables load following storage operations.

2.2.5.3.3 Post-operational Issues

Grid-scale energy storage represents a new asset type for KCP&L operations. The BESS has presented a few challenges and has required exceptional preparations and training.

- **Post-Deployment Training** – The BESS is a high voltage source that lacks visible or audible warning conditions typically present at traditional generators such as a combustion engine running. As a result, KCP&L Field crews have undergone extensive training to address BESS system awareness and on-site safety during maintenance and emergency response activities.
- **Alarming** – The BESS is an extremely complex system with numerous alarms and component failure conditions. While the SMS and BESS control systems are capable of isolating alarmed components or battery cells, on numerous occasions, various alarms have caused delays in testing or normal charge/discharge operations due to alarm investigation and troubleshooting. Some example alarm or failure conditions that have been encountered include:
 - Voltage imbalance between battery cells. Out of balance cells are automatically omitted from charge/discharge events, reducing the active capacity of the BESS.
 - Environmental control system failure requiring emergency repair. Operations ceased due to cell overheat risk.
- **Component Replacement** – Various component replacements have been difficult and time consuming to accomplish due to a lack of local vendor support.

To be updated in future releases of this report.

2.2.5.3.4 Lessons Learned

KCP&L has learned some key lessons throughout the past year of BESS operations.

- Since lithium cells require a relatively narrow operating temperature range, the environmental control system is vital to proper operations. It should consist of a hardened design intended to withstand extreme conditions and high reliability. The system should be inspected regularly to ensure proper operation. KCP&L recommends inspection and test of the environmental control and other support systems for the BESS every quarter or prior to each seasonal change.
- Due to the complexity and lack of experience with grid-scale energy storage assets by vendors and within KCP&L, the BESS required a long and tedious operational learning curve. Despite extensive documentation from vendors, numerous conditions and operational applications required consultation and/or direct support from vendors. For example, programming the charge/discharge schedule within the SMS was not documented well enough for KCP&L personnel to execute reliably without intermittent support from vendor representatives. Also, some alarm scenarios arose that weren't well defined in advance or within documentation to facilitate KCP&L direct troubleshooting. KCP&L recommends extensive hand-on training of key personnel in the presence of vendor representatives on all planned operational applications, alarms, and known emergency scenarios. This may represent a significant expense and inconvenience for internal personnel but will result in timely resolution to a majority of anomalous conditions and enable the asset to have greater overall availability.
- Locating this BESS was limited by the KCP&L SmartGrid Demonstration Project geographical footprint and the research goal to demonstrate circuit islanding (needed a circuit with load levels that could be managed by the BESS). As a result, the BESS is interconnected at the head of a short stable urban circuit. This circuit typically exhibits stable primary voltages and power factor thus limiting the operational value and demonstration value of the BESS. Despite these limitations, net impacts of the BESS are clearly observable in operational circuit data. KCP&L recommends narrowing applications for grid-scale energy storage assets to one or two key distribution network trouble areas.
- Lithium polymer battery cell systems are well suited for high frequency and high power applications that require the system to transition from charging to discharging quickly. Target applications might include frequency regulation, renewable integration and ramp-rate management, renewable output smoothing, etc. However, due to a comparatively high cost for energy volume (kWh), this battery technology may not be well suited for energy shifting or peak shaving applications.

To be updated in future releases of this report.

2.2.5.4 Solar PV

As part of the Smart Grid Demonstration Project, KCP&L is working to install approximately 180 kW of diverse solar photovoltaic (PV) systems on commercial properties throughout the pilot project area. The PV systems, with the exception of those installed on utility property, were established through a lease agreement in which KCP&L leases roof-top space but owns and maintains the PV system for a multi-year contract period. Each system will be directly grid connected and metered independently for tracking purposes.

2.2.5.4.1 Build

KCP&L completed the installation of nine separate PV systems listed in with a total nameplate capacity of 176.9 kW. Installed systems are summarized in Table 2-13.

Each of the solar PV systems is connected directly to the grid through an AMI meter. The kWh generated and consumed by the system is captured in 15-minute interval data and sent to KCP&L's Data Mining and Analysis Tool, DataRaker. DataRaker provides the ability to display and download the data for analysis.

Table 2-13: Smart Grid PV Systems Installed

System Location	Panel Technology	Inverter	Capacity (kW)	In-Service Date
Project Living Proof (Demonstration Home)	Monocrystalline	Sunverge	3.15	01/19/2011
Paseo High School Gymnasium Roof-top	Monocrystalline	String	99.18	04/19/2012
Innovation Park (Midtown Substation)	Monocrystalline	String	5.00	10/17/2012
Crosstown Substation	Multiple	SV & Micro	29.33	06/07/2013
MRIGlobal	Polycrystalline	Sunverge	10.56	05/16/2013
UMKC Flarsheim Hall	Polycrystalline	Sunverge	4.32	08/18/2013
UMKC Student Union	Polycrystalline	String	5.28	08/18/2013
Blue Hills	Polycrystalline	Micro	10.08	08/18/2013
KCMO Swope Park Office	Polycrystalline	Micro	10.00	12/31/2013
			176.90	

2.2.5.4.1.1 **Solar Panels [15]**

Two industry-standard types of panels, monocrystalline and polycrystalline, were used throughout the SmartGrid installation area. The difference between Monocrystalline solar cells are produced from a single crystal of silicon, while polycrystalline solar cells are produced from a piece of silicon consisting of many crystals. Since polycrystalline cells contain many crystals, they have a less perfect surface than monocrystalline, and thus absorb slightly less solar energy and produce slightly less electricity per square foot. On the plus side, the process of creating the silicon for a polycrystalline cell is much simpler, so these cells are generally cheaper per square foot. The cost of each type of panel per Watt of power output works out to be about the same, but polycrystalline panels are slightly larger than equivalent monocrystalline panels.

2.2.5.4.1.2 **Racking Systems [15]**

The "Evolution" series racking system, manufactured by DynoRaxx, was used for the solar installations. These racking systems are made from 100% fiberglass, which gives them a couple advantages over metal racking systems. First, the racks do not experience the same thermal expansion issues as traditional metal racking systems do, which can cause key connection points in the system to loosen and fail. Also, traditional metal racking systems can damage unprotected roof surfaces. With the DynoRaxx, KCP&L felt confident that the customer's property would be protected for the life of the system.

2.2.5.4.1.3 Inverters [15]

Three different types of inverters were used for installations in this project:

- **Micro Inverters** – Micro inverters produce grid-matching power directly at the back of the panel. Arrays of panels are connected in parallel to each other and fed to the grid. This has the major advantage that a single failing panel or inverter will not take the entire string offline. The Enphase M215 Micro Inverters and associated cables and Enphase Envoy monitoring system were installed at Blue Hills Community Center.
- **Sunverge Inverter** – The Sunverge Solar Integration System (SIS) is a PV array and battery. It is an intelligent communication platform through which utilities can send messages, tips, instructional demand responses and load management messages to their customers. Sunverge Integration Systems were installed at Project Living Proof, MRIGlobal, and UMKC's Flarsheim Hall.
- **String Inverters** – In a grid-tied system, the solar panels are wired together in series (a "string" of panels) which increases the voltage and keeps the current low so that wiring is simpler and wire size can be smaller. String inverters were installed at Paseo High School, Innovation Park, and the UMKC Student Union.

2.2.5.4.1.4 Data Mining and Analysis Tool (DMAT)

Each of the solar PV systems is connected directly to the grid through an AMI meter. The kWh generated and consumed by the system is captured in 15-minute interval data and sent to KCP&L's Data Mining and Analysis Tool, DataRaker. DataRaker provides the ability to display and download the data for analysis.

2.2.5.4.2 Integration

An overview of system-to-system interfaces relevant to the PV array is illustrated in Figure 2-70.

Figure 2-67: KCP&L SmartGrid Demonstration Project PV Integration



Recording the Solar PV energy production requires minimal system-to-system and system-to-device interfaces. These integration touch points are as follows:

- All PV arrays are direct grid-connected with independent utility revenue-grade metering. The PV arrays don't send messages to the Meter (MTR); rather, they are connected to the meter, so the meter simply reads the received contributions from solar.
- '15 Minute Interval Data' sent from the MTR to the Data Mining and Analysis Tool (DMAT) for use in reporting. The aggregated totals in these data feeds are broken down into received (what solar provides) and delivered (what the customer uses).

2.2.5.4.3 Post-Implementation Operational Issues

Following the installation of the solar PV systems, several post-implementation operational issues needed to be mitigated and considered. These issues are as follows:

- Since the PV arrays would be sending power to the grid as well as receiving power, there was some confusion over direct grid metering conventions for received and delivered kWh. Delivered kWh could mean that the PV array was delivering kWh to the grid, or it could mean that the grid was delivering kWh to the array.

- There was also some debate over which department should be responsible for physical maintenance of the PV systems once they were installed.
- The Sunverge Solar Integration System (SIS) is made up of a PV array and a battery. As such, its metering configuration is different from the configuration of PV arrays with string or micro inverters. Crews needed to be aware of what type of system they were installing.

To be updated in future releases of this report.

2.2.5.4.4 Lessons Learned

Throughout the build, implementation, and daily operation of the solar PV arrays, several considerations were realized and should be noted for future implementations. These Lessons Learned are as follows:

- Establishing roof lease agreements with building and home owners proved difficult and tedious with regards to liabilities.
- A consistent utility standard for distributed generation should be established both for net metering and direct grid connect.

To be updated in future releases of this report.

2.2.5.5 VCMS

The Vehicle Charge Management System (VCMS) deployed an integrated network of electric vehicle charging stations for the SmartGrid Demonstration Project. The VCMS and Electric Vehicle Charging Stations (EVCSs) provide customers with the convenience of public charging, while also providing KCP&L with further demand response resources and capabilities.

2.2.5.5.1 Build

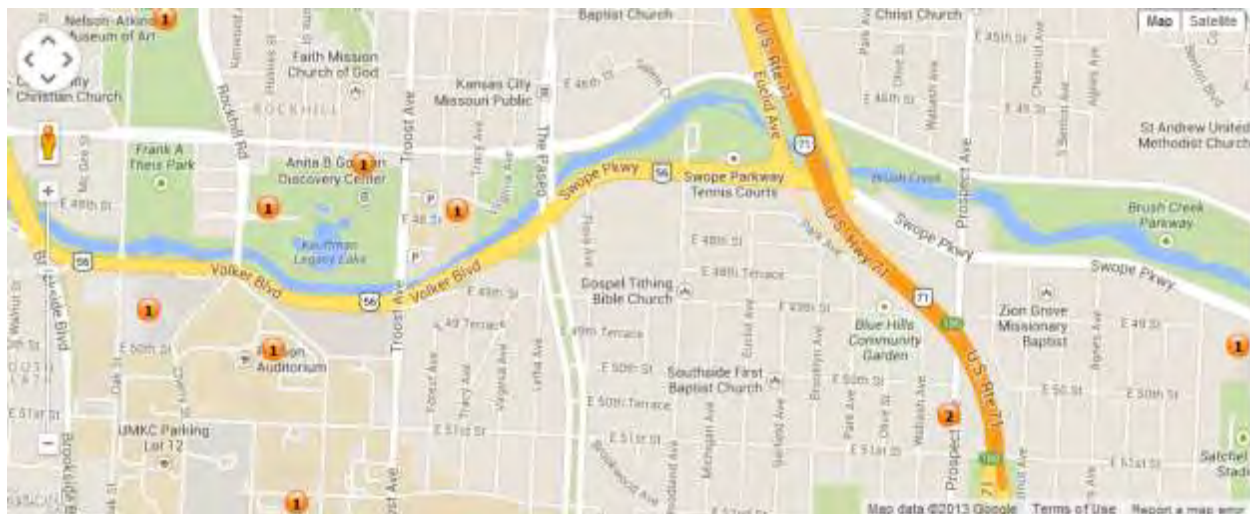
A total of ten EVCSs have been deployed during this implementation. Supply and installation of the EVCSs was managed by LilyPad EV. Each EVCS consists of a dual port, level 2 (240V) Coulomb CT2021 Charging Station with SAE J1772 standard connectors. Each EVCS is equipped with a cellular modem enabling two-way communications with the ChargePoint web platform. This allows electric vehicle owners to locate and reserve individual EVCS using web mapping applications. These charging stations are free for electric vehicle owners to use.

KCP&L monitors and manages each EVCS via the ChargePoint web platform as well. Station summaries, including usage and inventory reports, reservation schedules, and audit reports, are readily available through the platform. KCP&L is also able to manage access control, station provisioning, station alarms, and peak load configurations.

The EVCS locations are:

- Demonstration House
- Midtown Substation
- Midwest Research Institute
- Nelson-Atkins Museum of Art
- UMKC – University Center
- UMKC – Chemical Lab
- Blue Hills Community Center – 2 stations
- Kauffman Foundation
- City of KCMO – Swope Pkwy

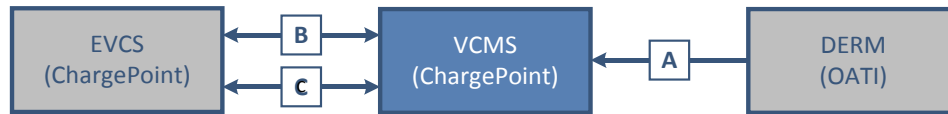
Figure 2-68: ChargePoint Map of SmartGrid EVCSs



2.2.5.5.2 Integration

An overview of system-to-system interfaces relevant to VCMS and applicable messages is illustrated in Figure 2-69.

Figure 2-69: KCP&L SmartGrid Demonstration Project VCMS Integration



The Vehicle Charge Management System is a fairly independent backend system, communicating with only one other “system” – the DERM. The VCMS also communicates with all ten Electric Vehicle Charging Stations (EVCS). These interfaces are summarized as follows:

- A. 'Demand Response Event' request initiated from DERM to VCMS. These messages are sent via the Internet (not through KCP&L’s ESB, like most of the other vendor-to-vendor communications), and they utilize ChargePoint’s existing API. They are used to notify the VCMS of creation, modification, or cancellation of impending DR events to the charge station infrastructure.
- B. 'Demand Response Event' requests initiated from VCMS to the Electric Vehicle Charge Station (EVCS), and 'Charge Station Status' messages about the real time status of charging stations sent from the EVCS to the VCMS for display on the ChargePoint GUI. Messages in this interface are passed via the Internet using the OpenCharge Protocol.
- C. 'Charge Station Status and Usage' data passed between the VCMS and the EVCS. The ChargePoint infrastructure is capable of communicating a variety of commands and status messages between individual charging stations and the VCMS. Some examples include usage data, network status, current charge/discharge status, messages for display on the station screens, and reservation information. Messages in this interface are passed via the Internet using the OpenCharge Protocol.

2.2.5.5.3 Post-Implementation Operational Issues

EVCS status alerts are sent to KCP&L from ChargePoint, and then follow-up actions taken if needed. Any technical issues that arise with charging stations are reported to LilyPad EV for resolution. LilyPad EV handles all equipment repairs and replacements.

To be completed in future releases of this report.

2.2.5.5.4 Lessons Learned

Throughout the build, implementation, and daily operation of the Vehicle Charge Management System, several considerations were realized and should be noted for future implementations. These Lessons Learned are as follows:

- Location is one of the most critical factors in determining EVCS usage. Highly visible, high-traffic areas such as museums, office buildings, and schools are more frequently utilized than some of the less accessible locations.
- Overall usage has increased since the project’s first EVCS were installed. Unfortunately, KCP&L does not have the ability to see how many unique vehicles use the system on a daily basis.

To be updated in future releases of this report.

2.3 Implementation Testing Plans

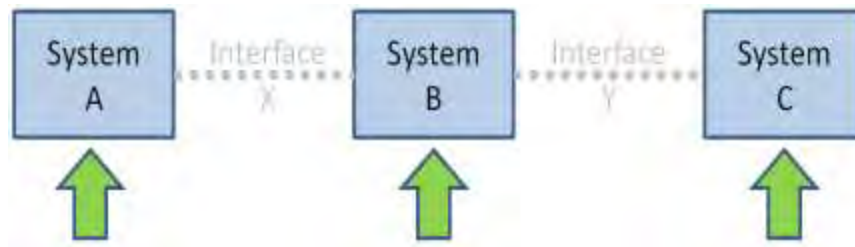
Throughout the prior Implementation section, testing efforts were frequently mentioned in a cursory manner allowing the main focus to stay on the specific considerations for individual systems and integration points. However, as outlined in this section, a very robust and methodical testing approach was pursued to ensure that the implemented systems and interfaces worked as required to successfully demonstrate the scope of this initiative. While each system and interface had its own unique considerations, the philosophical approach was consistent and is elaborated upon here.

All testing efforts were governed by an overarching test strategy document produced early in project which articulated the general roles, responsibilities, and activities to be performed; it is included in Appendix H. To this end, testing was performed as an iterative approach progressing through the following incrementally higher levels of sophistication and will be further described in later sub-sections:

- **System Testing** – This stage of testing was focused on the individual, standalone systems to ensure their internal configurations and functions worked as required. This sub-section articulates considerations for environment setup and configuration, vendor co-located Factory Acceptance Testing, and Kansas City located Site Acceptance Testing. This sub-section concludes with an inventory of the subset of test books included in the appendix of this document; the subset corresponds to only those systems central to the interoperable focus of this initiative. Additional details to be discussed in Section 2.3.1.
- **Integration Testing** – This stage of testing was focused on the highly concentrated verification of communications between two individual systems and/or an individual system and integrated end-point devices; testing ensured that data is properly sent and received. This sub-section articulates considerations for environment setup and configuration, vendor co-located Factory Acceptance Testing, and Kansas City located Site Acceptance Testing. This sub-section concludes with an inventory of the subset of test books included in the appendix of this document; the subset corresponds to only those systems central to the interoperable focus of this initiative. Additional details to be discussed in Section 2.3.2.
- **End-to-End Interoperability Testing** – This stage of testing continues to build upon the earlier detailed testing and allows for verification of cross-system functionality throughout the ecosystem to ensure expected behavior at all points. This sub-section articulates the distinguishing characteristics of “Interoperability Testing”, defines the inventory of systematic data flows, and defines the structure of the interoperability test plans. This sub-section concludes with an inventory of the interoperability test plans included in the appendix. Additional details to be discussed in Section 2.3.3.
- **End-to-End Field Demonstrations** – This stage of testing allowed for the final verification of functionality and documentation of scripts which would be used to facilitate tours and demonstrations. This sub-section articulates the distinguishing characteristics of “Field Demonstrations”, defines the inventory of documented demonstration scripts, and defines the structure of the field demonstration script. This sub-section concludes with an inventory of the scripts included in the appendix. Additional details to be discussed in Section 2.3.4.

2.3.1 System Testing

System Testing involved testing of the individual, standalone systems prior to integration and interface testing. This ensured that the core system configurations and hard-coded capabilities were setup and working as expected. While not testing any of the integration points (which is covered in a subsequent phase of testing), system testing was primarily focused on User Interface (UI), internal algorithms, configurations and data models to verify that these were working to support the overall goals.

Figure 2-70: System Testing

This preliminary testing was vital to ensure that each system and its component functions were working in a stable and dependable manner. Establishment of this firm foundation minimized destabilizing variables in subsequent testing phases and allowed testing and remediation efforts to be focused only on the system without any complicating factors.

Testing efforts began with high-level planning to ensure that environments and staff were available and ready. While environment considerations are elaborated on below, staffing impacts were crucial from the beginning of planning efforts. By ensuring staff availability early on, they were able to participate in design workshops, configuration reviews, and training sessions to maximize their familiarity with the systems. To this end, system tests were handled as independent test efforts with different Subject Matter Experts (SMEs) assigned to different systems and functional capabilities as befitting their individual expertise. The highly skilled SMEs were responsible for the testing of each individual system and confirming adherence to requirements throughout various stages of detailed test planning activities (test script authoring), Factory (FAT), and Site Acceptance (SAT) Testing efforts.

System Testing activities were performed on every system comprising KCP&L's overall SmartGrid implementation. In this way, the formalized methodology and terminology outlined within this section can be read as an elaboration of the general testing efforts called out for individual systems throughout Section 2.2. However, whereas that section includes explicit segmentations of the implementation (particularly where multi-phase approaches were pursued), this section is more of an implicitly performed activity performed within those explicitly defined phases. Also, given the Interoperability objectives of this demonstration project, some of the details and test book inventory in particular, have been filtered to only include detailed descriptions for system testing which enabled 61968, OpenADR, and ZigBee capabilities.

2.3.1.1 Environments

Environments represent a collection of end-point devices and servers that host systems which are isolated in one way or another to enable safe testing with minimal downside. While the environment itself may be isolated and/or partitioned, the numerous systems within an environment can and eventually are connected to one another to enable advanced testing. However, for purposes of individual System Tests at KCP&L, very few of the interfaces were required which allowed preliminary System Testing to be performed in parallel with integration implementation (which in turn would be tested in a subsequent effort).

For KCP&L's implementation, there were two main types of environmental considerations applicable to System Testing: 1) Vendor-Hosted vs. Internally-Hosted Systems and 2) Environment Delineation and Code Promotion. These are explored in greater detail in the following sub-sections:

2.3.1.1.1 Vendor-Hosted vs. Internally-Hosted Systems

All systems for this implementation fall into one of the two following buckets. The specific status of each individual system are documented in their respective implementation descriptions in Section 2.2.

- **VENDOR-HOSTED** – This server hardware was owned and operated by vendors. The vendor had responsibility to perform all hardware and software maintenance at their facilities. The vendor was also responsible for all software upgrades and supported KCP&L as necessary to ensure sufficient integration access was established. As defects were identified, the vendor remediated and applied to their servers in coordination with KCP&L.
- **INTERNALLY-HOSTED** – This hardware was owned and operated by KCP&L. Servers for INTERNALLY HOSTED Systems were procured by KCP&L and configured with standard KCP&L enterprise software (e.g. virus scanning, etc.). This hardware was ultimately sited at KCP&L facilities. As a result, whenever software changes were delivered, it was KCP&L's responsibility to install software to servers.

2.3.1.1.2 Environment Delineation & Code Promotion

At incremental points of the systems development lifecycle, different environments were used as a means to isolate software advanced to different levels of maturity and stability. Each incremental environment had additional capabilities in terms of input and output data types.

2.3.1.1.2.1 DEVELOPMENT / SUPPORT ENVIRONMENTS

These servers were initially used by vendors for development, configuration, and pre-testing activities. At early stages of development, several systems in these environments were originally sited at vendor facilities for preliminary configuration even if they were not destined for a VENDOR-HOSTED configuration. These system environments are primarily used to ensure that minimal levels of functionality were working in tightly controlled conditions allowing vendors to make significant advancements independently.

Configuration and test executions were performed by vendors with the result that KCP&L end-users had very limited access to this environment - typically only in coordination with vendor staff. At later points in the product lifecycle, the development environment could remain independent, but its configurations would be synchronized with the DEMO environment allowing vendors to investigate issues that are discovered in the LAB and DEMO environments (at which point the environment is generally considered the SUPPORT environment). For systems destined for a VENDOR-HOSTED configuration, the vendor provided equipment was initially stood up to enable preliminary demonstration and testing. For systems destined for an INTERNALLY-HOSTED configuration, KCP&L was responsible for hardware procurement and shipped the physical equipment to appropriate locations for initial configuration and setup.

2.3.1.1.2.2 LAB ENVIRONMENT

These servers were used in close coordination with DEVELOPMENT servers; as vendors stabilize modules of code, they promoted them into this environment where KCP&L end-users had significantly greater access. For systems destined for a VENDOR-HOSTED configuration, the vendor provided equipment was stabilized to enable incremental demonstration and testing. For systems destined for an INTERNALLY-HOSTED configuration, KCP&L was responsible for hardware procurement and shipped the physical equipment to appropriate locations for initial configuration and setup; KCP&L staff then had remote access to the servers to test as needed. Note that INTERNALLY-HOSTED LAB servers may be remotely configured, before they were transitioned to KCP&L facilities during later INTEGRATION Testing. By establishing a distinction between LAB and DEVELOPMENT, vendors were free to pursue solutions which could inadvertently break other functionality; by performing these actions in DEVELOPMENT, the LAB environment can be used without fear of "tripping" over work that is still being worked.

2.3.1.1.2.3 DEMO ENVIRONMENT

These servers were the final point of the promotion path for compiled software and operated in a production context. Given that integration capabilities were minimal during System Testing, efforts continued to be focused on ensuring that the systems had appropriate user access permissions and stable execution of its core capabilities. These systems existed in parallel to the LAB systems and were available for use simultaneously to the LAB systems, but had different data to reflect their use as production systems.

VENDOR-HOSTED DEMO systems remained at vendor sites but were implemented with end-state remote access capabilities. INTERNALLY-HOSTED DEMO systems were separate systems that were setup in parallel to LAB systems. These servers and systems were ultimately integrated into the overall DEMO environment and were physically setup in secure locations. These systems were procured by KCP&L and had been setup to have similar configurations and settings as tested in the LAB environment.

Tight controls were in place to ensure that any code promotions were socialized and approved by pertinent parties. Whenever new functionality was deployed into this environment, preliminary testing was performed to ensure that it was working in the new environment and that no new defects had been introduced due to nuances of the environment. KCP&L end-users had access to the systems based on prescribed system access permissions; caution was used when performing operations in these systems because they would ultimately be integrated with other systems and devices that would have real-world implications. Also since this was a production environment, habits needed to be established to engage and coordinate with DSO and field crews as necessary to ensure safe operating conditions.

2.3.1.2 Factory Acceptance Testing (FAT)

This was the capstone activity to the main system development activities performed by the vendor. It was conducted at Vendor-based facilities and KCP&L testing team members travelled to the vendor site to perform the testing on the system. Factory Acceptance Testing (FAT) was executed to demonstrate that the core capabilities were operational and that the system was ready to be migrated for more robust, KCP&L hands-on testing. As FAT was a prerequisite to installation on site, System FAT was done to ensure the system met the pre-set specifications and all functional requirements were met as specified in the design requirements. It was typical that testing activities would result in identification of functions that did not work as expected. In these cases, identified defects would be documented and prioritized for resolution (fixed immediately where possible).

FAT included both structured and unstructured testing to thoroughly test the base functionality of the custom systems and their sub-components. When executed, efforts were mainly performed by the vendor team, but the KCP&L testing team was involved at the vendor site to monitor the FAT activities, identify defects, and track them to resolution. Where possible, the vendor team endeavored to have major defects resolved at the vendor site and during the FAT activities. Changes and fixes could be installed easily at the vendor site rather than at KCP&L where the constraints would increase (involving KCP&L change control and diminished familiarity with installation protocols). The two main stages to FAT were as follows:

2.3.1.2.1 System Factory Acceptance Test (FAT) Planning

Prior to the KCP&L System FAT teams traveling to vendor facilities, significant efforts were conducted in advance to ensure maximum effectiveness while onsite. These activities included:

- **Standard Test Book Reviews** – Standard test books were created and available from vendors for their products. These were provided to KCP&L in the early stages of the project for planning purposes. Standard test books were reviewed by the test team to ensure the tests were comprehensive and that the detailed steps are logical.

- **Test Book Customization** –In some cases, the test team determined that some functionality was not required and removed those functional tests. Alternatively, the test team determined other cases where the standard test book was insufficient and that greater testing was required. In these cases, additional test cases and steps were drafted and included into the test book. The customized test books were then shared with the vendor to ensure agreement on the scope of the test execution effort.

2.3.1.2.2 System Factory Acceptance Test (FAT) Execution

Based on the preparations directly above, the KCP&L System FAT teams began efforts to review the functionality as configured

- **Pre-FAT Execution** – As vendors concluded their initial configuration efforts in the DEVELOPMENT environments, they began comparing the implemented functionality against the tests documented in the test book. Many of these efforts were performed independently by the vendor, but in preparation for FAT execution some of these tests were monitored by the KCP&L testing teams. Upon successful demonstration of preliminary functionality, the system code and configurations were migrated out of the DEVELOPMENT and into LAB where it was ready for formalized FAT execution.
- **Structured Testing** – Once the vendors were sufficiently confident of their system's configuration, the KCP&L team traveled to the vendor facility to jointly work through the documented test book and verify that it was working as expected in the LAB environment. This portion of testing was primarily performed by the vendors with KCP&L staff monitoring the system performance. Much of this activity strictly adhered to the steps outlined in the test book documentation.
- **Unstructured Testing** – Conducted in parallel with Structured testing, this effort was somewhat more vague in that it allowed the testing team to be inspired and test functionality in ways not exactly documented to see how the system performed. Similar to the structured testing, the vendor performed the actions necessary in response to questions asked by KCP&L to see certain functionality. This was done because some of these tests were not possible to consider in advance due to a lack of understanding of system capabilities.
- **Variance Documentation** – Throughout the FAT execution, there were numerous functional items that did not perform within tolerances. These variances were documented and tracked to help increase the stability and functional capabilities of the system. Once a sufficient number of variances were resolved, the system was ready to be migrated out of the LAB environment into the DEMO environment for System Site Acceptance Testing (SAT).

2.3.1.3 Site Acceptance Testing (SAT)

This was the first step to deploying the systems for real-world use. It was used to demonstrate that the core capabilities verified in the controlled vendor environments continued to work in end-state environments. The system had already gone through FAT, but the relocation of the system and installation in a new environment and the additional nuances of real world connectivity (as compared to a more simulated environment at the vendor site) introduced new complexities and challenges into the system. The system must be further tested on site to ensure that the design specifications were met and that the system was ready to be fully integrated and ready for further exhaustive integration testing.

Site Acceptance Testing (SAT) followed a similar structure to FAT but additionally confirming that the system is stable at the KCP&L site with the real world data and complexities. Similarly, it was comprised

of structured and unstructured testing. The KCP&L testing team performed SAT activities completely autonomously, with occasional support from the vendors. The two main stages to SAT were as follows:

2.3.1.3.1 System Site Acceptance Test (SAT) Planning

Prior to the KCP&L System SAT teams beginning onsite testing, significant efforts were conducted in advance to ensure maximum effectiveness. These activities included:

- **Standard Test Book Reviews** – Standard test books were created and available from vendors for their products. These were provided to KCP&L in the early stages of the project for planning purposes. Standard test books were reviewed by the test team to ensure the tests were comprehensive and that the detailed steps are logical. These books were very similar to the test books used during Factory Acceptance Testing (FAT).
- **Test Book Customization** –In some cases, the test team determined that some functionality was not required and removed those functional tests. Alternatively, the test team determined other cases where the standard test book was insufficient and that greater testing was required. In these cases, additional test cases and steps were drafted and included into the test book. The customized test books were then shared with the vendor to ensure agreement on the scope of the test execution effort. In addition, the test team will begin to identify test data and scenarios that can be applied to the finalized test cases.

2.3.1.3.2 System Site Acceptance Test (SAT) Execution

Based on the preparations directly above, the KCP&L System SAT teams began efforts to review the functionality as configured

- **Pre-SAT Execution** – As the systems were prepared for SAT testing, changes were implemented in the DEMO environments. Vendors began shifting their VENDOR-HOSTED configurations to DEMO environments. KCP&L IT began receiving INTERNALLY-HOSTED hardware and installing as necessary. Where possible and ready, the systems were also migrated into the DEMO environments. In all cases, systems were established and stabilized. Systems were reviewed by the test team on a daily basis to ensure stability and readiness for more robust testing.
- **Structured Testing** – As the system stabilized, the KCP&L team began conducting tests from the documented test book and verified that it was working as expected in the DEMO environment. This portion of testing strictly adheres to the steps outlined in the documentation.
- **Unstructured Testing** – Conducted in parallel with Structured testing, this effort was somewhat more vague in that it allowed the testing team to be inspired and test functionality in ways not exactly documented to see how the system performed. This was done because some of these tests were not possible to consider in advance due to a lack of understanding of system capabilities.
- **Variance Documentation** – Throughout the SAT execution, there were numerous functional items that did not perform within tolerances. These variances were documented and tracked to help increase the stability and functional capabilities of the system. Once a sufficient number of variances had been resolved, the system is ready for additional levels of testing (e.g. Integration, Interoperability, Demonstration).

2.3.1.4 Details

As mentioned in the beginning of this section, System Testing was performed for all systems. As such, a test book was created and executed for each system. However, given the Smart Grid program's focus on 61968, OpenADR, and ZigBee capabilities, only a subset of test books are being included for reference as

part of this report. Table 2-14 lists the functional area and specific system test books which have been included in Appendix I. However, they are not the exact test books from the project and instead are a standardized iteration for purposes of this report to highlight the capabilities and testing objectives. In many cases, the actual test books included individual test steps on the specific systems and in some cases, included proprietary or confidential vendor information about their system's internal functionality.

Table 2-14: System Test Books

Functional Area	System	Appendix I: Sub-Appendix Location
Smart Substation	Substation HMI	I.1.1 HMI.FAT
		I.1.2 HMI.SAT
Smart Substation	SICAM	I.1.3 SICAM.FAT
		I.1.4 SICAM.SAT
Smart Substation	DCADA	I.1.5 DCADA.P3FAT
		I.1.6 DCADA.P3SAT
Smart Distribution	DMS	I.1.7 DMS.P1FAT
		I.1.8 DMS.P1SAT.P2P.SUB
		I.1.9 DMS.P2FAT.REDUNDANCY
		I.1.10 DMS.P2FAT.UI
		I.1.11 DMS.P2SAT.P2P.CB
		I.1.12 DMS.P2SAT.P2P.FCI
		I.1.13 DMS.P2SAT.REDUNDANCY
		I.1.14 DMS.P2SAT.UI
		I.1.15 DMS.P3FAT.651R
		I.1.16 DMS.P3FAT.CDNA
		I.1.17 DMS.P3FAT.RTAC (BATTERY)
Smart Distribution	HIS	I.1.18 DMS.P3SAT.CDNA
		I.1.19 DMS.P3SAT.P2P.651R
Smart Distribution	HIS	I.1.20 HIS.P3SAT
Smart Generation	DERM	I.1.21 DERM
Smart Metering	MDM	I.1.22 MDM
Smart Metering	AHE	I.1.23 AHE (Core)
		I.1.24 AHE (Meter Test)
Smart End-Use	HEMP	I.1.25 HEMP
Smart End-Use	HAN	I.1.26 HAN
		I.1.27 HAN (Additional Tests)

2.3.2 Integration Testing

Integration Testing involved testing of the individual connections between standalone systems to ensure accurate preliminary communications. This ensured that the core communications configurations and enabling functions were setup and working as expected. While not testing any comprehensive, end-to-end connectivity (which is covered in a subsequent phase of testing), integration testing was primarily focused on data transmission, data translation, data receipt, firewall configuration, and Message Queue (MQ) configuration to verify that these were working to support the overall goals. This testing consumed a considerable amount of project work due to the complexities between systems and the focus on quality which ensured the operation in a stable and dependable manner. Establishment of this solid communications framework minimized destabilizing variables in subsequent testing phases and allowed testing and remediation efforts to be focused only on the integration without any complicating factors.

Figure 2-71: Integration Testing

Testing efforts began with high-level planning to ensure that environments and staff were available and ready. While environment considerations are elaborated on below, staffing impacts were crucial from the beginning of planning efforts. By ensuring staff availability early on, they were able to participate in design workshops, configuration reviews, and training sessions to maximize their familiarity with the interface functions. To this end, integration tests were handled as independent test efforts with different Subject Matter Experts (SMEs) assigned to different systems and integration capabilities as befitting their individual expertise. The highly skilled SMEs were responsible for the testing of each individual integration point and confirming adherence to requirements throughout various stages of detailed test planning activities (test script authoring), Factory (FAT), and Site Acceptance (SAT) Testing efforts.

Integration Testing activities were performed on every interface connecting the various systems of KCP&L's overall SmartGrid implementation. In this way, the formalized methodology and terminology outlined within this section can be read as an elaboration of the general testing efforts called out for individual systems throughout Section 2.2. However, whereas that section includes explicit segmentations of the implementation (particularly where multi-phase approaches were pursued), this section is more of an implicitly performed activity performed within those explicitly defined phases. Also, given the Interoperability objectives of this demonstration project, some of the details and test book inventory in particular, have been filtered to only include detailed descriptions for system testing which enabled 61968, OpenADR, and ZigBee capabilities.

2.3.2.1 Environment

Environments represent a collection of end-point devices and servers that host systems which are isolated in one way or another to enable safe testing with minimal downside. In earlier testing efforts (particularly System Testing), the environments themselves are isolated and/or partitioned, but the systems within an environment are also autonomous. At this stage of testing, the environments remain independent, but the systems within were connected to one another to comprise a more comprehensive, integrated entity enabling advanced testing. However, for purposes of individual System Tests at KCP&L, very few of the interfaces were required which allowed preliminary System Testing to be performed in parallel with integration implementation (which in turn would be tested in a subsequent effort).

For KCP&L's implementation, there were three main types of environmental considerations applicable to System Testing: 1) Enterprise Service Bus (ESB) vs. Point-to-Point Integration, 2) Vendor-Hosted vs. Internally-Hosted Systems and 2) Environment Delineation and Code Promotion. While many of the high-level considerations from System Testing remain the same, they each have a different twist as applicable to integration testing. These are explored in greater detail in the following sub-sections:

2.3.2.1.1 Enterprise Service Bus (ESB) vs. Point-to-Point Integration

All systems interfaces for this implementation fall into one of the two following buckets. Specific status of individual interfaces are outlined in Section 2.2, but reiterated as pertinent here.

- ENTERPRISE SERVICE BUS (ESB) – This hardware was owned and operated by KCPL and acted as an intermediary layer of integration to ensure that data is properly transformed and made available to downstream systems. ESB capabilities were used more extensively for the interoperability functions leveraging 61968, OpenADR, and ZigBee standards. For many of these data exchanges, extra effort was pursued for the enhanced capabilities in this layer of exchange. As a result, extra dedicated testing was required to ensure that these data transformations were being properly performed.
- POINT-TO-POINT – Other systems had integration requirements to enable certain functions, but as they were not central to the interoperability demonstration, the integration was not pursued along the ESB channel. In these cases, interfaces were developed allowing direct, POINT-TO-POINT communications using proven web service and other proprietary capabilities to allow message transfers.

2.3.2.1.2 Vendor-Hosted vs. Internally-Hosted Systems

As mentioned in the system testing section, all systems are either internally-hosted or vendor-hosted. Keeping this in mind there are specific considerations applicable to integration testing with these different hosting situations.

- VENDOR-HOSTED – This hardware was owned and operated by vendors. For many of these systems interfacing with other VENDOR-HOSTED systems, significant effort was expended to route these communications through the ESB to the greatest extent possible. However, in certain circumstances, POINT-TO-POINT functionality was required for expediency (particularly in scenarios not subject to Interoperability Testing). In all VENDOR-HOSTED situations, testing activities were highly coordinated with vendor development teams to ensure that data flows were working as expected. When integration improvements were required, the vendors directly implemented changes to the systems on their premises.
- INTERNALLY-HOSTED – The hardware for these systems was owned and operated by KCP&L. To this end, the ESB itself was also an INTERNALLY-HOSTED system. As with VENDOR-HOSTED systems, these systems could also leverage the ESB or POINT-TO-POINT communications, but POINT-TO-POINT was more common. Of particular note, testing efforts for these systems could be conducted with greater autonomy, but when integration defects were discovered, additional documentation and coordinated demonstrations became necessary to ensure that vendors providing remote support were properly able to verify the root cause of issues.

2.3.2.1.3 Environment Delineation & Code Promotion

At incremental points of the systems development lifecycle, different environments were used as a means to isolate integration capabilities advanced to different levels of maturity and stability. Each incremental environment has additional capabilities in terms of data volumes and validity.

2.3.2.1.3.1 DEVELOPMENT / SUPPORT ENVIRONMENTS

As mentioned in the Systems Testing section, the DEVELOPMENT environments were used by vendors for their initial configurations efforts. It was also used by KCP&L technologists for development / configuration and pre-testing activities. At early stages of development, all systems were originally supported at vendor facilities.

These DEVELOPMENT environments were mostly independent which resulted in testing integration capabilities leveraging special development harnesses, integration simulators, and manual payload inputs/outputs. The goal of these activities was to ensure that systems were able to appropriately handle core data exchange capabilities. As a result, certain interfaces destined for connectivity via the

KCPL-hosted ESB were not connected in this environment. Instead, simulators were used to ensure that the upstream and downstream systems were properly able to handle expected payloads.

These environments were primarily used to ensure that minimal levels of functionality were working in tightly controlled conditions allowing vendors to make significant advancements independently. To this end, configuration and test executions were performed by vendors. KCPL end-users had very limited access to these environments; typically only in coordination with vendor staff. Upon preliminary confirmation of functionality by the vendor, any code or configuration changes were ready to be migrated to the LAB environment.

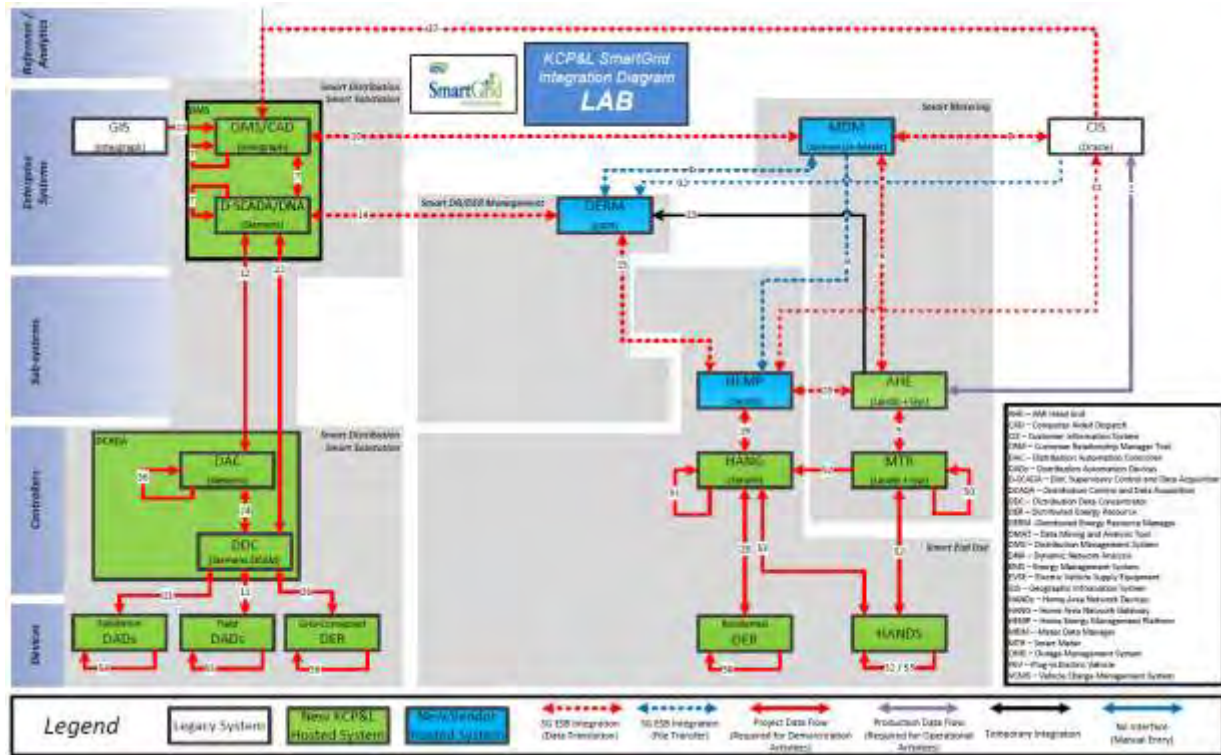
At later points in the product lifecycle, the development environment could remain independent, but its configurations were synchronized with the DEMO environment allowing vendors to investigate integration issues that were discovered in the LAB and DEMO environments. At this point, this environment was generally considered the SUPPORT environment.

2.3.2.1.3.2 LAB ENVIRONMENT

As mentioned in the System Testing section, the LAB environment was next in the code promotion process. However, as described here in the Integration Testing section, the naming rationale for the LAB becomes more appropriate for a number of reasons.

To start, this environment evolved to an integrated suite of systems allowing for the first instances of actual system to system communication. This subset of the entire end-state systems allowed for redundant testing capabilities of the most central interface pathways. Any VENDOR-HOSTED systems remained at vendor sites with preliminary integration capabilities to enable testing and when users access these systems, they do so remotely. INTERNALLY-HOSTED systems used remotely for System Testing, continued to be use remotely though temporarily connected to devices in KCP&Ls LAB facility for preliminary testing. For more advanced testing, the servers were resent to KCPL and were permanently integrated into the overall LAB environment. In general, these servers and systems were then physically setup in secure locations next to their corresponding instances of DEMO hardware. This enabled KCP&L to have a physical and virtual replication of the DEMO environment to determine system capabilities, limitations, and other functional considerations. To this end, VENDOR-HOSTED and INTERNALLY-HOSTED systems are integrated with each other via the ESB or POINT-TO-POINT protocols as required. Firewall, VPNs, and other cyber security features are leveraged for tightly controlled communications and to provide a safe environment to ensure that these configuration approaches are ready for promotion to the DEMO environment. The integrated systems are shown in Figure 2-72.

Figure 2-72: SmartGrid LAB Environment Integrated Systems



Furthermore, these systems are built around two physical laboratory rooms which were designed to include single instances or handfuls of end-use devices for distribution automation (DA) and home area network (HAN) testing capabilities. All systems and devices were integrated with each other to provide a safe area for testing.

The first LAB room (below) was setup with substation and DA equipment logically representing two real-world circuits. For demonstration purposes these circuits were represented by a dynamically interactive “light show” which could tangibly represent outages and sectionalizations being simulated in the systems.














The second LAB room (below) was setup with AMI and home area network (HAN) as a representation of end-use residential and commercial customers in the real world.



In all, the physical LABs included quite a few devices which were very important to KCP&L's ability to progress integration testing. Through the use of these numerous physical devices, in conjunction with their directly associated parent systems, the LAB environment was used for initial KCP&L verification of newly delivered capabilities. In addition, it also served as a means to retest variance fixes to core systems prior to implementation in the DEMO environment. Table 2-15 outlines the full inventory of all devices deployed for use in the LAB environment.

Table 2-15: Devices Deployed in LAB Environment

Device Type	Device Details	Count
Substation Protection Network Devices	 SEL 751A Feeder Breaker	2
	 Eberle REG-DA Load Tap Changer (LTC)	1
Distribution Automation (DA) Devices	 S&C Cap Bank Controllers	2
	 Horstmann Fault Current Indicator (FCI) Receiver and paired set of FCIs	1 "Family"
	 SEL 651R Recloser Controllers	5
	 SEL RTAC Battery Controller	1
Field Area Network (FAN) Devices	 Tropos 1310 – Edge Router	5
	 Tropos 6320 – Gateway Router	1
Smart Meters	 L+G AMI Meter	15
Home Area Network (HAN) Devices	 Tendril Programmable Controllable Thermostat (PCT)	5
	 Tendril In-Home Display (IHD)	5

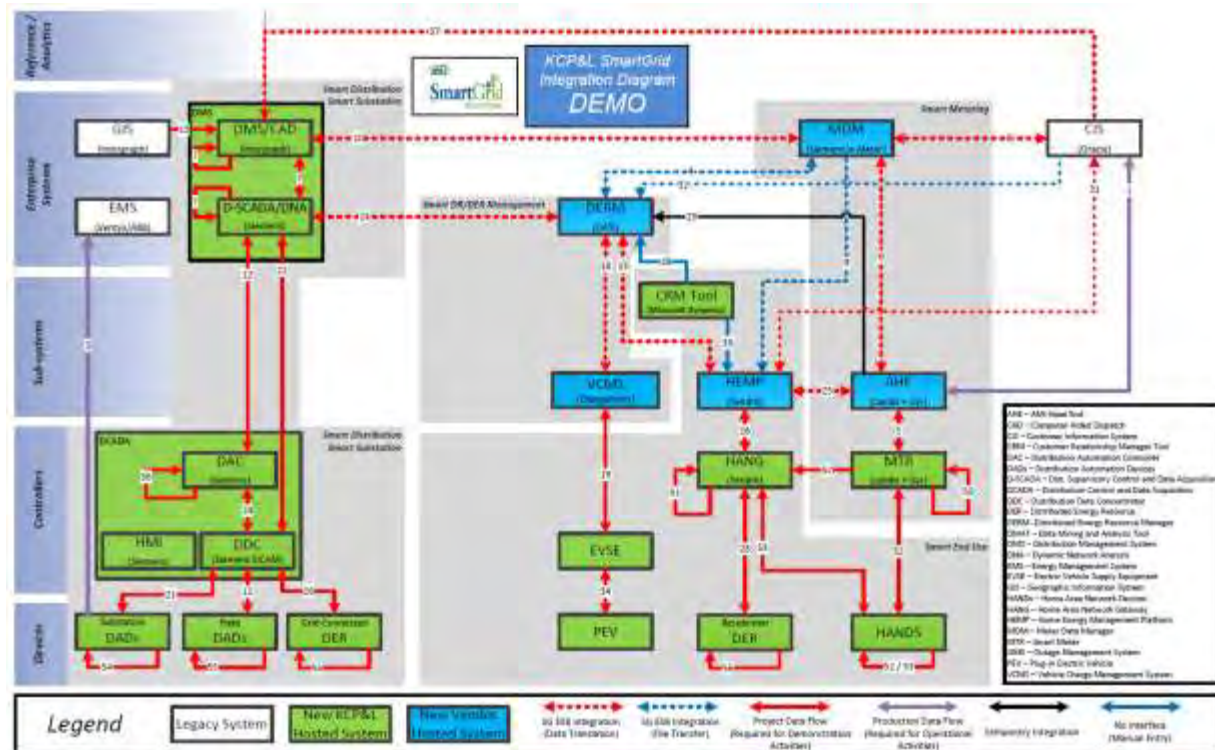
In general, LAB represented a controlled environment in which very specific test cases were conducted. Furthermore, it allowed users to establish an initial comfort level with newly delivered integration capabilities and variance fixes allowing for sandbox testing of communications between systems. This environment didn't impact any end-use customers and represented a safe zone to test out scenarios for any functionality to be promoted to the DEMO environment. This was the first time in the environment promotion pathway where KCP&L end-users had significant access to navigate the system and test its capabilities.

2.3.2.1.3.3 DEMO ENVIRONMENT

As mentioned in the System Testing section, the DEMO environment was the final environment of the code promotion process. Just as with the LAB environment, this environment also evolved from a collection of standalone systems. However, whereas the LAB evolved to establish communications with LAB devices, as an integrated suite of systems DEMO evolved to allow for system-to-system and system-to-real-world-device communication. As such, extreme care was taken while executing tests in this environment as they would have real-world impacts in many instances of use.

Any VENDOR-HOSTED systems remained at vendor sites with preliminary integration capabilities to enable testing; when users access these systems, they do so remotely. INTERNALLY-HOSTED systems were initially setup during System Testing but were now ready to be configured for communication with other systems. To this end, VENDOR-HOSTED and INTERNALLY-HOSTED systems were integrated with each other via the ESB or POINT-TO-POINT protocols as required. Firewall, VPNs, and other cyber-security features were leveraged for tightly controlled communications to provide a safe environment for communications. The integrated systems are shown in Figure 2-73.

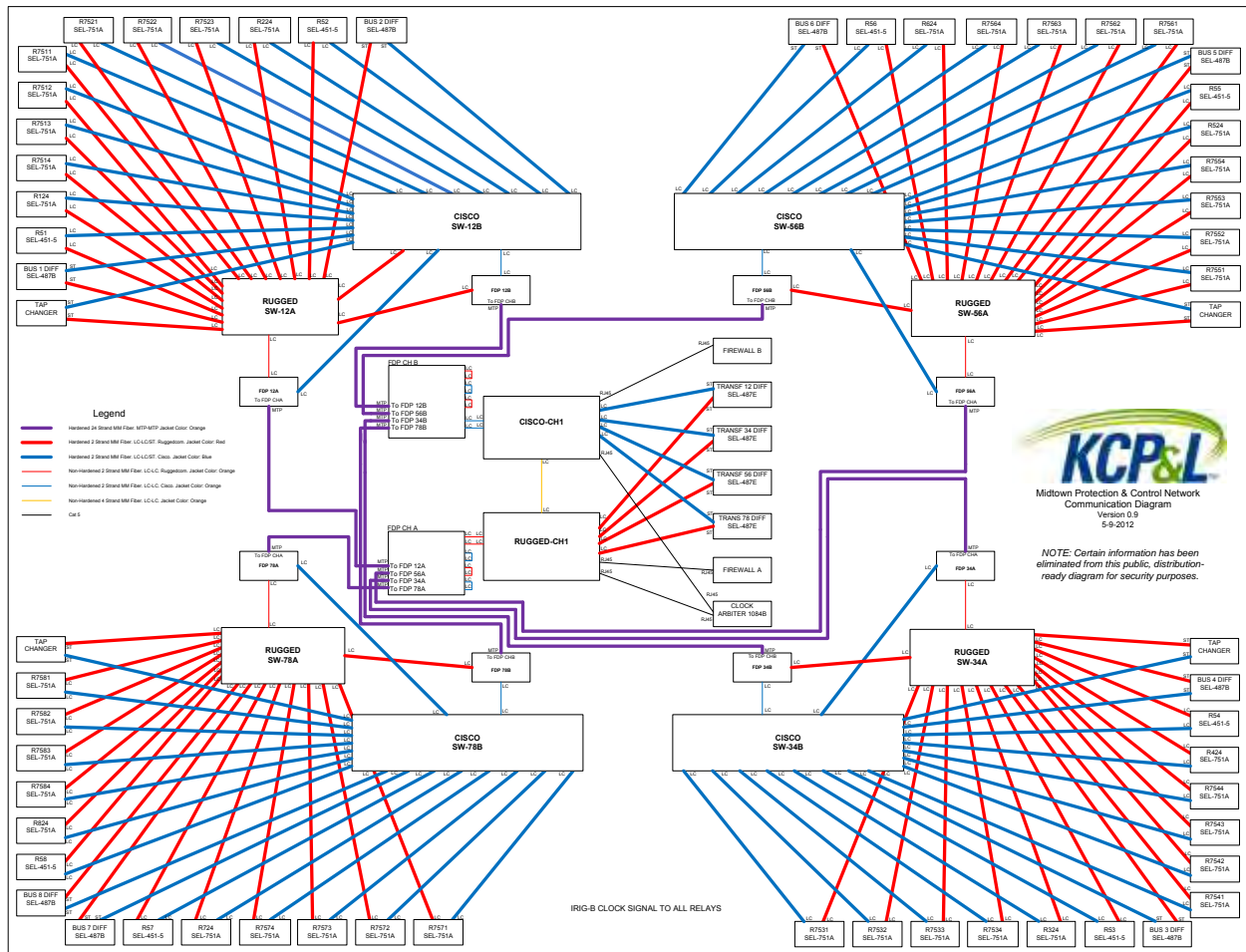
Figure 2-73: SmartGrid DEMO Environment Integrated Systems



Furthermore, in order for these systems to be fully tested in preparation for real-world use in this environment, it was absolutely imperative that they were able to communicate with various real world devices in addition to communicating between systems. Unlike the LAB environment, DEMO had significantly more devices which required deployment in real-world conditions. There were three main settings in which devices were deployed for the DEMO environment: Midtown Substation, Highly-Automated Circuits, and Smart-End Use Program Participant Residences.

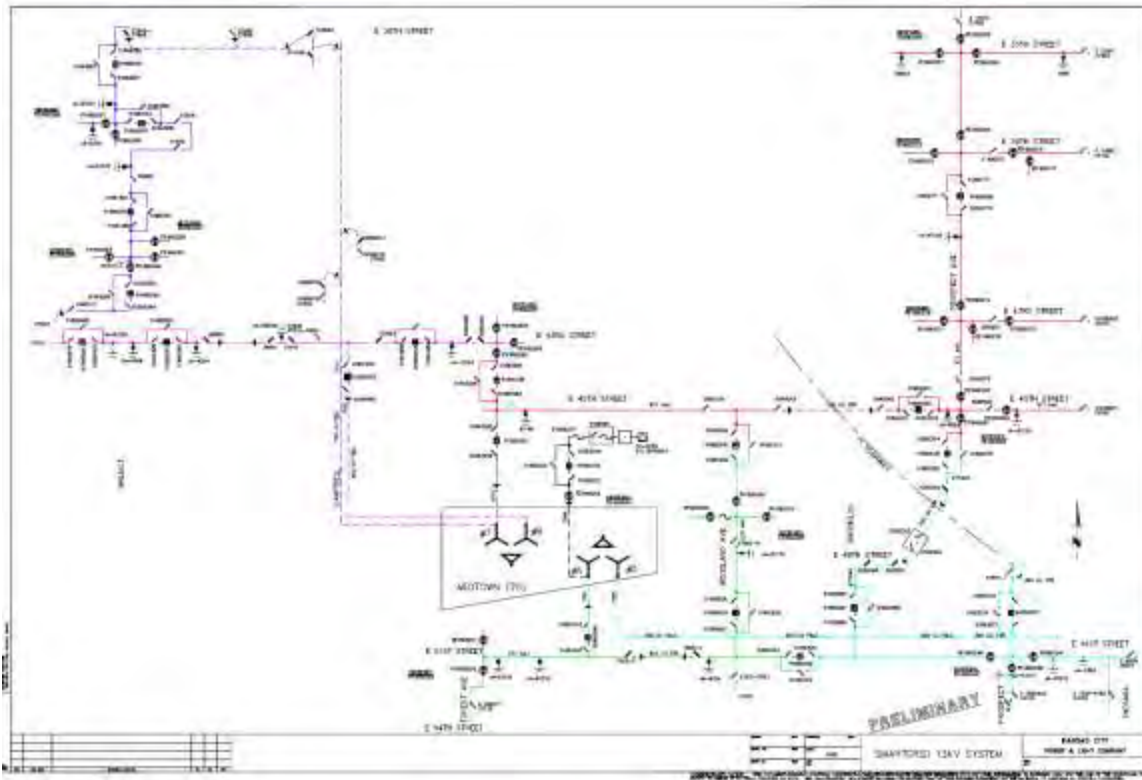
The first setting was KCP&L’s Midtown Substation. With the entire substation affected, significant coordination was required with various operations groups to ensure minimal disruption to customers and a safe operating environment for crews to deploy and connect the devices. The scope of the deployment is shown in Figure 2-74.

Figure 2-74: Midtown Substation



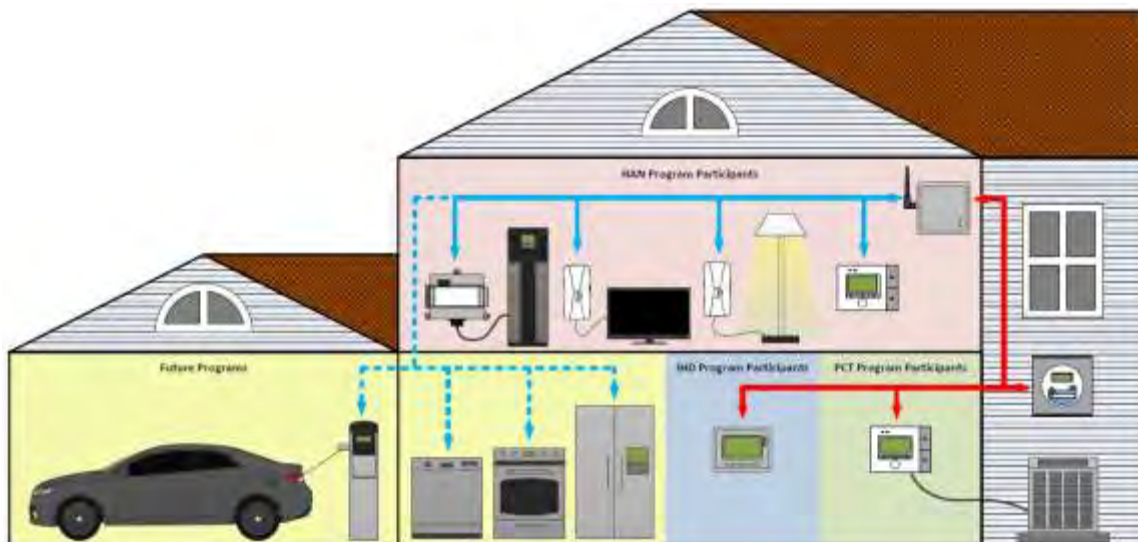
The second setting was a collection of six of KCP&L’s real-world highly-automated distribution feeders radiating from the Midtown Substation. As shown in the one-line diagram in Figure 2-75, circuits were chosen in such a way that various reclosers, capacitor banks, and faulted circuit indicators (FCIs) could work together to demonstrate the results of the DMS algorithms such as Volt/VAR Control (VVC), Fault Location (FLOC), Feeder Load Transfer (FLT), and Fault Isolation and Service Restoration (FISR).

Figure 2-75: Midtown Substation and Distribution Feeders



The third setting was a much larger collection of various KCP&L’s customers who opted to participate in one of the available Smart End-Use programs. These programs comprised the In Home Display Program (IHD), Programmable Controllable Thermostat Program (PCT), and the Home Area Network Program (HAN). Due to the relatively large number of participants in these programs, a representative diagram for the entire deployment is not feasible for this section, but Figure 2-76 does represent the scope of each of these programs to some degree. The full scope of this deployment should be appropriately considered when contemplating the overall scale of this environment.

Figure 2-76: SmartEnd-Use Home Configuration



In all, the physical device deployments in each setting were very important to KCP&L’s ability to progress integration testing in the DEMO environment. Through the use of these numerous physical devices, in conjunction with their directly associated parent systems, the DEMO environment was the final point in the promotion pathway and used for final KCP&L verification of operational capabilities. Table 2-16 outlines the full inventory of all devices deployed for use in the DEMO environment.

Table 2-16: Devices Deployed in DEMO Environment























Device Type	Device Details	Count	
Substation Protection Network Devices		SEL 451-5 Main Breaker	8
		SEL 487B Bus Differential	8
		SEL 487E Transformer Differential	4
		SEL 751A Feeder Breaker	31
		SEL 751A Tie Breakers	8
		Eberle REG-DA Load Tap Changer	4
Distribution Automation (DA) Devices		SEL 651R Controllers & paired Siemens Reclosers	10 Pairs
		SEL 651R Controllers & paired G&W Reclosers	10 Pairs
		S&C Cap Bank Controllers & paired S&C IntelliCAP+ Capacitor Banks	29 Pairs
		Horstmann Fault Current Indicator (FCI) Receivers and paired sets of FCIs	12 “Families”

Table 2-16: Devices Deployed in DEMO Environment (Continued)

Device Type	Device Details		Count
Distributed Energy Storage		SEL RTAC Battery Controller	1 Set
		S&C SMS Battery Inverter	
		Exergonix DESS CS1000	
Field Area Network (FAN) Devices		Tropos 1310 – Edge Router (Radios connected to DA Devices)	62
		Tropos 6320 – Base Router (Radios establishing back-bone communications)	43
Smart Meters		L+G AMI Meter – Residential	12,188
		L+G AMI Meter – Commercial	1,245
Home Area Network (HAN) Devices		Tendril Home Area Network Gateway (HANG)	59
		Tendril Programmable Controllable Thermostat (PCT)	109
		Tendril In-Home Display (IHD)	625
		Tendril Volt	117
		Tendril Load Control Switch (LCS)	12
PEV Charging Stations		ChargePoint Electric Vehicle Charging Station	9

In general, DEMO represented the least controlled environment in that it contained the most number of real-world complicating variables. As this environment impacted end-use customers, tight controls were in place to ensure that any code promotions are socialized and approved by pertinent parties prior to installation to the DEMO servers. Whenever new functionality was deployed into this environment, preliminary testing was performed to ensure that it was working in the new environment and that no new defects had been introduced due to nuances of the environment. KCPL end-users had access to the systems based on prescribed system access permissions; caution was used when performing operations between these systems because they could result in real-world operations. Also since this was a production environment care needed to be taken to engage and coordinate with DSO and field crews as necessary to ensure safe operating conditions.

2.3.2.2 Factory Acceptance Testing (FAT)

This was the capstone activity to the main integration development activities performed by the vendor. It was conducted at Vendor-based facilities and KCP&L testing team members travelled to the vendor site to perform the testing on the system. Factory Acceptance Testing (FAT) was executed to demonstrate that the integration capabilities were operational and that the system was ready to be migrated for more robust, KCP&L hands-on testing. As FAT was a prerequisite to installation and connection with other systems on site, Integration FAT was done to ensure the system and interfaces met the pre-set specifications and all functional requirements were met as specified in the design requirements. It was typical that testing activities would result in identification of integration functions that did not work as expected. In these cases, identified defects would be documented and prioritized for resolution (fixed immediately where possible).

FAT included both structured and unstructured testing to thoroughly test the base functionality of the interfaces. When executed, efforts were mainly performed by the vendor team, but the KCP&L testing team was involved at the vendor site to monitor the FAT activities, identify defects, and track them to resolution. Where possible, the vendor team endeavored to have major defects resolved at the vendor site and during the FAT activities. Changes and fixes could be installed easily at the vendor site rather than at KCP&L where the constraints would increase (involving KCP&L change control and diminished familiarity with installation protocols). In many cases, Integration FAT could be conducted during the same vendor site visit as System FAT, but performed after verifying the core system capabilities were working as expected. The two main stages to FAT were as follows:

2.3.2.2.1 Integration Factory Acceptance Test (FAT) Planning

Prior to the KCP&L Integration FAT teams traveling to vendor facilities, significant efforts were conducted in advance to ensure maximum effectiveness while onsite. These activities included:

- **Test Books** – Test books were created and available from vendors for their productized and customized interfaces. Given the more custom nature of integration between systems, vendors may have created these based on requirements specification. These were provided to KCP&L in the early stages of the project for planning purposes.
- **Customization** – Vendor provided test books were reviewed by the test team to ensure the tests were comprehensive and that the detailed steps were logical. In some cases, the test team determined that some functionality was not required and removed those functional tests. Alternatively, the test team may have determined that the test book was insufficient and that additional testing was required. In these cases, additional test cases and steps were drafted and included into the test book. The customized test books were then shared with the vendor to ensure agreement on the scope of the test execution effort.

2.3.2.2.2 Integration Factory Acceptance Test (FAT) Execution

Based on the preparations directly above, the KCP&L Integration FAT teams began efforts to review the functionality as configured:

- **Pre-FAT** – As vendors concluded their initial configuration efforts in the DEVELOPMENT environments, they began comparing the implemented functionality against the tests documented in the test books. Many of these efforts were performed independently by the vendor, but in preparation for FAT execution some of these tests were monitored by the KCP&L testing teams. Upon successful demonstration of preliminary integration functionality, the code and configurations were migrated out of the DEVELOPMENT environment and into LAB where it was ready for preliminary FAT execution.
- **Structured Testing** – Once the vendor was sufficiently confident of the system and integration configurations, the KCP&L team traveled to the vendor facility to jointly work through the documented test book and verify that the integration capabilities were working as expected. This portion of testing is primarily performed by the vendors with KCP&L staff monitoring the system performance. Much of this activity strictly adhered to the steps outlined in the documentation.
- **Unstructured Testing** – Conducted in parallel with Structured testing, this effort was somewhat more vague in that it allowed the testing team to be inspired and test functionality in ways not exactly documented to see how the interfaces performed. Similar to the structured testing, the vendor performed the actions necessary in response to questions asked by KCP&L to see certain functionality. This is done because some of these tests were not possible to be considered in advance due to a lack of understanding of interface capabilities.
- **Variance Documentation** – Throughout the FAT execution, there were numerous functional items that did not perform within tolerances. These variances were documented and tracked to help increase the stability and functional capabilities of the integration capabilities. Once a sufficient number of variances had been resolved, the system was migrated out of the Development environment into the DEMO environment for Integration Site Acceptance Testing.

2.3.2.3 Site Acceptance Testing (SAT)

This was the first step to deploying the interfaces and preparing them for real-world communications between systems. It was used to demonstrate that the core integration capabilities verified in the controlled vendor environments continued to work in end-state environments. The system had already gone through FAT, but the relocation of the system and installation in a new environment and the additional nuances of real world connectivity (as compared to a more simulated environment at the vendor site) introduced new complexities and challenges into the system. The interfaces and system responses must be further tested on site to ensure that the design specifications were met and that the individual interfaces were ready to be fully integrated and ready for further exhaustive end-to-end interoperability testing.

Site Acceptance Testing (SAT) followed a similar structure to FAT but additionally confirming that the interfaces were stable at the KCP&L site with the real world data and complexities. Similarly, it was comprised of structured and unstructured testing. The KCP&L testing team performed SAT activities completely autonomously, with occasional support from the vendors. In many cases, Integration SAT could be conducted in parallel with System SAT, but performed after verifying the core system capabilities were working as expected. The two main stages to SAT were as follows:

2.3.2.3.1 Integration Site Acceptance Test (SAT) Planning

Prior to the KCP&L Integration SAT teams beginning onsite testing, significant efforts were conducted in advance to ensure maximum effectiveness. These activities included:

- **Test Books** – Test books were created and available from vendors for their productized and customized interfaces. Given the more custom nature of integration between systems, vendors may have created these based on requirements specification. These were provided to KCP&L in the early stages of the project for planning purposes.
- **Customization** – Vendor provided test books were reviewed by the test team to ensure the tests were comprehensive and that the detailed steps were logical. In some cases, the test team determined that some functionality was not required and removed those functional tests. Alternatively, the test team may have determined that the test book was insufficient and that additional testing was required. In these cases, additional test cases and steps were drafted and included into the test book. The customized test books were then shared with the vendor to ensure agreement on the scope of the test execution effort. In addition, the test team will begin to identify test data and scenarios that can be applied to the finalized test cases.

2.3.2.3.2 Integration Site Acceptance Test (SAT) Execution

Based on the preparations directly above, the KCP&L Integration SAT teams began efforts to review the functionality as configured:

- **Pre-SAT** – As the systems were prepared for SAT testing, changes were implemented in the DEMO environments. Vendors began shifting their vendor-hosted configurations to DEMO environments. KCP&L IT received final internally-hosted hardware and installed as necessary. In all cases, interfaces were established and stabilized; special care was paid to ensure that KCP&L hosted ESB capabilities were working as expected to support integration. Systems and interfaces were reviewed by the test team on a daily basis to ensure stability and readiness for more robust testing.
- **Structured Testing** – As the interfaces stabilized, the KCP&L team began conducting tests from the documented test book and verified that it was working as expected. This portion of testing strictly adheres to the steps outlined in the documentation.
- **Unstructured Testing** – Conducted in parallel with Structured testing, this effort was somewhat more vague in that it allows the testing team to be inspired and test functionality in ways not exactly documented to see how the system performs. This was done because some of these tests were not possible to consider in advance due to a lack of understanding of interface capabilities.
- **Variance Documentation** – Throughout the SAT execution, there were numerous functional items that did not perform within tolerances. These variances were documented and tracked to help increase the stability and functional capabilities of the system and interfaces. Once a sufficient number of variances had been resolved, the systems and integration capabilities were ready for additional levels of testing (e.g. Interoperability, Demonstration).

2.3.2.4 Details

As mentioned in the beginning of this section, Integration Testing was performed for all system to system communications. As such, a test book was created and executed for each system interface. However, given the Smart Grid program's focus on 61968, OpenADR, and ZigBee capabilities, only a subset of test books are being included for reference as part of this report. The table below lists the functional area and specific system test books which have been included in Appendix I. However, they

are not the exact test books from the project and instead are a standardized iteration for purposes of this report to highlight the capabilities and testing objectives. In many cases, the actual test books included individual test steps on the specific systems and in some cases, included proprietary or confidential vendor information about their system's internal functionality.

Table 2-17: Integration Test Books

Functional Area	System Integration	Appendix I: Sub-Appendix Location
Smart Distribution	DMS-DERM	I.2.1 DMS-DERM (Joint Vendor Testing) I.2.2 DMS-DERM (DERM Focus)
Smart Distribution	OMS-MDM: Outage Restoration	I.2.3 OMS-MDM (Outage Restoration Event) I.2.4 OMS-MDM (Outage Restoration – Flex Sync)
Smart Generation	OMS-MDM: Power Status Verification	I.2.5 OMS-MDM (Power Status Verification)
Smart Metering	DERM-HEMP	I.2.6 DERM-HEMP (DERM Focus)
Smart Metering	AHE-MDM	I.2.7 AHE-MDM (L+G Adapter) I.2.8 AHE-MDM (MDM VPN) I.2.9 AHE-MDM (MTR Connect-System Side Processing) I.2.10 AHE-MDM (ESB Processing) I.2.11 AHE-MDM (Outage Restoration Event) I.2.12 AHE-MDM (Outage Restoration – Flex Sync) I.2.13 AHE-MDM (Power Status Verification)
Smart End-Use	MDM-CIS	I.2.14 MDM-CIS (Aggregation) I.2.15 MDM-CIS (RSO Detail) I.2.16 MDM-CIS (RSO E2E) I.2.17 MDM-CIS (RSO Online GUI) I.2.18 MDM-CIS (RSO Web Services) I.2.19 MDM-CIS (L+G Adapter) I.2.20 MDM-CIS (MDM VPN) I.2.21 MDM-CIS (Outage Restoration Event) I.2.22 MDM-CIS (Power Status Verification)
Smart End-Use	HEMP-AHE	I.2.23 HEMP-AHE (Network & Device Comms.)

2.3.3 End-to-End Interoperability Testing

End-to-End Interoperability Testing represents the final detailed testing effort in which each step of a given cross-system data flow is tested. In earlier stages of testing, verification efforts thoroughly confirmed the detailed functionality and communications between individual systems. This effort allowed for detailed, end-to-end functionality confirmation which could span multiple combinations of systems and connecting interfaces. To this end, this effort represented a convergence between all system-specific and integration capabilities previously tested. The test team's familiarity with the systems and interfaces up to this stage represented vital institutional knowledge that were key inputs to conducting these Interoperability tests and verifying End-to-End functionality.

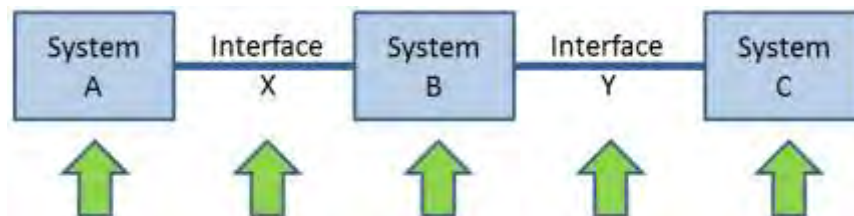
In this context, this section is broken down into the following subsections which give additional context to the scope of this effort:

- **Description** – A narrative overview of various special considerations and approaches applicable to this Interoperability Testing effort.
- **Interoperability Flows** – A description of the inventory of system and data flow for which Interoperability Test scripts were created.
- **Interoperability Test Scripts** – A detailed review of the test script documentation structure, inventory, and detailed cross reference of where certain scripts are captured in the appendix.

2.3.3.1 Description

End-to-End Interoperability Testing had a different focus than earlier stages of testing. Instead of detailed reviews of every possible permutation and function available, this testing effort was based on a definition of end-to-end data flows that achieved certain high-level objectives. These data flows, or scenarios, tended to be larger in scope, but fewer in number than the specific test books of earlier stages. As such, testing verified that the data flowed sequentially between systems to ensure that the data remains accurate through each step of the overall data transmission. Whereas inputs for earlier integration tests between systems may have been simulated data (due to lack of readiness in upstream systems and interfaces), the inputs for each step of Interoperability Tests were the outputs from earlier steps within the sequence for a given Interoperability flow. The tested capabilities include data translation, data receipt, firewall configuration, Message Queue (MQ) configuration and all native system algorithms. Given this detailed attention paid during testing, additional interoperability focused defects were discovered and remediated.

Figure 2-77: End-to-End Interoperability Testing



2.3.3.1.1 Resourcing

Testing efforts began with high-level planning to ensure that environments and staff were available and ready. While environment considerations are elaborated on below, staffing impacts were crucial from the beginning of planning efforts. By ensuring staff availability early on, they were able to participate in design workshops, configuration reviews, and training sessions for the individual systems and interfaces to maximize their familiarity with the interface functions. Furthermore, they were also able to participate in the detailed System and Integration test efforts to ensure familiarity with functionality at

all points of a given scenario. To this end, each interoperability scenario was handled as an independent test effort with different Subject Matter Experts (SMEs) assigned to different systems and integration capabilities as befitting their individual expertise.

2.3.3.1.2 Planning and Preparation

While the Interoperability Test Team participated in the earlier stage of testing, it was not their primary activity. Instead, they were focused on leveraging their ever-expanding knowledge of the various systems as a key influencer to defining the scope of the Interoperability Testing effort. These steps started with a review of KCP&L's use cases and integration diagram to define interoperability scenarios. The team kept these in consideration to define scenarios which would be vital to future demonstration and operational testing efforts. The resulting flows are listed in Section 2.3.4.2 below.

With these flows defined, the team advanced to define very specific Interoperability Test Scripts. Unlike the System and Integration test books which were compiled by the vendor and later reviewed and tweaked by KCP&L, these scripts were fully compiled by the KCP&L Interoperability test team. Given that these flows spanned multiple systems (from multiple vendors) and frequently included some custom KCP&L interface logic, no vendor was in a position to carefully stitch these scripts together. However, the results of these efforts were vital to the team's ability to execute these tightly integrated testing flows.

Additionally, since execution of these scripts would cross the purview of multiple vendors' ability to remediate, it was determined that any defects identified would be captured into a separate KCP&L controlled tool for managing defects. As tools were investigated, the selected tool also had the ability to manage testing progress as well as defects. As such, the tool was configured as the ultimate repository for all Interoperability Test script steps. Further configuration was pursued for the defect tracking which included characteristics of Impacted System, Responsible Party, Severity, and Resolution Status.

2.3.3.1.3 Test Execution

Sequentially, Interoperability Testing commenced for an individual scenario once each component system and interface comprising the entire data flow was working sufficiently well. This allowed for maximum stability of the individual systems and interface configurations to ensure that data traffic issues were more indicative of interoperability problems as opposed to more rudimentary issues. Furthermore, it ensured maximum accuracy of the data quality to ensure that expected data formats were properly compiled and transferred.

When testing efforts were pursued, some flows were reviewed in LAB environments and some were in DEMO (production-like). The environment used was primarily dependent on the data flow being tested and the goal of minimizing impacted customers. For data flows having a higher likelihood of impacting customers (e.g. outage & restoration and first responder functions), the LAB environment was used as a means of safely seeing functionality. For other advanced capabilities, the DEMO environment was perfectly feasible, as customers would not be negatively impacted, even though some extra coordination between KCP&L organizations was required to ensure safe operation of field devices (e.g. Battery DR and Volt/VAR Control)

Upon completion, Interoperability Testing resulted in very few incremental defects which is a testament to the quality design and test execution performed explicitly for the System and Integration tests. Where necessary, identified defects were logged in the defect management tool and progress was tracked allowing for resolution.

2.3.3.2 Interoperability Flows

As mentioned above, numerous data flows were compiled and reviewed for end-state functionality and the basis for procedural documentation. The scenarios listed below include the same functional

capabilities as outlined in the End-to-End Field Demonstration section (as Interoperability is the implicit preparation for that stage). Figure 2-78 was created to show the cross-system relationships between systems in given scenarios. As various scenarios were ready and proven out, this diagram was also used to track development/testing status (red/yellow/green indications on boxes and integration points) for high-level status reporting.

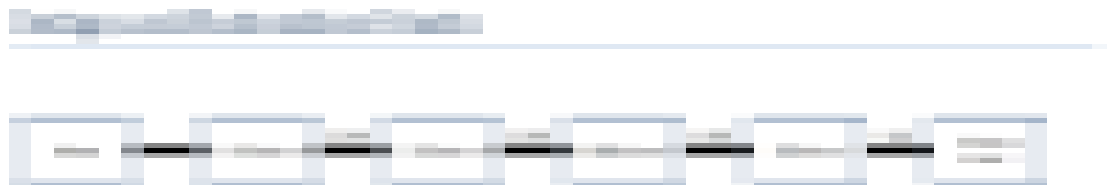
Figure 2-78: Interoperability Flows



2.3.3.3 Interoperability Test Scripts

For each of the flows documented, a detailed Interoperability Test Script was produced and ensured comprehensive testing of all required components of a given data flow. While the overall sequence of steps could become complex, the scripts themselves were designed to be simple, straightforward, and approachable. A breakdown of the script structure is shown below along with a list of available scripts included in the appendix for review.

- **Systems Integration Diagram** – The beginning of each scenario shows which servers/systems/devices are connected and communicating to allow the data to flow in an end to end manner. An example of this detail data flow is shown below.



The diagram can be interpreted as follows:

- **Boxes** – Specific servers or devices connected together to enable the data flow. In

some cases these will represent specific systems that went through System Testing efforts. In other cases (like “ESB Server”), the box will represent a server that enable data traffic to be routed properly and was a potential point of failure; as such it is explicitly listed for inclusion in end-to-end testing.

- **Lines** – Specific interfaces between servers or devices that enable data traffic. These largely correspond to the Integration Tests performed in earlier phases, but as applicable here, fewer nuances could be explored in great detail.
- **Preconditions** – Each testing scenario had some server setup required or specific devices which would be used during testing. This information was thought out in advance in a highly detailed fashion and included in this section. Later, during testing, this section would be referenced to ensure that the tested scenarios were precisely recreated and executed. An example of this detail data flow is shown below.

Remote Connect and On-Demand Read (Demo)

Precondition:

- Prior to entering a turn on order in GUI, make sure to change the Positive ID flag to 'P' in the green screens for each customer. In CIS+, pull up the customer ID on the PER screen (green screen) and panel left once for Positive ID field. Enter a 'C' in the Action field, 'P' in the Positive ID field and press Enter. (This is to verify that customer can open the account and turn on the meter. This has to be done before the meter service request)
- Meter has disconnect switch and SmartLink connected.

Remote Connect Meter Info – Production:

- Meter ID: 1284810439383 Service Point ID: 9324790610 Account Number: 5350203882

- **Test Steps** – The final section of each test script are the detailed test steps. Where necessary screenshots are embedded in the step to ensure accuracy and text is used to describe the necessary actions required. An example of a test step is included below:

Steps	Expected Results
1. Log in to the CIS system. 	1. Successfully logged in to the CIS+ system. 
2. Click on the "Jet" Search button. 	2. The JetSearch window pops up.

The diagram can be interpreted as follows:

- Detailed steps about what needs to happen with corresponding screenshot
- Detailed explanation about what the system should do as a result along with corresponding screenshot
- **Test Script Inventory** – Unlike the filtered test book inventories compiled for System and Integration Testing, every Interoperability Test script that was produced is included in Appendix J. Whereas the test books from the earlier stages were not the actual test books (due to standardization and proprietary content), these scripts were standardized from the outset, so the actual test scripts are included. That being said, these documents do include a number of test steps which some vendors have deemed to include proprietary or confidential information about their system’s internal functionality. The inventory of Interoperability Test Scripts is shown below.

Table 2-18: Interoperability Testing Documentation

Functional Area	System Integration	Appendix J: Sub-Appendix Location
Remote Connect / Disconnect	Connect – Customer Request	J.1: Remote Connect and Disconnect
Remote Connect / Disconnect	Disconnect – Customer Request	J.1: Remote Connect and Disconnect
Demand Response	DR – AMI Thermostat	J.2: Demand Response – AMI Thermostat
Demand Response	DR – HAN Devices	J.3: Demand Response – HAN Devices
Demand Response	DR – Battery	J.4: Demand Response – Battery
First Responder Functions	Volt/VAR Control	J.5: 1 st Responder Function – Volt/VAR Control
First Responder Functions	Feeder Load Transfer	J.6: 1 st Responder Function – Feeder Load Transfer
First Responder Functions	Fault Location / Fault Isolation & Svc Restoration	J.7: 1 st Responder Function – Fault Location, Isolation, and Service Restoration
Outage Analysis & Restoration Verification	Outage Event	J.8: Outage and Restoration Events
Outage Analysis & Restoration Verification	Restoration Event	J.8: Outage and Restoration Events
Outage Analysis & Restoration Verification	Restoration Verification	J.9: Power Status Verification
Battery Grid Operation – Power Mode	Local Control	J.10: Battery Grid Operation – Local Control (Discharge)
Battery Grid Operation – Power Mode	Fixed Discharge	J.11: Battery Grid Operation – Fixed kW (Discharge)
Battery Grid Operation – Power Mode	Load Following Discharge	J.12: Battery Grid Operation – Load Following (Discharge)

2.3.4 End-to-End Field Demonstrations

End-to-End Field Demonstrations represent the culmination of the incremental testing progression. In earlier stages of testing, verification efforts thoroughly confirmed the detailed functionality and communications between impacted systems. This effort allowed final functionality confirmation and preparation for demonstration to interested parties. To this end, this effort represented a convergence between formalized testing and the Education and Outreach objectives of this initiative. The test team's familiarity with the systems and interfaces up to and throughout this stage represented vital institutional knowledge that were key inputs to creating and preparing for demonstrations.

In this context, this section is broken down into the following subsections which give additional context to the scope of this effort and the educational materials resulting from its pursuit:

- **Description** – A narrative overview of various special considerations and approaches applicable to this demonstration effort.
- **Demonstration Flows** – A description of the inventory of system and data flow for which demonstration scripts were created.
- **Demonstration Scripts** – A detailed review of the demonstration script documentation structure and inventory and detailed cross reference of where certain scripts are captured in the appendix.

2.3.4.1 Description

End-to-End Field Demonstrations commenced in a similar manner to Interoperability testing in that it tested the same inventory of functional data flows with the same triggering inputs and concluding outputs. However, where Interoperability also involved a detailed review of the individual connections between standalone systems, at this stage for Field Demonstration scripting, minimal intervention between end-point systems was pursued. By having users actively verify functionality at the trigger and concluding points of a given data flow, all intermediary capabilities were shown to be implicitly functional. These capabilities include data translation, data receipt, firewall configuration, Message Queue (MQ) configuration and all native system algorithms. In so doing, the integrated solution was proven ready to be demonstrated to various audiences.

Figure 2-79: End-to-End Field Demonstration



Sequentially, the final communication verification indicative of this stage was pursued after Interoperability Testing was complete. This allowed for maximum stability of the systems and interface configurations to ensure that data traffic was not interrupted mid-transit. Furthermore, it ensured maximum accuracy of the data quality to ensure that expected data formats were properly compiled and transferred.

When verification efforts were pursued, some flows were reviewed in LAB environments and some were in DEMO (production-like). The environment used was primarily dependent on the data flow being tested and the goal of minimizing impacted customers. For data flows having a higher likelihood of impacting customers (e.g. outage restoration and first responder functions), the LAB environment was used as a means of safely seeing functionality. For other advanced capabilities, the DEMO environment

was perfectly feasible, as customers would not be negatively impacted, even though some extra coordination between KCP&L organizations was required to ensure safe operation of field devices (e.g. Battery DR and Volt/VAR Control).

Ultimately, all validation efforts during this stage were more a formality as the detailed verification of capabilities were conducted in the earlier Interoperability stage. An implication of this was that variances were not created during this stage, as all significant defects were identified and resolved prior to commencement.

All efforts to perform these verifications were performed by the Subject Matter Experts (SMEs) and team members that performed the Interoperability and earlier testing. By leveraging the same expertise, quality was maximized and transition efforts to different team members were minimized. As the process became more streamlined through repetition, a natural, steady-state sequence of tasks became established. The team then advanced efforts to document these steps in considerable detail for future use. Specifically, it was anticipated that non-SMEs could potentially be in a position to demonstrate the system at some future date when a SME was not available to conduct the demonstration. As such, the goal of this demonstration material was to capture as much pertinent SME process knowledge as possible for future use.

2.3.4.2 Demonstration Flows

As mentioned above, numerous data flows were compiled and reviewed for end-state functionality and the basis for procedural documentation. The demonstration flows listed in Figure 2-80 include the same functional capabilities as outlined in the Interoperability Testing section. However, given that the intended audience members for these demonstrations are anticipated to be non-technical, there will be no focus on the capabilities of the intermediary systems which have been greyed out.

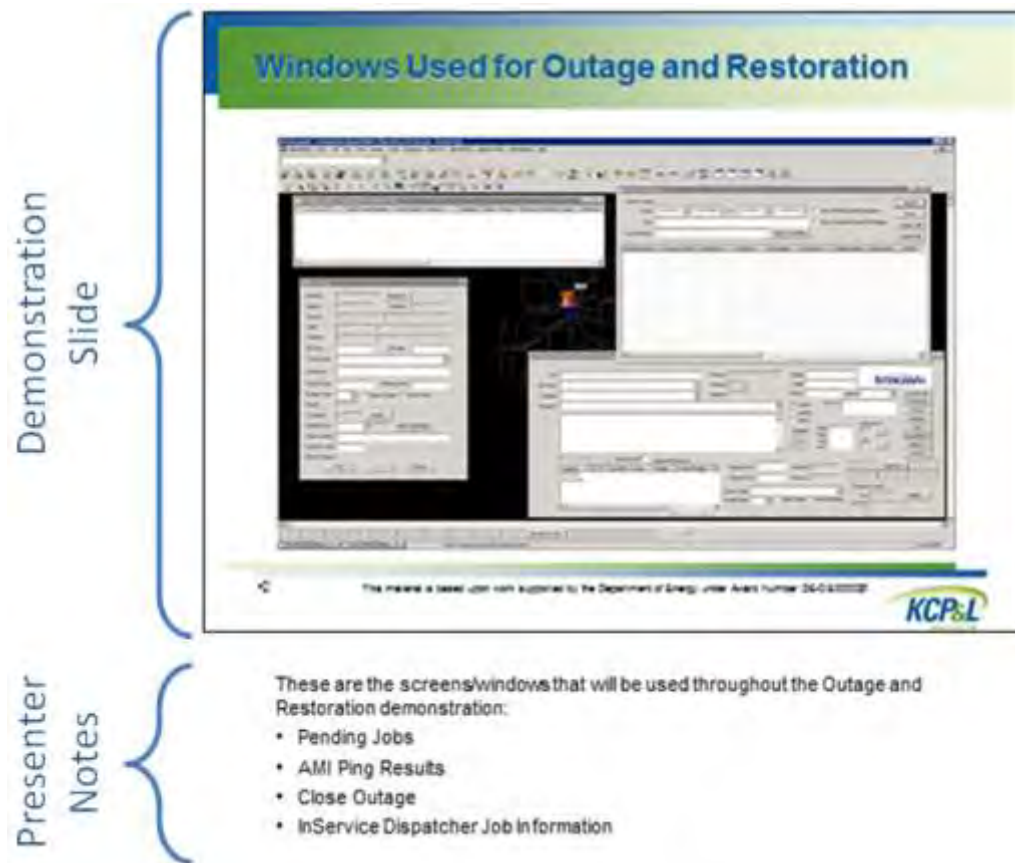
Figure 2-80: Demonstration Flows



2.3.4.3 Demonstration Scripts

For each of the flows documented, a detailed Demonstration Script was produced and available as support for anyone conducting a demonstration to interested audiences. While the overall sequence of steps could become complex, the scripts themselves were designed to be simple, straightforward, and approachable. A breakdown of the script structure is shown in Figure 2-81 along with a list of available scripts included in Appendix K for review.

Figure 2-81: Demonstration Script



- **Demonstration Slide** – Each demonstration script has a series of screen captures that show system capabilities in a step by step manner. These were intended to be detailed enough that if someone were trying to use the system itself, they should be able to follow the steps as outlined.
- **Presenter Notes** – In addition to the screenshots above, each demonstration script file will also include a number of notes, considerations, and talking points applicable to each slide. While not a requirement for a presentation being given, these serve to support the presenter as well as convey details to a reviewer who may be perusing the content.

Table 2-19: End-to-End Demonstration Scripts

Functional Area	System Integration	Appendix K: Sub-Appendix Location
Remote Connect / Disconnect	Connect – Customer Request	K.1: Remote Connect and Disconnect
Remote Connect / Disconnect	Disconnect – Customer Request	K.1: Remote Connect and Disconnect
Demand Response	DR – AMI Thermostat	K.2: Demand Response – AMI Thermostat
Demand Response	DR – HAN Devices	K.3: Demand Response – HAN Devices
Demand Response	DR – Battery	K.4: Demand Response – Battery
First Responder Functions	Volt/VAR Control	K.5: 1 st Responder Function – Volt/VAR Control
First Responder Functions	Feeder Load Transfer	K.6: 1 st Responder Function – Feeder Load Transfer
First Responder Functions	Fault Location / Fault Isolation & Svc Restoration	K.7: 1 st Responder Function – Fault Location and Service Restoration
Outage Analysis & Restoration Verification	Outage Event	K.8: Outage and Restoration Events
Outage Analysis & Restoration Verification	Restoration Event	K.8: Outage and Restoration Events
Outage Analysis & Restoration Verification	Restoration Verification	K.9: Power Status Verification
Battery Grid Operation – Power Mode	Local Control	K.10: Battery Grid Operation – Local Control (Discharge)
Battery Grid Operation – Power Mode	Fixed Discharge	K.11: Battery Grid Operation – Fixed kW (Discharge)
Battery Grid Operation – Power Mode	Load Following Discharge	K.12: Battery Grid Operation – Load Following (Discharge)

2.4 Operational Demonstration and Testing Plans

The KCP&L project has been divided into five sub-projects to demonstrate the deployed SmartGrid technologies and applications that enable specific DOE defined SmartGrid Functions. Table 2-20 lists all 24 Demonstration Applications, the SmartGrid Function they support, and the Sub Projects deploying each application.

This section contains an overview of each SmartGrid Function supported by the Demonstration Applications and a description of potential benefits from each enabled SmartGrid function. For each Demonstration Application, an Operational Demonstration Test Plan was developed that includes descriptions of the technology that will be applied, a description of expected results, relevant impact metrics, data to be collected and analyzed, and the benefit analysis method that will be used.

Table 2-20: KCP&L Operational Demonstration/Tests

Smart Grid Project Application Demonstrations/Tests		Demonstration Sub-Project				
		Smart Metering	Smart End-Use	Smart Substation	Smart Distribution	Smart Generation
Smart Grid Function	Application					
Automated Voltage & VAR Control	Integrated Volt/VAR Management (VVC)	s		s	B	
Real-Time Load Transfer	Feeder Load Transfer (FLT)	s		s	B	
Automated Feeder & Line Switching	Fault Isolation & Service Restoration (FISR)			s	B	
Automated Islanding & Reconnection	Feeder Islanding with Grid Battery			s	s	T
Diagnosis and Notification of Equipment Condition	Substation Protection Automation			T		
	Asset Condition Monitoring			B	B	
	Hierarchical Control (DCADA)			T	T	
Real-Time Load Measurement and Management	Automated Meter Reading (AMR)	B				
	Remote Meter Disconnect/Re-Connect	B				
	Meter Outage Restoration w/PSV (PSV)	B			B	
	Demand Response Events (DR)	B	s			B
Customer Electricity Use Optimization	Historical Interval Usage Information (HEMP)	s	B			
	In-Home Display (IHD)	s	B			
	Home Area Network (HAN)	s	B			
	Time-of-Use Rate (TOU)	B	B			
Distributed Production of Electricity	Distributed Roof-Top Solar Generation					T
Storing Electricity for Later Use	Electric Energy Time Shift					B
	Electric Supply Capacity				s	B
	T&D Upgrade Deferral				s	B
	Time of use Energy Cost Mgmt.		T			
	Electric Service Reliability		T			
	Renewable Energy Time Shift		T			
	PHEV Charging (VCM)					T

2.4.1 Automated Voltage and VAR Control

Automated voltage and VAR control requires coordinated operation of reactive power resources such as capacitor banks, voltage regulators, transformer load-tap changers, and DG with sensors, controls, and communications systems. These devices could operate autonomously in response to local events or in response to signals from a central control system.

2.4.1.1 DOE SGCT Function to Benefit Rationale

Automated voltage and VAR control (VVC) is performed through devices that can increase or lower voltage and can be switched or adjusted to keep the voltage in a required range. Control systems could determine when to operate these devices, and do so automatically. This function is the result of coordinated operation of reactive power resources such as capacitor banks, voltage regulators, transformer load-tap changers, and distributed generation (DG) with sensors, controls, and communications systems. These devices could operate autonomously in response to local events or in response to signals from a central control system. By better managing voltage and VAR resources, the transmission and distribution network can be optimized for electrical efficiency (lower losses), and can allow utilities to reduce load through “energy conservation voltage reduction” while maintaining adequate service voltage. These load reductions will reduce the amount of generation required. This function provides five benefits:

- **Reduced Ancillary Service Cost** - Ancillary services are necessary to ensure the reliable and efficient operation of the grid. As discussed above, ancillary services are provided by generators, and voltage and VAR support. The level of ancillary services required at any point in time is determined by the grid operator and/or energy market rules. To the extent that reactive power resources can be better coordinated to reduce load and reactive power requirements from generation, ancillary service costs for voltage and VAR support could be reduced, decreasing the cost for market participants and utilities.
- **Reduced Transmission and Distribution Operations Cost** – Automated voltage and VAR control eliminates the need to send a line worker or crew to the location of reactive devices in order to operate them. This reduces the cost associated with the field service worker(s) and service vehicle. The impact of this benefit is determined by estimating the percentage of a field crew's time is dedicated to capacitor switching, and then estimating the time saved by the field service personnel.
- **Reduced Electricity Losses** – Coordinating the settings of voltage control devices on the transmission and distribution system ensures that customer voltages remain within service tolerances, while minimizing the amount of reactive power provided. Optimizing voltage and VAR in this way can reduce the amount of transmission and distribution losses associated with delivering a given amount of energy.
- **Reduced CO₂ Emissions** – Energy reductions achieved through improved efficiency and energy conservation voltage reduction will reduce the amount of generation required to serve load. Assuming that the generation is fossil-based, emissions will be reduced.
- **Reduced SO_x, NO_x, and PM-2.5 Emissions** – Energy reductions achieved through improved efficiency and energy conservation voltage reduction will reduce the amount of generation required to serve load. Assuming that the generation is fossil-based, emissions will be reduced.

The KCP&L project team has identified two additional benefits provided by this function.

- **Deferred Generation Capacity Investments** – Energy reductions achieved through improved efficiency and energy conservation voltage reduction can be used to reduce the amount of central station generation required during peak times. This may improve the

overall load profile and allow a more efficient mix of generation resources to be dispatched. This could save utilities money on their generation costs.

- **Reduced Electricity Consumption/Cost** – Energy reductions from customer loads can be achieved through conservation voltage reduction. Changes in customer usage can result in reductions in the customers total cost of electricity and reduce the electricity that must be generated and pass through the T&D lines.

2.4.1.2 Integrated Volt/VAR Management

KCP&L Operational Test Plan

A. Description

KCP&L currently has a very active capacitor deployment and automation program where each capacitor operates autonomously in response to local conditions to satisfy the circuit operating (voltage and power factor) criteria. This VVC operational test will compare the operational performance of the SmartGrid Automated VVC program relative to the existing KCP&L capacitor program controls.

The SmartGrid Automated VVC function extends the legacy KCP&L VVC design parameters to include losses and objective functions. The four objective functions are to:

- Minimize the sum of power losses
- Minimize the power demand
- Maximize the substation transformer reactive power
- Maximize the difference between energy sales and energy prime cost

The SmartGrid Automated VVC program continuously monitors circuit conditions, uses a distribution power flow to calculate circuit voltage profile and losses; and centrally controls power transformer load tap changer (LTC) position, voltage regulators, and switchable capacitors to meet the prescribed objective functions.

We will evaluate each of the four objective functions in comparison to current KCP&L capacitor control schemes.

B. Expected Results

This operational demonstration is expected to yield the following:

- For each objective function we expect to see an incremental improvement in circuit operational performance indicators including:
 - Voltage profile
 - Power factor at circuit head
 - Electrical losses
 - Economics
- Based on the circuit performance improvements obtained under each VVC objective function, a recommended objective function would be selected for sustained operation of the SmartGrid Demonstration Circuits.
- Due to KCP&L's active capacitor deployment & automation program, a significant improvement may not be achievable.

C. Relevant Impact Metrics

The Operational Testing of this application will contribute to these Impact Metrics.

Distribution	Feeder Aggregated Average Real Load (MW)
Distribution	Feeder Aggregated Average Reactive Load (MVAR)
Distribution	Feeder Hourly Load Curves (MW)
Distribution	Feeder Hourly Reactive Load Curves (MVAR)
Distribution	Avoided Distribution Losses (MWh)

At each reporting milestone, operational test, or demonstration period, data will be compared to baseline data to determine a quantified impact. Quantified impacts measured will be reported in semi-annual impact metric reports.

D. Benefits Analysis Method/Factors

The DOE SGCT will be used to perform the Demonstration Project benefit analysis. For this application the following Smart Grid Function benefits will be quantified.

- Reduced Electricity Losses
- Deferred Generation Capacity Investments
- Reduced Electricity Consumption/Cost

Benefits will be calculated using SGCT formulas. The following factors will be measured, projected or calculated during the application operation and/or demonstration.

Reduced Electricity Losses

- Distribution Feeder Load (MW)
- Distribution Feeder Losses (MWh) (base & proj.)
- Distribution Losses (%) (base & proj.)

Deferred Generation Capacity Investment

- Distribution Feeder Load Reduction at Annual Peak Time (MW)

Reduced Energy Costs (Consumer)

- Reduced Total Annual Electric Consumption (kWh) by customer class.

E. Baseline Data & Control Groups

AMI metering that is deployed for all customers, circuits, and distributed energy resources within the Demonstration Project area. The following usage data will be available for baselines::

- 15 minute interval load data of all customers
- Average hourly interval load data by customer class
- 15 minute interval total load data for circuit
- Aggregated interval load data for all customers by circuit

The following circuit voltage data will be available from the HIS for analysis:

- Historical circuit voltage profile readings at SCADA enabled devices.

The following system level energy production data will be available for analysis:

- Historical and current hourly system energy production load profile data.
- Historical weather adjusted system energy production load profile data.

F. Testing Method/Methodology

The following points provide an overview of how the operational testing for this application will be accomplished:

- Testing for each control 'objective' function will be on a week on/week off basis, to compare current legacy protection schemes to one of the central control objectives.
- Individual seasonal testing and data collection periods will be established for operation under each control 'objective' function.
- Each objective function test will be 2 weeks (1 week on/1 week off). Testing will be done seasonally for each objective function. (4 periods of 8 weeks)
- During each test period, the DMS and VVC operational parameters will be adjusted to maximize the potential benefits achievable for 'objective' control function being tested.
- The AMI system will be used to collect customer and circuit load profile data for each Smart Grid project circuit. AMI customer and circuit data not involved in the test will be used as control for the analysis.
- DMS will collect voltage profile data for all SCADA enabled equipment and the AMI will collect under/over voltage alarms from customer AMI meters.

G. Analytical Method/Methodology

The following points provide an overview of the analytical methods that will be used to evaluate the impact and benefits of this application:

- AMI interval load data for all customer and circuit load meters within the Project area will be extracted from the MDM System through KCP&L's Data Mining and Analysis Tool (DMAT) (DataRaker). The DMAT has built in functionality that will enable the aggregation and calculation of hourly load profiles of customer loads grouped by Circuit.
- For each operational test period aggregated customer data by circuit will be compared to circuit load meter data to determine the distribution system 'losses'. The calculated distribution grid losses include technical (I^2R) losses along with unmetered load, theft and diversion.
- The DMS application provides a calculation of distribution (I^2R) technical losses. The delta DMS technical losses will be analyzed against the delta calculated distribution losses from the metering data.
- For each operational test period the off-week and control circuit data will be used as baseline data to determine a quantified impact (loss reduction, peak load reduction, etc.).
- For each operational test period DMS voltage for on/off week and control circuits will be used to determine the quantified impact on circuit voltage profile.
- Additionally, hourly pricing, hourly system load, hourly substation load (from SCADA), and hourly feeder load (AMI) from October 2012 through October 2014 will be obtained to determine potential savings over the entire project duration.

2.4.2 Real-Time Load Transfer

Real-time load transfer is achieved through real-time feeder reconfiguration and optimization to relieve load on equipment, improve asset utilization, improve distribution system efficiency, and enhance system performance.

2.4.2.1 DOE SGCT Function to Benefit Rationale

In areas that may have more than one distribution feeder, circuits may be switched and electrical feeds rerouted to make the distribution more efficient or more reliable. This function allows for real-time feeder reconfiguration and optimization to relieve load on equipment, improve asset utilization, improve distribution system efficiency, and enhance system reliability. This function provides these benefits:

- **Deferred Distribution Capacity Investments** – Load growth and feeder reconfiguration can lead to increased loading on lines and transformers, to the point where distribution capacity investments become necessary. Being able to automatically switch a portion of a distribution feeder A onto distribution feeder B will relieve the load on feeder A. In cases where feeder A and feeder B are connected to different substations, the load relief can have beneficial effects up to the substation level. This load shifting could enable utilities to postpone feeder upgrades for one or more years. Each year that a capital investment can be deferred can yield a significant savings in the utility’s revenue requirement (equal to the capital carrying charge of the upgrade). Therefore, Real-Time Load Transfer could yield direct savings based on postponed capital investment.
- **Reduced Electricity Losses** – Higher line loading tends to affect delivery losses more than average load, and managing this peak could lead to improvements in electricity delivery efficiency. By being able to balance load among substation transformers and distribution feeders, the utility could reduce delivery losses.
- **Reduced Major Outages** – Transferring portions of a distribution feeder load from one substation to another could enable a utility to restore service to some outage customers more quickly than if they had to wait until their normal feeder was fully restored. Performing this load shifting manually would be impractical. However, by being able to do this remotely, a utility might be able to justify the cost in the interest of restoring some customers more quickly.
- **Reduced CO2 Emissions** – Increased electricity delivery efficiency by managing peak line loads will reduce the amount of generation required to serve load. Assuming that the generation is fossil-based, emissions will be reduced.
- **Reduced SOx, NOx, and PM-2.5 Emissions** – Increased electricity delivery efficiency by managing peak line loads will reduce the amount of generation required to serve load. Assuming that the generation is fossil-based, emissions will be reduced.

2.4.2.2 Feeder Load Transfer

KCP&L Operational Test Plan

A. Description

KCP&L circuit configurations are currently established based on engineering planning studies and that focus on optimizing the distribution system under peak load conditions. The Feeder Load Transfer (FLT) application will perform a real-time analysis to determine the optimal radial distribution network configuration to serve the current load. The FLT analysis minimizes electrical losses while maintaining current and voltage levels within technical limits.

Automated switches with two-way communications were deployed on the twelve SmartGrid distribution circuits to allow remote circuit reconfiguration. FLT will develop switching plans to implement the recommend configuration which may be implemented automatically or manually by the distribution gird operator.

B. Expected Results

This operational demonstration is expected to yield the following:

- FLT analysis makes changes to the 'Normal' circuit configurations that will be more efficient and reduce distribution system losses.
- FLT may identify real-time, daily, or seasonal reconfigurations that will be more efficient and reduce distribution system losses.

C. Relevant Impact Metrics

The Operational Testing of this application will contribute to these Impact Metrics.

Distribution	Feeder Aggregated Average Real Load (MW)
Distribution	Feeder Aggregated Average Reactive Load (MVAR)
Distribution	Feeder Hourly Load Curves (MW)
Distribution	Feeder Hourly Reactive Load Curves (MVAR)
Distribution	Avoided Distribution Losses (MWh)

At each reporting milestone, operational test, or demonstration period, data will be compared to baseline data to determine a quantified impact. Quantified impacts measured will be reported in semi-annual impact metric reports.

D. Benefits Analysis Method/Factors

The DOE SGCT will be used to perform the Demonstration Project benefit analysis. For this application the following Smart Grid Function benefits will be quantified.

- Reduced Electricity Losses.
- Deferred Distribution Capacity Investments.

Benefits will be calculated using SGCT formulas. The following factors will be measured, projected or calculated during the application operation and/or demonstration.

Reduced Electricity Losses

- Distribution Feeder Load (MW)
- Distribution Feeder Loss Reduction (MWh) (base & proj.)
- Distribution Losses (%) (base & proj.)

Deferred Distribution Capacity Investments

- Distribution Feeder Load Reduction (MW)

E. Baseline Data & Control Groups

AMI metering that is deployed for all customers, circuits, and distributed energy resources within the Demonstration Project area. The following usage data will be available for baselines::

- 15 minute interval total load data for circuit
- Aggregated interval load data for all customers by circuit

The following system level energy production data will be available for analysis:

- Historical and current hourly average and marginal energy production cost data.
- Historical and current hourly system energy production load profile data.

F. Testing Method/Methodology:

The following points provide an overview of how the operational testing for this application will be accomplished:

- Testing for the FLT application will occur periodically throughout the operational period during different seasons, times of day, and system loading levels.
- FLT testing will be conducted independently of VVC and other application testing that impacts distribution grid characteristics.
- With grid reconfiguration, measurement of distribution grid losses is extremely difficult. Therefore, we will determine the improved grid efficiency based on the DNA analytic calculations. Grid loss impact will be measured in two ways; 1) the FLT application provides a calculation of loss savings that is expected based on the proposed reconfiguration, 2) the DNA State Estimation/Load Flow loss calculations will be recorded before and after the reconfiguration is implemented.
- During each test period, the DMS FLT operational parameters will be adjusted to maximize the potential benefits achievable.
- The AMI system will be used to collect circuit load profile data for each circuit. AMI circuit data not involved in the test will be used as control for the analysis.
- DMS will collect voltage profile data for all SCADA enabled equipment.

G. Analytical Method/Methodology

The following points provide an overview of the analytical methods that will be used to evaluate the impact and benefits of this application:

- AMI interval load data for all circuit load meters within the Project area will be aggregated to develop an hourly load profile of the combined circuit load.
- For each operational test, the before and after calculated grid losses will be compared to determine the reduction in technical (I^2R) losses.
- Total annual loss savings will be project by calculated by extrapolating the individual test results using the annual hourly load profile for the project area.
- For each operational test period, DMS voltage for on/off week and control circuits will be used to determine the quantified impact on circuit voltage profile.
- Additionally, hourly pricing, hourly system load, hourly substation load (from SCADA), and hourly feeder load (AMI) from October 2012 through October 2014 will be obtained to determine potential savings over the entire project duration.

2.4.3 Automated Feeder and Line Switching

Automated feeder switching is realized through automatic isolation and reconfiguration of faulted segments of distribution feeders via sensors, controls, switches, and communications systems. These devices can operate autonomously in response to local events or in response to signals from a central control system.

2.4.3.1 DOE SGCT Function to Benefit Rationale

Utilities design distribution feeders with switches so that portions of the feeder can be disconnected to isolate faults, or de-energized for maintenance. In most cases, these switches are manually operated, and require a service worker to travel to the switch location, coordinate switching orders with a dispatcher, and then physically operate the switch. Automatic Feeder Switching makes it possible to operate distribution switches autonomously in response to local events, or remotely in response to operator commands or a central control system.

Automatic Feeder Switching does not prevent outages; it simply reduces the scope of outage impacts in the longer term. This function is accomplished through the automatic isolation and reconfiguration of faulted segments of distribution feeders via sensors, controls, switches, and communications systems. Automatic Feeder Switching can reduce or eliminate the need for a human operator or field crew for operating distribution switches. This saves time, reduces labor cost, and eliminates “truck rolls”. This function can provide six benefits:

- **Reduced Transmission and Distribution Operations Cost** – Automated or remote controlled switching eliminates the need to send a line crew to the switch location in order to operate it. This reduces the cost associated with the field service worker(s) and service vehicle.
- **Reduced Sustained Outages** – Automated Feeder and Line Switching means that the faulted portions of feeders and lines can be isolated by opening switches. By reconnecting some customers quickly (within minutes), significant outage minutes can be saved. This only works when a significant number of customers receive service upstream of the fault, with an automated switch between them and the fault. This function presumes that the switching is done within the scope of a single feeder. Automatic switching does not prevent the outage for all customers; it simply reduces the scope of its impact in the longer term.
- **Reduced Restoration Cost** – Being able to operate distribution switches without rolling trucks means lower restoration costs.
- **Reduced CO2 Emissions** – Fewer truck rolls for switching means less fuel consumed by a service vehicle or line truck and leads to reduced emissions.
- **Reduced SOx, NOx, and PM-2.5 Emissions** – Fewer truck rolls for switching means less fuel consumed by a service vehicle or line truck and leads to reduced emissions.
- **Reduced Oil Usage** – Fewer truck rolls for switching means less fuel consumed by a service vehicle or line truck and leads to reduced oil usage.

2.4.3.2 Fault Isolation and Service Restoration

KCP&L Operational Test Plan
<p>A. Description</p> <p>Fault isolation, fault location, circuit monitoring devices, and automatic circuit reconfiguration equipment will be deployed on the eleven SmartGrid distribution circuits. This will include two-way communications to enable system operators to continuously monitor and operate this equipment remotely. The systems will also automatically identify circuit faults and isolate them to smaller sections of the circuit when possible. Remaining sections of the circuit will be restored automatically without human intervention. Additionally, system operators will receive alerts regarding the faulted section and deploy field crews directly to the failed equipment, avoiding timely fault searching.</p>
<p>B. Expected Results</p> <p>This operational demonstration is expected to yield the following:</p> <ul style="list-style-type: none"> • Reliability will improve, resulting in significant reductions in SAIFI and SAIDI. It is estimated that SAIFI could be reduced by 20%, SAIDI by 30%. • Operational costs will be reduced as manual switching will be executed remotely and fault locations will reduce fault searching time. It is estimated that manual switching could be decreased by 3-6 truck rolls per circuit per year.

C. Relevant Impact Metrics

The Operational Testing of this application will contribute to these Impact Metrics.

Distribution	SAIFI
Distribution	SAIDI
Distribution	CAIDI
Distribution	Total Customers Served by SAIDI/SAIFI
Distribution	Major Event – No. of Customers Affected
Distribution	Major Event – No. of Customers Affected w/out FISR
Distribution	Major Event – Total Restoration Time (hours)
Distribution	Major Event – Total Restoration Time w/out FISR (hours)
Distribution	Truck Rolls Avoided
Distribution	Avoided Distribution Operation Vehicle Miles
Distribution	Avoided CO2 Emissions (tons)

At each reporting milestone, operational test, or demonstration period, data will be compared to baseline data to determine a quantified impact. Quantified impacts measured will be reported in semi-annual impact metric reports.

D. Benefits Analysis Method/Factors

The DOE SGCT will be used to perform the Demonstration Project benefit analysis. For this application the following Smart Grid Function benefits will be quantified.

- Reduced Sustained Outages
- Reduced Restoration Costs
- Reduced T&D Operations Costs
- Reduced CO2 Emissions

Benefits will be calculated using SGCT formulas. The following factors will be measured, projected or calculated during the application operation and/or demonstration.

Reduced Sustained Outages

- SAIDI (base & proj.)

Reduced Restoration Costs

- Avoided Distribution Restoration Costs (\$) (crew outage trouble shooting)

Reduced T&D Operations Costs

- Avoided Distribution Operations Costs (\$) (crew non-outage switching)

Reduced CO2 Emissions

- Avoided Truck Rolls

E. Baseline Data & Control Groups

The following historical system level reliability statistics will be available for analysis:

- System Average Interruption Frequency Index (SAIFI)
- System Average Interruption Duration Index (SAIDI)
- Customer Average Interruption Duration Index (CAIDI)

F. Testing Method/Methodology

The following points provide an overview of how the operational testing for this application will be accomplished:

- KCP&L's legacy OMS will continue to be used by the Distribution Dispatcher to work lights-out and other trouble calls.
- The legacy OMS will continue to record all outage events and restoration efforts.
- The Demonstration Project OMS will be used in study mode to perform an 'after the fact' analysis to determine how the FISR application would have impacted outage response and restoration efforts.

G. Analytical Method/Methodology

The following points provide an overview of the analytical methods that will be used to evaluate the impact and benefits of this application:

- In the 'after the fact' analysis of each major event the following data will be calculated to determine how the FISR application functions:
 - Major Event - No. of Customers Affected
 - Major Event - No. of Customers Affected w/out FISR
 - Major Event – Total Customer Outage Hours (hours)
 - Major Event – Total Customer Outage Hours w/out FISR (hours)
 - Major Event – Total Restoration Time (hours)
 - Major Event – Total Restoration Time w/out FISR (hours)

2.4.4 Automated Islanding and Reconnection

Automated islanding and reconnection is achieved by automated separation and subsequent reconnection (autonomous synchronization) of an independently operated portion of the T&D system (i.e., microgrid) from the interconnected electric grid. A microgrid is an integrated energy system consisting of interconnected loads and distributed energy resources which, as an integrated system, can operate in parallel with the grid or as an island.

2.4.4.1 DOE SGCT Function to Benefit Rationale

A microgrid is an integrated energy system consisting of interconnected loads and distributed energy resources which, as an integrated system, can operate in parallel with the grid or as an island. This disconnection and reconnection of the microgrid and the interconnected electric grid would be done automatically as needed based on grid conditions. This function leads to three benefits:

- **Reduced Sustained Outages** – Automated islanding and reconnection means portions of the system that include distributed generation can be isolated from areas with excessive damage. Customers within the island, or microgrid, will be served by the distributed generation until the utility can restore service to the area. Only the customers in the island experience reduced outage time from this improved reliability. While the outage may affect wide areas and large numbers of customers, the island will most likely be no larger than a single distribution feeder (i.e., < 5,000 customers) or smaller.
- **Reduced Major Outages** – Automated islanding and reconnection means portions of the system that include distributed generation can be isolated from areas with excessive damage. Customers within the island, or microgrid, will be served by the distributed generation until the utility can restore service to the area. Only the customers in the island experience reduced outage time from this improved reliability. While the outage

may affect wide areas, and large numbers of customers, the island will most likely be no larger than a single distribution feeder (i.e., < 5,000 customers) or smaller.

- **Reduced Restoration Cost** – When an outage event occurs, customers in the island who would have otherwise experienced an outage will not experience a service interruption. Therefore, the restoration area that crews need to attend to will be reduced which will reduce the number of crews needed to restore power and reduce costs.

2.4.4.2 Feeder Islanding with Grid Battery

KCP&L Technology Demonstration Plan	
A. Description	A 1.0 MWh, 1.0 MW-capable grid-connected Battery Energy Storage System (BESS) will be installed at the Midtown Substation with direct interconnect to a single radial 13.2 kV circuit, immediately downstream of the substation transformer. DMS based battery control functions will be implemented to allow the distribution grid operator to put the BESS in 'Islanding' mode and discharge the battery while a portion of the circuit is disconnected from the grid. Once the BESS is placed in 'Islanding' mode, it will maintain power to the isolated section until grid power is restored or the battery is fully discharged.
B. Expected Results	The technical demonstration of the grid connected battery in this application is expected to yield the following: <ul style="list-style-type: none"> • During a scheduled, controlled outage to the circuit, demonstrate that the BESS can restore power to customers after a brief outage. • When grid power is restored, the BESS will automatically synchronize to the grid and seamlessly connect back to grid power without a second outage.
C. Relevant Impact Metrics	The Technical Demonstration of this application will not contribute to any Impact Metrics.
D. Benefits Analysis Method/Factors	The Technical Demonstration of the use of the BESS in this application will not contribute to the project Benefits Analysis.
E. Baseline Data & Control Groups	The Technical Demonstration of this application does not require any Baseline Data or the establishment of any Control Groups.
F. Demonstration Method/Methodology	The following points provide an overview of how the technical demonstration of this application will be accomplished: <ul style="list-style-type: none"> • KCP&L will arrange a scheduled outage, for all customers on the feeder serving the BESS, at a time that will have minimal customer impact. • The Grid Operator will open the feeder breaker creating a feeder outage. • The Grid Operator will open the source side Recloser and the BESS will activate in "Islanding Mode" restoring power to customers downstream from the recloser. • The BESS will be allowed to sustain power to customers for a period of time. • The Grid Operator will close the feeder breaker restoring power to the source side of the recloser.

- The BESS will perform a sync-check and adjust BESS power output to synchronize the islanded section to the grid.
- Once the Islanded section is in-sync with the grid the BESS will close the recloser and discontinue discharge.

G. Analytical Method/Methodology

The Technical Demonstration of this application does not require any analytical calculations.

2.4.5 Diagnosis and Notification of Equipment Condition

Diagnosis and notification of equipment condition is defined as on-line monitoring and analysis of equipment, its performance, and operating environment in order to detect abnormal conditions (e.g., high number of equipment operations, temperature, or vibration). Asset managers and operations personnel can then be automatically notified to respond to conditions that increase the probability of equipment failure.

2.4.5.1 DOE SGCT Function to Benefit Rationale

Some equipment such as transformers and circuit breakers are critical to providing electric service to customers. Utilities test and maintain this equipment periodically in an effort to ensure that it operates reliably over a long service life. Because of the large amount of equipment, and the labor intensity of taking measurements and analyzing results, testing and maintenance can be very expensive, and may fail to identify critical equipment conditions before they lead to failure.

This function is the on-line monitoring and analysis of equipment, its performance and operating environment to detect abnormal conditions (e.g., high number of equipment operations, temperature, gas production or vibration). As a result, the function enables the equipment to automatically notify asset managers and operations to respond to a condition that increases a probability of equipment failure. This function results in seven benefits:

- **Reduced Equipment Failures** – Monitoring equipment “continuously” and receiving reports of its condition will help utilities identify potential trouble before it worsens and leads to failure.
- **Reduced Distribution Equipment Maintenance Cost** – The cost of sending technicians into the field to check equipment condition is high. Moreover, to ensure that they maintain equipment sufficiently and identify failure precursors, some utilities may conduct equipment testing and maintenance more often than is necessary. Online diagnosis and reporting of equipment condition would reduce or eliminate the need to send people out to check equipment.
- **Reduced Sustained Outages** – Some equipment failures cause outages, as well as environmental damage such as fires and spills. The time to restore power can be significant depending on the difficulty of the replacement, and the time it takes to obtain a replacement device. By utilizing on-line diagnosis and reporting of equipment condition, utilities could identify equipment problems before they cause outages.
- **Reduced Restoration Costs** – Outages caused by equipment failure will require restoration, and the utility will incur costs as a result. In some cases, the utility may pay a premium for the equipment and labor needed to restore service on short notice.
- **Reduced CO₂ Emissions** – Fewer truck rolls for switching means less fuel consumed by a service vehicle or line truck and leads to reduced emissions.
- **Reduced SO_x, NO_x, and PM-2.5 Emissions** – Fewer truck rolls for switching means less fuel consumed by a service vehicle or line truck and leads to reduced emissions.

- **Reduced Oil Usage** – Fewer truck rolls for equipment replacement means less fuel consumed by a service vehicle or line truck and leads to reduced oil consumption.

2.4.5.2 Substation Protection Automation

KCP&L Technology Demonstration Plan	
A. Description	An IEC 61850 compliant substation communication controller and substation protection network will be installed in the Midtown Substation along with various other component upgrades to enable substation protection automation. Component upgrades will include the replacement of electromechanical relays with intelligent electronic relays and the deployment of enhanced protection schemes. All new relays will communicate directly with the substation controller. The substation protection network will provide distributed intelligence at the substation that will enable execution of automated protection operations based on feedback from real-time monitoring of transformers, relays, cap banks, and other field equipment.
B. Expected Results	The technical demonstration of the Substation Protection Automation is expected to yield the following: <ul style="list-style-type: none"> • Substation Protection Automation will reduce operation and maintenance costs as manual or remote operations will be executed automatically. • Automated actions based on real-time feedback will also help prevent component failures or route power around component failures within the substation, thus improving reliability and further reducing operation and maintenance costs. • Implementation in accordance with IEC 61850 will provide experience and learning for the industry. • Monitoring of all substation equipment will provide better operating data for utility decision making.
C. Relevant Impact Metrics	The Technical Demonstration of this application will not contribute to any Impact Metrics.
D. Benefits Analysis Method/Factors	This Technical Demonstration will not contribute to the project Benefits Analysis.
E. Baseline Data & Control Groups	The Technical Demonstration of this application does not require any Baseline Data or the establishment of any Control Groups.
F. Demonstration Method/Methodology	The following points provide an overview of how the technical demonstration of this application will be accomplished: <ul style="list-style-type: none"> • Electronic relays will be deployed in Midtown substation in 2010. • IEC61850 GOOSE protection schemes will be deployed on the substation relays via CID files. GOOSE will be enabled via a setting in the relay settings files in December 2013. • The relays will begin collecting information from the cross triggering GOOSE scheme. • The SG team and KCP&L engineers will use the event information for enhanced visibility into substation events and real time device information.

G. Analytical Method/Methodology

The Technical Demonstration of this application does not require any analytical calculations.

2.4.5.3 Asset Condition Monitoring**KCP&L Technology Demonstration Plan****A. Description**

An asset condition monitoring and reporting infrastructure will be installed for all key substation and field devices throughout the Demonstration Project Area. The asset condition monitoring and reporting infrastructure to be implemented includes enhanced equipment sensors and control capabilities, real-time condition monitoring and alarming capabilities in the DMS, and the DMS-HIS for archival of reported conditions for later analysis.

B. Expected Results

The operational demonstration of this application is expected to yield the following:

- Analysis of condition monitoring data from currently available industry equipment controls will provide experience and learning for the industry.
- Implementation of report-by-exception condition monitoring data from current industry equipment controls will provide experience and learning for the industry.
- Demonstrate how remote asset condition reporting can reduce operation and maintenance costs as conditions can be determined remotely in real time.
- Record any actions based on real-time feedback that were used to help prevent component failures, thus improving reliability and further reducing operation and maintenance costs.

C. Relevant Impact Metrics

The Operational Testing of this application will contribute to these Impact Metrics.

Distribution	Feeder Aggregated Average Real Load (MW)
Distribution	Feeder Aggregated Average Reactive Load (MVAR)
Distribution	Feeder Hourly Load Curves (MW)
Distribution	Feeder Hourly Reactive Load Curves (MVAR)
Distribution	Avoided Distribution Losses (MWh)

At each reporting milestone, operational test, or demonstration period, data will be compared to baseline data to determine a quantified impact. Quantified impacts measured will be reported in semi-annual impact metric reports.

D. Benefits Analysis Method/Factors

The DOE SGCT will be used to perform the Demonstration Project benefit analysis. For this application the following Smart Grid Function benefits will be quantified.

- Reduced Equipment Failures
- Reduced Sustained Outages
- Reduced Restoration
- Reduced CO2 Emissions Costs

<p>Benefits will be calculated using SGCT formulas. The following factors will be measured, projected or calculated during the application operation and/or demonstration.</p> <p>Reduced Equipment Failures</p> <ul style="list-style-type: none"> • Capital Replacement of Failed Equipment (\$) • Portion Caused by Lack of Condition Diagnosis (%) <p>Reduced Sustained Outages</p> <ul style="list-style-type: none"> • SAIDI (base &proj.) <p>Reduced Restoration Costs</p> <ul style="list-style-type: none"> • Avoided Distribution Restoration Costs (\$) <p>Reduced CO2 Emissions</p> <ul style="list-style-type: none"> • Avoided Truck Rolls
<p>E. Baseline Data & Control Groups</p> <p>The Technical Demonstration of this application does not require any Baseline Data or the establishment of any Control Groups.</p>
<p>F. Demonstration Method/Methodology:</p> <p>The following points provide an overview of how the technical demonstration of this application will be accomplished:</p> <ul style="list-style-type: none"> • A fiber substation protection will be deployed at Midtown substation to enable communications to substation devices, and a Tropos wireless mesh network will be deployed throughout the demonstration project area to enable communications to field devices. • Intelligent Electronic Devices (IEDs) will be deployed in Midtown substation and along the 11 designated smart grid feeders extending from Midtown substation. • Data from the IEDs will be reported to a centralized data concentrator, and then sent to the DMS or DCADA for monitoring purposes. • The DMS or DCADA will utilize the substation and field device data as inputs to First Responder applications, and will send control commands back out to the devices.
<p>G. Analytical Method/Methodology</p> <p>The Technical Demonstration of this application does not require any analytical calculations.</p>

2.4.5.4 Substation Hierarchical Control

KCP&L Technology Demonstration Plan
<p>A. Description</p> <p>An IEC 61850 compliant substation automation network will be installed in the Midtown Substation along with automation control components to enable robust distributed automation functionality. The automation control components to be implemented include a substation communication controller for both substation and field devices; distributed automation controllers (DCADA); and an HMI for local monitoring and control of substation devices. The substation automation network will provide distributed intelligence at the substation that will enable execution of automated control operations based on feedback from real-time monitoring of transformers, relays, cap banks, and other field equipment installed throughout the circuits.</p>

B. Expected Results

The Technical Demonstration of this application is expected to yield the following:

- Evaluation of existing control system technologies to implement a distributed hierarchical control systems will provide experience and learning for the industry.
- Remote monitoring and operation of all substation equipment from a single location within the substation will provide an increased level of safety for the field operator.

C. Relevant Impact Metrics

The Technical Demonstration of this application will not contribute to any Impact Metrics.

D. Benefits Analysis Method/Factors

The Technical Demonstration of this application will not contribute to the project Benefits Analysis.

E. Baseline Data & Control Groups

The Technical Demonstration of this application does not require any Baseline Data or the establishment of any Control Groups.

F. Demonstration Method/Methodology:

The following points provide an overview of how the technical demonstration of this application will be accomplished:

- A fiber substation protection will be deployed at Midtown substation to enable communications to substation devices, and a Tropos wireless mesh network will be deployed throughout the demonstration project area to enable communications to field devices.
- Intelligent Electronic Devices (IEDs) will be deployed in Midtown substation and along the 11 designated smart grid feeders extending from Midtown substation.
- Data from the IEDs will be reported to a centralized data concentrator, and then sent to the substation DCADA and HMI for monitoring purposes.
- Verify that the DMS and the DCADA take similar action when given the same device statuses, depending on which system is in control of the substation.
- Verify that the HMI correctly reflects the substation device data in addition to the network status data.
- Verify that the user can control substation devices from the HMI.

G. Analytical Method/Methodology

The Technical Demonstration of this application does not require any analytical calculations.

2.4.6 Real-Time Load Measurement and Management

This function provides real-time measurement of customer consumption and management of load through Advanced Metering Infrastructure (AMI) systems (smart meters, two-way communications) and embedded appliance controllers that help customers make informed energy use decisions via real-time price signals, time-of-use (TOU) rates, and service options.

2.4.6.1 DOE SGCT Function to Benefit Rationale

Devices such as smart meters and appliance controllers can monitor the energy use of customer loads over the course of the day. These same devices can be used to help customers respond to pricing signals so that system load can be managed as a resource. Real-time measurement of customer consumption and management of load through Advanced Metering Infrastructure (AMI) systems and embedded appliance controllers help customers make informed energy use decisions via real-time price signals, time-of-use (TOU) rates, and service options. This function can provide eleven benefits:

- **Reduced Ancillary Service Cost** – The increased resolution of customer load data will improve load models and help grid operators to better forecast energy supply requirements. Improved forecasts, along with the ability to reduce customer demand effectively during critical periods, could reduce reserve margin requirements.
- **Deferred Distribution Capacity Investments** – Load growth and feeder reconfiguration can lead to increased loading on lines and transformers, to the point where distribution capacity investments become necessary. Smart meters and AMI will allow utilities to monitor customer loads and voltage more closely, and provide a platform for sending pricing signals that could influence consumption patterns. This could enable utilities to better anticipate and monitor feeder loading, and operate the distribution system closer to its limits. For example, it could be possible for a utility to delay building a new distribution feeder for one or more years without running the risk of low voltage problems. Each year that a capital investment can be deferred can yield a significant savings in the utility's revenue requirement (equal to the capital carrying charge of the upgrade). Therefore, Real-Time Load Measurement and Control could yield direct savings based on the time that it could postpone a capital investment.
- **Reduced Meter Reading Cost** – The data from smart meters can be automatically uploaded to a central meter data management system. This avoids the need to read meters manually, reducing the cost of performing this function.
- **Reduced Electricity Theft** – Smart meters can typically detect tampering. Moreover, a meter data management system can analyze customer usage to identify patterns that could indicate diversion.
- **Reduced Electricity Losses** – Peak load tends to affect delivery losses more than average load, and managing this peak could lead to improvements in electricity delivery efficiency. Being able to manage customer demand will give the utility the capability of reducing peak load, and thereby reduce delivery losses.
- **Reduced Sustained Outages** – Today, most utilities rely on customer calls to identify power outages and customer service representatives to enter the outage information into a computer system. Outage management systems have been designed to interpret this outage information and estimate the location of the fault based on the information. AMI systems perform outage detection based on the status of smart meters. This should improve the accuracy of outage notification, and reduce the time to restore service.

- **Reduced Major Outages** – Major outages occur as a result of hurricanes, ice storms, or other natural events that affect large geographical areas and tens of thousands of customers or more. Restoring electric service following these events typically takes a few days or more because of the massive damage that must be repaired on the distribution system. When utility crews move through an area making repairs to the distribution system, there are times when some customers fail to have their service restored because of unseen/overlooked damage. In such cases, when service is restored in the area, the utility crews may have left the area before the utility can receive a follow-up call from the customer saying that they are still without service. This means that the customer will be without service until a crew has time to come back to the area to fix the problem, and outage minutes will continue to increase. With AMI, utilities will be able to identify those customers who remain without power after the utility believes that power should be restored. This should make it easier to get a crew back to the location more quickly, and reduce the amount of time that the customer is outaged.
- **Reduced Restoration Cost** – AMI systems are being developed to perform outage detection based on the status of smart meters. This should improve the accuracy of outage notification and reduce the time to restore service. Reduced restoration times translate into reduced restoration costs because power can be restored with fewer restoration crew labor hours.
- **Reduced CO2 Emissions** – Manual meter reading requires that a person drive from meter to meter once each billing cycle. This produces CO2 emissions from the vehicle. Eliminating the vehicle miles traveled eliminates the associated emissions.
- **Reduced SOx, NOx, and PM-2.5 Emissions** – Polluting emissions associated with vehicle miles travelled are eliminated.
- **Reduced Oil Usage** – Eliminating vehicle miles traveled with automatic meter reading eliminates the associated fuel consumption.

2.4.6.2 Automated Meter Reading

KCP&L Operational Test Plan
<p>A. Description</p> <p>AMI will be deployed to the entire KCP&L SmartGrid Demonstration area. Deployment will include the installation of smart meters (capable of two-way communications, interval metering, and remote connect/disconnect) at approximately 14,000 residential, commercial, and industrial customers. Meters will measure, store, and wirelessly transmit 15-minute interval energy usage data to a central Meter Data Management (MDM) system where it will be available to other KCP&L systems. Communications between meters and the MDM will be accomplished through a dedicated RF-mesh Field Area Network (FAN) and KCP&L's private Wide Area Network (WAN).</p>
<p>B. Expected Results</p> <p>This operational demonstration of the AMI is expected to yield the following:</p> <ul style="list-style-type: none"> • AMI will capture meter reading at 15-minute intervals as opposed to the daily reads currently accomplished by KCP&L's Automated Meter Reading (AMR) system. • AMI will provide the interval metering and communication infrastructure required for many of the Demonstration Project applications. • AMI will demonstrate improved operational performance over the legacy AMR system, including the reporting of alarms/alerts indicating possible operational issues.

C. Relevant Impact Metrics

The Operational Testing of this application will contribute to these Impact Metrics.

AMI and CSA	Hourly Customer Electricity Usage – Res./Com./Ind. (kWh)
AMI and CSA	Monthly Customer Electricity Usage – Res./Com./Ind. (kWh)
AMI and CSA	Peak Load – Total (kW)
AMI and CSA	Peak Load by Customer Class – Res./Com./Ind. (kW)
AMI and CSA	Number of Meter Tamper Detections
AMI and CSA	Meter Data Completeness (%)
AMI and CSA	Meters Reporting Daily (%)

At each reporting milestone, operational test, or demonstration period, data will be compared to baseline data to determine a quantified impact. Quantified impacts measured will be reported in semi-annual impact metric reports.

D. Benefits Analysis Method/Factors

The DOE SGCT will be used to perform the Demonstration Project benefit analysis. For this application the following Smart Grid Function benefits will be quantified.

- Reduced Meter Reading Costs
- Reduced Electricity Theft

Benefits will be calculated using SGCT formulas. The following factors will be measured, projected or calculated during the application operation and/or demonstration.

Reduced Meter Reading Costs

- This benefit will not be realized as KCP&L already uses legacy AMR technology

Reduced Electricity Theft

- Number of Meter Tamper Detections (#) by customer class

E. Baseline Data & Control Groups

The Operational Analysis of this of this application does not require any Baseline Data or the establishment of any Control Groups.

F. Testing Method/Methodology:

The following points provide an overview of how the operational testing for this application will be accomplished:

- AMI interval metering that will be deployed in late 2010 to replace legacy AMR meters for all customers within the Demonstration Project area.
- AMI meter reading performance metrics tracking will be captured by the AHE.
- AMI meter reads and events will be processed by the AMI Head-End and sent to the MDM for analysis, reporting, and archival.

G. Analytical Method/Methodology

The following points provide an overview of the analytical methods that will be used to evaluate the impact and benefits of this application:

- AMI interval load data for all customers within the Project area will be extracted from the MDM System through KCP&L's Data Mining and Analysis Tool (DMAT) (DataRaker). The DMAT has built in functionality that will enable the aggregation and calculation of hourly load profiles by customer class.

2.4.6.3 Remote Meter Disconnect/Reconnect

KCP&L Operational Test Plan							
<p>A. Description</p> <p>AMI will be deployed to the entire KCP&L SmartGrid Demonstration area, approximately 14,000 residential and commercial customers. Nearly all of the AMI meters will have an integral switch capable of remote connect/disconnect capabilities. Integration between CIS, MDM, and the AMI will be implemented to automate remote connect/disconnect functionality to support customer requested connect/disconnect orders. Remote connect/disconnects for non-payment will not be implemented, due to current Public Service Commission requirements for the utility to attempt in-person contact prior to disconnect for non-payment.</p>							
<p>B. Expected Results</p> <p>This operational demonstration of the AMI is expected to yield the following:</p> <ul style="list-style-type: none"> • AMI two-way communications will enable KCP&L to remotely connect or disconnect customers from the KCP&L service center. • Truck rolls and Field Service Professional labor will be avoided for each remote connect/disconnect operation. 							
<p>C. Relevant Impact Metrics</p> <p>The Operational Testing of this application will contribute to these Impact Metrics.</p> <table border="1"> <tbody> <tr> <td>AMI and CSA</td> <td>Truck Rolls Avoided</td> </tr> <tr> <td>AMI and CSA</td> <td>Meter Operations Vehicle Miles Avoided</td> </tr> <tr> <td>AMI and CSA</td> <td>Avoided CO2 Emissions (tons)</td> </tr> </tbody> </table> <p>At each reporting milestone, operational test, or demonstration period, data will be compared to baseline data to determine a quantified impact. Quantified impacts measured will be reported in semi-annual impact metric reports.</p>		AMI and CSA	Truck Rolls Avoided	AMI and CSA	Meter Operations Vehicle Miles Avoided	AMI and CSA	Avoided CO2 Emissions (tons)
AMI and CSA	Truck Rolls Avoided						
AMI and CSA	Meter Operations Vehicle Miles Avoided						
AMI and CSA	Avoided CO2 Emissions (tons)						
<p>D. Benefits Analysis Method/Factors</p> <p>The DOE SGCT will be used to perform the Demonstration Project benefit analysis. For this application the following Smart Grid Function benefits will be quantified.</p> <ul style="list-style-type: none"> • Reduced Meter Reading Costs • Reduced CO2 Emissions <p>Benefits will be calculated using SGCT formulas. The following factors will be measured, projected or calculated during the application operation and/or demonstration.</p> <p>Reduced Meter Reading Costs</p> <ul style="list-style-type: none"> • Avoided Meter Operations Costs (\$) (FSP labor performing Connect/Disconnects) <p>Reduced CO2 Emissions</p> <ul style="list-style-type: none"> • Avoided Truck Rolls 							
<p>E. Baseline Data & Control Groups</p> <p>The Operational Analysis of this of this application does not require any Baseline Data or the establishment of any Control Groups.</p>							

F. Testing Method/Methodology:

The following points provide an overview of how the operational testing for this application will be accomplished:

- AMI interval metering that will be deployed in late 2010 to replace legacy AMR meters for all customers within the Demonstration Project area.
- Integration between CIS, MDM, and the AMI Head End will be implemented to automate the remote service order (connect/disconnect) processes.
- Remote connect/disconnect performance metrics tracking will be captured by the CIS service order subsystem.

G. Analytical Method/Methodology

The following points provide an overview of the analytical methods that will be used to evaluate the impact and benefits of this application:

- Avoided truck-rolls will be determined based on the number of successful remote connect and disconnect operations performed.

2.4.6.4 Meter Outage Restoration**KCP&L Technology Demonstration Plan****A. Description**

AMI will be deployed to the entire KCP&L SmartGrid Demonstration area, approximately 14,000 residential and commercial customers. Meters will wirelessly transmit power outage/restoration alerts via the AMI to a central Meter Data Management (MDM) system where it will be available to the OMS and other KCP&L systems. The MDM and AMI will also provide for on-demand verification of meter power status via the two-way communication network.

B. Expected Results

The operational demonstration of the AMI is expected to yield the following:

- Meter outage/restoration alerts will be transported via the AMI and MDM systems and received and processed by the OMS.
- AMI and MDM provide the active meter status in response to Power Status Verification requests issued by the OMS.
- Improved outage response should result from this application, but since the demonstration project systems are not used for production outage response; this benefit will not be measurable.

C. Relevant Impact Metrics

The Operational Testing of this application will contribute to these Impact Metrics.

AMI and CSA	SAIFI
AMI and CSA	SAIDI
AMI and CSA	CAIDI
AMI and CSA	Total Customers Served by SAIDI/SAIFI

At each reporting milestone, operational test, or demonstration period, data will be compared to baseline data to determine a quantified impact. Quantified impacts measured will be reported in semi-annual impact metric reports.

D. Benefits Analysis Method/Factors

The DOE SGCT will be used to perform the Demonstration Project benefit analysis. For this application the following Smart Grid Function benefits will be quantified.

- Reduced Sustained Outages

Benefits will be calculated using SGCT formulas. The following factors will be measured, projected or calculated during the application operation and/or demonstration.

Reduced Sustained Outages

- SAIDI (base &proj.)

E. Baseline Data & Control Groups

The following historical system level reliability statistics will be available for analysis:

- System Average Interruption Frequency Index (SAIFI)
- System Average Interruption Duration Index (SAIDI)
- Customer Average Interruption Duration Index (CAIDI)

F. Demonstration Method/Methodology:

The following points provide an overview of how the operational testing for this application will be accomplished:

- AMI interval metering that will be deployed in late 2010 to replace legacy AMR meters for all customers within the Demonstration Project area.
- Integration between AMI Head End, MDM, and the OMS will be implemented to process power outage/restoration event notifications and power status verification (request/reply) message flows.
- The Demonstration Project DMS-OMS will process and record all power outage/restore notifications for the demonstration project area in parallel to the production legacy OMS. The legacy OMS support all production outage restoration efforts.
- The Project Team will use the DMS-OMS to demonstrate benefit of using the PSV message flow to enhance outage restoration activities.

G. Analytical Method/Methodology

The Technical Demonstration of this application does not require any analytical calculations.

2.4.6.5 Demand Response Events**KCP&L Operational Test Plan****A. Description**

The implementation of a Distributed Energy Resource Management (DERM) System in conjunction with Programmable Communicating Thermostats (PCT) and other Home Area Network (HAN) connected devices will enable advanced utility utilization of demand response on the distribution system. The DERM will maintain a sophisticated distributed energy resource (DER) inventory and will be capable of forecasting, scheduling, selecting, and executing load control programs for all or select devices.

Two types of DR events will be implemented and tested. 1) for a 'stand-alone' PCTs communicating directly to the AMI, a Direct Load Control DR event will be issued through the

AMI system; 2) for HAN connected PCTs and devices, a 'Pay for Participation' DR event will be issued through the HEMP/HAN infrastructure. Demand response events then may be scheduled and executed system-wide (as is common practice now) or may now be isolated or grouped to only impact targeted circuits or sections of the distribution system to support reliability needs.

B. Expected Results

This operational demonstration is expected to yield the following:

- Implementation of DR events in accordance with OpenADR 2.0, IEC-61968-9, and ZigBee SEP 1.x will provide experience and learning for the industry.
- DERM/HEMP/AHE/PCT integration will enable utility-controlled reduction in kW on the entire system or on select groups of PCTs.
- DERM/HEMP/HAN integration will enable customer managed reduction in kW on the entire system or on selected groups of HAN connected PCTs and other devices.
- DERM will post process AMI data to determine the level of demand reduction achieved by each event participant.

C. Relevant Impact Metrics

The Operational Testing of this application will contribute to these Impact Metrics.

AMI and CSA	Direct Load Control Available via AMI (MW)
AMI and CSA	Direct Load Control Dispatched at Peak via AMI (MW)

At each reporting milestone, operational test, or demonstration period, data will be compared to baseline data to determine a quantified impact. Quantified impacts measured will be reported in semi-annual impact metric reports.

D. Benefits Analysis Method/Factors

The DOE SGCT will be used to perform the Demonstration Project benefit analysis. For this application the following Smart Grid Function benefits will be quantified.

- Deferred Generation Capacity Investment
- Deferred Distribution Capacity Investment

Benefits will be calculated using SGCT formulas. The following factors will be measured, projected or calculated during the application operation and/or demonstration.

Deferred Generation Capacity Investment

- Demand Response Used at Annual Peak Time (MW)

Deferred Distribution Capacity Investment

- Demand Response Used at Annual Peak Time (MW)

E. Baseline Data & Control Groups

AMI metering that is deployed for all customers, circuits, and distributed energy resources within the Demonstration Project area. The following usage data will be available for baselines::

- 15 minute interval load data of all customers.

The following system level energy production data will be available for analysis:

- Historical and current hourly system energy production load profile data.
- Historical weather adjusted system energy production load profile data.

Since the DR programs will be event-based, the DERM will construct baseline profiles for each program participant from available interval AMI metering data.

F. Testing Method/Methodology:

The following points provide an overview of how the operational testing for this application will be accomplished:

- DERM includes DR assets deployed by Smart End use programs
- User is capable of creating programs for thermostats and HANs in the DERM
- DMS identified potential overload or company system peak events and calls on the DERM for assistance
- DERM evaluates options and creates DR events
- DERM dispatches DR events
- DERM scheduled and executed DR events will be tracked by the DERM system and participant compliance will be tracked by the HEMP system
- Post event analysis to determine DR load reduction

G. Analytical Method/Methodology

The following points provide an overview of the analytical methods that will be used to evaluate the impact and benefits of this application:

- Interval load data for customers participating in DERM DR programs will be measured through KCP&L's AMI system deployed as part of the Project.
- The DERM will construct baseline profiles for each program participant from available interval AMI metering data.
- DERM scheduled and executed DR events will be tracked by the DERM system and participant compliance will be tracked by the HEMP system.
- The DERM will perform 'after the fact' analysis of each DR event to determine the level of demand reduction achieved by each event participant.
- The DERM analysis will be accomplished by directly comparing event day load profiles for each participating circuit to baseline load profiles.
- The difference at each daily time point should closely reflect DERM forecasted demand reduction potential throughout the event.

2.4.7 Customer Electricity Use Optimization

Customer electricity use optimization is possible if customers are provided with information to make educated decisions about their electricity use. Customers should be able to optimize toward multiple goals such as cost, reliability, convenience, and environmental impact.

2.4.7.1 DOE SGCT Function to Benefit Rationale

A key characteristic of the smart grid is that it motivates and includes the customer. This function enables customers to observe their consumption patterns and modify them according to their explicit or implicit objectives. These could include minimizing cost, maximizing reliability, or purchasing renewable energy, among others. Nine benefits are provided:

- **Deferred Generation Capacity Investments** – Utilities build generation, transmission, and distribution with capacity sufficient to serve the maximum amount of load that planning forecasts indicate. The trouble is, this capacity is only required for very short periods each year, when demand peaks. The smart grid can help reduce peak demand and flatten the load curve by giving customers the information and incentives to better manage their electricity usage. This should translate into lower infrastructure investments by utilities and cheaper electricity for customers.

- **Deferred Transmission Capacity Investments** – See Deferred Generation Capacity Investments, above.
- **Deferred Distribution Capacity Investments** – See Deferred Generation Capacity Investments, above.
- **Reduced Electricity Cost** – The information provided by smart meters and in-home displays may encourage customers to alter their usage patterns (demand response with price signals or direct load control), or conserve energy generally because they can see how much it costs and alter their behavior. Changes in usage can result in reductions in the total cost of electricity.
- **Reduced Ancillary Service Cost** – The ability to reduce customer demand effectively during critical periods could reduce reserve margin requirements.
- **Reduced Congestion Cost** – If customers have tools to manage their energy use, this could lead to a more conservative use of electricity especially at peak times, so less electricity must be passed through the T&D lines, which reduces congestion.
- **Reduced Electricity Losses** – Higher line loading tends to affect delivery losses more than average load, and managing this peak could lead to improvements in electricity delivery efficiency. If the customer is aware of their electricity use and shifts it to off-peak times, the losses may be reduced.
- **Reduced CO₂ Emissions** – Increased customer awareness of electricity use may lead to conservation which, in turn would decrease the electricity generation required and the associated emissions. Furthermore, customer pricing and incentives can be used to optimize the load shape (especially at peak) leading to increased system efficiency which will reduce the amount of generation required to serve load. Assuming that the generation is fossil-based, emissions will be reduced.
- **Reduced SO_x, NO_x, and PM-2.5 Emissions** – Increased customer awareness of electricity use may lead to conservation which, in turn would decrease the electricity generation required and the associated emissions. Furthermore, customer pricing and incentives can be used to optimize the load shape (especially at peak) leading to increased system efficiency which will reduce the amount of generation required to serve load. Assuming that the generation is fossil-based, emissions will be reduced.

2.4.7.2 Historical Interval Usage Access

KCP&L Operational Test Plan

A. Description

All customers in the Demonstration Project will be provided access to the KCP&L-hosted Home Energy Management Portal (HEMP), a website that presents customers with various tools with which they may visualize and analyze their detailed energy usage history. The HEMP website will be accessible through KCP&L's AccountLink website and provides customer with:

- Historical 15 minute interval usage information from their smart meter presented within user-friendly visualizations allowing them to evaluate their energy consumption
- A daily bill update that provides Bill to Date, days remaining in billing period, and an Estimated Bill Projection based on current consumption patterns.
- Information, tools, advice, and programs to manage and reduce electricity costs.

B. Expected Results

With the additional information that the HEMP provides the consumer, it is expected that:

- Customers will use the historical interval metering data available on the HEMP to better understand their total energy consumption and patterns.
- Customers will find the Bill to Date and Estimated Bill information provided on the HEMP useful in managing their energy usage costs.
- HEMP users will reduce their overall energy consumption. Other studies have shown that HEMP users may reduce their overall energy consumption by as much as 1-5%.

C. Relevant Impact Metrics

The Operational Testing of this application will contribute to these Impact Metrics.

AMI and CSA	Hourly Customer Electricity Usage – Res./Com./Ind. (kWh)
AMI and CSA	Monthly Customer Electricity Usage – Res./Com./Ind. (kWh)

At each reporting milestone, operational test, or demonstration period, customer usage data will be reported in semi-annual impact metric reports.

D. Benefits Analysis Method/Factors

The DOE SGCT will be used to perform the Demonstration Project benefit analysis. For this application the following Smart Grid Function benefits will be quantified.

- Reduced Electricity Costs

Benefits will be calculated using SGCT formulas. The following factors will be measured, projected or calculated during the application operation and/or demonstration.

Reduced Electricity Costs (Consumer)

- Reduced Total Annual Electric Consumption (kWh) by customer class.

E. Baseline Data & Control Groups

AMI metering that is deployed for all customers, circuits, and distributed energy resources within the Demonstration Project area. The following usage data will be available for baselines:

- 15 minute interval load data of all customers.
- Average hourly interval load data by customer class.

Legacy AMR metering is available for all other customers in the Kansas City metro area. The following usage data will be available for baselines and control groups:

- Daily kWh usage data for all customers
- Daily kWh usage data for all customers in the project area prior to AMI
- 15 minute interval load data for select control group customers outside the project area

Impacts to customer electricity usage and cost for HEMP users will be quantified through the use of a control group:

- Control group will consist of interval and daily load profile data (kWh) for selected customers outside the project area but of similar demographic and geographic vicinity
- Control group load profiles will be captured through the legacy AMR interval metering with increased data reporting

F. Testing Method/Methodology:

The following points provide an overview of how the operational testing for this application will be accomplished:

- 15 minute interval load data will be collected for all HEMP participants throughout the project period through KCP&L's AMI system deployed as part of the Project.
- All interval meter data will be stored in KCP&L's MDM System and DMAT.
- At the conclusion of the operational period (through October 2014), HEMP participants interval and aggregate usage data will be compared to coincident control group interval and aggregate usage data.

G. Analytical Method/Methodology

The following points provide an overview of the analytical methods that will be used to evaluate the impact and benefits of this application:

- Load profiles of HEMP participants will be compared to those of select control group customers on an hourly, daily, and monthly basis to evaluate the average or typical impact HEMP exhibits on measured participant energy usage. Calculated impacts will be assessed for statistical significance.
- Willing HEMP participants will be surveyed by a third party to solicit feedback on their experience using the HEMP website to determine their primary application of the tool and information provided.

2.4.7.3 In-Home Display**KCP&L Operational Test Plan****A. Description**

All customers in the Demonstration Project will be offered, at no cost, an In-Home Display (IHD). This IHD is a portable, digital display device that communicates with a customer's AMI meter via ZigBee and provides real-time energy usage monitoring. This enables them to gain improved awareness and thus better manage their personal energy usage and associated costs. The IHD essentially provides customers with a real-time "speedometer" and "odometer" for electric use in their home – giving them both current consumption rate information as well as access to visualize historical usage information.

The IHD will provide customers with:

- Real-time energy usage and cost information from their smart meter.
- Current price of energy based on their rate, current usage block, and/or TOU period.
- Daily bill update that provides Bill to Date, days remaining in billing period, and an Estimated Bill Projection based on current consumption patterns.
- Demand Response (DR) messages asking them to reduce load during peak times.
- Other Informational messages sent from the utility.

B. Expected Results

With the additional information that the IHD provides the consumer, it is expected that:

- Customers will use the real-time metering data available on the IHD to better understand their total energy consumption patterns and those of individual appliances.

- Customers will find the Bill to Date and Estimated Bill information provided on the IHD useful in managing the energy usage costs.
- IHD users will reduce their overall energy consumption. Other studies have shown that IHD users may reduce their overall energy consumption by as much as 2-7%.
- IHD user will voluntarily participate in DR events when notified via the IHD.

C. Relevant Impact Metrics

The Operational Testing of this application will contribute to these Impact Metrics.

AMI and CSA	Hourly Customer Electricity Usage – Res./Com./Ind. (kWh)
AMI and CSA	Monthly Customer Electricity Usage – Res./Com./Ind. (kWh)

At each reporting milestone, operational test, or demonstration period data customer usage data will be compiled and reported in semi-annual impact metric reports.

D. Benefits Analysis Method/Factors

The DOE SGCT will be used to perform the Demonstration Project benefit analysis. For this application the following Smart Grid Function benefits will be quantified.

- Reduced Electricity Costs

Benefits will be calculated using SGCT formulas. The following factors will be measured, projected or calculated during the application operation and/or demonstration.

Reduced Electricity Costs (Consumer)

- Reduced Total Annual Electric Consumption (kWh) by customer class.

E. Baseline Data & Control Groups

AMI metering that is deployed for all customers, circuits, and distributed energy resources within the Demonstration Project area. The following usage data will be available for baselines:

- 15 minute interval load data of all customers.
- Average hourly interval load data by customer class.

Legacy AMR metering is available for all other customers in the Kansas City metro area. The following usage data will be available for baselines and control groups:

- Daily kWh usage data for all customers
- Daily kWh usage data for all customers in the project area prior to AMI
- 15 minute Interval load data for select control group customers outside the project area

Impacts to customer electricity usage and cost for IHD users will be quantified through the use of a control group:

- Control group will consist of interval and daily load profile data (kWh) for selected customers outside the project area but of similar demographic and geographic vicinity.
- Control group load profiles will be captured through the legacy AMR interval metering with increased data reporting.
- Baseline data for HAN users with regards to demand response events will also consist of weather-adjusted previous or proxy day load profiles.

F. Testing Method/Methodology:

The following points provide an overview of how the operational testing for this application will be accomplished:

- 15 minute interval load data will be collected for all IHD participants throughout the project period through KCP&L's AMI system deployed as part of the Project
- All interval meter data will be stored in KCP&L's MDM System and DMAT
- At the conclusion of the operational period (through October 2014), IHD participants interval and aggregate usage data will be compared to coincident control group interval and aggregate usage data

G. Analytical Method/Methodology

The following points provide an overview of the analytical methods that will be used to evaluate the impact and benefits of this application:

- Load profiles of IHD participants will be compared to those of select control group customers on an hourly, daily, and monthly basis to evaluate the average or typical impact IHD exhibits on measured participant energy usage. Calculated impacts will be assessed for statistical significance.
- For impact during DR events, load profiles of IHD participants on event days will also be compared to previous or proxy day load profiles for the same customer. Previous or proxy days will be days without DR events.
- Willing IHD participants will be surveyed by a third party to solicit feedback on their experience using the IHD to determine their primary application of the tool and information provided.

2.4.7.4 Home Area Network**KCP&L Operational Test Plan****A. Description**

All customers in the Demonstration Project, that meet program criteria will be offered, at no cost, a Home Area Network (HAN). The HAN consists of a broadband gateway device communicating to the KCP&L meter and to numerous energy devices in customer home. Program participants will also receive a compatible programmable communicating thermostat (PCT) and two compatible load control switches. The PCT will be enrolled in the pilot utility DR program.

The gateway device will get real-time usage information directly from the customer's smart meter and will also establish communications between the utility Home Energy Management Portal (HEMP) via the customer supplied internet connection. The combination of HEMP/HAN functionality will provide customers:

- With a user-friendly visualization of real-time usage data from their smart meter via the HEMP and allow them to make energy usage decisions based on real-time usage and cost information
- The ability to remotely control their PCT and other energy consuming appliances via the load control switch(es) to manage their daily energy consumption

Additionally, the HAN will provide the capability for all HAN connected devices to participate in demand response events based on customer preferences.

B. Expected Results

With the additional control and information that the HAN provides the consumer, it is expected that:

- Customers will use the information on the HEMP to better understand their total energy consumption and patterns
- Customers will utilize the information and control provided via the HAN effective in managing their energy usage costs
- HAN users will reduce their overall energy consumption. Other studies have shown that HAN users may reduce their overall energy consumption by as much as 1-5%

For those that choose to combine HAN control capabilities with new voluntary TOU rate options, it is expected that the HAN users will

- Shift load to off peak times
- Voluntarily allow HAN-connected devices to participate in DR events

Additionally, the HAN deployments will be used to demonstrate customer incented DR events.

C. Relevant Impact Metrics

The Operational Testing of this application will contribute to these Impact Metrics.

AMI and CSA	Hourly Customer Electricity Usage – Res./Com./Ind. (kWh)
AMI and CSA	Monthly Customer Electricity Usage – Res./Com./Ind. (kWh)

At each reporting milestone, operational test, or demonstration period data customer usage data will be compiled and reported in semi-annual impact metric reports.

D. Benefits Analysis Method/Factors

The DOE SGCT will be used to perform the Demonstration Project benefit analysis. For this application the following Smart Grid Function benefits will be quantified.

- Deferred Generation Capacity Investments
- Reduced Electricity Costs

Benefits will be calculated using SGCT formulas. The following factors will be measured, projected or calculated during the application operation and/or demonstration.

Deferred Generation Capacity Investments

- Customer Load Reduction at Annual Peak Time (MW)

Reduced Electricity Costs (Consumer)

- Reduced Total Annual Electric Consumption (kWh) by customer class.

E. Baseline Data & Control Groups

AMI metering that is deployed for all customers, circuits, and distributed energy resources within the Demonstration Project area. The following usage data will be available for baselines:

- 15 minute interval load data of all customers.
- Average hourly interval load data by customer class.

Legacy AMR metering is available for all other customers in the Kansas City metro area. The following usage data will be available for baselines and control groups:

- Daily kWh usage data for all customers
- Daily kWh usage data for all customers in the project area prior to AMI
- 15 minute Interval load data for select control group customers outside the project area

Impacts to customer electricity usage and cost for HAN users will be quantified through the use of a control group:

- Control group will consist of interval and daily load profile data (kWh) for selected customers outside the project area but of similar demographic and geographic vicinity.
- Control group load profiles will be captured through the legacy AMR interval metering with increased data reporting.
- Baseline data for HAN users with regards to demand response events will also consist of weather-adjusted previous or proxy day load profiles

F. Testing Method/Methodology:

The following points provide an overview of how the operational testing for this application will be accomplished:

- 15 minute interval load data will be collected for all HAN participants throughout the project period through KCP&L's AMI system deployed as part of the Project
- All interval meter data will be stored in KCP&L's MDM System and DMAT
- At the conclusion of the operational period (through October 2014), HAN participants interval and aggregate usage data will be compared to coincident control group interval and aggregate usage data

G. Analytical Method/Methodology

The following points provide an overview of the analytical methods that will be used to evaluate the impact and benefits of this application:

- Load profiles of HAN participants will be compared to those of select control group customers on an hourly, daily, and monthly basis to evaluate the average or typical impact HAN exhibits on measured participant energy usage. Calculated impacts will be assessed for statistical significance.
- For impact during DR events, load profiles of HAN participants on event days will also be compared to previous or proxy day load profiles for the same customer. Previous or proxy days will be days without DR events.
- Willing HAN participants will be surveyed by a third party to solicit feedback on their experience using the HAN to determine their primary application of the tool and information provided.

2.4.7.5 Time-of-Use Rate

KCP&L Operational Test Plan

A. Description

All Residential customers in the Demonstration Project will be offered the ability to participate in a pilot Time-of-Use (TOU) rate. While designed to be revenue neutral, the pilot TOU tariff provides significant incentive for customers to shift load from peak periods to off-peak periods due to a relatively large difference between peak and off-peak prices during the summer months. On this pilot TOU rate, during summer months, the peak energy price (\$/kWh) is approximately six times greater than the off-peak price.

B. Expected Results

During the summer when the TOU rates are in effect, it is expected that TOU participants will:

- Shift load from peak to off-peak times
- Reduce their overall kWh consumption
- Achieve an overall reduction in their electricity bill

It is also expected that some TOU participants will also participate in IHD or HAN programs and that those dual participants may achieve greater savings than participants without devices.

C. Relevant Impact Metrics

The Operational Testing of this application will contribute to these Impact Metrics.

AMI and CSA	Hourly Customer Electricity Usage – Res./Com./Ind. (kWh)
AMI and CSA	Monthly Customer Electricity Usage – Res./Com./Ind. (kWh)

At each reporting milestone, operational test, or demonstration period data customer usage data will be compiled and reported in semi-annual impact metric reports.

D. Benefits Analysis Method/Factors

The DOE SGCT will be used to perform the Demonstration Project benefit analysis. For this application the following Smart Grid Function benefits will be quantified.

- Deferred Generation Capacity Investments
- Reduced Electricity Costs

Benefits will be calculated using SGCT formulas. The following factors will be measured, projected or calculated during the application operation and/or demonstration.

Deferred Generation Capacity Investments

- Customer Load Reduction at Annual Peak Time (MW)

Reduced Electricity Costs (Consumer)

- Reduced Total Annual Electric Consumption (kWh) by customer class.

E. Baseline Data & Control Groups

AMI metering that is deployed for all customers, circuits, and distributed energy resources within the Demonstration Project area. The following usage data will be available for baselines::

- 15 minute interval load data of all customers.
- Average hourly interval load data by customer class

Legacy AMR metering is available for all other customers in the Kansas City metro area. The following usage data will be available for baselines and control groups:

- Daily kWh usage data for all customers
- Daily kWh usage data for all customers in the project area prior to AMI
- 15 minute Interval load data for select control group customers outside the project area

The following system level energy production data will be available for analysis:

- Historical and current hourly average and marginal energy production cost data.
- Historical and current hourly system energy production load profile data.
- Historical weather adjusted system energy production load profile data.

Impacts to customer electricity usage and cost for TOU participants will be quantified through the use of a control group:

- Control group will consist of interval and daily load profile data (kWh) for selected customers outside the project area but of similar demographic and geographic vicinity
- Control group load profiles will be captured through the legacy AMR interval metering with increased data reporting

F. Testing Method/Methodology:

The following points provide an overview of how the operational testing for this application will be accomplished:

- 15 minute interval load data will be collected for all TOU participants throughout the project period through KCP&L's AMI system deployed as part of the Project.
- All interval meter data will be stored in KCP&L's MDM System and DMAT.
- At the conclusion of the operational period (through October 2014), TOU participants interval and aggregate usage data will be compared to coincident control group interval and aggregate usage data.

G. Analytical Method/Methodology

The following points provide an overview of the analytical methods that will be used to evaluate the impact and benefits of this application:

- AMI interval load data for each solar generation customers within the Project area will be extracted from the MDM System through KCP&L's Data Mining and Analysis Tool (DMAT) (DataRaker).
- The DMAT has built in functionality that will enable the aggregation and calculation of the following hourly load profiles.
 - Net Energy Solar Production from each Solar Generation site
 - Total Net Energy Solar Production for all Solar Generation sites.
 - Ave Net Energy Solar Production per kW of Solar Generation Nameplate Capacity
- Distributed Generation Use at Annual Peak Time (MW) will be determined by selecting the Total Net Energy Solar Production value at the System Annual Peak Hour.
- Annual Reduced Utility Electricity Cost analysis will performed by summing the hourly savings that are calculated from the hourly Total Net Energy Solar Production load profile data and the hourly average and marginal energy production cost data

2.4.8 Distributed Production of Electricity

Smart grid functions allow utilities to remotely operate DG systems to control output, defer upgrades to generation and T&D assets, and improve voltage regulation. This category includes dispatchable, distributed generation such as combined heat and power, fossil fuel powered backup generators, bio-fuel powered backup generators (e.g., biodiesel, waste to energy, digester gas) or geo-thermal energy. It also includes variable, distributed generation such as solar and wind.

2.4.8.1 DOE SGCT Function to Benefit Rationale

Distributed generation (DG) is located on the distribution system, either on primary distribution feeders or behind the meter. DG supports economic, reliability, and environmental benefits depending on the resource type. Solar photovoltaic panels may support the following benefits:

- **Deferred Generation Capacity Investments** - DG can be used to reduce the amount of central station generation required during peak times. This may improve the overall load profile and allow a more efficient mix of generation resources to be dispatched. This could save utilities money on their generation costs.
- **Reduced Ancillary Service Payments** – The reserve margin is a required capacity above the peak demand that must be available and is typically on the order of 12% to 15% of peak demand. If peak demand is reduced, reserve margin might be reduced -- requires that the peak be permanently reduced, not just occasionally or periodically (when the sun shines on peak). The availability of the DG resources is critical here.
- **Reduced Congestion Costs** – DG provides energy closer to the end use, so less electricity must be passed through the T&D lines, which reduces congestion.
- **Deferred Transmission Capacity Investments** – Utilities build transmission with capacity sufficient to serve the maximum amount of load that planning forecasts indicate. The trouble is, this capacity is only required for very short periods each year, when demand peaks. Providing generation capacity closer to the load reduces the power flow on transmission lines, potentially avoiding or deferring capacity upgrades. This may be particularly effective during peak load periods.
- **Deferred Distribution Capacity Investments** – DG could be used to relieve load on overloaded feeders, potentially extending the time before upgrades are required.
- **Reduced Electricity Losses** – By managing peak feeder loads with DG, peak feeder losses, which are higher than at non-peak times, would be reduced.
- **Reduced Electricity Costs** – DG could be used to reduce the cost of electricity during times when the price of "grid power" exceeds the cost of producing the electricity with DG. A consumer or the owner of an EER realizes savings on his electricity bill.
- **Reduced Sustained Outages** – The benefit to consumers is based on the value of service (VOS).⁶ Distributed generation could be used as a backup power supply for one or more customers until normal electric service could be restored. But, if it is used as part of the recovery of the system, then its value is already accounted for, so we can't count individual customer benefits.
- **Reduced CO2 Emissions** – Renewable-based DG can provide energy with greatly reduced net CO2 emissions produced by fossil-based electricity generators. However, depending on the type of DG and the central generation mix during peak and off-peak times, the impact can be positive or negative.
- **Reduced SOX, NOX, and PM-10 Emissions** – Renewable energy provides electricity without net SOX, NOX, and PM-10 emissions produced by fossil-based electricity generators providing energy and peak demand. However, depending on the type of DG and the central generation mix during peak and off-peak times.

2.4.8.2 Distributed Roof-Top Solar Generation (DG)

KCP&L Operational Test Plan

A. Description

Approximately 180 kW of distributed solar capacity will be installed within the SmartGrid Demonstration Project area by KCP&L. These systems will likely consist of one large commercial-scale system to be installed on a local school rooftop and various smaller distributed systems on homes and businesses throughout the project area. All solar systems are currently planned to be utility owned, installed on leased roof-tops, and connected on the utility side of the meter.

B. Expected Results

This technical demonstration is expected to yield the following:

- Development of a per unit 'solar generation' load curve that can be used to assess the impact of solar generation on customer, circuit, and system level analysis.
- Determine the coincidence of solar generation with system annual peak, expressed as a percentage solar generation nameplate rating.
- Determine the go forward viability of a 'leased roof top' business model for utility owned distributed solar generation.

C. Relevant Impact Metrics

The Technical Demonstration of this application will not contribute to any Impact Metrics.

D. Benefits Analysis Method/Factors

The DOE SGCT will be used to perform the Demonstration Project benefit analysis. For this application the following Smart Grid Function benefits will be quantified.

- Deferred Generation Capacity Investments
- Reduced Electricity Costs
- Reduced CO2 Emissions

Benefits will be calculated using SGCT formulas. The following factors will be measured, projected or calculated during the application operation and/or demonstration.

Deferred Generation Capacity Investments

- Distributed Generation Use at Annual Peak Time (MW)

Reduced Electricity Costs (Utility)

- Annual Distributed Generation Production (MWH)

Reduced CO2 Emissions

- Annual Distributed Generation Production (MWH)

E. Baseline Data & Control Groups

AMI metering that is deployed for all customers, circuits, and distributed energy resources within the Demonstration Project area. The following usage data will be available for baselines::

- 15 minute interval load data of all customers.
- Average hourly interval load data by customer class.
- 15 minute interval total load data for circuit.
- 15 minute interval delivered and received load data for each Solar DG site.

The following system level energy production data will be available for analysis:

- Historical and current hourly average and marginal energy production cost data.
- Historical and current hourly system energy production load profile data.
- Historical weather adjusted system energy production load profile data.

F. Testing Method/Methodology

The following points provide an overview of how the operational testing for this application will be accomplished:

- Solar generation production data at each site will be measured through the AMI system deployed as part of the Project. All data collected will be stored in KCP&L's Meter Data Management (MDM) System.

- The solar generation systems will be metered to measure energy received from and delivered to the grid to provide the net efficiency of the solar generation system. The load profile of energy delivered and received for each Solar Generation unit will be collected and available.

G. Analytical Method/Methodology

The following points provide an overview of the analytical methods that will be used to evaluate the impact and benefits of this application:

- AMI interval load data for each solar generation customers within the Project area will be extracted from the MDM System through KCP&L's Data Mining and Analysis Tool (DMAT) (DataRaker).
- The DMAT has built in functionality that will enable the aggregation and calculation of the following hourly load profiles.
 - Net Energy Solar Production from each Solar Generation site
 - Total Net Energy Solar Production for all Solar Generation sites.
 - Average Net Energy Solar Production per kW of Solar Generation Nameplate Capacity.
- Distributed Generation Use at Annual Peak Time (MW) will be determined by selecting the Total Net Energy Solar Production value at the System Annual Peak Hour.
- Annual Reduced Utility Electricity Cost analysis will performed by summing the hourly savings that are calculated from the hourly Total Net Energy Solar Production load profile data and the hourly average and marginal energy production cost data.

2.4.9 Storing Electricity for Later Use

Remote Control of electricity storage (ES) inflow/outflow reduces energy costs and enhances power generation and transmission and distribution capacity utilization.

2.4.9.1 DOE SGCT Function to Benefit Rationale

Electricity can be stored as chemical or mechanical energy and used later by consumers, utilities or grid operators. In distributed applications, energy storage technologies most likely utilize inverter-based electrical interfaces that can produce real and reactive power. Depending on the capacity and stored energy of these devices, they can provide the following economic, reliability, and environmental benefits.

- **Optimized Generator Operation** – The ability to respond to changes in load would enable grid operators to dispatch a more efficient mix of generation that could be optimized to reduce cost, including the cost associated with polluting emissions. Electricity storage can be used to absorb generator output as electrical load decreases, allowing the generators to remain in their optimum operating zone. The stored electricity could then be used later so that dispatching additional, less efficient generation could be avoided. The storage can have the effect of smoothing the load curve that the generation fleet must meet. This benefit includes two components: (1) avoided generator start-up costs and (2) improved performance due to improved heat rate efficiency and load shaving.
- **Deferred Generation Capacity Investments** – Electricity storage can be used to reduce the amount of central station generation required during peak times. This would tend to improve the overall load profile and allow a more efficient mix of generation resources to be dispatched. This can save utilities money on their generation costs.

- **Reduced Ancillary Services Cost** – Ancillary services including spinning reserve and frequency regulation can be provided by energy storage resources. The reserve margin is a required capacity above the peak demand that must be available and is typically +15% of peak demand. If peak demand is reduced, reserve margin would be reduced.
- **Reduced Congestion Cost** – Distributed energy resources provide energy closer to the end use, so less electricity must be passed through the T&D lines, which reduces congestion.
- **Deferred Transmission Capacity Investments** – Utilities build transmission with capacity sufficient to serve the maximum amount of load that planning forecasts indicate. The trouble is, this capacity is only required for very short periods each year, when demand peaks. Providing stored energy capacity closer to the load reduces the power flow on transmission lines, potentially avoiding or deferring capacity upgrades. This may be particularly effective during peak load periods.
- **Deferred Distribution Capacity Investments** – Electricity storage can also be used to relieve load on overloaded stations and feeders, potentially extending the time before upgrades or additions are required.
- **Reduced Electricity Losses** – By managing peak feeder loads with electricity storage, peak feeder losses, which are higher than at non-peak times, would be reduced.
- **Reduced Electricity Costs** – Electricity storage can be used to reduce the cost of electricity, particularly during times when the price of "grid power" is very high. A consumer or the owner of an enabled DER realizes savings on his electricity bill.
- **Reduced Sustained Outages** – Electricity storage can be used as a backup power supply for one or more customers until normal electric service can be restored. However, the backup would only be possible for a limited time (a few hours) depending on the amount of energy stored.
- **Reduced Momentary Outages** – When combined with the necessary control system, energy storage could act like an uninterruptible power supply (UPS), supporting end use load during a momentary outage.
- **Reduced Sags and Swells** – The same UPS capability could be used to enable load to ride through voltage sags and swells.
- **Reduced CO₂ Emissions** – Electricity storage can reduce electricity peak demand. This translates into a reduction in CO₂ emissions produced by fossil-based electricity generators. However, since electricity storage has an inherent inefficiency associated with it, electricity storage could increase overall CO₂ emissions if fossil fuel generators are used for charging.
- **Reduced SO_x, NO_x, and PM-10 Emissions** – Electricity storage can reduce electricity peak demand. This translates into a reduction in polluting emissions produced by fossil-based electricity generators. However, since electricity storage has an inherent inefficiency associated with it, electricity storage could increase overall emissions if fossil fuel generators are used for charging.
- **Reduced Oil Usage** – If plug-in electric vehicles are utilized as grid storage assets, they can also provide the additional benefit of reduced oil usage. PEVs increase the fuel efficiency of vehicles by using electric energy stored in their batteries to power the vehicle as opposed to using oil based fuel. This fuel efficiency gain translates into a reduction in oil consumption per mile traveled.

2.4.9.2 Electric Energy Time Shift

The Electric Energy Time-Shift application involves storing electricity when the price of electricity is low and discharging that electricity when the price of electricity is high. The energy that is discharged from the ES could be sold via the wholesale market, sold under terms of a power purchase agreement, or used by an integrated utility to reduce the overall cost of providing generation during peak times.

KCP&L Operational Test Plan

A. Description

A 1.0 MWh, 1.0 MW-capable grid-connected Battery Energy Storage System (BESS) will be installed at the Midtown Substation with direct interconnect to a single 13.2 kV circuit, immediately downstream of the substation transformer. A daily charge/discharge cycle will be implemented to demonstrate and evaluate the operational benefit of using the battery for electric energy time shift applications.

B. Expected Results

The operational demonstration of the grid connected battery in this application is expected to yield the following:

- The system is expected to operate at greater than 70% efficient with respect to net energy output versus input.
- Utility electric production costs will be reduced by charging the battery with low cost off-peak energy and discharging it at higher cost production times.

C. Relevant Impact Metrics

The Operational Testing of this application will contribute to these Impact Metrics.

Storage	Annual Storage Dispatch (kWh)
Storage	Average Energy Storage Efficiency (%)

At each reporting milestone, operational test, or demonstration period, data will be compared to baseline data to determine a quantified impact. Quantified impacts measured will be reported in semi-annual impact metric reports.

D. Benefits Analysis Method/Factors

The DOE SGCT will be used to perform the Demonstration Project benefit analysis. For this application the following Smart Grid Function benefits will be quantified.

- Reduced Electricity Costs

Benefits will be calculated using SGCT formulas. The following factors will be measured, projected or calculated during the application operation and/or demonstration.

Reduced Electricity Costs (Utility)

- Reduced Total Annual Electric Production Cost (\$)

Additionally, the DOE ESCT (Energy Storage Computational Tool) will be used to perform the benefit analysis for a utility owned GES system. The following Stationary Energy Storage applications will be combined in this analysis.

- Primary Application – Electric Energy Time Shift
- Secondary Application – Electric Supply Capacity
- Secondary Application – T&D Upgrade Deferral

Primary Benefit: Reduced Electricity Costs (Utility/Ratepayer)

- Calculation: Total Energy Discharged for Energy Time-Shift (MWh) x [Avg. Variable Peak Generation Cost (\$/MWh) - Avg. Variable Off-Peak Generation Cost (\$/MWh) / ES Efficiency (%)]

E. Baseline Data & Control Groups

AMI metering that is deployed for all customers, circuits, and distributed energy resources within the Demonstration Project area. The following usage data will be available for baselines::

- 15 minute interval total load data for the battery circuit.
- 15 minute interval delivered and received load data for the grid battery.

The following system level energy production data will be available for analysis.

- Historical and current hourly average and marginal energy production cost data.
- Historical and current hourly system energy production load profile data.
- Historical weather adjusted system energy production load profile data.

F. Testing Method/Methodology:

The following points provide an overview of how the operational testing for this application will be accomplished:

- Energy delivered and received to the BESS will be measured on the high side of the BESS interconnection transformer through the AMI system deployed as part of the Project. All data collected will be stored in KCP&L's Meter Data Management (MDM) System.
- Weekly daily charge/discharge cycle will be implemented to demonstrate and evaluate the operational benefit of using the battery for electric energy time shift applications. Charging will occur daily from 1-6 a.m. and discharge will occur from 3-7 p.m.
- Individual seasonal testing and data collection periods will be conducted to evaluate the potential impact of seasonal parasitic loads on overall BESS efficiency.

G. Analytical Method/Methodology

The following points provide an overview of how the operational testing for this application will be accomplished:

- AMI interval load data for the BESS will be extracted from the MDM System through KCP&L's Data Mining and Analysis Tool (DMAT) (DataRaker).
- The DMAT has built in functionality that will enable and calculation of the following hourly load profiles.
 - BESS Energy Discharged to grid.
 - BESS Energy Received from grid.
- An annual hourly charge/discharge load profile for the BESS will be constructed using the DMAT load profile data created for the application operational testing periods,
- The Annual BESS Efficiency will be calculated as (Annual BESS Energy Delivered)/(Annual BESS Energy Received)
- Annual Reduced Utility Electricity Cost will be calculated as $\Sigma[(\text{hourly BESS Energy Discharged}) \times (\text{hourly average/marginal energy production cost})] - \Sigma[(\text{hourly BESS Energy Received}) \times (\text{hourly average/marginal energy production cost})]$

2.4.9.3 Electric Supply Capacity

As demand on the electricity grid grows from year-to-year, the need to install additional generation capacity to meet this demand also grows. The Electric Supply Capacity application involves using ES to defer and/or to reduce the need to invest in new generation capacity. In a regulated market, a utility may install a marginal amount of ES to meet capacity needs thus deferring the need to invest in a larger conventional generation solution. In a deregulated market, where the electric supply capacity market is evolving, this application could involve selling ES capacity to the market in order to generate a capacity credit revenue stream for a non-utility merchant. However, this market is evolving and in some markets, generation capacity cost is included in wholesale energy prices.

KCP&L Operational Test Plan					
<p>A. Description</p> <p>A 1.0 MWh, 1.0 MW-capable grid-connected Battery Energy Storage System (BESS) will be installed at the Midtown Substation with direct interconnect to a single 13.2 kV circuit, immediately downstream of the substation transformer. DMS based battery control functions will be implemented to discharge the battery during time of peak generation requirements including:</p> <ul style="list-style-type: none"> • Block Discharge Mode for operator defined fixed discharge, and • DERM mode for discharge in response to DR events. 					
<p>B. Expected Results</p> <p>The operational demonstration of the grid connected battery in this application is expected to yield the following:</p> <ul style="list-style-type: none"> • Demonstration controlled operation of battery at time of system peak via operator initiated events and DERM initiated DR events. • Determination of the effective MW peak reduction for a 1MWH battery. We assume 80% of battery capacity will be dischargeable. 					
<p>C. Relevant Impact Metrics</p> <p>The Operational Testing of this application will contribute to these Impact Metrics.</p> <table border="1" data-bbox="256 1306 1365 1381"> <tr> <td>Storage</td> <td>Annual Storage Dispatch (kWh)</td> </tr> <tr> <td>Storage</td> <td>Average Energy Storage Efficiency (%)</td> </tr> </table> <p>At each reporting milestone, operational test, or demonstration period, data will be compared to baseline data to determine a quantified impact. Quantified impacts measured will be reported in semi-annual impact metric reports.</p>		Storage	Annual Storage Dispatch (kWh)	Storage	Average Energy Storage Efficiency (%)
Storage	Annual Storage Dispatch (kWh)				
Storage	Average Energy Storage Efficiency (%)				
<p>D. Benefits Analysis Method/Factors</p> <p>The DOE SGCT will be used to perform the Demonstration Project benefit analysis. For this application the following Smart Grid Function benefits will be quantified.</p> <ul style="list-style-type: none"> • Deferred Generation Capacity Investments <p>Benefits will be calculated using SGCT formulas. The following factors will be measured, projected or calculated during the application operation and/or demonstration.</p> <p>Deferred Generation Capacity Investments</p> <ul style="list-style-type: none"> • Energy Storage Use at Annual Peak Time (MW) 					

Additionally, the DOE ESCT will be used to perform the benefit analysis for a utility owned GES system. The following Stationary Energy Storage applications that will be combined in this analysis.

- Primary Application – Electric Energy Time Shift
- Secondary Application – Electric Supply Capacity
- Secondary Application – T&D Upgrade Deferral

Primary Benefit: Deferred Generation Capacity Investment (Utility/Ratepayer)

- Calculation: [Generation Capacity Deferred (MW) x Capital Cost of Deferred Generation Capacity (\$/MW) x Fixed Charge Rate] + [Yearly Fixed O&M Costs of Deferred Generation Capacity (\$/MW-yr) x Generation Capacity Deferred (MW)]

E. Baseline Data & Control Groups

AMI metering that is deployed for all customers, circuits, and distributed energy resources within the Demonstration Project area. The following usage data will be available for baselines:

- 15 minute interval total load data for the battery circuit.
- 15 minute interval delivered and received load data for the grid battery.

The following system level energy production data will be available for analysis.

- Historical and current hourly average and marginal energy production cost data.
- Historical and current hourly system energy production load profile data.
- Historical weather adjusted system energy production load profile data.

F. Testing Method/Methodology:

The following points provide an overview of how the operational testing for this application will be accomplished:

- Energy delivered and received to the BESS will be measured on the high side of the BESS interconnection transformer through the AMI system deployed as part of the Project. All data collected will be stored in KCP&L's Meter Data Management (MDM) System.
- BESS discharge for electricity supply capacity will be initiated in two ways; 1) the distribution grid operator can manually initiate a scheduled 'Block Mode' discharge, or 2) the DERM can schedule a DR event for the BESS.
- Multiple discharge events will be conducted to evaluate the potential maximum discharge levels that can be sustained for 1, 2, 3, & 4 hour discharge events.

G. Analytical Method/Methodology

The following points provide an overview of how the operational testing for this application will be accomplished:

- AMI interval load data for each BESS discharge for this application will be extracted from the MDM System through KCP&L's Data Mining and Analysis Tool (DMAT) (DataRaker).
- Multiple discharge events will be analyzed to the potential maximum discharge levels that can be sustained for 1, 2, 3, & 4 hour discharge events.
- Historical hourly system energy production load profile data will be analyzed to determine the optimum block discharge level and duration to maximize the BESS impact on capacity reduction.
- Due to other project operational testing requirements, it may not be possible to initiate a battery discharge event at system peak, but we will have determined what the impact would be if the BESS were normally available.

2.4.9.4 T&D Upgrade Deferral

Transmission and Distribution (T&D) Upgrade Deferral application involves installing ES in order to delay transmission and/or distribution system upgrades. The value of this application is derived from the fact that storage can be used to provide enough incremental capacity to defer the need for a large ‘lump’ investment in T&D equipment. If using an energy storage device to defer a T&D investment, proper consideration must be given to reliability. T&D capital investments must maintain the extremely high reliability of the electric delivery system. Therefore, any energy storage solution that defers the need for a T&D investment must similarly maintain the reliability of the system. For energy storage deployments this means ensuring that the storage solution has enough redundancy or modularity such that the effective reliability of the solution is adequate.

KCP&L Operational Test Plan

A. Description

A 1.0 MWh, 1.0 MW-capable grid-connected Battery Energy Storage System (BESS) will be installed at the Midtown Substation with direct interconnect to a single 13.2 kV circuit, immediately downstream of the substation transformer. DMS based control functions will be used to implement load-following discharge of the battery to demonstrate and evaluate the operational benefit of using the battery for electric T&D Upgrade Deferral applications. The operator will be able to select from the following grid level targets for the load-following function:

- Station Power Transformer
- Distribution Substation Bus
- Distribution Circuit

B. Expected Results

The operational demonstration of the grid connected battery in this application is expected to yield the following:

- Demonstrate load following discharge of battery based on real-time transformer, bus, and circuit loadings.
- Using several representative company distribution circuit load profiles, determination a representative distribution circuit peak reduction (kW) that can be achieved for a 1MWH battery.

C. Relevant Impact Metrics

The Operational Testing of this application will contribute to these Impact Metrics.

Storage	Annual Storage Dispatch (kWh)
Storage	Average Energy Storage Efficiency (%)

At each reporting milestone, operational test, or demonstration period, data will be compared to baseline data to determine a quantified impact. Quantified impacts measured will be reported in semi-annual impact metric reports.

D. Benefits Analysis Method/Factors

The DOE SGCT will be used to perform the Demonstration Project benefit analysis. For this application the following Smart Grid Function benefits will be quantified.

- Deferred Generation Capacity Investments
- Deferred Distribution Capacity Investments

Benefits will be calculated using SGCT formulas. The following factors will be measured, projected or calculated during the application operation and/or demonstration.

Deferred Generation Capacity Investments

- Energy Storage Use at Annual Peak Time (MW)

Deferred Distribution Capacity Investments

- Distribution Feeder Load Reduction (MW)

Additionally, the DOE ESCT will be used to perform the benefit analysis for a utility owned GES system. The following Stationary Energy Storage applications that will be combined in this analysis.

- Primary Application – Electric Energy Time Shift
- Secondary Application – Electric Supply Capacity
- Secondary Application – T&D Upgrade Deferral

Primary Benefit: Deferred Distribution Investments (Utility/Ratepayers)

- This yearly deferral amount only accrues between the initial and final year of transmission deferral.
- $[\text{Distribution Capacity Deferred (kVA)} \times \text{Capital Cost of Deferred Distribution Capacity (\$/kVA)} \times \text{Fixed Charge Rate}] + \text{Yearly O\&M Costs of Deferred Dist. Capacity (\$/yr)}$

E. Baseline Data & Control Groups

AMI metering that is deployed for all customers, circuits, and distributed energy resources within the Demonstration Project area. The following usage data will be available for baselines::

- 15 minute interval total load data for each Demonstration Project circuit.
- 15 minute interval delivered and received load data for the grid battery.

The following system level energy production data will be available for analysis.

- Historical and current hourly average and marginal energy production cost data.
- Historical and current hourly system energy production load profile data.
- Historical weather adjusted system energy production load profile data.

The following historical data is available from the company's EMS system.

- Historical substation hourly load profile data.
- Historical distribution circuit hourly load profile data.

F. Testing Method/Methodology:

The following points provide an overview of how the operational testing for this application will be accomplished:

- Energy delivered and received to the BESS will be measured on the high side of the BESS interconnection transformer through the AMI system deployed as part of the Project. All data collected will be stored in KCP&L's Meter Data Management (MDM) System.
- BESS discharge for T & D Upgrade Deferral will be initiated in by the distribution grid operator can manually setting BESS to 'Load Following' Mode in the DMS. The operator will select the load point (station transformer, bus, or circuit) on the grid to follow and the max load level to maintain.
- Multiple load following discharge events will be conducted to evaluate the potential distribution load reduction that can be achieved under various heavy load conditions.

G. Analytical Method/Methodology

The following points provide an overview of how the operational testing for this application will be accomplished:

- AMI interval load data for each BESS discharge for this application will be extracted from the MDM System through KCP&L's Data Mining and Analysis Tool (DMAT) (DataRaker).
- Multiple load following discharge events will be analyzed to evaluate the potential distribution load reduction that can be achieved under various loading conditions.
- Historical load profiles for other KCP&L substations and circuits that are substantially different from the SmartGrid Demonstration Circuits which will be analyzed to identify typical load profiles for which the BESS would have the greatest potential to defer distribution upgrades.
- The level of discharge for T&D Upgrade deferral that is coincident with annual system peak will be determined.

2.4.9.5 Time-of-Use Energy Cost Management

For the Time-of-use (TOU) Energy Cost Management application, energy end users (utility customers) would use ES devices to reduce their overall costs for electricity. They would accomplish this by charging the storage during off-peak periods when the electric energy price is low, then discharge the energy during times when on-peak TOU energy prices apply. This application is similar to Electric Energy Time-shift application, although electric energy savings are based on the customer's retail tariff, whereas the benefit for Electric Energy Time-shift is based on the prevailing wholesale price.

KCP&L Technology Demonstration Plan

A. Description

A consumer premise energy storage system (PESS) will be installed at the SmartGrid Demonstration House in conjunction with the 3.1 kW solar PV array. The will consist of an 11.7 kWh lithium-ion battery with a unique hybrid inverter/converter rated for 6kW discharge.

The premise energy storage system will be configured to demonstrate how the consumer can use the PESS in conjunction with multi-tiered TOU rates to reduce their overall cost for electricity. This will be accomplished by charging the storage during off-peak periods when the electric energy price is low or during time of excess solar PV production, then discharging the energy during times when on-peak TOU energy prices apply.

B. Expected Results

This technical demonstration is expected to yield the following:

- Typical daily charge/discharge load cycles will be developed and demonstrated at the Demonstration House.
- The 'Round Trip Efficiency of the Storage System' factor for the PESS will be determined. The system is expected to operate at greater than 70% efficient with respect to net energy output versus input.
- The 'Total Energy Discharged for TOU Energy' factor for the PESS will be determined. The system is expected to have approximately 10 kwh available daily for TOU discharge.
- The charge/discharge load cycles developed will be mathematically applied to several 'typical' load profiles to illustrate how a PESS system can be used with TOU rates to lower the customers energy cost.

C. Relevant Impact Metrics

The Technical Demonstration of this application will not contribute to any Impact Metrics.

D. Benefits Analysis Method/Factors

The DOE SGCT will be used to perform the Demonstration Project benefit analysis. For this application the following Smart Grid Function benefits will be quantified.

- Deferred Generation Capacity Investments
- Deferred Distribution Capacity Investments
- Reduced Electricity Costs

Benefits will be calculated using SGCT formulas. The following factors will be measured, projected or calculated during the application operation and/or demonstration.

Deferred Generation Capacity Investments (Utility)

- Energy Storage Use at Annual Peak Time (MW)

Deferred Distribution Capacity Investments (Utility)

- Distribution Feeder Load Reduction (MW)

Reduced Electricity Costs (Customer)

- Reduced Total Annual Electric Consumption (kWh) by customer class.

Additionally, the DOE ESCT will be used to perform the benefit analysis for a customer owned PESS system. The following Stationary Energy Storage applications that will be combined in this analysis.

- Primary Application - Time-of-Use Energy Cost Management
- Secondary Application – Renewable Energy Time Shift
- Secondary Application – Electric Service Reliability

Primary Benefit for TOU Energy Cost Management: Reduced Electricity Cost (Consumer)

- Calculation: Total Energy Discharged for TOU Energy x [Avg. On-Peak Retail Price of Electricity (\$/MWh) – Avg. Off-Peak Retail Price of Electricity (\$/MWh) /Storage System Round-trip Efficiency (%)]

Secondary Benefit: Deferred Generation Capacity Investment (Utility)

- A deferred generation investment benefit may result if many end-users take advantage of the TOU Energy Cost Management application since the shifting of energy from peak to off-peak by multiple End Users may allow base-load and intermediate generation capacity to meet peak generation needs.

E. Baseline Data & Control Groups

AMI metering that is deployed for all customers, circuits, and distributed energy resources within the Demonstration Project area. The following usage data will be available for baselines::

- 15 minute interval load data of all customers.
- Average hourly interval load data by customer class.
- 15 minute interval delivered and received load data for each Solar DG site.

F. Demonstration Method/Methodology:

The following points provide an overview of how the technical demonstration of this application will be accomplished:

- Energy delivered and received to the PESS will be measured by the PESS management system.
- A daily charge/discharge cycle will be implemented to demonstrate and evaluate the benefit of using the battery for electric energy time shift in conjunction with TOU rates. Charging will occur daily from 1-5 a.m. and discharge will occur from 3-7 p.m.
- The PESS will be operated in this mode for a minimum of two weeks to determine the Round Trip Efficiency of the Storage System factor.

G. Analytical Method/Methodology

The following points provide an overview of how the operational testing for this application will be accomplished:

- Energy delivered and received to the PESS measured by the PESS management system will be exported to Excel for analysis.
- The Round Trip Efficiency of the Storage System factor will be calculated as (PESS Energy Delivered)/(PESS Energy Received).
- The Reduced Electricity Cost for the consumer will be calculated using the ESCT formula.

2.4.9.6 Electric Service Reliability

The Electric Service Reliability application involves using electric energy storage to ensure highly reliable electric service. In the event of a complete power outage lasting more than a few seconds, the energy storage system provides enough energy to ride through outages of extended duration; complete an orderly shutdown of processes; and/or transition to on-site generation resources.

KCP&L Technology Demonstration Plan**A. Description**

A consumer side 11.7 kWh premise energy storage system (PESS) will be installed at the SmartGrid Demonstration House in conjunction with the 3.1 kW sola PV array. The PESS will consist of a 11.7 kWh lithium-ion battery with a unique hybrid inverter/converter rated for 6kW discharge. The PESS will be configured to provide emergency stand-by power to critical loads during extended power outages.

B. Expected Results

Emergency stand-by power functionality will be demonstrated at the Demonstration House.

C. Relevant Impact Metrics

The Technical Demonstration of this application will not contribute to any Impact Metrics.

D. Benefits Analysis Method/Factors

The DOE SGCT will be used to perform the Demonstration Project benefit analysis. For this application the following Smart Grid Function benefits will be quantified.

- Reduce Sustained Outages

Benefits will be calculated using SGCT formulas. The following factors will be measured, projected or calculated during the application operation and/or demonstration.

Reduce Sustained Outages

- SAIDI (base &proj.)

Additionally, the DOE ESCT will be used to perform a benefit analysis for a customer owned PESS system. The following Stationary Energy Storage applications that will be combined in this analysis.

- Primary Application - Time-of-Use Energy Cost Management
- Secondary Application – Renewable Energy Time Shift
- Secondary Application - Electric Service Reliability

Primary Benefit for Electric Service Reliability: Reduced Outages (Consumer)

- Calculation: $\sum \{ \text{Outage Minutes Avoided by Cust. Class (min)} \times \text{Average Hourly Load Not Served During Outage per Customer by class (kW)} \times \text{VOS by Cust. Class (\$/kWh)} \}$

E. Baseline Data & Control Groups

The following historical system level reliability statistics will be available for analysis:

- System Average Interruption Frequency Index (SAIFI)
- System Average Interruption Duration Index (SAIDI)
- Customer Average Interruption Duration Index (CAIDI)

F. Testing Method/Methodology:

The following points provide an overview of how the technical demonstration of this application will be accomplished:

- A customer critical load panel will be installed and connected to the PESS.
- Load served by the customer critical load panel will be measured by the PESS management system.
- Customer's main breaker will be opened simulating a power outage and the PESS will use its internal battery storage to maintain service to the critical loads panel.
- The PESS will be operated in this mode until the battery is discharged to determine the length of time the critical loads can be sustained from the battery storage alone.

G. Analytical Method/Methodology

The following points provide an overview of how the operational testing for this application will be accomplished:

- Energy delivered to the customer critical load panel will be measured by the PESS management system and will be exported to Excel for analysis.
- The length of time the PESS can sustain power to the customer critical load panel will be measured by the PESS management system.
- The Reduced Outage Benefit to the consumer will be calculated using the ESCT formula.

2.4.9.7 Renewable Energy Time Shift

The Renewables Energy Time-shift application involves storing electricity from renewable sources when the price of electricity is low and selling that stored energy when the price of electricity is higher. Because wind typically produces energy at night when electricity prices are low, the price differential between the electricity used to charge the battery and the electricity sold at peak can be very large. The energy that is discharged from the storage could be sold via the wholesale market, sold under terms of an energy purchase contract, or used by an integrated utility to reduce the overall cost of providing generation during peak times.

KCP&L Technology Demonstration Plan
<p>A. Description</p> <p>A consumer premise energy storage system (PESS) will be installed at the SmartGrid Demonstration House in conjunction with the 3.1 kW solar PV array. The PESS will consist of an 11.7 kWh lithium-ion battery with a unique hybrid inverter/converter rated for 6kW discharge. The PESS will be configured to store solar electric energy generated during peak generation times (11 am – 1 pm) and then discharge the stored energy during times of peak system load (typically 4 – 5 pm).</p>
<p>B. Expected Results</p> <p>This technical demonstration is expected to yield the following:</p> <ul style="list-style-type: none"> • Typical daily charge/discharge load cycles for renewable time shift will be developed and demonstrated at the Demonstration House. • The ‘Energy Discharged for Renewable Energy Time-Shift’ factor for the PESS will be determined. The system is expected to have approximately 10 kWh available daily for discharge. • The charge/discharge load cycles developed will be mathematically applied to several ‘typical’ load profiles to illustrate how a PESS system can be used with TOU rates to lower the customer’s energy cost.
<p>C. Relevant Impact Metrics</p> <p>The Technical Demonstration of this application will not contribute to any Impact Metrics.</p>
<p>D. Benefits Analysis Method/Factors</p> <p>The DOE SGCT will be used to perform the Demonstration Project benefit analysis. For this application the following Smart Grid Function benefits will be quantified.</p> <ul style="list-style-type: none"> • Deferred Generation Capacity Investments • Deferred Distribution Capacity Investments • Reduced Electricity Costs • Reduced CO2 Emissions <p>Benefits will be calculated using SGCT formulas. The following factors will be measured, projected or calculated during the application operation and/or demonstration.</p> <p>Reduced Electricity Costs (Utility)</p> <ul style="list-style-type: none"> • Reduced Total Annual Electric Consumption (kWh) by customer class. <p>Reduced CO2 Emissions</p> <ul style="list-style-type: none"> • Annual Distributed Generation Production (MWH)

Additionally, the DOE ESCT will be used to perform the benefit analysis for a customer owned PESS system. The following Stationary Energy Storage applications that will be combined in this analysis.

- Primary Application - Time-of-Use Energy Cost Management
- Secondary Application – Renewable Energy Time Shift
- Secondary Application – Electric Service Reliability

Primary Benefit for Renewable Energy Time Shift: Reduced Electricity Costs (Consumer)

- Calculation: Total Energy Discharged for Renewable Energy Time-Shift (MWh) x Avg. On-Peak Price of Electricity (\$/MWh)

E. Baseline Data & Control Groups

AMI metering that is deployed for all customers, circuits, and distributed energy resources within the Demonstration Project area. The following usage data will be available for baselines::

- 15 minute interval load data of all customers.
- 15 minute interval delivered and received load data for each Solar DG site.

F. Demonstration Method/Methodology:

The following points provide an overview of how the technical demonstration of this application will be accomplished:

- A customer solar electric generation system will be installed and connected to the PESS.
- Energy generated by the customer's solar electric generation system will be measured by the PESS management system.
- A daily charge/discharge program will be implemented to demonstrate and evaluate the benefit of using the PESS for solar generation time shift in conjunction with TOU rates. Charging will occur daily during off-peak rate times from available solar generation and discharge during on-peak rate times from 3-7 p.m.
- The PESS will be operated with this as its standard mode during multiple seasons.

G. Analytical Method/Methodology

The following points provide an overview of how the operational testing for this application will be accomplished:

- Energy delivered to the PESS by the solar generation system will be measured by the PESS management system and will be exported to Excel for analysis.
- Energy delivered and received by the PESS storage system will be measured by the PESS management system and will be exported to Excel for analysis.
- The customer's Reduced Electricity Cost will be calculated using the ESCT formulas.

2.4.9.8 PEV Charging (VCM)

The batteries in plug-in electric vehicles (PEVs) can be portrayed as non-stationary energy storage devices. As such, they are similar to stationary energy storage devices and support economic, reliability and environmental benefits. By increasing vehicle fuel efficiency, they also support Reduced Oil Usage, an Energy Security Benefit.

KCP&L Technology Demonstration Plan	
A. Description	The ChargePoint Vehicle Charge Management System (VCMS) and a total of ten Electric Vehicle Charging Stations (EVCSs) will be deployed within the Demonstration Project area. Each EVCS consists of a dual port, level 2 (240V) Coulomb Charging Station capable of charging two PEVs simultaneously. The EVCSs will be installed on the EVCS sponsor's side of the meter and the charging will be free to the public. The VCMS will be integrated with the DERM and will serve as the "control authority" for each EVCS during demand response events.
B. Expected Results	This technical demonstration is expected to yield the following: <ul style="list-style-type: none"> • Technical demonstration of 10 public accessible (PEV) charging stations providing PEV owners the convenience of public charging. • The DERM will dispatch DR events to the EVCS demonstrating how PEVs can participate in DR events. • KCP&L will be able to monitor, record, and summarize the charging patterns at each of the EVCS sites.
C. Relevant Impact Metrics	The Technical Demonstration of this application will not contribute to any Impact Metrics.
D. Benefits Analysis Method/Factors	The DOE SGCT will be used to perform the Demonstration Project benefit analysis. For this application the following Smart Grid Function benefits will be quantified. <ul style="list-style-type: none"> • Reduced CO2 Emissions Benefits will be calculated using SGCT formulas. The following factors will be measured, projected or calculated during the application operation and/or demonstration. <p>Reduced CO2 Emissions</p> <ul style="list-style-type: none"> • Annual Electricity Consumed by PEVs (kWh)
E. Baseline Data & Control Groups	The Technical Demonstration of this application does not require any Baseline Data or the establishment of any Control Groups.
F. Demonstration Method/Methodology:	The following points provide an overview of how the technical demonstration of this application will be accomplished: <ul style="list-style-type: none"> • Energy use at each PEV charging station will be measured through PEV Charge Management System and the AMI system deployed as part of the Project. All data collected by the AMI system will be stored in KCP&L's Meter Data Management (MDM) System.
G. Analytical Method/Methodology	The Technical Demonstration of this application does not require any analytical calculations.

2.5 Data Collection and Benefits Analysis

A key objective in KCP&L's SmartGrid Demonstration Project will be to quantify the costs and benefits of each of the solutions separately and as a complete solution. The Demonstration is designed as a regionally unique effort to display the benefits of single initiatives and the overall synergies and interrelations that can occur as a result of building complete programs. In KCP&L's budgeting process, the operating and capital costs of each of the SmartGrid Demonstration sub-projects are defined along with the potential benefits. These benefits include operational, economic, customer and environmental improvements.

The operational demonstration and testing plans, outlined in the previous section, have been developed to not only demonstrate the SmartGrid Functions achievable through end-to-end interoperability, but to also capture and quantify the operational benefits achieved by each of the SmartGrid applications. EPRI and the DOE have developed specific, quantifiable methodologies to translate benefit metrics into potential monetary value. KCP&L will use the DOE-developed metrics reporting and computational tools to evaluate the overall costs and benefits of the demonstrated SmartGrid technologies and functions.

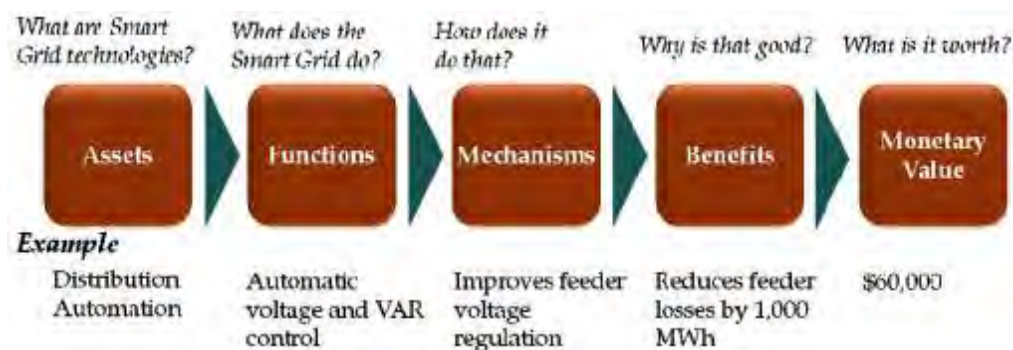
Additionally, where possible, KCP&L will quantify the cost effectiveness of the technology solutions developed for the demonstration vs. existing KCP&L grid automation technologies and solutions to determine the cost effectiveness of the demonstration technologies on a go-forward basis at KCP&L.

2.5.1 SmartGrid Computational Tool (SGCT) Analysis [16]

The DOE has developed a standard methodology and tool for evaluating the performance, costs, and benefits of all Smart Grid field projects including the SGIG and SGD programs. In developing this methodology, the DOE defined a standardized set of Smart Grid assets, functions, and benefits along with guidelines for calculating associated benefits. This methodology and tool allows the costs and benefits of all Smart Grid projects to be evaluated consistently.

The KCP&L Demonstration will use the DOE-developed Smart Grid Computational Tool (SGCT) to evaluate the overall costs and benefits in order to estimate the project's overall value. The SGCT allows the user to identify the assets to be deployed and functions to be demonstrated by the smart grid project and to calculate the costs and benefits in order to estimate the project's overall value. Figure 2-82 illustrates how the SGCT translates Smart Grid Assets into Monetary Value.

Figure 2-82: SGCT Translation of Smart Grid Assets to Monetary Value



Using the SGCT, the Smart Grid Project Team: 1) identified the Smart Grid Assets deployed; 2) identified the Smart Grid functions that the Demonstration would enable; and 3) for each function, identified the applicable benefit mechanisms. Based on these inputs, the SGCT, identified the expected benefits the project could achieve. Table 2-21 identifies the potential Demonstration project benefits by Smart Grid Function.

Table 2-21: SGCT Function-Benefit Chart for KCP&L Demonstration Project

Benefits			Smart Grid Functions										
			Delivery						Use	Other			
			Automated Feeder and Line Switching	Automated Islanding and Reconnection	Automated Voltage and VAR Control	Diagnostics & Application of Equipment Condition	Real-Time Load Allocation & Management	Real-time Load Transfer	Customer Electricity Use Optimization	Storing Electricity for Later Use	Distributed Production of Electricity		
Economic	Improved Asset Utilization	Optimized Generator Operation											
		Deferred Generation Capacity Investments											
		Reduced Ancillary Service Cost											
		Reduced Congestion Cost											
	T&D Capital Savings	Deferred Transmission Capacity Investments											
		Deferred Distribution Capacity Investments											
		Reduced Equipment Failures											
	T&D O&M Savings	Reduced T&D Equipment Maintenance Cost											
		Reduced T&D Operations Cost											
		Reduced Meter Reading Cost											
Theft Reduction	Reduced Electricity Theft												
Energy Efficiency	Reduced Electricity Losses												
Electricity Cost Savings	Reduced Electricity Cost												
Reliability	Power Interruptions	Reduced Sustained Outages											
		Reduced Major Outages											
		Reduced Restoration Cost											
	Power Quality	Reduced Momentary Outages											
		Reduced Sags and Swells											
Environmental	Air Emissions	Reduced CO2 Emissions											
		Reduced SOx, NOx, and PM-2.5 Emissions											
Security	Energy Security	Reduced Oil Usage (not monetized)											
		Reduced Wide-scale Blackouts											

The SGCT uses two different types of data to calculate benefits, baseline data and project data. Baseline data are intended to reflect what the state of the grid would have been during the project period assuming a “no-build” scenario. Project data reflect the actual state of the grid as the smart grid technology is implemented. All benefit assumptions rely on the calculated difference between baseline and project data at a given point in time.

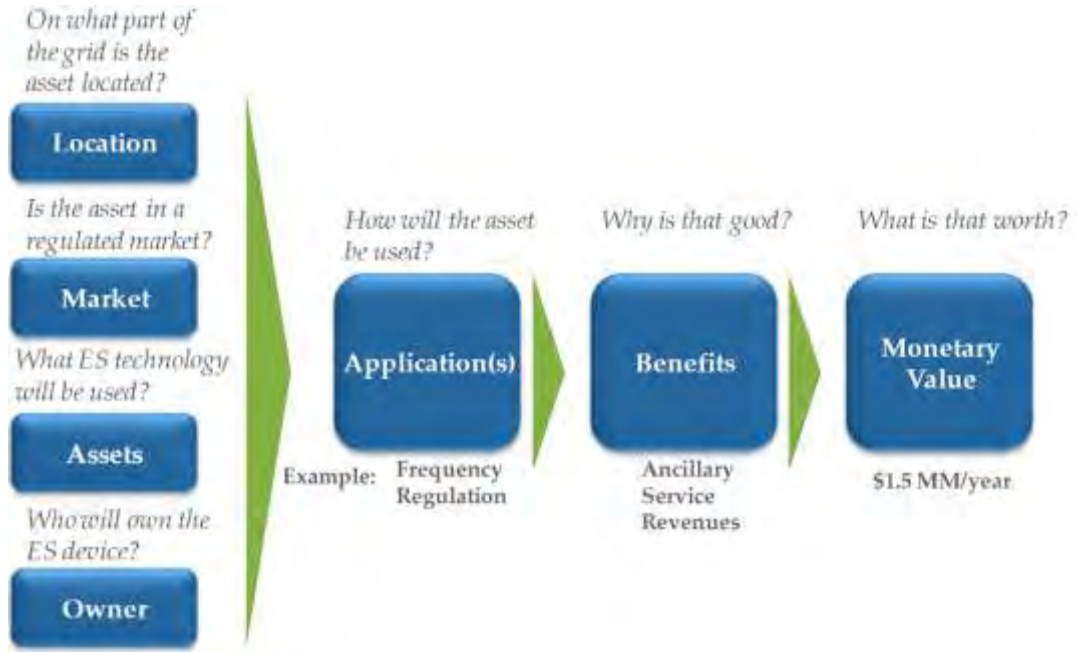
Baseline and project operational data will be gathered in accordance with the Operational Demonstration/Test Plans established for each demonstration application. KCP&L will then report data and impact metrics to the DOE as required. KCP&L will attempt to directly measure the baseline and project metrics required by SGCT. However, due to the number of Smart Grid Applications to be operationally demonstrated and tested, it may prove impractical to directly measure these annualized values. When necessary, shorter duration testing results will be extrapolated to annualized values for SGCT purposes.

2.5.2 Energy Storage Computational Tool (ESCT) Analysis [17]

Building on the methodology developed for evaluating the performance, costs, and benefits of Smart Grid projects, the DOE has developed a standard methodology and tool for evaluating the cost benefit of Energy Storage deployments.

The KCP&L Demonstration will use the DOE-developed Energy Storage Computational Tool (ESCT) to evaluate the overall costs and benefits in order to estimate the project’s overall value. The ESCT allows the user to identify the key characteristics of the energy storage deployment and how the energy storage system will be used. Figure 2-83 illustrates how the ESCT determines the monetary value for energy storage deployments. KCP&L will use the ESCT to perform separate analysis for the utility Bulk Energy Storage System (BESS) and the customer Premise Energy Storage System (PESS).

Figure 2-83: System ESCT Methodology for determining the monetary value of an ES deployment



2.5.2.1 Bulk Energy Storage System Analysis

Using the ESCT, the Smart Grid Project Team input the ES asset information, grid location, market, and ownership for the BESS. Based on these inputs, the ESCT, identified the expected benefits the BESS could achieve. Table 2-22 identifies the expected benefits by Energy Storage Application.

Table 2-22: ESCT Application-Benefit Matrix for KCP&L BESS Analysis

Location	Market	Owner	Application	Utility/Ratepayer						Societal				
				Optimized Generator Operation	Deferred Generation Capacity Investments	Deferred Transmission Investments	Deferred Distribution Investments	Reduced Electricity Losses	Reduced Electricity Cost	Reduced CO2 Emissions	Reduced SOx Emissions	Reduced NOx Emissions	Reduced PM Emissions	
Distribution	Regulated	Utility	Electric Energy Time-shift											
Distribution	Regulated	Utility	Electric Supply Capacity											
Distribution	Regulated	Utility	Transmission & Distribution (T&D) Upgrade Deferral											

BESS operational data will be gathered in accordance with the Operational Demonstration/Test Plans established for each demonstration application. KCP&L will attempt to directly measure the metrics required by ESCT. However, due to the number of Smart Grid Applications to be operationally demonstrated and tested, it may prove impractical to directly measure these annualized values. When necessary, shorter duration testing results will be extrapolated to annualized values for ESCT purposes.

2.5.2.2 Premise Energy Storage System Analysis

Using the ESCT, the Smart Grid Project Team input the ES asset information, grid location, market, and ownership for the PESS. Based on these inputs, the ESCT, identified the expected benefits the PESS could achieve. Table 2-23 identifies the expected benefits by Energy Storage Application.

Table 2-23: ESCT Application-Benefit Matrix for KCP&L PESS analysis

			Utility/Ratepayer					Consumer		Societal			
			Optimized Generator Operation	Deferred Generation Capacity Investments	Deferred Transmission Investments	Deferred Distribution Investments	Reduced Electricity Losses	Reduced Electricity Cost	Reduced Outages	Reduced CO2 Emissions	Reduced SOx Emissions	Reduced NOx Emissions	Reduced PM Emissions
Market	Owner	Application											
Regulated	End-User	Time-of-use (TOU) Energy Cost Management											
Regulated	End-User	Electric Service Reliability											
Regulated	End-User	Renewables Energy Time-shift											

PESS operational data will be gathered in accordance with the Operational Demonstration/Test Plans established for each demonstration application. KCP&L will attempt to directly measure the metrics required by ESCT. However, due to the number of Smart Grid Applications to be operationally demonstrated and tested, it may prove impractical to directly measure these annualized values. When necessary, shorter duration testing results will be extrapolated to annualized values for ESCT purposes.

2.5.3 KCP&L Go-Forward Benefit/Cost Analysis of Demonstration Technologies

KCP&L developed a DRAFT SmartGrid Vision, Architecture, and Road Map discussion document in 2008 as a potential guide to future KCP&L investments in advanced distribution technologies. The document produced was a technology road map focused on the deployment of the advanced distribution technologies needed to implement the SmartGrid functions as described in Title XIII of the Energy Independence and Security Act of 2007 (EISA).

With the passage of the American Recovery and Reinvestment Act of 2009 (ARRA) in February 2009, it became apparent that the SmartGrid deployments outlined in the draft road map may be too aggressive and possibly limiting from a technical point of view. The architecture, on which the plan was developed, was based on prior EPRI IntelliGrid research. It was unclear to what extent the NIST SmartGrid Interoperability Framework initiative funded by ARRA may change KCP&L's future SmartGrid architecture design and technology selections.

With technology architecture uncertainties and the aggressive schedule of the ARRA funded SmartGrid Investment Grants (3 years), KCP&L management decided to focus on pursuing a DOE SmartGrid Demonstration Grant. KCP&L is using its SmartGrid Demonstration project to:

- Define, implement & test a number of advanced distribution technologies and a Smart Grid system architecture based on the evolving NIST Smart Grid Interoperability Framework and Standards.
- Define and document the requirements of the various SmartGrid functions, technologies, and systems for potential future deployment company wide.

- Test, measure, analyze, and document the benefits of the various SmartGrid functions, technologies, systems, and grid operating practices.

The advanced distribution grid technologies being evaluated through KCP&L's SmartGrid Demonstration Project are foundational, enabling technologies that will provide traditional operational benefits to the utility while enabling new demand side management and pricing programs; integration of utility and customer owned distributed generation; greater grid utilization through increased monitoring and control of grid resources; and enhanced utilization of customer demand response capabilities.

Upon completion of the SmartGrid Demonstration Project, KCP&L plans to use the findings of the project to develop a well-founded SmartGrid Vision, Architecture, and Road Map that will provide the framework for evaluating the feasibility and guiding the implementation of SmartGrid technologies and will become an integral component of future IRP analysis and filings.

In developing the SmartGrid Road Map, KCP&L will use the build and impact metrics from the project and other DOE and EPRI SmartGrid demonstration projects to perform a cost/benefit analysis of each of the advanced distribution grid technologies considered for the road map.

KCP&L anticipates that the results of the SmartGrid Demonstration Project and subsequent benefit cost analyses will determine that several of the SmartGrid demonstration technologies will be cost effective, or at a minimum, KCP&L will understand under what conditions they become cost effective.

3 Results

This section will change for each TPR submission, and should document and summarize results from the demonstrated technologies.

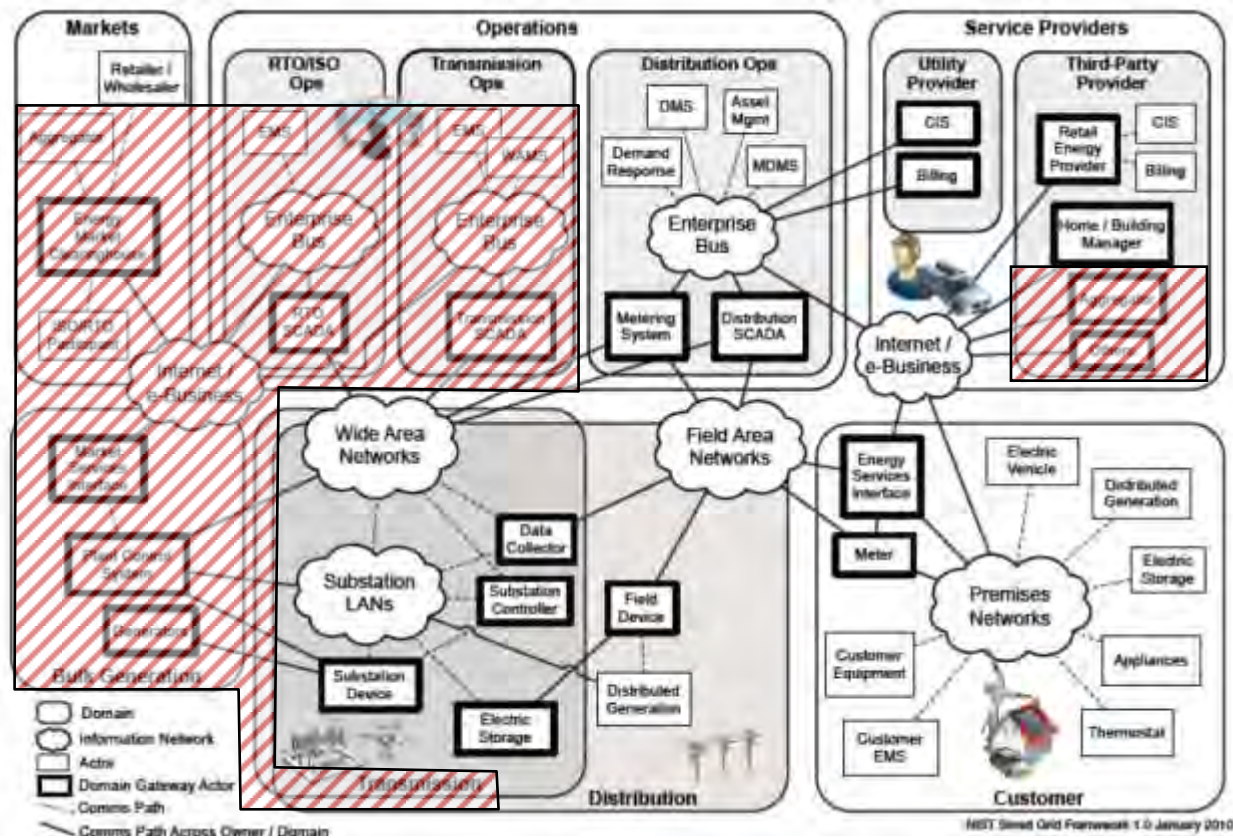
This section should contain the following:

- *Describe the operating performance and associated costs of Smart Grid technologies and systems demonstrated to date (which should align with build metrics reporting) and if it deviated from what was designed or planned during the reporting period (e.g., year) covered by each TPR. Attach the latest build metrics report. (In addition to monetary investments, reporting under build metrics, discuss applicable operating-related costs such as O&M, integration, and cyber security resulting from the demonstration.)*
- *Show results of different DOE Smart Grid Functions tested with respect to desired vs. actual performance, lessons learned, and recommendations for future actions (Table 1).*
- *List items that were to be completed since the last reporting period along with their status.*
- *Identify sources (i.e., what part of system or component) of any issues. List corrective actions taken to return system to 100% operation or data recording. Use clearly labeled graphs to clarify operations.*

3.1 Interoperability [5]

The KCP&L SmartGrid Demonstration Project's main objective is to demonstrate an end-to-end grid management system that involves the integration of ten (10) new systems/sub-systems, from six (6) project vendor partners, and seven (7) legacy KCP&L systems. Figure 3-6 illustrates the scope of the project demonstration integration relative to the NIST Logical Interface Reference Model. To meet the integration challenges associated with ensuring interoperability across the SmartGrid Demonstration Project KCP&L used a structured methodology highlighted in Section 2.1.1. The following sections provide the integration and interoperability design results from the application of this methodology.

Figure 3-1: KCP&L Project vs. NIST SmartGrid Logical Interface Reference Model



3.1.1 Integration Requirement Planning

The KCP&L SmartGrid Demonstration Project demonstrates an end-to-end grid management system that involves the integration of ten (10) new systems/sub-systems and seven (7) legacy KCP&L systems. With this large of an integration project the development of a common project understanding between all project participants was essential to project success.

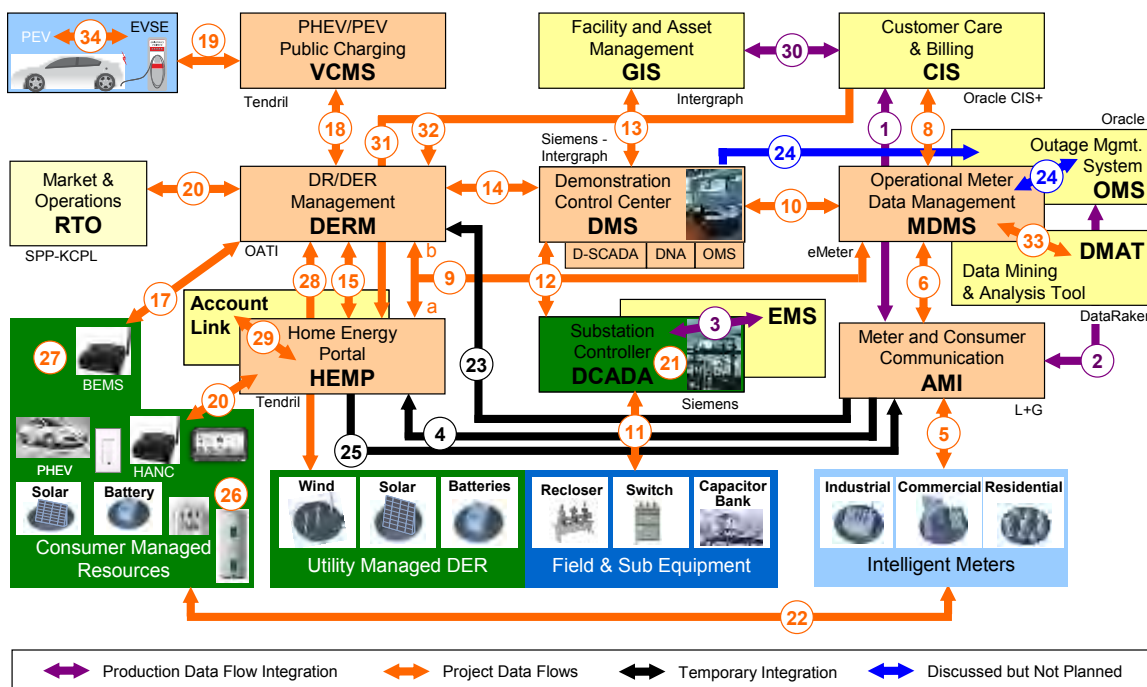
To reach this common understanding KCP&L initiated a series of conceptual design workshops and work efforts beginning in November 2009. Each workshop was facilitated by KCP&L and was attended by subject matter experts from each vendor partner, KCP&L enterprise architects, KCP&L SmartGrid project resources, and KCP&L subject matter experts. Approximately thirty (30) KCP&L employees and twenty (20) vendor partner participants were involved in the workshops.

The objectives of these initial efforts were to:

- Gain a high level understanding of role and functions of each of the new systems/sub-systems
- Establish an understanding of the functionality that the integrated solution is to demonstrate
- Identify and resolve any functionality gaps and overlaps in vendor products and the proposed integration
- Identify and characterize the nature of each of the major project integration points

Through these initial project scoping efforts, thirty-three (33) potentially significant integration points were identified and characterized. These interfaces are illustrated in Figure 3-7.

Figure 3-2: KCP&L SmartGrid Demonstration Systems Interfaces



3.1.2 Integration and Interoperability Requirement Definition

Use cases identify detailed workflows and the corresponding functional requirements for the KCP&L SmartGrid Demonstration Project implementation. Additionally, these use cases identify the data exchange points between the SmartGrid systems and devices using a Common Information Model (CIM) design, which allows the systems to exchange information independent of the manufacturer or vendor. This is important as utilities seek to actively deploy systems and devices from multiple manufacturers.

3.1.2.1 EPRI-Assisted Use Cases

As a member of EPRI’s five-year smart grid demonstration project, our demonstration system integration and interoperability requirements definition and design were supported through EPRI’s formalized smart grid demonstration project. We leveraged EPRI’s IntelliGridSM [1] methodology to define the technical foundation for the project that links electricity with communications and computer control systems to achieve gains in reliability, capacity, and customer services.

The IntelliGrid process is a structured methodology for identifying requirements based on business use cases. The IntelliGrid methodology is an open-standards, requirements-based approach for integrating data networks and equipment that enables interoperability between products and systems. This methodology provides tools and recommendations for standards and technologies when implementing systems such as advanced metering, distribution automation, and demand response and also provides an independent, unbiased approach for testing technologies and vendor products.

KCP&L and EPRI launched the formal IntelliGridSM methodology Use Case process for the project on August 12, 2010. EPRI assisted the KCP&L project team in applying the IntelliGridSM methodology to develop an initial set of four use cases:

1. First-Responder Applications—Distributed Control and Data Acquisition (DCADA) identifies feeder overload conditions and responds accordingly
2. Distributed Hierarchical Monitoring and Control—Interface between the Distribution Management System (DMS) and DCADA Integration
3. Distributed Energy Resource Management System (DERMS)—DMS to DERMS Integration
4. Customer Demand Response

3.1.2.2 KCP&L-Developed Use Cases

The KCP&L SmartGrid Demonstration Project has continued to develop use cases to define the integration requirements for the entire project. In total, more than 90 use cases have been developed to cover the entire breadth of the KCSG demonstration project. The use cases have been organized into the following groupings:

- Network Communications
- Automated Meter Information
- Meter Data Management
- Home Area Network Administration
- SmartEnd-Use
- Demand Response Management (DRM)
- Distribution Substation Automation
- First Responder
- DMS—SmartDistribution
- Pluggable Electric Vehicle Charging

The KCP&L SmartGrid Demonstration Project team has identified the Use Cases listed in Table 3-1 as the basis for defining project interoperability requirements and test plans. A summary description of each Use Cases is presented in Appendix B. As the Use Cases are fully developed and documented, they will be revised in future updates to this Technology Performance Report.

Table 3-1: SmartGrid Demonstration Project Use Cases

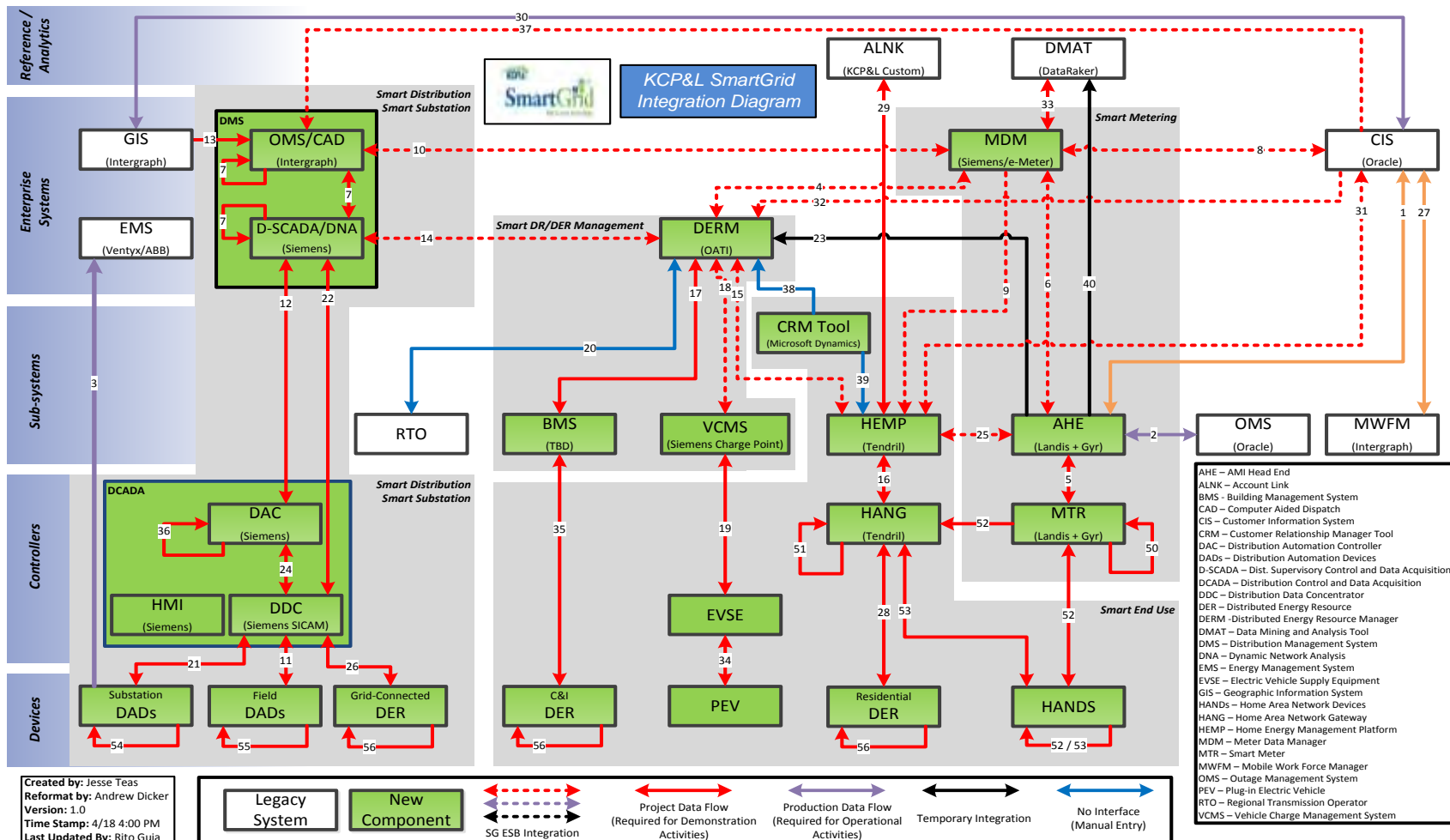
ID	Use Case Title
AMI-01	Customer Requested Remote Service Order Completion
AMI-02	On Demand Meter Read
AMI-03	On-Demand Meter Status Check
AMI-04	Automated Daily Meter Read
AMI-05	SmartMeter Alarm Events
AMI-06	SmartMeter Advisory Events
AMI-07	SmartMeter Log Only Events
AMI-08	SmartMeter Source Power Events
AMI-09	FAN Device Alarm Events
AMI-10	FAN Device Advisory Events
AMI-11	FAN Device Log Only Events
AMI-12	Remote SmartMeter Update
AMI-13	Field SmartMeter Update
AMI-14	Remote FAN Device Update
AMI-15	Field FAN Device Update
AMI-16	Remote Service Order Completion
AMI-17	SmartMeter Replaced by Field Crew
SUB-01	DCADA Monitors and Controls Substation Devices
SUB-02	DCADA Monitors and Controls Field Devices
SUB-03	Substation Transformer Dissolved Gas Analysis and Thermal Monitoring
SUB-04	Substation Transformer Dynamic Ratings
SUB-05	Feeder Cable Dynamic Ratings
1ST-01	DCADA Performs Fault Detection, Location, Isolation, and Restoration
1ST-02	DCADA Performs Volt/VAR Management
1ST-03	DCADA Performs Dynamic Voltage Reduction for Demand Response
1ST-04	DCADA Performs Localized Load Transfer due to Overload
1ST-05	DCADA Initiates Relay Protection Re-coordination (RPR)
DMS-01	DMS Network Model Maintenance
DMS-02	DMS Monitors and Controls Substation Devices
DMS-03	DMS Monitors and Controls Field Devices
DMS-04	DMS Processes Protective Device Alarms
DMS-05	DMS Performs Emergency Load Transfer
DMS-06	DMS Schedules Required Load Transfer
DMS-07	DMS Manages Scheduled Events for Grid-Connected DER
DMS-08	DMS Operator Returns Grid to NORMAL Configuration
DMS-09	DMS Performs Fault Detection, Location, Isolation, and Restoration
DMS-10	DMS Performs Volt/VAR Management
DMS-11	DMS Performs Dynamic Voltage Reduction for Demand Response
DMS-12	DMS Initiates Relay Protection Re-coordination
DRM-01	DR/DER Resource/Asset is Registered in DERM
DRM-02	DERM Manages DR/DER Resource Availability
DRM-03	DERM Distributes DR/DER Event Schedule to Resource/Asset to Control Authority
DRM-04	DMS Manages Grid-Connected DER Event Messages
DRM-05	Home Energy Management Portal Manages DR Event Messages
DRM-06	VCMS Manages DR Event Messages
DRM-07	Customer Opts Out of DR Events

ID	Use Case Title
DRM-08	Verification of DR/DER Event Participation
DRM-09	DERM Creates DR/DER Event for Bulk Power Systems
DRM-10	DERM Generates Retail Pricing Signals
DRM-11	DERM Distributes Demand Response Information Messages
SEU-01	Customer Views Historical Energy Information via Home Energy Management Platform
SEU-02	Customer In-Home Display – Basic Functions
SEU-03	Customer In-Home Display – Daily Bill True-Up
SEU-04	Customer Registers HAN Gateway to Home Energy Management Platform
SEU-05	Customer Uses HEMP to Provision HAN Device to HAN Gateway
SEU-06	Customer Programmable Communicating Thermostat Management
SEU-07	Customer Load Control Switch Management
SEU-08	Customer Initiates De-Provisioning of Customer HAN Device
SEU-09	Customer In-Home Display – Prepayment
SEU-10	Customer Registers for DSM Rates and Programs
SEU-11	Customer Configures HAN Device Settings via HEMP
SEU-12	Customer Configures HEMP with Energy Usage Preferences
SEU-13	HEMP Responds to Energy Signals
SEU-14	HEMP Manages Customer PEV Charging
HAN-01	Utility Commissions Home Area Network
HAN-02	Utility Provisions HAN Device to SmartMeter
HAN-03	Utility Sends Text Message to HAN Device
HAN-04	Utility Cancels Text Message
HAN-05	Utility Sends Pricing Signals to SmartMeter and HAN Devices
HAN-06	Utility Home Area Network Device Information
HAN-07	Utility De-Provisions HAN Device on Utility Home Area Network
HAN-08	Utility De-Commissions Utility Home Area Network
HAN-09	HAN Device Vendor Change Control
HAN-10	HAN Device Status Check
PEV-01	PEV Charging at a Public Charge Station
PEV-02	Customer Enrolls in Utility PEV Program
PEV-03	Customer Registers PEV to Home Premise
PEV-04	Customer PEV Charging at Home Premise
PEV-05	Un-Registered PEV Charging at Premise EVSI
PEV-06	Charge Validation and Settlement via Clearinghouse
PEV-07	Utility Controls PEV Charging at Public Charge Station
PEV-08	Utility Controls Customer On-Premise PEV Charging
MDM-01	MDM Distributes Daily Customer Updates
MDM-02	MDM Distributes Daily Meter Data
MDM-03	MDM Creates Billing Determinants
MDM-04	SmartMeter Inventory Management
NWK-01	Field Automation Network for Advanced Metering Infrastructure
NWK-02	Field Automation Network for Distribution Automation
NWK-03	Utility Home Area Network
NWK-04	Customer Home Area Network
NWK-05	PEV Charge Network
NWK-06	Substation Distribution Automation Network
NWK-07	Substation Distribution Protection Network

3.1.2.3 Project Integration/Interface Points

Through the use case requirement definition efforts, the SmartGrid Project Team identified additional integration/Interface points. These interfaces are illustrated graphically in Figure 3-8. Appendix C provides initial design characterizations for each of the identified interfaces.

Figure 3-3: KCP&L SmartGrid Systems Integration



3.1.3 SmartGrid Application Integration Architecture Design

One of the objectives of the project is to demonstrate end-to-end interoperability using the NIST SmartGrid Framework architecture. As Illustrated in Figure 3-1 and Figure 3-3, the KCP&L SmartGrid Demonstration Project integration architecture design is closely aligned with the NIST Framework and Roadmap for Smart Grid Interoperability Standards. The following subsections provide an overview of the integration architecture being implemented.

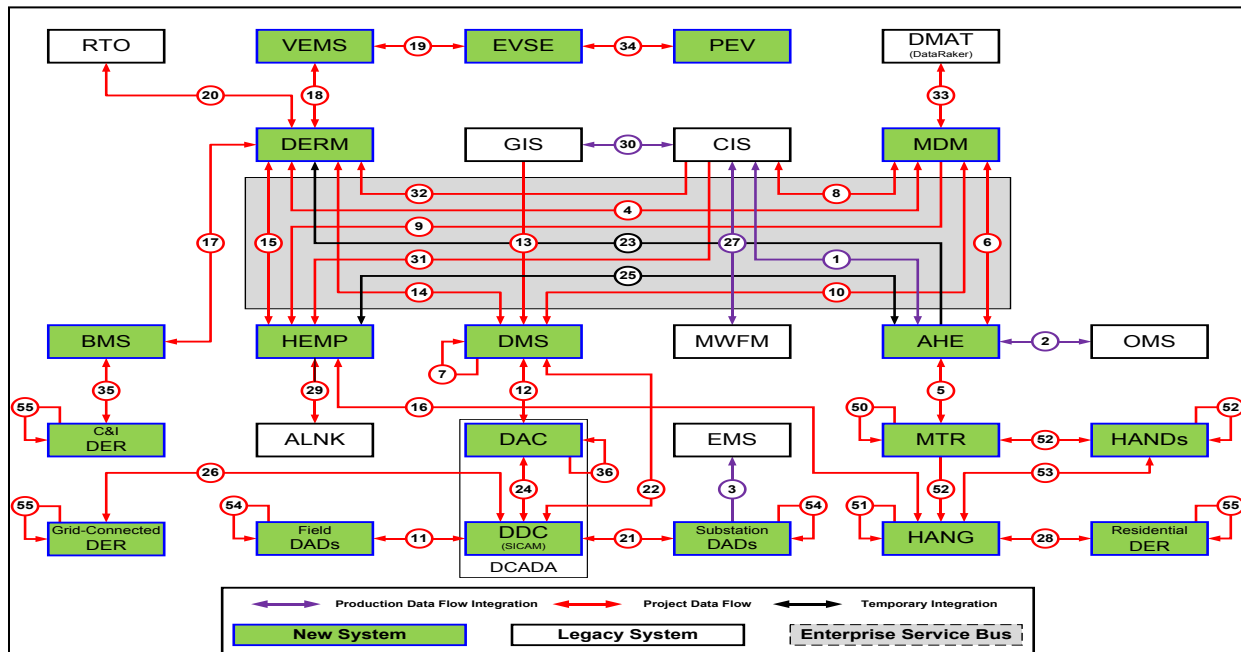
3.1.3.1 SmartGrid Enterprise Service Bus Framework

An Enterprise Service Bus (ESB) refers to a software architecture construct. This construct is typically implemented by technologies found in a category of middleware infrastructure products, usually based on recognized standards, which provide foundational services for more complex architectures via an event-driven and standards-based messaging engine (the bus).

The IEC 61968 series of standards is intended to support the inter-application integration of a utility enterprise that needs to connect disparate applications that are already built or new (legacy or purchased applications), each supported by dissimilar runtime environments. Therefore, these interface standards are relevant to loosely coupled applications with more heterogeneity in languages, operating systems, protocols, and management tools. This series of standards – which are intended to be implemented with middleware services that exchange messages among applications – support applications that need to exchange data every few seconds, minutes, or hours rather than waiting for a nightly batch run. They will complement—not replace—utility data warehouses, database gateways, and operational stores.

Figure 3-4, the KCP&L SmartGrid Master Interface Diagram, introduces the Enterprise Service Bus (ESB) and identifies the interfaces that should be considered for implementation with the ESB instead of point-to-point interfaces.

Figure 3-4: KCP&L SmartGrid Master Interface Diagram

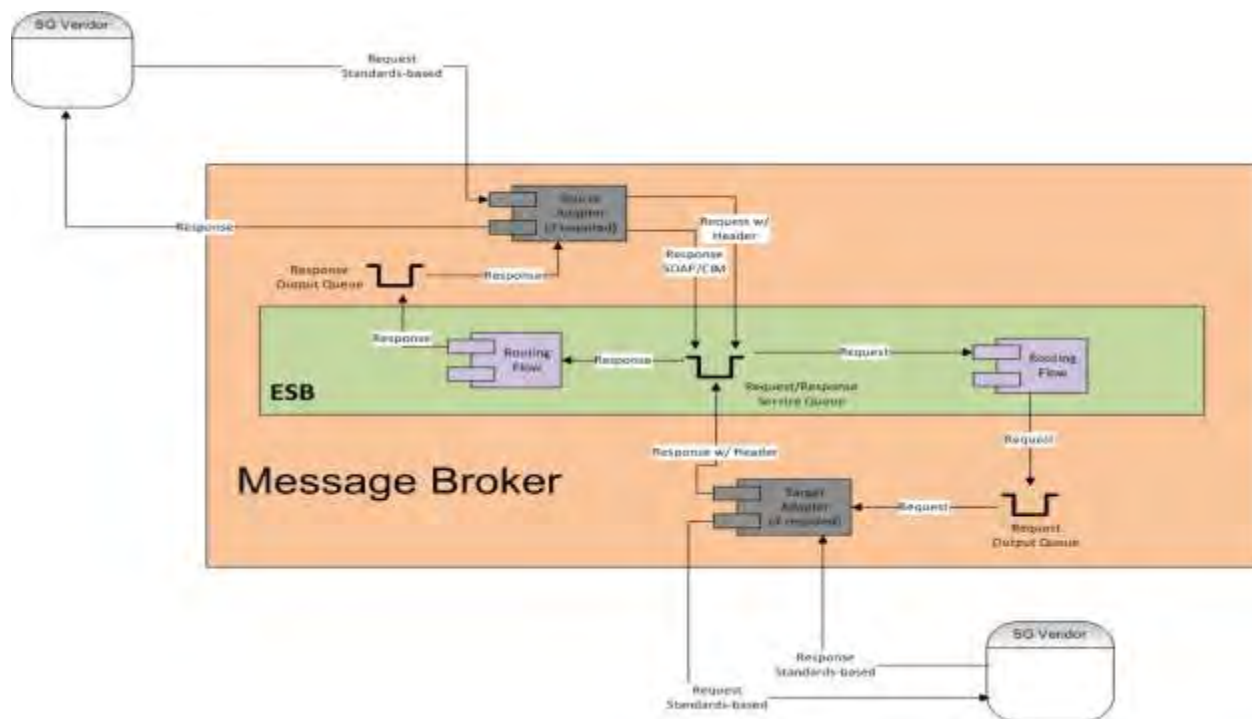


As KCP&L does not currently utilize an enterprise service bus (ESB) in its legacy architecture, the project is leveraging prior EPRI work [15] in developing the project's ESB framework to implement the SmartGrid system to system integration depicted in Figure 3-3 and Figure 3-4. The ESB framework will define how the message payloads will be conveyed using Web Services and the Java Message Service (JMS).

The Enterprise Service Bus (ESB) implemented for the SmartGrid Demonstration Project as illustrated in Figure 3-5 has been based on the following constructs:

- The SmartGrid ESB will utilize the existing KCP&L IBM Websphere MQ and IBM Websphere Message Broker as messaging platform and communication backbone
- The SmartGrid ESB will manage all routing flows and transport requirements using IBM Websphere MQ
- The SmartGrid ESB will implement a series of application adapters using IBM Websphere Message Broker
- The application adapters will manage any message translation, transformation, and/or any mediation required
- Any/all exchange of information between SmartGrid vendor partners must be routed and transported through KCP&L's network and SmartGrid ESB, where appropriate
- All SmartGrid vendor application must communicate to the SmartGrid ESB application adapters using Web Services, JMS, or MQ messaging
- Auditing capabilities will be implemented to log the state of the message as it flows through the ESB

Figure 3-5: KCP&L SmartGrid ESB Framework Example



3.1.4 Interoperability Standards

The development of the SmartGrid Demonstration Project Transmission & Distribution infrastructure involves many standards and numerous levels of integration. One of the objectives of the project is to demonstrate end-to-end interoperability using the following NIST SmartGrid Framework identified interoperability standards. The following subsections list the standards that have been incorporated into the project.

3.1.4.1 Back-Office Systems Integration Standards

- International Electrotechnical Commission (IEC) 61968-1 for general systems- and application-level interface architecture
- IEC 61968-3/61970 for application-level interfaces between the DERMS and DMS
- IEC 60870-6/TASE.2 (Inter-Control Center Communications Protocol, ICCP) for real-time internal DMS communications
- IEC 61968-9 for application-level interfaces with the AMI, Meter Data Management System (MDMS), Customer Information System (CIS), and DMS
- OpenADR 2.0 for demand response (DR) interfaces between DERMS and DR control authorities: Home Energy Management Portal (HEMP), DMS, Building Energy Management System (B-EMS) and Vehicle Control Management System (VCMS)

3.1.4.2 Field Device Communication Standards

- IEC 61850 for substation automation and communication with distributed resources
- IEC 61850 for communication to distributed automation (DA) devices over the Field Area Network (FAN) (when available)
- Distributed Network Protocol (DNP) 3.0/Internet Protocol (IP) for communication to DA devices over the FAN

3.1.4.3 In-Home Communication Standards

- OpenHAN for Home Area Network (HAN) device communication, measurement, and control architecture
- ZigBee for meter-based utility-managed HAN (UHAN) devices
- ZigBee and WIFI for customer-managed HAN (CHAN) devices
- Smart Energy Profile 1.x for UHAN communications
- Smart Energy Profile 2.x for CHAN communications

3.2 Cyber Security

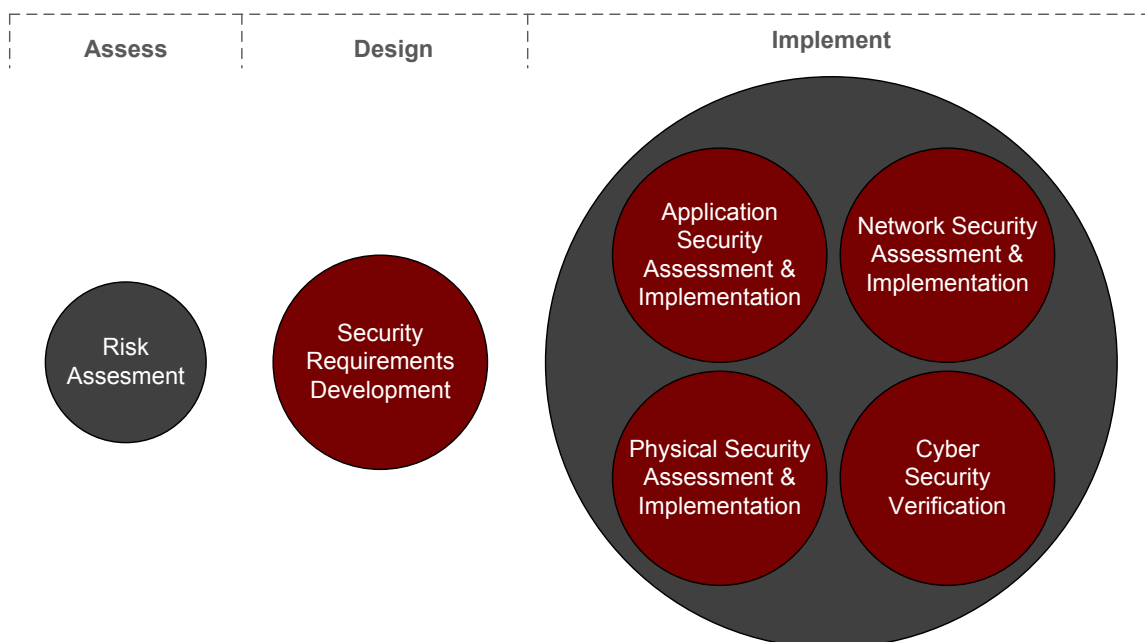
KCP&L chose to conduct a comprehensive risk assessment of all the systems within their Smart Grid Demonstration Project (SGDP). KCP&L made this decision to meet the requirements set forth in both their SmartGrid Cyber Security Plan [11] and the U.S. Department of Energy (DOE) Smart Grid Demonstration funding announcement [16] that states implementing sound cyber security controls for all Smart Grid systems.

To follow the KCP&L SmartGrid Cyber Security Plan, the risk assessment performed for the project was primarily based on the guidelines provided in the National Institute of Standards and Technology (NIST) in their Special Publication 800-30 – Guide for Conducting Risk Assessments (NIST SP 800-30) [12]. The NIST Interagency Report 7628 Volumes I-III (NISTIR-7628) [13] and the UCA [17] International Users Group’s Advanced Metering Infrastructure and Distribution Management (UCAIug AMI and UCAIug DM) Security Profiles were also used to conduct the analysis and provide cyber security suggestions for the KCP&L project.

KCP&L chose to focus on and address several areas of cyber security threats in the implementation of its SGDP. The focused cyber security threat areas included (but were not limited to): autonomous systems and malicious code, external attack, insider abuse and unauthorized acts, insider attack, legal and administrative actions, physical intrusion and/or theft and violent acts of man.

KCP&L developed and is in process of executing an effective cyber security plan tailored to identify, assess, and mitigate threats, risks, and vulnerabilities related to KCP&L’s SmartGrid implementation. The cyber security plan focused on three execution areas (see Figure 3-6). The first execution focus area (Assess) comprised of conducting a risk assessment of the KCP&L SGDP applications. The second focus area (Design) included creation and distribution of security requirements based on the risk assessment results to both KCP&L and vendor application developers. The third focus area (Implement) included four parallel sub-focus areas (Application Security Assessment & Implementation, Physical Security Assessment & Implementation, Network Security Assessment & Implementation, and Cyber Security Verification).

Figure 3-6: Cyber Security Plan Execution Focus Areas



3.2.1 Risk Assessment [18]

A complete risk assessment based on the NIST SP 800-30 was performed for twenty-one Smart Grid applications. The risk assessment results provided:

- Impact-based classifications for all Smart Grid applications
- Risk ratings for all Smart Grid applications
- Approaches for developing security requirements

Separate methodologies were developed to calculate the values of the risk rating model components: threat, vulnerability, likelihood, impact, and mitigation. Each methodology was applied uniformly to all systems to determine values of the components. The following subsections provide an overview of the risk assessment methodology and results. For more information, please see Appendix M for the risk assessment document in its entirety.

3.2.1.1 Scope of Assessment

As a prerequisite to the risk assessment, all systems within the KCP&L SmartGrid portfolio were identified along with their respective interfaces. This step formed the boundaries of the scope and created a foundation for the assessment. The resultant scope of the risk assessment was identified to include the Smart Grid systems listed in Table 3-2.

For the systems that were included in the scope, several methods were used to develop a deeper understanding of KCP&L's implementation of Smart Grid technologies. These methods included the review of system documents such as use cases, interface diagrams, and vendor software specifications. In addition, focus group interviews with the Subject Matter Experts (SMEs) were performed using a set of targeted questions. The result was a grouping of Smart Grid systems into several business function domains that were later used as one of the criteria to recommend the creation of security zones. The collaborative work with the SMEs also resulted in the classification of all system interfaces into one of the NIST-specified logical interface categories. This classification was later used to determine the security controls that will be required to secure the systems.

Table 3-2: Smart Grid Systems Included in the KCP&L Risk Assessment

Smart Grid Systems included in the Risk Assessment	Commonly Referred as:
Advanced Metering Infrastructure Head-End	AHE
AccountLink	ALNK
Building Management System	BMS
Customer Information System	CIS
Distributed Control and Data Acquisition	DCADA
Distributed Energy Resources – Commercial & Industrial	DER – C&I
Distributed Energy Resources – Grid-Connected	DER – Grid-Connected
Distributed Energy Resources Management System	DERM
Distributed Energy Resources – Residential	DER – Residential
Data Mining and Analysis Tool	DMAT
Distribution Management System	DMS
Energy Management System	EMS
Field Distribution Automation Devices	Field DADs
Geographic Information System	GIS
Home Area Network Devices	HANDs
Home Area Network Gateway	HANG
Home Energy Management Platform	HEMP
Meter Data Management System	MDM
SmartMeter	MTR
Substation Distribution Automation Devices	Substation DADs

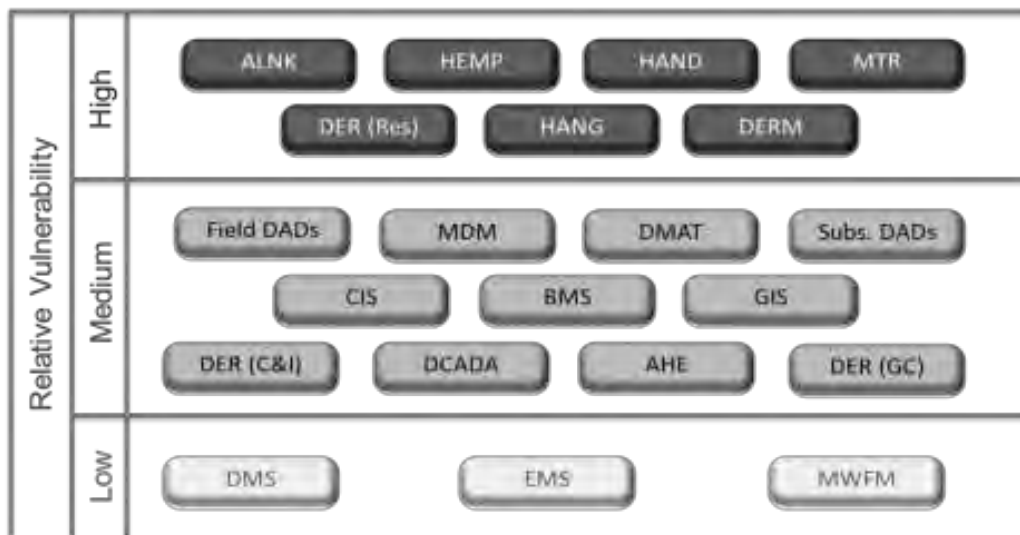
3.2.1.2 Risk Quantification

In order to assess the value of the threat component in the risk model, several internal and external threat sources were identified. The assessment not only included threat sources with an intention to harm the organization but also those resulting from unintentional acts and natural occurrences. Once the threat sources were identified, a list of motivations and possible threat actions taken by each threat source was produced. The value of the threat component for each system was determined by evaluating whether each threat source could impact the system. This value for each system thus equated to the number of threat sources identified to pose a risk to that system.

Vulnerability is defined as the susceptibility of a system to attacks. In the risk assessment, systems were evaluated for the broad categories of system vulnerabilities and operational vulnerabilities. System vulnerabilities directly affect one of the three cyber security goals of confidentiality, integrity, and availability. Operational vulnerabilities are further categorized into people, policy and procedural vulnerabilities. To provide a numerical value to the vulnerability of a system, an approach was used to quantify two of the fundamental reasons that make a system vulnerable. The resulting two variables were the relative technical ease of coordinating an attack and the relative ease of access to parts of the system.

A summary of the relative vulnerability ratings of the Smart Grid systems is graphically represented in Figure 3-7, where each system is placed in either the Low, Medium, or High region.

Figure 3-7: Graphical Representation of Relative Vulnerability Ratings



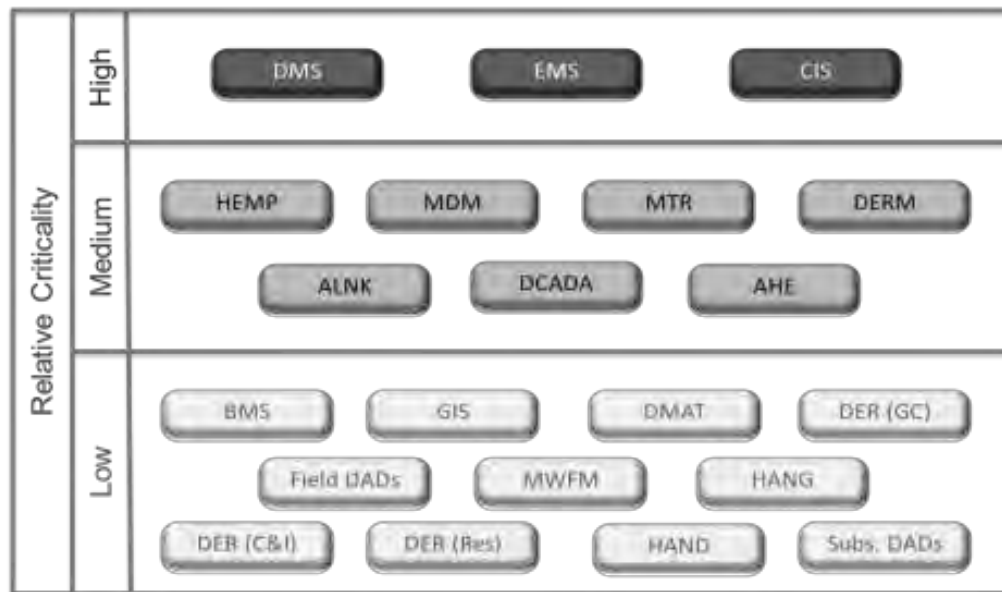
Several measurement criteria were used to assess the likelihood of an attack. These criteria included the evaluation of a potential threat source's motivation and capabilities as well as the nature and frequency of existing vulnerabilities. In the risk assessment, this component did not represent the likelihood of a successful attack, but merely the likelihood of an attack. Similar to the other risk model components, a rating methodology was developed to assign a value for likelihood to all systems. Each threat source was applied to each system and its likelihood of an attack was given a rating. The highest assigned likelihood rating of among the threat sources for a system was then used as that system's overall likelihood rating.

Impact (also referred to as criticality) can be defined as the effect or influence a successful attack may have on a system and/or the organization. Examples of impact include significant monetary damage, compromised consumer privacy, loss of important business operations for long periods of time, national-level damage to company reputation, and years of litigation. For the risk rating model, a

quantifying approach was developed to estimate the effects that a cyber-compromise of confidentiality, integrity, and/or availability would have on the system and the organization. The confidentiality impact was judged based on the qualitative assessment of the sensitivity of the system’s data and the effects of a data leak event. The integrity impact was assessed in terms of the cost of fixing a data integrity issue. Lastly, the availability impact was evaluated by considering the cost of lost productivity, lost opportunity, lost business image, or increased business cost caused if each system became unavailable for a certain length of time.

A summary of the relative criticality ratings of the Smart Grid systems is graphically represented in Figure 3-8, where each system is placed in the Low, Medium, or High region.

Figure 3-8: Graphical Representation of Relative Criticality Results



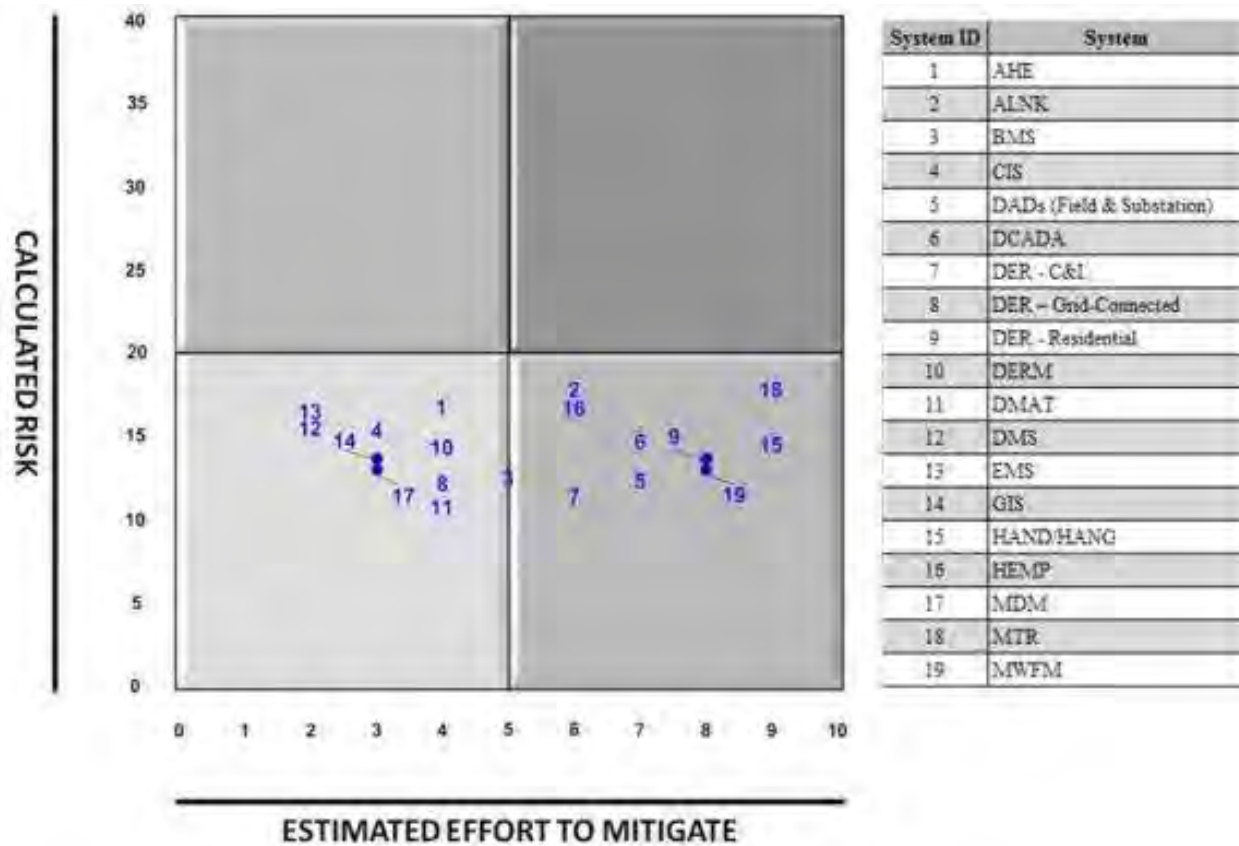
Mitigations are defined as risk reducing efforts or controls commissioned to protect a system’s vulnerabilities or diminish the impact or likelihood of an attack on a system. To assess the value of the mitigation component, first the cyber controls suggested in the NISTIR-7628 and the UCAIug AMI and DM Security Profiles were studied for their applicability to the KCP&L SmartGrid systems. Once the applicable sets of controls were identified, they were matched with the security controls mandated in KCP&L policies, standards, and processes. A methodology was created to quantify the existing mitigations so that it can be used in the risk rating model. The methodology was based on the assumption that all requirements stated in KCP&L policies, standards, and processes are enforced on all existing and new systems at KCP&L.

The primary purpose for the risk assessment was to identify the risk level of each Smart Grid system so that KCP&L can strategize its efforts towards securing the project as a whole. The prioritization task becomes less complex with a risk rating available for each system. The final risk rating for each system was calculated using the model:

$$Risk = Threat + Vulnerability + Likelihood + Impact - Mitigation$$

Once the risk ratings were calculated, the systems were plotted against an estimate of the effort required to further mitigate the systems’ vulnerabilities, likelihoods, and impacts. Figure 3-9 shows the systems plotted against the calculated overall risk rating and estimated effort to mitigate.

Figure 3-9: Risk Rating Categories



There is not, nor should there be, an “ideal” level of risk or a static “target” level of risk at which to aim. These calculated risk ratings should be used to prioritize efforts to reduce overall system risk. Risk may be reduced by mitigations and controls applied at the policy, network, or system level.

3.2.1.3 Risk Assessment Recommendations

There were ten major recommendations given in the risk assessment report. Some were technical in nature, such as assessing and implementing recommended security controls, or designing and implementing recommended network security zones. Others were more policy- and process-based, such as updating policies and documenting mitigation activities. The following list is an overview of the ten major recommendations:

- Implement the provided sets of security controls in a phased approach
- Implement the recommended conceptual security zones using network design techniques
- Create an implementation plan that covers the recommended security controls and security zones
- Update the KCP&L SmartGrid Cyber Security Plan to maintain focus on security and to meet DOE expectations
- Create security requirements for all systems to convert the security controls from concept to implementation
- Develop minimum security requirements for any Smart Grid system externally hosted by a third-party

- Update KCP&L policies, standards, and/or processes to include protection of Smart Grid systems based upon the provided set of procedural controls
- Create and execute test cases to verify the placement and functionality of the security controls
- Perform periodic security assessments to identify and mitigate new risks
- Participate in working groups to learn and create best practices and standards for securing the grid

3.2.2 Risk Mitigation

The completion of the risk assessment resulted in a set of actionable mitigation steps that can be taken by KCP&L to make its Smart Grid systems secure. The KCP&L SmartGrid Trust Model [11] was also used as an important reference while creating these mitigation recommendations. The KCP&L Trust Model domains (Secured, Restricted, Controlled, and Uncontrolled) were used to develop recommended security zones for KCP&L SmartGrid systems and to determine the security controls for data stored and/or generated by the systems. The trust model transport classes (Trusted, Managed, and Public) were used to determine the security controls for data transmitted between systems.

The mitigation recommendations resulting from the risk assessment fell into one of the following two types of security control implementations: creation of security zones and implementation of tailored control sets or implementation of industry-suggested control sets. Detailed descriptions of both security control implementations are covered in the following subsections.

3.2.2.1 Creation of Security Zones and Implementation of Tailored Control Sets

This type of security control implementation includes a collection of security controls specifically tailored for the Smart Grid project based upon security zones and interfaces between security zones. Each security zone includes Smart Grid systems that have the same criticality level and perform similar business functions. The goal of this implementation is to incorporate controls that will bring high risk systems down to a medium risk level and adequately protect the systems based on their impact levels. As such, the selection of controls in this type of implementation is also based on the risk and impact ratings calculated for each system as part of the end-to-end risk assessment.

Figure 3-10 provides a graphical view of the recommended security zones for the KCP&L SGDP.

Second, security control sets are created that tailor to the security zones and interfaces between them. Each control set is a collection of security requirements from the NISTIR-7628 Volume-I as well as many of the ones included in the UCAIug [17] AMI and DM Security Profiles. Figure 3-11 provides a visual representation of the control sets applicable to each security zone and its interfaces.

Figure 3-10: Representation of Smart Grid Applications in Respective Security Zones

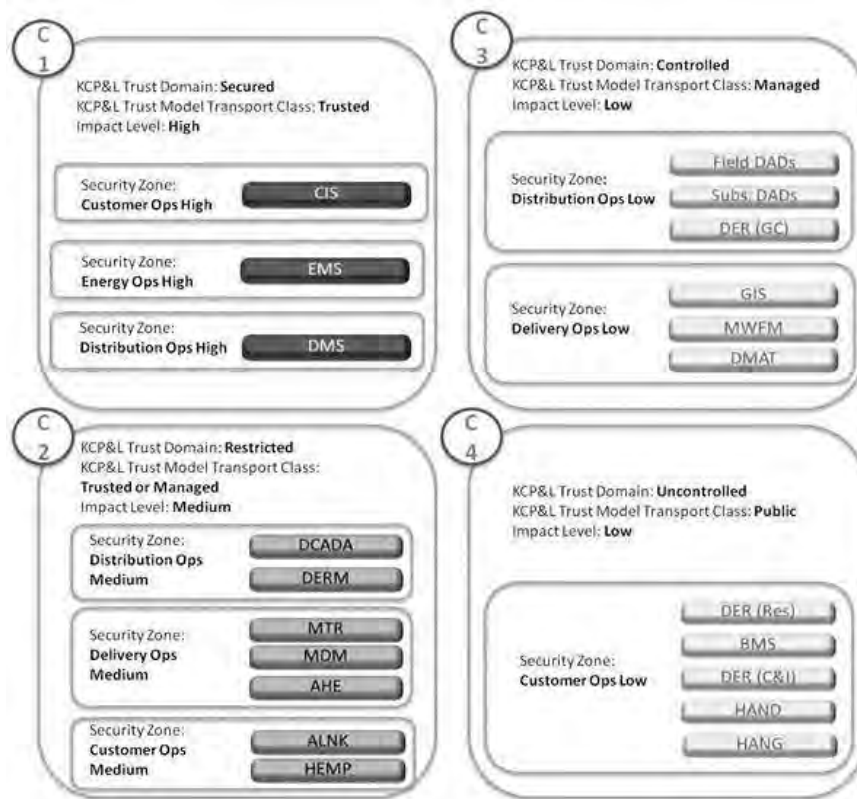
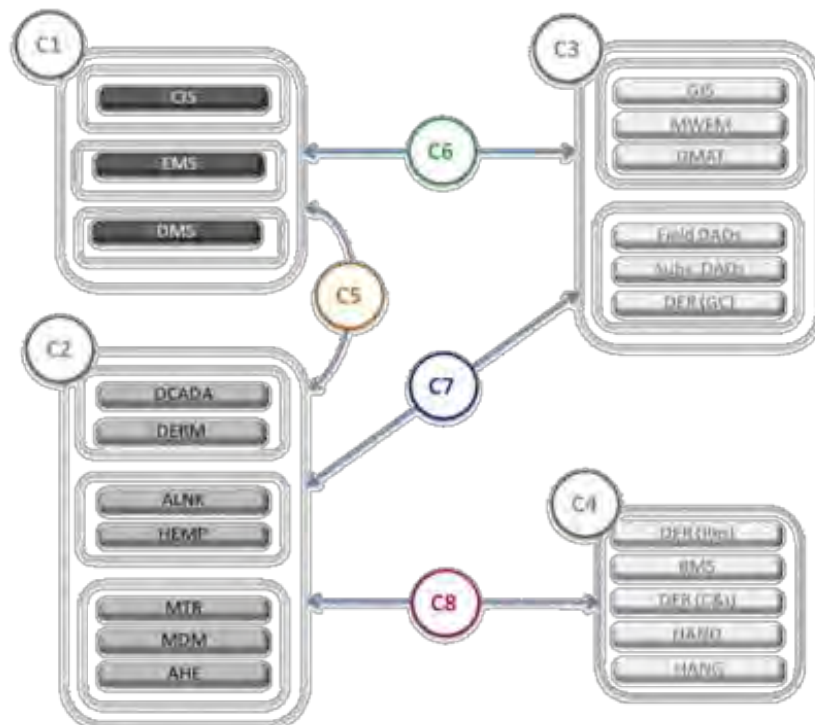


Figure 3-11: Representation of Control Sets for Inter-Security Zone Communication



3.2.2.2 Industry-Suggested Controls

The second type of security control implementation is a collection of controls based on industry best practices and guidelines. This type lists all the controls suggested in the NISTIR-7628 Volume-I [13] based strictly on the applicable logical interface categories and their recommended controls. These security requirements, if implemented to their fullest, should adequately secure the Smart Grid systems. It is worth noting that the controls recommended in the implementation type discussed in Section 3.2.2.1 are a subset of the controls recommended in this type.

Table 3-3 provides a summarized listing of the KCP&L SmartGrid systems along with their applicable NISTIR-7628 Logical Interface Categories. The table indicates that a majority of the NISTIR-7628 security requirements were found to be applicable to all the Smart Grid systems. To improve readability and act as a quick reference, the table lists requirements in the format “All except... the requirements found *not* to be applicable.”

Table 3-3: NISTIR-7628 Security Requirements Applicability by System

SmartGrid System	Applicable NISTIR-7628 Logical Interface Categories	Applicable NISTIR-7628 Security Controls
AHE	5, 13, 14	All Except: SG.AC-12, SG.IA-5, SG.SC-4, SG.SC-17
BMS	15	All Except: SG.AC-11, SG.AC-12, SG.AU-16, SG.IA-5, SG.SC-4, SG.SC-6, SG.SC-9, SG.SC-17, SG.SC-26, SG.SC-29
CIS	7, 8, 10	All Except: SG.SC-6, SG.SC-9, SG.SC-17
DCADA	1, 2, 3, 5	All Except: SG.AC-12, SG.AU-16, SG.SC-4, SG.SC-9, SG.SC-17, SG.SC-26
DER - C&I, DER - Grid-Connected, DER - Residential	11	All Except: SG.AC-11, SG.AC-12, SG.AC-14, SG.AU-16, SG.IA-4, SG.IA-5, SG.IA-6, SG.SC-3, SG.SC-4, SG.SC-5, SG.SC-6, SG.SC-7, SG.SC-9, SG.SC-17, SG.SC-26, SG.SC-29, SG.SI-7
DERM	8, 9, 16	All Except: SG.SC-6, SG.SC-17, SG.SC-29
DMS	5, 10	All Except: SG.AC-12, SG.AU-16, SG.IA-5, SG.SC-3, SG.SC-9, SG.SC-26
EMS	1	All Except: SG.AC-12, SG.AU-16, SG.SC-4, SG.SC-6, SG.SC-9, SG.SC-26
Field DADs, Substation DADs	11	All Except: SG.AC-11, SG.AC-12, SG.AC-14, SG.AU-16, SG.IA-4, SG.IA-5, SG.IA-6, SG.SC-3, SG.SC-4, SG.SC-5, SG.SC-6, SG.SC-7, SG.SC-9, SG.SC-26, SG.SC-29, SG.SI-7
GIS	10	All Except: SG.AC-12, SG.AU-16, SG.IA-5, SG.SC-3, SG.SC-6, SG.SC-9, SG.SC-26
HAND, HANG	15	All Except: SG.AC-11, SG.AC-12, SG.AU-16, SG.IA-5, SG.SC-6, SG.SC-4, SG.SC-9, SG.SC-26, SG.SC-29
HEMP	8, 16	All Except: SG.SC-5, SG.SC-6, SG.SC-29
MDM	7, 8, 10	All Except: SG.SC-6, SG.SC-9
MTR	15	All Except: SG.AC-11, SG.AC-12, SG.AU-16, SG.IA-5, SG.SC-4, SG.SC-6, SG.SC-9, SG.SC-26, SG.SC-29

3.2.3 Security Requirements Development

Using the tailored control sets from the risk assessment as a basis, KCP&L evaluated the security controls provided in the NISTIR-7628 to determine which controls were applicable to each system in the project for the following areas:

- Application Security
- Physical Security
- Network Security
- Policy/Procedural Controls

The NISTIR-7628 security controls are separated into nineteen control families predominantly based upon NIST SP 800-53. KCP&L found at least one control from all nineteen families to be applicable to the Smart Grid systems in the SGDP. Here is a list of the control families:

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Security Assessment and Authorization (CA)
- Configuration Management (CM)
- Continuity of Operations (CP)
- Identification and Authentication (IA)
- Information and Document Management (ID)
- Incident Response (IR)
- Smart Grid Information System Development and Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Security (PE)
- Planning (PL)
- Security Program Management (PM)
- Personnel Security (PS)
- Risk Management and Assessment (RA)
- Smart Grid Information System and Services Acquisition (SA)
- Smart Grid Information System and Communication Protection (SC)
- Smart Grid Information System and Information Integrity (SI)

KCP&L focused its security requirements evaluation on the new systems being deployed in the SGDP. For each new system being implemented, KCP&L determined which party would be responsible for implementing the desired security controls: KCP&L, the vendor(s), or a combination of KCP&L and the vendor(s). For the scope of the SGDP, KCP&L determined that a large subset of the security controls recommended in the tailored control sets (discussed in Section 3.2.2.1 above) were appropriate. Table 3-4 shows the systems that KCP&L developed security requirements for as part of the SGDP along with the number of NISTIR-7628 controls found to be applicable from each control family. For more information, please see Appendix N for the master spreadsheet that lists the specific controls found to be applicable for each of these Smart Grid systems.

Table 3-4: Master Security Controls

NISTIR 7628 Controls Family	Quantity of Applicable Controls						
	MDM	AMI	DERM	HEMP	DMS	DCADA DDC	BESS
Access Control	16	17	16	18	17	17	14
Awareness and Training	4	4	4	4	4	4	2
Audit and Accountability	11	11	11	11	12	12	12
Security Assessment and Authorization	6	6	6	6	6	6	6
Configuration Management	9	9	9	9	11	11	11
Continuity of Operations	8	8	8	8	10	10	9
Identification and Authentication	6	6	6	6	6	6	6
Information and Document Management	4	4	4	4	3	3	3
Incident Response	10	10	10	10	11	11	11
Smart Grid Information System Development and Maintenance	4	4	4	4	4	4	4
Media Protection	6	6	6	6	6	6	6
Physical and Environmental Security	10	10	10	10	11	11	11
Planning	0	0	0	1	4	4	4
Security Program Management	2	2	2	2	5	5	5
Personnel Security	8	8	8	8	8	8	8
Risk Management and Assessment	1	1	1	1	6	6	6
Smart Grid Information System and Services Acquisition	9	9	9	9	10	10	10
Smart Grid Information System and Communication Protection	17	17	17	17	19	19	18
Smart Grid Information System and Information Integrity	8	8	8	8	9	9	9

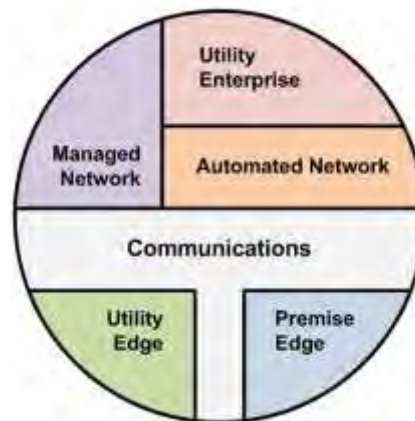
In addition to developing a list of applicable security controls for each Smart Grid system, KCP&L reviewed the design methodologies presented in the UCAIug Security Profiles (primarily for AMI and DM) for key cyber security issues and assessed their applicability to the SGDP.

For the AMI Security Profile, one of the concepts KCP&L focused on was the AMI Security Service Domains, which were discussed in Section 4.4 of that document. The domains identified in the profile are:

- Utility Enterprise
- Automated Network
- Managed Network
- Communications
- Utility Edge
- Premise Edge

KCP&L concentrated on the profile's recommendation that communication should only be allowed to flow between domains that are shown as having a common boundary as shown in Figure 3-12. In other words, KCP&L wanted to ensure that other utility enterprise applications (Utility Enterprise domain) such as OMS, DMS, or MDM would not have direct access to components of the AMI FAN (Communications domain). Only the AHE (Automated Network domain) or devices running field tools (Managed Network domain) should have direct access to components of the AMI FAN. Furthermore, there should be a logical separation between the different components of the AMI meter itself. For instance, the HAN interface of the meter (Premise Edge domain) such as a ZigBee radio should not be able to directly control the utility-owned and operated components of the meter such as the disconnect switch (Utility Edge domain).

Figure 3-12: AMI Security Service Domains [19]



For the DM Security Profile, KCP&L focused on a similar concept but one tailored toward network segmentation. In Section 4.1 of the profile, UCAIug recommends that any DM network architecture should be separated into the four following segments:

- DM Field Network
- DM Control Systems Server Network
- DM Controls Systems User Network
- Non-DM Utility Network

All four of the above segments should be private networks. Furthermore, only the Non-DM Utility Network segment should have direct access to public networks (the Internet). The other three segments should not have access to the Internet. In addition, only the DM Control Systems Server Network should have access to the DM Field Network. That is, the DM Control Systems User Network should not have direct access to the DM Field Network. DM users should interact with some sort of user interface that communicates (behind the scenes) to the DM back-office or substation servers, which in turn handle direct communication to the DM devices in the field or substation.

3.2.4 Application Security Assessment & Implementation

After determining what controls were applicable for each system, KCP&L developed and provided security requirements comprised of security controls from the NISTIR 7628 to the original equipment manufacturers (OEMs) via security surveys. For each requirement, the survey asked for the following responses:

- Specify whether the requirement is covered by responding “Yes”, “No”, or “Planned”
 - If “Yes”, provide the technical details of implementation
 - If “No”, provide reason
 - If “Planned”, provide planned date for conformity and technical details of implementation
- If requirement is covered, list the tests performed that validate that the requirement has been met
- Provide and list the supporting test documentation (cases, procedures, results, etc.)

In addition to the questions about specific NISTIR 7628 controls, KCP&L also asked a series of general questions of the OEMs that host a Smart Grid system:

- Specify whether there is an alternate data center in place to back up the system
- If so, specify whether it is protected the same way as the primary data center
- Specify whether any penetration tests have been performed on the system
- If so, provide results
- Specify whether the OEM has had any third-party security controls reviews performed
- If so, provide results
- Specify what types of encryption methods the system supports

A sample of a security survey sent to the OEMs is provided in Figure 3-13 below.

Figure 3-13: Excerpt from Vendor Cyber Security Survey

NISTIR 7628 Smart Grid Requirement Number	NISTIR 7628 Smart Grid Requirement Name	Is Requirement Implemented? (Yes/No/Planned)	If Yes: Provide technical details of implementation. If No: Provide a reason why. If Planned: Provide planned date of implementation and technical details of implementation.	If requirement has been implemented, please list the tests performed that validate the requirement being met.	Please list the supporting test documentation (cases/procedures, results) that is supplied to KCP&L as part of this questionnaire.
SGAC-1	Access Control Policy and Procedures				
SGAC-2	Remote Access Policy and Procedures				
SGAC-3	Account Management				
SGAC-4	Access Enforcement				

As part of the Implement focus area, KCP&L assessed responses to the security surveys to evaluate the cyber security readiness for both KCP&L and OEM-hosted systems as follows:

- If security requirements are met
- How security requirements are met
- If any third-party assessment (NISTIR-7628, NERC CIP, SSAE 16, etc.) have been performed
- What organizational controls will be implemented by either KCP&L or the OEMs
- What shared organizational controls will be implemented by both KCP&L and the OEMs
- What technical controls will be developed by either KCP&L or the OEMs

KCP&L experienced a variety of responses from the OEMs during this process. Some of them were quite responsive and willing to provide detailed feedback. Others were not as receptive at first but after more discussion, KCP&L was able to receive their responses to the survey. Unfortunately, there were a couple of OEMs that were not willing to fill out the survey. One of these OEMs agreed to discuss their security posture on a series of conference calls, while the other OEM provided the results of a third-party security assessment for KCP&L to review. In both cases, KCP&L applied the OEM’s feedback to the

security survey in order to approximate how well the OEM's security posture lined up with the requirements.

After assessing the various responses received by the OEMs, KCP&L identified what gaps were present for each system. The project team then either chose to implement additional security controls to cover the gaps (where feasible) or to accept the associated risk for the gaps as deemed appropriate within the scope of the SGDP. Due to the confidential nature of the security survey results, they have not been included in this report at this point in time.

3.2.5 Physical Security Assessment & Implementation

As part of the Implement focus area, KCP&L evaluated physical security controls for the KCP&L-hosted systems and one of the OEM-hosted systems (see Section 3.2.7 for more information on the OEM-hosted system). To establish a high level of physical access control and monitoring, the project team:

- Assessed the existing controls at the KCP&L corporate data center and found them to be appropriate for the SGDP
- Assessed the existing controls in the KCP&L operations control room and found them to be appropriate for the SGDP
- Designed and implemented physical security zones and requirements for the SGDP substation and SmartGrid Innovation Park
- Verified the controls that one of the OEMs has in place within their hosting facilities

Before implementation, KCP&L first designed a model for the physical security zones for both the SGDP substation and SmartGrid Innovation Park. The project team first identified all the various physical access points that existed in the substation and that were planned for the park. This consisted of any gates, doors, panels, or cabinets that did or would allow physical access to one or more Smart Grid assets. Then, KCP&L identified the various personnel roles that would require admittance through each of these access points:

- Corporate Security
- Distribution Operations (C&M Crews, Cable Splicers, Linemen, Metermen, etc.)
- Information Technology (Network Engineers, Systems Engineers, Telephone Techs., etc.)
- Transmission Operations (Relay Techs, Sub Electricians, Sub & System Protection Engrs.)
- Smart Grid Team
- Vendors
- General Public

After identifying the applicable personnel roles and which physical access points they would need clearance for, KCP&L determined how they wanted to implement access control for each of these access points. This consisted of either electronic access via a keycard reader or a physical key. In addition, the project team determined what types of mitigation would be required for the perimeter of each site and certain access control points within each site. This consisted of video surveillance, intrusion detection, and motion detection.

After designing physical security zones and requirements, KCP&L assessed the existing controls at the SGDP substation and found them to be appropriate for the scope of the project. For the SmartGrid Innovation Park, the project team implemented a physical security architecture that closely followed the security zones and physical security requirements that were developed earlier in the project.

KCP&L implemented access control for the perimeter of the SmartGrid Innovation Park using physical keys—different keys for the vehicle gate versus the pedestrian gate since each gate was intended for different types of personnel roles. Physical keys were also used to secure access to the grid-connected battery (BMS) and inverter (SMS) enclosures as well as the server and networking racks inside the

battery control enclosure. The project team implemented electronic card readers for access control to the battery control enclosure itself.

For mitigation measures, KCP&L implemented a combination of video surveillance, intrusion detection, and motion detection. Video cameras were installed to monitor the vehicle gate and pedestrian gate as well as the doors to the BMS, SMS, and battery control enclosures. In addition, the project team positioned the video cameras not only to monitor the perimeter but also numerous angles throughout the interior of the SmartGrid Innovation Park. KCP&L implemented intrusion detection via electronic card readers on the vehicle and pedestrian gates. Thus, if anyone without clearance attempts to gain physical access to the site, the local security system generates an alarm and sends it to KCP&L Corporate Security for notification. The project team implemented motion detection by utilizing microwave motion sensors along the perimeter of the park. Similar to the electronic card readers, the microwave motion detection system generates events and alarms and sends them to KCP&L Corporate Security for notification.

KCP&L utilized a local digital video recorder (DVR) to consolidate all of the video feeds captured by the video cameras installed throughout the SmartGrid Innovation Park. In addition, the project team utilized a local security panel to collect and analyze the various events detected by the electronic card readers and microwave motion sensors and to generate alarms as needed. Both the DVR and security panel utilized the KCP&L Corporate WAN backhaul to send their data upstream to the back office Corporate Security systems (see Section 3.2.6 for more information). Thus, new physical security controls were implemented as part of the SGDP, but they were incorporated into KCP&L's existing corporate physical security infrastructure.

3.2.6 Network Security Assessment & Implementation

As part of the Implement focus area, KCP&L assessed the Smart Grid network architecture and related security requirements. Based upon the results of the risk assessment, the project team:

- Created KCP&L network segregation requirements
- Created KCP&L high-level network architecture both for the overall SGDP and within the SGDP substation
- Implemented a Smart Grid network isolated from the KCP&L corporate network
- Implemented point-to-point virtual private network (VPN) connections to OEMs hosting Smart Grid applications
- Verified the network security architecture of one of the OEM's hosting facilities

KCP&L used several different references when creating network segregation requirements for the SGDP:

- Security zones from the cyber security risk assessment
- Security controls from NISTIR 7628
- Security domains recommendations from UCAIug AMI Security Profile
- Network segmentation recommendations from UCAIug DM Security Profile

For more information on the security zones from the cyber security risk assessment, see Section 3.2.2. As part of the effort to develop security requirements for each system, KCP&L identified which NISTIR 7628 security controls were applicable to the design of the network. For more information on the development of the security requirements, see Section 3.2.3. To see a complete list of all the applicable NISTIR controls, see Appendix N. In addition, see Section 3.2.3 for an explanation of the security domains and network segmentation recommendations from the UCAIug Security Profiles for AMI and DM. After establishing network segregation requirements, KCP&L focused on designing a network architecture for the SGDP. The project team first concentrated on the architecture for the SGDP

substation as most of the network build-out would take place there. Within the SGDP substation network architecture, KCP&L implemented the following secure enclaves (graphically depicted in Figure 3-14):

- **KCP&L Corporate Network** – This network provides KCP&L personnel in either the existing SGDP control house or battery control enclosure access to applications on the corporate network and a connection to the Internet. It is an extension of the back office KCP&L corporate network.
- **Substation Distribution Protection & Control Network** – This network consists of redundant fiber optic ring networks that connect all of the substation distribution automation devices that are designed for protection and control (relays and tap changers). The communication within this network is high-speed IEC 61850 compliant.
- **Smart Grid User Network** – This network allows KCP&L personnel to access information displayed to DMS operators in the control center via a DMS workstation installed in the battery control house. Role-based access control (RBAC) determines the privileges of each user. It is an extension of the back office Smart Grid User Network.
- **Substation Distribution Automation & Asset Management Network** – This network contains the systems that make the SGDP substation a “SmartSubstation”. This is comprised of DCADA and the substation HMI. In other words, this is the network segment that contains the Smart Grid substation-based servers and thus serves as the substation control network.
- **Substation Physical Security Network** – This network consists of the security host devices (DVR and security panel) installed in the new battery control enclosure. Each host device collects information from the security devices installed throughout the SmartGrid Innovation Park (video cameras, electronic badge readers, and motion detectors). The hosts send this information to Corporate Security via the KCP&L WAN.
- **Distribution Automation Network** – This wireless field area network provides a communication path for the DMS and DCADA to monitor and control the grid-connected battery and field distribution automation devices (capacitor banks, FCIs, and reclosers).
- **Field AMI Network** – This is the wireless mesh network used for communication between the SmartMeters installed throughout the project area. It also includes the AMI collectors, which serve as gateways for transmitting messages on and off the AMI network.

The three other secure enclaves shown in Figure 3-14 are the Substation Legacy T-SCADA Serial DNP Network, KCP&L TDM Telecom Network, and the KCP&L WAN. The first two are legacy networks and contain non IP-based communication. They exist alongside the IP-based network segments that KCP&L implemented as part of the SGDP. Their primary function is to collect status from the substation distribution automation devices (via serial-based communication) and backhaul the information to KCP&L’s EMS. The KCP&L WAN serves as the corporate backhaul for IP-based communication. Even though the network already existed prior to the SGDP, the project team utilized it to backhaul communication from the substation to the back office.

Anything within each network segment implemented as part of the SGDP (bulleted list above) is allowed to communicate to one another freely. However, all communication between each network segment is restricted to the minimum ports and services required for necessary message transfers between systems. This restriction is implemented using firewall rules.

Figure 3-14: Midtown Substation Network Architecture

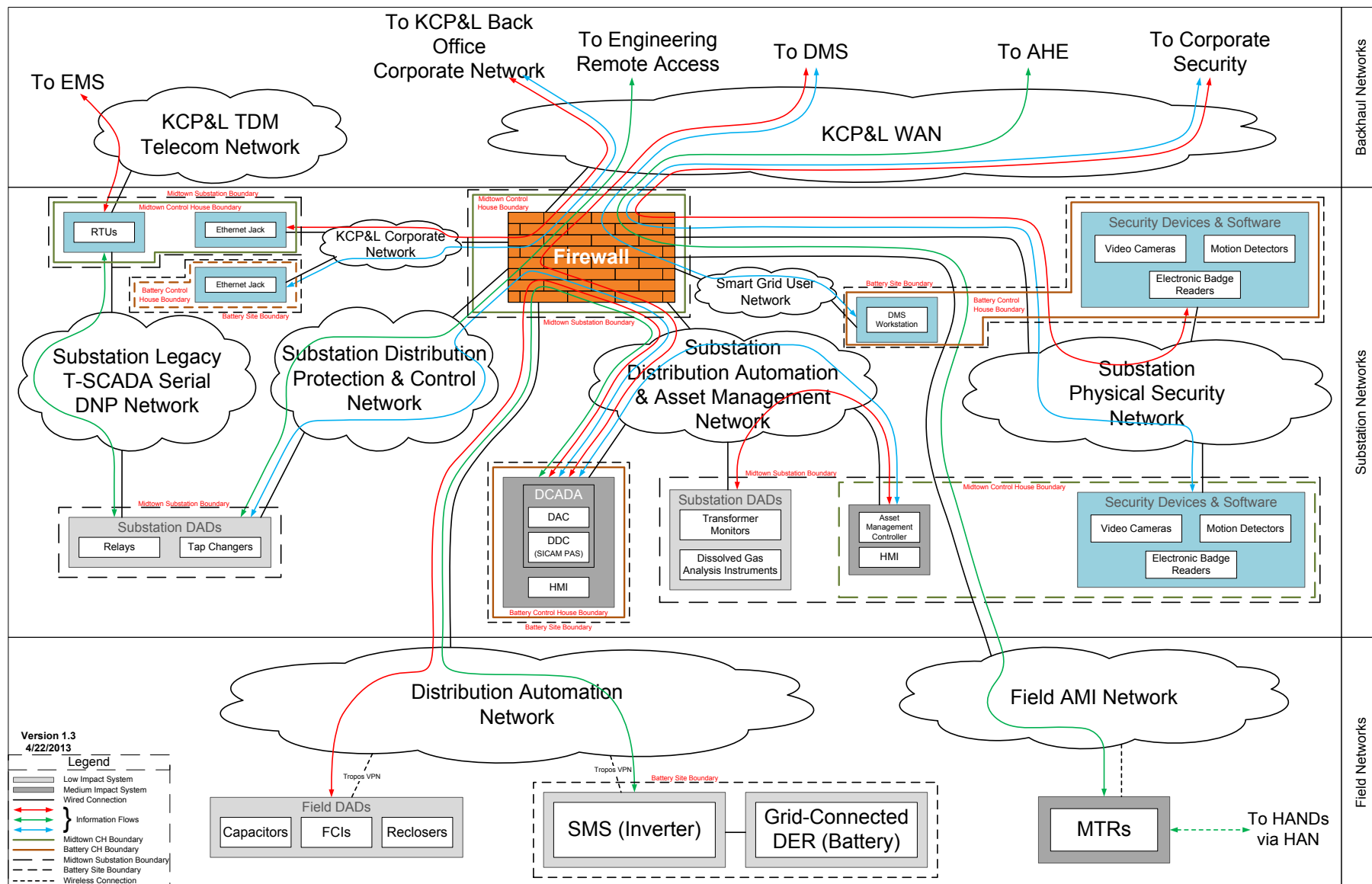
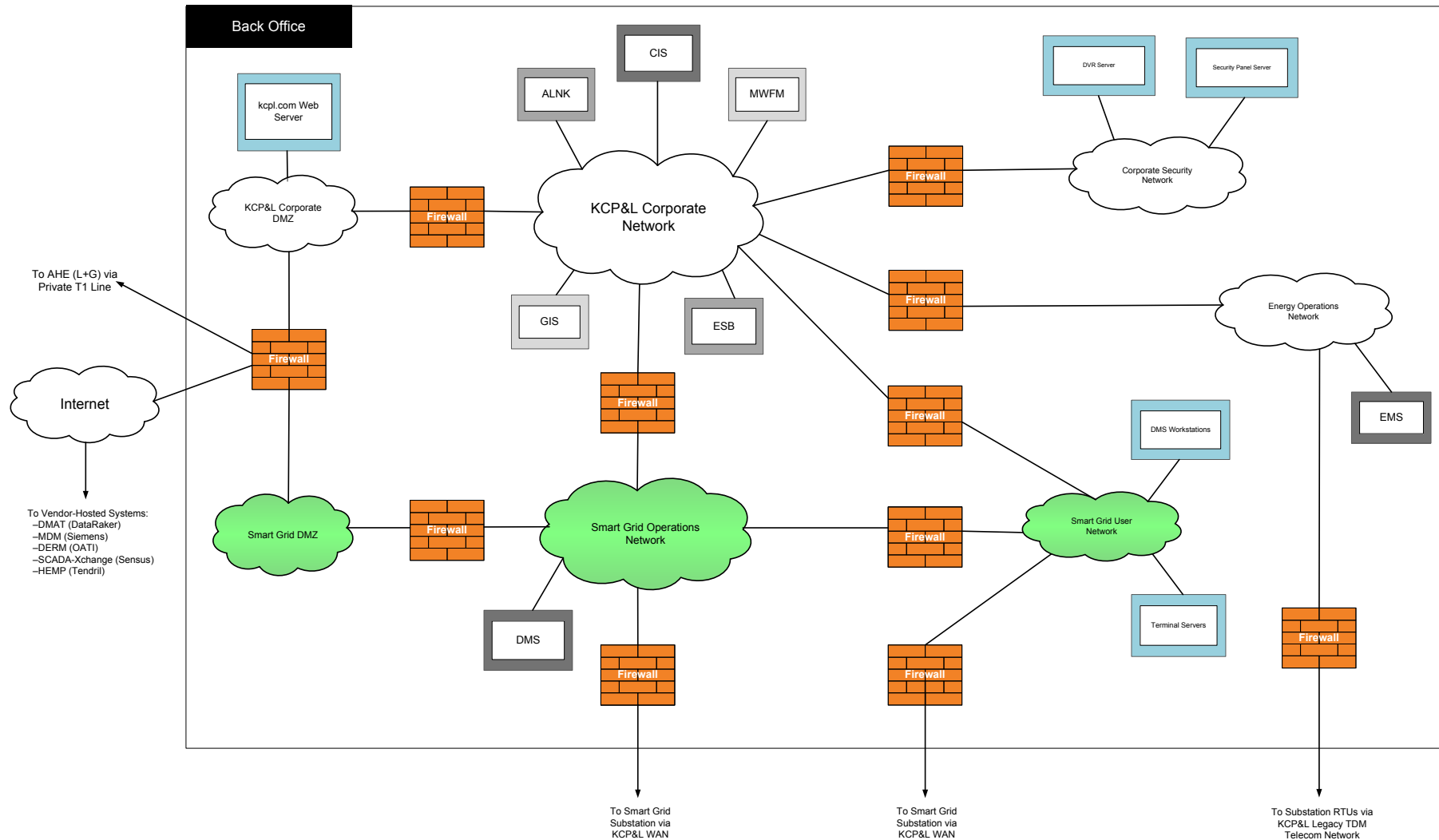
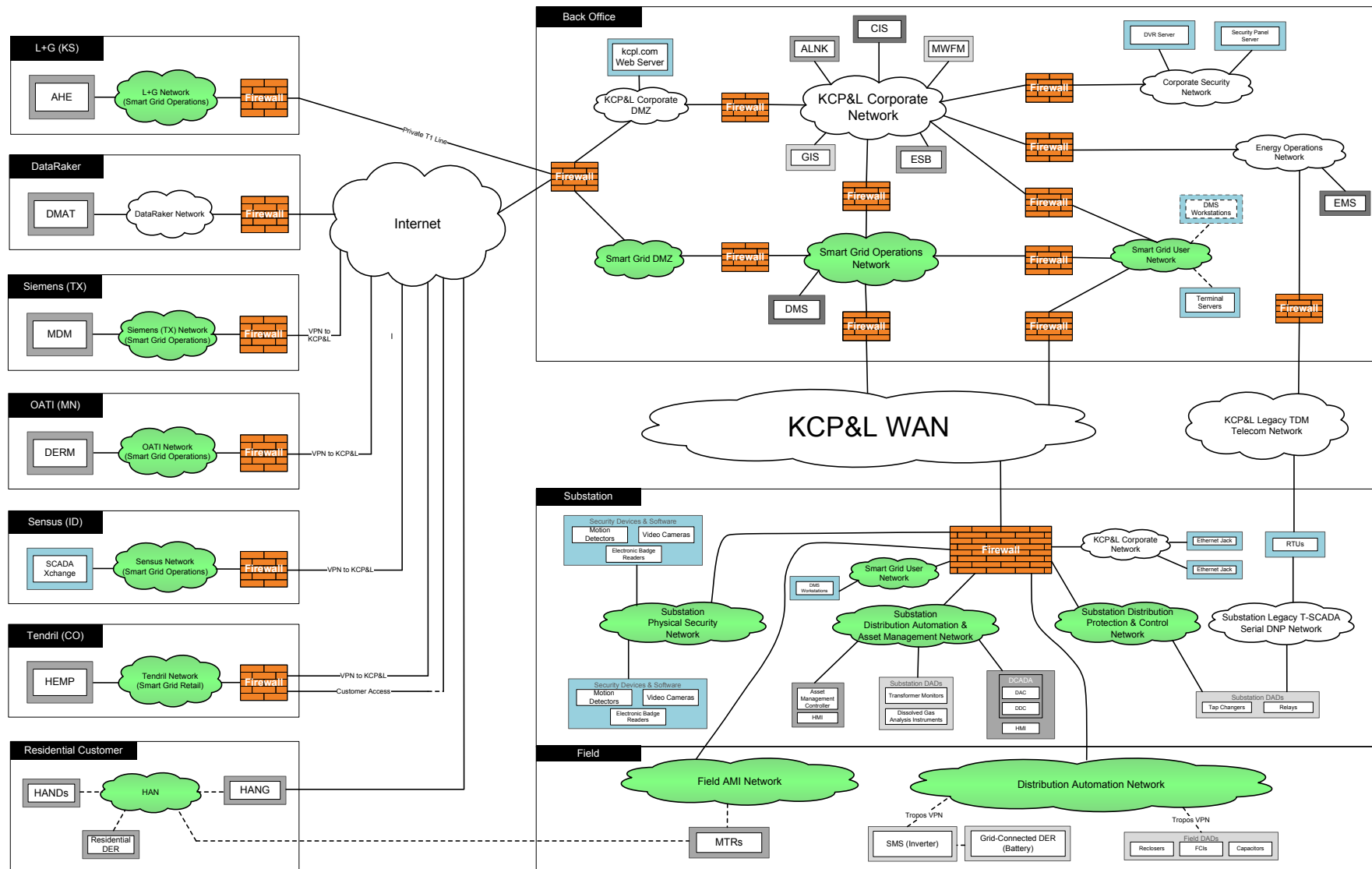


Figure 3-15: Back Office Network Architecture



Version 1.0
02-19-2013

Figure 3-16: Overall SmartGrid Network Architecture



Version 2.4
04-22-2013

Next, KCP&L designed the infrastructure for the back office Smart Grid systems. This architecture is shown in Figure 3-15. Similar to the SGDP substation network layout, the back office network architecture consisted of a combination of new and existing network segments. The new segments that KCP&L implemented as part of the SGDP are shaded green:

- **Smart Grid Operations Network** – This network contains the back office Smart Grid servers, which in the case of KCP&L’s implementation, are the DMS servers. If KCP&L had decided to also host the AHE, DERM, and MDM, they would have been considered part of this same segment.
- **Smart Grid User Network** – This network serves the same function as the one shown in the SGDP substation network architecture. However, this segment contains multiple DMS workstations and two Smart Grid terminal servers. The terminal servers are used as both DMS workstations and as a means for remote access to the various Smart Grid systems that reside both in the back office and in the substation network segments.
- **Smart Grid DMZ** – This network serves as the termination point for the various third-party VPN connections (discussed in further detail below) that the project team implemented as part of the SGDP. For further security, each third-party connection terminates in its own isolated network segment.

The other networks shown in Figure 3-15 existed prior to the SGDP. However, here is a short description of each:

- **KCP&L Corporate DMZ** – This network serves as an isolated environment for KCP&L prefers to keep off of their internal corporate network for security reasons. One example is KCP&L’s corporate website web server.
- **KCP&L Corporate Network** – This network serves as KCP&L’s primary location for its corporate business applications and most of the legacy systems that have interfaces to the new Smart Grid systems implemented as part of the SGDP including CIS, MWFM, GIS, and ALNK.
- **Corporate Security Network** – This network contains the back office corporate security servers that collect security events from KCP&L’s various locations including the SGDP substation.
- **Energy Operations Network** – This network contains KCP&L’s highly critical transmission control system (EMS).

Just like the various network segments within the SGDP substation network architecture, the communication between the newly implemented back office network segments as well as between KCP&L legacy network segments and any Smart Grid network segment is restricted by firewall rules. Only the necessary ports and services required for necessary message transfer between systems is allowed. In addition, all of the various Smart Grid network segments were implemented using a unique IP address space. Each specific Smart Grid network segment was isolated to its own subnet within the unique IP address space. This made it easier to design and implement the various VLANs and to make efficient use of the available pool of IP addresses.

To follow the recommendations provided by UCAIug in their DM Security Profile, KCP&L implemented the Smart Grid terminal servers contained within the back office Smart Grid User Network. This ensures that any KCP&L user coming from the KCP&L Corporate Network must first remote to one of the two terminal servers before being able to remote to one of the various Smart Grid systems. In addition, no Internet access is allowed to or from any of the various Smart Grid secure enclaves both in the back office and in the substation. Furthermore, to isolate Smart Grid traffic traveling between KCP&L physical sites, the project team utilized VPNs. This allowed KCP&L to utilize the existing KCP&L WAN to transport the information while still holding to the security requirements of the SGDP.

The final portion of the SGDP network architecture consists of how the internally-hosted Smart Grid systems interfaced with OEM-hosted ones (graphically shown in Figure 3-16). To ensure the same level of isolation and security requirements were in place for communication between KCP&L and these OEM-hosted systems, KCP&L implemented VPN connections over the Internet to the following OEMs (system hosted shown in parentheses):

- OATI (DERM)
- Sensus (SCADA-Xchange)
- Siemens (MDM)
- Tendril (HEMP)

Another VPN connection not shown on this diagram is the one to Siemens for the DMS Support System (a separate division and office location than the Siemens shown hosting the MDM). Most of the VPN connections are monitored and maintained by the corresponding OEM, but there are a couple that are monitored and maintained by KCP&L due to the OEM's inability to do so. As mentioned previously, each of the third-party VPN connections are terminated (on the KCP&L side) in separate, isolated environments represented by the Smart Grid DMZ cloud in Figure 3-16.

KCP&L utilized the existing private T1 lines to Landis+Gyr to transport communication to and from the AHE, which were managed by a combination of Landis+Gyr and KCP&L. As part of the SGDP, KCP&L implemented a new pair of private T1 lines that utilize MPLS (Multi-Protocol Label Switching) and encryption. In addition, the new T1 lines are completely monitored and maintained by Landis+Gyr.

KCP&L chose to not implement a VPN to DataRaker for communication to DMAT. This was because DMAT was a legacy system and all communication both to and from it consists of file transfers via SFTP. As such, utilizing the Internet for transport was considered acceptable as part of the SGDP.

KCP&L used a combination of external and internal firewalls to restrict communication in and out of the overall KCP&L Smart Grid network and between the various Smart Grid network segments both in the back office and in the substation. The external firewalls, managed by one group in KCP&L's IT, are used to restrict communication to and from each OEM-hosted system. The internal firewalls, managed by another group in KCP&L IT, are used to not only restrict communication between KCP&L's Corporate Network and any of the Smart Grid network segments but also between any two Smart Grid network segments. Thus, communication between two Smart Grid systems that reside on separate network segments must traverse at least one layer of firewalls regardless of its physical location.

3.2.7 Cyber Security Verification

The final sub-area within the Implement focus area was performing cyber security controls verifications for one of the vendor-hosted SGDP applications to ensure that guidelines in the NISTIR-7628 have been met. KCP&L chose to perform this verification on Landis+Gyr, the vendor hosting the AHE system. This verification process consisted of four phases:

1. Pre verification data collection and review
2. Onsite verification
3. Analysis
4. Report generation

Pre verification data collection and review consisted of sending a data request to Landis+Gyr to furnish the following documentation:

- A detailed list of servers and work stations that are used for hosting the AHE
- A diagram detailing the network topology of the hosted system
- Final responses to previously sent security questionnaire
- Copy of internal or third party audit reports (general IT or cyber security specific) performed for hosted site

- The reports, findings, and action plans of any vulnerability assessment performed within the last twelve calendar months
- A detailed description of implemented physical security controls to secure the hosted site

Landis+Gyr was very cooperative in providing nearly all of the request material prior to the onsite visit. Once the project team received the request documentation, they reviewed and prioritized focus areas for the onsite verification visit. Prioritization was based upon which NISTIR 7628 controls were deemed the most important and critical out of the full list of applicable security requirements.

The onsite verification visit consisted of interviewing Landis+Gyr personnel, observing the hosted environment, reviewing documentation, and reviewing evidence for twenty-two areas of cyber security and information technology controls:

1. Hosting services applicable to KCP&L
2. Secure Software Development Life Cycle (SDLC)
3. Security configuration management (Ports and services, Patch management, Malicious software prevention, and Logging, auditing and monitoring)
4. Access/account management
5. Change management
6. Network security architecture
7. Code management
8. Vulnerability and security assessments
9. Electronic access controls and monitoring
10. Physical access controls and monitoring
11. Cyber security incident response process and procedures
12. Data backup and restoration
13. Disaster recovery/continuity of operations
14. Data center operations
15. Information protection
16. Test environment
17. Testing methodology
18. Personnel security and training
19. Cyber security team
20. Leadership commitment/support
21. Internal/third-party audits
22. Industry participation

The onsite verification at Landis+Gyr took place over a period of two days. During those two days, Landis+Gyr provided a panel of security and auditing personnel to provide feedback to the questions that the KCP&L project team had prepared. Depending on the specific topic being discussed, Landis+Gyr brought in other SMEs to provide additional detailed information. Overall, Landis+Gyr was very accommodating and helpful during the entire visit.

In the analysis phase, KCP&L analyzed the information collected before and during the onsite visit. The analysis focused on determining whether Landis+Gyr's AHE system and hosting practices adhere to the guidelines set forth in the NISTIR-7628. For each of the twenty-two areas identified above, KCP&L assessed if Landis+Gyr:

1. Completely adheres to the guidelines
2. Partially adheres to the guidelines (including identification of gaps)
3. Does not adhere to the guidelines

After analyzing, KCP&L generated a report detailing the project team's analysis and identified the security gaps that Landis+Gyr had. Specifically, for each of the NISTIR 7628 controls that were prioritized for the onsite verification and for each of the twenty-two areas of cyber security and information technology controls, the report concluded whether Landis+Gyr's security controls were:

1. Satisfactory
2. Other than Satisfactory

After KCP&L finalized the report, the project team sent the report to the vendor for review and feedback. Landis+Gyr is currently reviewing the report. As such and due to the sensitive nature of the report's contents, the controls verification report has not been included in this Technology Performance Report at this point in time.

3.3 Education & Outreach

KCP&L's approach to public education and outreach for its SmartGrid Demonstration Project took a highly-targeted, multiple-channel approach to reach customers and other key stakeholders. Table 3-5 below identifies key stakeholders and communication methods that were utilized for each audience. Descriptions of the communication methods identified in Table 3-5 are grouped in the following subsections:

- All KCP&L Customers
- SmartGrid Demonstration Project Area Customers
- KCP&L Employees
- State Agencies, Legislators, and Regulators
- Electric Utilities and Smart Grid Industry
- Targeted Education & Outreach Initiatives
- Project Tours and Field Demonstrations

Table 3-5: SmartGrid Audience Communication Methods

Audiences	Audience Description	Communication Methods
All KCP&L Customers	<p>While customers living within the Demonstration Project area will be the first affected by SmartGrid initiatives, what KCP&L learns from the project will eventually impact all KCP&L customers. As such, outreach to the entirety of KCP&L's customer base will be an important part of SmartGrid communications.</p> <p><u>Key Stakeholders:</u></p> <ul style="list-style-type: none"> • Residential Customers • Commercial Customers • Industrial Customers 	<ol style="list-style-type: none"> 1. SmartGrid website 2. Radio advertising 3. Print advertising 4. Outdoor advertising 5. Energy fairs 6. SmartGrid Demonstration House 7. Social media 8. KC media coverage 9. SmartGrid education module for schools 10. KCP&L employee advocates 11. SmartGrid customer service representatives 12. SmartGrid office
SmartGrid Demonstration Project Area Customers	<p>Customers living within the SmartGrid Demonstration Project Area.</p> <p><u>Key Stakeholders:</u></p> <ul style="list-style-type: none"> • Individual Customers • Neighborhood Groups • Schools • Community Leaders • Elected Officials • Green Impact Zone Partners 	<ol style="list-style-type: none"> 1. All Communications Methods to All KCP&L Customers 2. Direct mail 3. SmartGrid welcome kit 4. SmartGrid DVD 5. E-mail outreach 6. Automated customer notification 7. Key leader briefings and mailings 8. Community organization meetings and newsletters 9. Neighborhood association meetings and newsletters 10. Church group meetings, displays and bulletins 11. Green Impact Zone staff 12. Ambassadors

Audiences	Audience Description	Communication Methods
KCP&L Employees	<p>As media coverage and interest of the project in the broader service territory increases, KCP&L employees will be asked by friends, family and neighbors about SmartGrid. The 3,600 KCP&L employees can be utilized as SmartGrid ambassadors, but KCP&L will need to provide them with ongoing communications in order to make them effective.</p> <p><u>Key Stakeholders:</u></p> <ul style="list-style-type: none"> • Customer Care Departments • Engineering and Operating Departments • KCP&L Employees Living in the Project Demonstration Area 	<ol style="list-style-type: none"> 1. The Source (employee newsletter) 2. Daily e-Source updates 3. TV monitors 4. Leadership Link videos 5. Managers Leadership Forum updates
State Agencies, Legislators, and Regulators	<p>The individuals in this audience are charged with representing the community. They include elected or appointed individuals, who are especially sensitive to activities that may affect their constituents.</p> <p><u>Key Stakeholders:</u></p> <ul style="list-style-type: none"> • Missouri Public Service Commission & Staff • Kansas Corporation Commission & Staff • Missouri Office of Public Counsel • Elected officials 	<ol style="list-style-type: none"> 1. SmartGrid educational workshops 2. MO & KS Commission Smart Grid staff participation in project workshops 3. MO SmartGrid stakeholder group meetings 4. Project technical reports 5. Project technical website
Electric Utilities and Smart Grid Industry	<p>One of the main goals of this project is to serve as a blueprint for future integrated Smart Grid demonstrations and implementations throughout the country. In order to do this, KCP&L will need to effectively communicate and share knowledge with other utilities and the Smart Grid industry as a whole.</p> <p><u>Key Stakeholders:</u></p> <ul style="list-style-type: none"> • Department of Energy • National Energy Technology Laboratory • National Institute of Standards & Technology • Smart Grid Interoperability Panel • Professional Associations • Labor Organizations 	<ol style="list-style-type: none"> 1. Project technical reports 2. Project technical website 3. EPRI's Smart Grid resource center (www.smartgrid.epri.com) 4. Workshops 5. Webcasts 6. Periodic publications 7. White papers/articles 8. SmartGrid Demonstration House 9. SmartSubstation Tour

3.3.1 All KCP&L Customers

Communicating with KCP&L's end users, both those located in the Demonstration Project area and those in the greater service area, was extremely important. By reaching out to the consumer, KCP&L worked to drive awareness and understanding of SmartGrid as well as encourage product acceptance and adoption.

3.3.1.1 Customer Focused SmartGrid Website

Although internet access is low in some parts of the SmartGrid Demonstration Project area, the KCP&L SmartGrid website was an important customer communication vehicle, both for KCP&L customers within the project area and in the broader service territory. The website provided key information about the Demonstration Project, including facts sheets, meter installation maps, timelines, upcoming events, news and FAQs. The MySmart Portal, MySmart Display, and MySmart Thermostat informational videos were also hosted on the website. The site is part of KCPL.com, but is also accessible via www.kcplsmartgrid.com (Figure 3-17). Over the course of the Demonstration Project, KCP&L continued to add to and enhance the site with user functionality, Flash-enabled graphics, video clips, testimonials and a series of short "How To" videos.

Figure 3-17: www.kcplsmartgrid.com Home Page Screenshot



3.3.1.2 Advertising

Paid advertising represents an important part of KCP&L's public education and outreach efforts, but the geographic boundaries of the Demonstration Project area presented some unique challenges. Paid advertising effectiveness and impact is a derivative of layering multiple avenues, building a reach of at least 70 percent, while still maintaining a healthy frequency of at least 4x. In order to achieve the necessary reach and frequency, KCP&L utilized a combination of radio, print and outdoor advertising.

- Radio – Due to the diverse age range of the Demonstration Project customers, it was important to use a medium that is high reaching. Radio is the second highest reaching medium available (after TV) and is also one of the most cost-effective mediums.
- Print – Despite the overall decrease in physical newspaper consumption, smaller, more-niche community papers (like those read in and around the Demonstration Project area) continue to hold their base as their traditionally older readership is less likely to consume their news online. Additionally, print offers a higher retention rate than radio, allowing KCP&L's message to resonate with customers without the requirement of higher frequencies.
- Outdoor – Urban environments like the Demonstration Project area are ideal settings for outdoor advertising. Even though population density is higher, residents are still very mobile — walking, driving and taking public transportation on a daily basis. This is also a medium that has a much wider mass-market focus. By placing billboards strategically in and around the Demonstration Project area, KCP&L was able to cover a broader customer base.

Table 3-6: Paid Advertising Initiatives

Initiative	Medium	Date
23 SmartGrid Billboards in Demonstration Project Area	Outdoor	June-Dec. 2012
KCATA Bus SmartGrid Signage	Outdoor	June-Dec. 2012
SmartGrid Innovation Park Battery Wrap	Outdoor	2012-Present

3.3.1.3 Energy Fairs

In addition to utilizing existing neighborhood and community meetings, KCP&L hosted a series of energy fairs in the Demonstration Project area. These educational events served as training workshops for those customers interested in learning more about SmartGrid, specifically the MySmart suite of products. They were also an ideal opportunity for KCP&L to get anecdotal feedback via one-on-one interaction with customers. The schedule of energy fairs was included in the welcome kits delivered to customers upon meter installation and was also listed on the website. In addition, KCP&L placed automated calls to customers who received their new SmartMeter, notifying them of upcoming energy fairs.

Table 3-7: Schedule of Energy Fairs

Location	Date	Attendance
Missouri Department of Conservation Discovery Center	Nov. 2, 2010	25
Paseo High School	Nov. 6, 2010	8
St. James United Methodist Church	Nov. 18, 2010	50
Paseo High School	Dec. 4, 2010	200
Missouri Department of Conservation Discovery Center	Jan. 15, 2011	Unknown

3.3.1.4 Social Media

Evidence points to significant use of mobile phones in the Demonstration Project area, making a social media strategy important to the overall public education and outreach effort as the Demonstration Project progressed. Texting, Twitter, YouTube, etc., informed residents about upcoming events, ways to increase energy efficiency and other important SmartGrid information. A mobile platform allowed real-time notification of installation appointments, completions and other notifications, improving the overall customer experience. Subsequently, KCP&L was able to engage in a two-way dialogue with customers and receive instant feedback on customer reaction/sentiment. The Demonstration Project social media strategy was balanced against KCP&L’s larger communications efforts and was conducted in coordination with the company’s broader social media strategy and rollout.

3.3.1.5 Kansas City Media Briefings

Although Smart Grid initiatives have been rolled out in other parts of the country, KCP&L’s Demonstration Project was the first to introduce these technologies to an urban core. As such, it attracted significant local media attention. Local media targets in the Kansas City area include *The Kansas City Star*, *Kansas City Business Journal*, *The Call*, *The Globe*, KMBZ 980 AM, KCUR 89.3 FM, WDAF-4, KSHB-41, KCTV-5 and KMBC-9. KCP&L had a set of statements prepared to respond to general media inquiries regarding SmartGrid. In addition, KCP&L identified a number of short- and long-term project milestones that served as opportunities for proactive media outreach. For example, on November 1, 2010, KCP&L conducted a SmartGrid media day featuring demonstrations of the MySmart suite of products.

Figure 3-18: Screenshot of SmartGrid News Story



Table 3-8: Kansas City Media Initiatives

Initiative	Outlet	Date
New KCP&L SmartGrid Customer Programs Begin	MARC Newsletter	Oct. 2010
SmartGrid Demonstration Project	MARC Annual Report Update	2010
SmartGrid Project Update	MARC newsletter	Jan. 2011
KCP&L to Receive Stimulus Grant for Kansas City SmartGrid Demonstration	Press Release	Nov. 24, 2009
KCP&L to Receive Stimulus Grant for Kansas City SmartGrid Demonstration	Press Conference	Nov. 24, 2009
KCP&L Launches SmartGrid Project	Press Release	Nov. 10, 2010
The Green Impact Zone	Under the Clock: The GIZ Blog	Mar. 27, 2009
KCP&L Smart Grid Places Customer in Control	Examiner.com	June 22, 2009
Details on GIZ are Sparse So Far	Kansas City Star	July 3, 2009
A Golden Opportunity for KC's Green Zone	Kansas City Star	Aug. 31, 2009
Green Impact Zone Funds Already in Use in Metro	Fox 4 KC	Sept. 1, 2009
Kansas City Power & Light Commits \$14M for Smart Grid Technology	Kansas City Business Journal	Sept. 1, 2009
Federal Officials Praise GIZ in KC's Urban Core	Kansas City Star	Sept. 1, 2009
Green Impact Zone Waits for New Pot of Smart Grid Funds	Kansas City Star	Oct. 27, 2009
GIZ Getting Off to Slow Start	Fox 4 KC	Nov. 19, 2009
KC's Electric Efficiency Get \$24 Million Boost	Kansas City Star	Nov. 24, 2009
Kcp7l will Get \$24M In Stimulus Money	Kansas City Business Journal	Nov. 24, 2009
\$24-Million Federal Grant Powers Smart Grid Plan	KCUR.org	Nov. 24, 2009
GIZ Report is Delayed	Kansas City Star	Dec. 1, 2009
An Innovative Step Toward Smarter Energy Use	Kansas City Star	Dec. 20, 2009
Stimulus Puts U.S. Renewable Energy Generation on Track to Double by 2012	Kansas City Business Journal	Dec. 21, 2009
Old Home Provides Tips on Efficiency	News-PressNow.com	Oct. 2, 2010
New Smart Technology to Save KCP&L Customers Money	Fox 4 KC	Nov. 10, 2010
Green Impact Zone: Putting Funds to Work	KCB Central	Nov. 2010
Kansas City Power & Light Meters Out Sustainability Effort	Kansas City Business Journal	Nov. 24, 2010
Project Living Proof	Greenability Magazine	Sept/Oct 2010
Episode 2: Energy Efficiency and Conservation – In-Studio Interview with Kevin Bryant	KCPT – Imagine KC	Jan. 27, 2011
KCP&L Completes Smart Meter Installation	Press Release	April 29, 2011
KCP&L Announces Solar Project in GIZ	Press Release	Oct. 28, 2011
KCP&L Officially Opens SmartGrid Innovation Park	Press Release	Oct. 12, 2012
Kansas City Power & Light Partners With Siemens for Smart Grid Demonstration Project	KCP&L Press Release	Feb. 1, 2011
Articles related to Press Release: Kansas City Power & Light Partners With Siemens for Smart Grid Demonstration Project	Various	Feb. 2-24, 2011
Exergonix Tests 1-MW Battery in Kansas City	Sustainable Business Oregon	Feb. 7, 2011
Reaching the End-User	Intelligent Utility – Online	March 9, 2011
Landis+Gyr Helps KCP&L Reach Important Milestone in SmartGrid Project; Utility Completes Initial Gridstream Smart Meter Installation	Energybiz Insider	May 10, 2011
Landis+Gyr Helps KCP&L Reach Important Milestone in SmartGrid Project; Utility Completes Initial Gridstream Smart Meter Installation	Intelligent Utility – Online	May 10, 2011

Initiative	Outlet	Date
Articles related to Press Release: KCP&L Announces Innovative Partnership with Google	Various	May 16-20, 2011
Articles related to Press Release: Kansas City Power and Light Leverages Siemens and eMeter for Additional Smart Grid Initiatives	Various	May 22-Sept. 19, 2011
KCP&L selects Siemens Energy to implement eMeter EnergyIP	PredictWallStreet.com	May 25, 2011
KCP&L selects Siemens Energy to implement eMeter EnergyIP	TMCnet.com	May 25, 2011
Growing jobs in KC's Green Impact Zone	Kansas City Star	June 14-15, 2011
Kansas City to Leverage Google for Smart Grid	Greentech Media	July 12, 2011
Google's FTTP networks to power smart grid applications	Fierce Telecom	July 15, 2011
Articles related to Press Release: Paseo Academy to get KCP&L solar project	Various	Oct. 28-31, 2011
Google's interest in splicing tech, utilities may benefit KCK	BizJournals.com	Nov. 15, 2011
Articles related to Press Release: Green Impact Zone makes a small impact so far in Kansas City	Various	Dec. 2-4, 2011
KCP&L and Google – A Next Generation Partnership	Electric Energy T&D Magazine – Online	Dec. 24, 2011
On the Hot Seat: KCP&L's Gail Allen	FierceSmartGrid	Apr. 25, 2012
Cybersecurity Roundtable: The Enemy is Unknown	Electric Light and Power	May 3, 2012
Leveraging Behavioral Science for Persistent Customer Engagement Webinars #1-4	Smart Grid Newsletter	June 11, 2012
Urban revitalization and grid modernization?	Intelligent Utility – Online	June 12, 2012
Five secret weapons to help seal smart grid deals	tED Magazine (The Electrical Distributor) – Online	June 13, 2012
Articles related to Press Release: ABB to supply broadband wireless network to KCP&L	Various	Aug. 29-30, 2012
Smart Grid M&A Watch: ABB Paid \$35M for Tropos	Greentech Media	Aug. 29, 2012
Who says smart grid work is slowing down? Not our latest list of project wins	Smart Grid Newsletter	Aug. 31 & Sept. 5, 2012
Preparing for the rapidly expanding analytics environment	Fierce Energy	Oct. 8, 2012
Articles related to Press Release: KCP&L, Exergonix, MRIGlobal Pilot New Energy Storage System	Various	Oct. 11-17, 2012
KCP&L first live test site for battery energy storage tech	Transmission & Distribution World – Online	Oct. 17, 2012

*Media initiatives continue.
Table to be updated in future releases of this report.*

3.3.2 SmartGrid Demonstration Project Area Customers

Communicating with KCP&L's end users, both those located in the Demonstration Project area and those in the greater service area, was extremely important. By reaching out to the consumer, KCP&L drove awareness and understanding of SmartGrid as well as encouraged product acceptance and adoption.

3.3.2.1 Direct Mail

One of the challenges of the Demonstration Project area is the high percentage of renters, making it a highly transient area, with residents constantly moving in and out. In addition to the broader mix of marketing and education efforts, KCP&L reached out to residents through a series of direct mail letters and postcards. These consistent and regular updates were particularly useful to new residents within the Demonstration Project area, especially those not already familiar with the project.

In early September 2010, all 14,000 KCP&L customers were sent a letter from Mike Deggendorf, KCP&L's Senior Vice President for Delivery. The letter welcomed them to the SmartGrid Demonstration Project and broadly explained both the customer benefits and next steps as the project got underway.

KCP&L also distributed a series of SmartGrid postcards to customers, staged to coincide with the meter installation schedule.

Table 3-9: Direct Mailing Timeline

Audience	Description	Date
All Demonstration Project Customers	Welcome to SmartGrid Letter	September 2010
All Demonstration Project Customers	Meter Installation Notification	On-Going
Green Impact Zone Customers	Product Postcard	October 2010
Broader Project Area Customers (outside Green Impact Zone)	SmartGrid Status Update	October 2010
Broader Project Area Customers (outside Green Impact Zone)	Product Postcard	January 2011
SmartGrid Demonstration Project Customers	SmartGrid Mailer Postcard	March 2011
MySmart Display Customers	MySmart Display Postcard	March 2011
MySmart Display Customers	"Sorry We Missed You" Notice	April 2011
All Demonstration Project Customers	Demo Home Open House Invitation	April 11, 2011
All Demonstration Project Customers	"Get Smarter" WebKey Mailer	2011
New Demonstration Project Customers	SmartGrid Welcome Letter	2012
All Demonstration Project Customers	Time-of-Use Rates Letter	2012

Direct mailings continue.

Table to be updated in future releases of this report.

3.3.2.2 SmartGrid Welcome Kit

For most customers, meter installation represented the first interaction with Smart Grid. At the time of SmartMeter installation, customers were provided with a KCP&L SmartGrid Demonstration Project welcome kit. Included in the welcome kit was a welcome book, MySmart product information, a SmartGrid DVD, information on community weatherization and energy assistance resources, a schedule of upcoming energy fairs and a compact fluorescent light bulb. The welcome kits were either given directly to the customer or left at the front door if no one was available.

Figure 3-19: SmartGrid Welcome Kit



3.3.2.3 SmartGrid DVD

Working with a local Women's Business Enterprise (WBE) video production company, KCP&L developed an overview video that creates general awareness and understanding of KCP&L's SmartGrid Demonstration Project and the customer benefits. Featured on the video are Mike Chesser, CEO of KCP&L; U.S. Rep. Emanuel Cleaver, II, Congressman for Missouri's 5th District; and Margaret May, Executive Director of the Ivanhoe Neighborhood Council. In addition, KCP&L worked with Tendril to develop two short instructional videos for MySmart Display and MySmart Portal, which are included as chapters on the DVD.

Figure 3-20: SmartGrid DVD



3.3.2.4 E-mail Outreach

KCP&L already has a well-established online service for its customers called AccountLink. Through AccountLink, customers can access their account information and billing history, and make payments online. There are already more than 2,800 AccountLink customers within the Demonstration Project area. With access to these customers' e-mail addresses, KCP&L was able to distribute targeted e-mails to customers who already used and were familiar with the company's online platform. The remainder of KCP&L customers were required to register for AccountLink the first time they signed on to MySmart Portal to view their usage information. As more customers were acquired and product adoption increased, more of the public education and outreach was conducted online via e-mail.

Table 3-10: E-mail Initiatives

Description	Audience	Date
MySmart Portal – Launch Notification	All SmartGrid Customers	2011
Get Smarter About Energy – Time-of-Use Program	All SmartGrid Customers	2012
Your “Get Smarter” Guide – MySmart Home Offering	SmartGrid Energy Optimizer Customers	2012
Your “Get Smarter” Guide – Time-of-Use Offering	All SmartGrid Customers	2012
Your “Get Smarter” Guide – KCP&L SmartGrid Q&A	All SmartGrid Customers	2012
Your “Get Smarter” Guide – MySmart Home and MySmart Portal Information	All SmartGrid Customers	2012
Your “Get Smarter” Guide – KCP&L SmartGrid Fall Events	All SmartGrid Customers	2012
Your “Get Smarter” Guide – MySmart Portal Makeover	All SmartGrid Customers	2012
Your “Get Smarter” Guide – MySmart Program Information	All SmartGrid Customers	2012
Your “Get Smarter” Guide – MySmart Portal Can Help Keep Your Home Toasty and You Penny-wise!	All SmartGrid Customers	2012

*E-mail initiatives continue.
Table to be updated in future releases of this report.*

3.3.2.5 Automated Customer Notification

KCP&L has had great success reaching customers for its Connections Program (energy efficiency and bill payment assistance) through the use of automated customer notification calls. These calls allow KCP&L to reach a large number of customers in a relatively short amount of time and at a low cost. In particular, KCP&L used automated calls to drive attendance to upcoming energy fairs, where members of the SmartGrid team provided an overview of the project as well as training on the MySmart suite of products.

3.3.2.6 Civic Outreach

A number of formal and informal community groups exist within the SmartGrid Demonstration Project area. KCP&L made efforts to engage in frequent communication with these groups to gather project feedback and communicate messages back to the end users.

3.3.2.6.1 Key Leaders

Critical to the success of the Demonstration Project public education and outreach effort was the endorsement and support of key community and neighborhood leaders. KCP&L partnered with community leaders within the Demonstration Project area to raise awareness of SmartGrid and other KCP&L initiatives, particularly the company's energy efficiency products and services. On September 14, 2010, KCP&L hosted about 40 key leaders at a SmartGrid briefing at the Green Impact Zone offices. This meeting was an opportunity to exchange information, answer questions and proactively address any concerns. This event was preceded by a letter that was mailed to approximately 150 community leaders providing them an update on the project. Continued, frequent, thorough two-way communication with key leaders over the course of the Demonstration Project allowed them to become effective ambassadors for KCP&L, built support for SmartGrid initiatives and eased any community concerns that may have arisen. KCP&L's Government Affairs department managed direct communications with key leaders and elected officials.

Table 3-11: Schedule of Events

Event	Location	Date	Attendance
June Community Event	Swope Parkway	June 12, 2010	1500
MPSC Training	Jefferson City, MO	July 23, 2010	10
Key Leader Community Briefing	GIZ HQ	Sept. 14, 2010	50
Halloweatherization	GIZ HQ	Oct. 30, 2010	300
Sustainability/SmG/Connections	Paseo High School	Dec. 4, 2010	400
Community Leader SmartGrid Event	Project Living Proof	March 10, 2011	35
South Kansas City Chamber of Commerce Tour of Project Living Proof	Project Living Proof	April 27, 2011	15

*Key Leader communication initiatives continue.
Table to be updated in future releases of this report.*

3.3.2.6.2 Community Organizations

A number of credible, well-established community organizations operate in and around the Demonstration Project area. Key organizations include Brush Creek Community Partners, Blue Hills Community Services, the Southtown Council and Swope Community Builders. These organizations have long-standing relationships with residents in the Green Impact Zone and beyond and were effective partners in educating residents and engaging them in SmartGrid initiatives. KCP&L Community Relations worked closely with these organizations and engaged community leaders via one-on-one communication. These organizations were also utilized to help spread information about the Demonstration Project at their regular meetings and through their organizational newsletters.

Table 3-12: Community Events

Event	Location	Date	Attendance
MySmart Display Customer Engagement Dinner	GIZ Office	Mar. 24, 2011	15
South Kansas City Chamber of Commerce Tour of Project Living Proof	Project Living Proof	April 27, 2011	15
Demonstration Home Grand Opening	Project Living Proof	April 30, 2011	250
Heartland Connection		Jan. 26, 2012	25
Meet Me At The Bridge	48 th and Troost Bridge	May 5, 2012	250
Night Out Against Crime	Swope Park	Aug. 7, 2012	300
Innovation Park Ribbon Cutting	Innovation Park	Oct. 12, 2012	100
Halloween Open House	Project Living Proof	Oct. 31, 2012	75

*Community Events initiatives continue.
Table to be updated in future releases of this report.*

3.3.2.6.3 Neighborhood Associations

Neighborhood associations are critical to Green Impact Zone initiatives. Their engagement in the SmartGrid Demonstration Project lent credibility and granted access to an established communication infrastructure. KCP&L worked closely with neighborhood organizations within the Demonstration Project area to build advocates and cultivate positive relationships in support of the Demonstration Project. Members of KCP&L's Community Relations team met with neighborhood associations regularly throughout the project. In addition to providing an overview of the Demonstration Project, these meetings allowed KCP&L to demonstrate the MySmart suite of products and speak directly to the customer benefits. KCP&L maintained ongoing communication with neighborhood associations throughout the course of the SmartGrid Demonstration Project.

Table 3-13: Schedule of Neighborhood Meetings

Neighborhood	Location	Date	Attendance
Town Fork Creek	Mazuma Credit Union	Sept. 25, 2010	30
Troostwood	Coffee Break	Oct. 2, 2010	8
Manheim Park	Immanuel Lutheran Church	Oct. 9, 2010	9
Squier Park	DeLaSalle High School	Oct. 19, 2010	10
Ivanhoe	Ivanhoe Neighborhood Council	Oct. 23, 2010	85
Blue Hills	Blue Hills Neighborhood Assn.	Oct. 23, 2010	80
Brush Creek Community Partners	Midwest Research Institute	Nov. 5, 2010	20
Oak Park	Brush Creek Community Center		N/A
Crestwood	TBD		N/A
Rockhill Homes	TBD		N/A
Country Side	Minsky's		N/A
Hyde Park	Central Presbyterian Church		N/A
49/63 Coalition	Rockhurst Community Center		N/A
Rockhill Crest	TBD		N/A
Ivanhoe	Ivanhoe Neighborhood Council	Feb. 25, 2012	30

*Neighborhood Meeting have continued.
Table to be updated in future releases of this report.*

3.3.2.6.4 *Faith Communities*

The primary churches in the Demonstration Project area represent important community hubs. KCP&L worked with these churches to educate their membership about SmartGrid initiatives to build awareness and encourage participation in the project. A designated KCP&L liaison worked with the large churches within the Demonstration Project area to communicate recent news and to educate leaders and residents about the project's components and benefits. In addition, KCP&L developed content appropriate for church displays and for publication in church bulletins.

3.3.2.6.5 *Schools*

The Green Impact Zone is home to three schools, and there are several more in the broader Demonstration Project area. Schools are excellent communication/education vehicles for both children and parents. KCP&L worked with the Kansas City, Missouri School District and University of Missouri-Kansas City to create a curriculum module to teach students about the Smart Grid, and its role in energy and energy efficiency. In addition to engaging students, school-based outreach reached parents, grandparents, neighbors, etc. and built a stronger sense of community around the Demonstration Project area. Students were able to assist in making energy improvements while learning about the benefits of energy efficiency.

Table 3-14: Schedule of School Events

School	Event	Date
Paseo High School	You & Sustainability	Dec. 4, 2010
Martin City Middle School	Project Living Proof Tour	June 3, 2011
Paseo High School	Information Session and Tour	Feb. 17, 2012
Grandview High School	Project Living Proof Tour	Nov. 7, 2012
Paseo High School/UMKC	Project Living Proof Tour	Nov. 19, 2012
Paseo High School	MySmart Solar Kick-off Event	Nov. 19, 2012

*School initiatives continue.
Table to be updated in future releases of this report.*

3.3.2.7 Consumer Advocate Interaction

Throughout the KCP&L SmartGrid Demonstration Project implementation, a number of paid and unpaid advocates were utilized to help spread information to the consumer.

3.3.2.7.1 KCP&L Employees

With the Demonstration Project, KCP&L had the unique opportunity to utilize the company's 3,600 employees as SmartGrid ambassadors. As media coverage and interest of the project in the broader service territory increased, employees were asked by friends, family and neighbors about SmartGrid. Starting in 2010 and continuing throughout the project, KCP&L made Demonstration Project updates a priority for internal employee communications. The project has been prominently featured in the employee newsletter, *The Source*, as well as in the daily e-Source updates, Leadership Link videos and at the managers Leadership Forum. In addition, KCP&L has a number of employees who live within the Demonstration Project area. These employees were contacted about being vocal advocates for the Demonstration Project within their neighborhoods. KCP&L created an employee volunteer program specifically for the Demonstration Project to enhance education, promote programs, install products, weatherize homes, etc. These efforts demonstrated KCP&L's commitment to the Green Impact Zone and its residents in a highly visible manner.

3.3.2.7.2 Green Impact Zone Staff

Much of the person-to-person interaction with residents occurred through the staff of the Green Impact Zone. KCP&L's project outreach coordinator managed these relationships to ensure that the Green Impact Zone team had the latest information about SmartGrid initiatives and was prepared to answer questions or to direct customers to additional KCP&L resources. In addition, KCP&L provided ongoing training to Green Impact Zone ambassadors about SmartGrid and maintained regular communication to ensure that education and outreach goals were achieved.

3.3.2.7.3 Ambassadors

In addition to the Green Impact Zone staff, much of the direct customer interaction within the Green Impact Zone portion of the Demonstration Project area occurred through community organizers known as ambassadors. Residents of the Green Impact Zone were recruited to be ambassadors and served as project spokespeople responsible for increasing awareness of SmartGrid and its benefits. They served as a resource for residents by providing them with information and updates on the Demonstration Project. KCP&L worked with the Green Impact Zone to recruit and train ambassadors and had on-going interaction to ensure education and outreach goals were achieved.

3.3.2.7.4 SmartGrid Office

In addition to all of the integrated ongoing channels outlined as part of the public education and outreach efforts, KCP&L wanted to be able to interact face-to-face with customers on a daily basis within the Demonstration Project area. KCP&L established a SmartGrid office within the Green Impact Zone offices at 4600 Paseo. In addition to greater customer interaction, having a KCP&L office staffed by SmartGrid team members within the Green Impact Zone strengthened communication with the Green Impact Zone team.

3.3.2.7.5 SmartGrid Customer Service Representatives

KCP&L hired and trained three dedicated customer service representatives to serve as the SmartGrid support team. These individuals were the first point of contact for customers who have questions, need additional information or want to sign up for SmartGrid products/services. In addition, having a dedicated team improved continuity and message consistency. The SmartGrid support team could be reached via dedicated phone numbers and a dedicated e-mail address.

3.3.3 KCP&L Employees

The project team utilized various forms of internal communication to educate KCP&L employees about the Smart Grid Demonstration Project and keep them informed about its progress.

3.3.3.1 Employee Newsletter (The Source)

The Source is a newsletter published for employees and retirees. The publication features articles about the company and its employees that foster a culture of collaboration, reinforce the values of the Guiding Principles, increase employee engagement, educate employees about company projects and initiatives and provide information that helps employees perform better at their jobs. It is distributed on a monthly basis. The Smart Grid Demonstration Project was featured in *The Source* on several occasions, as shown in Table 3-15.

Table 3-15: The Source Articles

Initiative	Date
This Grant Will Help Map Our Future	Dec 2009
KCP&L's SmartGrid Update	May 2010
KCP&L's SmartGrid	July/Aug 2010
New KCP&L SmartGrid Customer Program Launches	Oct 2010
Smart Answers to SmartGrid Questions	Nov 2010
Employees Keep SmartGrid On Track	March 2012
Our "Top-To-Bottom" SmartGrid Model Leads The Industry	Sept. 2012

*Employee communication initiatives continue.
Table to be updated in future releases of this report.*

3.3.3.2 E-Source

The Source e-News Update, distributed each Tuesday and Friday through e-mail, is KCP&L's internal electronic newsletter. The publication's goal is to communicate pertinent information to all employees in a timely and effective manner. Community involvement, news from throughout the service territory, meetings, upcoming company initiatives, training and safety information are commonly included in the *e-News Update*. The Smart Grid Demonstration Project was featured in *E-Source* on several occasions, as shown in Table 3-16.

Table 3-16: The E-Source Articles

Initiative	Date
SmartGrid Comes to Leadership Link	Oct 8, 2010
SmartGrid Meter Rollout Has Begun	Oct 26, 2010
A Battery-Powered Substation?	May 15, 2012
KCP&L Opens Innovation Park to Promote SmartGrid	Oct. 12, 2012

*Employee communication initiatives continue.
Table to be updated in future releases of this report.*

3.3.3.3 Employee Communications via TV Monitors, e-Mail, and Employee Meetings

The Smart Grid Demonstration Project was featured in other employee communications on several occasions, as shown in Table 3-17.

Table 3-17: Other Employee SmartGrid Communications

Initiative	Outlet	Date
KCP&L SmartGrid Demonstration Project	IT Briefing	Oct. 05, 2009
KCP&L SmartGrid Demonstration Project - IT Priority Requirements	IT Briefing	Oct. 16, 2009
SmartGrid Important Announcement	Internal Email	Nov 24, 2009
KCP&L SmartGrid Briefing	T&D SRS Team	Jan. 06, 2010
Customer Value Proposition	Presentation	July 28, 2010
SmartGrid Support Team Training	Presentation	Sept 13, 2010
SmartGrid Resident Employees' Lunch	1KC Place	Sept 14, 2010
Afternoon of Sharing	1KC Auditorium	Sept 27, 2010
SmartGrid Project Email to All Employees	Internal Email	Sept 07, 2010

*Employee communication initiatives continue.
Table to be updated in future releases of this report.*

3.3.3.4 Leadership Link Videos

During 2009 and 2010 KCP&L management produced Leadership Link, a series of short informational videos, designed to educate employees on current company initiatives and emerging industry trends. The Smart Grid Demonstration Project was featured in several Leadership Link videos', as shown in Table 3-18.

Table 3-18: Leadership Link Videos

Topic	Featured Management Team Member	Date
SmartGrid	Mike Deggendorf, Sr. VP Delivery	2009
Benefits of the SmartGrid Demonstration Project	Steve Gilkey, Sr. Dir., T & D Engr. & Planning	2010
Why the SmartGrid Project is in the Urban Core	Steve Gilkey, Sr. Dir., T & D Engr. & Planning	2010
SmartGrid Project Update	Steve Gilkey, Sr. Director, T & D Engineering	2010
Understanding SmartGrid	Bill Menge, Director SmartGrid	2010
Understanding SmartGrid (SmartEnd-Use)	Gail Allen, Sr. Mgr. Customer Solutions	2010
Understanding SmartGrid (Education & Outreach)	Paul Snider, Sr. Mgr. Government Affairs	2010
Understanding SmartGrid (SmartSub./Dist./Gen.)	Scott Grafelman, Mgr. Asset Mgmt. & Planning	2010
Understanding SmartGrid (SmartMeter)	Vicki Barszczak, Mgr. Mtr. Reading & Field Svc.	2010

3.3.3.5 SmartGrid Snippets

During the summer of 2012, the Smart Grid Demonstration Project team published a project-specific newsletter, SmartGrid Snippets, on a weekly basis. The SmartGrid Snippets communicated updates for each of the sub-projects, as well as key milestones, resolved issues, and new issues for the overall project.

3.3.3.6 SmartGrid Project Sponsor Team Meetings

Regular SmartGrid Project Sponsor Team meetings were conducted as a component of the comprehensive Project Management Plan executed by the project PMO. The SmartGrid Project Sponsor Team is comprised of the Project Director and key KCP&L executives. The Project Director and PMO staff conduct the briefings that cover overall project progress; address key strategic, operational, and financial issues; provide strategic guidance; and address other issues escalated by the PMO. These regular briefings help ensure that the KCP&L project sponsors are engaged and informed of project status on a continual basis.

3.3.3.7 Executive Management Briefings

In addition to the SmartGrid Project Sponsor Team meetings, the PMO had provided periodic SmartGrid Project updates and technology briefings to KCP&L Board of Directors and executive leadership teams. The following table provides a listing of these SmartGrid Project briefings and their respective audiences.

Table 3-19: Executive Management Briefings

Initiative	Outlet	Date
KCP&L SmartGrid Demonstration Project - Executive Review	Presentation	Dec. 09,2009
Senior Strategy Team Update	Presentation	April 27, 2010
Officers' Team Meeting	Presentation	Aug. 23, 2010
Executive One-on-One Updates	Presentation	Numerous
Vice President Staff Meetings	Presentation	Numerous
Board of Directors Meeting	Presentation	May 1, 2012
Executive Technology Tour & Overview	Innovation Park Tour	Nov. 27, 2012

*Management project briefings continue.
Table to be updated in future releases of this report.*

3.3.4 State Agencies, Legislators and Regulators

One of KCP&L's education and education objectives with the SmartGrid Demonstration Project was to transfer its knowledge, experience, and learning to state agencies, legislators and regulators. Table 3-20 provides a listing of SmartGrid Project briefings made to and the leader of these respective audiences. The following subsections describe additional communication channels that were used to communicate project experiences and learning more broadly to the respective agency staff.

Table 3-20: State Agency, Legislator and Regulator Briefings

Topics	Group	Date
KCP&L SmartGrid Project Overview	KS House Energy & Utility Committee	Jan. 25, 2011
KCP&L Smart Grid Demonstration Project	Citizens Utility Ratepayer Board	April 13, 2011
SmartGrid Vision & Strategic Objectives SmartGrid Project Overview & Project Area Customer Engagement & Education Project Components & Timeline	MO Commissioners	Sept. 07, 2011
KCP&L Smart Grid Demonstration Project	MO Public Service Commission SmartGrid Workshop	Nov. 29, 2011
Project Status Update	Kansas Corporation Commission Open Meeting	Feb. 29, 2012
SmartGrid Vision & Strategic Objectives SmartGrid Project Overview & Project Area Project Components & Timeline	KS House Energy & Utility Committee	March 02, 2012
SmartGrid Project Overview SmartGrid Education & Outreach Project Accomplishments & Milestones	KS House Energy & Environment Committee	Feb. 07, 2013
Project Status Update	MO Public Service Commission Agenda Session	March 27, 2013

*Project briefings continue.
Table to be updated in future releases of this report.*

3.3.4.1 State Regulatory Commission Proceedings

KCP&L's retail operations are regulated by both the Missouri Public Service Commission (MPSC) and the Kansas Corporation Commission (KCC). As such, KCP&L participates in any formal proceedings initiated by or with either regulatory body. The future Smart Grid is being discussed in a variety of proceedings. KCP&L will continue to participate and provide appropriate input to all future proceedings regarding the Smart Grid. The following subsections summarize some Commission proceedings during the course of the project that have directly involved Smart Grid topics.

3.3.4.1.1 MPSC PURPA Considerations Required by EISA

On December 19, 2007, the Energy Independence and Security Act of 2007 ("EISA") was signed into law, requiring state utility commissions to consider the standards set out in the EISA, including Smart Grid. On December 17, 2008 the MPSC established the workshops to do so. The docket opened for Smart Grid consideration was EW-2009-0292. Since establishment of this docket, KCP&L responded to requests for information and participated in a workshop on May 18, 2010 presenting information regarding its SmartGrid Demonstration Project. KCP&L also participated in a second MPSC-sponsored workshop that

included Smart Grid vendors on June 28 and June 29, 2010. KCP&L will continue to participate in this docket until its completion.

*This docket has concluded.
Discussion will be updated in future releases of this report.*

3.3.4.1.2 KCC PURPA Considerations Required by EISA

On December 19, 2008, the KCC opened Docket No. 09-GIME-360-GIE for the purpose of investigating the standards as directed by EISA. KCP&L supplied comments regarding the standards on January 30, 2009. On September 18, 2009, KCP&L participated in the KCC Smart Grid roundtable. On December 14, 2009, the KCC closed this docket, electing not to adopt the EISA Smart Grid standards.

3.3.4.1.3 MPSC Integrated Resource Planning (IRP) Rulemaking

On May 15, 2009, the MPSC opened Docket No. EW-2009-0415 for the purpose of conducting workshops and providing a repository for work done in conjunction with rewriting the commission rules and procedures related to the IRP that each utility must conduct. Workshops were held and KCP&L participated in those workshops. On March 10, 2010, the MPSC opened a rulemaking case, EX-2010-0254 and subsequently published its IRP Proposed Amendment in the Missouri Register on December 1, 2010. Comments are to be provided to the MPSC by January 3, 2011, and a Public Hearing is scheduled for January 6, 2011. The rule as proposed includes a provision requiring utilities to address “contemporary issues” which are intended to include Smart Grid functions in future integrated resource plans developed by all Missouri utilities.

*The IRP process continues.
Discussion will be updated in future releases of this report.*

3.3.4.2 MO and KS SmartGrid Stakeholder Groups

Because several aspects of the SmartGrid Demonstration Project require MPSC approvals, KCP&L initiated communication with various Missouri Smart Grid stakeholders to create an informal group. The purpose of this group is to inform relevant parties about the SmartGrid Demonstration Project and to solicit input from them.

The members of the stakeholder group include representatives of the MPSC Staff, Office of Public Counsel, and Missouri Department of Natural Resources. On July 23, 2010, the initial meeting was held with the Missouri SmartGrid stakeholder group to introduce team members and give an overview of the SmartGrid Demonstration Project. The following topics were discussed in the initial meeting:

- Smart Grid Vision and SmartGrid Demonstration Project Overview
- SmartGrid Demonstration Project Technology and Interoperability
- The Community and Our Customers
- The Customer Value Proposition
- SmartGrid Demonstration Project Timelines
- How We Continue to Collaborate

On September 20, 2010, another meeting was held with the MO SmartGrid Stakeholder group to specifically discuss the KCP&L SmartGrid Demonstration Project customer communication plan.

The idea of SmartGrid Stakeholder Group was so well received by the MO Stakeholders and since knowing that any future system-wide adoption of SmartGrid technologies may be reviewed by both the MO and KS commissions, KCP&L initiated a similar informal SmartGrid stakeholder group with the KCC

staff and other KS stakeholder groups. Table 3-21 provides a listing of the periodic stakeholder meetings that occurred to discuss technology choices, evaluation plans, customer programs, customer service issues and status updates.

Table 3-21: Stakeholder Project Update Meetings

Topic	Group	Date
Initial SmartGrid Project Overview	MO Stakeholders	July 23, 2010
Project Customer Communication Plan	MO Stakeholders	Sept. 20, 2010
SmartGrid Deployment Status	MO Stakeholder	Feb 24, 2011
RF Technical Overview & Selection	KS Stakeholder	March 30, 2011
Grid Systems & Technology Evaluation Strategy		
Smart End-Use Program Evaluation Strategy		
Project Status Update	MO Stakeholder	June 27, 2011
Metrics & Benefits Plan Summary	KS Stakeholder	July 15, 2011
Customer Product Road Map		
Distribution & Substation	MO Stakeholders	Aug. 26, 2011
Project Component Overview	KS Stakeholders	Aug. 26, 2011
SmartGrid Vision & Strategic Objectives	MO Commissioners	Sept. 07, 2011
SmartGrid Project Overview & Project Area		
Customer Engagement & Education		
Project Components & Timeline		
Project Status Update	MO Stakeholder	Oct. 21, 2011
Customer Engagement & Education	KS Stakeholder	Nov. 04, 2011
TOU Rate Design		
Solar Updates		
Project Status Update	MO Stakeholder	Jan. 30, 2012
Project Status Update	MO Stakeholder	April 30, 2012
Solar & EV Charging Selection	KS Stakeholder	May 15, 2012
TOU & Grid Battery Update		
Project Status Update	MO Stakeholder	July 26, 2012
SmartGrid Architecture Overview	KS Stakeholder	Aug. 09, 2012
SmartGrid Integration Road Map		
Project Status Update	MO Stakeholder	Nov. 02, 2012
SmartGrid Innovation Park & Ribbon Cutting	KS Stakeholder	Nov. 09, 2012
Project Status Update	MO Stakeholder	April 16, 2013
Interoperability Testing Overview	KS Stakeholder	April 19, 2013
Product Enrollment and TOU Stats		
DOE Financial Audit Results		
Project Status Update	MO Stakeholder	July 26, 2013
Integration & Interoperability Testing Update	KS Stakeholder	Aug. 19, 2013
SmartGrid Customer Products		
Grid Connected Battery		

*Stakeholder briefings continue.
Table to be updated in future releases of this report.*

3.3.4.3 MO and KS Commission Staff

The MPSC and KCC each received separate DOE funding to support additional Smart Grid staff and staff education. In addition to the more organized interactions with the commission described in the previous section, KCP&L invited both Missouri and Kansas Smart Grid staff to participate in several Demonstration Project design and knowledge transfer workshops and meetings. In addition to the regular SmartGrid Stakeholder meetings the MPSC and KCC staffs participated in the following project opportunities.

- KCP&L hosted a “Day of Sharing” on January 28, 2010 with the Green Impact Zone, which both the MPSC and KCC Smart Grid staff attended. They learned about the challenges and opportunities specific to the Green Impact Zone.
- On February 10 and 11, 2010, KCP&L hosted a Smart Grid technical conference with project vendor partners. Both the MPSC and KCC staffs were represented and were able to ask questions and broaden their understanding of the interdependencies the project vendors were working through.
- In October 2010, EPRI conducted a series of Smart Grid use case workshops with KCP&L subject matter experts. The Commission Smart Grid staff was represented at several of the sessions and was able to ask questions and broaden their understanding of the use case process and how it would be used to document the project interoperability requirements.

*Commission Staff communications continue.
Listing to be updated in future releases of this report.*

3.3.5 **Electric Utilities and Smart Grid Industry**

Another of KCP&L’s education and education responsibilities with the SmartGrid Demonstration Project was to transfer its project knowledge, experience, and learning to other utilities and the Smart Grid industry as a whole. The following sections describe some to the communications channels that were used to meet this requirement.

3.3.5.1 EPRI’s Smart Grid Demonstration Project Participation

As a member of EPRI’s five-year Smart Grid demonstration project, KCP&L’s technology transfer activities were coordinated through EPRI’s formalized Smart Grid demonstration project. Specifically, EPRI coordinated the sharing of field results, lessons learned, architectural challenges, issues impacting standards, key technology gaps and useful tools to help interoperability of Smart Grid technologies and systems related to the project. In addition, detailed project information was communicated via EPRI’s Smart Grid resource center (www.smartgrid.epri.com) and additional technology transfer activities including workshops, webcasts and periodic publications. The workshops included presentations on status of field demonstrations, lessons learned to date, architectural challenges, issues impacting standards and common interest areas to explore. Technical summaries in the form of presentations and white papers/articles were prepared for public dissemination. These publications included a synthesis of contributions to standards bodies and common messages to deliver to industry and public entities such as state and federal agencies.

*The EPRI SmartGrid Demonstration Project continues.
EPRI communications regarding the KCPL project will be provided in future releases of this report.*

3.3.5.2 Technical Project Website

KCP&L created an industry focused Demonstration Project website as an extension of its customer focused website, www.kcplsmartgrid.com/industry-resources. This website was created in collaboration with the project partners, and allowed agencies, legislators, regulators, other utilities and the Smart Grid industry as a whole to remain abreast of the Demonstration Project.

Figure 3-21: www.kcplsmartgrid.com/industry-resources Page Screenshot



3.3.5.3 Technical Publications

One of the most effective ways to transfer knowledge to a diverse audience is through technical publications. The publications, listed below, were prepared for public dissemination throughout the life of the SmartGrid Demonstration Project, and they included a combination of contributions to standards bodies and industry publications.

Table 3-22: Technical Publications

Title	Publication	Date
Wired for Success	Transmission & Distribution World	April 2012

*Project communication initiatives continue.
Table to be updated in future releases of this report.*

3.3.5.4 Industry Conferences

In addition to published documents, KCP&L sought to transfer knowledge and experience to industry groups through presentations at industry conferences. The presentations listed in the following table included content on project status, challenges faced, specific technical topics, interoperability issues or lessons learned.

Table 3-23: Industry Conference Presentations

Topics	Group	Date
KCP&L SmartGrid Overview	Mid-American Regulatory Conference	June 8, 2010
KCP&L SmartGrid Pilot and Energy Optimizer Program	Kansas Energy Conference 2010	Oct. 12, 2010
Business Transformations & The Smart Grid	GridWeek 2010	Oct. 18-21, 2010
Developing a SmartSubstation Architecture for the SmartGrid	GridWeek 2010	Oct. 18-21, 2010
Journey to Quality Through Automation Evolution	Galvin Electricity Initiative Conference	Dec. 2010
KCP&L SmartGrid	A&WMA-Midwest Section Annual Environmental Conference	Jan. 19, 2011
KCP&L SmartSubstation Demo - A Partnership with Siemens	DistribuTECH 2011	Feb. 2, 2011
From the Meter to the Customer – KCP&L’s SmartGrid Project Focuses On More Than The Technology	2011 Customer Service Conference & Exposition	April 4, 2011
KCP&L Smart Grid Demonstration Project	Distribution Automation 2011 Conference	April 28, 2011
Kansas City Power & Light’s End-to-End SmartGrid Demonstration	2011 Landis+Gyr Exchange User Conference	May 5, 2011
Kansas City Power & Light’s End-to-End SmartGrid Demonstration	Honeywell User Group Conference	June 5, 2011
KCP&L Smart Grid Demonstration Project	Siemens Energy Policy Panel	Sept. 13, 2011
KCP&L Smart Grid Demonstration Project	GridWeek 2011	Sept. 14, 2011
SmartGrid Demo and Home Area Networks	T&D World/CIGRE Game Changers Conference	Nov. 16, 2011

Topics	Group	Date
Layered Distribution Automation and KCP&L's SmartGrid Demo Project	Electric Light & Power Executive Conference	Jan. 22, 2012
KCP&L Smart Grid Demonstration Project	DistribuTECH 2012	January 24, 2012
From Enrollment to Engagement: A Roadmap to Reaching Your Customers	Smart Grid Customer Interaction Summit	April 19, 2012
Utilities and Behavioral Science: Creating Meaningful Consumer Engagement	2012 Smart Grid RoadShow	April 23-25, 2012
KCP&L SmartGrid Update	2012 Landis+Gyr Exchange User Conference	April 25, 2012
KCP&L Smart Grid Demonstration Project	2012 Sustainable Housing Conference	Sept. 20, 2012
KCP&L Smart Grid Demonstration Project	SGCC Peer Connect:	Sept. 25, 2012
KCP&L Smart Grid Demonstration Project	2012 Kansas Energy Conference	Sept. 26, 2012
KCP&L Smart Grid Demonstration Project	GridWeek 2012	Oct. 4, 2012
The Future of Energy and Creating a Sustainable Community	Sustainability Forum	Oct. 10, 2012
KCP&L Smart Grid Demonstration Project	OATI User Group Conference	Oct. 17, 2012
KCP&L Smart Grid Demonstration Project	Midwest Energy Policy Conference	Oct. 25, 2012
KCP&L Smart Grid Demonstration Project	CIGRE Grid of the Future Symposium	Oct. 29, 2012
Deploying a Distribution Management System in a Pilot Project	Minnesota Power Systems Conference	Nov. 7, 2012
Demonstrating and Uncovering the Benefits of a State-of-the-art Next Generation Smart Distribution System	DistribuTECH 2013	Jan. 29, 2013
Pushing the Envelope on Substation Automation: KCP&L's End-to-End Smart Substation and Smart Distribution Initiatives	DistribuTECH 2013	Jan. 29, 2013
KCP&L's End-to-end Smart Grid Demonstration Pushes the DR Event Messaging Standards Envelope	DistribuTECH 2013	Jan. 30, 2013
Innovative Methods and Solutions Drive KCP&L's End-to-end Smart Grid Program	DistribuTECH 2013	Jan. 30, 2013
Kansas City Power & Light: Advanced Distribution Automation to Deliver Electricity More Reliably and Efficiently	DistribuTECH 2013	Jan. 30, 2013
Lessons from the Field: Consumer Engagement is a Journey, Not A Destination	DistribuTECH 2013	Jan. 30, 2013
Success Stories in Integrating New Customer-facing Technologies	DistribuTECH 2013	Jan. 30, 2013
Priming the Pump: What's Working and Delivering Value from the Recovery Act - PANEL	DistribuTECH 2013	Jan. 30, 2013
Greening the Grid with Smart Generation: Small-scale Renewable Integration and Sustainability Initiatives at KCP&L	DistribuTECH 2013	Jan. 31, 2013
SmartGrid Demo Project with Focus on Communications	Mid Central UTC Annual Meeting	March 26, 2013
The Power of Web Portals	2013 CS Week	May 2, 2013
Advancements in Distribution Automation to Deliver Electricity More Reliably and Efficiently: A Kansas City Power & Light Case Study	UTC Telecom 2013	May 15, 2013
Integration of Variable Generation Resources - A Distribution Grid Perspective	OATI User Group Conference	Oct. 8, 2013

Topics	Group	Date
How Customer Engagement is Transforming Utility Operations	DistribuTECH 2014	Jan. 28, 2014
Pushing the Envelope on Substation Automation: Part2 - KCP&L's End-to-end Smart Substation and Smart Distribution Initiatives	DistribuTECH 2014	Jan. 28, 2014
Energy Storage: Technologies, Operations and Value Propositions	DistribuTECH 2014	Jan. 29, 2014
Integration of Smart Substations in Advance DMS: A Case for Integrated Self-healing Applications	DistribuTECH 2014	Jan. 30, 2014
Advanced Metering Insights: KCP&L's Evolution to AMI/MDM-based Smart Metering	DistribuTECH 2014	Jan. 30, 2014

*Industry conference participation continues.
Table to be updated in future releases of this report.*

3.3.5.5 Technical Education

In addition, KCP&L sought to transfer knowledge and experience through technical training sessions, such as workshops and webinars. These sessions included content on project status, challenges faced, specific technical topics, interoperability issues or lessons learned.

Table 3-24: Industry Webinars

Topics	Group	Date
KCP&L Smart Grid Demonstration Project	EPRI Peer Review Webcast	Feb. 3, 2010
Smart Grid Demonstration Project	EPRI Advisory Meeting	Sept. 13, 2010
KCP&L Smart Grid Demonstration Project	EPRI Project Update	Oct. 25, 2010
DOE Project Kick-Off Meeting	DOE Meeting	Jan 6, 2011
From the Meter to the Customer – KCP&L’s SmartGrid Project Focuses On More Than The Technology	Edison Electric Institute	March 21, 2011
KCP&L Smart Grid Demonstration Project	National League of Cities	June 3, 2011
KCP&L Smart Grid Demonstration Project	Oklahoma Gas & Electric SmartGrid Team	July 12, 2011
KCP&L Smart Grid Demonstration Project	Partnership for Emergency Planning	July 21, 2011
Software Giants and the Home Area Network	Game Changers	Sept. 21, 2011
KCP&L Smart Grid Demonstration Project	EPRI Smart Grid Demonstration and Public Action Group Meetings	Oct. 18, 2011
Online Portal and In-home Displays Offer an Experience Beyond Technology	Chartwell EMACS 2011	Oct. 26-28, 2011
KCP&L Smart Grid Demonstration Project	2011 APPA Facilities Drive-In Workshop	Nov. 16, 2011
KCP&L Smart Grid Demonstration Project	EPRI Deep-Dive Webcast	Nov. 17, 2011
The Consumer Journey: Leveraging Behavioral Science for Persistent Consumer Engagement	Smart Grid Newsletter Webinar	June 7, 2012
KCP&L Green Impact Zone SmartGrid Demonstration Project	DOE Peer-to-Peer Meetings	June 8, 2012
KCP&L Smart Grid Demonstration Project – Case Study Brief	EPRI Four-Year Update	July 23, 2012
2012 DOE Project Review	DOE Visit	Aug. 20, 2012
From Enrollment to Engagement: A Roadmap to Reaching Your Customers	Chartwell EMACS 2012	Oct. 11, 2012
KCP&L SmartGrid Demonstration Project	DOE/NRECA Midwest Peer-to-Peer	Dec. 12, 2012
Incentivizing Off Peak Programs	Chartwell Webinar	Dec. 13, 2012
KCP&L SmartGrid Demonstration Project Deep-Dive Webcast	EPRI Deep Dive	Feb. 21, 2013
Pricing/Rates: Customer Communications	Chartwell EMACS 2013	Oct. 8-11, 2013

*Project communication initiatives continue.
Table to be updated in future releases of this report.*

3.3.5.6 Local Business and Industry Association Presentations

In addition, KCP&L sought to inform and educate local business and industry organizations on Smart Grid concepts in general and provide an overview of the KCP&L demonstration project and how they, our customers, will benefit from the knowledge and experience KCP&L has gained from the project.

Table 3-25: Local Business and Industry Association Presentations

Topics	Group	Date
Introduction to KCP&L's Smart Grid Demonstration Project for the Green Impact Zone	Update to Mid America Regional Council	Aug. 17, 2009
KCP&L Smart Grid Demonstration Project	Green Impact Zone Key Leaders	Sept. 14, 2010
KCP&L Smart Grid Demonstration Project	Rotary Australian Exchange	April 21, 2011
KCP&L Smart Grid Demonstration Project	Northeast Johnson County Chamber of Commerce	April 21, 2011
KCP&L Smart Grid Demonstration Project	Kansas City Area Development Council – Education Alliance	April 29, 2011
KCP&L SmartGrid Customer Education	Paseo High School	Feb. 17, 2012
KCP&L Smart Grid Demonstration Project	Kansas State University Advisory Board	March 28, 2012
SmartGrid Demo Project and Demo House Tour	Kansas State University – Electrical Engineering Grad Students	April 27, 2012
KCP&L Smart Grid Demonstration Project	Midwest Society of Professional Engineers	May 24, 2012
KCP&L Smart Grid Demonstration Project	IEEE Gold Affinity Group	June 14, 2012
KCP&L Smart Grid Demonstration Project	Sierra Club Meeting (at Anita Gorman Discover Center)	Aug. 7, 2012
KCP&L Smart Grid Demonstration Project	Going Live Celebration	Oct. 12, 2012
KCP&L Smart Grid Demonstration Project	Paseo High School	Nov. 19, 2012
KCP&L Green Impact Zone SmartGrid Demonstration Project	IEEE PES Conference	Feb. 25, 2013
KCP&L Smart Grid Demonstration Project	UMKC	April 13, 2013
KCP&L Smart Grid Demonstration Project	Brush Creek Corridor Planning and Development Forum	May 21, 2013
KCP&L Smart Grid Demonstration Project	Project Management Institute - Kansas City Chapter – PDD Conference	Sept. 30, 2013
KCP&L Smart Grid Demonstration Project	Union Station - Saturday Science Seminar	Oct. 12, 2013

*Project communication initiatives continue.
Table to be updated in future releases of this report.*

3.3.6 Targeted Education & Outreach Initiatives

3.3.6.1 AMI Education & Outreach

KCP&L teams from Public Affairs and Corporate Communications developed multiple channels to communicate with customers during the entire implementation process. Information was mailed to the customers approximately 60 days prior to the first meter install explaining the project and letting them know what to expect. One month prior to scheduled meter change out the customer received a post card reminding them about the coming change. Another card with additional metering information was mailed one week prior to installation. Lastly, individuals and businesses received a phone call two days prior to installation.

- **Smart Grid Residential Customer Letter Final – August 31, 2010.** Mailed to all customers (residential and commercial) in early September 2010. The SmartGrid Fact Sheet was included.
- **KCP&L Smart Grid Mailer Postcard (residential and commercial).** Mailed to customers approximately four weeks prior to smart meter installation.
- **Smart Grid Meter Installation Postcard.** Mailed to customers approximately one week prior to smart meter installation.
- **Smart Grid Welcome Kit** letter, Fact Sheet, Sorry We Missed You panel (if applicable), and Welcome Kit Booklet. Distributed to customer in person on day of meter exchange.
- **KCP&L Smart Grid Demonstration House fact sheet.** Copies available to visitors at the Demonstration House.
- **FAQ.** Available on the web and distributed at events, along with the fact sheet.

All communication directed customers to a project specific web site, e-mail address, and phone number to contact in the event they had questions or needed more information.

KCP&L created a dedicated Smart Grid Support Team to inform customers of the process and answer questions specific to the project. These employees were able to set appointments for installation and give customers timely answers to technology and implementation questions.

For a portion of the project area, on the day a customer's meter was changed, Ambassadors went door to door offering residents an informational Welcome kit and addressed customer concerns face-to-face. Meter installers also made contact with residents immediately prior to exchange.

3.3.6.2 Residential SmartEnd-Use Products

To be completed in future releases of this report.

3.3.6.3 Residential TOU Rates

To be completed in future releases of this report...

3.3.6.4 SmartGrid Demonstration House

In 2006, the Metropolitan Energy Center (www.kcenergy.org), with assistance from KCP&L, advanced the idea for Project Living Proof (PLP), a demonstration house, located at 917 Emanuel Cleaver II Blvd., to promote the development of sustainable communities by showcasing weatherization, landscaping, efficient appliances and other energy-efficient features.

KCP&L again invested in this project and the demonstration house by deploying existing and emerging renewable energy and energy management technologies. The demonstration house allowed KCP&L customers to experience the future of the energy and see first-hand the new MySmart tools and products available to customers in the SmartGrid project area.

- **Smart Meter.** The smart meter unlocked the benefits of the SmartGrid by enabling two-way communication between the utility and the customer. This provided real-time energy usage information for consumer products such as the MySmart Portal, MySmart Display and MySmart Network. It also allowed customers to receive price signals and participate in “time of use” and other rate plans options.
- **MySmart Portal.** Each customer with a smart meter had access to a customized website to view usage information and receive additional updates on energy saving options.
- **MySmart Display.** This portable energy management tool provided consumers with access to current electricity usage and bill information.
- **MySmart Thermostat** The programmable thermostat helped customers save energy and helped KCP&L control peak demands.
- **Rooftop Solar.** The Solar Photovoltaic (PV) system was able to produce 3.15 kWh of solar power on a sunny day. This system was connected to KCP&L’s SmartGrid enabling KCP&L to view and manage output from the panel. See Figure 3-22.
- **Battery Storage.** The battery backup could store up to 8 kWh of energy from the Solar PV system, which was discharged to offset energy use during peak demand. Stored energy and energy from the Solar PV system could also be sold back to the grid.
- **Electric Vehicle Charging Station.** The 110V Coulomb Technologies charging station complemented the overall theme of the SmartGrid experience. KCP&L installed 10 charging stations in the project area and another 11 throughout the metropolitan area.
- **Energy Efficiency Programs.** KCP&L showcased its full suite of energy efficiency programs to benefit customers.
- **Weatherization.** The demo house, built in 1911, contained exposed demonstrations of proper air sealing, insulation, window tightening and replacement.

Tours of the Demonstration House were offered during weekdays.

Figure 3-22: Rooftop PV Installation on Project Living Proof Demonstration House



Figure 3-23: Sunverge Unit Installation at Project Living Proof Demonstration House



3.3.6.5 SmartGrid Innovation Park

The KCP&L SmartGrid Innovation Park, located north of KCP&L's Midtown Substation, represented an innovative and operational aggregation of smart grid technologies and provided a unique educational opportunity for the public. "KCP&L is committed to this SmartGrid Demonstration Project as a way to learn new ways to reduce electricity delivery costs, enhance reliability and make Kansas City smarter about energy," said President and CEO Terry Bassham. "But we also want to share what we are learning, and this park is a great way for all of our customers to come and learn more about the smart grid."

Park visitors saw how KCP&L is enhancing the electric grid in Kansas City's urban core by viewing:

- An informational kiosk that explained KCP&L's entire Demonstration Project, including how power distribution is enhanced with smart grid technologies, the customer in-home experience, and the history of electric meters.
- A sophisticated, 1.0 MW-hour grid-connected lithium ion battery storage system, one of the largest of its kind in the country.
- A public EV charging station with dual level II ports.
- A ground-mounted 5.0 kW PV array, one of 8 project-funded PV arrays.
- A demonstration of KCP&L's new smart distribution management systems.

Figure 3-24: KCP&L's Smart Grid Innovation Park Site Layout

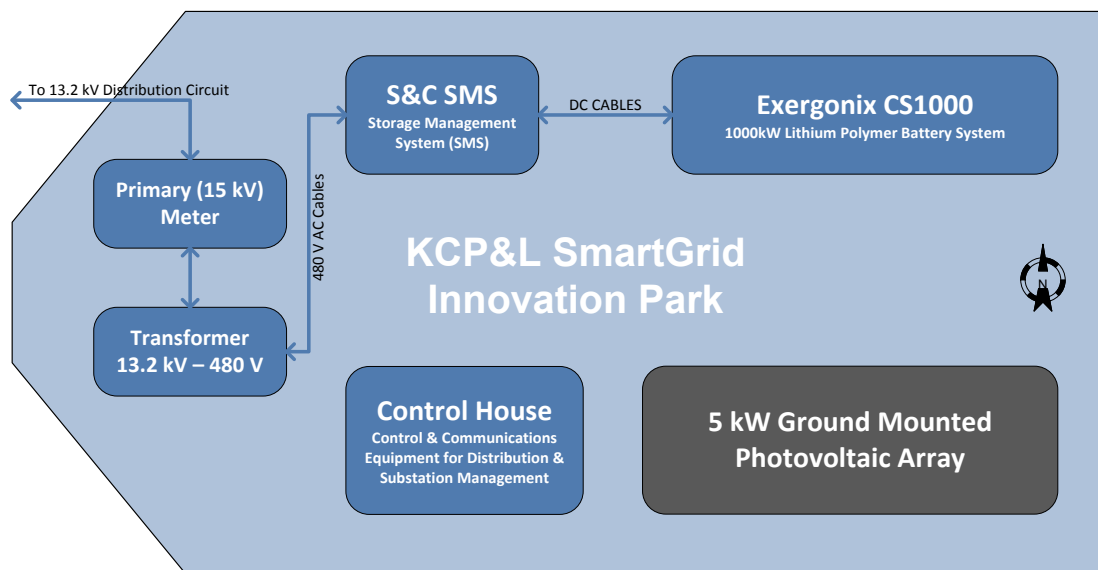


Figure 3-24 shows a layout of KCP&L's new Smart Grid Innovation Park. A ribbon cutting ceremony was held on October 12, 2012 to open the Innovation Park to the public. The event was attended by Congressman Emanuel Cleaver II, KCP&L CEO Terry Bassham, and about 100 other community leaders and representatives, along with reporters.

Figure 3-25: Battery Energy Storage System (BESS) at SmartGrid Innovation Park



Figure 3-26: 5 kW Photovoltaic Array at SmartGrid Innovation Park



Figure 3-27: Informational Kiosk at SmartGrid Innovation Park

3.3.7 Project Tours & Field Demonstrations

Hands-on training is often the most effective way to communicate with the target audience. During the Demonstration Project, project tours and field demonstrations provided an opportunity for the industry experts as well as the general public to get a first-hand look at SmartGrid possibilities.

3.3.7.1 SmartGrid Demonstration House Tour

As part of KCP&L's SmartGrid Demonstration Project, KCP&L was the lead sponsor of the Metropolitan Energy Center's Project Living Proof (PLP), an initiative that allowed KCP&L customers to experience the future of energy. PLP consisted of a demonstration house, located at 917 Emanuel Cleaver II Blvd., where visitors could see first-hand the new MySmart tools and products available to customers in the Demonstration Project area. The house facilitated communication by allowing customers to touch, feel, interact with and learn about Smart Meters, in-home displays, home area networking, hyper-efficient appliances and a PHEV charging station.

Table 3-26: Schedule of Demonstration House Tours

Tour	Date
MARC Tour	June 8, 2010
KCMO City Council and Key Staff Tour	June 11, 2010
Clean Energy Conference Attendees Tour	Oct. 20, 2010
KCP&L Board of Directors Tour	Oct. 25, 2010
Community Key Leaders Tour	Mar. 10, 2011
South Kansas City Chamber of Commerce Tour	April 27, 2011
Demonstration Home Grand Opening Tour	April 30, 2011

Tour	Date
Martin City Middle School	June 03, 2011
Kansas City Energy Future Tour	Nov. 09, 2011
Paseo High School Faculty and Staff Tour	Feb. 17, 2012
KCP&L Winning Culture Council Tour	March 30, 2012
Kansas State University Student Tour	April 27, 2012
Iatan IDEAL Partners Team Tour	April 30, 2012
South Kansas City Chamber of Commerce Tour	May 02, 2012
MPSC Staff Tour	June 26, 2012
KCP&L Intern Program Tour	June 29, 2012
KCP&L Board Member (Dr. David L. Bodde) Tour	July 19, 2012
SmartGrid Innovation Park Ribbon-Cutting Tour	Oct. 12, 2012
CIGRE Conference Attendees Tour	Oct. 30, 2012
Halloween Open House	Oct. 31, 2012
Grandview High School Green Tech Students Tour	Nov. 07, 2012
Paseo High School Students	Nov. 19, 2012
UMKC E-Save Team Tour	Nov. 19, 2012
KS State Representative (Tom Sloan) Tour	Nov. 28, 2012
Southtown Council's Leadership Tomorrow Tour	March 27, 2013
The Future of Energy – Communiversity Course	April 13, 2013
MPSC Summer Interns Tour	Aug. 01, 2013
Environmental Excellence Business Network (EEBN) Tour	Sept. 12, 2013
MPSC Staff Tour	Oct. 25, 2013

*Demonstration House tours continue.
Table to be updated in future releases of this report.*

3.3.7.2 SmartGrid Innovation Park Tour

This tour included a trip through the SmartGrid Innovation Park, where participants were able to see the DCADA system, a grid-connected battery, a solar generation installation, and an electric vehicle charging station associated with the SmartGrid Demonstration Project.

Table 3-27: Schedule of SmartGrid Innovation Park Events

Tour	Date
KCP&L Board Member (Dr. David L. Bodde) Tour	July 19, 2012
SmartGrid Innovation Park Ribbon Cutting Tours	Oct. 12, 2012
KCP&L DMS Team Tour	Oct. 12, 2012
CIGRE Conference Attendees Tour	Oct. 30, 2012
KCP&L Executive Management Tour	Nov. 27, 2012
KS State Representative (Tom Sloan) Tour	Nov. 28, 2012
Cerner Corporation Tour	Dec. 6, 2012
Mid-Central Utilities Telecom Council	March 26, 2013
MPSC Summer Interns Tour	Aug. 1, 2013
Environmental Excellence Business Network (EEBN) Tour	Sept. 12, 2013
MPSC Staff Tour	Oct. 25, 2013

*Innovation Park tours continue
Table to be updated in future releases of this report.*

3.3.7.3 Grid Management Systems Tour

These demonstrations show participants the back office side of the Demonstration Project. They were able to walk through the grid operations command center, and they learned about 'first responder' functions, the DMS and the DERM.

To be updated in future releases of this report

3.4 Operational Testing Results

To be completed in future releases of this report.

3.4.1 Automated Voltage and VAR Control

3.4.1.1 Integrated Volt/VAR Management

To be completed in future releases of this report.

3.4.2 Real-Time Load Transfer

3.4.2.1 Feeder Load Transfer (FLT)

To be completed in future releases of this report.

3.4.3 Automated Feeder and Line Switching

3.4.3.1 Fault Isolation and Service Restoration (FISR)

To be completed in future releases of this report.

3.4.4 Automated Islanding and Reconnection

3.4.4.1 Feeder Islanding with Grid Battery

To be completed in future releases of this report.

3.4.5 Diagnosis & Notification of Equipment Condition

3.4.5.1 Substation Protection Automation

To be completed in future releases of this report.

3.4.5.2 Asset Condition Monitoring

To be completed in future releases of this report.

3.4.5.3 Substation Hierarchical Control (DCADA)

To be completed in future releases of this report.

3.4.6 Real Time Load Measurement & Management

3.4.6.1 Automated Meter Reading (AMR)

To be completed in future releases of this report.

3.4.6.2 Remote Connect/Disconnect

To be completed in future releases of this report.

3.4.6.3 Outage Restoration

To be completed in future releases of this report.

3.4.6.4 Demand Response Events (DR)

To be completed in future releases of this report.

3.4.7 Customer Electricity Use Optimization (Information)

3.4.7.1 Historical Interval Usage Information (HEMP)

To be completed in future releases of this report.

3.4.7.2 In-Home Display (IHD)

To be completed in future releases of this report.

3.4.7.3 Home Area Network (HAN)

To be completed in future releases of this report.

3.4.7.4 Time-of-Use (TOU)

To be completed in future releases of this report.

3.4.8 Distributed Production of Energy

3.4.8.1 Distributed Roof-top Solar Generation (SDG)

To be completed in future releases of this report.

3.4.9 Storing Electricity for Later Use

If the Regional Demonstration contains an energy storage system, include information to demonstrate the performance of the energy storage system. Show measured or calculated technical, economic, and environmental health & safety (EHS) performance characteristics (Appendix A) from data collected and tests run to date based on, but not limited to, the approved MBRP.

To be completed in future releases of this report.

3.4.9.1 Electric Energy Time Shift

To be completed in future releases of this report.

3.4.9.2 Electric Supply Capacity

To be completed in future releases of this report.

3.4.9.3 T&D Upgrade Deferral

To be completed in future releases of this report.

3.4.9.4 Time-of-Use Energy Cost Management

To be completed in future releases of this report.

3.4.9.5 Electric Service Reliability

To be completed in future releases of this report.

3.4.9.6 Renewable Energy Time Shift

To be completed in future releases of this report.

3.4.9.7 PEV Charging (VCM)

To be completed in future releases of this report.

3.5 Metrics and Benefits Analysis

This section should describe the quantitative impact of Smart Grid technologies demonstrated relative to baseline and how those Smart Grid impacts translate to monetary benefits. This section should contain the following:

- Discuss impact metrics that were not captured in, or fell short of what was expected in, the approved MBRP.*
- Discuss any grid or non-grid connected benefits enabled to date both within and outside the DOE benefits framework based on, but not limited to, the approved MBRP (Table 2).*
- Show results of any ongoing benefits analysis. In the Final Technical Report, show final results of hypothetical/potential (for non grid-connected projects) or actual (for grid connected projects) benefits analysis.*

To be completed in future releases of this report.

3.5.1 Build Metrics

To be completed in future releases of this report.

3.5.2 Impact Metrics

To be completed in future releases of this report.

3.5.3 SmartGrid Computational Tool Analysis

To be completed in future releases of this report.

3.5.4 Energy Storage Computational Tool Analysis

To be completed in future releases of this report.

3.6 Stakeholder Feedback

If feasible, Recipients should include observations from various stakeholders (e.g., electric service providers, ratepayers, regulators, vendors) on how the Smart Grid project has impacted electric bills, economic development, environmental quality, security, safety, reliability, etc.

To be completed in future releases of this report.

This page intentionally blank.

4 Conclusions

To be completed in future releases of this report.

4.1 Performance Projections of Enterprise Deployment

Forecast or extrapolate the long term performance of the demonstration system from data collected to date.

To be completed in future releases of this report.

4.1.1 Smart Grid Functions

To be completed in future releases of this report.

4.1.2 Energy Storage Functions

To be completed in future releases of this report.

4.2 Technology Gaps

Identify where improvements in system performance, manufacturing processes, and/or component sourcing will impact these parameters.

To be completed in future releases of this report.

4.2.1 Interoperability

To be completed in future releases of this report.

4.2.2 Cyber Security

To be completed in future releases of this report.

4.2.3 Education & Outreach

To be completed in future releases of this report.

4.2.4 SmartMetering

To be completed in future releases of this report.

4.2.5 SmartEnd-Use

To be completed in future releases of this report.

4.2.6 SmartSubstation

To be completed in future releases of this report.

4.2.7 SmartDistribution

To be completed in future releases of this report.

4.2.8 SmartGeneration

To be completed in future releases of this report.

4.3 Lessons Learned and Best Practices

Provide a comprehensive discussion of the cumulative lessons learned (e.g., show a table in reverse date order where the latest lesson learned is listed first), and how they could be applied to improve performance and the overall cost/benefit relationship. Also discuss any best practices observed during the project that advance Smart Grid deployment.

To be completed in future releases of this report.

4.3.1 Interoperability

To be completed in future releases of this report.

4.3.2 Cyber Security

To be completed in future releases of this report.

4.3.3 Education & Outreach

To be completed in future releases of this report.

4.3.4 SmartMetering

To be completed in future releases of this report.

4.3.5 SmartEnd-Use

To be completed in future releases of this report.

4.3.6 SmartSubstation

To be completed in future releases of this report.

4.3.7 SmartDistribution

To be completed in future releases of this report.

4.3.8 SmartGeneration

To be completed in future releases of this report.

4.4 Project Impact on KCP&L's Future Plans for Smart Grid Deployment

Describe the project's impact on future plans for Smart Grid deployment

To be completed in future releases of this report.

5 Contacts

To be completed in future releases of this report.

This Page Intentionally Blank

6 References

- [1] KCP&L, *KCP&L Green Impact Zone SmartGrid Demonstration DOE-FOA-36 Grant Application*, 2009.
- [2] U.S. Department of Energy, *Guidebook for ARRA Smart Grid Program Metrics and Benefits*, 2010.
- [3] Burns & McDonnell, "Report on the IEC 61850 Communications Network," 2011.
- [4] E. Hedges and M. Olson, "Wired for Success," *T&D World*, April 2012.
- [5] KCP&L, *KCP&L Green Impact Zone SmartGrid Demonstration Metrics & Benefits Reporting Plan*, 2011.
- [6] KCP&L, *KCP&L Green Impact Zone SmartGrid Demonstration Interoperability Plan*, 2010.
- [7] NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2*, 2012.
- [8] GridWise Architecture Council, *GridWise Interoperability Context-Setting Framework*, 2008.
- [9] EPRI, "Guidelines for System Development using the IntelliGrid Methodology," 2008.
- [10] SGIP-CSWG, *DRAFT NISTIR 7628 Guidelines for Smart Grid Cyber Security*, 2010.
- [11] NIST, *NIST SGIP DRAFT SGAC Concept Whitepaper - Requirements Establishment for Getting to a Generic Smart Grid Conceptual Architecture*, 2010.
- [12] KCP&L, *KCP&L Green Impact Zone SmartGrid Demonstration Cyber Security Plan*, 2010.
- [13] *NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments*, 2012.
- [14] NIST, *NISTIR-7628 Smart Grid Cyber Security Strategy and Requirements*, 2010.
- [15] KCP&L, *KCP&L Green Impact Zone SmartGrid Demonstration Education & Outreach Plan*, 2010.
- [16] KCP&L, *KCP&L Green Impact Zone SmartGrid Demonstration Project Management Plan, Version 1.0*, 2010.
- [17] KCP&L, *KCP&L Green Impact Zone SmartGrid Demonstration Project Management Plan, Version 2.0*, 2011.
- [18] KCP&L, *KCP&L Green Impact Zone SmartGrid Demonstration Project Management Plan, Version 3.0*, 2012.
- [19] KCP&L, *KCP&L Green Impact Zone SmartGrid Demonstration Project Management Plan, Version 4.0*, 2013.
- [20] G. Allen, *KCP&L Distributed Generation - SolarPosition Paper*, 2013.
- [21] U.S. Department of Energy, *User Guide for the U.S. Department of Energy Smart Grid Computational Tool (SGCT), Version 2.0*, 2011.
- [22] U.S. Department of Energy, *ES Computational Tool (ESCT) Version 1.2 - User Guide*, 2012.
- [23] EPRI, "Enterprise Service Bus Implementation Profile (report #1018795)," 2009.
- [24] U.S. Department of Energy, National Energy Technology Laboratory, Funding Opportunity Number: DE-FOA-0000036, CFDA Number: 81.122 Electricity Delivery and Energy Reliability Research, Development and Analysis, *Financial Assistance Funding Opportunity Announcement*, 2009.
- [25] UCA International Users Group, [Online].
- [26] Burns & McDonnell, "KCP&L SmartGrid Demonstration Project Risk Assessment," 2011.
- [27] AMI-SEC Task Force (UCAIug), *Security Profile for Advanced Metering Infrastructure, Version 2.1*, 2012.
- [28] EPRI, *AEP Interoperability Test Plan: In Support of the AEP Ohio gridSMARTsm Demonstration Project*.
- [29] EPRI, *Kansas City Power and Light Company Smart Grid Host Site 2011 Progress Report*, 2012.

This Page Intentionally Blank

7 Abbreviations and Acronyms

ADA – Advanced Distribution Automation
AHE – AMI Head-End
AMI – Advanced Metering Infrastructure
AMR – Automated Meter Reading
AOS – Alexander Open Systems
BAC – Battery Automation Controller
BESS – Battery Energy Storage System
BMS – Building (Energy) Management System
CAD – Computer-Aided Dispatch
CID – Configured IED Description
CIM – Common Information Model
CIP – Critical Infrastructure Protection (NERC)
CIS – Customer Information System
CMEP – California Metering Exchange Protocol
CPHE – Customer Pilot Hosting Environment
CSWG – SGIP Cyber Security Working Group
CVR – Conservation Voltage Reduction
DA – Distribution Automation
DAC – Distribution Automation Controller
DAS – Data Acquisition System
DCADA – Distributed Control and Data Acquisition
DDC – Distribution Data Concentrator
DEMS – Distributed Energy Management System
DER – Distributed Energy Resource
DERM – Distributed Energy Resource Management
DG – Distributed Generation
DLC – Direct Load Control
DM – Distribution Management
DMAT – Data Mining and Analysis Tool
DMS – Distribution Management System
DNA – Distribution Network Analysis
DOE – Department of Energy
DR – Demand Response
D-SCADA – Distribution Supervisory Control and Data Acquisition
DSE – Data Synchronization Engine
DSPF – Distribution System Power Flow
DSSE – Distribution System State Estimator
DVC – Dynamic Voltage Control
EER – Enabled Energy Resource
EMS – Energy Management System
EPRI – Electric Power Research Institute
eRSTP – Enhanced Rapid Spanning Tree Protocol
ESB – Enterprise Service Bus
EV – Electric Vehicle
EVCS – Electric Vehicle Charge Station
EVSE – Electric Vehicle Supply Equipment
FAN – Field Area Network
FAT – Factory Acceptance Testing
FCI – Fault Current Indicator
FDIR – Fault Detection, Isolation and Restoration
FDP – Fiber Distribution Panels

FERC – Federal Energy Regulatory Commission
FISR – Fault Isolation and Service Restoration
FLOC – Fault Location
FLT – Feeder Load Transfer
FTE – Full Time Equivalent
GIS – Geographic Information System
GOOSE – Generic Object-Oriented Substation Event
GPE – Great Plains Energy
GWAC – GridWise Architecture Council
HAN – Home Area Network
HEMP – Home Energy Management Portal
HIS – Historical Information System
HMI – Human Machine Interface
IBEW – International Brotherhood of Electrical Workers
ICCP – Inter-Control Communications Protocol
IEC – International Electrotechnical Commission
IED – Intelligent Electronic Device
IEEE – Institute of Electrical and Electronics Engineers
IETF - Internet Engineering Task Force
IHD – In-Home Display
IMM – Information Model Management
IP – Internet Protocol
ISO – Independent System Operator
IVR – Integrated Voice Response
JMS – JAVA Messaging Service
KCC – Kansas Corporation Commission
KCP&L – Kansas City Power & Light
KCP&L-GMO – KCP&L Greater Missouri Operations Company
L+G – Landis + Gyr
LCS – Load Control Switch
LTC – Load Tap Changer
MARC – Mid-American Regional Council
MEC – Metropolitan Energy Center
MDM – Meter Data Management
MMS – Manufacturing Messaging Specification
MPLS – Multi-Protocol Label Switching
MQ – Message Queues
MPSC – Missouri Public Service Commission
MUDR – Metered Data Usage Repository
NERC – North American Electric Reliability Corporation
NRC – Nuclear Regulatory Commission
NIST – National Institute of Standards and Technology
NISTIR – NIST Interagency or Internal Reports
NIPP - U.S. National Infrastructure Protection Plan
NSPE – National Society of Professional Engineers
OASIS – Advancing Open Standards for the Information Society
OATI – Open Access Technology International
ODR – On-Demand Read
OMS – Outage Management System
OMSM – Outage Management Support Module
PAS – Power Automation System
PCS – Power Conditioning System
PCT – Programmable Communicating Thermostat
PESS – Premise Energy Storage System (battery)
PHEV – Plug-in Hybrid Electric Vehicle

PLC – Programmable Logic Controller
POA – Power Outage Analysis
PSV – Power Status Verification
PV – Photo Voltaic (Solar)
RDBMS – Relational Data Base Management System
REP - Resilient Ethernet Protocol
REST - Representational State Transfer
RSO – Remote Service Order
RSTP - Rapid Spanning Tree Protocol
RTAC - Real Time Automation Controller
RTO – Regional Transmission Organization
RTU – Remote Terminal Unit
RVA – Restoration Verification Analysis
SAAS – Software-As-A-Service
SAML – Security Assertion Markup Language
SAT – Site Acceptance Testing
SEL – Schweitzer Engineering Laboratory
SEP – Smart Energy Profile
SGAC – Smart Grid Architecture Committee
SGCT – Smart Grid Computational Tool
SGDG – Smart Grid Demonstration Grant
SGDP – SmartGrid Demonstration Project
SGIG – Smart Grid Investment Grant
SGIP – Smart Grid Interoperability Panel
SICAM – Siemens Integrated Control and Monitoring
SLPB – Superior Lithium Polymer Battery
SOA – Service-Oriented Architecture
SME – Subject Matter Expert
SMS – Storage Management System
SPN – Substation Protection Network
SPM – Switching Procedure Management
SPP – Southwest Power Pool
SSO – Single Sign-On
T&D – Transmission and Distribution
TOU – Time of Use
TPR – Technology Performance Report
TTM – Tunnel Text Message
UCAIug – UCA International Users Group
UI – User Interface
USABC – U.S. Advanced Battery Consortium
VCMS – Electric Vehicle Charge Management System
VEE – Validation, Estimation and Editing
VVC – Volt/VAR Control
WAN – Wide Area Network
WASA – Wide Area Situational Awareness
WC3 – World Wide Web Consortium
WS-I – OASIS Web Service Interoperability
XML – Extensible Markup Language

This Page Intentionally Blank

8 Appendices

APPENDIX A	BUILD & IMPACT METRICS	A-1
APPENDIX B	KCP&L SMART GRID USE CASES	B-1
APPENDIX C	KCP&L SMARTGRID MASTER INTERFACE LIST	C-1
APPENDIX D	IEC 61850 COMMUNICATIONS NETWORK	D-1
APPENDIX E	IEC 61850 SUBSTATION ETHERNET SWITCH TEST RESULTS	E-1
APPENDIX F	DEVICE POINTS LIST	F-1
APPENDIX G	BESS ACCEPTANCE TEST REPORT	G-1
APPENDIX H	SYSTEM DEPLOYMENT/GO-LIVE TEST STRATEGY	H-1
APPENDIX I	TEST PLAN WORKBOOKS.....	I-1
APPENDIX J	END-TO-END INTEROPERABILITY TESTING DOCUMENTATION	J-1
APPENDIX K	INTEROPERABILITY FIELD DEMONSTRATION SCRIPTS	K-1
APPENDIX L	SMARTGRID INTEROPERABILITY IMPLEMENTED	L-1
APPENDIX M	KCP&L SMARTGRID RISK ASSESSMENT MASTER REPORT	<i>FUTURE</i>
APPENDIX N	CYBER SECURITY CONTROLS MATRIX	N-1
APPENDIX O	AMI AUDIT RESULTS.....	<i>FUTURE</i>
APPENDIX P	EDUCATION & OUTREACH COLLATERAL.....	<i>FUTURE</i>
APPENDIX Q	EPRI SMARTEND-USE ANALYSIS RESULTS	<i>FUTURE</i>
APPENDIX R	NAVIGANT SMARTEND-USE PROGRAM ANALYSIS RESULTS.....	<i>FUTURE</i>
APPENDIX S	CUSTOMER SURVEY RESULTS.....	<i>FUTURE</i>
APPENDIX T	FINAL BUILD METRICS	<i>FUTURE</i>
APPENDIX U	FINAL IMPACT METRICS.....	<i>FUTURE</i>
APPENDIX V	RESERVED	TBD
APPENDIX W	RESERVED	TBD
APPENDIX X	RESERVED	TBD
APPENDIX Y	RESERVED	TBD
APPENDIX Z	RESERVED	TBD

This Page Intentionally Blank

Appendix A Build & Impact Metrics

A.1	Build Metrics	A-2
A.1.1	Build Metrics for KCP&L's AMI Assets	A-2
A.1.2	Build Metrics for KCP&L's Customer System Assets	A-3
A.1.3	Build Metrics for KCP&L's Electrical Distribution Assets	A-4
A.1.4	Build Metrics for KCP&L's Distributed Energy Resources	A-5
A.1.5	Build Metrics for KCP&L's Pricing Programs.....	A-5
A.2	Impact Metrics	A-6
A.2.1	Impact Metrics for KCP&L's AMI and Customer Systems.....	A-6
A.2.2	Impact Metrics for KCP&L's Electric Distribution Systems	A-7
A.2.3	Impact Metrics for Battery Energy Storage System (BESS)	A-8
A.3	Baseline Build Metrics	A-9
A.3.1	Baseline Build Metrics for KCP&L's AMI Assets.....	A-9
A.3.2	Baseline Build Metrics for KCP&L's Customer System Assets	A-10
A.3.3	Baseline Build Metrics for KCP&L's Electrical Distribution Assets.....	A-11
A.3.4	Baseline Build Metrics for KCP&L's Distributed Energy Resource Assets.....	A-12
A.4	Baseline Impact Metrics	A-13
A.4.1	Baseline Impact Metrics for KCP&L's AMI and Customer Systems	A-13
A.4.2	Baseline Impact Metrics for KCP&L's Electric Distribution Systems.....	A-14

A.1 Build Metrics

“Project Only” pertains to assets deployed only within this project scope DOE/Cost Share funding. “System-Wide” pertains to the total assets deployed on the KCP&L system, including those deployed within this project.

A.1.1 Build Metrics for KCP&L’s AMI Assets

BUILD METRICS: Advanced Metering Infrastructure Assets				
Metric	Value Units	Project-Only	System-Wide	Notes
End-Points (meters)	# endpoints	-	-	~14,000 planned
Portion of Customers with AMI				
Residential	# endpoints	-	-	~13,000 planned
Commercial	# endpoints	-	-	~1,000 planned
Industrial	# endpoints	-	-	None planned
Metering Features				
Interval Reads of 1 Hour or Less	minutes	-	-	15-min interval through all AMI endpoints
Remote Connection/Disconnection	Yes/No # endpoints	-	-	Not necessarily on all AMI endpoints
Outage Detection/Reporting	Yes/No # endpoints	-	-	All AMI endpoints but on system, not all AMR?
Power Quality Monitoring	Yes/No # endpoints	-	-	AMI will report voltage violations
Tamper Detection	Yes/No # endpoints	-	-	All AMI endpoints
Backhaul Communications Network	Description	Private Fiber	Private Fiber	KCP&L will use existing private fiber at the project substation for backhaul comm.
Meter Communications Network	Description	L+G Gridstream AMI Mesh (900 MHz)	L+G Gridstream AMI Mesh (900 MHz)	L+G AMI Mesh installed with this project and no other AMI is on the system
Head-end System	Description	L+G Gridstream	L+G Gridstream	L+G hosted head-end
Meter Data Management System	Description	eMeter	eMeter	New AMI MDM
Meter Data Analysis Systems	Description	MDM, DataRaker	MDM, DataRaker	Will use existing DMAT (DataRaker) and MDM for data analysis
Enterprise Systems Integration				
Billing	Yes/No Description	-	-	New AMI will be integrated with existing Billing system
Customer Information System	Yes/No Description	-	-	New AMI will be integrated with existing CIS
Outage Management System	Yes/No Description	-	-	New AMI will be integrated with existing OMS
Distribution Management System	Yes/No Description	-	-	New AMI will be integrated with New DMS

A.1.2 Build Metrics for KCP&L's Customer System Assets

BUILD METRICS: Customer System Assets				
Metric	Value Units	Project-Only	System-Wide	Notes
Home Area Network	# devices Description	-	-	400 Tendril HAN gateways to be deployed in conjunction with PCT and some plug load monitor/switches
In-Home Displays	# devices Description	-	-	1600 project IHDs to be deployed
Web Portal	# with access # active acct.	-	-	All AMI endpoints will have access
Energy Management Devices/Systems	# devices Description	-	-	3 commercial SmartGrid enabled BEMs
Direct Load Control Devices	# devices Description	-	-	None system-wide, to be deployed thru HAN and maybe others
Programmable Controllable Thermostat	# devices Description	-	-	Up to 1600 expected to be deployed (50,000 in Energy Optimizer Program)
Smart Appliances	# devices Description	-	-	No deployment on Project beyond appliances installed at Demonstration House

A.1.3 Build Metrics for KCP&L's Electrical Distribution Assets

BUILD METRICS: Electric Distribution System Assets				
Metric	Value Units	Project-Only	System-Wide	Notes
Portion of System with SCADA	%	N/A	N/A	SCADA already present in Demonstration Area.
Portion of System with Distribution Automation (DA)	%	-%	-%	Number of distribution feeders that have fully integrated DA equipment installed as a result of this project divided by total distribution feeders.
DA Devices				
Automated Feeder Switches	# devices	-	-	TBD switches / reclosers to be added on DA circuits
Automated Capacitors	# devices	-	-	Upgrading all cap controls and comm.
Automated Regulators	# devices	-	-	Incl. LTCs at substation
Feeder Monitors	# devices	-	-	End of line voltage monitors 3+ circuits
Remote Fault Indicators	# devices	-	-	On DA circuits
Transformer Monitors (line)	# devices	-	-	None planned
Smart Relays	# devices	-	-	All Midtown circuits
Fault Current Limiter	# devices	-	-	None planned
DA Communications Network	Yes/No Description	AMI Mesh	AMI Mesh	DA devices will use AMI Mesh network
Substation Transformer Monitor & Dynamic Ratings	# devices	-	-	All 161/13kV transformers will have temp & DGA monitoring installed. (4 transformers in total)
Distribution Feeder Cable Monitor & Dynamic Ratings	# devices	-	-	Deployment potential being investigated.
DA System Features/Applications				
Fault Location, Isolation and Service Restoration (FLISR)	Yes/No	-	-	
Voltage Optimization	Yes/No	-	-	Including DVC and CVR, Urban circuits already have DVC
Feeder Peak Load Management	Yes/No	-	-	Batt, DR will be added and enhanced.
Microgrids	Yes/No	-	-	None planned
Distribution Management System				
Integration with AMI	Yes/No	-	-	New DMS will integrate with AMI
Integration with Outage Management System	Yes/No	-	-	New DMS will integrate with OMS
Integration with Transmission Management System	Yes/No	N/A	N/A	None planned
Integration with Distributed Energy Resources	Yes/No	-	-	New DMS will integrate with DERM

A.1.4 Build Metrics for KCP&L's Distributed Energy Resources

BUILD METRICS: Distributed Energy Resources				
Metric	Value Units	Project-Only	System-Wide	Notes
Distributed Gen.: Number of Units	#	-	-	~180 kW distributed solar to be installed by the project. This metric only considers KCP&L-owned DG.
Distributed Gen.: Installed Capacity	MW	-	-	
Distributed Gen.: Energy Delivered	MWh	-	-	
Energy Storage: Number of Units	#	-	-	1x1.0MW grid battery and 1x8kW at demo home
Energy Storage.: Installed Capacity	MW	-	-	
Energy Storage: Energy Delivered	MWh	-	-	
PEV Charging: Number of Units	# points	-	-	10 charging points planned for project.
PEV Charging: Installed Capacity	kW	-	-	
PEV Charging: Energy Delivered	kWh	-	-	
DG (DER) Interconnection equipment	# of units	-	-	Grid batt, parallel gens, and DR devices

A.1.5 Build Metrics for KCP&L's Pricing Programs

BUILD METRICS: Pricing Programs				
Metric	Value Units	Project-Only	System-Wide	Notes
Retail Rate Design and Rate Level				
Flat	Yes/No # with access # enrolled Description	-	-	None planned
Flat with Critical Peak Pricing				None planned
Flat with Peak-Time Rebate				None planned
Tier				KCP&L has seasonal w/ declining block
Tier with Critical Peak Pricing				None planned
Tier with Peak-Time Rebate				None planned
Time-of-Use				Existing plus new piloted rates
Variable Peak Pricing				None planned
Time-of-Use with Critical Peak Pricing				Maybe
Time-of-Use with Peak-Time Rebate				Maybe
Real-Time Pricing				None planned
Real-Time Pricing with Critical Peak Pricing				None planned
Real-Time Pricing with Peak Time Rebate				None planned
Pre-Pay Pricing				Maybe
Net Metering				Yes
Rate Decoupling				None planned

A.2 Impact Metrics

A.2.1 Impact Metrics for KCP&L's AMI and Customer Systems

IMPACT METRICS: AMI and Customer Systems				
Metric	Value Units	Project-Level	System-Level	Notes
Metrics Related Primarily to Economic Benefits				
Hourly Customer Electricity Usage	kWh \$/kWh	- -	N/A N/A	
Monthly Customer Electricity Usage	kWh \$/kWh	- -	N/A N/A	
Peak Generation and Mix	MW Mix	N/A	N/A	Pilot project affects a small portion of KCP&L load and will have no discernable affect on these metrics.
Peak Load and Mix	MW Mix	N/A	N/A	
Annual Generation Cost	\$	N/A	N/A	
Hourly Generation Cost	\$/MWh	N/A	N/A	
Annual Electricity Production	MWh	N/A	N/A	
Ancillary Services Cost	\$	N/A	N/A	
Meter Operations Cost	\$	-	N/A	
Truck Rolls Avoided	#	-	N/A	
Metrics Related Primarily to Environmental Benefits				
Meter Operations Vehicle Miles	miles	-	N/A	Estimate based on average miles/roll
CO ₂ Emissions	tons	-	N/A	Prorated plant emissions and fleet emission associated with reduced vehicle miles
Pollutant Emissions (SO _x , NO _x , PM-2.5)	tons	-	N/A	
Metrics Related Primarily to AMI System Performance				
Meter Data Completeness	%	-	N/A	Considers only project AMI meters, no AMR metrics
Meters Reporting Daily by 2AM	%	-	N/A	

A.2.2 Impact Metrics for KCP&L's Electric Distribution Systems

IMPACT METRICS: Electric Distribution Systems				
Metric	Value Units	Project-Level	System-Level	Notes
Metrics Related Primarily to Economic Benefits				
Distribution Feeder or Equipment Overload Incidents	# incidents	-	N/A	
Distribution Feeder Load	MW MVAR	-	N/A	
Deferred Distribution Capacity Investments	\$	-	N/A	Only if an upgraded is deemed avoided through load mgmt.
Equipment Failure Incidents	# incidents	-	N/A	Failed project dist. equipment
Distribution Equipment Maintenance Cost	\$/semi- anum	-	N/A	Maintenance Cost as defined by KCP&L
Distribution Operations Cost	\$/semi- anum	-	N/A	Operations Cost as defined by KCP&L
Distribution Feeder Switching Operations	# manual switchings	-	N/A	Tally of manual switching events
Distribution Capacitor Switching Operations	# manual switchings	N/A	N/A	All capacitors have local/remote switching capabilities installed already.
Distribution Restoration Cost	\$/semi- anum	-	N/A	Estimated based on restoration activities tracked in MWMS
Distribution Losses (%)	%	-	N/A	Cum. of kWh lost b/w sub. and meters
Distribution Power Factor	project PF	-	N/A	PF for project circuits
Truck Rolls Avoided	# truck rolls	-	N/A	Activities that previously required a truck roll
Metrics Related Primarily to Reliability Benefits				
SAIFI	Index	-	N/A	
SAIDI/CAIDI	Index	-	N/A	
MAIFI	Index	-	N/A	
Outage Response Time	Minutes	-	N/A	If no events, will consider simulation
Major Event Information	Event Statistics	-	N/A	Describe each event that qualifies (#, etc.)
Number of High Impedance Faults Cleared	# faults cleared	-	N/A	Logged by DMS/DCADA?
Metrics Related Primarily to Environmental Benefits				
Distribution Operations Vehicle Miles	miles	-	N/A	Base on average system miles/roll
CO ₂ Emissions	tons	-	N/A	Prorated plant emissions and fleet emission associated with reduced vehicle miles
Pollutant Emissions (SO _x , NO _x , PM-2.5)	tons	-	N/A	

A.2.3 Impact Metrics for Battery Energy Storage System (BESS)

IMPACT METRICS: AMI and Customer Systems				
Metric	Value Units	Project-Level	System-Level	Notes
Metrics Related Primarily to Economic Benefits				
Hourly Customer Electricity Usage	kWh \$/kWh	- -	N/A N/A	
Monthly Customer Electricity Usage	kWh \$/kWh	- -	N/A N/A	
Peak Generation and Mix	MW Mix	N/A	N/A	Pilot project affects a small portion of KCP&L load and will have no discernable affect on these metrics.
Peak Load and Mix	MW Mix	N/A	N/A	
Annual Generation Cost	\$	N/A	N/A	
Hourly Generation Cost	\$/MWh	N/A	N/A	
Annual Electricity Production	MWh	N/A	N/A	
Ancillary Services Cost	\$	N/A	N/A	
Meter Operations Cost	\$	-	N/A	
Truck Rolls Avoided	#	-	N/A	
Metrics Related Primarily to Environmental Benefits				
Meter Operations Vehicle Miles	miles	-	N/A	Estimate based on average miles/roll
CO ₂ Emissions	tons	-	N/A	Prorated plant emissions and fleet emission associated with reduced vehicle miles
Pollutant Emissions (SO _x , NO _x , PM-2.5)	tons	-	N/A	
Metrics Related Primarily to AMI System Performance				
Meter Data Completeness	%	-	N/A	Considers only project AMI meters, no AMR metrics
Meters Reporting Daily by 2AM	%	-	N/A	

A.3 Baseline Build Metrics

Baseline Estimates are limited to the Project area, system, and assets.

A.3.1 Baseline Build Metrics for KCP&L's AMI Assets

BASELINE ESTIMATES FOR BUILD METRICS: AMI Assets				
Metric	Baseline Remarks	Baseline Estimate	Quarterly Forecast	Baseline Estimation Method
End-Points (smart meters):				
Residential	No AMI metering would be planned for installation in the KCP&L service territory without this project	0	-	
Commercial		0	-	
Industrial		0	-	
Metering Features:				
Interval reads of 1 hour or less	Some load research meters are read on 15 min. intervals thru the AMR for regulatory	0	-	No AMI without project
Remote Connection/Disconnection	No remote connect / disconnect meters would be installed without this project	0	-	
Outage Detection/Reporting	AMR has Outage Reporting	0	-	
Power quality monitoring	No PQ monitoring meters would be installed at residential without project	0	-	
Tamper detection	No tamper detection meters would be installed without this project	0	-	
Backhaul Communications Network	KCP&L has an existing fiber backhaul comm.. network that will be utilized by project	0	-	
Meter Communications Network	KCP&L has AMR but would not implement 2-way meter comm. without this project	0	-	
Head End system	KCP&L has AMR head-end but would not implement AMI head-end without this project	0	-	
Meter Data Management System	KCP&L would not implement MDMS without this project	0	-	
Enterprise systems integration:				
Billing	No AMI without project	0	-	Integrated w/ AMI
Customer information system	No AMI without project	0	-	Integrated w/ AMI
Outage management system	No AMI without project	0	-	Integrated w/ AMI
Distribution Management System	No AMI without project	0	-	Integrated w/ AMI

A.3.2 Baseline Build Metrics for KCP&L's Customer System Assets

BASELINE ESTIMATES FOR BUILD METRICS: Customer System Assets				
Metric	Baseline Remarks	Baseline Estimate	Quarterly Forecast	Baseline Estimation Method
Home Area Network	KCP&L would not implement HANs without this project	0	-	Number of HANs
In-Home Displays	KCP&L would not implement IHDs without this project	0	-	Number of IHDs
AMI Web Portal	KCP&L offers AccountLink (daily read data online access to all AMR customers)	0	-	This is a baseline of AMI Portal participants
Energy Management Devices/Systems	KCP&L would not interface with BEMSs without this project	0	-	Number of communicating BEMSs
Direct Load Control Devices	KCP&L would not implement DLCs without the project	0	-	Number of DLCs
Programmable Controllable Thermostat	KCP&L currently operates a successful PCT program, Energy Optimizer, which utilizes a paging system.	-		Number of EO participants (~50,000)

A.3.3 Baseline Build Metrics for KCP&L's Electric Distribution System Assets

BASELINE ESTIMATES FOR BUILD METRICS: Electric Distribution System Assets				
Metric	Baseline Remarks	Baseline Estimate	Quarterly Forecast	Baseline Estimation Method
Portion of System with SCADA	SCADA is already installed on project substation feeders and most of KCP&L system	N/A	N/A	Existing SCADA will remain in place on project substation. This project will install a distributed substation controller and new substation network that will operate in parallel with SCADA
Portion of project system with Distribution Automation (DA)	Some automated equipment exists within the project area but no circuits have comprehensive DA	0%	-	Portion of feeders with distributed automated control and monitoring
DA Devices				
Automated Feeder Switches	No Automated Feeder Switches would be installed on the project system	0	-	Number of automated feeder switches installed on project system
Automated Capacitors	Unknown how many additional Capacitors would be installed without this project.	0	-	Unknown how many additional Capacitors would be installed without this project.
Automated Regulators	KCP&L would not install automated regulators without this project	0	-	Number of automated regulators installed on project system
Feeder Monitors (voltage or current)	KCP&L would not install feeder voltage or current monitors without project	0	-	Number of feeder voltage monitors installed on project system
Remote Fault Indicators	KCP&L would not install RFIs without this project	0	-	Number of remote fault indicators installed on project system
Transformer Monitors(line)	Line transformer monitors would not be installed without this project	0	-	Number of line xfmr monitors installed on project system
Smart Relays	KCP&L would not install smart relays without this project	0	-	Number of smart relays installed on project system
DA Communications Network	KCP&L currently has segregated device communications (telemetry and cellnet). Advanced DA in this project will primarily utilize the AMI Mesh network.			
Substation Transformer Monitors & Dynamic Ratings	Transformer monitors and DGA would not be installed without this project	0	-	Number of xfmr monitors installed on project system

BASELINE ESTIMATES FOR BUILD METRICS: Electric Distribution System Assets				
Metric	Baseline Remarks	Baseline Estimate	Quarterly Forecast	Baseline Estimation Method
Distribution Feeder Cable Monitor & Dynamic Ratings	KCP&L would not install cable monitors without project	0	-	Number of devices
DA System Features/Applications				
Fault Location, Isolation and Service Restoration (FLISR)	KCP&L would not install FLISR without this project	No	-	
Voltage Optimization	KCP&L has no circuits with true voltage optimization but does have many circuits with voltage reduction capabilities through LTCs at the sub in conjunction with cap banks on the lines	No	-	Select circuits will get true voltage optimization through decentralized control
Feeder Peak Load Management	Project circuits currently have DVC and some DR devices which are controlled on a system-wide execution	No	-	System enabled and functional
Microgrids	KCP&L is not pursuing Microgrids in this project	No	-	N/A
Distribution Management System				
Integration with AMI	AMI would not be installed without this project	No	-	
Integration with Outage Management System	No DMS without this project	No	-	
Integration with Trans. Mgmt System (EMS)	No DMS without this project	No	-	
Integration with DER	No DMS without this project	No	-	
Fault Current Limiter	No DMS without this project	No	-	

A.3.4 Baseline Build Metrics for KCP&L's Distributed Energy Resource Assets

BASELINE ESTIMATES FOR BUILD METRICS: Distributed Energy Resource Assets				
Metric	Baseline Remarks	Baseline Estimate	Quarterly Forecast	Baseline Estimation Method
Distributed Gen.: Number of Units	No KCP&L owned DG would be implemented in the project area without project	0	-	Only refers to KCP&L-owned DG in project area
Distributed Gen.: Installed Capacity		0	-	
Distributed Gen.: Energy Delivered		0	-	
Energy Storage: Number of Units	Would not implement storage without project	0	-	Project area
Energy Storage.: Installed Capacity		0		
Energy Storage: Energy Delivered		0		
DER Integration	There would be no DERM without project	0	-	# of interfaces
PEV Charging: Number of Units	It is not likely that charging stations would have been installed in the project area without the project funding	0	-	
PEV Charging: Installed Capacity		0		
PEV Charging: Energy Delivered		0		

A.4 Baseline Impact Metrics

A.4.1 Baseline Impact Metrics for KPC&L's AMI and Customer System

BASELINE ESTIMATES FOR IMPACT METRICS: AMI and Customer Systems				
Metric	Baseline Remarks	Baseline Estimate	Quarterly Forecast	Baseline Estimation Method
Hourly Customer Electricity Usage	kWh \$/kWh	TBD		Baseline 8760 data for each group of smart grid customers
Monthly Customer Electricity Usage	kWh \$/kWh	TBD		Historical monthly consumption data
Peak Generation and Mix	MW Mix	N/A		N/A
Peak Load and Mix	MW Mix	N/A		N/A
Annual Generation Cost	\$	N/A		N/A
Hourly Generation Cost	\$/MWh	N/A		N/A
Annual Electricity Production	MWh	N/A		N/A
Ancillary Services Cost	\$	N/A		N/A
Meter Operations Cost	\$	TBD		Extracted from accounting systems
Truck Rolls Avoided	#	TBD		Based on automated or remote actions that previously manual
Meter Operations Vehicle Miles	Miles	TBD		Avg. travel distance times number of rolls avoided.
CO ₂ Emissions	tons	TBD		Prorated plant emissions and fleet emission associated with reduced vehicle miles
Pollutant Emissions (SO _x , NO _x , PM-2.5)	tons	TBD		
Meter Data Completeness	%	TBD		Portion of attempted reads missing or corrupt
Meters Reporting Daily by 2AM	%	TBD		Portion of meters successfully reporting by 2AM

A.4.2 Baseline Impact Metrics for KPC&L's Electric Distribution Systems

BASELINE ESTIMATES FOR IMPACT METRICS: Electric Distribution Systems				
Metric	Baseline Remarks	Baseline Estimate	Quarterly Forecast	Baseline Estimation Method
Distribution Feeder or Equipment Overload Incidents	#	TBD		Derived from historical records
Distribution Feeder Load	MW MVAR	TBD		Derived from historical records
Deferred Distribution Capacity Investments	\$	TBD		Derived from historical records
Equipment Failure Incidents	#	TBD		Derived from historical records
Distribution Equipment Maintenance Cost	\$	TBD		Derived from historical records
Distribution Operations Cost	\$	TBD		Derived from historical records
Distribution Feeder Switching Operations	#	TBD		Derived from historical records
Distribution Capacitor Switching Operations	#	TBD		Derived from historical records
Distribution Restoration Cost	\$	TBD		Derived from historical records
Distribution Losses (%)	%	TBD		Derived from historical records
Distribution Power Factor	pf	TBD		Derived from historical records
Truck Rolls Avoided	#	TBD		Derived from historical records
SAIFI	Index	TBD		Derived from historical records. Baseline estimates are calculated very differently from project observation
SAIDI/CAIDI	Index	TBD		
MAIFI	Index	TBD		
Outage Response Time	Minutes	TBD		Derived from historical records
Major Event Information	Event Statistics	TBD		Derived from historical records
Number of High Impedance Faults Cleared	#	TBD		Derived from historical records
Distribution Operations Vehicle Miles	Miles	TBD		Derived from historical records
CO ₂ Emissions	tons	TBD		Derived from historical records
Pollutant Emissions (SO _x , NO _x , PM-2.5)	tons	TBD		Derived from historical records

Appendix B KCP&L SmartGrid Use Cases

B.1	Automated Metering Infrastructure (AMI)	B-2
B.2	SmartSubstation (SUB)	B-7
B.3	First Responder (1 ST).....	B-9
B.4	Distribution Management System (DMS)	B-10
B.5	Distributed Energy Resource Management (DRM)	B-12
B.6	SmartEnd-Use (SEU)	B-15
B.7	Home Area Network (HAN)	B-16
B.8	Plug-In Electric Vehicle (PEV).....	B-18
B.9	Meter Data Management (MDM)	B-19
B.10	Network (NWK)	B-19

B.1 Automated Metering Infrastructure (AMI)

B.1.1 Customer Requested Remote Service Order Completion

This Use Case describes the steps in a customer requested remote service order completion. Traditionally, utilities send a field technician to the Customer premise to (dis)connect service to the meter. With an Automated Metering Infrastructure, the (dis)connect can be performed remotely by initiating a remote service order request. The remote service order request could be made due to customer move-in/out or for billing related reasons. The customer move-in/out and reinstatement for payment received allow for the use of remote service order completion directly. A disconnect for non-payment, however, requires a technician to be deployed to the premise for proper notification prior to the actual disconnect. See Section 3.3.2 for Regulations.

This Use Cases addresses three service types that can be completed using an automated procedure.

- Customer move out with landlord revert
- Customer move out without landlord revert
- Customer move in

The standard turn-on and turn-off operations are batched for daily processing by CIS. The disconnect for non-payment is processed in quasi real-time to reduce the chances that a Customer will receive their final disconnect notice and contact a Customer Service Representative prior to the batch processing.

B.1.2 On-Demand Meter Read

An on-demand meter read may be requested by multiple systems for a number of reasons. The process is carried out by transferring a meter read request message from the requesting system to the desired SmartMeter. In order to obtain a real-time meter read, the meter read request will travel to the SmartMeter via the Field Automation Network. The SmartMeter then sends the requested meter read data back to the requesting system via the Field Automation Network. The meter read data can be analyzed and processed as needed upon receipt by the requesting system.

This Use Case describes the process of the Customer Information System (or other system) requesting and receiving an on-demand meter read from a SmartMeter.

B.1.3 On-Demand Meter Status Check

Once the Distribution Management System software is integrated with the Meter Data Management System and AMI Head End, the network operations personnel can automatically check the status of the SmartMeter. This functionality has the potential to limit field visits to verify service status by service technicians. It can also be used to verify that service has been restored in the event of an outage.

An on-demand meter status check may be requested by multiple persons, systems, or organizations for a number of reasons including service status verification, SmartMeter health/functionality, power restoration, and service (dis)connect status. The process is carried out by transferring a meter read request message from the requesting system to the desired SmartMeter via the Field Automation Network. The SmartMeter then sends the requested meter read data back to the requesting system via the Field Automation Network.

B.1.4 Automated Daily Meter Read

This Use Case describes the automated meter reading process. The SmartMeter records interval usage readings every fifteen minutes and pushes the data to the AMI Head-End every four hours throughout the day. Each SmartMeter uses a random offset to level traffic across the AMI network. Daily register

readings (total daily usage) are taken at midnight and pushed to the AMI Head-End at a random offset after midnight. The random offsets are used to level traffic across the AMI network with the goal of having all daily register readings to the AMI Head-End by 4:00 AM.

While each SmartMeter is pushing data to the AMI Head-End every four hours, the AMI Head-End is sending data to the Meter Data Management System on a different schedule. The AMI Head-End aggregates data from multiple SmartMeters and pushes a batch file to the Meter Data Management System on an hourly basis. This batch file can contain both interval and register data.

In addition to pushing data to the Meter Data Management System, the AMI Head-End contains the intelligence to recognize when meter reading data is missing and make specific requests to SmartMeters for the missing data to be resent. Once the data is retrieved, it is sent to the Meter Data Management System with the next hourly data push.

B.1.5 SmartMeter Alarm Events

The Advanced Metering Infrastructure system provides each SmartMeter with event capabilities to inform the Utility that the status of the SmartMeter has changed. Events are enabled within the SmartMeter to proactively identify possible tampering and/or diversion conditions, power quality conditions, and device status conditions. Each SmartMeter Event can be configured to one of the four following statuses: Log Only, Advisory, Alarm, or Disabled. These configurations can vary from SmartMeter to SmartMeter depending on the application. Events enabled on the SmartMeter may represent, but are not limited to, the following categories:

- Power Quality
- Meter Health
- Revenue Protection

This Use Case details the process of a SmartMeter sending an Event with an Alarm status after a status change within the SmartMeter. The SmartMeter sends any Alarm Events to the AMI Head-End in real-time. From there, the Alarm Event may be sent on to the Meter Data Management System.

B.1.6 SmartMeter Advisory Events

The Advanced Metering Infrastructure system provides each SmartMeter with event capabilities to inform the Utility that the status of the SmartMeter has changed. Events are enabled within the SmartMeter to proactively identify possible tampering and/or diversion conditions, power quality conditions, and device status conditions. Each SmartMeter Event can be configured to one of the four following statuses: Log Only, Advisory, Alarm, or Disabled. These configurations can vary from SmartMeter to SmartMeter depending on the application. Events enabled on the SmartMeter may represent, but are not limited to, the following categories:

- Power Quality
- Meter Health
- Revenue Protection

This Use Case details the process of a SmartMeter sending an Event with an Advisory status after a status change within the SmartMeter. The SmartMeter sends any Advisory Events to the AMI Head-End every four hours, with the next SmartMeter data push. From there, the Advisory Event may be sent on to the Meter Data Management System.

B.1.7 SmartMeter Log Only Events

The Advanced Metering Infrastructure system provides each SmartMeter with event capabilities to inform the Utility that the status of the SmartMeter has changed. Events are enabled within the SmartMeter to proactively identify possible tampering and/or diversion conditions, power quality conditions, and device status conditions. Each SmartMeter Event can be configured to one of the four following statuses: Log Only, Advisory, Alarm, or Disabled. These configurations can vary from SmartMeter to SmartMeter depending on the application. Events enabled on the SmartMeter may represent, but are not limited to, the following categories:

- Power Quality
- Meter Health
- Revenue Protection

This Use Case details the process of a SmartMeter sub-device sending an Event with a Log Only status after a status change within the SmartMeter. The SmartMeter sub-device sends any Log Only Events to the Meter FAN Radio, where they are logged and maintained for diagnostics and troubleshooting purposes. Log Only Events can be retrieved by sending a command to the SmartMeter via the AMI Head End or other system.

B.1.8 SmartMeter Source Power Events

The Advanced Metering Infrastructure (AMI) system provides each SmartMeter with event capabilities to inform the Utility that the status of the SmartMeter has changed. Events are enabled within the SmartMeter to proactively identify possible tampering and/or diversion conditions, power quality conditions, and device status conditions. Each SmartMeter Event can be configured to one of the four following statuses: Log Only, Advisory, Alarm, or Disabled. These configurations can vary from SmartMeter to SmartMeter depending on the application. Events enabled on the SmartMeter may represent, but are not limited to, the following categories:

- Power Quality
- Meter Health
- Revenue Protection

This Use Case details a specific type of Alarm Event – those dealing with SmartMeter source power. The outage event serves as a surrogate for the Customer’s call, often allowing the problem to be fixed before the Customer even becomes aware of the outage. AMI systems also help the Outage Management System (OMS) and dispatcher understand and efficiently respond to widespread outage conditions. The restoration event will follow a similar path and will notify the Utility when power has been restored to a SmartMeter.

This Use Case is detailed in two sequences that describe outage events and restoration events. When a power outage is detected at a SmartMeter, an outage event message is sent from that SmartMeter to the Meter Data Management System. The Meter Data Management System determines whether or not the outage information needs to be sent to the Distribution Management System for processing. Once power is restored to a SmartMeter, a restoration event message is sent from that SmartMeter to the Meter Data Management System. The Meter Data Management System then sends the restoration information to the Distribution Management System for processing.

B.1.9 FAN Device Alarm Events

The Field Automation Network (FAN) within the Advanced Metering Infrastructure system provides each device with event capabilities to inform the Utility that the status of the FAN device has changed. Events

are enabled within the devices to proactively identify possible tampering and/or diversion conditions, source power quality conditions, and FAN device status conditions. Each FAN device event can be configured to one of the four following statuses: Log Only, Advisory, Alarm, or Disabled. These configurations can vary from FAN device to FAN device depending on the application. Events enabled on a FAN device may represent, but are not limited to, the following categories:

- Source Power Quality
- Device Health
- Revenue Protection

This Use Case details the process of a FAN device sending an Event with an Alarm status after a status change within the FAN device. The FAN device sends any Alarm Events to the AMI Head-End in real-time.

B.1.10 FAN Device Advisory Events

The Field Automation Network (FAN) within the Advanced Metering Infrastructure system provides each device with event capabilities to inform the Utility that the status of the FAN device has changed. Events are enabled within the devices to proactively identify possible tampering and/or diversion conditions, source power quality conditions, and FAN device status conditions. Each FAN device event can be configured to one of the four following statuses: Log Only, Advisory, Alarm, or Disabled. These configurations can vary from FAN device to FAN device depending on the application. Events enabled on a FAN device may represent, but are not limited to, the following categories:

- Source Power Quality
- Device Health
- Revenue Protection

This Use Case details the process of a FAN device sending an Event with an Advisory status after a status change within the FAN device. The FAN device sends any Advisory Events to the AMI Head-End every four hours, with the next FAN device data push. From there, the Advisory Event may be sent on to the Meter Data Management System.

B.1.11 FAN Device Log Only Events

The Field Automation Network (FAN) within the Advanced Metering Infrastructure system provides each device with event capabilities to inform the Utility that the status of the FAN device has changed. Events are enabled within the devices to proactively identify possible tampering and/or diversion conditions, source power quality conditions, and FAN device status conditions. Each FAN device event can be configured to one of the four following statuses: Log Only, Advisory, Alarm, or Disabled. These configurations can vary from FAN device to FAN device depending on the application. Events enabled on a FAN device may represent, but are not limited to, the following categories:

- Source Power Quality
- Device Health
- Revenue Protection

This Use Case details the process of a FAN device logging an Event with a Log Only status after a status change within the FAN device. The FAN device logs any Log Only Events to internal memory, where they are logged and maintained for diagnostics and troubleshooting purposes. Log Only Events can be retrieved by sending a command to the FAN device via the AMI Head End or other system.

B.1.12 Events Remote SmartMeter Update

The SmartMeter is adaptive to the Utility's changing environment, and it has the capacity to be remotely modified via the Field Automation Network. The SmartMeter program, which defines the functionality of the SmartMeter, can be modified from one rate structure to another. For example, the SmartMeters can be modified from flat rate meters to time-of-use meters. The SmartMeter configuration, which determines the program settings, can be modified to incorporate specific settings of the current meter program. For example, if the SmartMeter program is defined as a time-of-use meter, then the Utility could update the configuration to modify the time-of-use bucket definitions. Both the program and the configuration can be updated remotely.

In addition to updating the SmartMeter program and configuration remotely, the SmartMeter firmware can be updated remotely via the Field Automation Network. The SmartMeter consists of three independent sub-devices which all have their own firmware. These sub-devices are the Meter FAN Radio, Meter Metrology Board and Energy Services Interface Radio. The SmartMeter vendor can issue a firmware update for any or all of these sub-devices for various reasons (bug fixes, feature enhancements, manufacturing changes, etc.). These updates can be completed remotely.

This Use Case describes how SmartMeter program updates, configuration updates, and firmware updates are implemented remotely via the Field Automation Network.

B.1.13 Field SmartMeter Update

The SmartMeter is adaptive to the Utility's changing environment, and it has the capacity to be modified by a field technician. Each SmartMeter has an Opticom port allowing the meter program, configuration, and firmware to be updated by field technicians. Using a laptop equipped with an Opticom probe and the SmartMeter vendor programming software, the technician can update the SmartMeter program file, configuration file, or the firmware to any of the sub-devices within the SmartMeter.

The SmartMeter program, which defines the functionality of the SmartMeter, can be modified from one rate structure to another. For example, the SmartMeters can be modified from flat rate meters to time-of-use meters. The SmartMeter configuration, which determines the program settings, can be modified to incorporate specific settings of the current meter program. For example, if the SmartMeter program is defined as a time-of-use meter, then the Utility could update the configuration to modify the time-of-use bucket definitions. Both the program and the configuration can be updated in the field.

In addition to updating the SmartMeter program and configuration, the SmartMeter firmware can also be updated in the field. The SmartMeter consists of three independent sub-devices which all have their own firmware. These sub-devices are the Meter FAN Radio, Meter Metrology Board and Energy Services Interface Radio. The SmartMeter vendor can issue a firmware update for any or all of these sub-devices for various reasons (bug fixes, feature enhancements, manufacturing changes, etc.).

This Use Case describes how SmartMeter program, configuration, and firmware updates are implemented in the field by a field technician.

B.1.14 Remote FAN Device Update

The Field Automation Network (FAN) devices are adaptive to the Utility's changing environment, and they have the capacity to be remotely modified via the FAN. The FAN devices include FAN Endpoint Nodes, FAN Routers, and FAN Collectors. The FAN device configuration, which defines how frequently data is pushed from the devices, can be updated remotely. The FAN Device firmware can also be updated remotely.

This Use Case describes how FAN device configuration and firmware updates are implemented remotely via the Field Automation Network.

B.1.15 Field FAN Device Update

The Field Automation Network (FAN) devices are adaptive to the Utility's changing environment, and they have the capacity to be modified by a field technician. The FAN devices include FAN Endpoint Nodes, FAN Routers, and FAN Collectors. Each FAN device has an Opticom port allowing the FAN device configuration (defining how frequently data is pushed from the device) and firmware to be updated by field technicians. Using a laptop equipped with an Opticom probe and the vendor programming software, the technician can update the FAN device configuration file or firmware to any of the FAN devices.

This Use Case describes how FAN device configuration and firmware updates are implemented in the field by a field technician.

B.1.16 Remote Service Order Completion

This Use Case describes the steps in a remote service order completion. Traditionally, utilities send a field technician to the Customer premise to (dis)connect service to the meter. With an Automated Metering Infrastructure, the (dis)connect can be performed remotely by initiating a remote service order request. The remote service order request could be made due to customer move-in/out or for billing related reasons. The customer move-in/out and reinstatement for payment received allow for the use of remote service order completion directly. A disconnect for non-payment, however, requires a technician to be deployed to the premise for proper notification prior to the actual disconnect. See Section 3.3.2 for Regulations.

This Use Cases addresses four service types that can be completed using an automated procedure.

- Turn On at Meter
- Turn Off at Meter
- Service Investigation Order for Vacant with Usage

The standard turn-on and turn-off operations are batched for daily processing by CIS. The disconnect for non-payment is processed in quasi real-time to reduce the chances that a Customer will receive their final disconnect notice and contact a Customer Service Representative prior to the batch processing.

B.1.17 SmartMeter Replaced by Field Crew (*Future*)

B.2 SmartSubstation (SUB)

B.2.1 DCADA Monitors and Controls Substation Devices

This Use Case describes the Distributed Control and Data Acquisition System (DCADA) monitoring and control of substation devices. The DCADA system monitoring process works in two ways: 1) DCADA polling a substation device for status and 2) a substation device reporting status (or status change) to DCADA due to an exception. When the Distribution Automation Device (DAD) in the substation needs to be operated, DCADA sends a control signal to the device. DCADA makes use of the Substation Distribution Protection Network to communicate with substation devices. The Distribution Data Concentrator is a sub-system of DCADA that is utilized to communicate with Distribution Automation Devices (DADs). The substation devices include various DADs such as transformer tap changer controls, bus, tie, and feeder breaker relays, capacitor bank controls, and automated switches.

B.2.2 DCADA Monitors and Controls Field Devices

This Use Case describes the Distributed Control and Data Acquisition System (DCADA) monitoring and control of field devices. The DCADA system monitoring process works in two ways: DCADA polling a field device for status and a field device reporting status (or status change) to DCADA due to an exception. When the configuration settings of a Distribution Automation Device in the field need to be updated, DCADA sends a control signal to the device. DCADA makes use of the Field Automation Network to communicate with field devices. The Distribution Data Concentrator is a sub-system of DCADA that is utilized to communicate with Distribution Automation Devices. The field devices include various Distribution Automation Devices such as voltage monitors, automated reclosers, capacitor bank controls, voltage regulators, automated switches and fault indicators.

B.2.3 Substation Transformer DGA & Thermal Monitoring (*Future*)

Monitoring devices and probes are installed on Substation transformers that are capable of sampling and evaluating dissolved gasses and recording oil-temperature. The probes will continuously monitor oil temperature and will send Dissolved Gas Analysis (DGA) data to DCADA system as often as once per hour. DCADA will contain a rule engine with preconfigured asset-specific parameters that trigger alarms, alerting D-SCADA when transformers are in condition that requires additional analysis.

B.2.4 Substation Transformer Dynamic Ratings (*Future*)

This Use Case describes the process of calculating dynamic ratings for substation transformers to maximize energy throughput. Dynamic transformer ratings are calculated by a DCADA Dynamic Transformer Rating (DTR) module using a series of algorithms. These algorithms utilize asset and condition data obtained from Dissolved Gas Analysis (DGA) devices, transformer sensors, substation sensors, and the EAMS. DGA devices provide dissolved gas levels, moisture, and partial discharge information. Transformer sensors provide information about other transformer components beyond the tank and windings, such as Load Tap Changers and Cooling System Status. Weather data can be incorporated from local Substation sensors or National Weather Service. DGA device data and substation sensor data are both delivered to DTRS via a Data Concentrator. EAMS information includes the transformer's static rating and other information, which might include heat run test data and historical loading data.

The dynamic transformer ratings consist of a normal rating and a series of 3 emergency ratings (15 minute, 30 minute, and one hour). After calculating this series of dynamic ratings, the DTR module updates the dynamic transformer rating values in the local DCADA data base.

B.2.5 Feeder Cable Dynamic Ratings (*Future*)

This Use Case describes the process of calculating dynamic Feeder Cable ratings to maximize energy throughput. Dynamic transformer ratings are calculated by a DCADA Dynamic Cable Rating (DCR) module using a series of algorithms. These algorithms utilize asset condition data obtained from duct temperature sensors, substation sensors, and the EAMS. Weather data can be incorporated from local substation sensors or National Weather Service. EAMS information includes the cable's static rating and other information, which might include historical loading data.

The dynamic cable ratings consist of a normal rating and a series of 3 emergency ratings (15 minute, 30 minute, and one hour). After calculating this series of dynamic ratings, the DCR module updates the dynamic transformer rating values in the local DCADA database.

B.3 First Responder (1ST)

B.3.1 DCADA Performs Fault Detection, Location, Isolation, and Restoration

Many types of faults can occur on a line section of a distribution system. Transient faults can be cleared after power has been disconnected for a short period of time. Transient faults are cleared by distribution automation devices, such as reclosers. Persistent faults can only be cleared by removing power from the line section where the fault has occurred and dispatching a field crew. Fault management applications are used to locate distribution network faults and provide fault isolation and service restoration. The fault location capabilities determine the location of permanent faults, whereas fault isolation and service restoration capabilities isolate the faulty section or area of distribution network and provide possible switching procedure to restore service.

This use case describes how the Distributed Control and Data Acquisition System (DCADA) responds to a persistent fault on a line section by approximately locating the fault, isolating the faulted line segment, and restoring service to customers through automated switching. Ultimately, the DCADA passes control authority to the Distribution Management System to dispatch field crews, correct the fault, and complete service restoration to Customers.

B.3.2 DCADA Performs Volt-Var Management

This Use Case describes the Volt/Var Control (VVC) functionality of the Distributed Control and Data Acquisition System (DCADA). The VVC can be executed through a centralized, a decentralized or a hybrid approach. Under normal operating conditions, the VVC manages voltage along an entire distribution circuit to achieve a voltage profile based upon KCP&L design parameters.

The primary objective of VVC functionality is to satisfy voltage and loading constraints. VVC functionality can be executed to satisfy any of the following 4 objective functions.

- Minimize subsystem power losses
- Minimize power demand
- Maximize generated reactive power
- Maximize revenue

This Use Case describes VVC execution via a distributed logical architecture.

B.3.3 DCADA Performs Dynamic Voltage Reduction for Demand Response (*Future*)

B.3.4 DCADA Performs Localized Load Transfer due to Overload

This Use Case describes the process by which Distribution Control and Data Acquisition (DCADA) to identify and respond to a feeder overload condition within its area of control. This function involves the DCADA communicating in a coordinated manner with the various Distribution Automation Devices (DADs) in both the field and the substation via the Substation Distribution Protection Network (SDPN) and the Distribution Automation Network (DAN).

B.3.5 DCADA Initiates Relay Protection Re-coordination (RPR) (*Future*)

This application adjusts the relay protection settings to real-time conditions based on the preset rules. This is accomplished through analysis of relay protection settings and operational mode of switching devices (i.e., whether the switching device is in switch or recloser mode), while considering the real-time connectivity, tagging, and severe weather conditions. The application is called to perform after feeder reconfiguration and in the case when conditions are changed and fuse saving is required. The updates

needed to meet the Smart Grid requirements include coordinating feeder protection and re-synchronization with Distributed Energy Resources and with Micro-grids.

B.4 Distribution Management System (DMS)

B.4.1 DMS Network Model Maintenance

Map technician updates the electrical connectivity model (topology model) and the monitoring and control equipment relationships to the electrical devices after receiving notification of a change in the characteristics of the electrical network.

B.4.2 DMS Monitors and Controls Substation Devices

This Use Case describes the Distribution Supervisory Control and Data Acquisition System (D-SCADA) monitoring and control of substation devices. The D-SCADA system monitoring process works in two ways: the D-SCADA can poll a substation device for status, or a substation device can report the status (or status change) to D-SCADA due to an exception. When the configuration settings of a Distribution Automation Device in the substation need to be updated, D-SCADA sends a control signal to the device. D-SCADA makes use of the Distribution Management System Virtual Private Network, the Distribution Data Concentrator, and the Substation Distribution Protection Network to communicate with substation devices. The Distribution Data Concentrator is a sub-system of the Distributed Control and Data Acquisition System (DCADA) that is utilized to communicate with Distribution Automation Devices. The substation devices include various Distribution Automation Devices such as relays, voltage monitors, transformer tap changer controls, breaker relays, capacitor bank controls, voltage regulators, and automated switches.

B.4.3 DMS Monitors and Controls Field Devices

This Use Case describes the Distribution Supervisory Control and Data Acquisition System (D-SCADA) monitoring and control of field devices. The D-SCADA system monitoring process works in two ways: the D-SCADA can poll a field device for status, or a field device can report the status (or status change) to D-SCADA due to an exception. When the configuration settings of a Distribution Automation Device in the field need to be updated, D-SCADA sends a control signal to the device. D-SCADA makes use of the Distribution Management System Virtual Private Network, the Distribution Data Concentrator, and the Field Automation Network to communicate with field devices. The Distribution Data Concentrator is a sub-system of the Distributed Control and Data Acquisition System (DCADA) that is utilized to communicate with Distribution Automation Devices. The field devices include various Distribution Automation Devices such as automated reclosers, capacitor bank controls, fault indicators, and battery energy storage systems.

B.4.4 DMS Processes Protective Device Alarms

Utilities are constrained in their response to outages by the sensors and the information currently available to them. SCADA systems typically extend only to the substation. By definition, AMI is the only system that extends to the edges of a utility network, sensing every line segment and transformer on the system. This AMI capability is used in conjunction with OMS functions to predict outage locations and to verify power restoration, enabling utilities to proactively identify customers whose power has yet to be restored.

When outages reported by other systems such as SCADA, DCADA (Distributed Control and Data Acquisition) System, or protective devices themselves, these outages can be immediately recorded as confirmed and bypass or discontinue the OMS prediction process. This Use Case will outline the systems interaction anticipated when the D-SCADA processes protective device alarms and send the appropriate messages to OMS and MDM systems.

- The OMS, upon notification that a protective device has operated will create a confirmed outage for that device and discontinue any downstream outage prediction processing.
- The MDM, upon notification that a protective device has operated will mark all downstream customers as out of service. It will continue to process meter grid alerts, but will discontinue sending any meter out notifications to OMS.

B.4.5 DMS Performs Emergency Load Transfer

The Distribution Management System (DMS) can trigger emergency load reduction for several reasons. At the substation level, the Distributed Control and Data Acquisition System (DCADA) might detect an immediate overload (or approaching overload trend; within the next hour) within its area of control that it cannot resolve even after utilizing the “first responder” Feeder Load Transfer (FLT) application. As a result, the DCADA notifies and passes control to the DMS Operator for load reduction. The DMS Operator calls upon Demand Response (DR) programs and/or grid-connected Distributed Energy Resources (DER) via the Distributed Energy Resource Management System (DERM). The DERM determines this solution to the overload based on priorities and economics and commits the appropriate assets for load reduction.

Emergency load reduction can also be initiated as a result of monitoring conducted at the DMS level, either through the Distribution System State Estimator (DSSE) application or the Distribution Supervisory Control and Data Acquisition (D-SCADA) sub-system. During DMS-initiated emergency load reduction, the DMS Operator calls upon one or multiple strategies in order to solve the problem. The DMS Operator could utilize FLT, DR programs, or grid-connected DER. If the overload condition still exists, then the DMS requests emergency DR from the DERM. The DERM determines this solution to the overload based on priorities and economics and commits the appropriate assets for load reduction.

B.4.6 DMS Schedules Required Load Transfer

The Distribution Management System Operator (DMSOP) can initiate a Studycase in the Distribution Management System (DMS) at any time. The operator might choose to run a Studycase each morning, or he could run a Studycase when he thinks the system load might be problematic due to weather, system maintenance, or some other issue. The Studycase will show the DMSOP the predicted condition of the distribution system during a certain time period in the future. The DMSOP will have 168 hourly values for all loads at his disposal. These values can be modified by using the correction coefficient to represent the expected future network conditions.

Upon creation of a Studycase, the DMS runs Distribution System Power Flow (DSPF) to determine whether any overloads are predicted during the Studycase time period. If so, the DMSOP uses a combination of iterative switching of Demand Response (DR) and Distributed Energy Resources (DER) in the DERM application to determine an optimal solution to the predicted overloads. Once the DMSOP is satisfied with the outcome, he can save the proposed schedule to be applied at the appropriate time. This solution will be verified before executing it in order to see if any changes have occurred between the study and execution time affecting the validity of the original solution.

B.4.7 DMS Manages Scheduled Events for Grid-Connected DER

The Utility will make use of various Distributed Energy Resources as needed to temporarily reduce or shift load on the distribution system. Distributed Energy Resources may include distributed generation sources and distributed storage devices. The Utility will implement a Distributed Energy Resource Management System to schedule, track, and dispatch the various Distributed Energy Resources that are available for Utility use. This Use Case describes the process by which the Distribution Management System manages scheduled event to dispatch grid-connected DER for grid reliability and/or economic reasons.

B.4.8 DMS Operator Returns Grid to NORMAL Configuration

This Use Case describes what activities are performed by the DMS Operator in the control center when the grid must be returned to its normal operating conditions after completion of service restoration, maintenance, or repair to a portion of the grid. The DMS Operator sends the appropriate switching commands to the field devices needed to restore each feeder to NORMAL Configuration.

B.4.9 DMS Performs Fault Detection, Location, Isolation, and Restoration

Many types of faults can occur on a line section of a distribution system. Transient faults can be cleared after power has been disconnected for a short period of time. Transient faults are cleared by distribution automation devices, such as reclosers. Persistent faults can only be cleared by removing power from the line section where the fault has occurred and dispatching a field crew. Fault management is a Distribution Network Analysis (DNA) application to locate distribution network faults and providing fault isolation and service restoration. Fault location function defines the location of permanent faults whereas fault isolation and service restoration function isolates the faulty section or area of distribution network and provides possible switching procedure to restore service.

This use case describes how the Distribution Supervisory Control and Data Acquisition System respond to a persistent fault on a line section.

B.4.10 DMS Performs Volt-Var Management

This Use Case describes the Volt/Var Control (VVC) functionality of the Distribution Management System (DMS). The VVC can be executed through a centralized, a decentralized or a hybrid approach. Under normal operating conditions, the VVC manages voltage along an entire distribution circuit to achieve a voltage profile based upon KCP&L design parameters.

The primary objective of VVC functionality is to satisfy voltage and loading constraints. VVC functionality can be event triggered, manually executed or run periodically. It can be executed to satisfy any of the following 4 objective functions.

- Minimize subsystem power losses
- Minimize power demand
- Maximize generated reactive power
- Maximize revenue

This use case describes VVC execution via a centralized architecture.

B.4.11 DMS Performs Dynamic Voltage Reduction for Demand Response

This Use Case describes the Volt/var Control (VVC) functionality of the Distribution Network Analysis within the Distribution Management System (DMS). The VVC is executed through distributed logical architecture as opposed to a fully integrated, centralized environment. For load reduction scenarios, the VVC can lower the line voltage through a technique known as Dynamic Voltage Control (DVC).

B.4.12 DMS Initiates Relay Protection Re-coordination (*Future*)

B.5 Distributed Energy Resources Management (DRM)

Distributed Energy Resources Management (DERM), includes multiple forms of Distributed Generation (DG), storage and Demand Response (DR) resources.

B.5.1 DR/DER Resource/Asset is Registered in DERM

B.5.2 DERM Manages DR/DER Resource Availability

B.5.3 DERM Distributes DR/DER Event Schedule to Resource/Asset to Control Authority

The Utility will make use of various Distributed Energy Resources (DER) and Demand Response (DR) as needed to temporarily reduce or shift load on the distribution system. DER may include in-home devices, building management systems, and distributed generation and storage devices. The Utility may dispatch the DER for grid-reliability and/or economic reasons. DR and DER will be utilized in the following three categories:

- Grid-Connected
- Residential
- Commercial and Industrial

The Utility will implement a Distributed Energy Resource Management System (DERM) to determine the availability of the various DER for Utility use and schedule them when needed for a DR/DER event. The DERM will communicate with the above three categories of DER through the following systems:

- Distribution Management System, which acts as the control authority for Grid-Connected DER
- Home Energy Management Portal, which acts as the control authority for Residential DR (located at the Residential Customer premise)
- Commercial Building Management System, which acts as the control authority for Commercial and Industrial DR (located at the Commercial and Industrial Customer premise)
- Vehicle Charge Management System, which acts as the control authority for Electric Vehicle Charging Stations (EVCS) (located at Residential and Commercial and Industrial Customer premise)

This Use Case describes the process by which the DERM sends DR/DER event schedules to one or multiple residential, commercial and industrial, and grid-connected DER control authorities after DER have been committed and a DR/DER Event has been scheduled.

B.5.4 DMS Manages Grid-Connected DER Event Messages

The Distribution Management System (DMS) is the control authority for Grid-Connected Distributed Energy Resources (DER). Distributed Energy Resources include small-scale generation or energy storage of any kind. DER can exist in a number of forms, including photovoltaic panels, batteries, or wind generators. The location of proposed and future DER could be either inside or outside of a substation, but all DER will be associated with a particular substation and will be treated as field devices. Although the communication to the DER will occur via a substation Distribution Data Concentrator (DDC), the control authority for the DER is the DMS. This Use Case describes how the DMS manages the schedules of Grid-Connected DER.

B.5.5 Home Energy Management Platform Manages DR Event Messages

When the Distributed Energy Resource Management System schedules a Demand Response (DR) event, the event details are pushed to the Home Energy Management Platform (HEMP). The HEMP is then responsible for delivering the DR event message to Home Area Network (HAN) devices via the Advanced Metering Infrastructure (AMI) and the HAN Gateway (HANG). This use case describes how create,

modify, and cancel DR event messages are pushed from the HEMP to HAN devices via the AMI or the HANG.

B.5.6 VCMS Manages DR Event Messages (*Future*)

The Vehicle Charge Management System (VCMS) is the control authority for the Electric Vehicle Charging Stations (EVCS). EVCSs are the physical electrical cord and connectors that are specified by applicable Society of Automotive Engineers (SAE) standards to provide transfer of electric energy from the charging point to the Plug-In Electric Vehicle (PEV), which is a motorized car or truck that runs either exclusively or partially on stored battery power. An Electric Vehicle, which relies only on electric propulsion, and a Plug-In-Hybrid Vehicle, which includes an alternative source of propulsion power, are two examples of PEVs. PEVs may be located at private or public locations. This Use Case describes how the VCMS manages the schedules of the EVCS.

B.5.7 Customer Opt's Out of DR Events

When the Distributed Energy Resource Management System (DERM) schedules a Demand Response (DR) event, the event details are pushed to Home Area Network (HAN) devices, as described in Use Case DRM-05. In some cases, the Customer may choose to not participate in the DR Event. This may occur either before or after the DR Event has started. The Customer may use either the HAN device or the Home Energy Management Platform as a portal to opt out of a scheduled event. This use case describes how the CUST opts out of scheduled DR Events.

B.5.8 Verification of DR/DER Event Participation

Upon completion of a Demand Response (DR) /Distributed Energy Resources (DER) event, the Utility needs to know which customers participated in the event and which customers did not. In some cases, the Utility uses this information to determine customer compensation. In all cases, the Distributed Energy Resource Management System (DERM) uses this information to modify its forecasting algorithms to better predict load reduction for the next DR/DER event.

This Use Case describes the process by which the DERM receives participation verification from the following systems:

- Distribution Management System (for Grid-Connected DER)
- Home Energy Management Portal
- Commercial Building Management System
- Vehicle Energy Management System

B.5.9 DERM Creates DR/DER Event for Bulk Power Systems

B.5.10 DERM Generates Retail Pricing Signals (*Future*)

B.5.11 DERM Distributes Demand Response Information Messages (*Future*)

B.6 SmartEnd-Use (SEU)

B.6.1 Customer Views Historical Energy Information via Home Energy Management Platform

This Use Case describes the steps by which a Customer can access, view and analyze their historical energy usage via the Internet using the Home Energy Management Platform. The Meter Data Management System pushes updated meter usage data to the Home Energy Management Platform on a daily basis, and this information is stored internally. Upon Customer request, the Home Energy Management Platform displays the Customer's historical usage data.

B.6.2 Customer In-Home Display – Basic Functions

This Use Case describes the basic functions of the In-Home Display. As defined here, the basic functions include the display of real-time energy usage, current energy prices, and Utility-generated text messages.

B.6.3 Customer In-Home Display – Daily Bill True-Up

This Use Case describes the process of sending a Daily Bill TrueUp to the In-Home Display within a Customer premise. The In-Home Display calculates the daily and monthly usage based on regular readings received from the SmartMeter. These values are only estimates and the Daily Bill TrueUp process allows the Utility to send validated billing data to the In-Home Display for display to the Customer. The Daily Bill TrueUp message is sent as a special text message through the Field Automation Network to the SmartMeter and to the In-Home Display using the Home Area Network.

B.6.4 Customer Registers HAN Gateway to Home Energy Management Platform

This Use Case describes the process by which a Customer can register a Home Area Network (HAN) Gateway to the Home Energy Management Platform. The Utility limits the scope and number of devices that can be connected directly to the Energy Services Interface within the SmartMeter and also closely manages the communications across the Field Automation Network. Once provisioned to the SmartMeter and registered to the Home Energy Management Platform, the HAN Gateway creates the Customer HAN allowing the Customer to introduce more functionality into their HAN. The HAN Gateway includes an IP Interface for connection to the Internet allowing for third-party developed products to interact with the HAN Devices in the Customer premise.

B.6.5 Customer Uses HEMP to Provision HAN Device to HAN Gateway

This Use Case describes the steps by which a Customer can provision Home Area Network (HAN) devices to an existing HAN Gateway. The HAN Gateway communicates with the SmartMeter and allows the Customer to expand the size and scope of their HAN. Devices are authenticated on the Customer HAN through the Home Energy Management Platform, ensuring that only desired devices are allowed to communicate with the HAN infrastructure.

B.6.6 Customer Programmable Communicating Thermostat Management

This Use Case examines the management, by the Customer, of the Programmable Communicating Thermostat (PCT). Using the Programmable Communicating Thermostat and the Home Energy Management Platform (HEMP), the Customer has the option of controlling their thermostat directly or remotely. The Home Energy Management Platform is synchronized with the Programmable Communicating Thermostat such that both serve as a source of accurate, real-time information regarding the thermostat settings. The Home Energy Management Platform can communicate with the Thermostat via the Internet/Home Area Network Gateway (HANG) or through the Utility's Field Automation Network (FAN).

This Use Case covers the Customer management of the Programmable Communicating Thermostat in four sequences.

- Customer Changes Settings of PCT on UHAN and Information is Pushed to HEMP via FAN
- Customer Changes Settings of PCT on CHAN and Information is Pushed to HEMP via Internet
- Customer Changes HEMP Settings and Information is Pushed to PCT on UHAN via FAN
- Customer Changes HEMP Settings and Information is Pushed to PCT on CHAN via Internet

B.6.7 Customer Load Control Switch Management

This Use Case examines the management, by the Customer, of the Load Control Switch (LCS). Using the Load Control Switch and the Home Energy Management Platform (HEMP), the Customer has the option of controlling large energy consuming devices remotely. The Home Energy Management Platform can communicate with the Load Control Switch via the Utility's Field Automation Network (FAN) or via the Internet.

B.6.8 Customer Initiates De-Provisioning of Customer HAN Device

This Use Case describes the process by which a Customer can initiate the de-provisioning of a Home Area Network device. This Use Case applies to Home Area Network devices that are Customer owned and have been provisioned to the Home Area Network Gateway. This request could be made for a variety of reasons, such as replacing a device, moving, etc.

B.6.9 Customer In-Home Display – Prepayment (*Future*)

B.6.10 Customer Registers for DSM Rates and Programs (*Future*)

B.6.11 Customer Configures HAN Device Settings via HEMP (*Future*)

B.6.12 Customer Configures HEMP with Energy Usage Preferences (*Future*)

B.6.13 HEMP Responds to Energy Signals (*Future*)

B.6.14 HEMP Manages Customer PEV Charging (*Future*)

B.7 Home Area Network (HAN)

B.7.1 Utility Commissions Home Area Network

This Use Case describes the commissioning of the Home Area Network by the Utility. Specifically, the Utility commissions the Utility Home Area Network using the Energy Services Interface radio in the SmartMeter. In addition to the Energy Services Interface radio, the Utility Home Area Network contains other ZigBee enabled devices approved by the Utility for presence on the Utility Home Area Network. The most common devices that will be added to the Utility Home Area Network will be Programmable Communicating Thermostats, Load Control Switches, In-Home Displays and Home Area Network Gateway devices.

B.7.2 Utility Provisions HAN Device to SmartMeter

This Use Case describes the steps, initiated by the Customer, to provision a Home Area Network (HAN) Device to the SmartMeter. The Customer provides the unique identifying information for the HAN Device to the Utility, and then the Utility enters a provisioning request into its back-office systems. The Utility limits and controls the devices that can be provisioned to the SmartMeter, and the Customer has little involvement in the process beyond providing the identifying information for the HAN Device. The HAN Devices that can be provisioned to the SmartMeter include Programmable Communicating Thermostats, Load Controls Switches, In-Home Displays and HAN Gateway Devices.

B.7.3 Utility Sends Text Message to HAN Device

This Use Case describes how the Utility sends text messages to devices on the Home Area Network (HAN). This use case occurs when the Utility needs to communicate information with the customer. The messages could include marketing related correspondence or advisory messages regarding upcoming pricing changes. The text messages can reach the HAN devices via two distinct paths.

- Utility Sends Text Message to Utility HAN Devices via Field Automation Network
- Utility Sends Text Message to Customer HAN Devices via HAN Gateway

As a general rule, text messages intended for HAN devices on the Utility HAN (provisioned to the SmartMeter) will travel through the Field Automation Network. Text messages intended for HAN devices on the Customer HAN (provisioned to the HAN Gateway) will travel through the Internet. All text message confirmations will follow the same delivery path as the original text message.

B.7.4 Utility Cancels Text Message

This Use Case describes how the Utility cancels previously sent text messages to devices on the Home Area Network (HAN). When text messages are sent to Home Area Network (HAN) devices, both a start time and duration are included in the message. The HAN devices store the incoming text messages, and, at the indicated start time, they display the text messages to the Customer for the specified duration. The Utility can cancel a text message that is scheduled for display at a future start time. Upon cancellation it will be removed from the HAN device message queue. The Utility can also cancel the currently displayed message to have it removed from the HAN device display prior to its scheduled expiration time. The Utility has the option to request a confirmation that the text message was successfully cancelled.

- Utility Cancels Text Message to Utility HAN Devices via Field Automation Network
- Utility Cancels Text Message to Customer HAN Devices via HAN Gateway

As a general rule, text message cancellation messages for HAN devices on the Utility HAN (provisioned to the SmartMeter) will travel through the Field Automation Network. Text message cancellation messages intended for HAN devices on the Customer HAN (provisioned to the HAN Gateway) will travel through the Internet. All text message confirmations will follow the same delivery path as the original text message.

B.7.5 Utility Sends Pricing Signals to SmartMeter and HAN Devices

This Use Case describes how the Utility sends pricing signals to the SmartMeter and devices on the Utility Home Area Network (UHAN). This Use Case occurs when the Utility needs to communicate pricing information with the customer. This pricing information could be in the form of flat rate, time-of-use (TOU) or critical peak (CP) pricing. Pricing information is communicated to the SmartMeter using the Field Automation Network (FAN). When requested by the Pricing Signals, responses to Pricing Signals are passed from the Home Area Network devices to the Utility back-office systems via the FAN.

B.7.6 Utility Home Area Network Device Information

This Use Case describes the process by which a Utility back-office system queries the Advanced Metering Infrastructure (AMI) Head-End for information on a specific Home Area Network (HAN) device. This information returned includes device MAC Address, Installation Code, Device Type, Installation Date and Pair ID. Under specific situations, the AMI Head-End may also query the HAN device for a subset of this information.

B.7.7 Utility De-Provisions HAN Device on Utility Home Area Network

This Use Case describes the steps taken by the Utility to de-provision a Home Area Network (HAN) device from the SmartMeter. This might be done if there are issues with the HAN device or if the HAN device is to be replaced. Upon completion of this Use Case the HAN device could be re-provisioned to the Utility HAN if desired.

B.7.8 Utility De-Commissions Utility Home Area Network

This Use Case describes the process to decommission a Utility Home Area Network (HAN). This might be done if a customer moves or if problems with a HAN device necessitate resetting the Utility HAN. This process would also be completed prior to a planned SmartMeter exchange. To properly decommission the Utility HAN, the HAN devices must first be de-provisioned from the HAN. Upon completion of this Use Case, the Customer Home Area Network (if it exists) can still function, but it can't communicate with the Utility. Pricing information and Utility status messages can no longer be sent to the Home Area Network Devices via the Field Automation Network.

B.7.9 HAN Device Vendor Change Control (*Future*)

This Use Case describes the process followed by the Utility to approve Home Area Network (HAN) devices for inclusion in the HAN by communicating directly with the SmartMeter. This process is not intended to apply to HAN devices purchased by the Customer for inclusion in the HAN by communicating directly with a gateway device. This process should be followed when evaluating product enhancements from existing HAN device vendors, evaluating new HAN device vendors or evaluating HAN devices not currently allowed to communicate with the SmartMeter.

B.7.10 HAN Device Status Check (*Future*)

This Use Case describes the steps taken to remotely check the status of a Home Area Network (HAN) device operating at the Customer premise and communicating to the SmartMeter. This function could be used by Customer Service Representatives to assist in troubleshooting Customer complaints about their HAN devices. It could also be used by the Utility to gather information about which HAN devices are being used and how. We need to determine, technically, what information needs to be returned from the HAN. This will determine which ZigBee command is used.

B.8 Plug-In Electric Vehicle (PEV)

B.8.1 PEV Charging at a Public Charge Station (*Future*)

B.8.2 Customer Enrolls in Utility PEV Program (*Future*)

B.8.3 Customer Registers PEV to Home Premise (*Future*)

B.8.4 Customer PEV Charging at Home Premise EVSI (*Future*)**B.8.5 Unregistered PEV Charging at Premise EVSI (*Future*)****B.8.6 Charge Validation and Settlement via Clearinghouse (*Future*)****B.8.7 Utility Controls PEV Charging at Public Charge Station (*Future*)****B.8.8 Utility Controls Customer On-Premise PEV Charging (*Future*)****B.9 Meter Data Management (MDM)****B.9.1 MDM Distributes Daily Customer Updates (*Future*)****B.9.2 MDM Distributes Daily Meter Data (*Future*)****B.9.3 MDM Creates Billing Determinants (*Future*)****B.9.4 SmartMeter Inventory Management (*Future*)**

This Use Case describes the management of Utility owned SmartMeters. Throughout the lifecycle of the SmartMeter it will be received at the Utility from the vendor, installed at a Customer premise, tested for return to inventory and periodically retrieved for statistical sampling purposes.

At each step along the way the Meter Data Management System (MDM) must be able to account for the whereabouts of the SmartMeter and communicate this status to other systems within the Advanced Metering Infrastructure (AMI). This collaboration minimizes required human intervention in the meter reading process and maximizes the Utility's return on the metering assets.

B.10 Network**B.10.1 Field Automation Network for Advanced Metering Infrastructure**

The Advanced Metering Infrastructure (AMI) provides flexible, two-way communications between the SmartMeter and the AMI Head-End. This is accomplished through the implementation of a hierarchical, RF mesh network of devices known as the Field Automation Network (FAN). The FAN can be used for many applications including meter reading, smart end-use, and demand response.

FAN systems promise to provide advanced energy monitoring and recording, sophisticated tariff/rate program data collection, and load management command and control capabilities. Additionally, these powerful mechanisms will enable consumers to better manage their energy usage and allow the grid to run more efficiently from both a cost and energy delivery perspective. These advanced capabilities will

also allow utilities to provision and configure the advanced SmartMeters in the field, thus offering new rate programs and energy monitoring and control.

This Use Case describes the processes of data traveling via the FAN from the AMI Head-End to the SmartMeter and from the SmartMeter to the AMI Head-End.

B.10.2 Field Automation Network for Distribution Automation

The Advanced Metering Infrastructure (AMI) provides flexible, two-way communications for Distribution Automation (DA) and Distributed Energy Resource (DER) functionality between a Distribution Automation Device Controller (DADC) or a Distributed Energy Resource Controller (DERC) and the Distribution Data Concentrator (DDC). This is accomplished through the implementation of an RF mesh network of devices known as the Distribution Automation Network (DAN). The DAN can be used for many applications including DA, DER, Volt/var Management, and Fault Detection, Location, Isolation, and Restoration (FDLIR).

This Use Case describes the following processes:

- DA messages sent from the DDC to a DADC via the DAN
- DA Messages sent from a DADC to the DDC via the DAN
- DER messages sent from the DDC to a DERC via the DAN
- DER Messages sent from a DERC to the DDC via the DAN

B.10.3 Utility Home Area Network

This Use Case describes the functionality of, and devices that comprise, the Utility Home Area Network. The Utility Home Area Network is formed by the ZigBee radio in the SmartMeter and exists as a conduit to get Utility information (energy prices, Utility text messages, etc.) into the Customer premise, as well as to provide control of energy consuming devices for demand response purposes. The Utility owns and manages all Home Area Network devices that are included in the Utility Home Area Network. Together, the Utility Home Area Network and Customer Home Area Network comprise the Home Area Network.

B.10.4 Customer Home Area Network

This Use Case describes the functionality of, and devices that comprise, the Customer Home Area Network. The Customer Home Area Network is formed by one of the ZigBee radios in the Home Area Network Gateway and exists to allow the Customer to expand the number of devices on their Home Area Network. The Home Area Network Gateway also contains an IP Interface, allowing for Internet access to Home Area Network devices. The Customer owns and manages all Home Area Network devices that are included in the Customer Home Area Network. Together, the Utility Home Area Network and Customer Home Area Network comprise the Home Area Network.

B.10.5 PEV Charge Network (*Future*)

B.10.6 Substation Distribution Automation Network

B.10.7 Substation Distribution Protection Network

The deployment of Smart Grid technologies presents various new challenges to the Utility industry. For instance, the implementation of IEC 61850 and the reliance on communication networks instead of direct wiring represents a fundamental change in protection and control system design and operation.

Substation control networks are deployed in harsh environments and transport critical data, which results in demanding requirements of the network and its components. The network must have high availability and low latency, providing fast, reliable communication between networked devices. Networking equipment deployed in these networks must be environmentally hardened, as it may be deployed in enclosures with limited climate control, requiring the equipment to operate across extreme humidity and temperature ranges. Therefore, a reliable physical architecture for the network is needed along with ruggedized, highly reliable network components.

Topology selection is based on a balance of several factors. The chosen topology of a highly reliable control network should achieve the following:

- Provide high-bandwidth, low-latency communications
- Minimize or eliminate single points of failure for cabling and equipment
- Minimize infrastructure costs

This Use Case describes the data flow of high-priority protection and control functions, including IEC 61850 Generic Object-Oriented Substation Event (GOOSE) messages between protective relays and Manufacturing Message Specification (MMS) between substation devices and the Distributed Control and Data Acquisition (DCADA) within the substation via a high-speed, Ethernet communication network.

This page intentionally blank.

Appendix C KCP&L SmartGrid Master Interface List

Msg ID	Name of Process/Transaction	Description of Process/Transaction	Producer (Actor 1)	Receiver (Actor 2)	Transport Network	Network Protocols	Information Object Name	Information Object Description	Interface Standard	Standard Msg Name	Standard Msg Code	Use Case
1.a.1	Daily Bill TrueUp Msg Transfer	CIS sends Daily Bill TrueUp Msg to AHE	CIS	AHE			Daily Bill TrueUp Msg	Tunnel Text Msg from CIS to AHE that contains Daily Bill TrueUp data.	IEC 61968-9	CREATE(HANDeviceControl s)	12.19.6.290	SEU-03
1.b.1	Remote Service Order Completion Msg Transfer	AHE sends Remote Service Order Completion Msg to CIS	AHE	CIS			Remote Service Order Completion Msg	Response from MFR indicating that the Remote Service Order Request was received and implemented.	IEC 61968-9	CREATED(EndDeviceControl s)	3.31.6.68	AMI-08
2.a.1	Outage Event Msg Transfer		AHE	OMS								
2.b.1			OMS	AHE								
3.a.1	Control Signals		DAD	EMS								
4.a.1	Customer usage data (post VEE)		MDM	DERM								
4.b.1			DERM	MDM								
5.a.1	On-Demand Meter Read Request Transfer	AHE sends On-Demand Meter Read Request to MFR via FAN	AHE	MFR	FAN	L+G Proprietary	On-Demand Meter Read Request	Request from AHE to MMB's internal reading table for current meter usage data.	L+G Proprietary	Command(OnDemandRead)		AMI-02
5.a.2	On-Demand Meter Status Request Transfer	AHE sends On-Demand Meter Status Request to MFR via FAN	AHE	MFR	FAN	L+G Proprietary	On-Demand Meter Status Request	Request from AHE to MMB's internal reading table for current meter reading data. This data is used to determine meter status.	L+G Proprietary	Command(OnDemandRead)		AMI-03
5.a.3	Remote Service Order Request Transfer	AHE sends Remote Service Order Request to MFR	AHE	MFR	FAN	L+G Proprietary	Remote Service Order Request	Remote request entered into AHE by AMIOP or external system.	IEC 61968-9	CREATE(EndDeviceControl s) CREATE(MeterReadings)	3.31.6.68	AMI-08
5.a.4	Commission HAN Command Transfer	AHE sends Commission HAN Command to MFR via FAN	AHE	MFR	FAN	L+G Proprietary	Commission HAN Command	Command from the AHE to the MTR to turn on the ESI and enable the UHAN.	L+G Proprietary	Command(CommissionHAN)		HAN-01
5.a.5	Provision HAND Command Transfer	AHE sends Provision HAND Command to MFR via FAN	AHE	MFR	FAN	L+G Proprietary	Provision HAND Command	Request from AHE to MTR for HAND provisioning. Contains Meter ID, HAND MAC Address and HAND Install Code, and Allow Joining duration.	L+G - Aligns with SEP 1.0	Command(ProvisionHANDDev ices)		HAN-02
5.a.6	Text Msg Transfer	AHE sends Text Msg to MFR via FAN	AHE	MFR	FAN	L+G Proprietary	Text Msg	Request from AHE to ESI to send a text Msg to HAND. Contains text Msg, start time, duration and confirmation flag.	L+G - Aligns with SEP 1.0	Command(HANMsg)		HAN-03
5.a.7	Cancel Text Msg Request Transfer	AHE sends Cancel Text Msg Request to MFR via FAN	AHE	MFR	FAN	L+G Proprietary	Cancel Text Msg Request	Request from AHE to ESI to cancel a previously sent text Msg. Includes ID of previously sent Msg and, optionally, requests an acknowledgement of receipt.	L+G - Aligns with SEP 1.0	Command(CancelTextMsg)		HAN-04
5.a.8	Pricing Signals Transfer	AHE sends Pricing Signals to MFR via FAN	AHE	MFR	FAN	L+G Proprietary	Pricing Signals	Pricing information sent from AHE to ESI. Contains flat, time-of-use, or critical peak pricing.	L+G - Aligns with SEP 1.0	Command(HANPricing)		HAN-05
5.a.9	HAND Pairing Info Request Transfer	AHE sends HAND Pairing Info Request to MFR via FAN	AHE	MFR	FAN	L+G Proprietary	HAND Pairing Info Request	Request from AHE to ESI for HAND pairing information.	L+G - Aligns with SEP 1.0	Command(GetPairingDetails)		HAN-06
5.a.10	HAND De-Provision Request Transfer	AHE sends HAND De-Provision Request to MFR via FAN	AHE	MFR	FAN	L+G Proprietary	HAND De-Provision Request	Request sent from AHE to ESI for the de-provisioning of a HAND.	L+G - Aligns with SEP 1.0	Command(DeProvisionHANDev ices)		HAN-07
5.a.11	UHAN De-Commission Request Transfer	AHE sends UHAN De-Commission Request to MFR via FAN	AHE	MFR	FAN	L+G Proprietary	UHAN De-Commission Request	Request from AHE to ESI for de-commissioning of the UHAN.	L+G Proprietary	Command(DecommissionHAN)		HAN-08
5.a.12	DR Event Msg Transfer	AHE sends DR Event Msg to MFR via FAN	AHE	MFR	FAN	L+G Proprietary	DR Event Msg	Msg from AHE to ESI, through MFR, that contains the load curtailment details for a specific MTR. Details are based upon the type of DR event and user defined preferences in the HEMP.	L+G - Aligns with SEP 1.0	Command(LoadControl)	TBD	UDR-02
5.a.13	Gap-Filling Meter Read Request Transfer	AHE sends Gap-Filling Meter Read Request to MFR via FAN	AHE	MFR	FAN	L+G Proprietary	Gap-Filling Meter Read Request	Request from AHE to MMB for a specific set of interval and/or register MTR data.	L+G Proprietary	GET(MeterReadings)	TBD	AMI-04
5.a.14	MTR Program Update Transfer	AHE sends MTR Program Update to MFR of target MTR via FAN	AHE	MFR	FAN	L+G Proprietary	MTR Program Update	TBD	TBD	TBD	TBD	AMI-12
5.a.15	MTR Configuration Update Transfer	AHE sends MTR Configuration Update to MFR of target MTR via FAN	AHE	MFR	FAN	L+G Proprietary	MTR Configuration Update	TBD	TBD	TBD	TBD	AMI-12
5.a.16	MFR Firmware Update Transfer	AHE sends MFR Firmware Update to MFR of target MTR via FAN	AHE	MFR	FAN	L+G Proprietary	MFR Firmware Update	TBD	TBD	TBD	TBD	AMI-12
5.a.17	MMB Firmware Update Transfer	AHE sends MMB Firmware Update to MFR of target MTR via FAN	AHE	MFR	FAN	L+G Proprietary	MMB Firmware Update	TBD	TBD	TBD	TBD	AMI-12

Msg ID	Name of Process/Transaction	Description of Process/Transaction	Producer (Actor 1)	Receiver (Actor 2)	Transport Network	Network Protocols	Information Object Name	Information Object Description	Interface Standard	Standard Msg Name	Standard Msg Code	Use Case
5.a.18	ESI Firmware Update Transfer	AHE sends ESI Firmware Update to MFR of target MTR via FAN	AHE	MFR	FAN	L+G Proprietary	ESI Firmware Update	TBD	TBD	TBD	TBD	AMI-12
5.a.19	Daily Bill TrueUp Msg Transfer	AHE sends Daily Bill TrueUp Msg to MFR via FAN	AHE	MFR	FAN	L+G Proprietary	Daily Bill TrueUp Msg	Tunnel Text Msg from AHE to ESI that contains Daily Bill TrueUp data.	L+G - Aligns with SEP 1.0	Command(HANMsg)		SEU-03
5.a.20	HEMP Settings Update Transfer	AHE sends HEMP Settings Update to MFR via FAN	AHE	MFR	FAN	L+G Proprietary	HEMP Settings Update	Msg from AHE to ESI containing changes to the HEMP settings including set point, fan operation and daily/weekly schedule.	Aligns with SEP 1.0	Demand Resonse and Load Control Cluster	ZigBee SEP 1.0 § D.2	SEU-06
5.a.21	HEMP Settings Update Transfer	AHE sends HEMP Settings Update to MFR via FAN	AHE	MFR	FAN	L+G Proprietary	HEMP Settings Update	Msg from AHE to ESI containing changes to the HEMP settings. Includes schedule and on/off state.	Aligns with SEP 1.0	Demand Resonse and Load Control Cluster	ZigBee SEP 1.0 § D.2	SEU-07
5.b.1	On-Demand Meter Read Data Transfer	MFR sends On-Demand Meter Read Data to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	On-Demand Meter Read Data	Current meter usage data retrieved from MMB's internal reading table and sent to AHE.	L+G Proprietary	Response(Readings)		AMI-02
5.b.2	On-Demand Meter Status Response Transfer	MFR sends On-Demand Meter Status Response to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	On-Demand Meter Status Response	Current meter reading data retrieved from MMB's internal reading table and sent to AHE. This data is used to determine meter status.	L+G Proprietary	Response(Readings)		AMI-03
5.b.3	Aggregated Meter Read Data Transfer	MFR pulls Interval and Register Meter Read Data stored since its last data push and sends it to the AHE via FAN	MFR	AHE	FAN	L+G Proprietary	Aggregated Meter Read Data	Aggregated data (could include Interval Meter Read Data and Register Meter Read Data) from a single MTR compiled at the MFR and sent to the AHE.	L+G Proprietary	TBD		AMI-04
5.b.4	Outage Event Msg Transfer	MFR sends Outage Event Msg to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	Outage Event Msg	Msg generated by a MTR and sent from the MFR to the AHE when the MFR detects a sustained voltage loss lasting at least 30 seconds.	L+G Proprietary	Event (Endpoint Power Outage)		AMI-08
5.b.5	Restoration Event Msg Transfer	MFR sends Restoration Event Msg to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	Restoration Event Msg	Msg generated by a MTR and sent from the MFR to the AHE when the MFR detects a voltage following an outage.	L+G Proprietary	Event (Endpoint Power Restore)		AMI-08
5.b.6	Advisory Event Msg Transfer	MFR sends Advisory Event Msg to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	Advisory Event Msg	Msg generated in MTR and sent from the MFR to the AHE. Contains any MTR events defined as "advisory" that were created since the last data push.	L+G Proprietary	Various. See AMI-06 for details.	Various. See AMI-06 for details.	AMI-06
5.b.7	Alarm Event Msg Transfer	MFR sends Alarm Event Msg to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	Alarm Event Msg	Msg generated in MTR and sent from the MFR to the AHE. Contains any MTR events defined as "alarm".	L+G Proprietary	Various. See AMI-05 for details.	Various. See AMI-05 for details.	AMI-05
5.b.8	Remote Service Order Completion Msg Transfer	MFR issues Remote Service Order Completion Msg to the AHE via FAN	MFR	AHE	FAN	L+G Proprietary	Remote Service Order Completion Msg	Response from MFR indicating that the Remote Service Order Request was received and implemented.	IEC 61968-9	CREATED(EndDeviceControls) CREATED(MeterReading)		AMI-08
5.b.9	HAN Commissioned Response Transfer	MFR sends HAN Commissioned Response to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	HAN Commissioned Response Transfer	Response from the ESI to the AHE indicating that the ESI has been enabled and the UHAN has been established. Contains Meter ID and HAN Network ID.	L+G Proprietary	Response(HANCommissioned)		HAN-01
5.b.10	Ready-to-Pair Response Transfer	MFR sends Ready-to-Pair Response to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	Ready-to-Pair Response	Response from MTR to AHE indicating UHAN is commissioned and ESI is ready to begin the pairing process.	L+G - Aligns with SEP 1.0	Response(Ready-to-Pair)		HAN-02
5.b.11	Provision Complete Response Transfer	MFR sends Provision Complete Response to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	Provision Complete Response	Response from MTR to AHE indicating that HAN has been provisioned to ESI.	L+G - Aligns with SEP 1.0	Response(PairingComplete)		HAN-02
5.b.12	Text Msg Response Transfer	MFR sends Text Msg Response to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	Text Msg Response	Confirmation from ESI to AHE that CUST acknowledged receipt of text Msg. Requirement for this Msg is controlled by the Text Msg.	L+G - Aligns with SEP 1.0	Response(TextMsgCreated)		HAN-03
5.b.13	Cancel Text Msg Confirmation Transfer	MFR sends Cancel Text Msg Confirmation to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	Cancel Text Msg Confirmation	Optional Msg from ESI to AHE indicating successful cancellation of a previously sent text Msg. Requirement for this Msg is controlled by the Cancel Text Msg Request.	L+G - Aligns with SEP 1.0	Response(TextMsgCancelled)		HAN-04
5.b.14	Pricing Signals Acknowledgement Transfer	MFR sends Pricing Signals Acknowledgement to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	Pricing Signals Acknowledgement	Acknowledgement from ESI to AHE that Pricing Signals were received. Requirement for this Msg is controlled by the Pricing Signals.	L+G - Aligns with SEP 1.0	Response(HANPricing)		HAN-05
5.b.15	HAND Pairing Info Response Transfer	MFR sends HAND Pairing Info Response to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	HAND Pairing Info Response	Response from ESI to AHE containing HAND pairing information. Response includes MAC Address, Device Type and Pair ID.	L+G - Aligns with SEP 1.0	Response(PairingDetails)		HAN-06
5.b.16	HAND De-Provision Confirmation Transfer	MFR sends HAND De-Provision Confirmation to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	HAND De-Provision Confirmation	Confirmation from ESI to AHE that the HAND has been de-provisioned.	L+G - Aligns with SEP 1.0	Response(HANDDeviceDevisioned)		HAN-07
5.b.17	UHAN De-Commission Confirmation Transfer	MFR sends UHAN De-Commission Confirmation to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	UHAN De-Commission Confirmation	Response from ESI to AHE confirming that the UHAN has been de-commissioned.	L+G Proprietary	Response(HANDdecommissioned)		HAN-08

Msg ID	Name of Process/Transaction	Description of Process/Transaction	Producer (Actor 1)	Receiver (Actor 2)	Transport Network	Network Protocols	Information Object Name	Information Object Description	Interface Standard	Standard Msg Name	Standard Msg Code	Use Case
5.b.18	DR Event Received Acknowledgement Transfer	MFR sends DR Event Received Acknowledgement to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	DR Event Received Acknowledgement	Response Msg from ESI to AHE, through MFR, indicating that the demand response event has been scheduled at the PCT.	L+G - Aligns with SEP 1.0	Response(LoadControl)	TBD	UDR-02
5.b.19	Gap-Filling Meter Read Data Transfer	MFR sends Gap-Filling Meter Read Data to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	Gap-Filling Meter Read Data	Interval and/or register MTR data for a specific period of time that is retrieved from MMB and sent to AHE.	L+G Proprietary	REPLY(MeterReadings)	TBD	AMI-04
5.b.20	MTR Program Update Confirmation Transfer	MFR sends MTR Program Update Confirmation to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	MTR Program Update Confirmation	TBD	TBD	TBD	TBD	AMI-12
5.b.21	MTR Configuration Update Confirmation Transfer	MFR sends MTR Configuration Update Confirmation to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	MTR Configuration Update Confirmation	TBD	TBD	TBD	TBD	AMI-12
5.b.22	MFR Firmware Update Confirmation Transfer	MFR sends MFR Firmware Update Confirmation to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	MFR Firmware Update Confirmation	TBD	TBD	TBD	TBD	AMI-12
5.b.23	MMB Firmware Update Confirmation Transfer	MFR sends MMB Firmware Update Confirmation to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	MMB Firmware Update Confirmation	TBD	TBD	TBD	TBD	AMI-12
5.b.24	ESI Firmware Update Confirmation Transfer	MFR sends ESI Firmware Update Confirmation to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	ESI Firmware Update Confirmation	TBD	TBD	TBD	TBD	AMI-12
5.b.25	PCT Settings Update Transfer	MFR sends PCT Settings Update to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	PCT Settings Update	Msg from ESI to AHE containing changes to the PCT settings including set point, fan operation and daily/weekly schedule.	ZigBee SEP 1.0	Thermostat Settings Attribute Set	ZCL 1.0 § 6.3.2.2.2	SEU-06
5.b.26	DR Event Started Msg Transfer	MFR sends DR Event Started Msg to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	DR Event Started Msg	Msg from ESI to AHE, through MFR, indicating that the demand response event has started.	L+G - Aligns with SEP 1.0	Response(LoadControl)		UDR-02
5.b.27	DR Event Completed Msg Transfer	MFR sends DR Event Completed Msg to AHE via FAN	MFR	AHE	FAN	L+G Proprietary	DR Event Completed Msg	Msg from ESI to AHE, through MFR, indicating that the demand response event has ended.	L+G - Aligns with SEP 1.0	Response(LoadControl)		UDR-02
6.a.1	On-Demand Meter Read Request Transfer	MDM sends On-Demand Meter Read Request to appropriate AHE via ESB	MDM	AHE	ESB		On-Demand Meter Read Request	Request from MDM to AHE for current meter usage data.	IEC 61968-9	REPLY(MeterReading)		AMI-02
6.a.2	On-Demand Meter Status Request Transfer	MDM sends On-Demand Meter Status Request to appropriate AHE via ESB	MDM	AHE	ESB		On-Demand Meter Status Request	Request from DMS (or other system) to AHE for current meter status, which is accomplished through a meter reading.	IEC 61968-9	GET(MeterReading)	TBD	AMI-03
6.a.3	Remote Service Order Completion Msg Transfer											
6.b.1	On-Demand Meter Read Data Transfer	AHE sends On-Demand Meter Read Data to MDM via ESB	AHE	MDM	ESB		On-Demand Meter Read Data	Current meter usage data retrieved from MMB's internal reading table and sent from AHE to CIS (or other system).	IEC 61968-9	REPLY(MeterReading)		AMI-02
6.b.2	On-Demand Meter Status Response Transfer	AHE sends On-Demand Meter Status Response to MDM via ESB	AHE	MDM	ESB		On-Demand Meter Status Response	Current meter reading data retrieved from MMB's internal reading table and sent from AHE to DMS (or other system). This data is used to determine meter status.	IEC 61968-9	REPLY(MeterReading)	TBD	AMI-03
6.b.3	Aggregated Multi-Meter Data Transfer	AHE pulls Aggregated Meter Read Data from multiple MTRs stored since its last data push and sends it to the MDM via ESB	AHE	MDM	ESB		Aggregated Multi-Meter Data	Aggregated data from multiple MTRs compiled at the AHE and sent as a batch file to the MDM.	IEC 61968-9	TBD		AMI-04
6.b.4	Outage Event Msg Transfer	AHE sends Outage Event Msg to MDM via ESB	AHE	MDM	ESB		Outage Event Msg	Msg generated by a MTR and sent from the AHE to the MDM when the MFR detects a sustained voltage loss lasting at least 30 seconds.	IEC 61968-9	CREATED(EndDeviceEvents)	3.26.9.185	AMI-08
6.b.5	Restoration Event Msg Transfer	AHE sends Restoration Event Msg to MDM via ESB	AHE	MDM	ESB		Restoration Event Msg	Msg generated by a MTR and sent from the AHE to the MDM when the MFR detects a voltage following an outage.	IEC 61968-9	CREATED(EndDeviceEvents)	3.26.9.216	AMI-08
6.b.6	Advisory Alert Msg Transfer	AHE sends Advisory Event Msg to MDM via ESB	AHE	MDM	ESB		Advisory Event Msg	Msg sent from the AHE to the MDM. Contains any MTR events defined as "advisory" that were created since the last data push.	IEC 61968-9	CREATED(EndDeviceEvents) Various. See AMI-06 for details.	Various. See AMI-06 for details.	AMI-06
6.b.7	Alarm Event Msg Transfer	AHE sends Alarm Event Msg to MDM via ESB	AHE	MDM	ESB		Alarm Event Msg	Msg sent from the AHE to the MDM. Contains any MTR events defined as "alarm".	IEC 61968-9	CREATED(EndDeviceEvents) Various. See AMI-05 for details.	Various. See AMI-05 for details.	AMI-05
6.b.8	Remote Service Order Completion Msg Transfer	AHE forwards Remote Service Order Completion Msg to MDM	AHE	MDM	ESB		Remote Service Order Completion Msg	Response from MFR indicating that the Remote Service Order Request was received and implemented.	IEC 61968-9	CREATED(EndDeviceControl)	3.31.6.68	

Msg ID	Name of Process/Transaction	Description of Process/Transaction	Producer (Actor 1)	Receiver (Actor 2)	Transport Network	Network Protocols	Information Object Name	Information Object Description	Interface Standard	Standard Msg Name	Standard Msg Code	Use Case
6.b.9	HAN Commissioned Response Transfer	AHE sends HAN Commissioned Response to MDM via ESB	AHE	MDM	ESB		HAN Commissioned Response	Response from AHE to MDM and external system that initiated HAN Commissioning, if applicable, that ESI has been enabled and the UHAN has been established. Contains Meter ID and HAN Network ID.	IEC 61968-9	CREATED(HANDeviceEvents)	12.23.17.42	HAN-01
6.b.10	Provision Complete Response Transfer	AHE sends Provision Complete Response to MDM via ESB	AHE	MDM	ESB		Provision Complete Response	Response from AHE to MDM and HEMP indicating that HAND has been provisioned to ESI.	IEC 61968-9	CREATED(EndDeviceEvents)	12.7.16.242	HAN-02
6.b.11	Text Msg Response Transfer	AHE sends Text Msg Response to MDM via ESB	AHE	MDM	ESB		Text Msg Response	Confirmation from AHE to HEMP (or other originating system) that CUST acknowledged receipt of text Msg. Requirement for this Msg is controlled by the Text Msg. For FAN-delivered Text Msgs, AHE also sends this response to MDM.	IEC 61968-9	CREATED(HANDeviceEvents)	12.19.17.290	HAN-03
6.b.12	Cancel Text Msg Confirmation Transfer	AHE sends Cancel Text Msg Confirmation to MDM via ESB	AHE	MDM	ESB		Cancel Text Msg Confirmation	Optional Msg from AHE to HEMP (or other originating system) and MDM indicating successful cancellation of a previously sent text Msg. Requirement for this Msg is controlled by the Cancel Text Msg Request.	IEC 61968-9	CREATED(HANDeviceEvents)	12.19.17.24	HAN-04
6.b.13	Pricing Signals Acknowledgement Transfer	AHE sends Pricing Signals Acknowledgement to MDM via ESB	AHE	MDM	ESB		Pricing Signals Acknowledgement	Acknowledgement from AHE to DERM and MDM that Pricing Signals were received. Requirement for this Msg is controlled by the Pricing Signals.	IEC 61968-9	CREATED(HANDeviceEvents)	12.23.17.291	HAN-05
6.b.14	HAND De-Provision Confirmation Transfer	AHE sends HAND De-Provision Confirmation to MDM via ESB	AHE	MDM	ESB		HAND De-Provision Confirmation	Confirmation from AHE to HEMP and MDM that the HAND has been de-provisioned.	IEC 61968-9	CREATED(EndDeviceEvents)	12.39.17.212 12.40.17.212 12.41.17.212 12.42.17.212 12.43.17.212 12.44.17.212 12.45.17.212 12.46.17.212 12.47.17.212	HAN-07
6.b.15	UHAN De-Commission Confirmation Transfer	AHE sends UHAN De-Commission Confirmation to MDM via ESB	AHE	MDM	ESB		UHAN De-Commission Confirmation	Response from AHE to HEMP and MDM confirming that the UHAN has been de-commissioned.	IEC 61968-9	CREATED(HANDeviceEvents)	12.23.17.68	HAN-08
6.b.16			AHE	MDM	ESB							
6.b.17			AHE	MDM	ESB							
6.b.18			AHE	MDM	ESB							
6.b.19	MTR Program Update Confirmation Transfer	AHE sends MTR Program Update Confirmation to MDM via ESB	AHE	MDM	ESB		MTR Program Update Confirmation	TBD	TBD	TBD	TBD	AMI-12
6.b.20	MTR Configuration Update Confirmation Transfer	AHE sends MTR Configuration Update Confirmation to MDM via ESB	AHE	MDM	ESB		MTR Configuration Update Confirmation	TBD	TBD	TBD	TBD	AMI-12
6.b.21	MFR Firmware Update Confirmation Transfer	AHE sends MFR Firmware Update Confirmation to MDM via ESB	AHE	MDM	ESB		MFR Firmware Update Confirmation	TBD	TBD	TBD	TBD	AMI-12
6.b.22	MMB Firmware Update Confirmation Transfer	AHE sends MMB Firmware Update Confirmation to MDM via ESB	AHE	MDM	ESB		MMB Firmware Update Confirmation	TBD	TBD	TBD	TBD	AMI-12
6.b.23	ESI Firmware Update Confirmation Transfer	AHE sends ESI Firmware Update Confirmation to MDM via ESB	AHE	MDM	ESB		ESI Firmware Update Confirmation	TBD	TBD	TBD	TBD	AMI-12
7.a.1	Analog and Status Data, alerts											
7.b.1	Fault Detected Msg Transfer	DMS sends Fault Detected Msg to internal sub-systems (D-SCADA and OMS)	DMS	D-SCADA			Fault Detected Msg	A signal sent from the DAC to the DMS & other internal systems indicating the DAD has detected a fault.	IEC 61850	TBD		1st-01
7.b.2	Recloser Open and Fault Detected Msg Transfer	DMS sends Recloser Open and Fault Detected Msg to internal sub-systems (D-SCADA and OMS)	DMS	D-SCADA			Recloser Open & Fault Detected Msg	A signal sent from the DAC to the DMS & other internal systems indicating the Recloser is open due to a fault.	IEC 61850 or DNP3	TBD		1st-01
7.b.3	DAD Status Update Transfer	DMS sends DAD Status Update to internal sub-systems	DMS	D-SCADA			DAD Status Update	A Msg sent from the DAC to the DMS & other internal systems containing the configuration settings of the DAD.	IEC 61850 or DNP3	TBD		1st-01
7.b.4	Lock-Out Signal Transfer	DMS sends Lock-Out Signal to internal sub-systems (D-SCADA and OMS)	DMS	D-SCADA			Lock-Out Signal	A signal sent from the DAC to the DMS & other internal systems indicating the CBR is locked due to the fault.	IEC 61850 or DNP3	TBD		1st-01
7.c.1												
7.d.1												

Msg ID	Name of Process/Transaction	Description of Process/Transaction	Producer (Actor 1)	Receiver (Actor 2)	Transport Network	Network Protocols	Information Object Name	Information Object Description	Interface Standard	Standard Msg Name	Standard Msg Code	Use Case
7.e.1	Restoration requests											
7.f.1	Work order completion notifications											
7.g.1												
8.a.1	On-Demand Meter Read Request	CIS issues On-Demand Meter Read Request to MDM via ESB	CIS	MDM	ESB		On-Demand Meter Read Request	Request from CIS (or other system) to MDM for current meter usage data.	IEC 61968-9	GET(MeterReading)		AMI-02
8.b.1	On-Demand Meter Read Data Transfer	MDM sends On-Demand meter Read Data to CIS via the ESB	MDM	CIS	ESB		On-Demand Meter Read Data	Current meter usage data retrieved from MMB's internal reading table and sent from AHE to CIS (or other system).	IEC 61968-9	REPLY(MeterReading)		AMI-02
9.a.1	Historical Usage Transfer	MDM sends Historical Usage to HEMP via ESB	MDM	HEMP	ESB		Historical Usage	Response from MDM to HEMP containing historical energy usage for a specific CUST over a specified time range.	IEC 61968-9	REPLY(MeterReadings)	TBD	SEU-01
9.b.1	Historical Usage Request Transfer	HEMP sends Historical Usage Request to MDM via ESB	HEMP	MDM	ESB		Historical Usage Request	Request from HEMP to MDM for historical energy usage for a specific CUST for a specified time range.	IEC 61968-9	GET(MeterReadings)	TBD	SEU-01
10.a.1	On-Demand Meter Status Request	DMS issues On-Demand Meter Status Request to MDM via ESB	DMS	MDM	ESB		On-Demand Meter Status Request	Request from DMS (or other system) to AHE for current meter status, which is accomplished through a meter reading.	IEC 61968-9	GET(MeterReading)	TBD	AMI-03
10.a.2	Lock-Out Signal Transfer	DMS sends Lock-Out Signal to MDM via ESB	DMS	MDM	ESB		Lock-Out Signal	A signal sent from the DMS to the MDM indicating the CBR is locked due to the fault via the ESB.	IEC 61850	TBD		1st-01
10.b.1	On-Demand Meter Status Response Transfer	MDM sends On-Demand Meter Status Response to DMS via ESB	MDM	DMS	ESB		On-Demand Meter Status Response	Current meter reading data retrieved from MMB's internal reading table and sent from AHE to DMS (or other system). This data is used to determine meter status.	IEC 61968-9	REPLY(MeterReading)	TBD	AMI-03
10.b.2	Outage Event Msg Transfer	MDM sends Outage Event Msg to DMS via ESB, if necessary	MDM	DMS	ESB		Outage Event Msg	Msg generated by a MTR and sent from the MDM to the DMS when the MFR detects a sustained voltage loss lasting at least 30 seconds.	IEC 61968-9	CREATED(EndDeviceEvents)	3.26.9.185	AMI-08
10.b.3	Restoration Event Msg Transfer	MDM sends Restoration Event Msg to DMS via ESB	MDM	DMS	ESB		Restoration Event Msg	Msg generated by a MTR and sent from the MDM to the DMS when the MFR detects a voltage following an outage.	IEC 61968-9	CREATED(EndDeviceEvents)	3.26.9.216	AMI-08
11.a.1	DAD Status Request Transfer	DDC sends DAD Status Request to DAD via SDPN/DAN	DDC	DAD	DAN		DAD Status Request	A Msg sent from the DAC to the DDC & DAD containing a request for the configuration settings of the DAD.	DNP3	TBD		1st-01
11.a.2	Circuit Reconfiguration Transfer	DDC sends Circuit Reconfiguration to DAD via SDPN/DAN	DDC	DAD	DAN		Circuit Reconfiguration	A command sent from a DAC to the DAD containing the configuration settings of the DAD.	IEC 61850 or DNP3	TBD		1st-01
11.a.3	DAD Status Request Transfer	DDC sends DAD Status Request to all DADs within the area of control via the SDPN/DAN	DDC	DAD	DAN		DAD Status Request	Monitor request sent by DCADA to DAD to determine optimal system parameters.	IEC 61850 or DNP3	TBD		1st-02
11.a.4	DAD Control Signal Transfer	DDC sends DAD Control Signal to all relevant DADs via SDPN/DAN	DDC	DAD	DAN		DAD Control Signal	Updated configuration settings for a Substation or Field DAD as determined by VVC.	IEC 61850 or DNP3	TBD		1st-02
11.a.5	DAD Control Signal Transfer	DDC sends DAD Control Signal to DAD via DAN to initiate load reduction	DDC	DAD	DAN		Field DAD Control Signal	Configuration settings for a Field DAD sent from the DCADA to a Field DAD.	DNP3	TBD		1st-04
11.b.1	DAD Status Response Transfer	DAD sends DAD Status Response to DDC via SDPN/DAN	DAD	DDC	DAN		DAD Status Response	A Msg sent from a DAD to the DDC containing the configuration settings of the DAD.	DNP3	TBD		1st-01
11.b.2	DAD Status Update Transfer	DAD sends DAD Status Update to DDC via SDPN/DAN	DAD	DDC	DAN		DAD Status Update	A Msg sent from a DAD to the DAC containing the configuration settings of the DAD.	IEC 61850 or DNP3	TBD		1st-01
11.b.3	DAD Status Response Transfer	DAD sends DAD Status Response to DDC via SDPN/DAN	DAD	DDC	DAN		DAD Status Response	Response from DAD to DCADA that DAD Status has been sent.	IEC 61850 or DNP3	TBD		1st-02
11.b.4	DAD Alarm Report	Field DAD sends DAD Alarm to DDC via DAN	DAD	DDC	DAN		Field DAD Alarm	An alarm Msg sent from a Field DAD to the DCADA to report an alert condition that has occurred at the DAD.	DNP3	TBD		1st-04
11.b.5	DAD Status Report	DAD sends DAD Status Update to DDC via DAN	DAD	DDC	DAN		Field DAD Status	A Msg containing DAD status sent from a Field DAD to the DCADA.	DNP3	TBD		1st-04
12.a.1			DMS	DAC	Backhaul WAN							
12.b.1	Fault Detected Msg Transfer	DAC sends Fault Detected Msg to DMS	DAC	DMS			Fault Detected Msg	A signal sent from the DAC to the DMS & other internal systems indicating the DAD has detected a fault.	IEC 61850	TBD		1st-01

Msg ID	Name of Process/Transaction	Description of Process/Transaction	Producer (Actor 1)	Receiver (Actor 2)	Transport Network	Network Protocols	Information Object Name	Information Object Description	Interface Standard	Standard Msg Name	Standard Msg Code	Use Case
12.b.2	Estimated Fault Isolation Msg Transfer	DAC sends Estimated Fault Isolation Msg to DMS	DAC	DMS			Estimated Fault Isolation Msg	A command sent by the DAC to a DAD to isolate a fault that has occurred.	IEC 61850	TBD		1st-01
12.b.3	Recloser Open and Fault Detected Msg Transfer	DCADA sends Recloser Open and Fault Detected Msg to DMS	DAC	DMS			Recloser Open & Fault Detected Msg	A signal sent from the DAC to the DMS & other internal systems indicating the Recloser is open due to a fault.	IEC 61850 or DNP3	TBD		1st-01
12.b.4	DAD Status Update Transfer	DAC sends DAD Status Update to DMS	DAC	DMS			DAD Status Update	A Msg sent from the DAC to the DMS & other internal systems containing the configuration settings of the DAD.	IEC 61850 or DNP3	TBD		1st-01
12.b.5	Lock-Out Signal Transfer	DCADA sends Lock-Out Signal to DMS	DAC	DMS			Lock-Out Signal	A signal sent to the DAC from a DAD indicating the CBR is locked due to the fault.	IEC 61850 or DNP3	TBD		1st-01
12.b.6	Network Configuration Update Transfer	DCADA sends a distribution system Network Configuration Update to the DMS	DAC	DMS			Network Configuration Update	Updated configuration settings for relevant DADs is sent to DMS.	IEC 61850 or DNP3	TBD		1st-02
12.c.1					Backhaul WAN							
12.d.1					Backhaul WAN							
13.a.1			GIS	DMS								
14.a.1	Switch status updates, everything included in DMS-05 and DMS-06		D-SCADA	DERM								
14.b.1			DERM	D-SCADA								
14.c.1												
14.d.1												
15.a.1	Schedule DR Event Msg Transfer	DERM sends Schedule DR Event Msg to HEMP	DERM	HEMP			Schedule DR Event Msg	Msg from DERM to HEMP that initiates a utility scheduled demand response event.	IEC 61968-9	TBD		UDR-02
15.b.1	Confirmation/acknowledgement of DR event create, modify, delete, opt out information, availability info			HEMP	DERM							
16.a.1	Text Msg Transfer	HEMP sends Text Msg to IPI	HEMP	IPI	Internet	IP	Text Msg	Request from HEMP to CHR to send a text Msg to HAND. Contains text Msg, start time, duration and confirmation flag.	Tendril - Aligns with SEP 1.0			HAN-03
16.a.2	Provision HAND Command Transfer	HEMP sends Provision HAND Command to IPI	HEMP	IPI	Internet	IP	Provision HAND Command	Command from HEMP to CHR to open the provision window and allow HANDS to join the HAN.	Tendril - Aligns with SEP 1.0	Proprietary		SEU-05
16.a.3	HEMP Settings Update Transfer	HEMP sends HEMP Settings Update to IPI	HEMP	IPI	Internet	IP	HEMP Settings Update	Msg from HEMP to CHR containing changes to the HEMP settings including set point, fan operation and daily/weekly schedule.	Tendril - Aligns with SEP 1.0			SEU-06
16.a.4	HEMP Settings Update Transfer	HEMP sends HEMP Settings Update to IPI	HEMP	IPI	Internet	IP	HEMP Settings Update	Msg from HEMP to CHR containing changes to the HEMP settings. Includes schedule and on/off state.	Tendril - Aligns with SEP 1.0			SEU-07
16.a.5	HAND De-Provision Request Transfer	HEMP sends HAND De-Provision Request to IPI	HEMP	IPI	Internet	IP	HAND De-Provision Request	Request from HEMP to CHR to de-provision a HAND from the HAN.	Aligns with ZigBee SEP 1.0			SEU-08
16.a.6	Cancel Text Msg Request Transfer	HEMP sends Cancel Text Msg Request to IPI	HEMP	IPI	Internet	IP	Cancel Text Msg Request	Request from HEMP to CHR to cancel a previously sent text Msg. Includes ID of previously sent Msg and, optionally, requests and acknowledgement of receipt.	Tendril - Aligns with SEP 1.0			HAN-04
16.b.1	Text Msg Response Transfer	IPI sends Text Msg Response to HEMP	IPI	HEMP	Internet	IP	Text Msg Response	Confirmation from CHR to HEMP that CUST acknowledged receipt of text Msg. Requirement for this Msg is controlled by the Text Msg.	Tendril - Aligns with SEP 1.0			HAN-03
16.b.2	HANG Information Transfer	HANG sends HANG Information to HEMP	HANG	HEMP	Internet	IP	HANG Information	MAC Address and Install Code for the HANG. Provided by the HANG manufacturer and typically printed on a sticker applied to the device.	Tendril - Aligns with SEP 1.0	MAC Address Install Code		SEU-04
16.b.3	Ready-to-Pair Response Transfer	IPI sends Ready-to-Pair Response to HEMP	IPI	HEMP	Internet	IP	Ready-to-Pair Response	Response from CHR to HEMP acknowledging that the provision window is open and the CHR is ready to join new HANDS to the HAN.	Tendril - Aligns with SEP 1.0	Proprietary		SEU-05
16.b.4	Provision Complete Response Transfer	IPI sends Provision Complete Response to HEMP	IPI	HEMP	Internet	IP	Provision Complete Response	Response from CHR to HEMP indicating that the HAND has been provisioned to the CHR and joined the HAN.	Tendril - Aligns with SEP 1.0	Proprietary		SEU-05

Msg ID	Name of Process/Transaction	Description of Process/Transaction	Producer (Actor 1)	Receiver (Actor 2)	Transport Network	Network Protocols	Information Object Name	Information Object Description	Interface Standard	Standard Msg Name	Standard Msg Code	Use Case
16.b.5	PCT Settings Update Transfer	IPI sends PCT Settings Update to HEMP	IPI	HEMP	Internet	IP	PCT Settings Update	Msg from CHR to HEMP containing changes to the PCT settings including set point, fan operation and daily/weekly schedule.	Tendrill - Aligns with SEP 1.0			SEU-06
16.b.6	HAND De-Provision Confirmation Transfer	IPI sends HAND De-Provision Confirmation to HEMP	IPI	HEMP	Internet	IP	HAND De-Provision Confirmation	Confirmation from CHR to HEMP that HAND has been de-provisioned from HANG.	Aligns with ZigBee SEP 1.0			SEU-08
16.b.7	Cancel Text Msg Response Transfer	IPI sends Cancel Text Msg Response to HEMP	IPI	HEMP	Internet	IP	Cancel Text Msg Confirmation	Confirmation from CHR to HEMP indicating successful cancellation of a previously sent text Msg.	Tendrill - Aligns with SEP 1.0			HAN-04
17.a.1	Modify DR event, delete DR event, availability request, pricing information		DERM	BMS								
17.b.1	Confirmation/acknowledgement of DR event create, modify, delete, opt out information, availability info		BMS	DERM								
18.a.1			DERM	VCMS								
18.b.1			VCMS	DERM								
19.a.1			VCMS	EVSE								
19.b.1			EVSE	VCMS								
20.a.1	Current (projected schedules) DR available		DERM	RTO								
20.b.1	Potentially query for available DR		RTO	DERM								
21.a.1	DAD Status Request Transfer	DDC sends DAD Status Request to DAD via DAN/SDPN	DDC	DAD	SDPN		DAD Status Request	A Msg sent from the DAC to the DDC & DAD containing a request for the configuration settings of the DAD.	IEC 61850	TBD		1st-01
21.a.2	Circuit Reconfiguration Transfer	DDC sends Circuit Reconfiguration to DAD via DAN/SDPN	DDC	DAD	SDPN		Circuit Reconfiguration	A command sent from a DAC to the DAD containing the configuration settings of the DAD.	IEC 61850 or DNP3	TBD		1st-01
21.a.3	DAD Status Request Transfer	DDC sends DAD Status Request to all DADs within the area of control via DAN/SDPN	DDC	DAD	SDPN		DAD Status Request	Monitor request sent by DCADA to DAD to determine optimal system parameters.	IEC 61850 or DNP3	TBD		1st-02
21.a.4	DAD Control Signal Transfer	DDC sends DAD Control Signal to all relevant DADs via DAN/SDPN	DDC	DAD	SDPN		DAD Control Signal	Updated configuration settings for a Substation or Field DAD as determined by VVC.	IEC 61850 or DNP3	TBD		1st-02
21.a.5	DAD Control Signal Transfer	DDC sends DAD Control Signal to DAD via SDPN to initiate load reduction	DDC	DAD	SDPN		Substation DAD Control Signal	Configuration settings for a Substation DAD sent from the DCADA to a Substation DAD.	IEC 61850	TBD		1st-04
21.b.1	Fault Detected Msg Transfer	RELAY sends Fault Detected Msg to DDC via SDPN	DAD	DDC	SDPN		Fault Detected Msg	A signal sent to the DAC from a DAD indicating the DAD has detected a fault.	IEC 61850	TBD		1st-01
21.b.2	DAD Status Response Transfer	DAD sends DAD Status Response to DDC via DAN/SDPN	DAD	DDC	SDPN		DAD Status Response	A Msg sent from a DAD to the DDC containing the configuration settings of the DAD.	IEC 61850	TBD		1st-01
21.b.3	Recloser Open and Fault Detected Msg Transfer	RECL sends Recloser Open and Fault Detected Msg to DDC via SDPN	DAD	DDC	SDPN		Recloser Open & Fault Detected Msg	A signal sent to the DAC from a DAD indicating the Recloser is open due to a fault that has occurred.	IEC 61850	TBD		1st-01
21.b.4	DAD Status Update Transfer	DAD sends DAD Status Update to DDC via DAN/SDPN	DAD	DDC	SDPN		DAD Status Update	A Msg sent from a DAD to the DAC containing the configuration settings of the DAD.	IEC 61850 or DNP3	TBD		1st-01
21.b.5	Lock-Out Signal Transfer	RELAY sends Lock-Out Signal to DDC via SDPN	DAD	DDC	SDPN		Lock-Out Signal	A signal sent to the DAC from a DAD indicating the CBR is locked due to the fault.	IEC 61850 or DNP3	TBD		1st-01
21.b.6	DAD Status Response Transfer	DAD sends DAD Status Response to DDC via DAN/SDPN	DAD	DDC	SDPN		DAD Status Response	Response from DAD to DCADA that DAD Status has been sent.	IEC 61850 or DNP3	TBD		1st-02
21.b.7	DAD Alarm Report	Substation DAD sends DAD Alarm to DDC via SDPN	DAD	DDC	SDPN		Substation DAD Alarm	An alarm Msg sent from a Substation DAD to the DCADA to report an alert condition that has occurred at the DAD.	IEC 61850	TBD		1st-04
21.b.8	DAD Status Report	DAD sends DAD Status Update to DDC via SDPN	DAD	DDC	SDPN		Substation DAD Status	A Msg containing DAD status sent from a Substation DAD to the DCADA.	IEC 61850	TBD		1st-04
22.a.1	Control signals, requests (event and oscillography logs), settings		D-SCADA	DDC								
22.b.1	Analog and Status Data, alerts		DDC	D-SCADA								

Msg ID	Name of Process/Transaction	Description of Process/Transaction	Producer (Actor 1)	Receiver (Actor 2)	Transport Network	Network Protocols	Information Object Name	Information Object Description	Interface Standard	Standard Msg Name	Standard Msg Code	Use Case
23.a.1	Pricing Signals Transfer	DERM sends Pricing Signals to AHE via ESB	DERM	AHE	ESB		Pricing Signals	Pricing information sent from DERM to AHE. Contains flat, time-of-use, or critical peak pricing.	IEC 61968-9	CREATE(HANDeviceControl s)	12.23.6.291	HAN-05
23.b.1	Pricing Signals Acknowledgement Transfer	AHE sends Pricing Signals Acknowledgement to DERM via ESB	AHE	DERM	ESB		Pricing Signal Acknowledgement	Acknowledgement from AHE to MDM and DERM that Pricing Signals were received. Requirement for this Msg is controlled by the Pricing Signals.	IEC 61968-9	CREATED(HANDeviceEvent s)	12.23.17.291	HAN-05
24.a.1	DAD Status Request Transfer	DAC begins Fault Isolation Calculation by sending DAD Status Request to DDC	DAC	DDC			DAD Status Request	A Msg sent from the DAC to the DDC & DAD containing a request for the configuration settings of the DAD.	IEC 61850 or DNP3	TBD		1st-01
24.a.2	Circuit Reconfiguration Transfer	DAC sends Circuit Reconfiguration Command to DDC	DAC	DDC			Circuit Reconfiguration	A command sent from a DAC to the DAD containing the configuration settings of the DAD.	IEC 61850 or DNP3	TBD		1st-01
24.a.3	DAD Status Request Transfer	DCADA sends a DAD Status Request to DDC	DAC	DDC			DAD Status Request	Monitor request sent by DCADA to DAD to determine optimal system parameters.	IEC 61850 or DNP3	TBD		1st-02
24.a.4	DAD Control Signal Transfer	DAC creates and sends a DAD Control Signal to DDC	DAC	DDC			DAD Control Signal	Updated configuration settings for a Substation or Field DAD as determined by VVC.	IEC 61850 or DNP3	TBD		1st-02
24.a.5	DAD Control Signal Transfer	DAC sends DAD Control Signal to DDC	DAC	DDC			DAD Control Signal	Configuration settings for a Substation/Field DAD sent from the DCADA to a Substation DAD.	IEC 61850	TBD		1st-04
24.a.6	DAD Control Signal Transfer	DAC sends DAD Control Signal to DDC	DAC	DDC			Field DAD Control Signal	Configuration settings for a Field DAD sent from the DCADA to a Field DAD.	DNP3	TBD		1st-04
24.b.1	Fault Detected Msg Transfer	DDC sends Fault Detected Msg to DAC	DDC	DAC			Fault Detected Msg	A signal sent to the DAC from a DAD indicating the DAD has detected a fault.	IEC 61850	TBD		1st-01
24.b.2	DAD Status Response Transfer	DDC sends DAD Status Response to DAC	DDC	DAC			DAD Status Response	A Msg sent from a DAD to the DDC containing the configuration settings of the DAD.	IEC 61850	TBD		1st-01
24.b.3	Recloser Open and Fault Detected Msg Transfer	DDC sends Recloser Open and Fault Detected Msg to DAC	DDC	DAC			Recloser Open & Fault Detected Msg	A signal sent to the DAC from a DAD indicating the Recloser is open due to a fault that has occurred.	IEC 61850	TBD		1st-01
24.b.4	DAD Status Update Transfer	DDC sends DAD Status Update to DAC	DDC	DAC			DAD Status Update	A Msg sent from a DAD to the DAC containing the configuration settings of the DAD.	IEC 61850 or DNP3	TBD		1st-01
24.b.5	Lock-Out Signal Transfer	DDC sends Lock-Out Signal to DAC	DDC	DAC			Lock-Out Signal	A signal sent to the DAC from a DAD indicating the CBR is locked due to the fault.	IEC 61850 or DNP3	TBD		1st-01
24.b.6	DAD Status Response Transfer	DDC sends DAD Status Response to DCADA	DDC	DAC			DAD Status Response	Response from DAD to DCADA that DAD Status has been sent.	IEC 61850 or DNP3	TBD		1st-02
24.b.7	DAD Alarm Transfer	DDC sends DAD Alarm to DAC	DDC	DAC			Substation DAD Alarm	An alarm Msg sent from a Substation DAD to the DCADA to report an alert condition that has occurred at the DAD.	IEC 61850	TBD		1st-04
24.b.8	DAD Alarm Transfer	DDC sends DAD Alarm to DAC	DDC	DAC			Field DAD Alarm	An alarm Msg sent from a Field DAD to the DCADA to report an alert condition that has occurred at the DAD.	DNP3	TBD		1st-04
24.b.9	DAD Status Transfer	DDC sends DAD Status Update to DAC	DDC	DAC			Substation DAD Status	A Msg containing DAD status sent from a Substation DAD to the DCADA.	IEC 61850	TBD		1st-04
24.b.10	DAD Status Transfer	DDC sends DAD Status Update to DAC	DDC	DAC			Field DAD Status	A Msg containing DAD status sent from a Field DAD to the DCADA.	DNP3	TBD		1st-04
25.a.1	Provision HAND Command Transfer	HEMP sends Provision HAND Command to AHE via ESB	HEMP	AHE	ESB		Provision HAND Command	Request from administrative portion of HEMP to AHE for HAND provisioning. Contains Meter ID, HAND MAC Address and HAND Install Code, and Allow Joining duration.	IEC 61968-9	CREATE(HANDeviceAssets)		HAN-02
25.a.2	Text Msg Transfer	HEMP sends Text Msg to AHE via ESB	HEMP	AHE	ESB		Text Msg	Request from HEMP (or other external system) to AHE to send a text Msg to HAND. Contains text Msg, start time, duration and confirmation flag.	IEC 61968-9	CREATE(HANDeviceControl s)	12.19.6.290	HAN-03
25.a.3	Cancel Text Msg Request Transfer	HEMP sends Cancel Text Msg Request to AHE via ESB	HEMP	AHE	ESB		Cancel Text Msg Request	Request from HEMP (or other Utility back-office system) to AHE to cancel a previously sent text Msg. Includes ID of previously sent Msg and, optionally, requests an acknowledgement of receipt.	IEC 61968-9	CREATE(HANDeviceControl s)	12.19.6.24	HAN-04
25.a.4	HAND Info Request Transfer	HEMP sends HAND Info Request to AHE via ESB	HEMP	AHE	ESB		HAND Info Request	Request from HEMP (or other Utility back-office system) to AHE for HAND information.	IEC 61968-9	GET(HANDeviceAssets)		HAN-06
25.a.5	HAND Pairing Info Request Transfer	HEMP sends HAND Pairing Info Request to AHE via ESB	HEMP	AHE	ESB		HAND Pairing Info Request	Request from HEMP (or other Utility back-office system) to AHE for HAND pairing information.	IEC 61968-9	GET(HANDeviceAssets)		HAN-06

Msg ID	Name of Process/Transaction	Description of Process/Transaction	Producer (Actor 1)	Receiver (Actor 2)	Transport Network	Network Protocols	Information Object Name	Information Object Description	Interface Standard	Standard Msg Name	Standard Msg Code	Use Case
25.a.6	HAND De-Provision Request Transfer	HEMP sends HAND De-Provision Request to AHE via ESB	HEMP	AHE	ESB		HAND De-Provision Request	Request sent from HEMP to AHE for the de-provisioning of a HAND.	IEC 61968-9	DELETE(HANDeviceAssets)		HAN-07
25.a.7	UHAN De-Commission Request Transfer	HEMP sends UHAN De-Commission Request to AHE via ESB	HEMP	AHE	ESB		UHAN De-Commission Request	Request from HEMP to AHE for de-commissioning of the UHAN.	IEC 61968-9	CREATE(HANDeviceControl s)	12.23.6.68	HAN-08
25.a.8	DR Event Msg Transfer	HEMP sends DR Event Msg Transfer to AHE	HEMP	AHE	ESB		DR Event Msg	Msg from HEMP to AHE that contains the load curtailment details for a specific MTR. Details are based upon the type of DR event and user defined preferences in the HEMP.	IEC 61968-9	CREATE(HANDeviceControl s)	12.15.6.236	UDR-02
25.a.9	HEMP Settings Update Transfer	HEMP sends HEMP Settings Update to AHE via ESB	HEMP	AHE	ESB		HEMP Settings Update	Msg from HEMP to AHE containing changes to the HEMP settings including set point, fan operation and daily/weekly schedule.	IEC 61968-9	CREATE(PANDeviceAssets)		SEU-06
25.a.10	HEMP Settings Update Transfer	HEMP sends HEMP Settings Update to AHE via ESB	HEMP	AHE	ESB		HEMP Settings Update	Msg from HEMP to AHE containing changes to the HEMP settings. Includes schedule and on/off state.	IEC 61968-9	CREATE(PANDeviceAssets)		SEU-07
25.a.11	Commission HAN Command Transfer	HEMP (or other Utility back-office system) sends Commission HAN Command to AHE via ESB	HEMP	AHE	ESB		Commission HAN Command	Command from HEMP to AHE for commissioning the UHAN.	IEC 61968-9	CREATE(HANDeviceControl s)	12.23.6.42	HAN-01
25.b.1	Ready-to-Pair Response Transfer	AHE sends Ready-to-Pair Response to HEMP via ESB	AHE	HEMP	ESB		Ready-to-Pair Response	Response from AHE to HEMP indicating UHAN is commissioned and ESI is ready to begin the pairing process.	IEC 61968-9	CREATED(EndDeviceEvents)	12.7.7.76	HAN-02
25.b.2	Provision Complete Response Transfer	AHE sends Provision Complete Response to HEMP via ESB	AHE	HEMP	ESB		Provision Complete Response	Response from AHE to MDM and HEMP indicating that HAND has been provisioned to ESI.	IEC 61968-9	CREATED(EndDeviceEvents)	12.7.16.242	HAN-02
25.b.3	Text Msg Response Transfer	AHE sends Text Msg Response to HEMP via ESB	AHE	HEMP	ESB		Text Msg Response	Confirmation from AHE to HEMP (or other originating system) that CUST acknowledged receipt of text Msg. Requirement for this Msg is controlled by the Text Msg. For FAN-delivered Text Msgs, AHE also sends this response to MDM.	IEC 61968-9	CREATED(HANDeviceEvent s)	12.19.17.290	HAN-03
25.b.4	Cancel Text Msg Confirmation Transfer	AHE sends Cancel Text Msg Confirmation to HEMP via ESB	AHE	HEMP	ESB		Cancel Text Msg Confirmation	Optional Msg from AHE to HEMP (or other originating system) and MDM indicating successful cancellation of a previously sent text Msg. Requirement for this Msg is controlled by the Cancel Text Msg Request.	IEC 61968-9	CREATED(HANDeviceEvent s)	12.19.17.24	HAN-04
25.b.5	HAND Info Response Transfer	AHE sends HAND Info Response to HEMP via ESB	AHE	HEMP	ESB		HAND Info Response	Response from AHE to HEMP (or originating Utility back-office system) containing HAND information. Response includes MAC Address, Device Type, Installation Code, Installation Date and Pair ID.	IEC 61968-9	REPLY(HANDeviceAssets)		HAN-06
25.b.6	HAND Pairing Info Response Transfer	AHE sends HAND Pairing Info Response to HEMP via ESB	AHE	HEMP	ESB		HAND Pairing Info Response	Response from AHE to HEMP (or originating Utility back-office system) containing HAND pairing information. Response includes MAC Address, Device Type and Pair ID.	IEC 61968-9	REPLY(HANDeviceAssets)		HAN-06
25.b.7	HAND De-Provision Confirmation Transfer	AHE sends HAND De-Provision Confirmation to HEMP via ESB	AHE	HEMP	ESB		HAND De-Provision Confirmation	Confirmation from AHE to HEMP and MDM that the HAND has been de-provisioned.	IEC 61968-9	CREATED(EndDeviceEvents)	12.39.17.212 12.40.17.212 12.41.17.212 12.42.17.212 12.43.17.212 12.44.17.212 12.45.17.212 12.46.17.212 12.47.17.212	HAN-07
25.b.8	UHAN De-Commission Confirmation Transfer	AHE sends UHAN De-Commission Confirmation to HEMP via ESB	AHE	HEMP	ESB		UHAN De-Commission Confirmation	Response from AHE to HEMP and MDM confirming that the UHAN has been de-commissioned.	IEC 61968-9	CREATED(HANDeviceEvent s)	12.23.17.68	HAN-08
25.b.9	DR Event Received Acknowledgement Transfer	AHE sends DR Event Received Acknowledgement to HEMP via ESB	AHE	HEMP	ESB		DR Event Received Acknowledgement	Response Msg from AHE to HEMP indicating that the demand response event has been scheduled at the PCT.	IEC 61968-9	CREATED(HANDeviceEvent s)	12.15.17.236	UDR-02
25.b.10	PCT Settings Update Transfer	AHE sends PCT Settings Update to HEMP via ESB	AHE	HEMP	ESB		PCT Settings Update	Msg from AHE to HEMP containing changes to the PT settings including set point, fan operation and daily/weekly schedule.	IEC 61968-9	CREATED(PANDeviceAsset s)		SEU-06
25.b.11	DR Event Started Msg Transfer	AHE sends DR Event Started Msg to HEMP via ESB	AHE	HEMP	ESB		DR Event Started Msg	Msg from AHE to HEMP indicating that the demand response event has started.	IEC 61968-9	CREATED(HANDeviceEvent s)	TBD	UDR-02

Msg ID	Name of Process/Transaction	Description of Process/Transaction	Producer (Actor 1)	Receiver (Actor 2)	Transport Network	Network Protocols	Information Object Name	Information Object Description	Interface Standard	Standard Msg Name	Standard Msg Code	Use Case
25.b.12	DR Event Completed Msg Transfer	AHE sends DR Event Completed Msg to HEMP via ESB	AHE	HEMP	ESB		DR Event Completed Msg	Msg from AHE to HEMP indicating that the demand response event has ended.	IEC 61968-9	CREATED(HANDeviceEvents)	TBD	UDR-02
25.b.13	HAN Commissioned Response Transfer	AHE sends HAN Commissioned Response to HEMP (or originating Utility back-office system) via ESB	AHE	HEMP	ESB		HAN Commissioned Response	Response from AHE to MDM and HEMP indicating that ESI has been enabled and the UHAN has been established. Contains Meter ID and HAN Network ID.	IEC 61968-9	CREATED(HANDeviceEvents)	12.23.17.42	HAN-01
26.a.1	Create, modify, delete DR event, control signals		DDC	DER								
26.b.1	Analog and Status Data, alerts, acknowledgements		DER	DDC								
27.a.1			CIS	MWFM								
27.b.1	Customer-ready-to-disconnect Msg (triggers remote disconnect)		MWFM	CIS								
28.a.1			HANG	DER								
28.b.1			DER	HANG								
29.a.1			ALINK	HEMP								
29.b.1	Single sign on info		HEMP	ALINK								
30.a.1	Customer connectivity information		CIS	GIS								
30.b.1	Customer connectivity information		GIS	CIS								
31.a.1	Customer account information and programs		CIS	HEMP								
32.a.1	Customer account information and programs, devices to be controlled (with utility managed DR)		CIS	DERM								
33.a.1	Interval data and register reads		DMAT	MDM								
33.b.1	Request interval data		MDM	DMAT								
34.a.1			EVSE	PEV								
34.b.1			PEV	EVSE								
35.a.1			BMS	DER								
35.b.1			DER	BMS								
36.a.1			DAC	DAC								
36.b.1			DAC	DAC								
37.a.1			CIS	DMS								
38.a.1			CRM	DERM								
39.a.1			CRM	HEMP								
40.a.1			AHE	DMAT								
41.a.1												
41.b.1												
42.a.1												
42.b.1												
43.a.1												
43.b.1												
44.a.1												
44.b.1												
45.a.1												
45.b.1												

Msg ID	Name of Process/Transaction	Description of Process/Transaction	Producer (Actor 1)	Receiver (Actor 2)	Transport Network	Network Protocols	Information Object Name	Information Object Description	Interface Standard	Standard Msg Name	Standard Msg Code	Use Case
46.a.1												
46.b.1												
47.a.1												
47.b.1												
48.a.1												
48.b.1												
49.a.1												
49.b.1												
50.a.1	On-Demand Meter Read Request Transfer	MFR sends On-Demand Meter Read Request to MMB	MFR	MMB	Meter Internal	L+G Proprietary	On-Demand Meter Read Request	Request from AHE to MMB's internal reading table for current meter usage data.	L+G Proprietary	Command(OnDemandRead)		AMI-02
50.a.2	Gap-Filling Meter Read Request Transfer	MFR sends Gap-Filling Meter Read Request to MMB	MFR	MMB	Meter Internal	L+G Proprietary	Gap-Filling Meter Read Request	Request from AHE to MMB for a specific set of interval and/or register MTR data.	L+G Proprietary	GET(MeterReading)	TBD	AMI-04
50.a.3	On-Demand Meter Status Request Transfer	MFR sends On-Demand Meter Status Request to MMB	MFR	MMB	Meter Internal	L+G Proprietary	On-Demand Meter Status Request	Request from AHE to MMB's internal reading table for current meter reading data. This data is used to determine meter status.	L+G Proprietary	Command(OnDemandRead)		AMI-03
50.a.4	MTR Program Update Transfer	MFR sends MTR Program Update to MMB	MFR	MMB	Meter Internal	L+G Proprietary	MTR Program Update	TBD	TBD	TBD	TBD	AMI-12
50.a.5	MTR Configuration Update Transfer	MFR sends MTR Configuration Update to MMB	MFR	MMB	Meter Internal	L+G Proprietary	MTR Configuration Update	TBD	TBD	TBD	TBD	AMI-12
50.a.6	MMB Firmware Update Transfer	MFR sends MMB Firmware Update to MMB	MFR	MMB	Meter Internal	L+G Proprietary	MMB Firmware Update	TBD	TBD	TBD	TBD	AMI-12
50.b.1	On-Demand Meter Read Data Transfer	MMB sends On-Demand Meter Read Data to MFR	MMB	MFR	Meter Internal	L+G Proprietary	On-Demand Meter Read Data	Current meter usage data retrieved from MMB's internal reading table and sent to AHE.	L+G Proprietary	Response(Readings)		AMI-02
50.b.2	Interval Meter Read Data Transfer	MMB sends Interval Meter Read Data to MFR	MMB	MFR	Meter Internal	L+G Proprietary	Interval Meter Read Data	ANSI C12.19 formatted interval usage data generated and stored in the MMB's reading table and sent to MFR.	L+G Proprietary	IntervalReadings		AMI-04
50.b.3	Register Meter Read Data Transfer	MMB sends Register Meter Read Data to MFR	MMB	MFR	Meter Internal	L+G Proprietary	Register Meter Read Data	ANSI C12.19 formatted total daily usage reading generated and stored in the MMB's register and sent to MFR.	L+G Proprietary	RegisterReadings		AMI-04
50.b.4	Advisory Event Msg Transfer	ESI, MMB, or MFR sends Advisory Event Msg to MFR	MMB	MFR	Meter Internal	L+G Proprietary	Advisory Event Msg	Msg generated in a MTR sub-device and sent to the MFR. Contains any MTR events defined as "advisory".	L+G Proprietary	Various. See AMI-06 for details.	Various. See AMI-06 for details.	AMI-06
50.b.5	Log Only Event Msg Transfer	ESI, MMB, or MFR sends Log Only Event Msg to MFR	MMB	MFR	Meter Internal	L+G Proprietary	Log Only Event Msg	Msg generated in a MTR sub-device and sent to the MFR. Contains any MTR events defined as "log only".	L+G Proprietary	Various. See AMI-07 for details.	Various. See AMI-07 for details.	AMI-07
50.b.6	Alarm Event Msg Transfer	ESI, MMB, or MFR sends Alarm Event Msg to MFR	MMB	MFR	Meter Internal	L+G Proprietary	Alarm Event Msg	Msg generated in a MTR sub-device and sent to the MFR. Contains any MTR events defined as "alarm".	L+G Proprietary	Various. See AMI-05 for details.	Various. See AMI-05 for details.	AMI-05
50.b.7	On-Demand Meter Status Response Transfer	MMB sends On-Demand Meter Status Response to MFR	MMB	MFR	Meter Internal	L+G Proprietary	On-Demand Meter Status Response	Current meter reading data retrieved from MMB's internal reading table and sent to AHE. This data is used to determine meter status.	L+G Proprietary	Response(Readings)		AMI-03
50.b.8	MTR Program Update Confirmation Transfer	MMB sends MTR Program Update Confirmation to MFR	MMB	MFR	Meter Internal	L+G Proprietary	MTR Program Update Confirmation	TBD	TBD	TBD	TBD	AMI-12
50.b.9	MTR Configuration Update Confirmation Transfer	MMB sends MTR Configuration Update Confirmation to MFR	MMB	MFR	Meter Internal	L+G Proprietary	MTR Configuration Update Confirmation	TBD	TBD	TBD	TBD	AMI-12
50.b.10	MMB Firmware Update Confirmation Transfer	MMB sends MMB Firmware Update Confirmation to MFR	MMB	MFR	Meter Internal	L+G Proprietary	MMB Firmware Update Confirmation	TBD	TBD	TBD	TBD	AMI-12
50.b.11	Gap-Filling Meter Read Data Transfer	MMB sends Gap-Filling Meter Read Data to MFR	MMB	MFR	Meter Internal	L+G Proprietary	Gap-Filling Meter Read Data	Interval and/or register MTR data for a specific period of time that is retrieved from MMB and sent to AHE.	L+G Proprietary	REPLY(MeterReadings)	TBD	AMI-04
50.c.1					Meter Internal	L+G Proprietary			L+G Proprietary			
50.d.1					Meter Internal	L+G Proprietary			L+G Proprietary			
50.e.1					Meter Internal	L+G Proprietary			L+G Proprietary			
50.f.1	Commission HAN Command Transfer	MFR sends Commission HAN Command to ESI	MFR	ESI	Meter Internal	L+G Proprietary	Commission HAN Command	Command from the AHE to the MTR to turn on the ESI and enable the UHAN.	L+G Proprietary	Command(CommissionHAN)		HAN-01

Msg ID	Name of Process/Transaction	Description of Process/Transaction	Producer (Actor 1)	Receiver (Actor 2)	Transport Network	Network Protocols	Information Object Name	Information Object Description	Interface Standard	Standard Msg Name	Standard Msg Code	Use Case
50.f.2	Provision HAND Command Transfer	MFR sends Provision HAND Command to ESI	MFR	ESI	Meter Internal	L+G Proprietary	Provision HAND Command	Request from AHE to MTR for HAND provisioning. Contains Meter ID, HAND MAC Address and HAND Install Code, and Allow Joining duration.	L+G - Aligns with SEP 1.0	Command(ProvisionHANDevice)		HAN-02
50.f.3	Text Msg Transfer	MFR sends Text Msg to ESI	MFR	ESI	Meter Internal	L+G Proprietary	Text Msg	Request from AHE to ESI to send a text Msg to HAND. Contains text Msg, start time, duration and confirmation flag.	L+G - Aligns with SEP 1.0	Command(HANMsg)		HAN-03
50.f.4	Cancel Text Msg Request Transfer	MFR sends Cancel Text Msg Request to ESI	MFR	ESI	Meter Internal	L+G Proprietary	Cancel Text Msg Request	Request from AHE to ESI to cancel a previously sent text Msg. Includes ID of previously sent Msg and, optionally, requests an acknowledgement of receipt.	L+G - Aligns with SEP 1.0	Command(CancelTextMsg)		HAN-04
50.f.5	Pricing Signals Transfer	MFR sends Pricing Signals to ESI	MFR	ESI	Meter Internal	L+G Proprietary	Pricing Signals	Pricing information sent from AHE to ESI. Contains flat, time-of-use, or critical peak pricing.	L+G - Aligns with SEP 1.0	Command(HANPricing)		HAN-05
50.f.6	HAND Pairing Info Request Transfer	MFR sends HAND Pairing Info Request to ESI	MFR	ESI	Meter Internal	L+G Proprietary	HAND Pairing Info Request	Request from AHE to ESI for HAND pairing information.	L+G - Aligns with SEP 1.0	Command(GetPairingDetails)		HAN-06
50.f.7	HAND De-Provision Request Transfer	MFR sends HAND De-Provision Request to ESI	MFR	ESI	Meter Internal	L+G Proprietary	HAND De-Provision Request	Request sent from AHE to ESI for the de-provisioning of a HAND.	L+G - Aligns with SEP 1.0	Command(DeProvisionHANDevice)		HAN-07
50.f.8	UHAN De-Commission Request Transfer	MFR sends UHAN De-Commission Request to ESI	MFR	ESI	Meter Internal	L+G Proprietary	UHAN De-Commission Request	Request from AHE to ESI for de-commissioning of the UHAN.	L+G Proprietary	Command(DeCommissionHAN)		HAN-08
50.f.9	DR Event Msg Transfer	MFR sends DR Event Msg to ESI	MFR	ESI	Meter Internal	L+G Proprietary	DR Event Msg	Msg from AHE to ESI, through MFR, that contains the load curtailment details for a specific MTR. Details are based upon the type of DR event and user defined preferences in the HEMP.	L+G - Aligns with SEP 1.0	Command(LoadControl)	TBD	UDR-02
50.f.10	ESI Firmware Update Transfer	MFR sends ESI Firmware Update to ESI	MFR	ESI	Meter Internal	L+G Proprietary	ESI Firmware Update	TBD	TBD	TBD	TBD	AMI-12
50.f.11	Daily Bill TrueUp Msg Transfer	MFR sends Daily Bill TrueUp Msg to ESI	MFR	ESI	Meter Internal	L+G Proprietary	Daily Bill TrueUp Msg	Tunnel Text Msg from AHE to ESI that contains Daily Bill TrueUp data.	L+G - Aligns with SEP 1.0	Command(HANMsg)		SEU-03
50.f.12	HEMP Settings Update Transfer	MFR sends HEMP Settings Update to ESI	MFR	ESI	Meter Internal	L+G Proprietary	HEMP Settings Update	Msg from AHE to ESI containing changes to the HEMP settings including set point, fan operation and daily/weekly schedule.	ZigBee SEP 1.0	Thermostat Settings Attribute Set	ZCL 1.0 § 6.3.2.2.2	SEU-06
50.f.13	HEMP Settings Update Transfer	MFR sends HEMP Settings Update to ESI	MFR	ESI	Meter Internal	L+G Proprietary	HEMP Settings Update	Msg from AHE to ESI containing changes to the HEMP settings. Includes schedule and on/off state.	Aligns with SEP 1.0	Demand Resonse and Load Control Cluster	ZigBee SEP 1.0 § D.2	SEU-07
50.g.1	HAN Commissioned Response Transfer	ESI sends HAN Commissioned Response to MFR	ESI	MFR	Meter Internal	L+G Proprietary	HAN Commissioned Response	Response from the ESI to the AHE indicating that the ESI has been enabled and the UHAN has been established. Contains Meter ID and HAN Network ID.	L+G Proprietary	Response(HANCommissioned)		HAN-01
50.g.2	Ready-toPair Response Transfer	ESI sends Ready-to-Pair Response to MFR	ESI	MFR	Meter Internal	L+G Proprietary	Ready-to-Pair Response	Response from MTR to AHE indicating UHAN is commissioned and ESI is ready to begin the pairing process.	L+G - Aligns with SEP 1.0	Response(Ready-to-Pair)		HAN-02
50.g.3	Provision Complete Response Transfer	ESI sends Provision Complete Response to MFR	ESI	MFR	Meter Internal	L+G Proprietary	Provision Complete Response	Response from MTR to AHE indicating that HAND has been provisioned to ESI.	L+G - Aligns with SEP 1.0	Response(PairingComplete)		HAN-02
50.g.4	Advisory Event Msg Transfer	ESI, MMB, or MFR sends Alarm Event Msg to MFR	ESI	MFR	Meter Internal	L+G Proprietary	Advisory Event Msg	Msg generated in a MTR sub-device and sent to the MFR. Contains any MTR events defined as "advisory".	L+G Proprietary	Various. See AMI-06 for details.	Various. See AMI-06 for details.	AMI-06
50.g.5	Log Only Event Msg Transfer	ESI, MMB, or MFR sends Log Only Event Msg to MFR	ESI	MFR	Meter Internal	L+G Proprietary	Log Only Event Msg	Msg generated in a MTR sub-device and sent to the MFR. Contains any MTR events defined as "log only".	L+G Proprietary	Various. See AMI-07 for details.	Various. See AMI-07 for details.	AMI-07
50.g.6	Alarm Event Msg Transfer	ESI, MMB, or MFR sends Alarm Event Msg to MFR	ESI	MFR	Meter Internal	L+G Proprietary	Alarm Event Msg	Msg generated in a MTR sub-device and sent to the MFR. Contains any MTR events defined as "alarm".	L+G Proprietary	Various. See AMI-05 for details.	Various. See AMI-05 for details.	AMI-05
50.g.7	Text Msg Response Transfer	ESI sends Text Msg Responce to MFR	ESI	MFR	Meter Internal	L+G Proprietary	Text Msg Response	Confirmation from ESI to AHE that CUST acknowledged receipt of text Msg. Requirement for this Msg is controlled by the Text Msg.	L+G - Aligns with SEP 1.0	Response(TextMsgCreated)		HAN-03
50.g.8	Cancel Text Msg Confirmation Transfer	ESI sends Cancel Text Msg Confirmation to MFR	ESI	MFR	Meter Internal	L+G Proprietary	Cancel Text Msg Confirmation	Optional Msg from ESI to AHE indicating successful cancellation of a previously sent text Msg. Requirement for this Msg is controlled by the Cancel Text Msg Request.	L+G - Aligns with SEP 1.0	Response(TextMsgCancelled)		HAN-04
50.g.9	Pricing Signals Acknowledgement Transfer	ESI sends Pricing Signals Acknowledgement to MFR	ESI	MFR	Meter Internal	L+G Proprietary	Pricing Signals Acknowledgement	Acknowledgement from ESI to AHE that Pricing Signals were received. Requirement for this Msg is controlled by the Pricing Signals.	L+G - Aligns with SEP 1.0	Response(HANPricing)		HAN-05
50.g.10	HAND Pairing Info Response Transfer	ESI sends HAND Pairing Info Response to MFR	ESI	MFR	Meter Internal	L+G Proprietary	HAND Pairing Info Response	Response from ESI to AHE containing HAND pairing information. Response includes MAC Address, Device Type and Pair ID.	L+G - Aligns with SEP 1.0	Response(PairingDetails)		HAN-06

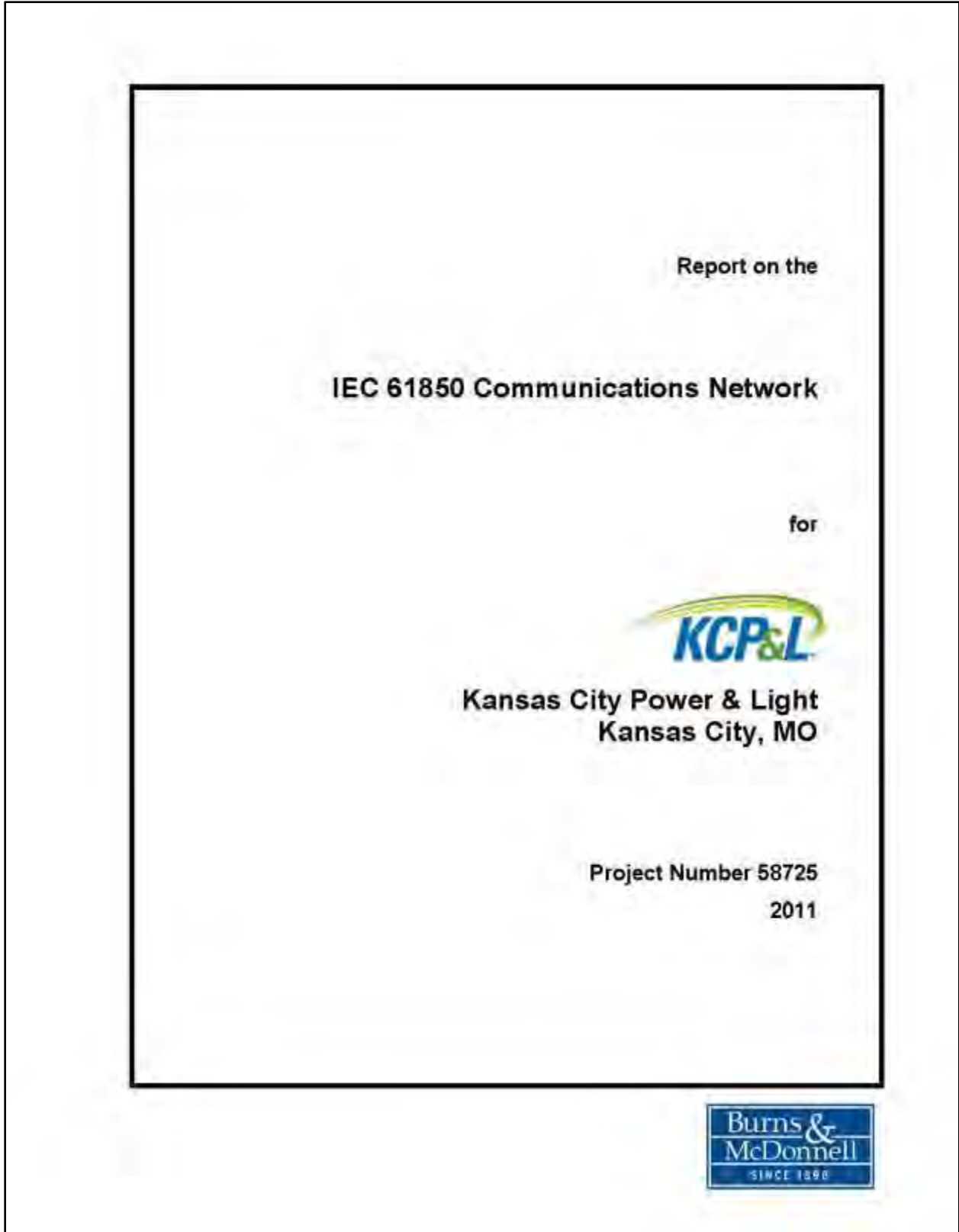
Msg ID	Name of Process/Transaction	Description of Process/Transaction	Producer (Actor 1)	Receiver (Actor 2)	Transport Network	Network Protocols	Information Object Name	Information Object Description	Interface Standard	Standard Msg Name	Standard Msg Code	Use Case
50.g.11	HAND De-Provision Confirmation Transfer	ESI sends HAND De-Provision Confirmation to MFR	ESI	MFR	Meter Internal	L+G Proprietary	HAND De-Provision Confirmation	Confirmation from ESI to AHE that the HAND has been de-provisioned.	L+G - Aligns with SEP 1.0	Response(HANDeviceDeprvisioned)		HAN-07
50.g.12	UHAN De-Commission Confirmation Transfer	ESI sends UHAN De-Commission Confirmation to MFR	ESI	MFR	Meter Internal	L+G Proprietary	UHAN De-Commission Confirmation	Response from ESI to AHE confirming that the UHAN has been de-commissioned.	L+G Proprietary	Response(HANDeCommissioned)		HAN-08
50.g.13	DR Event Received Acknowledgement Transfer	ESI sends DR Event Received Acknowledgement to MFR	ESI	MFR	Meter Internal	L+G Proprietary	DR Event Received Acknowledgement	Response Msg from ESI to AHE, through MFR, indicating that the demand response event has been scheduled at the PCT.	L+G - Aligns with SEP 1.0	Response(LoadControl)		UDR-02
50.g.14	ESI Firmware Update Confirmation Transfer	ESI sends ESI Firmware Update Confirmation to MFR	ESI	MFR	Meter Internal	L+G Proprietary	ESI Firmware Update Confirmation	TBD	TBD	TBD	TBD	AMI-12
50.g.15	PCT Settings Update Transfer	ESI sends PCT Settings Update to MFR	ESI	MFR	Meter Internal	L+G Proprietary	PCT Settings Update	Msg from ESI to AHE containing changes to the PCT settings including set point, fan operation and daily/weekly schedule.	ZigBee SEP 1.0	Thermostat Settings Attribute Set	ZCL 1.0 § 6.3.2.2.2	SEU-06
50.g.16	DR Event Started Msg Transfer	ESI sends DR Evnet Started Msg to MFR	ESI	MFR	Meter Internal	L+G Proprietary	DR Event Started Msg	Msg from ESI to AHE, through MFR, indicating that the demand response event has started.	L+G - Aligns with SEP 1.0	Response(LoadControl)	n/a	UDR-02
50.g.17	DR Event Completed Msg Transfer	ESI sends DR Evnet Completed Msg to MFR	ESI	MFR	Meter Internal	L+G Proprietary	DR Event Completed Msg	Msg from ESI to AHE, through MFR, indicating that the demand response event has ended.	L+G - Aligns with SEP 1.0	Response(LoadControl)	n/a	UDR-02
50.h.1					Meter Internal	L+G Proprietary			L+G Proprietary			
51.a.1	Text Msg Transfer	IPI sends Text Msg to CHR	IPI	CHR	HANG Internal	Tendrill Proprietary	Text Message	Request from HEMP to CHR to send a text Msg to HAND. Contains text Msg, start time, duration and confirmation flag.	Tendrill - Aligns with SEP 1.0			HAN-03
51.a.2	Provision HAND Command Transfer	IPI sends Provision HAND Command Transfer to CHR	IPI	CHR	HANG Internal	Tendrill Proprietary	Provision HAND Command	Command from HEMP to CHR to open the provision window and allow HANDS to join the HAN.	Tendrill - Aligns with SEP 1.0	Proprietary		SEU-05
51.a.3	HEMP Settings Update Transfer	IPI sends HEMP Settings Update to CHR	IPI	CHR	HANG Internal	Tendrill Proprietary	HEMP Settings Update	Msg from HEMP to CHR containing changes to the HEMP settings including set point, fan operation and daily/weekly schedule.	Tendrill - Aligns with SEP 1.0			SEU-06
51.a.4	HEMP Settings Update Transfer	IPI sends HEMP Settings Update to CHR	IPI	CHR	HANG Internal	Tendrill Proprietary	HEMP Settings Update	Msg from HEMP to CHR containing changes to the HEMP settings. Includes schedule and on/off state.	Tendrill - Aligns with SEP 1.0			SEU-07
51.a.5	HAND De-Provision Request Transfer	IPI sends HAND De-Provision Request to CHR	IPI	CHR	HANG Internal	Tendrill Proprietary	HAND De-Provision Request	Request from HEMP to CHR to de-provision a HAND from the HANG.	Aligns with ZigBee SEP 1.0			SEU-08
51.a.6	Cancel Text Msg Transfer	IPI sends Cancel Text Msg to CHR	IPI	CHR	HANG Internal	Tendrill Proprietary	Cancel Text Msg Request	Request from HEMP to CHR to cancel a previously sent text Msg. Includes ID of previously sent text Msg and, optionally, requests an acknowledgement of receipt.	Tendrill - Aligns with SEP 1.0			HAN-04
51.b.1	Text Msg Response Transfer	CHR sends Text Msg Response to IPI	CHR	IPI	HANG Internal	Tendrill Proprietary	Text Msg Response	Confirmation from CHR to HEMP that CUST acknowledged receipt of text Msg. Requirement for this Msg is controlled by the Text Msg.	Tendrill - Aligns with SEP 1.0			HAN-03
51.b.2	Ready-to-Pair Response Transfer	CHR sends Ready-to-Pair Response to IPI	CHR	IPI	HANG Internal	Tendrill Proprietary	Ready-to-Pair Response	Response from CHR to HEMP acknowledging that the prvision window is open and the CHR is ready to join new HANDS to the HAN.	Tendrill - Aligns with SEP 1.0	Proprietary		SEU-05
51.b.3	Provision Complete Response Transfer	CHR sends Provision Complete Response to IPI	CHR	IPI	HANG Internal	Tendrill Proprietary	Provision Complete Response	Response from CHR to HEMP indicating that the HAND has been provisioned to the CHR and joined the CHAN.	Tendrill - Aligns with SEP 1.0	Proprietary		SEU-05
51.b.4	PCT Settings Update Transfer	CHR sends PCT Settings Update to IPI	CHR	IPI	HANG Internal	Tendrill Proprietary	PCT Settings Update	Msg from CHR to HEMP containing changes to the PCT settings including set point, fan operation and daily/weekly schedule.	Tendrill - Aligns with SEP 1.0			SEU-06
51.b.5	HAND De-Provision Confirmation Transfer	CHR sends HAND De-Provision Confirmation to IPI	CHR	IPI	HANG Internal	Tendrill Proprietary	HAND De-Provision Confirmation	Confirmation from CHR to HEMP that HAND has been de-provisioned from HANG.	Aligns with ZigBee SEP 1.0			SEU-08
51.b.6	Cancel Text Msg Response Transfer	CHR sends Cancel Text Msg Response to IPI	CHR	IPI	HANG Internal	Tendrill Proprietary	Cancel Text Msg Confirmation	Confirmation from CHR to HEMP indicating successful cancellation of a previously sent text Msg.	Tendrill - Aligns with SEP 1.0			HAN-04
51.c.1												
51.d.1												
51.e.1												
51.f.1												

Msg ID	Name of Process/Transaction	Description of Process/Transaction	Producer (Actor 1)	Receiver (Actor 2)	Transport Network	Network Protocols	Information Object Name	Information Object Description	Interface Standard	Standard Msg Name	Standard Msg Code	Use Case
52.a.1	Text Msg Transfer	ESI sends Text Msg to HAND via UHAN	ESI	HAND	UHAN	IEEE 802.15.4	Text Msg	Request from ESI to HAND to display a text Msg. Contains text Msg, start time, duration and confirmation flag.	ZigBee SEP 1.0	Display Msg	SEP 1.0 § D.5.2.3.1	HAN-03
52.a.2	Cancel Text Msg Request Transfer	ESI sends Cancel Text Msg Request to HAND via UHAN	ESI	HAND	UHAN	IEEE 802.15.4	Cancel Text Msg Request	Request from ESI to HAND to cancel a previously sent text Msg. Includes ID of previously sent Msg and, optionally, requests an acknowledgement of receipt.	ZigBee SEP 1.0	Cancel Msg	SEP 1.0 § D.5.2.3.2	HAN-04
52.a.3	Pricing Signals Transfer	ESI sends Pricing Signals to HAND via UHAN	ESI	HAND	UHAN	IEEE 802.15.4	Pricing Signals	Pricing information sent from ESI to HAND. Contains flat, time-of-use, or critical peak pricing.	ZigBee SEP 1.0	Publish Price	SEP 1.0 § D.4.2.4.1	HAN-05
52.a.4	HAND Pairing Info Request Transfer	ESI sends HAND Pairing Info Request to HAND via UHAN	ESI	HAND	UHAN	IEEE 802.15.4	HAND Pairing Info Request	Request from ESI to HAND for HAND pairing information.	ZigBee SEP 1.0	Device Discovery	ZigBee-2007 § 2.4.2.1	HAN-06
52.a.5	HAND De-Provision Request Transfer	ESI sends HAND De-Provision Request to HAND via UHAN	ESI	HAND	UHAN	IEEE 802.15.4	HAND De-Provision Request	Request from ESI to HAND for the HAND to leave the UHAN.	ZigBee SEP 1.0	Leave Command	ZigBee-2007 § 3.4.4	HAN-07 HAN-08
52.a.6	DR Event Msg Transfer	ESI sends DR Event Msg to PCT via UHAN	ESI	PCT	UHAN	IEEE 802.15.4	DR Event Msg	Msg from ESI to PCT that contains the load curtailment details for a specific MTR. Details are based upon the type of DR event and user defined preferences in the HEMP.	ZigBee SEP 1.0	Load Control Event	n/a	UDR-02
52.a.7	Daily Bill TrueUp Msg Transfer	ESI sends Daily Bill TrueUp Msg to IHD via UHAN	ESI	IHD	UHAN	IEEE 802.15.4	Daily Bill TrueUp Msg	Tunnel Text Msg from ESI to IHD that contains Daily Bill TrueUp data.	ZigBee SEP 1.0	Display Msg	SEP 1.0 § D.5.2.3.1	SEU-03
52.a.8	Real-Time Energy Usage Response Transfer	ESI sends Real-Time Energy Usage Response to IHD via UHAN	ESI	IHD	UHAN	IEEE 802.15.4	Real-Time Energy Usage Response	Response from ESI to IHD containing real-time energy usage.	ZigBee SEP 1.0	Instantaneous Demand	SEP 1.0 § D.3.2.2.5.1	SEU-02
52.a.9	Current Price Response Transfer	ESI sends Current Price Response to IHD via UHAN	ESI	IHD	UHAN	IEEE 802.15.4	Current Price Response	Response from ESI to IHD containing current energy prices.	ZigBee SEP 1.0	Publish Price	SEP 1.0 § D.4.2.4.1	SEU-02
52.a.10	Text Msg Response Transfer	ESI sends Text Msg Response to IHD via UHAN	ESI	IHD	UHAN	IEEE 802.15.4	Text Msg Response	Response from ESI to IHD containing the latest utility-generated text Msg.	ZigBee SEP 1.0	Display Msg	SEP 1.0 § D.5.2.3.1	SEU-02
52.a.11	HEMP Settings Update Transfer	ESI sends HEMP Settings Update to PCT via UHAN	ESI	PCT	UHAN	IEEE 802.15.4	HEMP Settings Update	Msg from ESI to PCT containing changes to the HEMP settings including set point, fan operation and daily/weekly schedule.	ZigBee SEP 1.0	Thermostat Settings Attribute Cluster	ZCL 1.0 § 6.3.2.2.2	SEU-06
52.a.12	HEMP Settings Update Transfer	ESI sends HEMP Settings Update to LCS via UHAN	ESI	LCS	UHAN	IEEE 802.15.4	HEMP Settings Update	Message from ESI to LCS containing changes to the HEMP settings. Includes schedule and on/off state.	ZigBee SEP 1.0	Demand Response and Load Control Cluster	ZigBee SEP 1.0 § D.2	SEU-07
52.a.13	ZigBee Command Transfer	ESI sends ZigBee Command to HAND via UHAN	ESI	HAND	UHAN	IEEE 802.15.4	ZigBee Command	Generic ZigBee compliant command originating from either the ESI or a HAND. The destination could be a HAND or the ESI.	ZigBee SEP 1.0	Various	n/a	NWK-03
52.b.1	Text Msg Resonse Transfer	HAND sends Text Msg Response to ESI via UHAN	HAND	ESI	UHAN	IEEE 802.15.4	Text Msg Response	Confirmation from HAND to ESI that CUST acknowledged receipt of text Msg. Requirement for this Msg is controlled by the Text Msg.	ZigBee SEP 1.0	Msg Confirmation	SEP 1.0 § D.5.3.3.2	HAN-03
52.b.2	Cancel Text Msg Confirmation Transfer	HAND sends Cancel Text Msg Confirmation to ESI via UHAN	HAND	ESI	UHAN	IEEE 802.15.4	Cancel Text Msg Confirmation	Optional Msg from HAND to ESI indicating successful cancellation of a previously sent text Msg. Requirement for this Msg is controlled by the Cancel Text Msg Request.	ZigBee SEP 1.0	Msg Confirmation	SEP 1.0 § D.5.3.3.2	HAN-04
52.b.3	Pricing Signals Acknowledgement Transfer	HAND sends Pricing Signals Acknowledgement to ESI via UHAN	HAND	ESI	UHAN	IEEE 802.15.4	Pricing Signals Acknowledgement	Acknowledgement from HAND to ESI that Pricing Signals were received. Requirement for this Msg is controlled by the Pricing Signals.	ZigBee SEP 1.0	Publish Price Response	SEP 1.0 § D.4.2.4.1	HAN-05
52.b.4	HAND Pairing Info Response Transfer	HAND sends HAND Pairing Info Response to ESI via UHAN	HAND	ESI	UHAN	IEEE 802.15.4	HAND Pairing Info Response	Response from HAND to ESI containing HAND pairing information. Response includes MAC Address, Device Type and Pair ID.	ZigBee SEP 1.0	Simple Descriptor Startup Parameters Attribute Set	ZigBee 2007 § 2.3.2.5 ZCL 2008 § 3.15.2.21	HAN-06
52.b.5	DR Event Received Acknowledgement Transfer	PCT sends DR Event Received Acknowledgement to ESI via UHAN	PCT	ESI	UHAN	IEEE 802.15.4	DR Event Received Acknowledgement	Response from PCT to ESI indicating that the demand response event has been scheduled at the PCT.	ZigBee SEP 1.0	Report Event Status Command	n/a	UDR-02
52.b.6	Real-Time Energy Usage Request Transfer	IHD sends Real-Time Energy Usage Request to ESI via UHAN	IHD	ESI	UHAN	IEEE 802.15.4	Real-Time Energy Request	Request from IHD to ESI for real-time energy usage.	ZigBee SEP 1.0	Instantaneous Demand	SEP 1.0 § D.3.2.2.5.1	SEU-02
52.b.7	Current Price Request Transfer	IHD sends Current Price Request to ESI via UHAN	IHD	ESI	UHAN	IEEE 802.15.4	Current Price Request	Request from IHD to ESI for current energy prices.	ZigBee SEP 1.0	Get Current Price	SEP 1.0 § D.4.2.3.1	SEU-02
52.b.8	Text Msg Request Transfer	IHD sends Text Msg Request to ESI via UHAN	IHD	ESI	UHAN	IEEE 802.15.4	Text Msg Request	Request from IHD to ESI for latest utility-generated text Msg.	ZigBee SEP 1.0	Get Last Msg	SEP 1.0 § D.5.3.3.1	SEU-02

Msg ID	Name of Process/Transaction	Description of Process/Transaction	Producer (Actor 1)	Receiver (Actor 2)	Transport Network	Network Protocols	Information Object Name	Information Object Description	Interface Standard	Standard Msg Name	Standard Msg Code	Use Case
52.b.9	PCT Settings Update Transfer	PCT sends PCT Settings Update to ESI via UHAN	PCT	ESI	UHAN	IEEE 802.15.4	PCT Settings Update	Msg from PCT to ESI containing changes to the PCT settings including set point, fan operation and daily/weekly schedule.	ZigBee SEP 1.0	Thermostat Settings Attribute Cluster	ZCL 1.0 § 6.3.2.2.2	SEU-06
52.b.10	ZigBee Command Transfer	HAND sends ZigBee Command to ESI via UHAN	HAND	ESI	UHAN	IEEE 802.15.4	ZigBee Command	Generic ZigBee compliant command originating from either the ESI or a HAND. The destination could be a HAND or the ESI.	ZigBee SEP 1.0	Various	n/a	NWK-03
52.b.11	DR Event Started Msg Transfer	PCT sends DR Event Started Msg to ESI via UHAN	PCT	ESI	UHAN	IEEE 802.15.4	DR Event Started Msg	Msg from PCT to ESI indicating that the demand response event has started.	ZigBee SEP 1.0	Report Event Status Command	n/a	UDR-02
52.b.12	DR Event Completed Msg Transfer	PCT sends DR Evnet Completed Msg to ESI via UHAN	PCT	ESI	UHAN	IEEE 802.15.4	DR Event Completed Msg	Msg from PCT to ESI indicating that the demand response event has ended.	ZigBee SEP 1.0	Report Event Status Command	n/a	UDR-02
52.c.1	ZigBee Command Transfer	HAND sends ZigBee Command to another HAND via UHAN	HAND	HAND	UHAN	IEEE 802.15.4	ZigBee Command	Generic ZigBee compliant command originating from either the ESI or a HAND. The destination could be a HAND or the ESI.	ZigBee SEP 1.0	Various	n/a	NWK-03
53.a.1	Text Msg Transfer	CHR sends Text Msg to HAND via CHAN	CHR	HAND	CHAN	IEEE 802.15.4	Text Msg	Request from CHR to HAND to display a text Msg. Contains text Msg, start time, duration and confirmation flag.	ZigBee SEP 1.0	Display Msg	SEP 1.0 § D.5.2.3.1	HAN-03
53.a.2	HEMP Settings Update Transfer	CHR sends HEMP Settings Update to LCS via CHAN	CHR	LCS	CHAN	IEEE 802.15.4	HEMP Settings Update	Msg from CHR to LCS containing changes to the HEMP settings. Includes schedule and on/off state.	ZigBee SEP 1.0	Demand Response and Load Control Cluster	ZigBee SEP 1.0 § D.2	SEU-07
53.a.3	HAND De-Provision Request	CHR sends HAND De-Provision Request to HAND via CHAN	CHR	HAND	CHAN	IEEE 802.15.4	HAND De-Provision Request	Request from CHR to HAND to de-provision a HAND from the HANG.	ZigBee SEP 1.0	Leave Command	ZigBee 2007 § 3.4.4	SEU-08
53.a.4	ZigBee Command Transfer	CHR sends ZigBee Command to HAND via CHAN	CHR	HAND	CHAN	IEEE 802.15.4	ZigBee Command	Generic ZigBee compliant command originating from either the CHR or a HAND. The destination could be a HAND or the CHR.	ZigBee SEP 1.0	Various	n/a	NWK-04
53.a.5	Cancel Text Msg Transfer	CHR sends Cancel Text Msg request to HAND via CHAN	CHR	HAND	CHAN	IEEE 802.15.4	Cancel Text Msg Request	Request from CHR to HAND to cancel a previously sent text Msg. Includes ID of previously sent Msg and, optionally, requests an acknowledgement of receipt.	ZigBee SEP 1.0	Cancel Msg	SEP 1.0 § D.5.2.3.2	HAN-04
53.a.6	HEMP Settings Update Transfer	CHR sends HEMP Settings Update to PCT via UHAN	CHR	PCT	CHAN	IEEE 802.15.4	HEMP Settings Update	Msg from CHR to PCT containing changes to the HEMP settings including set point, fan operation and daily/weekly schedule.	ZigBee SEP 1.0	Thermostat Settings Attribute Cluster	ZCL 1.0 § 6.3.2.2.2	SEU-06
53.b.1	Text Msg Response Transfer	HAND sends Text Msg Response to CHR via CHAN	HAND	CHR	CHAN	IEEE 802.15.4	Text Msg Response	Confirmation from HAND to CHR that CUST acknowledged receipt of text Msg. Requirement for this Msg is controlled by the Text Msg.	ZigBee SEP 1.0	Msg Confirmation	SEP 1.0 § D.5.3.3.2	HAN-03
53.b.2	ZigBee Command Transfer	HAND sends ZigBee Command to CHR via CHAN	HAND	CHR	CHAN	IEEE 802.15.4	ZigBee Command	Generic ZigBee compliant command originating from either the CHR or a HAND. The destination could be a HAND or the CHR.	ZigBee SEP 1.0	Various	n/a	NWK-04
53.b.3	Cancel Text Msg Response Transfer	HAND sends Cancel Text Msg Response to CHR via CHAN	HAND	CHR	CHAN	IEEE 802.15.4	Cancel Text Msg Confirmation	Confirmation from HAND to CHR indicating successful cancellation of a previously sent text Msg.	ZigBee SEP 1.0	Msg Confirmation	SEP 1.0 § D.5.3.3.2	HAN-04
53.b.4	PCT Settings Update Transfer	PCT sends PCT Settings Update to CHR via CHAN	PCT	CHR	CHAN	IEEE 802.15.5	PCT Settings Update	Msg from PCT to CHR containing changes to the PCT settings including set point, fan operation and daily/weekly schedule.	ZigBee SEP 1.0	Thermostat Settings Attribute Cluster	ZCL 1.0 § 6.3.2.2.2	SEU-06
53.c.1	ZigBee Command Transfer	HAND sends ZigBee Command to another HAND via CHAN	HAND	HAND	CHAN	IEEE 802.15.4	ZigBee Command	Generic ZigBee compliant command originating from either the CHR or a HAND. The destination could be a HAND or the CHR.	ZigBee SEP 1.0	Various	n/a	NWK-04
54.a.1			DAD	DAD	SDPN							
54.b.1			DAD	DAD	SDPN							
55.a.1			DAD	DAD	FAN							
55.b.1			DAD	DAD	FAN							
56.a.1			DER	DER								
56.b.1			DER	DER								
57.a.1												
57.b.1												

Msg ID	Name of Process/Transaction	Description of Process/Transaction	Producer (Actor 1)	Receiver (Actor 2)	Transport Network	Network Protocols	Information Object Name	Information Object Description	Interface Standard	Standard Msg Name	Standard Msg Code	Use Case
100.a.1	Data Packet Transfer	MFR sends RF Data Packet to another MFR via RF mesh	MFR	MFR		L+G Proprietary	RF Data Packet	Any packet of data sent via RF mesh from the FANC to the MFR or from the MFR to the FANC.	L+G Proprietary	Any data transmitted via the FAN		NWK-01
101.a.1	Data Packet Transfer	FANE sends RF Data Packet to MFR via RF mesh	FANE	MFR		L+G Proprietary	RF Data Packet	Any packet of data sent via RF mesh from the FANC to the MFR or from the MFR to the FANC.	L+G Proprietary	Any data transmitted via the FAN		NWK-01
101.b.1	Data Packet Transfer	MFR sends RF Data Packet to FANE via RF mesh	MFR	FANE		L+G Proprietary	RF Data Packet	Any packet of data sent via RF mesh from the FANC to the MFR or from the MFR to the FANC.	L+G Proprietary	Any data transmitted via the FAN		NWK-01
102.a.1	Data Packet Transfer	FANR sends RF Data Packet to MFR via RF mesh	FANR	MFR		L+G Proprietary	RF Data Packet	Any packet of data sent via RF mesh from the FANC to the MFR or from the MFR to the FANC.	L+G Proprietary	Any data transmitted via the FAN		NWK-01
102.b.1	Data Packet Transfer	MFR sends RF Data Packet to FANR via RF mesh	MFR	FANR		L+G Proprietary	RF Data Packet	Any packet of data sent via RF mesh from the FANC to the MFR or from the MFR to the FANC.	L+G Proprietary	Any data transmitted via the FAN		NWK-01
103.a.1	Data Packet Transfer	FANC sends RF Data Packet to MFR via RF mesh	FANC	MFR		L+G Proprietary	RF Data Packet	Any packet of data sent via RF mesh from the FANC to the MFR or from the MFR to the FANC.	L+G Proprietary	Any data transmitted via the FAN		NWK-01
103.b.1	Data Packet Transfer	MFR sends RF Data Packet to FANC via RF mesh	MFR	FANC		L+G Proprietary	RF Data Packet	Any packet of data sent via RF mesh from the FANC to the MFR or from the MFR to the FANC.	L+G Proprietary	Any data transmitted via the FAN		NWK-01
104.a.1	Data Packet Transfer	FANE sends RF Data Packet to another FANE via RF mesh	FANE	FANE		L+G Proprietary	RF Data Packet	Any packet of data sent via RF mesh from the FANC to the MFR or from the MFR to the FANC.	L+G Proprietary	Any data transmitted via the FAN		NWK-01
105.a.1	Data Packet Transfer	FANR sends RF Data Packet to FANE via RF mesh	FANR	FANE		L+G Proprietary	RF Data Packet	Any packet of data sent via RF mesh from the FANC to the MFR or from the MFR to the FANC.	L+G Proprietary	Any data transmitted via the FAN		NWK-01
105.b.1	Data Packet Transfer	FANE sends RF Data Packet to FANR via RF mesh	FANE	FANR		L+G Proprietary	RF Data Packet	Any packet of data sent via RF mesh from the FANC to the MFR or from the MFR to the FANC.	L+G Proprietary	Any data transmitted via the FAN		NWK-01
106.a.1	Data Packet Transfer	FANC sends RF Data Packet to FANE via RF mesh	FANC	FANE		L+G Proprietary	RF Data Packet	Any packet of data sent via RF mesh from the FANC to the MFR or from the MFR to the FANC.	L+G Proprietary	Any data transmitted via the FAN		NWK-01
106.b.1	Data Packet Transfer	FANE sends RF Data Packet to FANC via RF mesh	FANE	FANC		L+G Proprietary	RF Data Packet	Any packet of data sent via RF mesh from the FANC to the MFR or from the MFR to the FANC.	L+G Proprietary	Any data transmitted via the FAN		NWK-01
107.a.1	Data Packet Transfer	FANR sends RF Data Packet to another FANR via RF mesh	FANR	FANR		L+G Proprietary	RF Data Packet	Any packet of data sent via RF mesh from the FANC to the MFR or from the MFR to the FANC.	L+G Proprietary	Any data transmitted via the FAN		NWK-01
108.a.1	Data Packet Transfer	FANC sends RF Data Packet to FANR via RF mesh	FANC	FANR		L+G Proprietary	RF Data Packet	Any packet of data sent via RF mesh from the FANC to the MFR or from the MFR to the FANC.	L+G Proprietary	Any data transmitted via the FAN		NWK-01
108.b.1	Data Packet Transfer	FANR sends RF Data Packet to FANC via RF mesh	FANR	FANC		L+G Proprietary	RF Data Packet	Any packet of data sent via RF mesh from the FANC to the MFR or from the MFR to the FANC.	L+G Proprietary	Any data transmitted via the FAN		NWK-01
109.a.1	Data Packet Transfer	AHE sends TCP/IP Data Packet to FANC via the Backhaul WAN	AHE	FANC		TCP/IP	TCP/IP Data Packet	Any TCP/IP formatted packet of data sent from the AHE to the FANC or from the FANC to the AHE.	TCP/IP	Any data transmitted via the FAN		NWK-01
109.b.1	Data Packet Transfer	FANC sends TCP/IP Data Packet to AHE via the Backhaul WAN	FANC	AHE		TCP/IP	TCP/IP Data Packet	Any TCP/IP formatted packet of data sent from the AHE to the FANC or from the FANC to the AHE.	TCP/IP	Any data transmitted via the FAN		NWK-01
110.a.1			DDC	FANC								
110.b.1			FANC	DDC								
111.a.1			FANE	DADC								
111.b.1			DADC	FANE								
112.a.1			FANE	DERC								
112.b.1			DERC	FANE								

Appendix D IEC 61850 Communications Network



IEC 61850 Substation Control Network

prepared for

**Kansas City Power & Light
Kansas City, Missouri**

January 2011

Project No. 58725

prepared by

Burns & McDonnell Engineering Company, Inc.





January 7, 2011

Scott Grafelman, P.E.
Mgr. Asset Management & Planning
Kansas City Power & Light
P.O. Box 418679
Kansas City, MO 64141-9679

KCP&L Smart Grid Demonstration Project – IEC 61850 Communications Network

Dear Mr. Grafelman:

We are pleased to submit the final version of the report *IEC 61850 Communications Network for the Midtown Substation*. This report provides recommendations for configuration of an Ethernet communications network to support protection and control functions including IEC 61850 GOOSE messaging between protective relays at the Midtown Substation. The report also includes background information which forms the basis of many aspects of the associated technical specification for this network.

Our recommendation outlines the operating parameters that should be considered during the design and equipment selection processes, as well as when implementing the communications network to support protective relaying applications. This report contains sections on the operations, infrastructure, configuration, and security which detail the impacts various decisions are likely to have on the network performance and reliability. The report is intended to be a reference for the Network Services, Substation Protection, and Relay System Protection departments of KCP&L as they work together to design and operate this network.

The following sections are included in the report:

- **Operations:** Outlines operational implications of installing communications equipment in power delivery substations.
- **Infrastructure:** Details interconnection and hardware requirements of the network.
- **Configuration:** Details device configuration parameters that should be implemented in the network hardware.
- **Security:** Details setting that should be configured to secure the network.

Thank you for the opportunity to continue our consulting services to Kansas City Power & Light.

Sincerely,

Matthew Olson P.E.
Project Manager

9480 Ward Parkway • Kansas City, MO 64114-3319
Tel: 816 333-9400 • Fax: 816 333-3699 • www.burnsmcd.com

INDEX AND CERTIFICATION

IEC 61850 Substation Control Network

Project 58725

Report Index

<u>Section Number</u>	<u>Section Title</u>	<u>Number of Pages</u>
1	Introduction	1
2	Operations	2
3	Network Infrastructure	10
4	Network Performance	6
5	Security	2
6	Recommendations	1
Appendix A	Specification	4

Certification

I hereby certify, as a Professional Engineer in the state of Missouri, that the information in the document was assembled under my direct personal charge. This report is not intended or represented to be suitable for reuse by the Kansas City Power & Light or others without specific verification or adaptation by the Engineer. This certification is made in accordance with the provisions of the applicable laws and rules of the State of Missouri.



[Handwritten Signature]
 James G. Cupp, PE Missouri License # 25698
 Date: 1/7/11
 (Reproductions are not valid unless signed, dated, and embossed with Engineer's seal)

TABLE OF CONTENTS

	<u>Page No.</u>
1.0 INTRODUCTION	1-1
2.0 OPERATIONS	2-1
2.1 Network Management Strategy	2-1
2.2 Documentation	2-1
2.3 Deployment and Maintenance	2-2
3.0 NETWORK INFRASTRUCTURE	3-1
3.1 Network Architecture	3-1
3.1.1 Network Topology	3-1
3.1.2 Fiber Optic Infrastructure	3-2
3.2 Midtown Substation Network Configuration	3-3
3.2.1 Electrical and Communications Network Topology	3-3
3.2.2 Hardware Requirements	3-6
3.2.3 Physical Considerations	3-7
3.2.4 Reliability versus Complexity	3-7
3.3 Environmental and Physical Hardware Requirements	3-9
3.3.1 Environmental Operating Requirements	3-9
3.3.2 Substation Integration Requirements	3-10
4.0 NETWORK PERFORMANCE	4-1
4.1 Latency and Jitter Requirements	4-1
4.1.1 Quality of Service	4-1
4.1.2 Application of VLANs	4-2
4.1.3 Broadcast Storm Control and Port Rate Limiting	4-2
4.2 Network Fault Recovery	4-3
4.2.1 Network Fault Recovery in Ethernet Switches	4-3
4.2.2 Network Fault Recovery in Connected Equipment	4-4
4.2.3 Unidirectional Link Failure Detection	4-5
4.3 Network Management	4-5
5.0 SECURITY	5-1
5.1 Zones of Security	5-1
5.2 Regulatory Compliance	5-1
5.3 Other Security Considerations	5-2
6.0 RECOMMENDATIONS	6-1
6.1 Summary of Analysis	6-1
6.2 Key Recommendations	6-1

APPENDIX A - SPECIFICATION

LIST OF FIGURES

<u>Figure No.</u>		<u>Page No.</u>
3.1	Midtown Substation One Line Diagram.....	3-4
3.2	Midtown Substation IEC 61850 Information Flow.....	3-5
3.3	Proposed Midtown Substation Ethernet Network Configuration.....	3-5
3.4	Proposed Midtown Substation Switchgear Enclosure Wiring.....	3-6
3.5	Proposed Midtown Substation Fiber Routing.....	3-8
3.6	Network Hardware Mounted in Panel.....	3-11

1.0 INTRODUCTION

Kansas City Power & Light (KCP&L) is currently conducting its Smart Grid Demonstration Project, which seeks to deploy a broad range of advanced power delivery technologies. One of the key initiatives being pursued is the “Smart Substation”, an upgrade to KCP&L’s Midtown Substation that distributes electric power to the Green Impact Zone. This project includes upgrades to protection and control equipment and the deployment of an Ethernet-based substation control network utilizing the IEC 61850 network architecture.

This report presents a high-level design for the IEC 61850 control network, and provides recommended specifications for the design and procurement of the network. This report provides recommendations for designing, provisioning, and operating an IEC 61850 control network jointly between the Network Services, Substation Protection, and Relay System Protection departments of KCP&L. The recommendations provided are not all-inclusive, but are meant to identify the new operating and design requirements to each department operating this joint network.

The recommended specifications provided in this report are universally applicable to IEC 61850 networks at KCP&L, and not limited to Midtown Substation. Many of the recommendations assume that the networks will be deployed in distribution automation applications—other considerations may apply when deploying IEC 61850 networks in transmission infrastructure.

Topics discussed in this report include:

- Documentation and Operating Considerations
- Network Topology and Fiber Infrastructure
- Network Availability and Reliability
- Network Security

* * * * *

2.0 OPERATIONS

The deployment of Smart Grid technologies presents various new challenges to the utility industry. For instance, the implementation of IEC 61850 and the reliance on communication networks instead of direct wiring represents a fundamental change in protection and control system design and operation. This shift in philosophy requires different departments within an organization to bring their various knowledge bases and skill sets together. In many cases, these are departments that have limited experience working together. Therefore it is beneficial for these groups to develop a strategic plan defining each group's roles and responsibilities in operating and maintaining new assets. Deployment of IEC 61850 networks requires Network Services, Substation Protection, and Relay System Protection departments to develop such strategies for a number of items including network documentation, deployment, and maintenance.

2.1 NETWORK MANAGEMENT STRATEGY

Other utilities have assigned the responsibility for managing all protection and control equipment, including the network hardware and associated access credentials, to the protection control engineering and maintenance departments. Enterprise change management processes are often established to facilitate incorporation of the expertise of the network engineering and security groups into the network. These groups are involved in the equipment selection, network design, and modification processes before implementation. In addition, they provide consultation and assist in troubleshooting on an as needed basis.

2.2 DOCUMENTATION

The IEC 61850 network should be treated like any other protection and control system, and should only be used for protection and control purposes. Using a dedicated network for protection and control prevents other network systems or applications in the substation from being required to follow the documentation, testing, and outage coordination procedures required for changes to protection and control systems. Therefore, it is advantageous to keep complete documentation readily available to substation personnel who may need access. Network device settings should be recorded and filed with the associated relay settings and other substation

documentation. Likewise, the physical wiring of the network should be documented on drawings maintained with the related substation drawings.

2.3 DEPLOYMENT AND MAINTANANCE

The IEC 61850 network equipment will be installed in limited-access areas such as distribution switchgear, which can be hazardous to personnel. The network equipment should only be installed and serviced by relay technicians or other personnel trained to work in these hazardous areas.

Field deployment of incorrect equipment configurations or settings could negatively impact the reliability of the power grid. Therefore, new settings should be verified in a laboratory environment prior to actual field deployment. Any changes to the settings should be coordinated with the Electrical System Operator in order to obtain scheduled outages. These changes should be performed onsite while locally connected to the network, removing any risk of a configuration change disabling the network and interrupting service.

Spare network hardware should be stored and maintained following the processes currently in place for protection and control equipment. The network devices should be capable of copying their configuration data and firmware to locally attached flash memory on a daily basis to facilitate a rapid and up-to-date transfer of the configuration to a spare device if needed. This aids rapid deployment and field replacement of networking equipment by providing the substation technicians who maintain the network access to equipment and configuration information.

By implementing the above recommendations, a clear understanding of roles and responsibilities can be established while incorporating the collective knowledge of the enterprise into the design and operation of the IEC 61850 network.

* * * * *

3.0 NETWORK INFRASTRUCTURE

Substation control networks are deployed in harsh environments and transport critical data, which results in demanding requirements of the network and its components. The network must have high availability and low latency, providing fast, reliable communication between networked devices. Networking equipment deployed in these networks must be environmentally hardened, as it may be deployed in enclosures with limited climate control, requiring the equipment to operate across extreme humidity and temperature ranges. Therefore, a reliable physical architecture for the network is needed along with ruggedized, highly reliable network components. Recommended network architecture and hardware requirements are presented below.

3.1 NETWORK ARCHITECTURE

The recommended IEC 61850 substation control network configuration consists of redundant 1 Gbps Ethernet backbones routed throughout the substation. These backbones will interconnect remote primary and backup Ethernet switches installed in various switchgear enclosures to main Ethernet switches located in the main control enclosure. Protective relays, equipped with redundant Ethernet ports, will connect to the appropriate primary and backup remote switches using 100 Mbps Ethernet.

3.1.1 Network Topology

Topology selection is based on a balance of several factors. The chosen topology of a highly reliable control network should achieve the following.

- Provide high-bandwidth, low-latency communications
- Minimize or eliminate single points of failure for cabling and equipment
- Minimize infrastructure costs

The recommended approach is to deploy the IEC 61850 network using a redundant Ethernet ring architecture.

Ring architectures allow for self-healing networks, increasing availability and reliability. The Ethernet switches comprising the network are arranged in rings, providing redundant pathways between two points in the network via the Ethernet backbone. This configuration protects

against loss of communication between devices due to failure of a communication link or loss of an intermediate switch. Loss of communication only occurs when there is a failure in the edge switch to which one of the two communicating devices is connected.

To further increase reliability, redundant rings can be deployed. This allows devices with redundant Ethernet interfaces to take advantage of a standby Ethernet network, reducing the probability of a loss of station control due to failure of any single piece of network equipment. This redundant ring configuration eliminates single points of failure for all Ethernet hardware when the communication devices are configured in fail-over mode.

Aside from enhanced fault recovery, the additional redundancy can significantly ease maintenance of the network, as any single network device can be completely removed from service without network disruption or loss of station control. Direct connections should be made between primary and backup switches in each control enclosure, providing a local link for traffic in the event any enclosure is isolated from the rest of the network.

3.1.2 Fiber Optic Infrastructure

The network should be constructed using fiber optic cabling in order to be confidently extended beyond the control enclosure and throughout the substation switchyard. Fiber-based communications are immune to the electromagnetic interference (EMI) that is prevalent in high voltage facilities. The use of fiber allows the Ethernet network cabling to be installed along side control cables without concern about equipment damage due to ground potential differences within the substation or EMI affecting inter-relay communications.

Gigabit Ethernet can be carried over multimode (1000BaseSX) or single-mode fiber (1000BaseLX). Communication links using 1000BaseSX over distances in excess of 500 feet are susceptible to signal degradation due to dispersion. Therefore, 1000BaseLX, which can reach distances of 10 kilometers or more, is recommended for the 1 Gbps Ethernet backbones connecting the switches distributed throughout the substation. Deployment of single-mode fiber will allow the network to be extended as required, without distance limitation concerns, and will also allow higher bandwidth to be used in the future. (10 Gbps Ethernet is easily supported on

single-mode fiber.) This additional bandwidth capacity could be valuable should future plans involve more data intensive applications such as IEC 61850 process bus and phasor measurement. The cost difference between deploying single-mode and multimode fiber is negligible.

While single-mode fiber is optimal for the Ethernet backbone, multimode fiber should be used for the shorter 100 Mbps Ethernet (100BaseFX) connections between relays and switches. This is because the Ethernet interfaces commonly available in the relays only support multimode fiber.

3.2 MIDTOWN SUBSTATION NETWORK CONFIGURATION

3.2.1 Electrical and Communications Network Topology

The electrical network configuration at Midtown Substation consists of a 161-kV four bay ring bus with a transmission line and distribution transformer in each bay. Three of the four distribution transformers have dual secondary windings, each feeding separate distribution buses connected to four distribution feeders. Each distribution bus has a tie to another bus that forms a ring around the low side of the substation. This configuration is shown in Figure 3.1.

A key part of the Smart Substation design is to automate restoration of service to customers after a fault. Breakers will be operated using traditional hard wired relay logic. Generic Object Oriented Substation Event (GOOSE) messaging will be used to operate the tie bus remediation scheme, serving as a test case to monitor the control function of the IEC 61850 network.

Distributing the communications infrastructure into the switchgear ensures that communication between adjacent switchgear can remain operational even if a failure damages other parts of the station. Key benefits of substation automation may not be realized unless a decentralized communication design that mimics the automation architecture is used. See Figure 3.2 for a diagram of GOOSE information flow at the Midtown Substation.

IEC 61850 Substation Control Network

Network Infrastructure

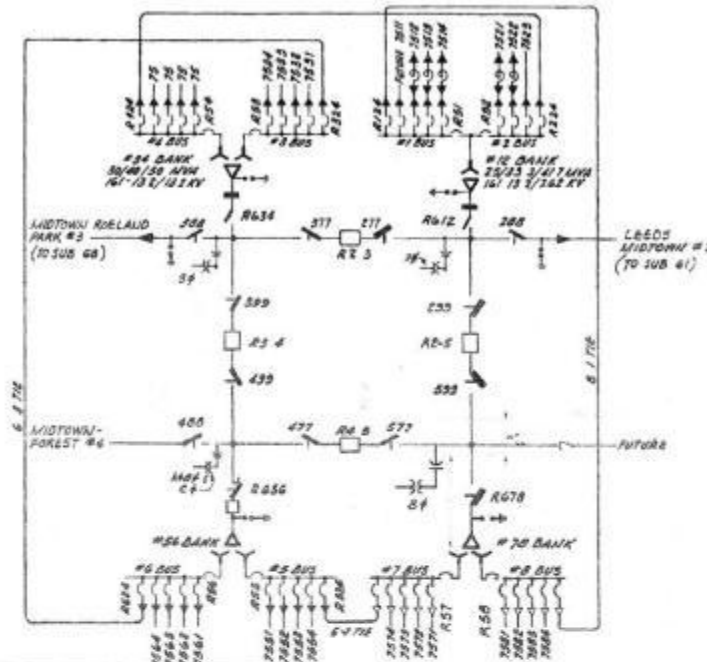


Figure 3.1. Midtown Substation One Line Diagram

It is recommended that the switches comprising the Ethernet rings be interconnected in a configuration mimicking the electrical configuration of the station. Each Ethernet ring should contain one main switch located in the control enclosure, and four remote switches distributed throughout the substation switchgear. This gives control equipment in each switchgear enclosure direct access to its adjacent facilities without passing network traffic through a centralized switch. This arrangement (illustrated in Figure 3.3) reduces latency for GOOSE messages and decentralizes the risk of failures in other parts of the station without introducing excessive latency for SCADA messages between the SICAM data concentrator and relays using the IEC 61850 Manufacture Message Specification (MMS). The redundant main switches in the control enclosure will connect to the Siemens SICAM data concentrator, transformer relay equipment, and the human machine interface. The remote switches will connect to the relay equipment located in the switchgear and to the 1000BaseLX Ethernet backbone. This arrangement is illustrated in Figure 3.3.

IEC 61850 Substation Control Network Network Infrastructure

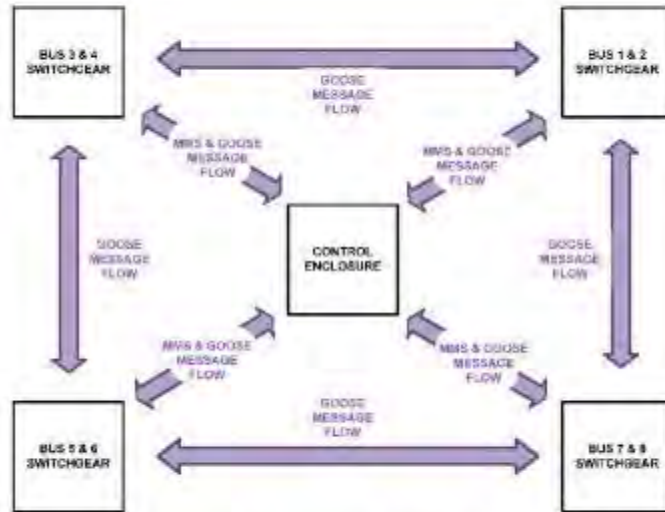


Figure 3.2. Midtown Substation IEC 61850 Information Flow

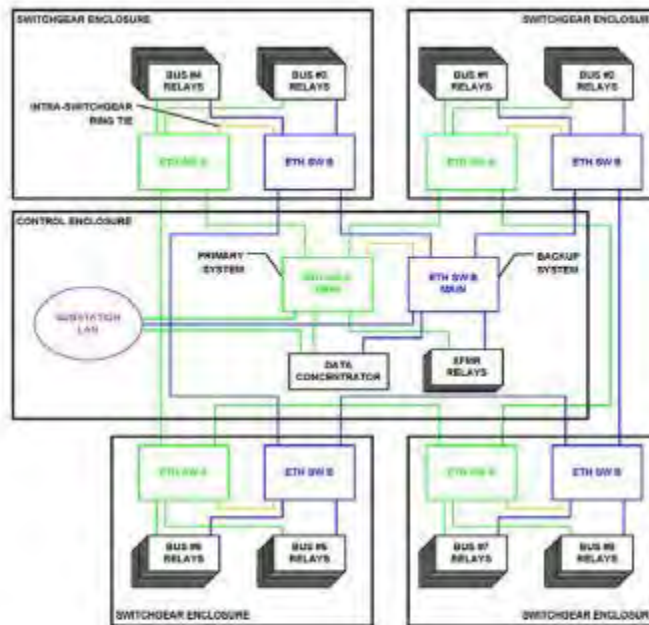


Figure 3.3. Proposed Midtown Substation Ethernet Network Configuration

The typical equipment arrangement at Midtown Substation consists of two independent distribution buses within the same switchgear enclosure. The remote switches support protection and control equipment for the two buses. It is recommended that the primary switch be installed in an auxiliary panel associated with one of the buses, while the backup switch is installed in an auxiliary panel associated with the other bus. Switch installation in different locations within the switchgear adds reliability. For example, the primary remote switch might be installed in panels related to Bus 1, while the backup switch is located in panels for Bus 2. Relays within the same switchgear enclosure should be connected to both the primary and backup remote switches located within that enclosure. This arrangement is illustrated in Figure 3.4.

3.2.2 Hardware Requirements

All Ethernet switches must have the following features in order to implement these recommendations:

- (16) 100BaseFX fiber ports for connections to protection and control equipment
- (2) 1000BaseLX fiber ports for connections between Ethernet switches

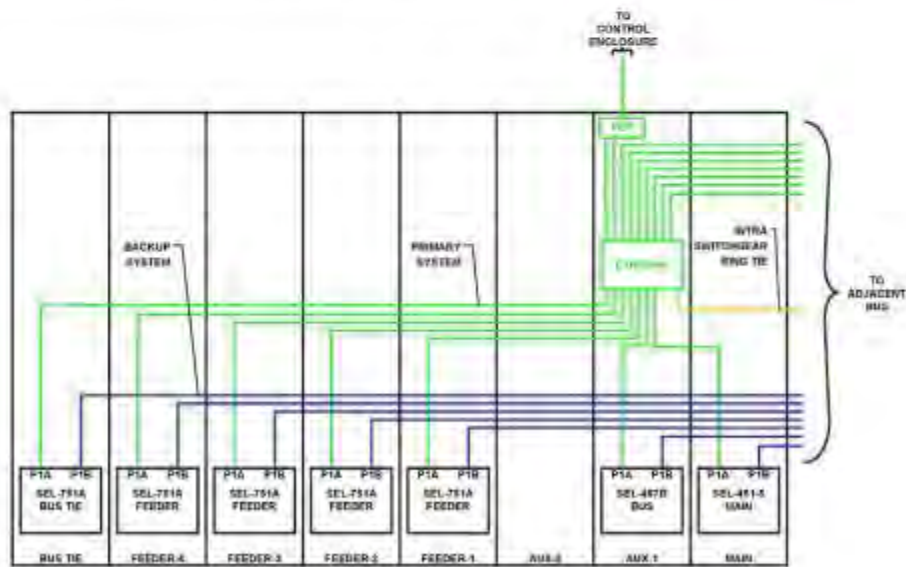


Figure 3.4. Proposed Midtown Substation Switchgear Enclosure Wiring

- (1) 100BaseT copper port for technician access

All relay equipment must have the following features in order to implement these recommendations:

- (2) 100BaseFX fiber ports for connections to the primary and backup Ethernet rings
- Fail-over capabilities for switching between Ethernet interfaces during a network fault

3.2.3 Physical Considerations

The Midtown Substation physical infrastructure is laid out in a star configuration with one cable trench for each bay in the ring bus. These trenches extend from the control enclosure, which is in the center of the substation, out to each switchgear enclosure. The recommended architecture consists of two twelve-fiber, single-mode fiber optic cables installed between each switchgear enclosure and the main control enclosure. Fiber distribution panels (FDPs) would be installed in each switch location, as well as within the control enclosure.

For the specific case at Midtown Substation, it is impractical to install new conduit directly between each switchgear enclosure to create a truly physical ring, so it is recommended that the Ethernet switches be connected in a ring by patching in the FDPs located in the control enclosure. These new fiber optic cables will be installed in the existing cable trench with other control cables. Figure 3.5 illustrates of how the fiber optic cabling should be routed and where FDPs should be installed at Midtown Substation.

3.2.4 Reliability versus Complexity

The fundamental design criteria for IEC 61850 network operations is reliable information flow. Traditionally reliability has been improved by adding redundancy to protection and control applications, especially in more critical systems such as those protecting high voltage transmission infrastructure. The benefits, cost, and complexity of each additional degree of reliability added to the design should be considered. This application of IEC 61850 is part of a pilot, and the recommended design provides KCP&L with opportunities to test a variety of configurations, some of which may not economically optimal for all deployments. The Midtown Substation is a distribution substation, which is a lower risk location to test IEC 61850 than

transmission station. However, it is recommended that the pilot network be designed for transmission-grade reliability, facilitating testing networks with varying levels of redundancy in a single location. For example, distribution-only configurations may require less redundancy, and can be easily tested at the pilot location by eliminating redundant connections as desired.

The choice of how redundant designs are for future projects will have to be considered based on the results of this pilot and needs of the future deployment. Choosing where to add redundancy in a given network design is a balance between determining where to place redundancy to eliminate likely failure points and the likelihood that this new redundancy will increase the risk of failure due to operational complexity. At Midtown substation this balance is tested in three aspects of the design.

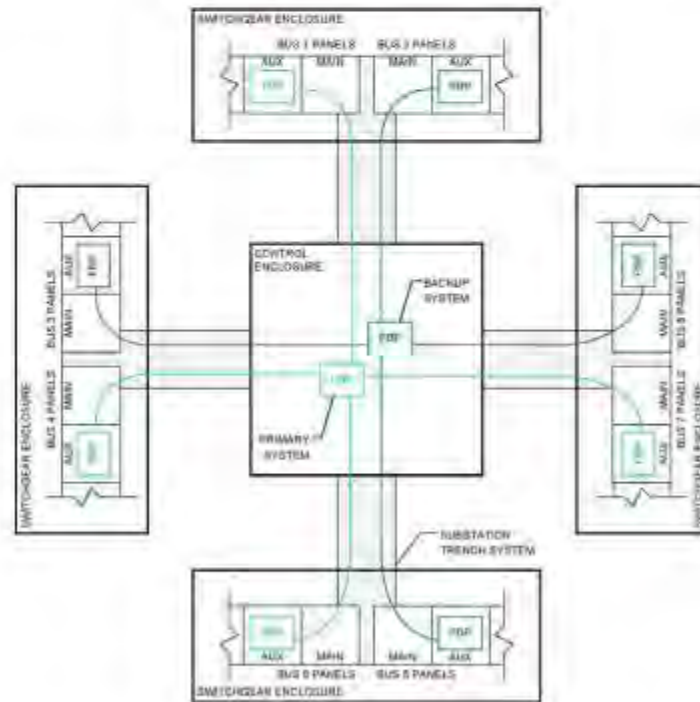


Figure 3.5. Proposed Midtown Substation Fiber Routing

First, all devices are specified to have redundancy, which is required because the time needed to repair a failed interface is outside of the acceptable operating parameters. Secondly, the recommendation to implement redundant rings is made because the cost and complexity of doing so are minimal. The devices have the spare interfaces, the fiber is available, and the time to connect and configure this is negligible if the layer two loop blocking protocol handles this added complexity transparently. If the protocol supported by the selected switch requires manual, link-specific configuration, then having two rings becomes less appealing as the complexity of the configuration increases significantly. Lastly, the choice to have redundant fiber cables between the control enclosure and switch gear adds minimal complexity to the operation of the network, but only marginally improves the reliability while increasing costs. Given that the likelihood of fiber cable failure is low and there is no diversity between the two cable routes at the pilot site since they must reside in the same cable trench, implementation of this configuration is less desirable at Midtown Substation, but may be applicable elsewhere.

3.3 ENVIRONMENTAL AND PHYSICAL HARDWARE REQUIREMENTS

Substation environments place atypical requirements on communications equipment. The equipment may be installed in locations that have no form of climate control. Available power sources and mounting locations often differ from those normally encountered in more traditional telecommunications applications. Also, the equipment is exposed to EMI and electrical surges not typically encountered except in high voltage environments. These issues should be addressed when procuring the networking equipment deployed as part of the IEC 61850 substation control network.

3.3.1 Environmental Operating Requirements

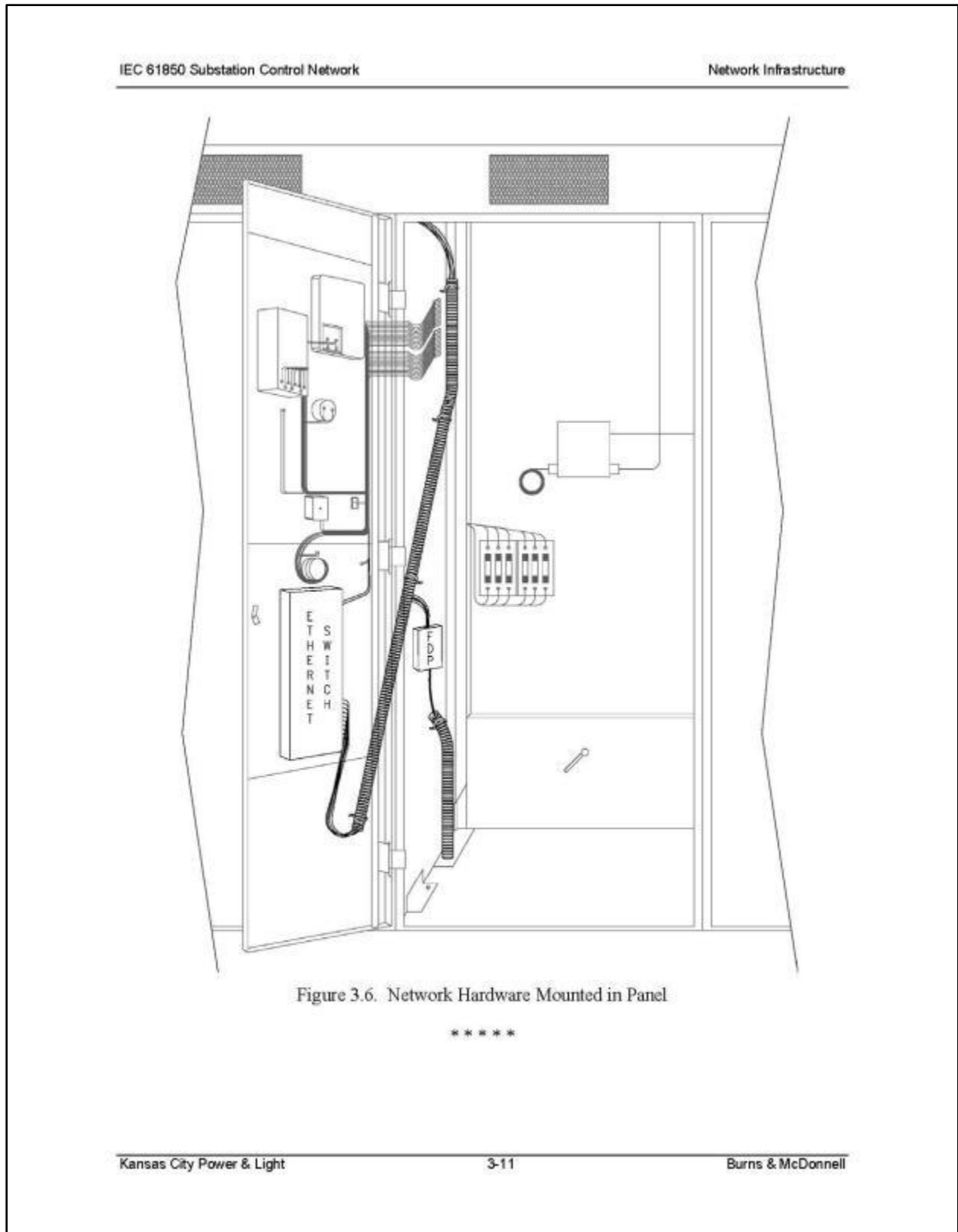
All hardware comprising the IEC 61850 substation control network should be designed for operation in harsh environments. The equipment should meet the IEEE 1613 and IEC 61850-3 requirements for operational humidity and temperature ranges. (5 % to 95 % (non-condensing); -40°C to $+85^{\circ}\text{C}$, respectively.) This is especially important at Midtown Substation, where some of the switchgear enclosures where the Ethernet switches and relays will be installed are not climate controlled. Further, the equipment should be convectively cooled, employing no moving parts or fans.

Networking hardware installed in electrical transmission facilities should also meet a number of electrical requirements. This hardware should have undergone type testing for surge withstand capability, immunity to radiated electromagnetic fields, and immunity to electrostatic discharge, all according to the IEEE C37.90 series of standards.

3.3.2 Substation Integration Requirements

Substation battery systems commonly operate at 125 VDC rather than the -48 VDC normally used for telecommunications equipment, and provide a floating power system without a reference to ground. It is therefore recommended that the network equipment deployed in the IEC 61850 network be capable of operating at floating voltages from 90 VDC to 155 VDC for compatibility with the substation facility. The selected equipment should also have provisions for redundant power supplies, should future applications require additional levels of reliability.

Equipment mounting requirements can also pose challenges in substations, especially when mounting equipment inside of switchgear. Equipment in substations is normally mounted in panels rather than racks, and is wired from the rear. This is atypical of most networking hardware, which requires rack mounting and front panel wiring. Nevertheless, network devices that support panel mounting and wiring from the rear are available for substation applications. Ethernet ports and associated port indication lighting, as well as screw terminal power connections should be provided on the rear of the selected networking hardware. The selected hardware should also have port and system indication lighting on the front of the device as well, so that device status can be easily observed without accessing the wiring side of the control panel. Often, as is the case at Midtown Substation, space behind the panel face is limited, and thus the depth of the switch, including fiber connections, cable management trays, and other such hardware should not exceed 18" if being flush mounted in a panel. Because of this depth limitation, the switch should be mounted on the inside face of the door as shown in Figure 3.6, which illustrates a potential arrangement for mounting the network hardware and wiring in a panel.



4.0 NETWORK PERFORMANCE

Protection and control algorithms are designed to isolate faults in the electrical system as quickly as possible. When using a communication-enabled protection scheme, it is critical that the control information be reliably delivered across a network with minimum delay. Failure of timely communication on the network may lead to safety concerns, significant loss of revenue, equipment damage, and system instability.

4.1 LATENCY AND JITTER REQUIREMENTS

Network latency is the maximum time required for a message to traverse the network. Implementation of GOOSE messaging requires that the network to be able to consistently forward messages with latency of no more than 4 milliseconds, with inter-frame jitter less than 500 microseconds. To ensure these latency and jitter criteria are met, the network equipment should support quality of service (QoS), virtual local area networks (VLANs), and traffic limiting functionality.

4.1.1 Quality of Service

The network infrastructure should be configured to support QoS as defined by the IEEE 802.1p standard. QoS uses the class of service bits within an IEEE 802.1q VLAN header to prioritize traffic forwarded across the network. GOOSE messages should be configured to use class of service (CoS) value of "6", making it the highest priority traffic on the network besides network configuration traffic. The classification for GOOSE should be based on Ethernet frame type 0x88b8 used to designate the GOOSE protocol. To ensure the QoS policy is implemented consistently across the network, when a packet ingresses the network at a access port it should be checked for proper QoS classification and re-marked appropriately. All other IEC 61850 traffic should be re-marked with a CoS value of "5" or lower. Further, the switches should be configured to use the strict priority queuing algorithm to ensure the lowest jitter and latency for GOOSE messages. Because this is a dedicated network where link congestion is not anticipated, a QoS policing policy is not recommended.

4.1.2 Application of VLANs

The use of virtual LANs adds limited benefit, because the single-purposed network being recommended is intended to support only protection and control applications. Nevertheless, configuring all ports to mark traffic for a specific VLAN ensures that all protection and control traffic on the network is transported in a VLAN dedicated to this purpose, and any traffic on other VLANs should be investigated. If other protection and control applications are added in the future, other VLANs might be put into service to support them.

All unused ports should be administratively shutdown and added to a VLAN ID dedicated to inactive ports. This ensures that unintentional or unwanted device connections to unused ports do not function. These measures improve network security, and make the network less susceptible to disturbances which may introduce latency.

4.1.3 Broadcast Storm Control and Port Rate Limiting

Limiting data transported across the network from individual devices is a way to prevent inadvertent or malicious network congestion, which in turn reduces jitter and latency. Broadcast storm control and port rate limiting are features that should be supported by the Ethernet switches for implementing this concept.

Broadcast storm control should be enabled and configured on all interfaces, limiting broadcast traffic on an interface to no more than 20% of all traffic. This feature should be tested on all switch hardware to ensure that GOOSE multicast traffic is not counted against this total. If it is, then this parameter should be raised to 60%.

Port rate limiting should be enabled on all 100 Mbps interfaces. Rate limits on each device port should be set to 10% of the hardware speed, or 10 Mbps. This provides sufficient bandwidth to support relay communications. This restricts network flow from a port to a fraction of the total bandwidth available, ensuring that malfunctioning or maliciously programmed devices cannot deny service to other network ports by "flooding" the network with traffic.

4.2 NETWORK FAULT RECOVERY

The required level of network availability can be made possible by using ringed or meshed network topologies, high-speed layer two loop blocking algorithms, and unidirectional link failure detection to enable rapid fault recovery. However, the features implemented for this purpose should be capable of fault recovery in an acceptable time frame. Selection and configuration of these features should account for the time delays associated with the network failure detection mechanisms of the networked equipment and the recovery time of the layer two loop blocking algorithm employed.

4.2.1 Network Fault Recovery in Ethernet Switches

Physical network rings, as recommended here, provide redundancy resulting in higher network availability. However, the Ethernet protocol cannot function properly when the logical network consists of rings. Layer two loop blocking algorithms prevent the occurrence of logical rings by blocking certain ports when connected in a physical ring. Each time a link is added or removed from the network, the layer two loop blocking algorithm will determine which links should be removed from the ring to prevent a loop in the network. This is accomplished by blocking frame forwarding on one end of the disabled link. If a fault occurs on an active link, the algorithm activates the blocked ports, restoring connectivity.

Standard layer two loop blocking algorithms like Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (rSTP) allow a network to reconfigure itself and recover after an equipment or link failure. Traditional STP recovery times can be up to 30 seconds, and rSTP can take up to two seconds, both failing to meet the recovery times required for protection and control applications. However, a number of manufacturers of environmentally-hardened switches have developed proprietary loop blocking algorithms based on STP, which are capable of loop fault recovery in under 50 milliseconds.

The proprietary nature of these layer two loop blocking protocols needs to be a key point of consideration in equipment selection for IEC 61850 networks. These protocols are vendor specific, so the entire network must be built from hardware that supports that proprietary protocol. This often requires the entire IEC 61850 network to be built from one manufacturer's

equipment, and possibly from only one series of devices. For example, different switches and router products from the same manufacture may not support the same protocol. Further, the level of complexity required to implement these protocols varies among switch manufacturers, as does the amount of quality documentation available. For example, some protocols require link specific parameters to be configured, while others simply require the protocol to be enabled on the chassis. Therefore, the complexity of implementing and maintain the system should factor in to the hardware selection process.

4.2.2 Network Fault Recovery in Connected Equipment

Each of the SEL relays being used on this project has two Ethernet interfaces, and supports two modes of operation. The first mode is a method in which adjacent relays are connected together forming a chain of relays. The relays do not support layer two loop blocking protocols, making this feature incompatible with Ethernet switch rings. This method is primarily intended for applications in stations without Ethernet switches.

In the second mode of operation, only one of the Ethernet interfaces is active at a time, and the redundant interface is in standby mode. When the relay detects a failure of the active interface, it activates the standby interface. The relay then operates on this standby interface until it detects a failure or the relay is restarted. This second mode of failure detection has maximum recovery times of 104 milliseconds in SEL 7XX series relays and 4 milliseconds in the SEL4XX series relays.

The network should support link aggregation groups to facilitate redundant Ethernet connections between the switch core and other redundantly connected devices such as the SICAM data concentrator, human machine interface, and the uplink to the firewall for connection to other networks. Multi-chassis link aggregation is the best method for providing redundant network connections to end devices supporting simultaneous operation of both links. This feature increases available bandwidth, while decreasing failure recovery times without the use of a layer 2 loop blocking protocol.

4.2.3 Unidirectional Link Failure Detection

An additional consideration arises when using fiber optic connections between the switches. A network fault can occur in which one of the fibers comprising a link becomes inoperable, creating a unidirectional communication link. These links can be difficult for failure detection algorithms to identify because only one of the communicating devices will detect the failure.

Unidirectional link failure detection features should be enabled in the Ethernet hardware to detect this type of fault and expedite recovery. Here, the device that detects the failure turns off its transmitter, letting the other device know there is a problem. These devices can then use the aforementioned loop blocking protection algorithms to detect and circumvent the fault. Without this feature enabled, it can take significantly more time for the network to detect the fault, raising recovery times from 50 milliseconds to 500 milliseconds or more.

4.3 NETWORK MANAGEMENT

Operations, maintenance, and network engineering all serve roles in system operation, so they each need network information reported into the information management systems that they use to operate the network. The network hardware selected for this application should support the network management protocols and features used by these groups.

The Relay and System Protection Department is focused on the operation of the protection and control system as a whole. This IEC 61850 network is a part of that system, and thus should be compatible with the substation monitoring systems that they use. The human machine interface used by the System Protection Department may not support the Simple Network Management Protocol (SNMP) which is often used by Network Services to manage network equipment. Thus the network equipment selected for the IEC 61850 substation network should support commonly used SCADA protocols including MODBUS and DNP. These protocols should support the display of device status, link status, and layer two loop blocking protocol status information.

The Network Services Department will have a shared responsibility for reliable network operation, and will likely prefer to manage the network using Secure Shell (SSH) and SNMP. The SNMP implementation on the IEC 61850 network should be capable of reporting resource

IEC 61850 Substation Control Network

Network Performance

statistics such as memory, processor, and link utilization. Other conditions such as temperature, power supply failures, interface state changes, and login failures should also be reported.

The network should use the network time protocol (NTP) for time coordination between network devices to facilitate event correlation across the network.

Due to the static nature of protective relay devices, the use of dynamic network protocols including IP address assignment and host name lookup are not required. All devices on the network shall have statically assigned IP addresses used to address all nodes on the network, eliminating the need for a DHCP or DNS server.

* * * * *

5.0 SECURITY

5.1 ZONES OF SECURITY

To provide security to the protection and control network, multiple zones of security should be defined within the network. Boundaries should be created where the threat severity and operational requirements among contained devices are similar. Four zones are readily defined in and around the substation as follows.

- A field area network zone around the substation generally along the substation's distribution feeder network where distribution automation and metering equipment is located
- A wide area network zone encompassing equipment connecting the substation to other stations and the control center
- A substation local area network comprised of all locally-connected, non-protection-related devices
- A protection and control local area network connecting all protection and control devices

Security devices such as firewalls are recommended between each zone of security to limit communication between zones to authorize messages. Using isolated zones minimizes access points to the protection and control equipment, acting to mitigate the lack of security functions supported by the relays. (Note: many relays still do not support centralized authentication, logging, or port authentication.) Isolating the protection and control network also minimizes concerns about possible breaches of security by using virtual networks or software-based resource reservations of memory, link capacity, or processor usage.

5.2 REGULATORY COMPLIANCE

KCP&L does not currently consider the Midtown Substation to be a critical asset. Therefore, the recommended network has not been designed for complete compliance with the Critical Infrastructure Protection (CIP) Section 5, Version 3 regulations set forth by the North American Electric Corporation (NERC). However, where implementation of a feature that enables compliance with a specific requirement did not increase cost or complexity of the design, that feature was recommended. If protection and control devices with Ethernet interfaces and associated with the Midtown distribution facilities are declared critical cyber assets, metal clad

switchgear housing these devices will have to be physically secured regardless of where network switches are installed. The implementation of the MACsec protocol (IEEE 802.1AE) for link security between network switches would facilitate NERC CIP compliance, but was not recommended because of the lack of support on most currently available networking equipment.

5.3 OTHER SECURITY CONSIDERATIONS

The following protocols and practices are recommended to secure the network equipment. The network equipment should:

- Support and be configured to use an authenticating, authorizing, and accounting server to verify all user login requests using the RADIUS or TACACS+ protocols.
- Support and be configured to report all system events and alarms to a centralized log server using the Syslog protocol to facilitate system maintenance and system intrusion detection.
- Support port spanning and remote port spanning to copy all network traffic on all interfaces to a common span port where an intrusion detection probe could be connected.
- Be configured so all unused physical and logical ports are disabled.

If there is a choice of using a secure, encrypted protocol for a given purpose, it should be utilized and the unsecured variant should be disabled. This would include using SSH instead of Telnet, HTTPS instead of HTTP, SNMPv3 instead of SNMPv2c, and DNSSEC instead of DNP.

While the Midtown Substation is not a NERC Critical Asset, using the requirements of the regulation as a guideline when they do not add cost or complexity makes good business sense. The use of centralized authentication and logging services, which are assumed to be used in the organization today is one such case where following the standard is recommended. However, the cost and complexity considerations change if these services become considered critical themselves because the sites they support are declared as NERC critical assets. Other utilities have created independent authentication and logging services for power delivery applications to address this concern, as they were already doing to support their critical asset facilities.

* * * * *

6.0 RECOMMENDATIONS

6.1 SUMMARY OF ANALYSIS

The physical layout of the Midtown Substation, the networking components of the protective relaying equipment being deployed, and the desired functionality of the network have all been considered and investigated. The resulting information was analyzed in comparison with key industry standards and recommended best practices in order to determine the most appropriate design and operating criteria for the IEC 61850 control network. The resulting findings are detailed in this report, and the accompanying Specification provides detailed recommendations for network topology, hardware selection criteria, minimum network performance criteria, and key network operating procedures.

6.2 KEY RECOMMENDATIONS

- The network should be constructed using highly-ruggedized hardware that complies with relevant IEC and IEEE standards for equipment installed in electric power transmission facilities.
- Establish redundant Ethernet rings with networking devices distributed throughout the station switchgear for increased reliability.
- The network hardware should support security features that facilitate compliance with the Critical Infrastructure Protection (CIP) regulations set forth by the North American Electric Reliability Corporation (NERC).
- Network documentation should be maintained in the same location and manner as other protection and control documentation, and maintenance of the IEC 61850 control network equipment should be performed by technical personnel trained to work with and around protection and control equipment.

* * * * *

APPENDIX A – SPECIFICATION

A.0 SPECIFICATION

This Specification sets forth recommendations and standards for establishing an Ethernet-based local area network capable of facilitating communications for the IEC 61850 substation control network. Recommended physical characteristics of the networking hardware and network topology are provided, and the environmental and network performance criteria for the networking hardware are defined. Recommendations for monitoring, securing, and operating the network are also presented.

A.1 STANDARDS COMPLIANCE

The IEC 61850 substation control network and its components shall comply with the latest revisions, supplements, and amendments of the following:

- IEC 61850-3 – Communication Networks and Systems in Substations Part 3: General Requirements
- IEEE C37.90 – IEEE Standard for Relays and Relay Systems Associated with Electric Power Apparatus
- IEEE C37.90.1 – IEEE Standard for Surge Withstand Capability Tests for Relays and Relay Systems Associated with Electric Power Apparatus
- IEEE C37.90.2 – IEEE Standard for Withstand Capability of Relay Systems to Radiated Electromagnetic Interference from Transceivers
- IEEE C37.90.3 – IEEE Standard Electrostatic Discharge Tests for Protect. Relays
- IEEE 802.1AX – Link Aggregation
- IEEE 802.1p – Priority Queuing
- IEEE 802.1Q – VLAN Tagging
- IEEE 1613 – IEEE Standard Environmental and Testing Requirements for Communications Networking Devices Installed in Electric Power Substations

A.2 INFRASTRUCTURE

A.2.1 Recommended Configuration

The recommended IEC 61850 substation control network configuration consists of redundant (primary and backup) 1Gbps Ethernet backbones. These redundant Ethernet backbones shall be established using single-mode fiber deployed throughout the substation via the existing duct bank and trench systems in physical star, logical ring configurations. These fiber rings will

interconnect remote primary and backup switches installed in various switchgear enclosures and primary and backup main switches located within the main control enclosure. Protective relays, equipped with redundant Ethernet ports, will connect to the appropriate primary and redundant remote Ethernet switches using 100 Mbps Ethernet via multimode fiber.

A.2.2 Environmental and Physical Hardware Requirements

Networking hardware deployed as part of the IEC 61850 substation control network shall meet the following environmental and physical requirements in order to be easily and reliably integrated into a substation facility.

All hardware shall:

- Have an operational temperature range of -40°C to $+85^{\circ}\text{C}$, as defined by IEEE 1613
- Operate across an ambient humidity range of 5 % to 95 % (non-condensing)
- Have passed type testing for surge withstand capability in accordance with IEEE C37.90.1
- Have passed type testing for immunity to radiated, single-frequency electromagnetic fields in accordance with IEEE C37.90.2
- Have passed type testing for electrostatic discharge immunity in accordance with IEEE C37.90.3
- Be cooled by means which employ no moving parts or fans
- Be capable of rack or panel mounting, when panel mounted it shall be cable of maintaining the arc flash rating of the panel and be no more than 18" deep including fiber management
- Operate at 90 VDC to 155 VDC
- Have screw terminal power connections
- Have power connections on the rear
- Be capable of supporting redundant power supplies

Ethernet switches shall:

- Have jacks and port indication lighting for network connections on the rear
- Have port and system indication lights on the front
- Have provisions for simultaneously supporting a minimum of one (1) 100BaseT copper connection, (16) 100BaseFX fiber connections, and two (2) 1000BaseLX fiber connections

IEC 61850 Substation Control Network

Specification

- Have provisions for copying configuration and firmware files to a locally attached flash memory at specified time intervals

Relay equipment shall:

- Have provisions for supporting two (2) 100BaseFX fiber Ethernet connections

A.3 PERFORMANCE

The IEC 61850 substation control network shall meet or exceed the following network performance criteria.

- Communication links between all Ethernet switches shall be 1000BaseLX
- Communication links between IEDs and switches shall be 100BaseFX
- Maximum network latency shall not exceed 4 ms under normal operation
- Maximum network jitter shall not exceed 500 μ s
- Network shall be designed so no device sees more than two 158 ms outages per year
- GOOSE messages shall be prioritized at Class of Service priority level 6
- The maximum layer 2 loop blocking fault recovery time of the network shall be 50 ms

The networking hardware components comprising the IEC 61850 substation control network shall provide a means of:

- Implementing quality of service features (QOS, IEEE 802.1p)
- Implementing virtual local area network tagging (VLANs, IEEE 802.1Q)
- Implementing link aggregation groups (LAG, IEEE 802.1AX)
- Detecting unidirectional link failure
- Implement broadcast storm control by allowing broadcast traffic to be limited to a percent of total network traffic
- Port-based rate limiting
- Implementing high-performance (less than 50 ms convergence), layer two loop blocking algorithms
- Use static IP address assignments, and IP address in place of host names
- Implementing network management and monitoring capabilities including Simple Network Management Protocol (SNMP)

Kansas City Power & Light

A-3

Burns & McDonnell

- Supporting management information bases that describe processor, memory, and link utilization as well as layer two port forwarding state for monitoring any layer two blocking algorithms
- Centrally reporting network device log events to a centralized server using the Syslog protocol
- Implement the NTP time protocol for coordinating log file time stamps
- Implement the MODBUS or DNP3.0 standard for monitoring device and alarm status using common SCADA protocols
- Authenticating, authorizing, and accounting for all user login requests using RADIUS or TACACS+ protocols
- Disabling of all physical ports and network managed protocols
- Implementing port spanning to facilitate the installation of intrusion detection system probes

A.4 OPERATIONS

Recommended procedures for documentation and operation of the IEC 61850 substation control network follow.

- This network shall be used solely for protection and controls applications
- Network equipment shall be located within switchgear housings which are electrically hazardous. Access to these areas is restricted to qualified personnel; therefore all work will be performed by relay technicians.
- Network configuration changes shall be verified in a testing lab prior to field deployment
- Network settings changes and firmware updates shall be carried out on site while locally connected to the network. Changes shall be coordinated with the Electrical System Operator in order to obtain scheduled outages
- Network device settings shall be recorded by updating settings documents filed with associated relay settings and other substation documentation
- Changes to physical wiring shall be recorded by updating associated drawings
- Devices shall copy their configuration and firmware to a locally attached flash on a daily basis or when the configuration is saved to support simplified device replacement in the field
- Spare network hardware shall be stored and maintained following the processes currently in place for relaying equipment

* * * *

Appendix E IEC 61850 Substation Ethernet Switch Test Results



Kansas City Power & Light 61850 Substation Ethernet Switch Configuration and Test Results

Version 1.2
March 14, 2012

Prepared by Burns & McDonnell

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

Table of Contents

- 1. Background.....1
- 2. LAN Topology.....1
- 3. Switch Configuration Parameters.....4
 - 3.1. VLAN configuration.....4
 - 3.2. QoS configuration.....6
 - 3.3. IP configuration.....9
 - 3.4. Layer 2 loop-reduction protocol configuration.....10
- 4. Network Testing.....15
 - 4.1. Port failure testing.....15
 - 4.2. Layer 2 loop reduction protocol test setup.....18
 - 4.3. Cisco failover testing.....18
 - 4.4. RuggedCom failover testing.....23
 - 4.5. Combined ring failover testing.....24
- 5. Summary.....27

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

Table of Figures

Figure 1 - Cisco Ring 2
Figure 2 - RuggedCom Ring 2
Figure 3 - Combined Rings 3
Figure 4 - Cisco REP Topology 10
Figure 5 - Cisco REP/RSTP reference design from Cisco REP whitepaper 11
Figure 6 - Relay interface failover setup 16
Figure 7 - Typical inter-switch link failure scenario 18
Figure 8 - Cisco REP typical link failure setup 19
Figure 9 - Cisco REP+RSTP link failure setup 21
Figure 10 - Cisco RSTP link failure test setup 22
Figure 11- RuggedCom link failure test setup 23
Figure 12 - Combined ring test setup 25

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

1. Background

Ethernet switch testing was conducted to verify the configuration and performance of a multi-vendor, IEC 61850 LAN. Cisco CGS 2520 and RuggedCom 2100 Ethernet switches were selected by KCP&L for the Midtown Substation 61850 LAN trial.

The primary purpose of the inter-vendor testing was to determine the performance of using the proprietary Layer 2 loop-reduction protocols offered by each vendor. In addition to the industry-standard IEEE 802.1w, Rapid Spanning Tree Protocol (RSTP), each vendor offers a proprietary algorithm with faster than RSTP performance.

Cisco offers Resilient Ethernet Protocol (REP), which is designed to interoperate with RSTP. As specified in the Cisco Resilient Ethernet Protocol whitepaper, published by Cisco, "REP is designed to provide network and application convergence within 50 ms. In some scenarios, the network convergence times may increase to within 250 ms."

RuggedCom offers Enhanced Rapid Spanning Tree Protocol (eRSTP), which is designed as an extension of RSTP and offers backwards compatibility with RSTP. In a ring topology, RuggedCom estimates the worst case fault recovery time at 5 ms per switch in the ring. In KCP&L's ring of five switches, the worst case recovery time is estimated at 25 ms or less. RuggedCom advises that the 5 ms per switch estimate is very conservative.

2. LAN Topology

The topology KCP&L selected for the Midtown Substation 61850 LAN trial was tested in three parts, the Cisco ring, the RuggedCom ring, and the combined rings. These are shown here for reference later in this document.

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

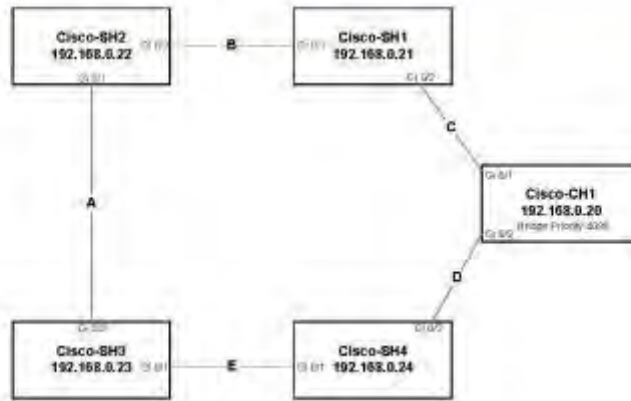


Figure 1 - Cisco Ring

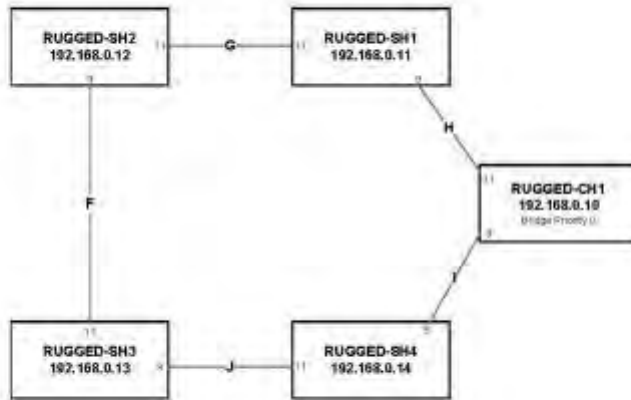


Figure 2 - RuggedCom Ring

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

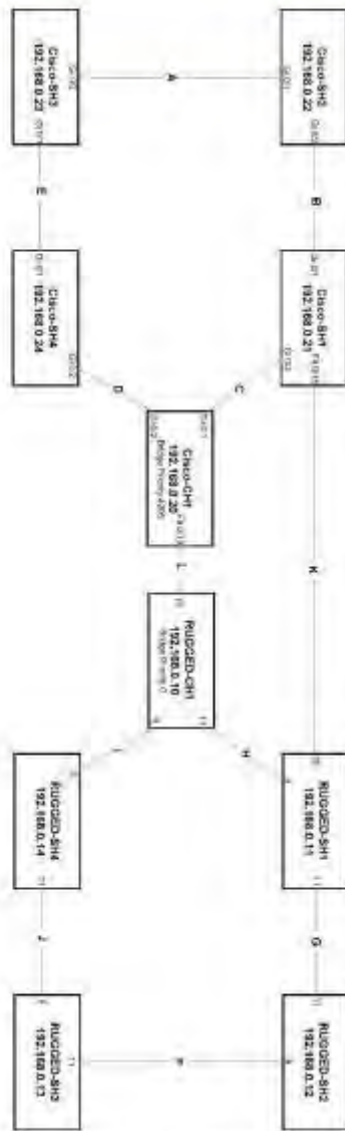


Figure 3 - Combined Rings

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

3. Switch Configuration Parameters

3.1. VLAN configuration

VLANs are configured on the KCP&L 61850 network to segregate the network and allow inter-vendor VLAN operation. SEL relays have a limitation when it comes to VLAN tagging their own packets. The SEL devices transmit and receive VLAN-tagged GOOSE messages, but are limited to untagged messages for MMS and IP remote access. Switch manufacturers handle mixed tagged/untagged traffic in different ways since a typical device will either VLAN-tag all packets or send all traffic untagged.

The Cisco and RuggedCom switches treat mixed untagged and tagged packets going into a trunk port in different ways. In addition to VLAN tags, GOOSE messages in the KCP&L 61850 substation also use the 802.1p Priority Code Point (PCP), also known as Class of Service (COS), tags to give GOOSE messages a different priority or Quality of Service (QoS) than other traffic on the LAN.

3.1.1. Cisco native VLAN implementation

By default, Cisco switches place untagged packets going into a trunk port onto VLAN 1 because VLAN 1 is considered the default VLAN. Changing the native VLAN of these ports is just changing the default VLAN for untagged traffic on the ingress of a trunk port. If a trunk port with a native VLAN receives a VLAN-tagged packet that matches the native VLAN number the switch will remove the VLAN tag from the packet on egress from another port with the same native VLAN. The desired behavior is to retain the VLAN tag from relay to relay in order to retain the VLAN tag on a GOOSE message, the VLAN number on a GOOSE message must be different than the native VLAN set on relay ports. This was the driver behind creating two VLANs for traffic leaving a relay port.

On an edge port (non-trunk port) the native VLAN would not be used since there would be no tagged traffic entering or leaving the port. Instead of using the native VLAN, the port would be set using the "switchport access" command to set the port VLAN.

3.1.2. RuggedCom PVID implementation

RuggedCom does not remove the VLAN tag from a GOOSE message even if it is the same as the Port VLAN ID (PVID) VLAN number. RuggedCom uses the term PVID to describe functionality similar to the Cisco native VLAN. The PVID is also used to set the VLAN for an untagged, edge port as well. The ports are configured as untagged trunk ports, meaning the ports will accept tagged and untagged traffic, as well as having the PVID set to put the untagged packets from the SEL relays on a specified VLAN.

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

3.1.3. VLAN assignments for the network

VLANs are numbered and designated for a specific type of traffic as follows for the Midtown Substation 61850 LAN trial on all switches:

VLAN ID	Traffic/Purpose
1	Unused
10	61850 GOOSE messages
20	All non-61850 GOOSE SEL relay traffic
75	Ethernet switch management

3.1.4. Cisco relay port VLAN configuration

Note that configurations for the Cisco switches will be shown as they appear in the configuration files, but RuggedCom configurations are shown as tables as the switches are configured using an ASCII menu instead of a command line interface (CLI).

The following is a typical relay port VLAN configuration on the Cisco CGS 2520:

```
interface FastEthernet0/1
  port-type nni
  switchport trunk native vlan 20
  switchport mode trunk
```

The relay ports are configured as trunk ports to allow VLAN tagged packets with a native VLAN of 20 to tag untagged packets on port ingress. The default port type setting on each port is network node interface (NNI) which is not changed as there is no technical reason to set the port as enhanced network interface (ENI) or user-network interface (UNI).

3.1.5. RuggedCom relay port VLAN configuration

On the RuggedCom switches, the relay ports are configured with the following parameters:

Parameter	Value
Type	Trunk
PVID	20
PVID Format	Untagged

The PVID is set to 20 for untagged traffic, and configured as a trunk for all tagged traffic. PVID format is set to untagged, meaning the PVID is applied to untagged traffic upon ingress into the port.

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

3.1.6. Cisco inter-switch port VLAN configuration

For any port facing another Ethernet switch, the following is a typical configuration for VLAN parameters:

```
interface GigabitEthernet0/1
  port-type nni
  switchport mode trunk
```

Ports are left in the default configuration of NNI, and configured as trunk ports. No native VLAN is configured since all traffic is tagged by the transmitting device or will be tagged at ingress to the LAN.

3.1.7. RuggedCom inter-switch port VLAN configuration

Parameter	Value
Type	Trunk
PVID	1
PVID Format	Tagged

Similar to the Cisco configuration, the PVID is not changed from the default value of "1" since all traffic sent between Ethernet switches will be tagged. The PVID format is set to "Tagged" as there should be no untagged traffic sent between switches.

3.2. QoS configuration

QoS classification in the Midtown Substation 61850 LAN trial is based on the layer 2, 802.1p class of service (COS) bits in the 802.1q VLAN tag. COS values are applied by the relays to each GOOSE message as it is transmitted. A COS value of "4" is being used for all GOOSE messages and COS value "4" is mapped to a high priority queue in the Ethernet switches to give GOOSE messages higher priority on the 61850 LAN than other relay traffic.

3.2.1. Cisco QoS setup procedure

The process for configuring QoS per the Cisco CGS 2520 documentation is as follows:

- a. Define a traffic class. Use the class-map [match-all | match-any] class-map-name global configuration command to define a traffic class and to enter class-map configuration mode. A traffic class contains three elements: a name, an instruction on how to evaluate the configured match commands (if more than one match command is configured in the class map), and a series of match commands.
- b. Create a traffic policy to associate the traffic class with one or more QoS features. You use the policy-map policy-map-name global configuration command to create a traffic policy and to enter policy-map configuration mode. A traffic policy defines

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

the QoS features to associate with the specified traffic class. A traffic policy contains three elements: a name, a traffic class (specified with the class policy-map configuration command), and the QoS policies configured in the class.

- c. Attach the traffic policy to an interface. You use the service-policy interface configuration command to attach the policy map to an interface for packets entering or leaving the interface. You must specify whether the traffic policy characteristics should be applied to incoming or outgoing packets. For example, entering the service-policy output class1 interface configuration command attaches all the characteristics of the traffic policy named class1 to the specified interface. All packets leaving the specified interface are evaluated according to the criteria specified in the traffic policy named class1.

Policy maps are either input policy maps or output policy maps, attached to packets as they enter or leave the switch by service policies applied to interfaces. Input policy maps perform policing and marking on received traffic. Policed packets can be dropped or reduced in priority (marked down) if they exceed the maximum permitted rates. Output policy maps perform scheduling and queuing on traffic as it leaves the switch.

Input policies and output policies have the same basic structure; the difference is in the characteristics that they regulate. Input policy map classification criteria include matching a CoS, a DSCP, or an IP precedence value or matching an access control list (ACL) or VLAN ID (for per-port, per-VLAN QoS). Output policy map classification criteria include matching a CoS, a DSCP, an IP precedence, or a QoS group value.

Classification distinguishes one kind of traffic from another by examining the fields in the packet header. When a packet is received, the switch examines the header and identifies all key packet fields. A packet can be classified based on an ACL, on the DSCP, the CoS, or the IP precedence value in the packet, or by the VLAN ID. Figure 36-3 has examples of classification information carried in a Layer 2 or a Layer 3 IP packet header, using six bits from the deprecated IP type of service (ToS) field to carry the classification information.

As explained previously, you use an MQC class map to name a specific traffic flow (or class) and to isolate it from all other traffic. A class map defines the criteria used to match against a specific traffic flow to further classify it. If you have more than one type of traffic that you want to classify, you can create another class map and use a different name. When you enter the class-map command with a class-map name, the switch enters the class-map configuration mode. In this mode, you define the match criterion for the traffic by using the match class-map configuration command. After a packet is matched against the class-map criteria, it is acted on by the associated action specified in a policy map.

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

You can match more than one criterion for classification. You can also create a class map that requires that all matching criteria in the class map be in the packet header by using the class map match-all class-map name global configuration command to enter class map configuration mode.

To configure the type of content used to classify packets, you use the match class-map configuration command to specify the classification criteria. If a packet matches the configured criteria, it belongs to a specific class and is forwarded according to the specified policy. For example, you can use the match class-map command with CoS, IP DSCP, and IP precedence values. These values are referred to as markings on a packet. You can also match an access group, a QoS group, or a VLAN ID or ID range for per-port, per-VLAN QoS.

3.2.2. Cisco QoS configuration

Using the Cisco process for implementing QoS, the following was configured on all Cisco Ethernet switches:

```
class-map match-any GOOSE
  match cos 4

policy-map output1
  class GOOSE
    priority

policy-map input1
  class GOOSE
    set cos 4

interface FastEthernet0/1
  service-policy input input1

interface GigabitEthernet0/1
  service-policy output1 output1
```

The class-map is applied to check for COS value of "4" and the map is named "GOOSE." The output policy-map is named "output1" and gives anything classified by the "GOOSE" class-map priority forwarding. Priority queuing can be applied to a single class of traffic to apply a strict queuing scheme to that class of traffic. The input policy-map is named "input1" and is applied to the "GOOSE" class-map to set the COS value to "4." This input policy is required because the Cisco CGS 2520 removes the COS tag at port ingress and a policy must be put in place to write the value back onto each GOOSE message. There is no setting to honor the COS value that was set by a relay and forward the packet with the value. It must be removed and rewritten on network ingress.

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

Device ports configured with the input policy applied to re-tag the packets on ingress. Inter-switch ports are configured with the output policy to ensure that traffic being forwarded between switches is done with GOOSE set as priority traffic.

3.2.3. RuggedCom QoS configuration

QoS on the RuggedCom Ethernet switches is applied with the following configuration:

Parameter	Value
CoS Weighting	8:4:2:1
Port Default Priority	0
Inspect TOS	Yes
COS Value 0 Priority	Normal
COS Value 4 Priority	Critical
Ingress Limit	1000 kbps
Ingress Type	Broadcast

Traffic queuing is configured with a fair policy of 8:4:2:1, which is the ratio applied to queuing packets from each of the four queues in the RuggedCom switches. The high and medium queues are currently not in use, which leaves the GOOSE (critical) to non-GOOSE (normal) traffic ratio at 8:1. Individual ports are set with a default priority of "0" meaning that all traffic is normal by default, but the ports are also set to inspect the TOS (COS) value and apply it if it is present. This allows the switch to honor the COS bits set by the relays on GOOSE messages.

COS value of "0" is mapped to the normal queue and the COS value of "4" is mapped to the critical queue. Additionally, the port ingress limiter is set to 1000 kbps of broadcast traffic to limit any device transmitting more than 1000 kbps of broadcast traffic at any given time to limit how much of the network bandwidth a broadcast storm can affect at any time.

3.3. IP configuration

Switch management IP addresses are configured in the 192.168.0.0/24 address space. There were no IP addresses assigned by KCP&L and the 192.168.0.0/24 space was known to be available. The management addresses were assigned as place-holder addresses until permanent addresses could be assigned.

3.3.1. Cisco management IP configuration

IP addressing on the Cisco switches is applied to the VLAN 75 interface as follows where "X" is set to a unique value for each Ethernet switch:

```
interface Vlan75
 ip address 192.168.0.X 255.255.255.0
```

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

3.3.2. RuggedCom management IP configuration

IP addressing on the RuggedCom switches is applied to VLAN 75 as follows:

Parameter	Value
Type	VLAN
VLAN ID	75
Address Type	Static
Address	192.168.0.X
Subnet	255.255.255.0

3.4. Layer 2 loop-reduction protocol configuration

Given that Ethernet does not allow active loops to exist in the network, a layer 2 loop-reduction protocol must be used to allow redundant links to be connected without causing broadcast loops in the network. As discussed in section 0, Cisco allows the use of REP and RSTP, and RuggedCom allows the use of eRSTP and RSTP.

Both REP and RSTP were evaluated on the Cisco ring since both protocols cannot be run on the same links at the same time and there were issues with REP and RSTP interoperability. In the RuggedCom configuration, eRSTP is backward compatible with RSTP, so there was no need to test the protocols separately.

3.4.1. Cisco REP configuration

REP was configured for testing using the following topology in the Cisco ring:



Figure 4 - Cisco REP Topology

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

This topology, with the RSTP link, allows the addition of the RuggedCom ring that is not REP compatible. The REP/RSTP configuration was designed using the Cisco Resilient Ethernet Protocol whitepaper, similar to the design shown in Figure 5.

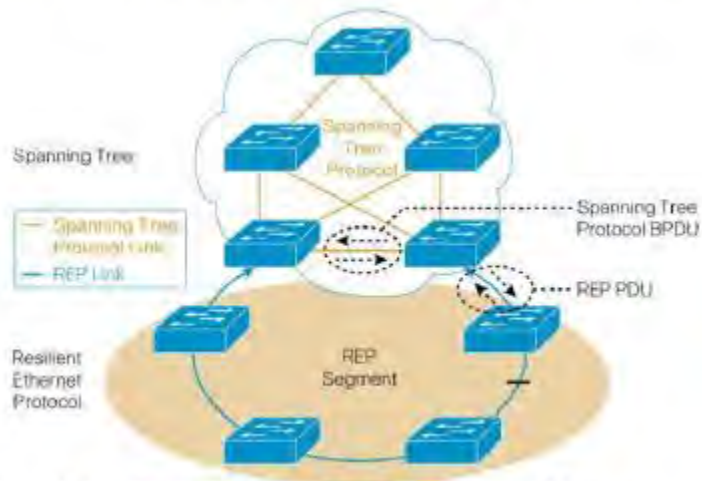


Figure 5 - Cisco REP/RSTP reference design from Cisco REP whitepaper

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

The following commands were run on the Cisco Ethernet switches to configure REP:

Cisco-CH1:

```
rep admin vlan 75
spanning-tree mode rapid-pvst

interface GigabitEthernet0/1

interface GigabitEthernet0/2
port-type nni
switchport mode trunk
rep segment 1 edge
rep ston stp
```

Cisco-SH1:

```
rep admin vlan 75
spanning-tree mode rapid-pvst

interface GigabitEthernet0/1
port-type nni
switchport mode trunk
rep segment 1 edge
rep ston stp

interface GigabitEthernet0/2
```

Cisco-SH2:

```
rep admin vlan 75
spanning-tree mode rapid-pvst

interface GigabitEthernet0/1
port-type nni
switchport mode trunk
rep segment 1

interface GigabitEthernet0/2
port-type nni
switchport mode trunk
rep segment 1
```

Cisco-SH3:

```
rep admin vlan 75
spanning-tree mode rapid-pvst
```

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

```
interface GigabitEthernet0/1
  port-type nni
  switchport mode trunk
  rep segment 1

interface GigabitEthernet0/2
  port-type nni
  switchport mode trunk
  rep segment 1
```

Cisco-SH4:

```
rep admin vlan 75
spanning-tree mode rapid-pvst

interface GigabitEthernet0/1
  port-type nni
  switchport mode trunk
  rep segment 1

interface GigabitEthernet0/2
  port-type nni
  switchport mode trunk
  rep segment 1
```

This configuration will enable RSTP on link "C" by default since REP is not enabled on that link. All other links are part of REP segment 1 with REP edge ports set on Cisco-SH1 port Gi 0/2 and Cisco-CH1 port Gi 0/1.

3.4.2. Cisco RSTP configuration

Testing on the Cisco Ethernet switches using only RSTP was also conducted due to difficulties with REP/RSTP interoperability that are discussed in in the test results. The Cisco RSTP configuration is as follows on all inter-switch links. All REP configuration was removed from all ports prior to enable RSTP and Cisco-CH1 was configured with a priority of 4096 which, in the combined topology, would make it the secondary root switch, or the primary root switch in the Cisco ring.

Cisco-CH1:

```
spanning-tree mode rapid-pvst
spanning-tree vlan 1-4094 priority 4096
```

Cisco-SH1:

```
spanning-tree mode rapid-pvst
```

Cisco-SH2:

```
spanning-tree mode rapid-pvst
```

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

Cisco-SH3:

```
spanning-tree mode rapid-pvst
```

Cisco-SH4:

```
spanning-tree mode rapid-pvst
```

Ports facing non-switch devices:

```
spanning-tree portfast trunk
```

The ports are set to portfast to prevent blocking on the port when the spanning-tree protocol sends a Topology Change Notification (TCN) to prevent unnecessary downtime on the port during convergence. This also provides a safety mechanism in the instance that another Ethernet switch is connected to a device port, RSTP is still enabled on the port to prevent switching loops.

3.4.3. RuggedCom eRSTP configuration

Default values for the inter-switch links were used, and the eRSTP configuration was left running with default values with the exception of the bridge priority of Rugged-CH1. It was changed to "0" designating it as the primary root bridge in the RuggedCom ring and combined rings. Some of the RSTP timers needed to be lowered to achieve faster convergence in the combined rings.

eRSTP Parameters:

Parameter	Value
Max Network Diameter	4*MaxAgeTime
BPDU Guard Timeout	Don't Shutdown
Fast Root Failover	On
IEEE802.1w Interoperability	On
Cost Style	32 bit

eRSTP parameters were left set as default values. The parameter of note is that 802.1w interoperability was left enabled for RSTP interoperability with the Cisco devices.

Bridge RSTP Parameters:

Parameter	Value
Version Support	RSTP
Bridge Priority (excluding CH1)	32768
Hello Time	1 s
Max Age Time	6 s

Bridge RSTP parameters were tuned for lower failover times, specifically Hello and Max Age were lowered to the lowest possible values.

Port RSTP Parameters (Typical):

Parameter	Value
-----------	-------

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

Enabled	Enabled
STP Cost	1 s
RSTP Cost	6 s
Edge Port	Auto

On each relay port, RSTP is enabled and each relay port is configured to detect if it is an edge port. If no RSTP bridge protocol data units (BPDUs) are received on a port, it is set to an edge port and will not go into a blocking state when a TCN is sent out on the network, which is the same as the Cisco portfast setting. This is set to automatic to provide a safety mechanism in the event that another Ethernet switch were connected to a relay port, RSTP would still be active on the port to prevent any loops in the network.

4. Network Testing

There were two types of tests run on the network to determine network convergence following two types of failures that can occur on an Ethernet LAN: Port failures and link failures.

4.1. Port failure testing

4.1.1. Port failure test setup

To test port failure in a practical situation, an SEL-451 relay was connected to the network with redundant interfaces. Since GOOSE is a layer 2 multicast message, there are no issues with aging packets out of the MAC table. This means that no special protocols or timers are needed to make sure GOOSE messages are transmitted or received once a relay interface switches to a redundant switch.

There is an issue with IP communications following a port switchover. Relays must provide a gratuitous ARP upon interface switchover to advertise to the network that the interface MAC has moved to a new switch. This topic is beyond the scope of this testing as it is not dependent on the Ethernet LAN but on the relay itself. This information is being included here for completeness.

The relay is the same during all tests; the internal relay interface failover is a constant during the tests. The failover was performed by disconnecting the 100BaseT copper interface from one of the switches, causing a failover to the 100BaseFX fiber interface of the relay. This measures the difference between the vendors in detecting the connection on the 100BaseFX interface and bringing up the link. Additionally, this prevented a situation where a fiber is being disconnected from a port with light from the fiber still being seen by the switch and/or relay during disconnect and keeping the interface active after the intended disconnect time.

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

To measure the outage duration, GOOSE messages were generated from the relay at an interval of approximately 0.01 seconds between messages giving a 10 ms resolution for the test results. A packet capture was set up on another network port, configured as a device port to capture packets as they would be seen by another relay on the network. This recreates a scenario similar to an event where a port fails while a relay is attempting to send a trip message.

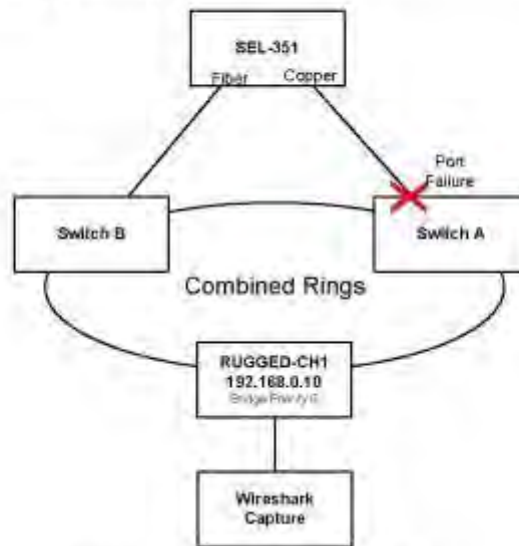


Figure 6 - Relay interface failover setup

4.1.2. Port failure test results – Failing RuggedCom to Cisco

With the copper interface of the relay active and connected to the RuggedCom switch, the copper cable was disconnected to fail the relay over to the fiber interface.

Test	Outage Duration
Trial #1	150 ms
Trial #2	130 ms
Trial #3	170 ms
Trial #4	140 ms
Trial #5	140 ms

Test Summary	Outage Duration
Min	130 ms
Max	170 ms

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

Average	150 ms
---------	--------

4.1.1. Port failure test results – Failing Cisco to RuggedCom

With the copper interface of the relay active and connected to the RuggedCom switch, the copper cable was disconnected to fail the relay over to the fiber interface.

Test	Outage Duration
Trial #1	290 ms
Trial #2	250 ms
Trial #3	250 ms
Trial #4	280 ms
Trial #5	270 ms

Test Summary	Outage Duration
Min	250 ms
Max	290 ms
Average	270 ms

Given the difference in times between the Cisco and RuggedCom failover times, a test was conducted with the relay only connected to RuggedCom switches. The results were nearly identical with the inter-vendor failover testing.

Test	Outage Duration
Trial #1	260 ms
Trial #2	280 ms

4.1.1. Port failure test results – Summary

During the tests, the average time required to fail an interface to a Cisco switch was 150 ms, and the average time required to fail an interface to a RuggedCom switch was 270 ms.

The test records were shown for inter-vendor failures since the current network design uses both vendors, and no device is planned to have two interfaces connected to a single vendor's Ethernet switch. Additional tests were run to confirm the difference in results on the RuggedCom switches to be the result of the time it takes to establish the optical connection between the RuggedCom switch and the SEL-451 and not an issue between the vendors.

A note for final implementation: The ports on the Cisco CGS switches used in the lab may require attenuators or different optics when connected to SEL relays within the substation. The optical transmit power on the 100BaseFX optics in the Cisco CGS are

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

10 km range optics and were too bright for the optical receiver in the SEL relay used for lab testing. This may not be the case depending on relays and conditions in the substation, but it was an issue during lab testing that required the use of an air gap to act as an optical attenuator.

4.2. Layer 2 loop reduction protocol test setup

Testing REP, eRSTP and RSTP was done using a packet generator sending GOOSE packets at 1000 packets/second. This packet rate was chosen to give 1 ms resolution to the results. The packets were received by a packet capture at the furthest logical point in the network from the source. This means that the generator and capture were placed on opposite sides of the blocking port for REP or eRSTP, forcing the packets on the longest path through the network. A link on the active traffic path was failed and the outage time for GOOSE messages was measured. The outage time was recorded as the difference in time between the reception of the first GOOSE message after repair and the last message received before the break.

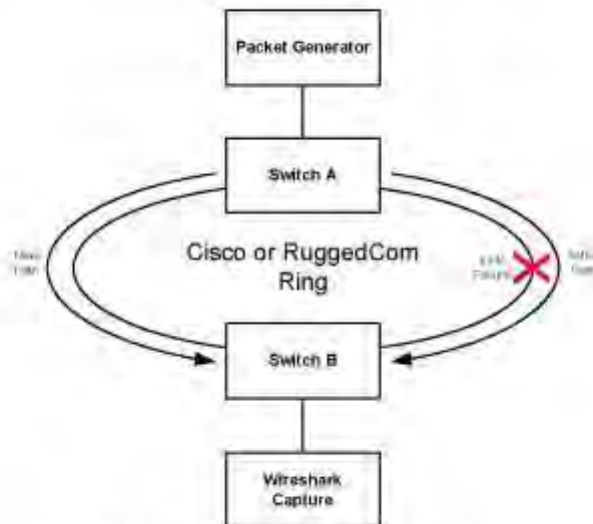


Figure 7 - Typical inter-switch link failure scenario

4.3. Cisco failover testing

4.3.1. Cisco REP link failure test setup

An example of the REP topology is provided below for reference with a sample failure scenario.

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

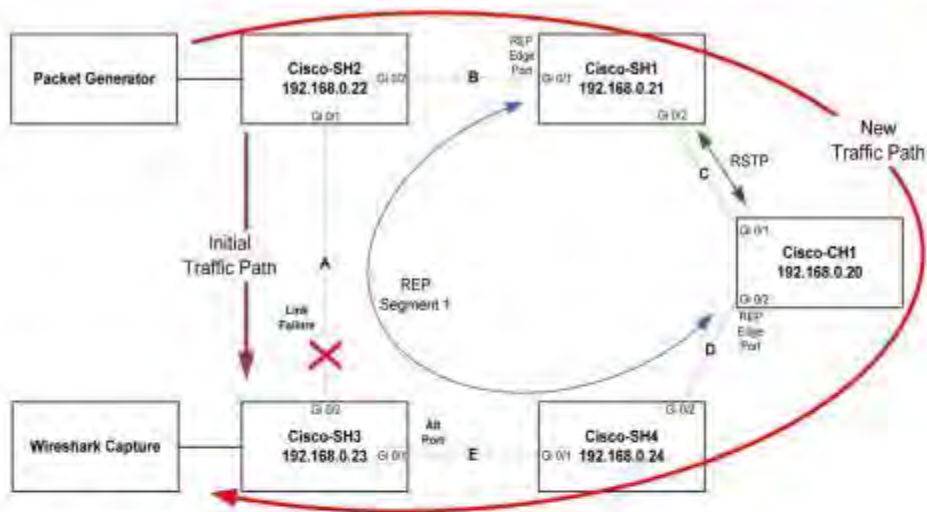


Figure 8 - Cisco REP typical link failure setup

To test network convergence times for the REP protocol, links were failed according to the location of the Alternate Port. Traffic was generated across the shortest path between the traffic generation and capture with the Alt (blocking) port on an adjacent link (this is shown as link E in Figure 8). A port on the shortest path (in Figure 8, this would be a port on link “A”) was disconnected forcing the traffic to travel the longest path to reach the capture. This was done to simulate the worst case failure on this topology.

4.3.2. Cisco REP link failure test results

The table below details the test results from the Cisco REP link failure tests. The table gives the test results according to test number, outage duration, which link was broken, and which port was blocking the loop prior to the link failure.

Test	Outage Duration	Link Broken	Alt Port – Before Break
Trial #1	36 ms	B	SH2 - Gi 0/1
Trial #2	43 ms	A	SH3 - Gi 0/1
Trial #3	113 ms	A	SH3 - Gi 0/1
Trial #4	96 ms	A	SH3 - Gi 0/1
Trial #5	7 ms	E	SH3 - Gi 0/2
Trial #6	119 ms	E	SH3 - Gi 0/2
Trial #7	99 ms	E	SH3 - Gi 0/2

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

Trial #8	39 ms	A	SH2 - Gi 0/2
Trial #9	76 ms	A	SH2 - Gi 0/2
Trial #10	141 ms	A	SH2 - Gi 0/2

Table 1 - Cisco REP test results

Test Summary	Outage Duration
Min	7 ms
Max	141 ms
Average	77 ms

Table 2 - Cisco REP test summary

The REP convergence time varied greatly between tests depending on which link was broken. The first two tests showed sub 50 ms convergence times in accordance with the Cisco whitepaper. Unless configured specifically to avoid this behavior, the REP Alt port will move onto the last link that was failed. If all links are active, a network running RSTP will always converge with the same blocking port due to how costs are calculated in the network.

The third test exposed an odd behavior with REP so additional tests were conducted to establish a pattern. If a link is failed the Alt port moves to the failed link when it is reconnected. If the Alt port is moved back to the original link by failing a different port, and the original failure is repeated, the convergence time goes up to values at or over 100 ms. The highest measured value was 141 ms.

To clarify how this was repeated, assume that the network state is that shown in Figure 8, and link "A" is failed and the outage is measured. A port on link "A" will now become the Alt port. To repeat the same test, link "E" is failed which will move the Alt port back to link "E" as shown in the diagram, and now link "A" can be failed again and measured. The second failure of "A" is where REP did not meet the sub 50 ms convergence time.

4.3.3. Cisco REP+RSTP link failure test results

The next test conducted tested the ability to fail the RSTP link "C" in the Cisco ring. STCN notifications were set on both REP edge ports, but failing the RSTP link isolates switches on either side of the Alt port. It is expected that a REP TCN notification would be sent into the REP segment to unblock the Alt port, but this is not the case. The Alt port remained after the failure.

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

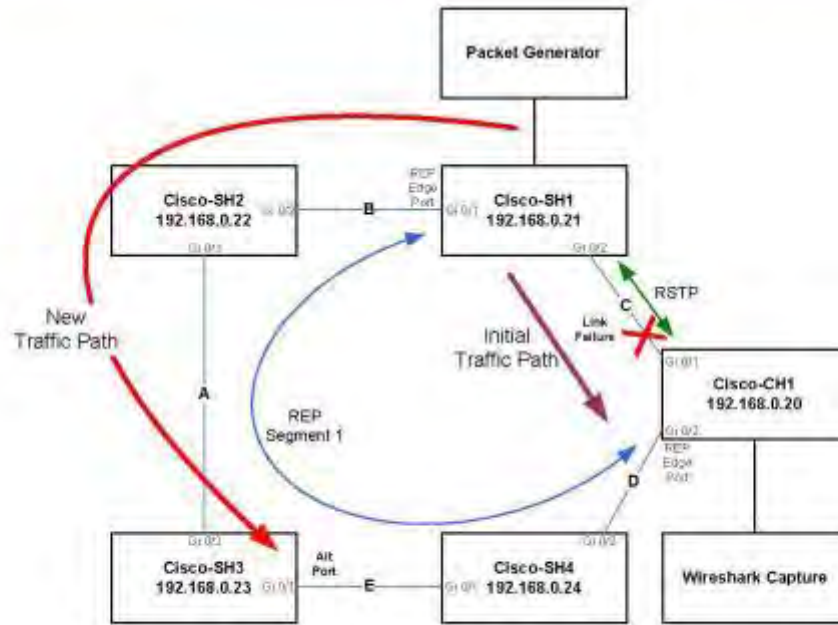


Figure 9 - Cisco REP+RSTP link failure setup

Test	Outage Duration	Switchback Time
Trial #1	N/A	N/A
Trial #2	N/A	N/A

4.3.4. Cisco RSTP link failure test results

Given the issue with REP and RSTP, the Cisco ring was reset to use only RSTP in the configuration show in Figure 10.

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

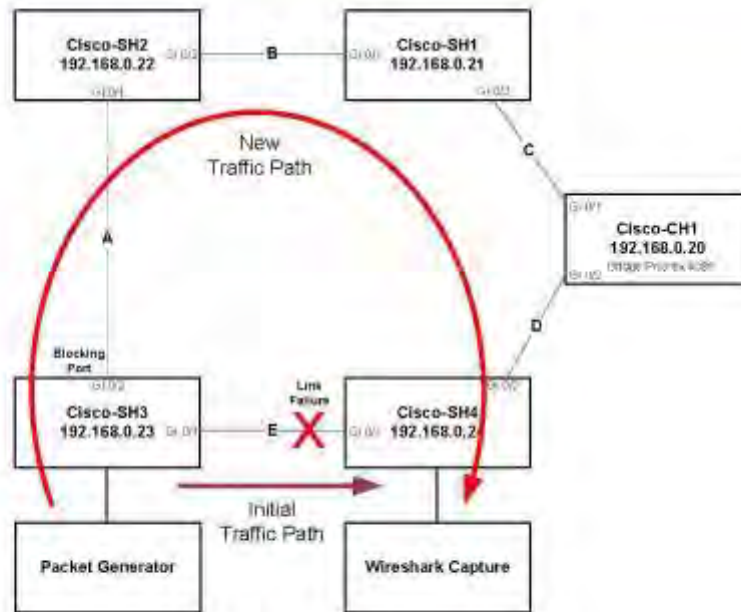


Figure 10 - Cisco RSTP link failure test setup

Test	Outage Duration	Switchback Time
Trial #1	94 ms	Not Recorded
Trial #2	143 ms	24 ms
Trial #3	164 ms	24 ms
Trial #4	123 ms	33 ms
Trial #5	154 ms	32 ms

Table 3 - Cisco RSTP test results

Test Summary	Outage Duration	Switchback Time
Min	94 ms	24 ms
Max	154 ms	33 ms
Average	136 ms	27 ms

Table 4 - Cisco RSTP test summary

Cisco RSTP convergence times were more consistent than the REP convergence times and the repair times only varied by 7 ms from the minimum to maximum measured values.

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

4.4. RuggedCom failover testing

4.4.1. RuggedCom eRSTP link failure test results

The RuggedCom ring and traffic generators were setup similar to the Cisco REP and RSTP test configuration, which the traffic generator and capture on an adjacent link that was failed to force the traffic on the longest path in the network as shown in Figure 11.

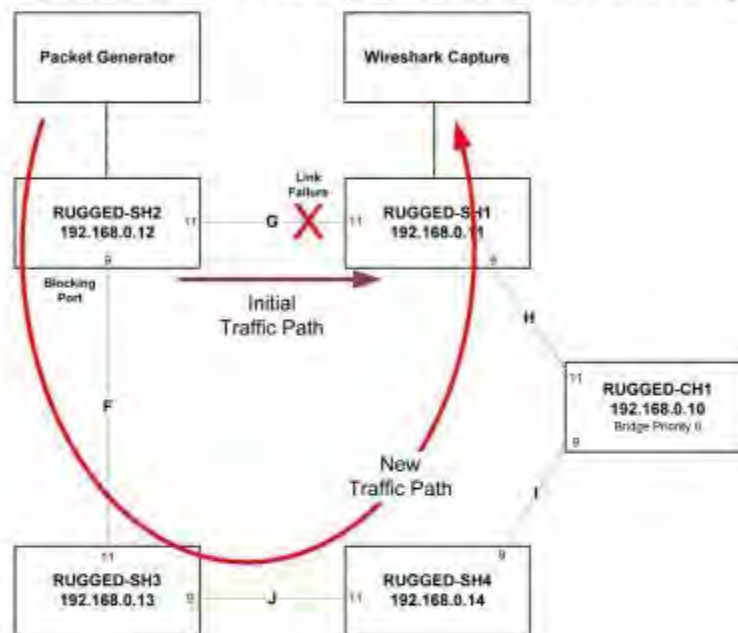


Figure 11- RuggedCom link failure test setup

Test	Outage Duration	Switchback Time
Trial #1	14 ms	Not Recorded
Trial #2	13 ms	6 ms
Trial #3	13 ms	6 ms
Trial #4	14 ms	4 ms
Trial #5	14 ms	6 ms

Table 5 - RuggedCom eRSTP test results

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

Test Summary	Outage Duration	Switchback Time
Min	13 ms	4 ms
Max	14 ms	6 ms
Average	14 ms	6 ms

Table 6 - RuggedCom eRSTP test summary

Failover times and repair times were very consistent with eRSTP. Using the method provided by RuggedCom, 25 ms would be the budgeted convergence time for the network, which was higher than the 14 ms measured convergence time.

4.5. Combined ring failover testing

On the combined ring, three tests were conducted: A failure between two Cisco switches, a failure between two RuggedCom switches, and a failure between a Cisco and RuggedCom switch. Due to the difficulties with setting up REP + RSTP in the same configuration, the Cisco switches were configured with only RSTP and the RuggedCom switches were configured with eRSTP.

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

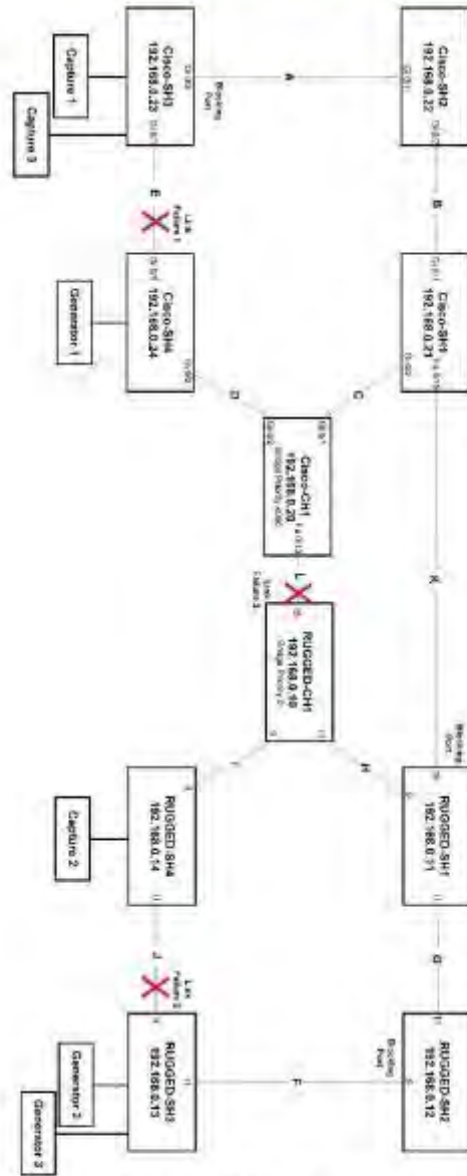


Figure 12 - Combined ring test setup

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

4.5.1. Cisco-Cisco link failure test results

Link "E" was failed in the network to test a failure in the Cisco ring as shown in Figure 12.

Test	Outage Duration	Switchback Time
Trial #1	152 ms	26 ms
Trial #2	132 ms	27 ms
Trial #3	124 ms	26 ms
Trial #4	142 ms	27 ms
Trial #5	185 ms	26 ms

Table 7 – Cisco-Cisco combined ring test results

Test Summary	Outage Duration	Switchback Time
Min	124 ms	26 ms
Max	185 ms	27 ms
Average	147 ms	26 ms

Table 8 - Cisco-Cisco combined ring test summary

These test results were consistent with the tests conducted on the Cisco ring, with the average convergence time 11 ms more than the average time from the previous tests and the average repair time within 1 ms of the previous average.

4.5.2. RuggedCom-RuggedCom link failure test results

Link "J" was failed in the network to test a failure in the Cisco ring as shown in Figure 12.

Test	Outage Duration	Switchback Time
Trial #1	30 ms	9 ms
Trial #2	29 ms	9 ms
Trial #3	30 ms	10 ms
Trial #4	30 ms	10 ms
Trial #5	30 ms	10 ms

Table 9 – RuggedCom-RuggedCom combined ring test results

Test Summary	Outage Duration	Switchback Time
Min	29 ms	9 ms
Max	30 ms	10 ms
Average	30 ms	10 ms

Table 10 - RuggedCom-RuggedCom combined ring test summary

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

These test results had an average convergence time of 16 ms more than the average time from the previous tests and the average repair time 4 ms more than the previous average. The convergence results agree with the method RuggedCom uses to estimate convergence time, which is estimated at 50 ms using the RuggedCom method which gives conservative results.

4.5.1 Cisco-RuggedCom link failure test results

Link "L" was failed in the network to test a failure between the rings as shown in Figure 12.

Test	Outage Duration	Switchback Time
Trial #1	5.802 s	7.99 s

Table 11 – Cisco-RuggedCom combined ring test results

The test between vendors proved to have some interoperability difficulties as the convergence time and repair time were over 5 seconds. This time is the result of timeout values in the RuggedCom RSTP settings. This test was conducted several times, the first of which was using the default RSTP timers on the RuggedCom switches which were set at 60 seconds, and the convergence time was around 60 seconds.

5. Summary

Throughout the testing, intra-vendor performance was mostly consistent with each of the vendors. There was a reproducible anomaly with specific failure scenarios with REP in the Cisco ring. Other convergence times in the Cisco ring were in the sub 50 ms range. Cisco RSTP convergence was very consistent with repair times, but the convergence times were never under 50 ms, and typically more than 100 ms. Additionally there was difficulty configuring REP to interoperate with RSTP in an intra-vendor setup, so there was no testing conducted in an inter-vendor configuration.

Cisco showed consistently better times when failing a single relay port by approximately 120 ms on average with an SEL-451. There were no other relays available for comparison so this could be an issue with the SEL-451 specifically.

The RuggedCom implementation of eRSTP is very consistent with convergence and repair times and was across every test that was run on the RuggedCom and combined rings. Both convergence and repair times on each test were within 1 ms of every other respective convergence and repair time for each configuration.

VLAN configuration had to be adapted, and an extra VLAN was added to accommodate the way Cisco handles tagged traffic going into a trunk port with a native VLAN.

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

Although the workaround poses no operational issues, the difference in the way each manufacturer handles both tagged and untagged packets on a trunk port caused some issues during the initial configuration.

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

6. Follow-up Testing

Another test network was setup and configured in the Burns & McDonnell lab after the initial testing at KCP&L to perform additional tests on the devices to investigate two specific issues. These issues are: 1) The greater than 50 ms recovery time when failing the Cisco-Cisco REP segments and 2) the greater than five second recovery time observed when failing the Cisco-RuggedCom links.

During a follow-up conversation with Cisco regarding the issue, Cisco confirmed that they were able to reproduce the first issue with REP failure times exceeding 50 ms. They mentioned the possibility of light from the fiber jumpers shining into the SFP optical receiver during the disconnection causing the connection to stay up but no valid data reaching the other end. They were able to achieve the desired sub 50 ms recovery times by issuing a "shutdown" command to a port to cause the link failure. It is Burns & McDonnell's that this does not simulate an actual failure in the network for two reasons: 1) An equipment failure or fiber cut is never initiated with software and 2) it is possible that the code in the router is written to send the notification that the port is down immediately before actually shutting down the port. If the second scenario is true, it would show better-than-actual failover times. It is Burns & McDonnell's opinion that feasible failure scenarios must be initiated external to the router during normal operation, i.e. power failure, link failure through disconnection, and removing interface and management cards.

To eliminate the possibility of optical receivers causing issues with the link failure times, another test was designed to remove the entire SFP module instead of just unplugging the fiber jumper. With this method of link failure, the connection being broken is no longer an optical link but instead a low voltage, electrical connection. An optical connection may not have enough attenuation to be considered failed by the equipment until it has been removed several millimeters. The electrical connection from the chassis to the SFP is broken as soon as the electrical contacts are physically separated. The Cisco-Cisco REP link failure was then tested again to determine if this was the issue or if the issue is caused by the REP protocol. The test results from the testing at KCP&L's facilities were not consistent, but there was a reliable means to reproduce recovery times over 50 ms. Similar results were achieved by pulling the SFP modules versus pulling the fiber optic jumper connections.

The second issue with the Cisco-RuggedCom connection causing greater than five second recovery times was also tested again in the Burns & McDonnell lab. This issue was not thoroughly investigated during the testing at KCP&L's facility due to time constraints. After further testing and configuration, the recovery time from a failure is not an issue, but the multi-second delay is caused when reconnecting a specific connection. There also appears to be an issue with RSTP between the vendors in general, the Cisco switches will become the root switch even when a RuggedCom has a lower STP priority. This doesn't appear to cause a forwarding loop in the network, but it is abnormal behavior for RSTP to have two root switches in the network. The link that causes the delay when reconnected is

KCP&L 61850 Substation Ethernet Switch Configuration and Test Results

the link between the Cisco root switch and the RuggedCom root switch. Changing the forwarding delay on the Cisco switches directly affects the recovery time when that link is reconnected, the recovery time is approximately twice the value of the forwarding delay. Changing the forwarding delay on the RuggedCom switches does not affect the recovery time. This value can only be set as low as four seconds per the standard, which allows an 8 second recovery time for a reconnection between the two rings.

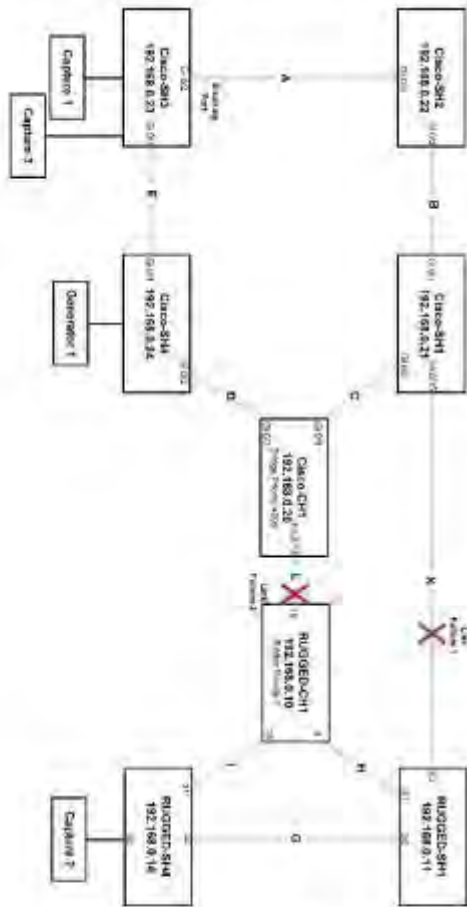


Figure 13 – Additional test setup

This page intentionally blank.

Appendix F Device Points List

F.1	Substation Devices	
	F.1.1 Bus Differential Relay	F-3
	F.1.2 Bus Main Breaker	F-4
	F.1.3 Feeder Breaker	F-5
	F.1.4 Feeder Breaker – non smart grid	F-7
	F.1.5 Load Tap Changer	F-9
	F.1.6 Tie Breaker	F-10
	F.1.7 Transformer Differential Relay	F-12
F.2	Field Devices	
	F.2.1 Battery Controller	F-13
	F.2.2 Cap Bank Controller – Standard	F-15
	F.2.3 Cap Bank Controller – VAR	F-17
	F.2.4 FCI Indicators and Receiver	F-19
	F.2.5 Recloser Controller	F-26

This page intentionally blank.

SEL-487B: Bus Differential Relay

Name	Point Type	61850 Name	ICCP Name
86B Lockout Operated	Status	ANN.IN1GGIO9.Ind01.stVal	KCPLD1:DATAVALUE~ANN\$IN1GGIO9\$Ind01\$SsVal0007510.state
Software or Hardware Alarm	Status	ANN.OUT1GGIO14.Ind06.stVal	KCPLD1:DATAVALUE~ANN\$OUT1GGIO14\$Ind06\$SsVal0007510.state

SEL 451-5: Bus Main Breaker

Name	Point Type	61850 Name	ICCP Name
Device Status	Status	PRO.BKR1CSWI1.Pos.stVal	KCPLD1:DATAVALUE~PRO\$BKR1CSW1\$Pos\$Val0007510.state
Local - Remote	Status	ANN.IN1GGIO14.Ind03.stVal	KCPLD1:DATAVALUE~ANN\$IN1GGIO14\$Ind03\$Val0007510.state
86M Lockout Operated	Status	ANN.IN2GGIO15.Ind01.stVal	KCPLD1:DATAVALUE~ANN\$IN2GGIO15\$Ind01\$Val0007510.state
Slow Breaker Indication	Status	ANN.KCPLGGIO20.Ind01.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO20\$Ind01\$Val0007510.state
Loss of Potential	Status	ANN.KCPLGGIO20.Ind02.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO20\$Ind02\$Val0007510.state
Contact Wear - 3 Phase	Status	ANN.KCPLGGIO20.Ind03.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO20\$Ind03\$Val0007510.state
Hardware Alarm	Status	ANN.KCPLGGIO20.Ind04.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO20\$Ind04\$Val0007510.state
Software Alarm	Status	ANN.KCPLGGIO20.Ind05.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO20\$Ind05\$Val0007510.state
Fault - Phase A	Status	ANN.KCPLGGIO20.Ind06.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO20\$Ind06\$Val0007510.state
Fault - Phase B	Status	ANN.KCPLGGIO20.Ind07.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO20\$Ind07\$Val0007510.state
Fault - Phase C	Status	ANN.KCPLGGIO20.Ind08.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO20\$Ind08\$Val0007510.state
Fault - Ground	Status	ANN.KCPLGGIO20.Ind09.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO20\$Ind09\$Val0007510.state
Trip Coil Monitor	Status	ANN.KCPLGGIO20.Ind12.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO20\$Ind12\$Val0007510.state

SEL-751A: Feeder Breaker

Name	Point Type	61850 Name	ICCP Name
Device Status	Status	PRO.BKR1CSWI1.Pos.stVal	KCPLD1:DATAVALUE~PRO\$BKR1CSWI1\$Pos\$Val0007514.state
Local - Remote	Status	ANN.INCGGIO13.Ind01.stVal	KCPLD1:DATAVALUE~ANN\$INCGGIO13\$Ind01\$Val0007514.state
79CO - Reclose - Enabled Status	Status	ANN.LTGGIO5.Ind08.stVal	KCPLD1:DATAVALUE~ANN\$LTGGIO5\$Ind08\$Val0007514.state
50CO - Ground - Enabled Status	Status	ANN.LTGGIO5.Ind05.stVal	KCPLD1:DATAVALUE~ANN\$LTGGIO5\$Ind05\$Val0007514.state
Close Failure	Status	ANN.LTGGIO5.Ind03.stVal	KCPLD1:DATAVALUE~ANN\$LTGGIO5\$Ind03\$Val0007514.state
Under Frequency Trip	Status	ANN.LTGGIO5.Ind02.stVal	KCPLD1:DATAVALUE~ANN\$LTGGIO5\$Ind02\$Val0007514.state
High Current Lockout	Status	ANN.LTGGIO5.Ind07.stVal	KCPLD1:DATAVALUE~ANN\$LTGGIO5\$Ind07\$Val0007514.state
Slow Breaker Indication	Status	ANN.SVTGGIO4.Ind11.stVal	KCPLD1:DATAVALUE~ANN\$SVTGGIO4\$Ind11\$Val0007514.state
Contact Wear - 3 Phase	Status	ANN.KCPLGGIO24.Ind01.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO24\$Ind01\$Val0007514.state
Feeder Lockout Operated	Status	ANN.LTGGIO5.Ind01.stVal	KCPLD1:DATAVALUE~ANN\$LTGGIO5\$Ind01\$Val0007514.state
Trip Coil Monitor	Status	ANN.SVTGGIO4.Ind08.stVal	KCPLD1:DATAVALUE~ANN\$SVTGGIO4\$Ind08\$Val0007514.state
Instantaneous	Status	ANN.TLEDGGIO6.Ind03.stVal	KCPLD1:DATAVALUE~ANN\$TLEDGGIO6\$Ind03\$Val0007514.state
Phase Overcurrent	Status	ANN.TLEDGGIO6.Ind04.stVal	KCPLD1:DATAVALUE~ANN\$TLEDGGIO6\$Ind04\$Val0007514.state
Ground Neutral Overcurrent	Status	ANN.TLEDGGIO6.Ind05.stVal	KCPLD1:DATAVALUE~ANN\$TLEDGGIO6\$Ind05\$Val0007514.state
Negative Sequence Overcurrent	Status	ANN.TLEDGGIO6.Ind06.stVal	KCPLD1:DATAVALUE~ANN\$TLEDGGIO6\$Ind06\$Val0007514.state
Over Under Frequency	Status	ANN.TLEDGGIO6.Ind07.stVal	KCPLD1:DATAVALUE~ANN\$TLEDGGIO6\$Ind07\$Val0007514.state
Breaker Failure	Status	ANN.TLEDGGIO6.Ind08.stVal	KCPLD1:DATAVALUE~ANN\$TLEDGGIO6\$Ind08\$Val0007514.state
Hardware Alarm	Status	ANN.KCPLGGIO24.Ind02.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO24\$Ind02\$Val0007514.state
Software Alarm	Status	ANN.KCPLGGIO24.Ind03.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO24\$Ind03\$Val0007514.state
Fault - Phase A	Status	ANN.KCPLGGIO24.Ind04.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO24\$Ind04\$Val0007514.state
Fault - Phase B	Status	ANN.KCPLGGIO24.Ind05.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO24\$Ind05\$Val0007514.state
Fault - Phase C	Status	ANN.KCPLGGIO24.Ind06.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO24\$Ind06\$Val0007514.state
Fault - Ground	Status	ANN.KCPLGGIO24.Ind07.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO24\$Ind07\$Val0007514.state
Loss of Potential	Status	PRO.LOPPTUV3.Str.general	KCPLD1:DATAVALUE~PRO\$LOPPTUV3\$Str\$general0007514.state
EMS - DMS Indicator	Status	ANN.LTGGIO5.Ind04.stVal	KCPLD1:DATAVALUE~ANN\$LTGGIO5\$Ind04\$Val0007514.state
Device Operate	Control	CON.RBGGIO2.SPCSO11.ctlVal/CON.RBGGIO2.SPCSO12.ctlVal	KCPLD1:DeviceOperate~CON\$DevOp\$c0007514
79CO - Reclose	Control	CON.RBGGIO2.SPCSO13.ctlVal/CON.RBGGIO2.SPCSO14.ctlVal	KCPLD1:DeviceOperate~CON\$RclsEnb\$c0007514
50CO - Ground	Control	CON.RBGGIO2.SPCSO15.ctlVal/CON.RBGGIO2.SPCSO16.ctlVal	KCPLD1:DeviceOperate~CON\$GndEnb\$c0007514
Real Power - 3 Phase	Analog	MET.METMMXU1.TotW.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$TotW\$mag0007514.value
Reactive Power - 3 Phase	Analog	MET.METMMXU1.TotVar.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$TotVar\$mag0007514.value
Apparent Power - 3 Phase	Analog	MET.METMMXU1.TotVA.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$TotVA\$mag0007514.value
Power Factor - 3 Phase	Analog	MET.METMMXU1.TotPF.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$TotPF\$mag0007514.value
Current - Phase A	Analog	MET.METMMXU1.A.phsA.cVal.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$A\$phsA\$mag0007514.value
Current - Phase B	Analog	MET.METMMXU1.A.phsB.cVal.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$A\$phsB\$mag0007514.value
Current - Phase C	Analog	MET.METMMXU1.A.phsC.cVal.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$A\$phsC\$mag0007514.value

SEL-751A: Feeder Breaker

Name	Point Type	61850 Name	ICCP Name
Voltage - Phase A	Analog	MET.METMMXU1.PhV.phsA.cVal.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$PhV\$phsA\$mag0007514.value
Voltage - Phase B	Analog	MET.METMMXU1.PhV.phsB.cVal.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$PhV\$phsB\$mag0007514.value
Voltage - Phase C	Analog	MET.METMMXU1.PhV.phsC.cVal.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$PhV\$phsC\$mag0007514.value
Current - Neutral	Analog	MET.METMMXU1.A.neut.cVal.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$A\$neut\$mag0007514.value
Real Power - Phase A	Analog	MET.METMMXU1.W.phsA.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$W\$phsA\$mag0007514.value
Real Power - Phase B	Analog	MET.METMMXU1.W.phsB.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$W\$phsB\$mag0007514.value
Real Power - Phase C	Analog	MET.METMMXU1.W.phsC.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$W\$phsC\$mag0007514.value
Reactive Power - Phase A	Analog	MET.METMMXU1.VAr.phsA.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$VAr\$phsA\$mag0007514.value
Reactive Power - Phase B	Analog	MET.METMMXU1.VAr.phsB.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$VAr\$phsB\$mag0007514.value
Reactive Power - Phase C	Analog	MET.METMMXU1.VAr.phsC.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$VAr\$phsC\$mag0007514.value
Apparent Power - Phase A	Analog	MET.METMMXU1.VA.phsA.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$VA\$phsA\$mag0007514.value
Apparent Power - Phase B	Analog	MET.METMMXU1.VA.phsB.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$VA\$phsB\$mag0007514.value
Apparent Power - Phase C	Analog	MET.METMMXU1.VA.phsC.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$VA\$phsC\$mag0007514.value
Power Factor - Phase A	Analog	MET.METMMXU1.PF.phsA.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$PF\$phsA\$mag0007514.value
Power Factor - Phase B	Analog	MET.METMMXU1.PF.phsB.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$PF\$phsB\$mag0007514.value
Power Factor - Phase C	Analog	MET.METMMXU1.PF.phsC.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$PF\$phsC\$mag0007514.value
Current - Positive Sequence	Analog	MET.METMSQI1.SeqA.c1.cVal.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$SeqA\$c1\$mag0007514.value
Current - Negative Sequence	Analog	MET.METMSQI1.SeqA.c2.cVal.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$SeqA\$c2\$mag0007514.value
Current - Zero Sequence	Analog	MET.METMSQI1.SeqA.c3.cVal.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$SeqA\$c3\$mag0007514.value
Voltage - Positive Sequence	Analog	MET.METMSQI1.SeqV.c1.cVal.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$SeqV\$c1\$mag0007514.value
Voltage - Negative Sequence	Analog	MET.METMSQI1.SeqV.c2.cVal.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$SeqV\$c2\$mag0007514.value
Voltage - Zero Sequence	Analog	MET.METMSQI1.SeqV.c3.cVal.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$SeqV\$c3\$mag0007514.value
Current Imbalance	Analog	MET.METMSQI1.MaxImbA.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$MaxImbA\$mag0007514.value
Voltage Imbalance	Analog	MET.METMSQI1.MaxImbV.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$MaxImbV\$mag0007514.value
Current - Average	Analog	MET.METMSTA1.AvAmps.mag	KCPLD1:DATAVALUE~MET\$METMSTA1\$AvAmps\$mag0007514.value
Current - Max - Phase A	Analog	MET.METMSTA1.MaxA.phsA.mag	KCPLD1:DATAVALUE~MET\$METMSTA1\$MaxA\$phA\$mag0007514.value
Current - Max - Phase B	Analog	MET.METMSTA1.MaxA.phsB.mag	KCPLD1:DATAVALUE~MET\$METMSTA1\$MaxA\$phB\$mag0007514.value
Current - Max - Phase C	Analog	MET.METMSTA1.MaxA.phsC.mag	KCPLD1:DATAVALUE~MET\$METMSTA1\$MaxA\$phC\$mag0007514.value
Current - Max - Neutral	Analog	MET.METMSTA1.MaxA.neut.mag	KCPLD1:DATAVALUE~MET\$METMSTA1\$MaxA\$neu\$mag0007514.value

SEL-751A: Feeder Breaker (Non Smart Grid Feeder)

Name	Point Type	61850 Name	ICCP Name
Device Status	Status	PRO.BKR1CSWI1.Pos.stVal	KCPLD1:DATAVALUE~PRO\$BKR1CSWI1\$Pos\$stVal0007511.state
Local - Remote	Status	ANN.INCGGIO13.Ind01.stVal	KCPLD1:DATAVALUE~ANN\$INCGGIO13\$Ind01\$stVal0007511.state
79CO - Reclose - Enabled Status	Status	ANN.LTGGIO5.Ind08.stVal	KCPLD1:DATAVALUE~ANN\$LTGGIO5\$Ind08\$stVal0007511.state
50CO - Ground - Enabled Status	Status	ANN.LTGGIO5.Ind05.stVal	KCPLD1:DATAVALUE~ANN\$LTGGIO5\$Ind05\$stVal0007511.state
Close Failure	Status	ANN.LTGGIO5.Ind03.stVal	KCPLD1:DATAVALUE~ANN\$LTGGIO5\$Ind03\$stVal0007511.state
Under Frequency Trip	Status	ANN.LTGGIO5.Ind02.stVal	KCPLD1:DATAVALUE~ANN\$LTGGIO5\$Ind02\$stVal0007511.state
High Current Lockout	Status	ANN.LTGGIO5.Ind07.stVal	KCPLD1:DATAVALUE~ANN\$LTGGIO5\$Ind07\$stVal0007511.state
Slow Breaker Indication	Status	ANN.SVTGGIO4.Ind11.stVal	KCPLD1:DATAVALUE~ANN\$SVTGGIO4\$Ind11\$stVal0007511.state
Contact Wear - 3 Phase	Status	ANN.KCPLGGIO24.Ind01.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO24\$Ind01\$stVal0007511.state
Feeder Lockout Operated	Status	ANN.LTGGIO5.Ind01.stVal	KCPLD1:DATAVALUE~ANN\$LTGGIO5\$Ind01\$stVal0007511.state
Trip Coil Monitor	Status	ANN.SVTGGIO4.Ind08.stVal	KCPLD1:DATAVALUE~ANN\$SVTGGIO4\$Ind08\$stVal0007511.state
Instantaneous	Status	ANN.TLEDGGIO6.Ind03.stVal	KCPLD1:DATAVALUE~ANN\$TLEDGGIO6\$Ind03\$stVal0007511.state
Phase Overcurrent	Status	ANN.TLEDGGIO6.Ind04.stVal	KCPLD1:DATAVALUE~ANN\$TLEDGGIO6\$Ind04\$stVal0007511.state
Ground Neutral Overcurrent	Status	ANN.TLEDGGIO6.Ind05.stVal	KCPLD1:DATAVALUE~ANN\$TLEDGGIO6\$Ind05\$stVal0007511.state
Negative Sequence Overcurrent	Status	ANN.TLEDGGIO6.Ind06.stVal	KCPLD1:DATAVALUE~ANN\$TLEDGGIO6\$Ind06\$stVal0007511.state
Over Under Frequency	Status	ANN.TLEDGGIO6.Ind07.stVal	KCPLD1:DATAVALUE~ANN\$TLEDGGIO6\$Ind07\$stVal0007511.state
Breaker Failure	Status	ANN.TLEDGGIO6.Ind08.stVal	KCPLD1:DATAVALUE~ANN\$TLEDGGIO6\$Ind08\$stVal0007511.state
Hardware Alarm	Status	ANN.KCPLGGIO24.Ind02.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO24\$Ind02\$stVal0007511.state
Software Alarm	Status	ANN.KCPLGGIO24.Ind03.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO24\$Ind03\$stVal0007511.state
Fault - Phase A	Status	ANN.KCPLGGIO24.Ind04.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO24\$Ind04\$stVal0007511.state
Fault - Phase B	Status	ANN.KCPLGGIO24.Ind05.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO24\$Ind05\$stVal0007511.state
Fault - Phase C	Status	ANN.KCPLGGIO24.Ind06.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO24\$Ind06\$stVal0007511.state
Fault - Ground	Status	ANN.KCPLGGIO24.Ind07.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO24\$Ind07\$stVal0007511.state
Loss of Potential	Status	PRO.LOPPTUV3.Str.general	KCPLD1:DATAVALUE~PRO\$LOPPTUV3\$Str\$general0007511.state
Real Power - 3 Phase	Analog	MET.METMMXU1.TotW.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$TotW\$mag0007511.value
Reactive Power - 3 Phase	Analog	MET.METMMXU1.TotVAr.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$TotVAr\$mag0007511.value
Apparent Power - 3 Phase	Analog	MET.METMMXU1.TotVA.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$TotVA\$mag0007511.value
Power Factor - 3 Phase	Analog	MET.METMMXU1.TotPF.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$TotPF\$mag0007511.value
Current - Phase A	Analog	MET.METMMXU1.A.phsA.cVal.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$A\$phsA\$mag0007511.value
Current - Phase B	Analog	MET.METMMXU1.A.phsB.cVal.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$A\$phsB\$mag0007511.value
Current - Phase C	Analog	MET.METMMXU1.A.phsC.cVal.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$A\$phsC\$mag0007511.value
Voltage - Phase A	Analog	MET.METMMXU1.PhV.phsA.cVal.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$PhV\$phsA\$mag0007511.value
Voltage - Phase B	Analog	MET.METMMXU1.PhV.phsB.cVal.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$PhV\$phsB\$mag0007511.value
Voltage - Phase C	Analog	MET.METMMXU1.PhV.phsC.cVal.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$PhV\$phsC\$mag0007511.value
Current - Neutral	Analog	MET.METMMXU1.A.neut.cVal.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$A\$neut\$mag0007511.value

SEL-751A: Feeder Breaker (Non Smart Grid Feeder)

Name	Point Type	61850 Name	ICCP Name
Real Power - Phase A	Analog	MET.METMMXU1.W.phsA.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$W\$phsA\$mag0007511.value
Real Power - Phase B	Analog	MET.METMMXU1.W.phsB.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$W\$phsB\$mag0007511.value
Real Power - Phase C	Analog	MET.METMMXU1.W.phsC.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$W\$phsC\$mag0007511.value
Reactive Power - Phase A	Analog	MET.METMMXU1.VAr.phsA.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$VAr\$phsA\$mag0007511.value
Reactive Power - Phase B	Analog	MET.METMMXU1.VAr.phsB.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$VAr\$phsB\$mag0007511.value
Reactive Power - Phase C	Analog	MET.METMMXU1.VAr.phsC.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$VAr\$phsC\$mag0007511.value
Apparent Power - Phase A	Analog	MET.METMMXU1.VA.phsA.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$VA\$phsA\$mag0007511.value
Apparent Power - Phase B	Analog	MET.METMMXU1.VA.phsB.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$VA\$phsB\$mag0007511.value
Apparent Power - Phase C	Analog	MET.METMMXU1.VA.phsC.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$VA\$phsC\$mag0007511.value
Power Factor - Phase A	Analog	MET.METMMXU1.PF.phsA.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$PF\$phsA\$mag0007511.value
Power Factor - Phase B	Analog	MET.METMMXU1.PF.phsB.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$PF\$phsB\$mag0007511.value
Power Factor - Phase C	Analog	MET.METMMXU1.PF.phsC.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$PF\$phsC\$mag0007511.value
Current - Positive Sequence	Analog	MET.METMSQI1.SeqA.c1.cVal.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$SeqA\$c1\$mag0007511.value
Current - Negative Sequence	Analog	MET.METMSQI1.SeqA.c2.cVal.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$SeqA\$c2\$mag0007511.value
Current - Zero Sequence	Analog	MET.METMSQI1.SeqA.c3.cVal.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$SeqA\$c3\$mag0007511.value
Voltage - Positive Sequence	Analog	MET.METMSQI1.SeqV.c1.cVal.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$SeqV\$c1\$mag0007511.value
Voltage - Negative Sequence	Analog	MET.METMSQI1.SeqV.c2.cVal.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$SeqV\$c2\$mag0007511.value
Voltage - Zero Sequence	Analog	MET.METMSQI1.SeqV.c3.cVal.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$SeqV\$c3\$mag0007511.value
Current Imbalance	Analog	MET.METMSQI1.MaxImbA.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$MaxImbA\$mag0007511.value
Voltage Imbalance	Analog	MET.METMSQI1.MaxImbV.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$MaxImbV\$mag0007511.value
Current - Average	Analog	MET.METMSTA1.AvAmps.mag	KCPLD1:DATAVALUE~MET\$METMSTA1\$AvAmps\$mag0007511.value
Current - Max - Phase A	Analog	MET.METMSTA1.MaxA.phsA.mag	KCPLD1:DATAVALUE~MET\$METMSTA1\$MaxA\$phA\$mag0007511.value
Current - Max - Phase B	Analog	MET.METMSTA1.MaxA.phsB.mag	KCPLD1:DATAVALUE~MET\$METMSTA1\$MaxA\$phB\$mag0007511.value
Current - Max - Phase C	Analog	MET.METMSTA1.MaxA.phsC.mag	KCPLD1:DATAVALUE~MET\$METMSTA1\$MaxA\$phC\$mag0007511.value
Current - Max - Neutral	Analog	MET.METMSTA1.MaxA.neut.mag	KCPLD1:DATAVALUE~MET\$METMSTA1\$MaxA\$neu\$mag0007511.value

Eberle REG-DA: Load Tap Changer

Name	Point Type	61850 Name	ICCP Name
Auto - Manual	Status	A/ATCC.Auto.stVal	KCPLD1:DATAVALUE~ATCC\$Auto\$stVal1847437.state
Position - Status	Status	A/ATCC.TapChg.valWTr.posVal	KCPLD1:DATAVALUE~ATCC\$Tapchg\$valWTr\$pos1847437.state
Position - Control	Control	A/ATCC.TapChg.Oper.ctlVal	KCPLD1:DeviceOperate~ATCC\$Tapchg\$Oper\$ct1847437
Auto - Manual	Control	A/ATCC.Auto.Oper.ctlVal	KCPLD1:DeviceOperate~ATCC\$Auto\$Oper\$ct1847437

SEL-751A: Tie Breaker

Name	Point Type	61850 Name	ICCP Name
Device Status	Status	PRO.BKR1CSWI1.Pos.stVal	KCPLD1:DATAVALUE~PRO\$BKR1CSWI1\$Pos\$Val0007519.state
Local - Remote	Status	ANN.INCGGIO13.Ind01.stVal	KCPLD1:DATAVALUE~ANN\$INCGGIO13\$Ind01\$Val0007519.state
Auto - Manual	Status	ANN.LTGGIO5.Ind02.stVal	KCPLD1:DATAVALUE~ANN\$LTGGIO5\$Ind02\$Val0007519.state
Slow Breaker Indication	Status	ANN.SVTGGIO4.Ind11.stVal	KCPLD1:DATAVALUE~ANN\$SVTGGIO4\$Ind11\$Val0007519.state
Contact Wear - 3 Phase	Status	ANN.KCPLGGIO24.Ind01.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO24\$Ind01\$Val0007519.state
86BT Lockout Operated	Status	ANN.INCGGIO13.Ind04.stVal	KCPLD1:DATAVALUE~ANN\$INCGGIO13\$Ind04\$Val0007519.state
Trip Coil Monitor	Status	ANN.SVTGGIO4.Ind08.stVal	KCPLD1:DATAVALUE~ANN\$SVTGGIO4\$Ind08\$Val0007519.state
Instantaneous	Status	ANN.TLEDGGIO6.Ind03.stVal	KCPLD1:DATAVALUE~ANN\$TLEDGGIO6\$Ind03\$Val0007519.state
Phase Overcurrent	Status	ANN.TLEDGGIO6.Ind04.stVal	KCPLD1:DATAVALUE~ANN\$TLEDGGIO6\$Ind04\$Val0007519.state
Ground Neutral Overcurrent	Status	ANN.TLEDGGIO6.Ind05.stVal	KCPLD1:DATAVALUE~ANN\$TLEDGGIO6\$Ind05\$Val0007519.state
Negative Sequence Overcurrent	Status	ANN.TLEDGGIO6.Ind06.stVal	KCPLD1:DATAVALUE~ANN\$TLEDGGIO6\$Ind06\$Val0007519.state
Over Under Frequency	Status	ANN.TLEDGGIO6.Ind07.stVal	KCPLD1:DATAVALUE~ANN\$TLEDGGIO6\$Ind07\$Val0007519.state
Breaker Failure	Status	ANN.TLEDGGIO6.Ind08.stVal	KCPLD1:DATAVALUE~ANN\$TLEDGGIO6\$Ind08\$Val0007519.state
Hardware Alarm	Status	ANN.KCPLGGIO24.Ind02.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO24\$Ind02\$Val0007519.state
Software Alarm	Status	ANN.KCPLGGIO24.Ind03.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO24\$Ind03\$Val0007519.state
Fault - Phase A	Status	ANN.KCPLGGIO24.Ind04.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO24\$Ind04\$Val0007519.state
Fault - Phase B	Status	ANN.KCPLGGIO24.Ind05.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO24\$Ind05\$Val0007519.state
Fault - Phase C	Status	ANN.KCPLGGIO24.Ind06.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO24\$Ind06\$Val0007519.state
Fault - Ground	Status	ANN.KCPLGGIO24.Ind07.stVal	KCPLD1:DATAVALUE~ANN\$KCPLGGIO24\$Ind07\$Val0007519.state
Loss of Potential	Status	PRO.LOPPTUV3.Str.general	KCPLD1:DATAVALUE~PRO\$LOPPTUV3\$Str\$general0007519.state
Real Power - 3 Phase	Analog	MET.METMMXU1.TotW.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$TotW\$mag0007519.value
Reactive Power - 3 Phase	Analog	MET.METMMXU1.TotVAr.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$TotVAr\$mag0007519.value
Apparent Power - 3 Phase	Analog	MET.METMMXU1.TotVA.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$TotVA\$mag0007519.value
Power Factor - 3 Phase	Analog	MET.METMMXU1.TotPF.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$TotPF\$mag0007519.value
Current - Phase A	Analog	MET.METMMXU1.A.phsA.cVal.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$A\$phsA\$mag0007519.value
Current - Phase B	Analog	MET.METMMXU1.A.phsB.cVal.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$A\$phsB\$mag0007519.value
Current - Phase C	Analog	MET.METMMXU1.A.phsC.cVal.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$A\$phsC\$mag0007519.value
Voltage - Phase A	Analog	MET.METMMXU1.PhV.phsA.cVal.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$PhV\$phsA\$mag0007519.value
Voltage - Phase B	Analog	MET.METMMXU1.PhV.phsB.cVal.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$PhV\$phsB\$mag0007519.value
Voltage - Phase C	Analog	MET.METMMXU1.PhV.phsC.cVal.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$PhV\$phsC\$mag0007519.value
Current - Neutral	Analog	MET.METMMXU1.A.neut.cVal.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$A\$neut\$mag0007519.value
Real Power - Phase A	Analog	MET.METMMXU1.W.phsA.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$W\$phsA\$mag0007519.value
Real Power - Phase B	Analog	MET.METMMXU1.W.phsB.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$W\$phsB\$mag0007519.value
Real Power - Phase C	Analog	MET.METMMXU1.W.phsC.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$W\$phsC\$mag0007519.value
Reactive Power - Phase A	Analog	MET.METMMXU1.VAr.phsA.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$VAr\$phsA\$mag0007519.value

SEL-751A: Tie Breaker

Name	Point Type	61850 Name	ICCP Name
Reactive Power - Phase B	Analog	MET.METMMXU1.VAr.phsB.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$VAr\$phsB\$mag0007519.value
Reactive Power - Phase C	Analog	MET.METMMXU1.VAr.phsC.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$VAr\$phsC\$mag0007519.value
Apparent Power - Phase A	Analog	MET.METMMXU1.VA.phsA.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$VA\$phsA\$mag0007519.value
Apparent Power - Phase B	Analog	MET.METMMXU1.VA.phsB.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$VA\$phsB\$mag0007519.value
Apparent Power - Phase C	Analog	MET.METMMXU1.VA.phsC.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$VA\$phsC\$mag0007519.value
Power Factor - Phase A	Analog	MET.METMMXU1.PF.phsA.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$PF\$phsA\$mag0007519.value
Power Factor - Phase B	Analog	MET.METMMXU1.PF.phsB.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$PF\$phsB\$mag0007519.value
Power Factor - Phase C	Analog	MET.METMMXU1.PF.phsC.mag	KCPLD1:DATAVALUE~MET\$METMMXU1\$PF\$phsC\$mag0007519.value
Current - Positive Sequence	Analog	MET.METMSQI1.SeqA.c1.cVal.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$SeqA\$c1\$mag0007519.value
Current - Negative Sequence	Analog	MET.METMSQI1.SeqA.c2.cVal.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$SeqA\$c2\$mag0007519.value
Current - Zero Sequence	Analog	MET.METMSQI1.SeqA.c3.cVal.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$SeqA\$c3\$mag0007519.value
Voltage - Positive Sequence	Analog	MET.METMSQI1.SeqV.c1.cVal.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$SeqV\$c1\$mag0007519.value
Voltage - Negative Sequence	Analog	MET.METMSQI1.SeqV.c2.cVal.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$SeqV\$c2\$mag0007519.value
Voltage - Zero Sequence	Analog	MET.METMSQI1.SeqV.c3.cVal.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$SeqV\$c3\$mag0007519.value
Current Imbalance	Analog	MET.METMSQI1.MaxImbA.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$MaxImbA\$mag0007519.value
Voltage Imbalance	Analog	MET.METMSQI1.MaxImbV.mag	KCPLD1:DATAVALUE~MET\$METMSQI1\$MaxImbV\$mag0007519.value
Current - Average	Analog	MET.METMSTA1.AvAmps.mag	KCPLD1:DATAVALUE~MET\$METMSTA1\$AvAmps\$mag0007519.value
Current - Max - Phase A	Analog	MET.METMSTA1.MaxA.phsA.mag	KCPLD1:DATAVALUE~MET\$METMSTA1\$MaxA\$phA\$mag0007519.value
Current - Max - Phase B	Analog	MET.METMSTA1.MaxA.phsB.mag	KCPLD1:DATAVALUE~MET\$METMSTA1\$MaxA\$phB\$mag0007519.value
Current - Max - Phase C	Analog	MET.METMSTA1.MaxA.phsC.mag	KCPLD1:DATAVALUE~MET\$METMSTA1\$MaxA\$phC\$mag0007519.value
Current - Max - Neutral	Analog	MET.METMSTA1.MaxA.neut.mag	KCPLD1:DATAVALUE~MET\$METMSTA1\$MaxA\$neu\$mag0007519.value

SEL-487E: Transformer Differential Relay

Name	Point Type	61850 Name	ICCP Name
Device Status	Status	PRO.S52AXCBR1.Pos.stVal	KCPLD1:DATAVALUE~PRO\$S52AXCBR1\$Pos\$stVal1856556.state
Real Power - 3 Phase - Terminal T	Analog	MET.METTMMXU2.TotW.mag.f	KCPLD1:DATAVALUE~MET\$METTMMXU2\$TotW\$mag1856556.value
Reactive Power - 3 Phase - Terminal T	Analog	MET.METTMMXU2.TotVar.mag.f	KCPLD1:DATAVALUE~MET\$METTMMXU2\$TotVar\$mag1856556.value
Apparent Power - 3 Phase - Terminal T	Analog	MET.METTMMXU2.TotVA.mag.f	KCPLD1:DATAVALUE~MET\$METTMMXU2\$TotVA\$mag1856556.value
Power Factor - 3 Phase - Terminal T	Analog	MET.METTMMXU2.TotPF.mag.f	KCPLD1:DATAVALUE~MET\$METTMMXU2\$TotPF\$mag1856556.value
Frequency - Terminal T	Analog	MET.METTMMXU2.Hz.mag.f	KCPLD1:DATAVALUE~MET\$METTMMXU2\$Hz\$mag1856556.value
Current - Phase A - Terminal T	Analog	MET.METTMMXU2.A1.phsA.cVal.mag.f	KCPLD1:DATAVALUE~MET\$METTMMXU2\$A\$phsA\$mag1856556.value
Current - Phase B - Terminal T	Analog	MET.METTMMXU2.A1.phsB.cVal.mag.f	KCPLD1:DATAVALUE~MET\$METTMMXU2\$A\$phsB\$mag1856556.value
Current - Phase C - Terminal T	Analog	MET.METTMMXU2.A1.phsC.cVal.mag.f	KCPLD1:DATAVALUE~MET\$METTMMXU2\$A\$phsC\$mag1856556.value
Real Power - 3 Phase - Terminal U	Analog	MET.METUMMXU3.TotW.mag.f	KCPLD1:DATAVALUE~MET\$METUMMXU3\$TotW\$mag1856556.value
Reactive Power - 3 Phase - Terminal U	Analog	MET.METUMMXU3.TotVar.mag.f	KCPLD1:DATAVALUE~MET\$METUMMXU3\$TotVar\$mag1856556.value
Apparent Power - 3 Phase - Terminal U	Analog	MET.METUMMXU3.TotVA.mag.f	KCPLD1:DATAVALUE~MET\$METUMMXU3\$TotVA\$mag1856556.value
Power Factor - 3 Phase - Terminal U	Analog	MET.METUMMXU3.TotPF.mag.f	KCPLD1:DATAVALUE~MET\$METUMMXU3\$TotPF\$mag1856556.value
Frequency - Terminal U	Analog	MET.METUMMXU3.Hz.mag.f	KCPLD1:DATAVALUE~MET\$METUMMXU3\$Hz\$mag1856556.value
Current - Phase A - Terminal U	Analog	MET.METUMMXU3.A1.phsA.cVal.mag.f	KCPLD1:DATAVALUE~MET\$METUMMXU3\$A\$phsA\$mag1856556.value
Current - Phase B - Terminal U	Analog	MET.METUMMXU3.A1.phsB.cVal.mag.f	KCPLD1:DATAVALUE~MET\$METUMMXU3\$A\$phsB\$mag1856556.value
Current - Phase C - Terminal U	Analog	MET.METUMMXU3.A1.phsC.cVal.mag.f	KCPLD1:DATAVALUE~MET\$METUMMXU3\$A\$phsC\$mag1856556.value
Voltage - Phase A - Terminal V	Analog	MET.METSMMXU1.PhV1.phsA.cVal.mag.f	KCPLD1:DATAVALUE~MET\$METSMMXU1\$PV1\$pA\$mag1856556.value
Voltage - Phase B - Terminal V	Analog	MET.METSMMXU1.PhV1.phsB.cVal.mag.f	KCPLD1:DATAVALUE~MET\$METSMMXU1\$PV1\$pB\$mag1856556.value
Voltage - Phase C - Terminal V	Analog	MET.METSMMXU1.PhV1.phsC.cVal.mag.f	KCPLD1:DATAVALUE~MET\$METSMMXU1\$PV1\$pC\$mag1856556.value
Voltage - Phase A - Terminal Z	Analog	MET.METSMMXU1.PhV2.phsA.cVal.mag.f	KCPLD1:DATAVALUE~MET\$METSMMXU1\$PV2\$pA\$mag1856556.value
Voltage - Phase B - Terminal Z	Analog	MET.METSMMXU1.PhV2.phsB.cVal.mag.f	KCPLD1:DATAVALUE~MET\$METSMMXU1\$PV2\$pB\$mag1856556.value
Voltage - Phase C - Terminal Z	Analog	MET.METSMMXU1.PhV2.phsC.cVal.mag.f	KCPLD1:DATAVALUE~MET\$METSMMXU1\$PV2\$pC\$mag1856556.value

SEL 3530-4: Battery Controller

Name	Point Type	DNP Point	ICCP Name
BESS Status	DI	0	KCPLD1:DATAVALUE~ANN\$BESSSts\$1111111.state
Schedule Override Status	DI	1	KCPLD1:DATAVALUE~ANN\$SchdlOvrds\$1111111.state
Alarm - Warning	DI	2	KCPLD1:DATAVALUE~ANN\$AlmMast\$1111111.state
Alarm - Isolate	DI	3	KCPLD1:DATAVALUE~ANN\$AlmIso\$1111111.state
Alarm - Inhibit	DI	4	KCPLD1:DATAVALUE~ANN\$AlmInh\$1111111.state
Alarm - Trip Offline	DI	5	KCPLD1:DATAVALUE~ANN\$AlmTrpOff\$1111111.state
Local - Remote	DI	6	KCPLD1:DATAVALUE~ANN\$LocRem\$1111111.state
BESS Active	DO	0	KCPLD1:DeviceOperate~CON\$BESSAct\$1111111
Schedule Override	DO	1	KCPLD1:DeviceOperate~CON\$SchdlOvrds\$1111111
Reset Battery	DO	2	KCPLD1:DeviceOperate~CON\$Rst\$1111111
Energy Available (%)	AI	0	KCPLD1:DATAVALUE~MET\$EAvail\$1111111.value
Active State	AI	1	KCPLD1:DATAVALUE~MET\$ActSte\$1111111.value
Active Status	AI	2	KCPLD1:DATAVALUE~MET\$ActSts\$1111111.value
Power Mode	AI	3	KCPLD1:DATAVALUE~MET\$PwrMode\$1111111.value
Reactive Mode	AI	4	KCPLD1:DATAVALUE~MET\$VARMode\$1111111.value
Charge Mode	AI	5	KCPLD1:DATAVALUE~MET\$CrgMode\$1111111.value
kW - Max Discharge Rate	AI	6	KCPLD1:DATAVALUE~MET\$kWMax\$1111111.value
kW - Load Following	AI	7	KCPLD1:DATAVALUE~MET\$kWLF\$1111111.value
kW - Discharge Start Time (2400)	AI	8	KCPLD1:DATAVALUE~MET\$kWStart\$1111111.value
kW - Discharge Duration (min)	AI	9	KCPLD1:DATAVALUE~MET\$kWDur\$1111111.value
kVAR - Max Discharge Rate	AI	10	KCPLD1:DATAVALUE~MET\$kVARMax\$1111111.value
kVAR - Fixed PF	AI	11	KCPLD1:DATAVALUE~MET\$FxdPF\$1111111.value
kVAR - Discharge Start Time (2400)	AI	12	KCPLD1:DATAVALUE~MET\$kVARStart\$1111111.value
kVAR - Discharge Duration (min)	AI	13	KCPLD1:DATAVALUE~MET\$kVARDur\$1111111.value
kW - Max Charge Rate	AI	14	KCPLD1:DATAVALUE~MET\$CrgMax\$1111111.value
kW - Charge Following	AI	15	KCPLD1:DATAVALUE~MET\$CrgLF\$1111111.value
kW - Charge Start Time (2400)	AI	16	KCPLD1:DATAVALUE~MET\$CrgStart\$1111111.value
kW - Charge Duration (min)	AI	17	KCPLD1:DATAVALUE~MET\$CrgDur\$1111111.value
Recalculation Time (sec)	AI	18	KCPLD1:DATAVALUE~MET\$Recalc\$1111111.value
Set Power Mode	AO	0	KCPLD1:DeviceOperate~CO\$PwrMode\$1111111
Set Reactive Mode	AO	1	KCPLD1:DeviceOperate~CO\$VARMode\$1111111
Set Charge Mode	AO	2	KCPLD1:DeviceOperate~CO\$CrgMode\$1111111
kW - Set Max Discharge Rate	AO	3	KCPLD1:DeviceOperate~CO\$kWMax\$1111111
kW - Set Load Following	AO	4	KCPLD1:DeviceOperate~CO\$kWLF\$1111111
kW - Set Discharge Start Time (2400)	AO	5	KCPLD1:DeviceOperate~CO\$kWStart\$1111111

SEL 3530-4: Battery Controller

Name	Point Type	DNP Point	ICCP Name
kW - Set Discharge Duration (min)	AO	6	KCPLD1:DeviceOperate~CO\$kWDur\$11111111
kVAR - Set Max Discharge Rate	AO	7	KCPLD1:DeviceOperate~CO\$kVARMaX\$11111111
kVAR - Set Fixed PF	AO	8	KCPLD1:DeviceOperate~CO\$FxdPF\$11111111
kVAR - Set Discharge Start Time (2400)	AO	9	KCPLD1:DeviceOperate~CO\$kVARStart\$11111111
kVAR - Set Discharge Duration (min)	AO	10	KCPLD1:DeviceOperate~CO\$kVARDur\$11111111
kW - Set Max Charge Rate	AO	11	KCPLD1:DeviceOperate~CO\$CrgMax\$11111111
kW - Set Charge Following	AO	12	KCPLD1:DeviceOperate~CO\$CrgLF\$11111111
kW - Set Charge Start Time (2400)	AO	13	KCPLD1:DeviceOperate~CO\$CrgStart\$11111111
kW - Set Charge Duration (min)	AO	14	KCPLD1:DeviceOperate~CO\$CrgDur\$11111111
Set Recalculation Time (sec)	AO	15	KCPLD1:DeviceOperate~CO\$Recalc\$11111111

S&C IntelliCAP Plus: Capacitor Bank Controller (Standard)

Name	Point Type	DNP Point	ICCP Name
Device Status	DI	0	KCPLD1:DATAVALUE~ANN\$DevSts\$2222222.state
Auto - Manual Status	DI	2	KCPLD1:DATAVALUE~ANN\$AutoMan\$2222222.state
Local - Remote	DI	3	KCPLD1:DATAVALUE~ANN\$LocRem\$2222222.state
Alarm Summary	DI	4	KCPLD1:DATAVALUE~ANN\$AlmSum\$2222222.state
SCADA Override Status	DI	5	KCPLD1:DATAVALUE~ANN\$SCADAQvrd\$2222222.state
Over Voltage	DI	6	KCPLD1:DATAVALUE~ANN\$OverV\$2222222.state
Under Voltage	DI	7	KCPLD1:DATAVALUE~ANN\$UndrV\$2222222.state
Emergency Voltage Override	DI	8	KCPLD1:DATAVALUE~ANN\$EmerVOvrd\$2222222.state
Reclose Block	DI	9	KCPLD1:DATAVALUE~ANN\$RclsBlck\$2222222.state
Maximum Daily Cycles	DI	10	KCPLD1:DATAVALUE~ANN\$MaxDayCyc\$2222222.state
Load Fuse Blown	DI	11	KCPLD1:DATAVALUE~ANN\$FuseBlwn\$2222222.state
Temperature Sensor Error	DI	12	KCPLD1:DATAVALUE~ANN\$TmpSnsErr\$2222222.state
Neutral Sensor - Lockout	DI	18	KCPLD1:DATAVALUE~ANN\$NeuSnsLOS\$2222222.state
Neutral Sensor - Continuous	DI	19	KCPLD1:DATAVALUE~ANN\$NeuSnsCont\$2222222.state
Neutral Sensor - Zero	DI	20	KCPLD1:DATAVALUE~ANN\$NeuSns0\$2222222.state
Device Operate	DO	0	KCPLD1:DeviceOperate~CON\$DevOp\$2222222
Auto - Manual	DO	1	KCPLD1:DeviceOperate~CON\$AutoMan\$2222222
SCADA Override Mode	DO	2	KCPLD1:DeviceOperate~CON\$SCADAQvrd\$2222222
Reset Neutral Lockout	DO	3	KCPLD1:DeviceOperate~CON\$RstNeuLO\$2222222
Reset Alarms	DO	5	KCPLD1:DeviceOperate~CON\$RstAlm\$2222222
Inhibit Automatic Operation Timer	DO	6	KCPLD1:DeviceOperate~CON\$InhbtAuto\$2222222
Control Strategy	AI	2	KCPLD1:DATAVALUE~MET\$CtrlStrgy\$2222222.value
Voltage - Secondary	AI	4	KCPLD1:DATAVALUE~MET\$SecV\$2222222.value
Time Remaining in SCADA Override Mode	AI	6	KCPLD1:DATAVALUE~MET\$SCADAQvrdTmr\$2222222.value
Current - Neutral RMS - Fundamental	AI	7	KCPLD1:DATAVALUE~MET\$NeuCur\$2222222.value
THD - Voltage	AI	13	KCPLD1:DATAVALUE~MET\$THDV\$2222222.value
THD - Neutral	AI	21	KCPLD1:DATAVALUE~MET\$THDNeu\$2222222.value
Last Switch In or Out Voltage Delta	AI	25	KCPLD1:DATAVALUE~MET\$SwVdlt\$2222222.value

S&C IntelliCAP Plus: Capacitor Bank Controller (Standard)

Name	Point Type	DNP Point	ICCP Name
Current - Neutral RMS - Total	AI	26	KCPLD1:DATAVALUE~MET\$TotNeuCur\$2222222.value
Last Switch Operation Reason	AI	28	KCPLD1:DATAVALUE~MET\$OpCode\$2222222.value

S&C IntelliCAP Plus: Capacitor Bank Controller (VAR)

Name	Point Type	DNP Point	ICCP Name
Device Status	DI	0	KCPLD1:DATAVALUE~ANN\$DevSts\$3333333.state
Auto - Manual Status	DI	2	KCPLD1:DATAVALUE~ANN\$AutoMan\$3333333.state
Local - Remote	DI	3	KCPLD1:DATAVALUE~ANN\$LocRem\$3333333.state
Alarm Summary	DI	4	KCPLD1:DATAVALUE~ANN\$AlmSum\$3333333.state
SCADA Override Status	DI	5	KCPLD1:DATAVALUE~ANN\$SCADAOvrd\$3333333.state
Over Voltage	DI	6	KCPLD1:DATAVALUE~ANN\$OverV\$3333333.state
Under Voltage	DI	7	KCPLD1:DATAVALUE~ANN\$UndrV\$3333333.state
Emergency Voltage Override	DI	8	KCPLD1:DATAVALUE~ANN\$EmerVOvrd\$3333333.state
Reclose Block	DI	9	KCPLD1:DATAVALUE~ANN\$RclsBlck\$3333333.state
Maximum Daily Cycles	DI	10	KCPLD1:DATAVALUE~ANN\$MaxDayCyc\$3333333.state
Load Fuse Blown	DI	11	KCPLD1:DATAVALUE~ANN\$FuseBlwn\$3333333.state
Temperature Sensor Error	DI	12	KCPLD1:DATAVALUE~ANN\$TmpSnsErr\$3333333.state
Neutral Sensor - Option	DI	16	KCPLD1:DATAVALUE~ANN\$NeuSnsOpt\$3333333.state
Neutral Sensor - Lockout	DI	18	KCPLD1:DATAVALUE~ANN\$NeuSnsLO\$3333333.state
Neutral Sensor - Continuous	DI	19	KCPLD1:DATAVALUE~ANN\$NeuSnsCont\$3333333.state
Neutral Sensor - Zero	DI	20	KCPLD1:DATAVALUE~ANN\$NeuSns0\$3333333.state
VAR Option	DI	21	KCPLD1:DATAVALUE~ANN\$VAROpt\$3333333.state
Current Direction	DI	22	KCPLD1:DATAVALUE~ANN\$CurDir\$3333333.state
Low Switching VAR Delta	DI	23	KCPLD1:DATAVALUE~ANN\$LoSwVARDlt\$3333333.state
Current Sensor Location	DI	26	KCPLD1:DATAVALUE~ANN\$CurSnsLoc\$3333333.state
Device Operate	DO	0	KCPLD1:DeviceOperate~CON\$DevOp\$3333333
Auto - Manual	DO	1	KCPLD1:DeviceOperate~CON\$AutoMan\$3333333
SCADA Override Mode	DO	2	KCPLD1:DeviceOperate~CON\$SCADAOvrd\$3333333
Reset Neutral Lockout	DO	3	KCPLD1:DeviceOperate~CON\$RstNeuLO\$3333333
Reset Alarms	DO	5	KCPLD1:DeviceOperate~CON\$RstAlm\$3333333
Inhibit Automatic Operation Timer	DO	6	KCPLD1:DeviceOperate~CON\$InhbtAuto\$3333333
Control Strategy	AI	2	KCPLD1:DATAVALUE~MET\$CtrlStrgy\$3333333.value
Voltage - Secondary	AI	4	KCPLD1:DATAVALUE~MET\$SecV\$3333333.value
Voltage - Primary (kV)	AI	5	KCPLD1:DATAVALUE~MET\$PriV\$3333333.value
Time Remaining in SCADA Override Mode	AI	6	KCPLD1:DATAVALUE~MET\$SCADAOvrdTmr\$3333333.value
Current - Neutral RMS - Fundamental	AI	7	KCPLD1:DATAVALUE~MET\$NeuCur\$3333333.value
Current - Phase A	AI	8	KCPLD1:DATAVALUE~MET\$Cur\$3333333.value
Reactive Power - 3 Phase (kVAR)	AI	10	KCPLD1:DATAVALUE~MET\$TotVAR\$3333333.value
Apparent Power - 3 Phase (kVA)	AI	11	KCPLD1:DATAVALUE~MET\$TotVA\$3333333.value
Real Power - 3 Phase (kW)	AI	12	KCPLD1:DATAVALUE~MET\$TotW\$3333333.value

S&C IntelliCAP Plus: Capacitor Bank Controller (VAR)

Name	Point Type	DNP Point	ICCP Name
THD - Voltage	AI	13	KCPLD1:DATAVALUE~MET\$THDV\$3333333.value
THD - Current	AI	17	KCPLD1:DATAVALUE~MET\$THDCur\$3333333.value
THD - Neutral	AI	21	KCPLD1:DATAVALUE~MET\$THDNeu\$3333333.value
Last Switch In or Out Voltage Delta	AI	25	KCPLD1:DATAVALUE~MET\$SwVDit\$3333333.value
Current - Neutral RMS - Total	AI	26	KCPLD1:DATAVALUE~MET\$TotNeuCur\$3333333.value
Last kVAR Delta	AI	27	KCPLD1:DATAVALUE~MET\$VARDit\$3333333.value
Last Switch Operation Reason	AI	28	KCPLD1:DATAVALUE~MET\$OpCode\$3333333.value

Horstmann: Fault Current Indicators and Receiver

Name	Point Type	DNP Point	ICCP Name
FCI Comm Failure	DI	0	KCPLD1:DATAVALUE~ANN\$CommFail\$8888888.state
Smart Controller Reporter Operational	DI	2	KCPLD1:DATAVALUE~ANN\$DeviceOn\$8888888.state
Voltage - Low DC	DI	4	KCPLD1:DATAVALUE~ANN\$LoDCV\$8888888.state
Reset Smart Reporter Controller	DO	0	KCPLD1:DeviceOperate~CON\$RstSmtRptCtrl\$8888888
Reset All Momentary and Permanent Fault Counters	DO	1	KCPLD1:DeviceOperate~CON\$RstFltCnt\$8888888
Reset All FCIs	DO	2	KCPLD1:DeviceOperate~CON\$RstFCIs\$8888888
FCI Comm Fail	AI	0	KCPLD1:DATAVALUE~MET\$CommFail\$8888888.value
Low Battery	AI	1	KCPLD1:DATAVALUE~MET\$LoBatt\$8888888.value
Over Current - Phase A	DI	5	KCPLD1:DATAVALUE~ANN\$OverCur1PhA\$8888888.state
Permanent Fault - Phase A	DI	6	KCPLD1:DATAVALUE~ANN\$PermFlt1PhA\$8888888.state
Momentary Fault - Phase A	DI	7	KCPLD1:DATAVALUE~ANN\$MmtFlt1PhA\$8888888.state
Overhead Line Current Loss - Phase A	DI	8	KCPLD1:DATAVALUE~ANN\$OvhdCurLoss1PhA\$8888888.state
Loss of Voltage - Phase A	DI	9	KCPLD1:DATAVALUE~ANN\$VLoss1PhA\$8888888.state
Over Current - Phase B	DI	10	KCPLD1:DATAVALUE~ANN\$OverCur1PhB\$8888888.state
Permanent Fault - Phase B	DI	11	KCPLD1:DATAVALUE~ANN\$PermFlt1PhB\$8888888.state
Momentary Fault - Phase B	DI	12	KCPLD1:DATAVALUE~ANN\$MmtFlt1PhB\$8888888.state
Overhead Line Current Loss - Phase B	DI	13	KCPLD1:DATAVALUE~ANN\$OvhdCurLoss1PhB\$8888888.state
Loss of Voltage - Phase B	DI	14	KCPLD1:DATAVALUE~ANN\$VLoss1PhB\$8888888.state
Over Current - Phase C	DI	15	KCPLD1:DATAVALUE~ANN\$OverCur1PhC\$8888888.state
Permanent Fault - Phase C	DI	16	KCPLD1:DATAVALUE~ANN\$PermFlt1PhC\$8888888.state
Momentary Fault - Phase C	DI	17	KCPLD1:DATAVALUE~ANN\$MmtFlt1PhC\$8888888.state

Horstmann: Fault Current Indicators and Receiver

Name	Point Type	DNP Point	ICCP Name
Overhead Line Current Loss - Phase C	DI	18	KCPLD1:DATAVALUE~ANN\$OvhdCurLoss1PhC\$8888888.state
Loss of Voltage - Phase C	DI	19	KCPLD1:DATAVALUE~ANN\$VLoss1PhC\$8888888.state
Temporary Faults - Phase A	CTR	0	KCPLD1:DATAVALUE~CTR\$TempFit1PhA\$8888888.value
Permanent Faults - Phase A	CTR	1	KCPLD1:DATAVALUE~CTR\$PermFit1PhA\$8888888.value
Temporary Faults - Phase B	CTR	2	KCPLD1:DATAVALUE~CTR\$TempFit1PhB\$8888888.value
Permanent Faults - Phase B	CTR	3	KCPLD1:DATAVALUE~CTR\$PermFit1PhB\$8888888.value
Temporary Faults - Phase C	CTR	4	KCPLD1:DATAVALUE~CTR\$TempFit1PhC\$8888888.value
Permanent Faults - Phase C	CTR	5	KCPLD1:DATAVALUE~CTR\$PermFit1PhC\$8888888.value
Fault Current - Phase A	AI	2	KCPLD1:DATAVALUE~MET\$FitCur1PhA\$8888888.value
Fault Duration - Phase A	AI	3	KCPLD1:DATAVALUE~MET\$FitDur1PhA\$8888888.value
Last Known Good Current - Phase A	AI	4	KCPLD1:DATAVALUE~MET\$LKGCur1PhA\$8888888.value
Current - Average - Phase A	AI	5	KCPLD1:DATAVALUE~MET\$CurAvg1PhA\$8888888.value
Fault Current - Phase B	AI	11	KCPLD1:DATAVALUE~MET\$FitCur1PhB\$8888888.value
Fault Duration - Phase B	AI	12	KCPLD1:DATAVALUE~MET\$FitDur1PhB\$8888888.value
Last Known Good Current - Phase B	AI	13	KCPLD1:DATAVALUE~MET\$LKGCur1PhB\$8888888.value
Current - Average - Phase B	AI	14	KCPLD1:DATAVALUE~MET\$CurAvg1PhB\$8888888.value
Fault Current - Phase C	AI	20	KCPLD1:DATAVALUE~MET\$FitCur1PhC\$8888888.value

Horstmann: Fault Current Indicators and Receiver

Name	Point Type	DNP Point	ICCP Name
Fault Duration - Phase C	AI	21	KCPLD1:DATAVALUE~MET\$FitDur1PhC\$8888888.value
Last Known Good Current - Phase C	AI	22	KCPLD1:DATAVALUE~MET\$LKGCur1PhC\$8888888.value
Current - Average - Phase C	AI	23	KCPLD1:DATAVALUE~MET\$CurAvg1PhC\$8888888.value
Over Current - Phase A	DI	20	KCPLD1:DATAVALUE~ANN\$OverCur2PhA\$8888888.state
Permanent Fault - Phase A	DI	21	KCPLD1:DATAVALUE~ANN\$PermFlt2PhA\$8888888.state
Momentary Fault - Phase A	DI	22	KCPLD1:DATAVALUE~ANN\$MmtFlt2PhA\$8888888.state
Overhead Line Current Loss - Phase A	DI	23	KCPLD1:DATAVALUE~ANN\$OvhdCurLoss2PhA\$8888888.state
Loss of Voltage - Phase A	DI	24	KCPLD1:DATAVALUE~ANN\$VLoss2PhA\$8888888.state
Over Current - Phase B	DI	25	KCPLD1:DATAVALUE~ANN\$OverCur2PhB\$8888888.state
Permanent Fault - Phase B	DI	26	KCPLD1:DATAVALUE~ANN\$PermFlt2PhB\$8888888.state
Momentary Fault - Phase B	DI	27	KCPLD1:DATAVALUE~ANN\$MmtFlt2PhB\$8888888.state
Overhead Line Current Loss - Phase B	DI	28	KCPLD1:DATAVALUE~ANN\$OvhdCurLoss2PhB\$8888888.state
Loss of Voltage - Phase B	DI	29	KCPLD1:DATAVALUE~ANN\$VLoss2PhB\$8888888.state
Over Current - Phase C	DI	30	KCPLD1:DATAVALUE~ANN\$OverCur2PhC\$8888888.state
Permanent Fault - Phase C	DI	31	KCPLD1:DATAVALUE~ANN\$PermFlt2PhC\$8888888.state
Momentary Fault - Phase C	DI	32	KCPLD1:DATAVALUE~ANN\$MmtFlt2PhC\$8888888.state
Overhead Line Current Loss - Phase C	DI	33	KCPLD1:DATAVALUE~ANN\$OvhdCurLoss2PhC\$8888888.state

Horstmann: Fault Current Indicators and Receiver

Name	Point Type	DNP Point	ICCP Name
Loss of Voltage - Phase C	DI	34	KCPLD1:DATAVALUE~ANN\$VLoss2PhC\$8888888.state
Temporary Faults - Phase A	CTR	6	KCPLD1:DATAVALUE~CTR\$TempFlt2PhA\$8888888.value
Permanent Faults - Phase A	CTR	7	KCPLD1:DATAVALUE~CTR\$PermFlt2PhA\$8888888.value
Temporary Faults - Phase B	CTR	8	KCPLD1:DATAVALUE~CTR\$TempFlt2PhB\$8888888.value
Permanent Faults - Phase B	CTR	9	KCPLD1:DATAVALUE~CTR\$PermFlt2PhB\$8888888.value
Temporary Faults - Phase C	CTR	10	KCPLD1:DATAVALUE~CTR\$TempFlt2PhC\$8888888.value
Permanent Faults - Phase C	CTR	11	KCPLD1:DATAVALUE~CTR\$PermFlt2PhC\$8888888.value
Fault Current - Phase A	AI	29	KCPLD1:DATAVALUE~MET\$FltCur2PhA\$8888888.value
Fault Duration - Phase A	AI	30	KCPLD1:DATAVALUE~MET\$FltDur2PhA\$8888888.value
Last Known Good Current - Phase A	AI	31	KCPLD1:DATAVALUE~MET\$LKGCur2PhA\$8888888.value
Current - Average - Phase A	AI	32	KCPLD1:DATAVALUE~MET\$CurAvg2PhA\$8888888.value
Fault Current - Phase B	AI	38	KCPLD1:DATAVALUE~MET\$FltCur2PhB\$8888888.value
Fault Duration - Phase B	AI	39	KCPLD1:DATAVALUE~MET\$FltDur2PhB\$8888888.value
Last Known Good Current - Phase B	AI	40	KCPLD1:DATAVALUE~MET\$LKGCur2PhB\$8888888.value
Current - Average - Phase B	AI	41	KCPLD1:DATAVALUE~MET\$CurAvg2PhB\$8888888.value
Fault Current - Phase C	AI	47	KCPLD1:DATAVALUE~MET\$FltCur2PhC\$8888888.value
Fault Duration - Phase C	AI	48	KCPLD1:DATAVALUE~MET\$FltDur2PhC\$8888888.value

Horstmann: Fault Current Indicators and Receiver

Name	Point Type	DNP Point	ICCP Name
Last Known Good Current - Phase C	AI	49	KCPLD1:DATAVALUE~MET\$LKGCur2PhC\$8888888.value
Current - Average - Phase C	AI	50	KCPLD1:DATAVALUE~MET\$CurAvg2PhC\$8888888.value
Over Current - Phase A	DI	35	KCPLD1:DATAVALUE~ANN\$OverCur3PhA\$8888888.state
Permanent Fault - Phase A	DI	36	KCPLD1:DATAVALUE~ANN\$PermFit3PhA\$8888888.state
Momentary Fault - Phase A	DI	37	KCPLD1:DATAVALUE~ANN\$MmtFit3PhA\$8888888.state
Overhead Line Current Loss - Phase A	DI	38	KCPLD1:DATAVALUE~ANN\$OvhdCurLoss3PhA\$8888888.state
Loss of Voltage - Phase A	DI	39	KCPLD1:DATAVALUE~ANN\$VLoss3PhA\$8888888.state
Over Current - Phase B	DI	40	KCPLD1:DATAVALUE~ANN\$OverCur3PhB\$8888888.state
Permanent Fault - Phase B	DI	41	KCPLD1:DATAVALUE~ANN\$PermFit3PhB\$8888888.state
Momentary Fault - Phase B	DI	42	KCPLD1:DATAVALUE~ANN\$MmtFit3PhB\$8888888.state
Overhead Line Current Loss - Phase B	DI	43	KCPLD1:DATAVALUE~ANN\$OvhdCurLoss3PhB\$8888888.state
Loss of Voltage - Phase B	DI	44	KCPLD1:DATAVALUE~ANN\$VLoss3PhB\$8888888.state
Over Current - Phase C	DI	45	KCPLD1:DATAVALUE~ANN\$OverCur3PhC\$8888888.state
Permanent Fault - Phase C	DI	46	KCPLD1:DATAVALUE~ANN\$PermFit3PhC\$8888888.state
Momentary Fault - Phase C	DI	47	KCPLD1:DATAVALUE~ANN\$MmtFit3PhC\$8888888.state
Overhead Line Current Loss - Phase C	DI	48	KCPLD1:DATAVALUE~ANN\$OvhdCurLoss3PhC\$8888888.state
Loss of Voltage - Phase C	DI	49	KCPLD1:DATAVALUE~ANN\$VLoss3PhC\$8888888.state

Horstmann: Fault Current Indicators and Receiver

Name	Point Type	DNP Point	ICCP Name
Temporary Faults - Phase A	CTR	12	KCPLD1:DATAVALUE~CTR\$TempFit3PhA\$8888888.value
Permanent Faults - Phase A	CTR	13	KCPLD1:DATAVALUE~CTR\$PermFit3PhA\$8888888.value
Temporary Faults - Phase B	CTR	14	KCPLD1:DATAVALUE~CTR\$TempFit3PhB\$8888888.value
Permanent Faults - Phase B	CTR	15	KCPLD1:DATAVALUE~CTR\$PermFit3PhB\$8888888.value
Temporary Faults - Phase C	CTR	16	KCPLD1:DATAVALUE~CTR\$TempFit3PhC\$8888888.value
Permanent Faults - Phase C	CTR	17	KCPLD1:DATAVALUE~CTR\$PermFit3PhC\$8888888.value
Fault Current - Phase A	AI	56	KCPLD1:DATAVALUE~MET\$FitCur3PhA\$8888888.value
Fault Duration - Phase A	AI	57	KCPLD1:DATAVALUE~MET\$FitDur3PhA\$8888888.value
Last Known Good Current - Phase A	AI	58	KCPLD1:DATAVALUE~MET\$LKGCur3PhA\$8888888.value
Current - Average - Phase A	AI	59	KCPLD1:DATAVALUE~MET\$CurAvg3PhA\$8888888.value
Fault Current - Phase B	AI	65	KCPLD1:DATAVALUE~MET\$FitCur3PhB\$8888888.value
Fault Duration - Phase B	AI	66	KCPLD1:DATAVALUE~MET\$FitDur3PhB\$8888888.value
Last Known Good Current - Phase B	AI	67	KCPLD1:DATAVALUE~MET\$LKGCur3PhB\$8888888.value
Current - Average - Phase B	AI	68	KCPLD1:DATAVALUE~MET\$CurAvg3PhB\$8888888.value
Fault Current - Phase C	AI	74	KCPLD1:DATAVALUE~MET\$FitCur3PhC\$8888888.value
Fault Duration - Phase C	AI	75	KCPLD1:DATAVALUE~MET\$FitDur3PhC\$8888888.value
Last Known Good Current - Phase C	AI	76	KCPLD1:DATAVALUE~MET\$LKGCur3PhC\$8888888.value

Horstmann: Fault Current Indicators and Receiver

Name	Point Type	DNP Point	ICCP Name
Current - Average - Phase C	AI	77	KCPLD1:DATAVALUE~MET\$CurAvg3PhC\$8888888.value
Over Current - Phase A	DI	50	KCPLD1:DATAVALUE~ANN\$OverCur4PhA\$8888888.state
Permanent Fault - Phase A	DI	51	KCPLD1:DATAVALUE~ANN\$PermFlt4PhA\$8888888.state
Momentary Fault - Phase A	DI	52	KCPLD1:DATAVALUE~ANN\$MmtFlt4PhA\$8888888.state
Overhead Line Current Loss - Phase A	DI	53	KCPLD1:DATAVALUE~ANN\$OvhdCurLoss4PhA\$8888888.state
Loss of Voltage - Phase A	DI	54	KCPLD1:DATAVALUE~ANN\$VLoss4PhA\$8888888.state
Over Current - Phase B	DI	55	KCPLD1:DATAVALUE~ANN\$OverCur4PhB\$8888888.state
Permanent Fault - Phase B	DI	56	KCPLD1:DATAVALUE~ANN\$PermFlt4PhB\$8888888.state
Momentary Fault - Phase B	DI	57	KCPLD1:DATAVALUE~ANN\$MmtFlt4PhB\$8888888.state
Overhead Line Current Loss - Phase B	DI	58	KCPLD1:DATAVALUE~ANN\$OvhdCurLoss4PhB\$8888888.state
Loss of Voltage - Phase B	DI	59	KCPLD1:DATAVALUE~ANN\$VLoss4PhB\$8888888.state
Over Current - Phase C	DI	60	KCPLD1:DATAVALUE~ANN\$OverCur4PhC\$8888888.state
Permanent Fault - Phase C	DI	61	KCPLD1:DATAVALUE~ANN\$PermFlt4PhC\$8888888.state
Momentary Fault - Phase C	DI	62	KCPLD1:DATAVALUE~ANN\$MmtFlt4PhC\$8888888.state
Overhead Line Current Loss - Phase C	DI	63	KCPLD1:DATAVALUE~ANN\$OvhdCurLoss4PhC\$8888888.state
Loss of Voltage - Phase C	DI	64	KCPLD1:DATAVALUE~ANN\$VLoss4PhC\$8888888.state
Temporary Faults - Phase A	CTR	18	KCPLD1:DATAVALUE~CTR\$TempFlt4PhA\$8888888.value
Permanent Faults - Phase A	CTR	19	KCPLD1:DATAVALUE~CTR\$PermFlt4PhA\$8888888.value
Temporary Faults - Phase B	CTR	20	KCPLD1:DATAVALUE~CTR\$TempFlt4PhB\$8888888.value
Permanent Faults - Phase B	CTR	21	KCPLD1:DATAVALUE~CTR\$PermFlt4PhB\$8888888.value
Temporary Faults - Phase C	CTR	22	KCPLD1:DATAVALUE~CTR\$TempFlt4PhC\$8888888.value
Permanent Faults - Phase C	CTR	23	KCPLD1:DATAVALUE~CTR\$PermFlt4PhC\$8888888.value
Fault Current - Phase A	AI	83	KCPLD1:DATAVALUE~MET\$FltCur4PhA\$8888888.value
Fault Duration - Phase A	AI	84	KCPLD1:DATAVALUE~MET\$FltDur4PhA\$8888888.value
Last Known Good Current - Phase A	AI	85	KCPLD1:DATAVALUE~MET\$LKGCur4PhA\$8888888.value
Current - Average - Phase A	AI	86	KCPLD1:DATAVALUE~MET\$CurAvg4PhA\$8888888.value
Fault Current - Phase B	AI	92	KCPLD1:DATAVALUE~MET\$FltCur4PhB\$8888888.value
Fault Duration - Phase B	AI	93	KCPLD1:DATAVALUE~MET\$FltDur4PhB\$8888888.value
Last Known Good Current - Phase B	AI	94	KCPLD1:DATAVALUE~MET\$LKGCur4PhB\$8888888.value
Current - Average - Phase B	AI	95	KCPLD1:DATAVALUE~MET\$CurAvg4PhB\$8888888.value
Fault Current - Phase C	AI	101	KCPLD1:DATAVALUE~MET\$FltCur4PhC\$8888888.value
Fault Duration - Phase C	AI	102	KCPLD1:DATAVALUE~MET\$FltDur4PhC\$8888888.value
Last Known Good Current - Phase C	AI	103	KCPLD1:DATAVALUE~MET\$LKGCur4PhC\$8888888.value
Current - Average - Phase C	AI	104	KCPLD1:DATAVALUE~MET\$CurAvg4PhC\$8888888.value

SEL 651R: Recloser Controller

Name	Point Type	DNP Point	ICCP Name
Enabled	DI	0	KCPLD1:DATAVALUE~ANN\$Enbl\$4444444.state
Device Status	DI	1	KCPLD1:DATAVALUE~ANN\$DevSts\$4444444.state
Loss of Potential	DI	2	KCPLD1:DATAVALUE~ANN\$PotentialLoss\$4444444.state
Fault - Phase C	DI	3	KCPLD1:DATAVALUE~ANN\$FltPhC\$4444444.state
Fault - Phase B	DI	4	KCPLD1:DATAVALUE~ANN\$FltPhB\$4444444.state
Fault - Phase A	DI	5	KCPLD1:DATAVALUE~ANN\$FltPhA\$4444444.state
Sync Check Elements	DI	6	KCPLD1:DATAVALUE~ANN\$SyncChkElem\$4444444.state
Cabinet Door	DI	7	KCPLD1:DATAVALUE~ANN\$CabDoor\$4444444.state
50CO - Ground Overcurrent Status	DI	8	KCPLD1:DATAVALUE~ANN\$GndEnbl\$4444444.state
79CO - Reclosing Status	DI	9	KCPLD1:DATAVALUE~ANN\$RclsEnbl\$4444444.state
Local - Remote	DI	10	KCPLD1:DATAVALUE~ANN\$LocRem\$4444444.state
Fast Curves Status	DI	11	KCPLD1:DATAVALUE~ANN\$FstCrv\$4444444.state
Push Buttons Locked	DI	12	KCPLD1:DATAVALUE~ANN\$PshButLock\$4444444.state
Hot Line Tag Status	DI	13	KCPLD1:DATAVALUE~ANN\$HotLnTag\$4444444.state
Aux 1 Status	DI	14	KCPLD1:DATAVALUE~ANN\$Aux1\$4444444.state
Aux 2 Status	DI	15	KCPLD1:DATAVALUE~ANN\$Aux2\$4444444.state
Aux 3 Status	DI	16	KCPLD1:DATAVALUE~ANN\$Aux3\$4444444.state
Battery Failure	DI	17	KCPLD1:DATAVALUE~ANN\$BattFail\$4444444.state
External Power	DI	18	KCPLD1:DATAVALUE~ANN\$ExtPwr\$4444444.state
Lockout	DI	19	KCPLD1:DATAVALUE~ANN\$RclsLO\$4444444.state
Current Direction	DI	20	KCPLD1:DATAVALUE~ANN\$CurDir\$4444444.state
Contact Wear - 3 Phase	DI	21	KCPLD1:DATAVALUE~ANN\$BCW3Ph\$4444444.state
Clock Present	DI	22	KCPLD1:DATAVALUE~ANN\$ClkPres\$4444444.state
Hardware Alarm	DI	23	KCPLD1:DATAVALUE~ANN\$HWAlm\$4444444.state
Software Alarm	DI	24	KCPLD1:DATAVALUE~ANN\$SWAlm\$4444444.state
Aux 1	DO	25	KCPLD1:DeviceOperate~CON\$Aux1\$4444444
Aux 2	DO	26	KCPLD1:DeviceOperate~CON\$Aux2\$4444444
Aux 3	DO	27	KCPLD1:DeviceOperate~CON\$Aux3\$4444444
50CO - Ground Overcurrent	DO	29	KCPLD1:DeviceOperate~CON\$GndEnbl\$4444444
79CO - Reclosing	DO	30	KCPLD1:DeviceOperate~CON\$RclsEnbl\$4444444
Fast Curves	DO	31	KCPLD1:DeviceOperate~CON\$FstCrv\$4444444
Hot Line Tag	DO	32	KCPLD1:DeviceOperate~CON\$HotLnTag\$4444444
Device Operate	DO	33	KCPLD1:DeviceOperate~CON\$DevOp\$4444444
Reset Front Panel Targets	DO	34	KCPLD1:DeviceOperate~CON\$RstFrntPnlTgt\$4444444
Active Settings Group	CTR	0	KCPLD1:DATAVALUE~CTR\$ActSetGrp\$4444444.value

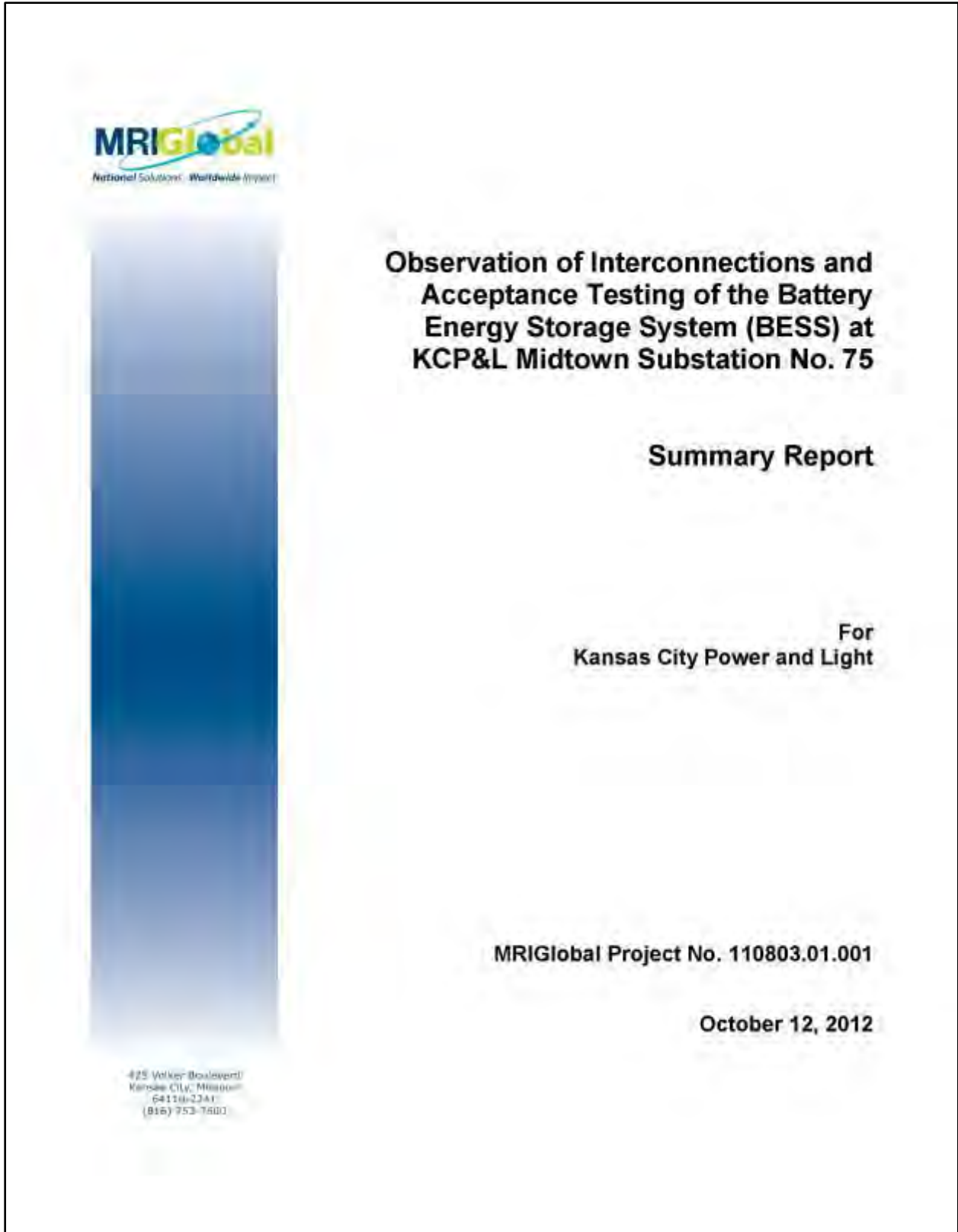
SEL 651R: Recloser Controller

Name	Point Type	DNP Point	ICCP Name
Internal Breaker Trips - Phase A	CTR	1	KCPLD1:DATAVALUE~CTR\$IntBrkTripPhA\$4444444.value
Internal Breaker Trips - Phase B	CTR	2	KCPLD1:DATAVALUE~CTR\$IntBrkTripPhB\$4444444.value
Internal Breaker Trips - Phase C	CTR	3	KCPLD1:DATAVALUE~CTR\$IntBrkTripPhC\$4444444.value
External Breaker Trips - Phase A	CTR	4	KCPLD1:DATAVALUE~CTR\$ExtBrkTripPhA\$4444444.value
External Breaker Trips - Phase B	CTR	5	KCPLD1:DATAVALUE~CTR\$ExtBrkTripPhB\$4444444.value
External Breaker Trips - Phase C	CTR	6	KCPLD1:DATAVALUE~CTR\$ExtBrkTripPhC\$4444444.value
Current - Phase A	AI	0	KCPLD1:DATAVALUE~MET\$CurPhA\$4444444.value
Current - Phase B	AI	1	KCPLD1:DATAVALUE~MET\$CurPhB\$4444444.value
Current - Phase C	AI	2	KCPLD1:DATAVALUE~MET\$CurPhC\$4444444.value
Current - Neutral	AI	3	KCPLD1:DATAVALUE~MET\$CurNeu\$4444444.value
Current - Ground	AI	4	KCPLD1:DATAVALUE~MET\$CurGnd\$4444444.value
Voltage - Phase A - Y (kV)	AI	5	KCPLD1:DATAVALUE~MET\$VPhAY\$4444444.value
Voltage - Phase B - Y (kV)	AI	6	KCPLD1:DATAVALUE~MET\$VPhBY\$4444444.value
Voltage - Phase C - Y (kV)	AI	7	KCPLD1:DATAVALUE~MET\$VPhCY\$4444444.value
Voltage - Phase A - Z (kV)	AI	8	KCPLD1:DATAVALUE~MET\$VPhAZ\$4444444.value
Voltage - Phase B - Z (kV)	AI	9	KCPLD1:DATAVALUE~MET\$VPhBZ\$4444444.value
Voltage - Phase C - Z (kV)	AI	10	KCPLD1:DATAVALUE~MET\$VPhCZ\$4444444.value
Real Power - Phase A (kW)	AI	11	KCPLD1:DATAVALUE~MET\$KWPhA\$4444444.value
Real Power - Phase B (kW)	AI	12	KCPLD1:DATAVALUE~MET\$KWPhB\$4444444.value
Real Power - Phase C (kW)	AI	13	KCPLD1:DATAVALUE~MET\$KWPhC\$4444444.value
Real Power - 3 Phase (kW)	AI	14	KCPLD1:DATAVALUE~MET\$KW3Ph\$4444444.value
Reactive Power - Phase A (kVAR)	AI	15	KCPLD1:DATAVALUE~MET\$KVARPhA\$4444444.value
Reactive Power - Phase B (kVAR)	AI	16	KCPLD1:DATAVALUE~MET\$KVARPhB\$4444444.value
Reactive Power - Phase C (kVAR)	AI	17	KCPLD1:DATAVALUE~MET\$KVARPhC\$4444444.value
Reactive Power - 3 Phase (kVAR)	AI	18	KCPLD1:DATAVALUE~MET\$KVAR3Ph\$4444444.value
Frequency	AI	19	KCPLD1:DATAVALUE~MET\$Freq\$4444444.value
Contact Wear - Phase A	AI	20	KCPLD1:DATAVALUE~MET\$BCWPhA\$4444444.value
Contact Wear - Phase B	AI	21	KCPLD1:DATAVALUE~MET\$BCWPhB\$4444444.value
Contact Wear - Phase C	AI	22	KCPLD1:DATAVALUE~MET\$BCWPhC\$4444444.value
Fault Type	AI	23	KCPLD1:DATAVALUE~MET\$FltType\$4444444.value
Fault Recloser Shot Counter	AI	24	KCPLD1:DATAVALUE~MET\$FltRclsShotCnt\$4444444.value
Fault Time	AI	25	KCPLD1:DATAVALUE~MET\$FltTm\$4444444.value
Fault Current - Phase A	AI	26	KCPLD1:DATAVALUE~MET\$FltCurPhA\$4444444.value
Fault Current - Phase B	AI	27	KCPLD1:DATAVALUE~MET\$FltCurPhB\$4444444.value
Fault Current - Phase C	AI	28	KCPLD1:DATAVALUE~MET\$FltCurPhC\$4444444.value

SEL 651R: Recloser Controller

Name	Point Type	DNP Point	ICCP Name
Fault Current - Ground	AI	29	KCPLD1:DATAVALUE~MET\$FitCurGnd\$4444444.value
Apparent Power - Phase A (kVA)	AI	30	KCPLD1:DATAVALUE~MET\$KVAPhA\$4444444.value
Apparent Power - Phase B (kVA)	AI	31	KCPLD1:DATAVALUE~MET\$KVAPhB\$4444444.value
Apparent Power - Phase C (kVA)	AI	32	KCPLD1:DATAVALUE~MET\$KVAPhC\$4444444.value
Apparent Power - 3 Phase (kVA)	AI	33	KCPLD1:DATAVALUE~MET\$KVA3Ph\$4444444.value
THD - Current - Phase A	AI	34	KCPLD1:DATAVALUE~MET\$THDCurPhA\$4444444.value
THD - Current - Phase B	AI	35	KCPLD1:DATAVALUE~MET\$THDCurPhB\$4444444.value
THD - Current - Phase C	AI	36	KCPLD1:DATAVALUE~MET\$THDCurPhC\$4444444.value
THD - Current - Neutral	AI	37	KCPLD1:DATAVALUE~MET\$THDCurNeu\$4444444.value
THD - Voltage - Phase A - Y	AI	38	KCPLD1:DATAVALUE~MET\$THDVPhAY\$4444444.value
THD - Voltage - Phase B - Y	AI	39	KCPLD1:DATAVALUE~MET\$THDVPhBY\$4444444.value
THD - Voltage - Phase C - Y	AI	40	KCPLD1:DATAVALUE~MET\$THDVPhCY\$4444444.value
THD - Voltage - Phase A - Z	AI	41	KCPLD1:DATAVALUE~MET\$THDVPhAZ\$4444444.value
THD - Voltage - Phase B - Z	AI	42	KCPLD1:DATAVALUE~MET\$THDVPhBZ\$4444444.value
THD - Voltage - Phase C - Z	AI	43	KCPLD1:DATAVALUE~MET\$THDVPhCZ\$4444444.value
Battery Voltage	AI	44	KCPLD1:DATAVALUE~MET\$BattV\$4444444.value
Battery Current	AI	45	KCPLD1:DATAVALUE~MET\$BattCur\$4444444.value
Set Active Settings Group	AO	0	KCPLD1:DeviceOperate~CO\$ActSetGrp\$4444444

Appendix G BESS Acceptance Test Report



**Observation of Interconnections and
Acceptance Testing of the Battery
Energy Storage System (BESS) at
KCP&L Midtown Substation No. 75**

Summary Report

For
Kansas City Power and Light
1200 Main
Kansas City, Missouri 64141

MRIGlobal Project No. 110803.01.001

October 12, 2012

Contents

Section 1. Introduction.....	1
Section 2. General Observations.....	2
Section 3. Specific Technical and Organizational Observations	3
3.1 Technical Observations During the Phase 1 Testing (May 18 to May 23)	3
3.2 Technical Observations During the Phase 2 Testing (June 28).....	5
3.3 Organizational Observations	5
Section 4. Summary of Recommendations.....	7
4.1 Technical Recommendations.....	7
4.2 Organizational Recommendations.....	7

Attachment

Attachment A—Statement of Work

Section 1. Introduction

MRIGlobal was contracted to provide technical advisory support to Kansas City Power and Light (KCP&L) throughout acceptance testing of the Battery Energy Storage System (BESS) at KCP&L Midtown Substation No. 75 in Kansas City, Missouri (Attachment A provides the Statement of Work for this contract). The BESS testing was conducted from mid-May through the end of June 2012, and additional testing may be conducted during fall of 2012. This report fulfills the requirements of Item 1d in the Statement of Work, which requires MRIGlobal to provide a letter summary of observations, review of battery performance, and any other special observations or recommendations regarding potential future use of the battery. In case additional testing is done in the future, MRIGlobal will draft an addendum to this report.

Major system components included (1) BESS, provided by Exergonix; and (2) a Storage Management System (SMS), provided by S&C. The SMS is a two-way inverter which acts as the controller and integrator of the BESS to the overall KCP&L electrical grid.

Initial testing began on May 17 and continued through May 23, at which point a failure in improperly rated wiring was installed in a critical area which caused an arc that resulted in electrical damage forcing a delay to testing activities. On June 28, testing resumed and all needed technical observations were completed.

Section 2. General Observations

In preparation for the testing, MRIGlobal reviewed the following documents:

- “*Acceptance Testing of the BESS at Midtown Substation,*” authored by S&C Equipment
- “*Grid Connected Battery System Functional Specification,*” authored by KCP&L
- “*Exergonix Energy Storage Systems,*” authored by Exergonix

The first two documents were supplied by KCP&L in support of the Statement of Work while Exergonix supplied the third document directly to MRIGlobal. These documents were well written and covered the points needed to verify that the equipment being supplied would meet the needs of the Smart Grid Design.

Based on the information in these documents, MRIGlobal assumed that every system element would be in place, checked, and ready for testing as a complete system prior to the start of Phase 1 testing. However, in actual practice at the site, only a partial test of separate components was conducted by staff who may not have been well-versed enough to actually provide interconnection of the BESS to an electric utility distribution system. Staff performing the BESS integration and testing were professional and completed assignments successfully, but they appeared to lack the detailed documentation necessary and were only available intermittently to support these efforts. For future work we recommend that KCP&L dedicate a representative mix of key personnel to this project with no conflicting assignments. See Section 4 for additional specific recommendations.

During the first phase of testing (conducted in May), MRIGlobal observed that although the contractor, Exergonix, was assigned responsibility for the testing in the “*BESS Commissioning Report*” by KCP&L (March 27, 2012), they were never onsite except for a few brief visits to check in. Instead, Exergonix relied on Myungshin, a subcontractor, and S&C to handle all the site work. Additional onsite staffing on their part may have provided better support to KCP&L, Myungshin, and S&C to resolve the technical and contractual issues that arose throughout testing. Myungshin and S&C worked together at the site on interconnections and software issues but significant delays were caused by miscommunications and an inability for the onsite personnel from Myungshin to provide S&C the information needed to finalize software parameters critical to effective communications between the SMS and the BESS control systems.

Section 3.

Specific Technical and Organizational Observations

MRIGlobal had numerous technical and organizational observations during the first and second phases of testing, which are described in the following subsections.

3.1 Technical Observations During the Phase 1 Testing (May 18 to May 23)

Upon arrival at the site, MRIGlobal noted that some one-line diagrams and additional limited schematics were available; however, the team needed more detailed information to properly wire up the potential transformers, current transformers, and S&C controls. There were no wiring diagrams to show what S&C required for connections. In addition, no kilowatt hour meter was installed initially to monitor the input/output of the BESS. In spite of these issues, the KCP&L relay crew was proficient and accepting of MRIGlobal oversight which resulted in a successful connection.

Subsequently, based on MRIGlobal's recommendations, a digital grid kilowatt hour meter was installed to meter and record the kW, kVAR, kVA, volts, amps, and harmonics of the energy flowing in and out of the BESS system. The installed meter was a grid-type meter based on PT/CT metrology instead of a standard kWh meter used at an industrial service drop as originally planned. Although there are protective measures within the SMS and the BESS to warn of failure of a component, this type of meter will provide the added measure of early warning of a component failure. However, as of testing completion, the meter was not working correctly after installation and this was mentioned to the KCP&L System Protection staff.

In response to observed electrical interference, Exergonix arranged for a thorough check-out of the BESS to determine the root cause of substantial interference in the electronics. After this checkout, Myungshin personnel installed a hospital-grade isolation transformer which did not correct the interference. This did rule out the control power source, 480-V feed from the site transformer, as the cause of the problem. It is quite probable the cause of the problem is from within the BESS. However, technical diagrams of the internal components were not provided and, as of testing completion, the root cause of the interference was not determined. Potential causes include low-voltage wiring, Ethernet cables co-located with high-voltage/high-current cables, or twisted pair shielded cable (if used) that may be grounded at both ends or not grounded at all. It is quite probable the source of the problem is within the BESS, given that the first BESS unit produced by the vendor (installed at another utility) is having similar problems with noise/interference.

From May 18 through May 22, 2012, various system checks were performed and system parameters were adjusted in order to get all components communicating properly. Successful testing of the BESS was completed, including a full charge (above 95% depth of charge with a full recharge taking approximately 59 minutes), and a full discharge (below 20% depth of charge, taking approximately 49 minutes). Verbal guidance for testing by Exergonix and its

MRIGlobal-20121110003-01-001_3

subcontractors advised against discharging below 20% depth of charge. A full range of VAR (volt-ampere reactive) control, both leading and lagging, was successfully completed by the SMS/BESS system.

On May 23, training of SMS and BESS for KCP&L site crew was completed prior to attempting another full charge of the BESS. During charge, the SMS display showed that one of the BESS's battery banks was not charging properly, at which point it was discovered that the insulation rating on a cable feeding a newly added DC-to-DC inverter, necessary for the BESS to supply its own control power, was inadequate. The DC-to-DC inverter arrived and was installed prior to this charge cycle. The lack of insulation and proximity caused a DC arc across both banks of 800-V breakers and ignited a minor electrical fire that subsequently halted testing until June 28 (start of Phase 2), after repairs were completed. It is fortunate that there were no personnel in proximity to the breakers when the arc occurred. This event underscores the importance of conducting a detailed review of any electrical modifications to the BESS that are conducted in the field to ensure that design and components are adequate for their intended purpose. In response to the arc, MRIGlobal recommended the following, which were corrected prior to Phase 2 testing:

- a. Clean up the DC breaker junction boxes of arc products.
- b. Clean up the DC cables and replace shrink tubing on the DC cables.
- c. Replace the DC terminal blocks just below the DC breakers.
- d. Replace all the small conductors in the junction boxes.
- e. Replace the capacitors in the junction boxes.
- f. Replace the DC current sensors in the junction boxes.
- g. Rerun all the tests that were done. The DC arcing might have damaged the electronic components in both the BESS and the SMS.
- h. Replace 800-V DC-to-DC converter and install cable rated for 1,200 V and use 1,200 V-rated fuses to connect the 800-V DC-to-DC converter to the 800-V buss.

Overall, S&C has a very good unit for controlling the BESS. However, there are some issues with the SMS that KCP&L and S&C should be aware of:

1. A pure third harmonic current was measured on the 13.2-kV current transformers of 3.14 amps primary. It is not obvious where the third harmonic is coming from. It is possibly from the SMS or the BESS.
2. Why is the 480-V potential transformer's secondary wired into the main board as delta? If the 480-V PTs are wired phase-to-ground and the secondary into the main computer board as delta, that introduces a 30-degree shift into the sensing and will not give correct matching to the step down 13.2-kV/480-V transformer. Is this phase shift accounted for in the control software? The voltage sensing was rewired to regulate on the 13.2-kV side and the delta connection on the main board was connected wye. When the 13.2-kV PTs out on the pole are installed and wired, the main computer board may need to be rewired to wye. MRIGlobal recommends having the S&C territory manager ask the factory to

explain why the delta connections are used and why S&C wants to regulate on the 480 buss in the SMS.

3.2 Technical Observations During the Phase 2 Testing (June 28)

Charging and discharging of the BESS began on June 28, at approximately 10:20 a.m. The weather was hot, approximately 100°F, which was beneficial to measure the elevated temperature response of the BESS as the internal battery cells were subjected to more severe cycling than normal operation and under high ambient temperatures. As anticipated, the cell temperature ran a little higher than the previous commissioning tests, up to 47°C.

The first full discharge that was attempted resulted in a trip of the system after about 16 minutes into the test. Apparently, the SEL (Schweitzer Engineering Laboratories) relay on the 13-kV feed measured a three-phase fault of about 150 amps and sent an instantaneous trip (Reference Code No. 50) to the SMS "E-STOP." This in turn tripped the three breakers in the SMS and the two DC breakers in the BESS. The fault data was downloaded from the SEL relay showing that the bank of three-phase SCR's *all fired at the same time* creating single phase instead of three-phase current. The S&C technician postulated that the Myungshin technicians may have caused a "lockup" of the computer chip in the SMS control system when they repaired the BESS by failing to disconnect them from the SMS during the repair. The S&C technician requested that S&C send a new SMS board which still had not arrived by completion of testing. During one-and-a-half subsequent cycles of charge and discharge the problem was not observed again. MRIGlobal cannot confirm that the Myungshin technicians caused the breakers to trip, but this seems like a reasonable hypothesis.

Some other problems that were found and corrected were as follows:

1. A warning signal from the BESS is interpreted as an alarm as the SMS was not programed to handle both warning and alarm messages. Therefore, warning signals would shut down the SMS choppers prematurely. As a temporary fix, the warning thresholds within the BESS control system were raised to be equal with the alarm/trip thresholds.
2. The failed cable from the 800-V DC breakers to the 800 DC-to-DC converter was replaced by higher-rated cable, 600 V versus the previous 300 V, and as an added precaution, a single conductor pair was used for each feed, positive and negative, to ensure adequate insulation and protection from arcing. The single conductor in each phase including the cable jacket should give the phase a 1,200-V capacity. Theoretically, the phase-to-ground voltage at the highest voltage should only be 395 and 456 V, resulting in some margin of safety going forward.

3.3 Organizational Observations

The Burns & McDonnell Project Manager took charge of holding the site meetings and coordination of the various groups plus writing the daily reports. The KCP&L crews gave great

MRIGlobal-2011110803-01-001_2

support and helped in every way they could. During our presence at the site, MRIGlobal did not observe Exergonix providing any sort of site support and there were no Exergonix representatives who took part in the testing or commissioning of the units during either Phase 1 or Phase 2 of testing.

Section 4. Summary of Recommendations

Based on observations from Phase 1 and Phase 2 testing events, MRIGlobal offers the following technical and organizational recommendations for KCP&L's consideration for continued testing of the BESS system or similar projects in the future.

4.1 Technical Recommendations

1. Document the detailed specifications for the desired and the current system(s) as was done on this project.
2. Acquire or establish comprehensive single line technical diagrams and connections diagrams from each equipment supplier.
 - a. S&C Electric one-line drawings need to be updated to "*as built*."
 - b. S&C Electric SMS control system one-line display also needs to be updated to "*as built*."
3. After acquiring one-line technical diagrams, prepare a complete one line diagram of the entire system and detailed interconnection prints.
4. Develop the detailed testing specifications and procedures, for the complete system, in advance of testing activities.
5. In order to provide a more complete consultation, MRIGlobal will need the meter software to read and/or interpret the data on the installed kilowatt meter. It is recommended that the following data be made available to MRIGlobal to evaluate the performance of the BESS:
 - a. In/Out kWh
 - b. In/Out kVAR
 - c. In/Out kW demand 15 or 30 minute basis
 - d. Power Factor
 - e. Harmonics to the 32nd

4.2 Organizational Recommendations

MRIGlobal has the following recommendations for KCP&L to enhance the organizational and project coordination aspects of such a project in the future.

1. To the extent possible, arrange for a project team that is 100% dedicated to the project and ensure that they have the support from other departments as necessary so that the organization as a whole has pride of ownership in the installed system.

2. Assign a project manager that can dedicate 100% of their time to the project. Select the project manager or their assistant with extensive experience in electrical distribution systems, digital relay systems, metering systems, SCADA software, and demonstrated team leading skills.

Attachment

Attachment A

Statement of Work

STANDALONE STATEMENT OF WORK FOR THE PURCHASE OF CONSULTING SERVICES

THIS STANDALONE STATEMENT OF WORK is dated May 16, 2012, by and between Great Plains Energy Services Incorporated ("GPES") and MRIGlobal ("Supplier").

A. Scope of Consulting Services

GPES's Battery Energy Storage System (BESS) will be undergoing site acceptance testing during installation and commissioning procedures at the GPES Midtown Substation for GPES's Smart Grid demonstration project. Supplier will provide oversight in the development of the acceptance testing protocols in the following areas:

1. Provide technical advisory support to GPES during the development and oversight of acceptance testing protocols.
8. *Perform or simulate all modes listed in the BESS specifications document.*
9. *Perform a full discharge cycle followed by a full charge cycle. This test shall demonstrate that the BESS's capabilities, efficiencies, response, and features are as proposed by the battery provider.*
10. *Check total harmonic distortion to verify that the BESS outputs clean power at a variety of power output levels.*

Specifically, technical advisory support will include the following tasks:

- a. Provide technical review of acceptance testing protocols and documentation developed by the battery provider and modify the protocol and supporting documentation as necessary for application to the GPES Smart Grid system.
- b. Provide onsite technical advisory support and oversight during actual acceptance testing activities in Kansas City in the mid-May to early June 2012 timeframe (estimated to require onsite presence at the project site not exceeding 5 days). The onsite presence will not include performing any tests or install/operate any test equipment.
- c. Review technical reports prepared by the battery provider for documentation of the acceptance testing results.
- d. Prepare a letter report not exceeding 5 pages in length summarizing observations during the tests conducted, review of the battery performance results obtained during the installation and commissioning process, and any special observations and recommendations regarding the potential future use of the battery.

B. Project Managers

The Project Managers for the Consulting Services related to this Statement of Work are as follows:

GPES:	Ed Hedges Phone: 816.245.3861 Email: ed.hedges@kcpl.com
Supplier:	Sayan Chakraborti Phone: 816.753.7600 Ext. 1505 Email: schakraborti@mriglobal.org

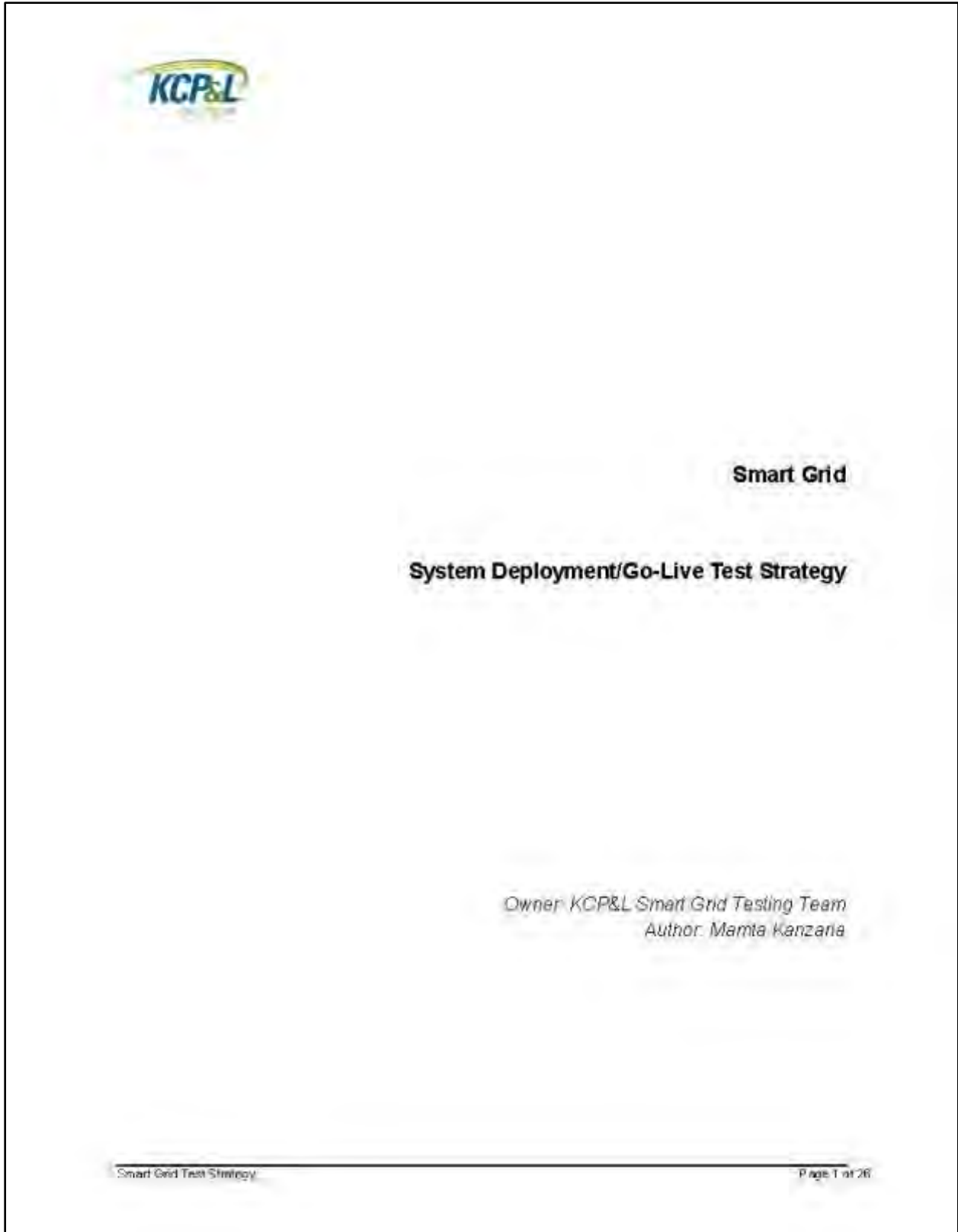
1

Att. 1

MRIGlobal-NSSI.1)0803-01-001_R

This page intentionally blank.

Appendix H System Deployment/Go-Live Test Strategy





Document History

Revision History

Revision Number	Revision Date	Summary of Changes	Author
0.1	January 5, 2012	Initial Draft	M. Kanzaria
0.2	January 12, 2012	Revised draft	M. Kanzaria
0.3	January 24, 2012	Revised draft	M. Kanzaria
1.0	January 31, 2012	Revised draft	M. Kanzaria
1.1	February 2, 2012	Revised draft with Ed's changes	M. Kanzaria
1.2	February 16, 2012	Made revisions based on conversation with Ed	M. Kanzaria
1.3	February 17, 2012	Revised draft	M. Kanzaria



Approvals

This document requires following approvals

Name	Title	Date
Ed Hedges	SmartGrid Senior SG SME	



Table of Contents

1.0	Project Introduction	5
1.1	Document Identification	6
2.0	Types of Testing	7
2.1	Test Levels	7
2.2	Functional Types of Test	9
3.0	Test Roles & Responsibilities	10
4.0	Test Control Procedures	11
4.1	Test Deliverables Reviews	11
4.2	Defect Management	11
4.3	Issue Management	11
5.0	Test Execution Criteria	12
5.1	Entry Criteria	12
5.2	Exit Criteria	13
5.3	Suspension Criteria	13
5.4	Resumption Criteria	13
6.0	Testing Deliverables	13
6.1	Test Plan	14
6.2	Test Case	14
6.3	Test Status Reports	14
6.4	Test Data	14
6.5	Test Results	14
7.0	Defect Management	15
7.1	Defect Severities	16
7.2	Defect Types	16
	Appendix – Glossary of Testing Terms	18



1.0 Project Introduction

This document represents the Testing Strategy for the Kansas City Power & Light Company (KCP&L) SmartGrid Demonstration (Demonstration Project). The KCP&L SmartGrid Demonstration Project is classified as a Regional Demonstration. For the Demonstration Project, KCP&L intends to deploy an end-to-end Smart Grid that will include advanced renewable generation, distributed energy storage resources, leading edge substation and distribution automation and control, energy management interfaces, and innovative end-use devices. The Project will focus on the area served by KCP&L's Midtown Substation, involving approximately 14,000 commercial and residential customers across twelve circuits and encompassing five square miles. This Project will be accomplished in cooperation with the Green Impact Zone of Missouri which is addressing transportation and urban revitalization in the same area through grants from the U.S. Department of Transportation and other sources.

The KCP&L SmartGrid Demonstration intends to:

- Create a complete, end-to-end Smart Grid – from smart generation to smart end-use – that will deliver improved operational performance, electricity reliability, and customer service focused on a major substation in an urban location.
- Apply new technologies, applications, protocols, communications, and business models that will be evaluated, demonstrated, and refined to achieve improved operations, increased energy efficiency, reduced energy delivery costs, and improved environmental performance.
- Demonstrate a best-in-class approach to technology integration, application development, and partnership collaboration, allowing KCP&L to advance the progression of complete smart grid solutions, employing interoperability standards, rather than single, packaged applications.
- Provide the critical energy infrastructure required to support a targeted urban revitalization effort – Kansas City's Green Impact Zone.

The Demonstration Project will introduce new technologies in the substation and the distribution network as well as advanced renewable supply resources such as large-scale energy storage to improve electricity delivery and offset peak electrical demand. Also, in conjunction with smart meters, end-users will be provided historical and actual real-time usage information, web-based energy management tools, and innovative end-use devices to allow them to optimize energy consumption.

There will be 6 project vendor partners teams involved in this effort:

Project Component	Partner
Smart Substation, Distribution Management System (DMS), ADA First Responder, Meter Data Management (MDM)	Siemens Energy, Inc.
Distributed Energy Resource Management System (DERM)	Open Access Technology, Inc. (DATI)
Automated Metering Infrastructure (AMI)	Landis+Gyr AG
Home Energy Management & Devices	Tendril, Inc.
Grid Connected Battery Storage IED	Exergonix, Inc.
Technical Project Assistance	EPR



1.1 Document Identification

This test strategy document is aimed at detailing the testing approach to support The KCP&L SmartGrid Demonstration Project. This document is a "living" document and will continuously evolve.

The integration of testing into the overall project and/or operational life cycle is a critical aspect for any real-time operational organization. The planning, managing, and execution of testing begins with efforts to define & refine the integration of it into the normal project activities.

It begins with proactively engaging a testing team (testing team being either as part of the IT organization or as defined for a given project) as early as possible allows for testing activities/planning to begin when information is first readily available. Any type of early participation from a testing team can increase not just the quality of the product/solution but reduce the number of defects/issues that can normally occur when testing is fully engaged). It is aimed at establishing a common understanding between all parties. This document serves as a means of communicating the overall testing approach in order to:

- Gain agreement and enable a coordinated effort among all stakeholders on the overall testing approach
- Demonstrate to management and other stakeholders that the approach is sound and achievable
- Define how the overall appropriate testing principles and practices will be applied in order to mitigate the project risks, manage the testing risks, and identify any exposures
- Provide a common approach and a common terminology to use for testing across the project
- Serves a foundation for future efforts, specifically test planning



2.0 Types of Testing

This section defines the types and levels of testing that will be performed across the KCP&L SmartGrid Demonstration Project. The levels correspond with different stages of development and represent known levels of physical integration and quality. The test types describe what kind of functional and structural testing will be performed.

The program will be tested in steps, in line with the build releases for each project stream, from individual units of code through integrated subsystems to the deployed releases and to the final system.

2.1 Test Levels

Testing proceeds through various physical levels of the program lifecycle. Each completed level represents a milestone on the project plan and each stage represents a known level of physical integration and quality.

At a high-level, these are the potential levels of testing that could occur within the KCP&L SmartGrid Demonstration Project:

1. **Requirements/Use Case Testing:** Requirements/use case testing involves the verification and validation of requirements through static and dynamic tests. The validation testing of requirements is covered under User Acceptance Testing.
2. **Unit Testing:** Unit level test is the initial testing of new and changed code in a module. It verifies the program specifications to the internal logic of the program or module and validates the logic. Unit testing of integration points also will be performed at this time. Unit testing is primarily performed by the vendor.
3. **System Testing:** System level tests verify proper execution of the entire application components. Both functional and structural types of tests are performed to verify that the system is functionally and operationally sound. This testing will be led by designated sub project lead.
4. **Integration Testing:** Integration level tests verify proper execution of application components. Communication between modules within the sub-system is tested in a controlled and isolated environment within the project. This testing will be primarily covered by application system testing but tracked by the Integration test lead.
5. **FAT:** Factory Acceptance Test verifies that the configured system (Hardware and Software) meets the functional requirements described in the approved design requirements. FAT will only occur for the DMS and will be performed KCP&L with the vendor observing. DERM may do some DMS related testing at this time.
6. **SAT:** Site Acceptance Test follows a similar structure as the FAT with confirmation that the system integrates properly with the field wiring and substation equipment, reconfirming the functional requirements. SAT will only occur for DMS and will be coordinated by KCP&L. DERM may do some DMS related testing at this time.
7. **User Acceptance Testing:** Acceptance tests verify that the system meets user requirements as specified. It simulates the user environment and emphasizes security, documentation and regression tests and will demonstrate that the system performs as expected to the sponsor and



end-user so that they may accept the system. This testing will be led by designated sub project lead.

8. **Interoperability Testing:** Operability tests verify that the application can operate in the production environment. Interoperability testing will be focused on end-to-end transactions based upon predefined scenarios and will be more process focused compared to integration testing. This will be led by the Integration test lead in coordination with the KCP&L SmartGrid Demonstration Project Management Office and SmartGrid Technology Planning Manager.
9. **Performance Testing:** A structural type of test which verifies that the application meets the expected level of performance in a production-like environment. This testing still needs to be defined for the Smart Grid demonstration project.
10. **Security Testing:** Testing to determine that an information system protects data and maintains functionality as intended and designated security controls are applied. This testing should take place primarily during system testing, with the VPN connection being tested during integration testing.



2.2 Functional Types of Test

The following is a list of the types of functional tests which may be included as part of testing:

Audit and Controls: Verifies the adequacy and effectiveness of controls and completeness of configuration file testing and data processing results. It is normally carried out as part of System Testing once the primary application functions have been stabilized.

Conversion: Verifies the compatibility of converted programs, data and procedures with the "old" ones that are being converted or replaced. It normally starts early in development and continues.

(User) Documentation and Procedures: Verifies that the interface between the system and the people works and is useable. It also, verifies that the instruction guides are helpful and accurate. It is normally done after the externals of the system are stabilized.

Error Handling: A functional type of test that verifies the system functions for detecting and responding to exception conditions. Completeness of error handling determines the usability of a system and ensures that errors are properly handled.

Function: Verifies that each business function operates according to the Detailed Requirements, the External and Internal Design documents. It is normally done as part of Integration, System and User Acceptance Testing.

Installation: Verifies that applications / power system components can be easily installed and run in the target environment. It is normally done for network systems, multiple location installs and vendor packages after System Testing / FAT, possibly in parallel with Business Acceptance Testing.

Interface / Inter-system: Verifies that the interconnection between applications and systems functions correctly. It is normally done as part of System Testing.

Parallel: Verifies that same input on "old" and "new" systems produces same results. It is more an implementation than a testing strategy and is normally done to compare an old application with its replacement or when automating manual systems.

Regression: Verifies that, as a result of making changes to one part of the system, unwanted changes were not introduced to other parts. It is normally done as the last part of System Testing.

Transaction Flow: Verifies the proper and complete processing of a transaction from the time it enters the system to the time of its completion or exit from the system. It is normally done in interoperability when the application is demonstrably stable.

Usability: Verifies that the final product is user-friendly and easy to use. It is normally done as part of functional testing during User Acceptance Testing.

Security: A test focus area defined as the assurance that the system/data resources will be protected against accidental and/or intentional modification or misuse.



3.0 Test Roles & Responsibilities

The following section details the typical roles & responsibilities associated with a testing effort and/or testing team. The roles & responsibilities detailed in this section are simply guidelines and can be modified accordingly.

Interoperability Test Lead

- Development of testing strategy and the management of test planning for interoperability testing efforts
- Assignment of testers to actual test functions (this will include business users, as well as the members of the Integration Testing Team within the PMO) for interoperability testing efforts
- Ensure adherence to the defined testing scope for integration testing efforts
- Management of test design by ensuring testers are collaborating with each other and the appropriate development and/or business representatives for interoperability testing efforts
- Controlling and monitoring test execution and prioritizing issues, coordinating with testers, developers, users and project managers for interoperability testing efforts
- Providing routine test status and defect tracking reports for interoperability testing efforts
- Coordinate with KCP&L IT Team to define responsibilities and ensure unified and coordinated approach to interoperability testing
- Coordinate with vendors to determine which environments will be available for interoperability testing
- Providing insight on defect and testing management tracking systems
- Provide guidance to sub-project leads for testing efforts

Sub-Project Leads

- Responsible for coordinating and managing testing efforts in assigned project areas
- Development of testing strategy and the management of test planning for respective assigned project areas
- Assignment of testers to actual test functions (this will include assigned business users, as well as the members of the Integration Testing Team within the PMO) for respective assigned project areas
- Ensure adherence to the defined testing scope for respective assigned project areas
- Management of test design by ensuring testers are collaborating with each other and the appropriate development and/or business representatives for respective assigned project areas
- Controlling and monitoring test execution and prioritizing issues, coordinating with testers, developers, users and project managers for respective assigned project areas
- Provide testing updates and defect tracking reports in their respective assigned project areas
- Tracking of issues and resolutions related to their assigned project areas
- Ensure adherence to defined testing scope in assigned project areas

Testers (Integration and Sub-project)

- Plan and document test coverage for assigned areas of test
- Execute planned testing
- Report issues and defects through defect tracking process
- Retest "fixed" defects until appropriately resolved
- Report (as scheduled) progress and issues
- Notify immediately if progress is halted due to issues/defect



4.0 Test Control Procedures

The following section describes procedures followed during the testing phases. These procedures help to monitor, evaluate, and manage the progress and effectiveness of the testing effort. They are vital to ensuring the success of the testing effort.

4.1 Test Deliverables Reviews

The respective sub project teams will perform reviews of key test deliverables for each test type (i.e. test plans, test results, etc.). A meeting notice, with related documents, will be e-mailed to each participant. These reviews should take place before testing begins to ensure agreement on testing goals and artifacts. The reviews should also be conducted following testing to verify that the tests have adequately verified system functionality.

4.2 Defect Management

A regular meeting will be held to discuss reported defects encountered during testing. The vendor development staff will provide status updates on all defects reported and the Testing team will provide additional defect information if needed. Members of the project team will participate as needed to resolve open issues.

In addition a call will be needed to review open defects with vendors. This call may be combined with the aforementioned call or held separately depending on the number of defects opened.

Each sub area lead will be responsible for managing defects and following up for resolution.

4.3 Issue Management

When issues are encountered during testing, the testers will create an issue report and will either communicate it to the appropriate lead/manager and/or log it within the appropriate defect management tool. When an issue is resolved or more information is required, the developer will change the status of the issue to indicate the current state. Once an issue is verified as resolved by the testers, the testers will close the defect.



5.0 Test Execution Criteria

The Entry and Exit Criteria describe the requirements that must be met before the system begins the testing phase and completes the testing phase, respectively. Suspend criteria describe the conditions under which the testing effort will stop temporarily. Resumption criteria are the conditions that must be met in order to resume testing following a suspension of activity. The following section provides examples for those criteria.

5.1 Entry Criteria

The system may enter the testing phase once all dependent deliverables have been met and all testing artifacts are ready for use. It will be at the discretion of the lead and/or testing manager to determine additional criteria is necessary to ensure sufficient testing coverage of the system.

Testing Type	Entry Criteria
Unit	<ul style="list-style-type: none"> • Design specifications must be completed and approved. • Unit Test Plan and respective test data are completed • Exit Criteria for Unit Testing are established and approved • Interfaces have been set up • Test data has been completed
Integration	<ul style="list-style-type: none"> • Unit Testing is successfully completed for all systems. • Integration test plan and test data are completed • Exit Criteria for Integration Testing are established and approved
User Acceptance	<ul style="list-style-type: none"> • Unit Testing complete, Integration Testing complete • Other system(s) participating in user acceptance testing have passed their own Unit Testing, and Integration Testing • User Acceptance Test Plan and test data are completed • Exit Criteria for User Acceptance Testing are established and approved
Regression	<ul style="list-style-type: none"> • Issues causing Regression Testing have been identified (if applicable) • Other system(s) participating in Regression Testing have passed their own Unit Testing • Test cases and scripts to be used for Regression Testing are identified (typically use either System/Integration Test or User Acceptance Test scripts and data) • Exit Criteria for Regression Testing are established and approved (typically use the exit criteria from the test scripts and data used to conduct Regression Testing, User Acceptance Testing or System Testing)
Performance	<ul style="list-style-type: none"> • Unit Testing and Integration Testing are complete • Other system(s) participating in performance testing have passed their own Unit Testing and Integration Testing • Performance test plan and test data are completed • Exit Criteria for Performance Testing are established and approved



5.2 Exit Criteria

The system may leave the testing phase once all testing objectives for all types of testing have been met successfully. The objectives for each type of testing will be documented in the testing deliverables. Each testing type will document testing objectives. As a guide, the following conditions must be met for any type of testing:

- The system passes the test cases without significant unresolved issues or problems.
- Any unresolved issue or problem has been documented and accepted by the business and technical leaders. In this case, the issue or problem must have a clear path to resolution.

5.3 Suspension Criteria

Testing activity will be suspended if certain criteria are encountered. Those criteria include but not limited to:

- Hardware/software/testing environment is not available at the times indicated in the project schedule.
- Source code contains one or more critical defects, which seriously prevents or drastically limits testing progress.
- Assigned test resources are not available when needed by the test team.

5.4 Resumption Criteria

If testing is suspended, resumption will only occur when the problem(s) that caused the suspension has been resolved. When a critical defect is the cause of the suspension, it must be resolved by the development, testing and/or operations staff, as applicable, before testing is resumed.

6.0 Testing Deliverables

This section provides a detailed description of the expected deliverables for testing. Unless otherwise stated, the functional business owners are (see Roles and Responsibilities section) responsible for creating and managing the deliverables for the respective testing activity. Testing templates will be provided for each of the deliverables which will be used project wide to ensure consistency among documentation.



6.1 Test Plan

A test plan defines the objectives and scope of the testing effort and identifies the methodology/approach that the tester/testing team will use to facilitate the tests. Where possible, it will also identify the hardware, software and/or tools required for testing and the features and functions that will be tested, if applicable. It will include any risks factors, a testing schedule, and responsible testers. Smart Grid vendors will be responsible for providing initial test plans to be included in testing efforts.

6.2 Test Case

A test case describes a sequence of steps using data input, action, or event and an expected response, to determine if a feature of the system is working according to the design specifications. Test cases will be driven from use cases or requirements (when available).

6.3 Test Status Reports

The respective team and/or individual will produce testing status reports as testing activity is conducted. The content of the status reports should remain focused on the testing objective, scope and scheduled milestones currently being addressed. It is useful to state each of these at the beginning of each status report and then publish the achievements or goals accomplished during the current reporting period, as well as those that will be accomplished during the next reporting period. Any known risks that will directly impact the testing effort need to be itemized here, especially any "showstoppers" that will prevent any further testing of one or more aspects of the system. Templates will be provided.

6.4 Test Data

Test data will be used during the various types of testing. Test Data must contain a reasonable sample of both valid and invalid data to be used in normal and exception conditions to adequately test the system component and/or system.

Due to the nature of this project and the number of vendors involved, vendors will need to create data and coordination of "end-to-end" test data will be required.

6.5 Test Results

Test Results will be the collection of test cases and test data used in the execution of the testing activity. These test results will be made of test cases marked with the actual testing results and include any artifact(s) used to verify successful completion of the test or error discovered during the testing.



7.0 Defect Management

During the course of testing, defects will be recorded and managed using the incident reporting/defect management tool. Currently KCP&L does not have a defect management tool, but appropriate diligence will be done to find or create one. Vendors may have their own defect management systems which will may require coordination with KCP&L's system. At a minimum, the following data will be captured for each defect reported:

Field	Description
Defect Description (Short):	Intended to be a short one sentence description of the issue.
Defect Identified By	Name of person who discovered defect
Identification Date / Time:	Date/time the defect was identified
Test Case Impacted:	Indicate the Test Case ID# for the test case that was being executed when the defect was identified; the project management team will identify and flag any dependent or downstream test cases that may be blocked or otherwise impacted by this defect.
System Impact:	List the system(s) where this defect occurred/sub process.
Estimated Severity	Severity (Critical - Low) rating based on impact as perceived by the person who discovered the defect; this may be modified by the project management team once additional impacts have been fully assessed
Assigned To:	Name of resource assigned to investigate and resolve the issue.
Defect Description (Long)	Long form description of the issue which should include a list of steps taken that led to the defect, the difference between the expected result of the test case and the actual result per the defect, any screenshots, test data being used, and any other information that will be useful for reporting, tracking, management and resolution of the defect
Steps to Reproduce	Summary of the steps necessary to reproduce this defect
Category	Defect category (will be a drop down menu)
Status	Status of defect
Add related issue	Linked defects
Due date	Date defect is expected to be resolved
Vendor Defect Management Tool#	To track defect in vendor's defect management system
Domain	Domain in Smart Grid project
Phase	Phase
Sub Project Area	Which sub project area this testing occurred in

All high/medium reported defects should be resolved prior to beginning the next phase of testing.



7.1 Defect Severities

The following defect severities serve as a guideline and can be modified accordingly.

Critical – Defects marked as Critical priority are considered showstoppers and prohibit further testing. These defects should be given highest priority. This priority should be used only for issues which affect areas which are on the required SmartGrid demonstration list.

High – Defects marked as high priority are considered high importance and prohibit further testing for functionality not listed on the required SmartGrid demonstration list. Furthermore, these defects will be given priority attention after 'Critical' defects and should be resolved promptly to ensure the integrity of the testing timeline. This will be used for non-required demonstration functionality while critical will be used for required demonstration functionality.

Medium – Defects marked as Medium priority are considered of medium importance to the testing timeline and do not prohibit further testing. Medium defects will be handled after 'Critical' and 'High' priority defects have been resolved.

Low – Defects marked as Low priority are considered of minor importance to the testing timeline and do not prohibit further testing. Low defects will be handled after all 'High' and 'Medium' defects have been resolved.

Enhancement – Defects marked as an 'Enhancement' can be delayed to a future release/iteration or not addressed at all. It can also be defined as a recommendation to be addressed in a future release/iteration.

7.2 Defect Types

The following defect types serve as a guideline and can be modified accordingly.

Training/User Error – Defect which does not require a resolution because the tester misinterpreted the requirements/design or was unfamiliar with the system functionality.

Code Defect – Defect that includes all standard application code as well as stored procedures, scripts, etc.

Database Defect/Configuration – Defect that includes problems with metadata, database schema, indexes, field characteristics, permissions, etc.

Environment Configuration – Defect that includes server permissions, application configuration on or between servers, memory configuration, corrupted build, incorrect build, etc.

Documentation – Defect in which the requirement or design specification was incorrect. Defect is resolved through a documentation change, not a code change.

Unit Testing – Defect in which should have been found during unit testing prior to delivery to UAT and/or Performance. This will be limited to evident defects agreed to by the Development and Test Managers which should have been noted in Unit Test. An example includes clicking on an O.K. button in a GUI screen and the GUI crashes or no data flowing between integrated applications.



Enhancement – Additional functionality identified during test that was not part of previously defined scope or requirements. Initially this may be considered a defect but later realized to be an enhancement.

Duplicate – Defects identified in a previous trouble ticket but not realized until after a new ticket has been opened. In this case, one ticket would be closed as a duplicate in favor of the other.

Security/Security violation – This will be used to track security-related issues.

ESB/Integration – This will be used to track issues with the ESB, etc.



Appendix – Glossary of Testing Terms

This glossary defines the testing terms used in this test strategy and the subsequent test documents.

Term	Definition
Acceptance Criteria	The definition of the results expected from the test cases used for acceptance testing. The product must meet these criteria before implementation can be approved.
Acceptance Testing	(1) Formal testing conducted to determine whether or not a system satisfies its acceptance criteria and to enable the client to determine whether or not to accept the system. (2) Formal testing conducted to enable a user, client, or other authorized entity to determine whether to accept a system or component.
Acceptance Test Plan	Describes the steps the client will use to verify that the constructed system meets the acceptance criteria. It defines the approach to be taken for acceptance testing activities. The plan identifies the items to be tested, the test objectives, the acceptance criteria, the testing to be performed, test schedules, entry/exit criteria, staff requirements, reporting requirements, evaluation criteria, and any risks requiring contingency planning.
Ad-hoc Testing	A loosely structured testing approach that allows test developers to be creative in their test selection and execution. Ad-hoc testing is targeted at known or suspected problem areas.
Audit and Controls Testing	A functional type of test that verifies the adequacy and effectiveness of controls and completeness of data processing results.
Backup and Recovery Testing	A structural type of test that verifies the capability of the application to be restarted after a failure.
Black Box Testing	Evaluation techniques that are executed without knowledge of the program's implementation. The tests are based on an analysis of the specification of the component without reference to its internal workings.
Bottom-up Testing	Approach to integration testing where the lowest level components/devices are tested first then used to facilitate the testing of higher level components. This process is repeated until the component at the top of the hierarchy is tested. See "Top-down."
Branch Testing	A white box testing technique that requires each branch or decision point to be taken once.
Build	(1) An operational version of a system or component that incorporates a specified subset of the capabilities that the final product will provide. Builds are defined whenever the complete system cannot be developed and delivered in a single increment. (2) A collection of programs within a system that are functionally independent. A build can be tested as a unit and can be installed independent of the rest of the system.
Business Function	A set of related activities that comprise a stand-alone unit of business. It may be defined as a process that results in the achievement of a business objective. It is characterized by well-defined start and finish activities and a workflow or pattern.



Term	Definition
Causal Analysis	The evaluation of the cause of major errors, to determine actions that will prevent recurrence of similar errors.
Change Control	The process, by which a change is proposed, evaluated, approved or rejected, scheduled, and tracked.
Change Management	A process methodology to identify the configuration of a release and to manage all changes through change control, data recording, and updating of baselines.
Change Request	A documented proposal for a change of one or more work items or work item parts.
Condition Testing	A white box test method that requires all decision conditions be executed once for true and once for false.
Configuration Management	(1) The process of identifying and defining the configuration items in a system, controlling the release and change of these items throughout the system life cycle, recording and reporting the status of configuration items and change requests, and verifying the completeness and correctness of configuration items. (2) A discipline applying technical and administrative direction and surveillance to (a) identify and document the functional and physical characteristics of a configuration items, (b) control changes to those characteristics, and (c) record and report change processing and implementation status.
Conversion testing	A functional type of test that verifies the compatibility of converted programs, data and procedures with the "old" ones that are being converted or replaced.
Coverage	The extent to which test data tests a program's functions, parameters, inputs, paths, branches, statements, conditions, modules or data flow paths.
Coverage Matrix	Documentation procedure to indicate the testing coverage of test cases compared to possible elements of a program environment (i.e., inputs, outputs, parameters, paths, cause-effects, equivalence partitioning, etc.)
Continuity of Processing	A test focus area defined as the ability to continue processing if problems occur. Included is the ability to backup and recover after a failure.
Correctness	A test focus area defined as the ability to process data according to prescribed rules and configuration. Controls over data flow across systems provide an assurance on accuracy and completeness.
Data flow Testing	Testing in which test cases are designed based on variable usage within the code.
Debugging	The process of locating, analyzing, and correcting suspected faults. Compare with testing.
Decision Coverage	Percentage of decision outcomes that have been exercised through (white box) testing.
Defect	A variance from expectations: (1) An accidental condition that causes a functional unit to fail to perform its required functions. (2) A manifestation of an error in software. A fault if encountered may cause a failure. Synonymous with bug.



Term	Definition
Defect Management	A set of processes to manage the tracking and fixing of defects found during testing and to perform causal analysis.
Documentation and Procedures Testing	A functional type of test that verifies that the interface between the system and the people works and is usable. It also verifies that the instruction guides are helpful and accurate.
Design Review	(1) A formal meeting at which the preliminary or detailed design of a system is presented to the user, customer or other interested parties for comment and approval. (2) The formal review of an existing or proposed design for the purpose of detection and remedy of design deficiencies that could affect fitness-for-use and environmental aspects of the product, process or service, and/or for identification of potential improvements of performance, safety and economic aspects.
Desk Check	Testing of software by the manual simulation of its execution. It is one of the static testing techniques.
Detailed Test Plan	The detailed plan for a specific level of dynamic testing. It defines what is to be tested and how it is to be tested. The plan typically identifies the items to be tested, the test objectives, the testing to be performed, test schedules, personnel requirements, reporting requirements, evaluation criteria, and any risks requiring contingency planning. It also includes the testing tools and techniques, test environment set up, entry and exit criteria, and administrative procedures and controls.
Driver	A program that exercises a system or system component by simulating the activity of a higher level component.
Dynamic Testing	Testing that is carried out by executing the code. Dynamic testing is a process of validation by exercising a work product and observing the behavior of its logic and its response to inputs.
Entry Criteria	A checklist of activities or work items that must be complete or exist, respectively, before the start of a given task within an activity or sub-activity.
Environment	See Test Environment.
Error	(1) A discrepancy between a computed, observed or measured value or condition and the true specified or theoretically correct value or condition. (2) A human action that results in software containing a fault. This includes omissions or misinterpretations, etc.
Error Guessing	A test case selection process that identifies test cases based on the knowledge and ability of the individual to anticipate probable errors.
Error Handling Testing	A functional type of test that verifies the system functions for detecting and responding to exception conditions. Completeness of error handling determines the usability of a system and ensures that errors are properly handled.
Execution Procedure	A sequence of manual or automated steps required to carry out part or all of a test design or execute a set of test cases.
Exit Criteria	(1) Actions that must happen before an activity is considered complete. (2) A checklist of activities or work items that must be complete or exist, respectively, prior to the end of a given process stage, activity, or sub-activity.




Term	Definition
Expected Results	Predicted output data and file conditions associated with a particular test case. Expected results, if achieved, will indicate whether the test was successful or not. Generated and documented with the test case prior to execution of the test.
Full Lifecycle Testing	The process of verifying the consistency, completeness, and correctness of software and related work products (such as documents and processes) at each stage of the development life cycle.
Function	(1) A specific purpose of an entity or its characteristic action. (2) A set of related control statements that perform a related operation. Functions are sub-units of modules.
Function Testing	A functional type of test, which verifies that each business function operates according to the detailed requirements, the external and internal design specifications.
Functional Testing	Selecting and executing test cases based on specified function requirements without knowledge or regard of the program structure. Also known as black box testing. See "Black Box Testing."
Functional Test Types	Those kinds of tests used to assure that the designed system meets the business requirements, including business functions, interfaces, usability, and error handling etc. See also Structural Test Types.
Implementation	(1) A realization of an abstraction in more concrete terms; in particular, in terms of hardware, software, or both (2) The process by which the Power System is commission into production (3) The process by which software release is installed in production and made available to end users
Inspection	(1) A group review quality improvement process for written material, consisting of two aspects: product (document itself) improvement and process improvement (of both document production and inspection) (3) A formal evaluation procedure in which the Power System design is inspected against as built. (2) A formal evaluation technique in which software requirements, design, or code are examined in detail by a person or group other than the author to detect faults, violations of development standards, and other problems. Contrast with walk-through.
Installation Testing	A functional type of test which verifies that the hardware, software and applications can be easily installed and run in the target environment.
Interface / Inter-system Testing	A functional type of test which verifies that the interconnection between applications and systems functions correctly.
Level of Testing	Refers to the progression of software and hardware testing through static and dynamic testing. Examples of <i>static testing</i> levels are Project Objectives Review, Requirements Walkthrough, Design (External and Internal) Review, Material and Code Inspection. Examples of <i>dynamic testing</i> levels are: Unit Testing, Development Integration Testing (DIT), Factory Acceptance testing (FAT), Site Acceptance Testing (SAT), Systems Integration Testing (SIT), User Acceptance Testing (UAT) and End to End Testing. Also known as a test level.



Term	Definition
Lifecycle	The software development process stages: Requirements, Design, Construction and Implementation.
Logical Path	A path that begins at an entry or decision statement and ends at a decision statement or exit.
Maintainability	A test focus area defined as the ability to locate and fix an error in the system. Can also be the ability to make dynamic changes to the system environment without making system changes.
Operability	A test focus area defined as the effort required (of support personnel) to learn and operate a manual or automated system. Contrast with Usability.
Operability Testing	A level of dynamic testing in which the operations of the system are validated in the real or closely simulated production environment.
Operational Testing	A structural type of test that verifies the ability of the power systems / applications to operate at an acceptable level of service in the production-like environment.
Parallel Testing	A functional type of test, which verifies that the same input on "old" and "new" systems, produces the same results. It is more of an implementation than a testing strategy.
Performance	A test focus area defined as the ability of the system to perform certain functions within a prescribed time.
Performance Testing	A structural type of test which verifies that the application meets the expected level of performance in a production-like environment.
Portability	A test focus area defined as ability for a system to operate in multiple operating environments.
Regression Testing	A functional type of test, which verifies that changes to one part of the system have not caused unintended adverse effects to other parts.
Reliability	A test focus area defined as the extent to which the system will provide the intended function without failing.
Requirement	(1) A condition or capability needed by the user to solve a problem or achieve an objective. (2) A condition or capability that must be met or possessed by a system or system component to satisfy a contract, standard, specification, or other formally imposed document. The set of all requirements forms the basis for subsequent development of the system or system component.
Review	A process or meeting during which a work product, or set of work products, is presented to project personnel, managers, users or other interested parties for comment or approval.
Root Cause Analysis	See Causal Analysis.
Security	A test focus area defined as the assurance that the system/data resources will be protected against accidental and/or intentional modification or misuse.



Term	Definition
Security Testing	A structural type of test which verifies that the application provides an adequate level of protection for confidential information and data belonging to other systems.
Software Quality	(1) The totality of features and characteristics of a software product that bear on its ability to satisfy given needs; for example, conform to specifications. (2) The degree to which software possesses a desired combination of attributes. (3) The degree to which a customer or user perceives that software meets his or her composite expectations. (4) The composite characteristics of software that determine the degree to which the software in use will meet the expectations of the customer.
Software Reliability	(1) The probability that software will not cause the failure of a system for a specified time under specified conditions. The probability is a function of the inputs to and use of the system as well as a function of the existence of faults in the software. The inputs to the system determine whether existing faults, if any, are encountered. (2) The ability of a program to perform a required function under stated conditions for a stated period of time.
Statement Testing	A white box testing technique that requires all code or logic statements to be executed at least once.
Static Testing	(1) The detailed examination of a work product's characteristics to an expected set of attributes, experiences and standards. The product under scrutiny is static and not exercised and therefore its behavior to changing inputs and environments cannot be assessed. (2) The process of evaluating a program without executing the program. See also desk checking, inspection, walk-through.
Stress / Volume Testing	A structural type of test that verifies that the power system / application has acceptable performance characteristics under peak load conditions.
Structural Function	Structural functions describe the technical attributes of a system.
Structural Test Types	Those kinds of tests that may be used to assure that the system is technically sound.
Sub-system	(1) A group of assemblies or components or both combined to perform a single function. (2) A group of functionally related components that are defined as elements of a system but not separately packaged.
System	A collection of components organized to accomplish a specific function or set of functions.
Systems Integration Testing	A dynamic level of testing which ensures that the systems integration activities appropriately address the integration of application subsystems, integration of applications with the infrastructure, and impact of change on the current live environment.
System Testing	A dynamic level of testing in which all the components that comprise a system are tested to verify that the system functions together as a whole.



Term	Definition
Test Bed	(1) A test environment containing the hardware, instrumentation tools, simulators, and other support software necessary for testing a system or system component. (2) A set of test files, (including databases and reference files), in a known state, used with input test data to test one or more test conditions, measuring against expected results.
Test Case	(1) A set of test inputs, execution conditions, and expected results developed for a particular objective, such as to exercise a particular program path or to verify compliance with a specific requirement. (2) The detailed objectives, data, procedures and expected results to conduct a test or part of a test.
Test Condition	A functional or structural attribute of an application, system, network, or component thereof to be tested.
Test Conditions Matrix	A worksheet used to formulate the test conditions that, if met, will produce the expected result. It is a tool used to assist in the design of test cases.
Test Conditions Coverage Matrix	A worksheet that is used for planning and for illustrating that all test conditions are covered by one or more test cases. Each test set has a Test Conditions Coverage Matrix. Rows are used to list the test conditions and columns are used to list all test cases in the test set.
Test Coverage Matrix	A worksheet used to plan and cross check to ensure all requirements and functions are covered adequately by test cases.
Test Data	The input data and file conditions associated with a specific test case.
Test Environment	The external conditions or factors that can directly or indirectly influence the execution and results of a test. This includes the physical as well as the operational environments. Examples of what is included in a test environment are: I/O and storage devices, data files, programs, JCL, communication lines, access control and security, databases, reference tables and files (version controlled), etc.
Test Focus Areas	Those attributes of an application/components that must be tested in order to assure that the business and structural requirements are satisfied
Test Level	See Level of Testing.
Test Log	A chronological record of all relevant details of a testing activity.
Test Matrices	A collection of tables and matrices used to relate functions to be tested with the test cases that do so. Worksheets used to assist in the design and verification of test cases.
Test Objectives	The tangible goals for assuring that the Test Focus areas previously selected as being relevant to a particular Business or Structural Function are being validated by the test.
Test Plan	A document prescribing the approach to be taken for intended testing activities. The plan typically identifies the items to be tested, the test objectives, the testing to be performed, test schedules, entry / exit criteria, personnel requirements, reporting requirements, evaluation criteria, and any risks requiring contingency planning.
Test Procedure	Detailed instructions for the setup, operation, and evaluation of results for a given test. A set of associated procedures is often combined to form a test procedures document.



Term	Definition
Test Report	A document describing the conduct and results of the testing carried out for a system or system component.
Test Run	A dated, time-stamped execution of a set of test cases.
Test Scenario	A high-level description of how a given business or technical requirement will be tested, including the expected outcome; later decomposed into sets of test conditions, each in turn, containing test cases.
Test Script	A sequence of actions that executes a test case. Test scripts include detailed instructions for set up, execution, and evaluation of results for a given test case.
Test Set	A collection of test conditions. Test sets are created for purposes of test execution only. A test set is created such that its size is manageable to run and its grouping of test conditions facilitates testing. The grouping reflects the application build strategy.
Test Sets Matrix	A worksheet that relates the test conditions to the test set in which the condition is to be tested. Rows list the test conditions and columns list the test sets. A checkmark in a cell indicates the test set will be used for the corresponding test condition.
Test Strategy	A high level description of major system-wide activities which collectively achieve the overall desired result as expressed by the testing objectives, given the constraints of time and money and the target level of quality. It outlines the approach to be used to ensure that the critical attributes of the system are tested adequately.
Test Type	See Type of Testing.
Testing	The process of exercising or evaluating a program, product, or system, by manual or automated means, to verify that it satisfies specified requirements, to identify differences between expected and actual results.
Top-down	Approach to integration testing where the component at the top of the component hierarchy is tested first, with lower level components being simulated by stubs. Tested components are then used to test lower level components. The process is repeated until the lowest level components have been tested.
Transaction Flow Testing	A functional type of test that verifies the proper and complete processing of a transaction from the time it enters the system to the time of its completion or exit from the system.
Unit Testing	The first level of dynamic testing and is the verification of new or changed code in a module to determine whether all new or modified paths function correctly.
Usability	A test focus area defined as the end-user effort required to learn and use the system. Contrast with Operability.
Usability Testing	A functional type of test which verifies that the final product is user-friendly and easy to use.
User Acceptance Testing	See Acceptance Testing.



Term	Definition
Validation	(1) The act of demonstrating that a work item is in compliance with the original requirement. For example, the code of a module would be validated against the input requirements it is intended to implement. Validation answers the question "Is the right system being built?" (2) Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use have been fulfilled. See "Verification".
Variance	A mismatch between the actual and expected results occurring in testing. It may result from errors in the item being tested, incorrect expected results, invalid test data, etc. See "Error".
Verification	(1) The act of demonstrating that a work item is satisfactory by using its predecessor work item. For example, the system is verified against module level design. Verification answers the question "Is the system being built right?" (2) Confirmation by examination and provision of objective evidence that specified requirements have been fulfilled. See "Validation."
Walkthrough	A review technique characterized by the author of the object under review guiding the progression of the review. Observations made in the review are documented and addressed. Less formal evaluation technique than an inspection.
White Box Testing	Evaluation techniques that are executed with the knowledge of the implementation of the components and programs. The objective of white box testing is to test the components/program's statements, configuration files, code paths, conditions, or data flow paths.
Work Item	A software development lifecycle work product.

Appendix I Test Plan Workbooks

I.1	System Test Book	I-3
	I.1.1 HMI.FAT	I-3
	I.1.2 HMI.SAT	I-17
	I.1.3 SICAM.FAT.....	I-19
	I.1.4 SICAM.SAT.....	I-29
	I.1.5 DCADA.P3FAT.....	I-33
	I.1.6 DCADA.P3SAT.....	I-35
	I.1.7 DMS.P1FAT.....	I-37
	I.1.8 DMS.P1SAT.P2P.SUB	I-38
	I.1.9 DMS.P2FAT.REDUNDANCY.....	I-51
	I.1.10 DMS.P2FAT.UI	I-56
	I.1.11 DMS.P2SAT.P2P.CB	I-59
	I.1.12 DMS.P2SAT.P2P.FCI.....	I-64
	I.1.13 DMS.P2SAT.REDUNDANCY.....	I-67
	I.1.14 DMS.P2SAT.UI	I-72
	I.1.15 DMS.P3FAT.651R	I-75
	I.1.16 DMS.P3FAT.CDNA	I-80
	I.1.17 DMS.P3FAT.RTAC (BATTERY).....	I-93
	I.1.18 DMS.P3SAT.CDNA	I-97
	I.1.19 DMS.P3SAT.P2P.651R	I-102
	I.1.20 HIS.P3SAT	I-107
	I.1.21 DERM	I-109
	I.1.22 MDM	I-115
	I.1.23 AHE (Core).....	I-117
	I.1.24 AHE (Meter Test).....	I-120
	I.1.25 HEMP	I-122
	I.1.26 HAN	I-124
	I.1.27 HAN (Additional Tests).....	I-125
I.2	Integration Test Book.....	I-131
	I.2.1 DMS-DERM (Joint Vendor Testing)	I-131
	I.2.2 DMS-DERM (DERM Focus)	I-139
	I.2.3 OMS-MDM (Outage Restoration Event).....	I-140
	I.2.4 OMS-MDM (Outage Restoration – Flex Sync)	I-142
	I.2.5 OMS-MDM (Power Status Verification)	I-143
	I.2.6 DERM-HEMP (DERM Focus)	I-146
	I.2.7 AHE-MDM (L+G Adapter)	I-149
	I.2.8 AHE-MDM (MDM VPN)	I-153
	I.2.9 AHE-MDM (MTR Content – System Side Processing).....	I-157
	I.2.10 AHE-MDM (ESB Processing)	I-158
	I.2.11 AHE-MDM (Outage Restoration Event).....	I-161
	I.2.12 AHE-MDM (Outage Restoration – Flex Sync)	I-163
	I.2.13 AHE-MDM (Power Status Verification)	I-164
	I.2.14 MDM-CIS (Aggregation)	I-167
	I.2.15 MDM-CIS (RSO Detail).....	I-168
	I.2.16 MDM-CIS (RSO E2E)	I-169
	I.2.17 MDM-CIS (RSO Online GUI).....	I-178
	I.2.18 MDM-CIS (RSO Web Services).....	I-179
	I.2.19 MDM-CIS (L+G Adapter).....	I-180
	I.2.20 MDM-CIS (MDM VPN).....	I-184
	I.2.21 MDM-CIS (Outage Restoration Event)	I-188
	I.2.22 MDM-CIS (Power Status Verification)	I-190
	I.2.23 HEMP-AHE (Network & Device Comms)	I-193

This page intentionally blank.

System Test Book - HMI FAT: Document Verification Checklist						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT001:1	Verify that the single line diagram is provided during the FAT.	N/A				
SYS.HMI.FAT001:2	Verify that the functional design specification is provided during the FAT.	N/A				
SYS.HMI.FAT001:3	Verify that the network architecture is provided during the FAT.	N/A				
SYS.HMI.FAT001:4	Verify that the network architecture of test system is provided during the FAT.	N/A				
SYS.HMI.FAT001:5	Verify that the system configuration description is provided during the FAT.	N/A				
SYS.HMI.FAT001:6	Verify that the signal is provided during the FAT.	N/A				
System Test Book - HMI FAT: Equipment Hardware Checklist						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT002:1	Verify that two SICAM PAS Station Units 2.20 are provided during the FAT.	N/A				
SYS.HMI.FAT002:2	Verify that one SEL 487B is provided during the FAT.	N/A				
SYS.HMI.FAT002:3	Verify that one SEL 487E is provided during the FAT.	N/A				
SYS.HMI.FAT002:4	Verify that one SEL 451 is provided during the FAT.	N/A				
SYS.HMI.FAT002:5	Verify that one SEL 751A is provided during the FAT.	N/A				
SYS.HMI.FAT002:6	Verify that one Arbiter GPS Clock is provided during the FAT.	N/A				
SYS.HMI.FAT002:7	Verify that one RSG2100 RuggedCom Ethernet Switch is provided during the FAT.	N/A				
SYS.HMI.FAT002:8	Verify that one Cisco Ethernet Switch is provided during the FAT.	N/A				
SYS.HMI.FAT002:9	Verify that one A-Eberle Tap Changer is provided during the FAT.	N/A				
SYS.HMI.FAT002:10	Verify that two HMI Servers are provided during the FAT.	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT002:11	Verify that two HMI Clients are provided during the FAT.	N/A				
System Test Book - HMI FAT: Equipment Software Checklist						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT003:1.1	Verify that the SICAM PAS Station Unit has Windows XP Embedded OS SP3 .	N/A				
SYS.HMI.FAT003:1.2.1	Verify that the SICAM PAS Station Unit has the SICAM PAS V7.01 Runtime & Configuration Dongle.	N/A				
SYS.HMI.FAT003:1.2.2	Verify that the SICAM PAS Station Unit has PAS Runtime.	N/A				
SYS.HMI.FAT003:1.2.3	Verify that the SICAM PAS Station Unit has PAS UI Large.	N/A				
SYS.HMI.FAT003:1.2.4	Verify that the SICAM PAS Station Unit has IEC61850 Client.	N/A				
SYS.HMI.FAT003:1.2.5	Verify that the SICAM PAS Station Unit has DNP3.0 MASTER.	N/A				
SYS.HMI.FAT003:1.2.6	Verify that the SICAM PAS Station Unit has DNP3.0 SLAVE.	N/A				
SYS.HMI.FAT003:1.2.7	Verify that the SICAM PAS Station Unit has AUTOMATION.	N/A				
SYS.HMI.FAT003:1.2.8	Verify that the SICAM PAS Station Unit has IEC61850 Server.	N/A				
SYS.HMI.FAT003:2.1	Verify that the SIMATIC RACK PC has Windows 2008 Server Standard installed.	N/A				
SYS.HMI.FAT003:2.2.1	Verify that the SIMATIC RACK PC has WinCC redundancy V7.0 installed.	N/A				
SYS.HMI.FAT003:2.2.2	Verify that the SIMATIC RACK PC has WinCC Server V7.0 installed.	N/A				
SYS.HMI.FAT003:2.2.3	Verify that the SIMATIC RACK PC has WinCC Runtime and Configuration (2048 tags) installed.	N/A				
SYS.HMI.FAT003:2.2.4	Verify that the SIMATIC RACK PC has WinCC Runtime (2048 tags) V7.0 installed.	N/A				
SYS.HMI.FAT003:2.2.5	Verify that the SIMATIC RACK PC has WinCC Runtime (128 tags) V7.0 installed.	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT003:2.2.6	Verify that the SIMATIC RACK PC has SICAM SCC upgrade Runtime and Configuration V7.01 installed.	N/A				
SYS.HMI.FAT003:2.2.7	Verify that the SIMATIC RACK PC has SICAM SCC upgrade Runtime V7.01 installed.	N/A				
System Test Book - HMI FAT: Redundancy & Self Healing at HMI Level						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT024:1	Verify that HMI-A and HMI-B are connected to the assigned Master Station Unit.	N/A				
SYS.HMI.FAT024:2	Simulate HMI-A failure by switching off the power supply.	Verify that communication to HMI-A is lost, and that HMI-B is still working and communicating to the station unit.				
SYS.HMI.FAT024:3	Return power to HMI-A by switching on the power supply.	Verify that HMI-A connects to the Master Station Unit.				
SYS.HMI.FAT024:4	Simulate HMI-B failure by switching off the power supply.	Verify that communication to HMI-B is lost, and that HMI-A is still working and communicating to the station unit.				
SYS.HMI.FAT024:5	Return power to HMI-B by switching on the power supply.	Verify that HMI-B connects to the Master Station Unit.				
SYS.HMI.FAT024:6	Disconnect one of the LAN cables connected to HMI-A.	Verify that the HMI is still in service and communicating to the Station server, and that there is no change in the Master standby assignment.				
System Test Book - HMI FAT: Communication Test						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT005:1.1	Ping the SEL 487E from HMI-A.	Verify ping is successful.				
SYS.HMI.FAT005:1.2	Ping the SEL 487B from HMI-A.	Verify ping is successful.				
SYS.HMI.FAT005:1.3	Ping the SEL 451-5 from HMI-A.	Verify ping is successful.				
SYS.HMI.FAT005:1.4	Ping the SEL 751A from HMI-A.	Verify ping is successful.				
SYS.HMI.FAT005:1.5	Ping the A-Eberle Tap Changer from HMI-A.	Verify ping is successful.				
SYS.HMI.FAT005:1.6	Ping the Station unit-1 from HMI-A.	Verify ping is successful.				
SYS.HMI.FAT005:1.7	Ping the Station unit-2 from HMI-A.	Verify ping is successful.				
SYS.HMI.FAT005:1.8	Ping the SEL 487E from HMI-B.	Verify ping is successful.				
SYS.HMI.FAT005:1.9	Ping the SEL 487B from HMI-B.	Verify ping is successful.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT005:1.10	Ping the SEL 451-5 from HMI-B.	Verify ping is successful.				
SYS.HMI.FAT005:1.11	Ping the SEL 751A from HMI-B.	Verify ping is successful.				
SYS.HMI.FAT005:1.12	Ping the A-Eberle Tap Changer from HMI-B.	Verify ping is successful.				
SYS.HMI.FAT005:1.13	Ping the Station unit-1 from HMI-B.	Verify ping is successful.				
SYS.HMI.FAT005:1.14	Ping the Station unit-2 from HMI-B.	Verify ping is successful.				
SYS.HMI.FAT005:2.1	Disconnect both network connections from HMI-A.	Verify that HMI-A is now pending up in SICAM PAS UI Operation.				
SYS.HMI.FAT005:2.2	Disconnect both network connections from HMI-B.	Verify that HMI-B is now pending up in SICAM PAS UI Operation.				
SYS.HMI.FAT005:3.1	Reconnect both network connections to HMI-A.	Verify that the connection to HMI-A is established and that HMI-A is now displayed as running in SICAM PAS UI Operation.				
SYS.HMI.FAT005:3.2	Reconnect both network connections to HMI-B.	Verify that the connection to HMI-B is established and that HMI-B is now displayed as running in SICAM PAS UI Operation.				
SYS.HMI.FAT005:4.1	Disconnect and then reconnect a network port from the Ruggedcom network switch.	Verify that the port goes down and then back up on both HMI-A and HMI-B.				
SYS.HMI.FAT005:4.2	Disconnect and then reconnect a network port from the Cisco network switch.	Verify that the port goes down and then back up on both HMI-A and HMI-B.				
System Test Book - HMI FAT: Time synchronization						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT006:1.1	Drift the time by five minutes on the HMI-A.	Verify that HMI-A resyncs with the GPS clock in 15-20 minutes time.				
SYS.HMI.FAT006:1.2	Drift the time by five minutes on the HMI-B.	Verify that HMI-B resyncs with the GPS clock in 15-20 minutes time.				
SYS.HMI.FAT006:1.3	Drift the time by five minutes on the HMI-C.	Verify that HMI-C resyncs with the GPS clock in 15-20 minutes time.				
SYS.HMI.FAT006:1.4	Drift the time by five minutes on the HMI-D.	Verify that HMI-D resyncs with the GPS clock in 15-20 minutes time.				
System Test Book - HMI FAT: One-Line Screen						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT007:1.1	Verify that the header of the screen is labeled as "Single line view".	N/A				
SYS.HMI.FAT007:1.2	Verify the naming conventions in the screen are as per the approved HMI screenshots.	N/A				
SYS.HMI.FAT007:1.3	Verify the information present in the screen are as per the approved HMI screenshots.	N/A				
SYS.HMI.FAT007:2.1	Simulate the binary indication to simulate breaker open/close from the SEL 487E relay.	Verify the change in the breaker status on the HMI as mentioned in the approved FDS.				
SYS.HMI.FAT007:2.2	From the A-Eberle Tap Changer simulate the Auto/Manual status.	Verify the text in the status box correspondingly changes on the HMI.				
SYS.HMI.FAT007:2.3	Increment the tap-position from the tap changer.	Verify the corresponding tap-position is being indicated on the screen.				
SYS.HMI.FAT007:3.1	Inject three phase voltage and current in SEL-487E relay in order to simulate active power and reactive power.	Verify the readings in the HMI screen matches with the front-panel display of the relay.				
SYS.HMI.FAT007:4.1	Operate a breaker on the HMI screen.	Verify the command is successfully passed to the relay.				
SYS.HMI.FAT007:4.2	Simulate the feedback from a successful breaker operation.	Verify the breaker status is updated on the HMI.				
SYS.HMI.FAT007:4.3	Verify that the command is recorded in the event list.	N/A				
System Test Book - HMI FAT: Bus Detail Screen						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT008:1.1	Verify that the header of the screen is labelled as per the approved HMI screenshots.	N/A				
SYS.HMI.FAT008:1.2	Verify the naming conventions in the screen are as per the approved HMI screenshots.	N/A				
SYS.HMI.FAT008:1.3	Verify the information present in the screen are as per the approved HMI screenshots.	N/A				
SYS.HMI.FAT008:2.1	Simulate the binary indication to simulate breaker open/close from the SEL 751A relay.	Verify the change in the breaker status in the HMI as mentioned in the approved FDS.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT008:2.2	Simulate the local/remote from the SEL-751A by energizing the corresponding binary input.	Verify there is a corresponding change in the status box in the HMI screen.				
SYS.HMI.FAT008:2.3	Simulate the auto/manual from the SEL-751A by energizing the corresponding binary input.	Verify there is a corresponding change in the status box in the HMI screen.				
SYS.HMI.FAT008:2.4	Simulate the local/remote from the SEL-451 by energizing the corresponding binary input.	Verify there is a corresponding change in the status box in the HMI screen.				
SYS.HMI.FAT008:2.5	Verify all the tested signals are recorded in the event list and/or alarm list.	N/A				
SYS.HMI.FAT008:3.1	Inject three phase voltage and current in SEL 751A relay in order to simulate few analog measurements.	Verify the readings in the HMI screen matches with the frontpanel display of the relay.				
SYS.HMI.FAT008:3.2	Inject three phase voltage and current in SEL 487E relay in order to simulate few analog measurements.	Verify the readings in the HMI screen matches with the front-panel display of the relay.				
SYS.HMI.FAT008:4.1	Operate a breaker on the HMI screen.	Verify the command is successfully passed to the relay.				
SYS.HMI.FAT008:4.2	Simulate the feedback from a successful breaker operation.	Verify the breaker status is updated on the HMI.				
SYS.HMI.FAT008:4.3	Verify that the command is recorded in the event list.	N/A				
System Test Book - HMI FAT: Network Overview Screen						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT009:1.1	Unplug any fiber-optic connection between two switches in the ring to simulate a failure.	Verify the corresponding line depicting the network cable starts blinking in the HMI for Ruggedcom.				
SYS.HMI.FAT009:1.2	Unplug any fiber-optic connection between two switches in the ring to simulate a failure.	Verify that the Ruggedcom switch starts blinking due to faulty connection detected in one of its ports.				
SYS.HMI.FAT009:1.3	Click on the push button to verify the status of the port being disconnected in the port assignment table.	Verify the corresponding message is also being reported in the Event and Alarm list for the Ruggedcom switch.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT009:1.4	Plug the network cable back into the port.	Verify blinking in the corresponding line depicting the network cable stops for the Ruggedcom switch.				
SYS.HMI.FAT009:1.5	Unplug the fiber-optic connection on the SEL 751A to simulate a failure.	Verify the corresponding line depicting the network cable starts blinking in the HMI for the Ruggedcom switch.				
SYS.HMI.FAT009:1.5	Unplug any fiber-optic connection on the SEL 751A to simulate a failure.	Verify that the Ruggedcom switch starts blinking due to faulty connection detected in one of its ports.				
SYS.HMI.FAT009:1.5	Click on the push button to verify the status of the port being disconnected in the port assignment table.	Verify the corresponding message is also being reported in the Event and Alarm list for the Ruggedcom switch.				
SYS.HMI.FAT009:1.5	Plug the network cable back into the port.	Verify blinking in the corresponding line depicting the network cable stops for the Ruggedcom switch.				
SYS.HMI.FAT009:1.6	Unplug the fiber-optic connection on the SEL 487B to simulate a failure.	Verify the corresponding line depicting the network cable starts blinking in the HMI for the Ruggedcom switch.				
SYS.HMI.FAT009:1.6	Unplug any fiber-optic connection on the SEL 487B to simulate a failure.	Verify that the Ruggedcom switch starts blinking due to faulty connection detected in one of its ports.				
SYS.HMI.FAT009:1.6	Click on the push button to verify the status of the port being disconnected in the port assignment table.	Verify the corresponding message is also being reported in the Event and Alarm list for the Ruggedcom switch.				
SYS.HMI.FAT009:1.6	Plug the network cable back into the port.	Verify blinking in the corresponding line depicting the network cable stops for the Ruggedcom switch.				
SYS.HMI.FAT009:1.7	Unplug the fiber-optic connection on the SEL 487E to simulate a failure.	Verify the corresponding line depicting the network cable starts blinking in the HMI for the Ruggedcom switch.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT009:1.7	Unplug any fiber-optic connection on the SEL 487E to simulate a failure.	Verify that the Ruggedcom switch starts blinking due to faulty connection detected in one of its ports.				
SYS.HMI.FAT009:1.7	Click on the push button to verify the status of the port being disconnected in the port assignment table.	Verify the corresponding message is also being reported in the Event and Alarm list for the Ruggedcom switch.				
SYS.HMI.FAT009:1.7	Plug the network cable back into the port.	Verify blinking in the corresponding line depicting the network cable stops for the Ruggedcom switch.				
SYS.HMI.FAT009:1.8	Unplug the fiber-optic connection on the SEL 451 to simulate a failure.	Verify the corresponding line depicting the network cable starts blinking in the HMI for the Ruggedcom switch.				
SYS.HMI.FAT009:1.8	Unplug any fiber-optic connection on the SEL 451 to simulate a failure.	Verify that the Ruggedcom switch starts blinking due to faulty connection detected in one of its ports.				
SYS.HMI.FAT009:1.8	Click on the push button to verify the status of the port being disconnected in the port assignment table.	Verify the corresponding message is also being reported in the Event and Alarm list for the Ruggedcom switch.				
SYS.HMI.FAT009:1.8	Plug the network cable back into the port.	Verify blinking in the corresponding line depicting the network cable stops for the Ruggedcom switch.				
SYS.HMI.FAT009:1.9	Unplug the fiber-optic connection on the REG-DA to simulate a failure.	Verify the corresponding line depicting the network cable starts blinking in the HMI for the Ruggedcom switch.				
SYS.HMI.FAT009:1.9	Unplug any fiber-optic connection on the REG-DA to simulate a failure.	Verify that the Ruggedcom switch starts blinking due to faulty connection detected in one of its ports.				
SYS.HMI.FAT009:1.9	Click on the push button to verify the status of the port being disconnected in the port assignment table.	Verify the corresponding message is also being reported in the Event and Alarm list for the Ruggedcom switch.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT009:1.9	Plug the network cable back into the port.	Verify blinking in the corresponding line depicting the network cable stops for the Ruggedcom switch.				
SYS.HMI.FAT009:2.1	Unplug any fiber-optic connection between two switches in the ring to simulate a failure.	Verify the corresponding line depicting the network cable starts blinking in the HMI for Cisco.				
SYS.HMI.FAT009:2.2	Unplug any fiber-optic connection between two switches in the ring to simulate a failure.	Verify that the Cisco switch starts blinking due to faulty connection detected in one of its ports.				
SYS.HMI.FAT009:2.3	Click on the push button to verify the status of the port being disconnected in the port assignment table.	Verify the corresponding message is also being reported in the Event and Alarm list for the Cisco switch.				
SYS.HMI.FAT009:2.4	Plug the network cable back into the port.	Verify blinking in the corresponding line depicting the network cable stops for the Cisco switch.				
SYS.HMI.FAT009:2.5	Unplug the fiber-optic connection on the SEL 751A to simulate a failure.	Verify the corresponding line depicting the network cable starts blinking in the HMI for the Cisco switch.				
SYS.HMI.FAT009:2.5	Unplug any fiber-optic connection on the SEL 751A to simulate a failure.	Verify that the Cisco switch starts blinking due to faulty connection detected in one of its ports.				
SYS.HMI.FAT009:2.5	Click on the push button to verify the status of the port being disconnected in the port assignment table.	Verify the corresponding message is also being reported in the Event and Alarm list for the Cisco switch.				
SYS.HMI.FAT009:2.5	Plug the network cable back into the port.	Verify blinking in the corresponding line depicting the network cable stops for the Cisco switch.				
SYS.HMI.FAT009:2.6	Unplug the fiber-optic connection on the SEL 487B to simulate a failure.	Verify the corresponding line depicting the network cable starts blinking in the HMI for the Cisco switch.				
SYS.HMI.FAT009:2.6	Unplug any fiber-optic connection on the SEL 487B to simulate a failure.	Verify that the Cisco switch starts blinking due to faulty connection detected in one of its ports.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT009:2.6	Click on the push button to verify the status of the port being disconnected in the port assignment table.	Verify the corresponding message is also being reported in the Event and Alarm list for the Cisco switch.				
SYS.HMI.FAT009:2.6	Plug the network cable back into the port.	Verify blinking in the corresponding line depicting the network cable stops for the Cisco switch.				
SYS.HMI.FAT009:2.7	Unplug the fiber-optic connection on the SEL 487E to simulate a failure.	Verify the corresponding line depicting the network cable starts blinking in the HMI for the Cisco switch.				
SYS.HMI.FAT009:2.7	Unplug any fiber-optic connection on the SEL 487E to simulate a failure.	Verify that the Cisco switch starts blinking due to faulty connection detected in one of its ports.				
SYS.HMI.FAT009:2.7	Click on the push button to verify the status of the port being disconnected in the port assignment table.	Verify the corresponding message is also being reported in the Event and Alarm list for the Cisco switch.				
SYS.HMI.FAT009:2.7	Plug the network cable back into the port.	Verify blinking in the corresponding line depicting the network cable stops for the Cisco switch.				
SYS.HMI.FAT009:2.8	Unplug the fiber-optic connection on the SEL 451 to simulate a failure.	Verify the corresponding line depicting the network cable starts blinking in the HMI for the Cisco switch.				
SYS.HMI.FAT009:2.8	Unplug any fiber-optic connection on the SEL 451 to simulate a failure.	Verify that the Cisco switch starts blinking due to faulty connection detected in one of its ports.				
SYS.HMI.FAT009:2.8	Click on the push button to verify the status of the port being disconnected in the port assignment table.	Verify the corresponding message is also being reported in the Event and Alarm list for the Cisco switch.				
SYS.HMI.FAT009:2.8	Plug the network cable back into the port.	Verify blinking in the corresponding line depicting the network cable stops for the Cisco switch.				
SYS.HMI.FAT009:2.9	Unplug the fiber-optic connection on the REG-DA to simulate a failure.	Verify the corresponding line depicting the network cable starts blinking in the HMI for the Cisco switch.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT009:2.9	Unplug any fiber-optic connection on the REG-DA to simulate a failure.	Verify that the Cisco switch starts blinking due to faulty connection detected in one of its ports.				
SYS.HMI.FAT009:2.9	Click on the push button to verify the status of the port being disconnected in the port assignment table.	Verify the corresponding message is also being reported in the Event and Alarm list for the Cisco switch.				
SYS.HMI.FAT009:2.9	Plug the network cable back into the port.	Verify blinking in the corresponding line depicting the network cable stops for the Cisco switch.				
System Test Book - HMI FAT: Device Diagnostic Screen						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT010:1	Turn-off the power supply to the SEL 451.	Verify that the status text for the device shows "Faulty".				
SYS.HMI.FAT010:1	Turn-on the power supply to the SEL 451.	Verify that the status text for the device shows "Normal".				
SYS.HMI.FAT010:2	Turn-off the power supply to the SEL 487B.	Verify that the status text for the device shows "Faulty".				
SYS.HMI.FAT010:2	Turn-on the power supply to the SEL 487B.	Verify that the status text for the device shows "Normal".				
SYS.HMI.FAT010:3	Turn-off the power supply to the SEL 751A.	Verify that the status text for the device shows "Faulty".				
SYS.HMI.FAT010:3	Turn-on the power supply to the SEL 751A.	Verify that the status text for the device shows "Normal".				
SYS.HMI.FAT010:4	Turn-off the power supply to the SEL 487E.	Verify that the status text for the device shows "Faulty".				
SYS.HMI.FAT010:4	Turn-on the power supply to the SEL 487E.	Verify that the status text for the device shows "Normal".				
SYS.HMI.FAT010:5	Turn-off the power supply to the RSG2100.	Verify that the status text for the device shows "Faulty".				
SYS.HMI.FAT010:5	Turn-on the power supply to the RSG2100.	Verify that the status text for the device shows "Normal".				
SYS.HMI.FAT010:6	Turn-off the power supply to the CSG2520.	Verify that the status text for the device shows "Faulty".				
SYS.HMI.FAT010:6	Turn-on the power supply to the CSG2520.	Verify that the status text for the device shows "Normal".				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT010:7	Turn-off the power supply to the REG-DA.	Verify that the status text for the device shows "Faulty".				
SYS.HMI.FAT010:7	Turn-on the power supply to the REG-DA.	Verify that the status text for the device shows "Normal".				
System Test Book - HMI FAT: Help Screen Checklist						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT021:1	Verify that the header of the screen is correct.	N/A				
SYS.HMI.FAT021:2	Verify explanation of used symbols.	N/A				
System Test Book - HMI FAT: User Administration Checklist						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT012:1.1	Login to HMI as Operator.	Operator word appears in Current User window of Basic Signaling Window.				
SYS.HMI.FAT012:1.2	Verify Operator can navigate through various displays including alarm list & event list.	N/A				
SYS.HMI.FAT012:1.3	Verify Operator can acknowledge the alarms.	N/A				
SYS.HMI.FAT012:1.4	Verify Operator cannot issue a control command.	N/A				
SYS.HMI.FAT012:2.1	Login to HMI as ITAdmin.	IT Admin word appears in Current User window of Basic Signaling Window.				
SYS.HMI.FAT012:2.2	Verify IT Admin can navigate only to "Network Overview" screen including alarm list & event list.	N/A				
SYS.HMI.FAT012:2.3	Verify IT Admin can acknowledge alarms.	N/A				
SYS.HMI.FAT012:2.4	Verify IT Admin cannot issue a control command.	N/A				
SYS.HMI.FAT012:3.1	Login to HMI as OTAdmin.	OT Admin word appears in Current User window of Basic Signaling Window.				
SYS.HMI.FAT012:3.2	Verify OT Admin can navigate to all screens including alarm list & event list except "Network Screen".	N/A				
SYS.HMI.FAT012:3.3	Verify OT Admin can acknowledge the alarms.	N/A				
SYS.HMI.FAT012:3.4	Verify OT Admin cannot issue a control command.	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT012:4.1	Login to HMI as Administrator	Administrator word appears in Current User window of Basic Signaling Window.				
SYS.HMI.FAT012:4.2	Verify Administrator can navigate through various displays including alarm & event list.	N/A				
SYS.HMI.FAT012:4.3	Administrator can acknowledge the alarms.	N/A				
SYS.HMI.FAT012:4.4	Administrator can issue a control command.	N/A				
SYS.HMI.FAT012:4.5	Administrator can access all programs of HMIs.	N/A				
System Test Book - HMI FAT: User Administration Checklist						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT017:2.1	Generate a persisting Alarm.	New persisting alarm appears in the alarm list in red background and white foreground with correct date and time stamping in the bottom of the list.				
SYS.HMI.FAT017:2.2	Generate a non-persisting Alarm.	New non-persisting alarm appears in the alarm list in green color.				
SYS.HMI.FAT017:2.3	Acknowledge persisting alarm.	Verify the text color and background color of the alarm message changes as stated above.				
SYS.HMI.FAT017:2.4	Acknowledge non-persistent alarm.	Verify the alarm is not longer present in the alarm list.				
SYS.HMI.FAT017:2.5	Check naming convention of alarms of one typical feeder according to signal list.	N/A				
SYS.HMI.FAT017:3.1	Generate many alarms from different panels, and apply filter for a specific feeder or device.	Only filtered alarms appear in list.				
SYS.HMI.FAT017:3.2	Scroll up and down in the Alarm list to see the previous/next alarms.	Scrolling facility is working.				
SYS.HMI.FAT017:3.3	Generate a persisting Alarm.	New persisting alarm appears in the event list in red background and white foreground with correct date and time stamping in the bottom of the list.				
SYS.HMI.FAT017:3.4	Generate a non-persisting Alarm.	New non-persisting alarm appears in the event list in green color.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.FAT017:3.5	Acknowledge persisting alarm.	Verify the text color and background color of the event message changes as stated above.				
SYS.HMI.FAT017:3.6	Acknowledge non-persistent alarm.	Verify the alarm is not longer present in the event list.				
SYS.HMI.FAT017:3.7	Check naming convention of alarms of one typical feeder according to signal list.	N/A				
SYS.HMI.FAT017:3.8	Generate many alarms from different panels, and apply filter for a specific feeder or device.	Only filtered events appear in list.				
SYS.HMI.FAT017:3.9	Scroll up and down in the Event list to see the previous/next alarms.	Scrolling facility is working.				

Supplemental SAT Test Book: FAT-003						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.SAT.FAT003.1	Verify SICAM status changes are reported and logged at the CC and					
SYS.HMI.SAT.FAT003.2	Verify that IED scanning is happening and data is correct not only					
SYS.HMI.SAT.FAT003.3	Verify users log on and log off					
SYS.HMI.SAT.FAT003.4	Verify system management and configuration displays and tools					
SYS.HMI.SAT.FAT003.5	Verify correct operation of the system components (system configuration overview, servers status, communications status, applications running,....)					
SYS.HMI.SAT.FAT003.6	Verify data consistency at all levels starting at the HMI and InService					
SYS.HMI.SAT.FAT003.7	Verify communication path status from the HMI					
Supplemental SAT Test Book: FAT-024						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.SAT.FAT024.1	Verify lan failure recovery for SICAM					
SYS.HMI.SAT.FAT024.2	Verify HMI servers and clients operation with LAN failures					
SYS.HMI.SAT.FAT024.3	Verify HMI operation with SICAMs with LAN failures					
SYS.HMI.SAT.FAT024.4	Verify HMI redundancy at the application level (caused by SW					
SYS.HMI.SAT.FAT024.5	Verify system behavior during individual servers power failures					
SYS.HMI.SAT.FAT024.6	Verify SICAM status changes are reported and logged at the CC and					
SYS.HMI.SAT.FAT024.7	Verify how servers' power failure affect HMI Clients.					
Supplemental SAT Test Book: FAT-005						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.SAT.FAT005.1	Verify communication failover and redundancy for communication					
Supplemental SAT Test Book: FAT-007						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.SAT.FAT007.1	Verify analog controls (set points), raise/lower (no return),....					
SYS.HMI.SAT.FAT007.2	Verify control action propagation in all modules and that execution is synchronized					
SYS.HMI.SAT.FAT007.3	Verify control command failures					
Supplemental SAT Test Book: FAT-008						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.SAT.FAT008.1	Verify analog controls (set points), raise/lower (no return),....					
SYS.HMI.SAT.FAT008.2	Verify control action propagation in all modules and that execution is synchronized					
SYS.HMI.SAT.FAT008.3	Verify control command failures					

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.SAT.FAT008.4	Check that all types of points and values are tested					
SYS.HMI.SAT.FAT008.5	Verify value representation, values and data quality					
SYS.HMI.SAT.FAT008.6	Verify data presented in Tabular displays					
SYS.HMI.SAT.FAT008.7	Verify alarm events					
SYS.HMI.SAT.FAT008.8	Verify all the alarm types and event reporting caused by data					
SYS.HMI.SAT.FAT008.9	Verify analog data deadband defined in the devices by checking the					
SYS.HMI.SAT.FAT008.10	Verify time needed for data presentation and control execution to					
Supplemental SAT Test Book: FAT-010						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.SAT.FAT010.1	Verify status reporting and logging at the HMI and CC					
SYS.HMI.SAT.FAT010.2	Verify communication management capabilities like force DNP3 scan, force alternative communication path,...					
Supplemental SAT Test Book: FAT-021						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.SAT.FAT021.1	Verify the availability of Help screen (Not only SICAM help)					
SYS.HMI.SAT.FAT021.2	Verify definition and use of KCPL defined help screens					
Supplemental SAT Test Book: FAT-012						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.SAT.FAT012.1	Verify only defined users can log on					
SYS.HMI.SAT.FAT012.2	Verify change in AOR					
SYS.HMI.SAT.FAT012.3	Verify authorization and permission changes for an AOR					
SYS.HMI.SAT.FAT012.4	Verify alarm and event list access					
Supplemental SAT Test Book: FAT-017						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HMI.SAT.FAT017.1	Verify alarm management capabilities (acknowledge, deletion,...)					
SYS.HMI.SAT.FAT017.2	Verify alarm list functions like filtering, queries, paging...					
SYS.HMI.SAT.FAT017.3	Verify that alarm error conditions and problems are reported and logged (list full, alarm processing not working,...)					
SYS.HMI.SAT.FAT017.4	Verify alarm management special conditions like max number of alarms reached, reduced view,...					
SYS.HMI.SAT.FAT017.5	Verify reporting and logging of alarm issues and list management					
SYS.HMI.SAT.FAT017.6	Verify queries and filtering capabilities in logs					

System Test Book - SICAM FAT: Document Verification Checklist						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.FAT001:1	Verify that the single line diagram is provided during the FAT.	N/A				
SYS.SCMS.FAT001:2	Verify that the functional design specification is provided during the FAT.	N/A				
SYS.SCMS.FAT001:3	Verify that the network architecture is provided during the FAT.	N/A				
SYS.SCMS.FAT001:4	Verify that the network architecture of test system is provided during the FAT.	N/A				
SYS.SCMS.FAT001:5	Verify that the system configuration description is provided during the FAT.	N/A				
SYS.SCMS.FAT001:6	Verify that the signal is provided during the FAT.	N/A				
System Test Book - SICAM FAT: Equipment Hardware Checklist						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.FAT002:1	Verify that two SICAM PAS Station Units 2.20 are provided during the FAT.	N/A				
SYS.SCMS.FAT002:2	Verify that one SEL 487B is provided during the FAT.	N/A				
SYS.SCMS.FAT002:3	Verify that one SEL 487E is provided during the FAT.	N/A				
SYS.SCMS.FAT002:4	Verify that one SEL 451 is provided during the FAT.	N/A				
SYS.SCMS.FAT002:5	Verify that one SEL 751A is provided during the FAT.	N/A				
SYS.SCMS.FAT002:6	Verify that one Arbiter GPS Clock is provided during the FAT.	N/A				
SYS.SCMS.FAT002:7	Verify that one RSG2100 RuggedCom Ethernet Switch is provided during the FAT.	N/A				
SYS.SCMS.FAT002:8	Verify that one Cisco Ethernet Switch is provided during the FAT.	N/A				
SYS.SCMS.FAT002:9	Verify that one A-Eberle Tap Changer is provided during the FAT.	N/A				
System Test Book - SICAM FAT: Equipment Software Checklist						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.FAT003:1.1	Verify that the SICAM PAS Station Unit has Windows XP Embedded OS SP3.	N/A				
SYS.SCMS.FAT003:1.2.1	Verify that the SICAM PAS Station Unit has the SICAM PAS V7.01 Runtime & Configuration Dongle.	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.FAT003:1.2.2	Verify that the SICAM PAS Station Unit has PAS Runtime.	N/A				
SYS.SCMS.FAT003:1.2.3	Verify that the SICAM PAS Station Unit has PAS UI Large.	N/A				
SYS.SCMS.FAT003:1.2.4	Verify that the SICAM PAS Station Unit has IEC61850 Client.	N/A				
SYS.SCMS.FAT003:1.2.5	Verify that the SICAM PAS Station Unit has DNP3.0 MASTER.	N/A				
SYS.SCMS.FAT003:1.2.6	Verify that the SICAM PAS Station Unit has DNP3.0 SLAVE.	N/A				
SYS.SCMS.FAT003:1.2.7	Verify that the SICAM PAS Station Unit has AUTOMATION.	N/A				
SYS.SCMS.FAT003:1.2.8	Verify that the SICAM PAS Station Unit has IEC61850 Server.	N/A				
SYS.SCMS.FAT003:1.3.1	SICAM PAS Backup DVD	N/A				
System Test Book - SICAM FAT: System Startup Behavior Checklist						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.FAT004:0.1	Verify that the SICAM station unit is connected to power.	N/A				
SYS.SCMS.FAT004:0.2	Verify that the SICAM station unit is connected to the network.	N/A				
SYS.SCMS.FAT004:0.3	Verify access to SICAM station unit available through external monitor or remote desktop session.	N/A				
SYS.SCMS.FAT004:1	Open UI Operation and verify that all applications within the UI Operation are running with GREEN Icon Indication on HVPAS1.	N/A				
SYS.SCMS.FAT004:2	Open UI Operation and verify that all applications within the UI Operation are running with GREEN Icon Indication on HVPAS2.	N/A				
System Test Book - SICAM FAT: Redundancy & Self Healing at Station Level						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.FAT005:1.1.1	Verify that Station Unit 1 is the assigned Active system.	N/A				
SYS.SCMS.FAT005:1.1.2	Verify that Station Unit 2 is the assigned Standby.	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.FAT005:1.1.3	Verify that DCADA Computers are connected to Active system (This is verified through PAS Operation).	N/A				
SYS.SCMS.FAT005:1.2	Simulate the Station Unit 1 Failure by switching off the power supplies to the station unit.	Verify that Station Unit 2 is assigned as the new active Station Unit and Station unit 1 is not communicating, and verify that DCADA computers are connected to the Active system (Station unit 2).				
SYS.SCMS.FAT005:1.3	Return power to Station Unit 1.	Verify that Station Unit 1 is assigned as the Standby system and Station unit 2 is assigned as Active, and verify that DCADA computers are still connected to the Active system.				
SYS.SCMS.FAT005:1.4.1	Disconnect any one redundant cable connection to the network switch.	Verify that ValueViewer indicates defected cable.				
SYS.SCMS.FAT005:1.4.2	Disconnect any one redundant cable connection to the network switch.	Verify that Station Unit 1 is still in service and communicating to the DCADA.				
SYS.SCMS.FAT005:1.4.3	Disconnect any one redundant cable connection to the network switch.	Verify that there is no change in the Active standby assignment in SICAM PAS Operation.				
SYS.SCMS.FAT005:2.1	Simulate the Station Unit 2 Failure by switching off the power supplies to the station unit.	Verify that Station Unit 1 is assigned as the new active Station Unit and Station unit 2 is not communicating, and verify that DCADA computers are connected to the Active system (Station unit 1).				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.FAT005:2.2	Return power to Station Unit 2.	Verify that Station Unit 2 is assigned as the Standby system and Station unit 1 is assigned as Active, and verify that DCADA computers are still connected to the Active system.				
SYS.SCMS.FAT005:2.3.1	Disconnect any one redundant cable connection to the network switch.	Verify that ValueViewer indicates defected cable.				
SYS.SCMS.FAT005:2.3.2	Disconnect any one redundant cable connection to the network switch.	Verify that Station Unit 2 is still in service and communicating to the DCADA.				
SYS.SCMS.FAT005:2.3.3	Disconnect any one redundant cable connection to the network switch.	Verify that there is no change in the Active standby assignment in SICAM PAS Operation.				
SYS.SCMS.FAT005:3.1.1	Unplug the network cables from Station unit 1.	Verify that Station unit 2 is assigned as Active and Station unit 1 is not communicating.				
SYS.SCMS.FAT005:3.1.2	Unplug the network cables from Station unit 1.	Verify the DCADA computers connect to the Active system (Station unit 2).				
SYS.SCMS.FAT005:3.2.1	Connect the network cables back to Station unit 1.	Verify that Station unit 1 is assigned as Active and Station unit 2 is standby.				
SYS.SCMS.FAT005:3.2.2	Connect the network cables back to Station unit 1.	Verify the DCADA computers connect to Active system (Station unit 1).				
SYS.SCMS.FAT005:3.3.1	Unplug the network cables from Station unit 2.	Verify that Station unit 1 is still assigned as Active system and Station unit 2 is not communicating.				
SYS.SCMS.FAT005:3.3.2	Unplug the network cables from Station unit 2.	Verify the DCADA computers connect to the Active system (Station unit 1).				
SYS.SCMS.FAT005:3.4.1	Connect the network cables back to Station unit 2.	Verify that Station unit 1 remains as Active system and Station unit 2 is standby.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.FAT005:3.4.2	Connect the network cables back to Station unit Z.	Verify the DCADA computers connect to the Active system (Station unit 1).				
System Test Book - SICAM FAT: Communication Test						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.FAT006:1.1.1	Ping the SEL 487E from station unit 1.	Verify ping is successful.				
SYS.SCMS.FAT006:1.1.2	Ping the SEL 487B from station unit 1.	Verify ping is successful.				
SYS.SCMS.FAT006:1.1.3	Ping the SEL 451-5 from station unit 1.	Verify ping is successful.				
SYS.SCMS.FAT006:1.1.4	Ping the SEL 751A from station unit 1.	Verify ping is successful.				
SYS.SCMS.FAT006:1.1.5	Ping the A-Eberle Tap Changer from station unit 1.	Verify ping is successful.				
SYS.SCMS.FAT006:1.1.6	Ping the Rugged-SH1 from station unit 1.	Verify ping is successful.				
SYS.SCMS.FAT006:1.1.7	Ping the Rugged-SH2 from station unit 1.	Verify ping is successful.				
SYS.SCMS.FAT006:1.1.8	Ping the Rugged-SH3 from station unit 1.	Verify ping is successful.				
SYS.SCMS.FAT006:1.1.9	Ping the Rugged-SH4 from station unit 1.	Verify ping is successful.				
SYS.SCMS.FAT006:1.1.10	Ping the Rugged-CH1 from station unit 1.	Verify ping is successful.				
SYS.SCMS.FAT006:1.1.11	Ping the Cisco-SH1 from station unit 1.	Verify ping is successful.				
SYS.SCMS.FAT006:1.1.12	Ping the Cisco-SH2 from station unit 1.	Verify ping is successful.				
SYS.SCMS.FAT006:1.1.13	Ping the Cisco-SH3 from station unit 1.	Verify ping is successful.				
SYS.SCMS.FAT006:1.1.14	Ping the Cisco-SH4 from station unit 1.	Verify ping is successful.				
SYS.SCMS.FAT006:1.1.15	Ping the Cisco-CH1 from station unit 1.	Verify ping is successful.				
SYS.SCMS.FAT006:1.2.1	Ping the SEL 487E from station unit 2.	Verify ping is successful.				
SYS.SCMS.FAT006:1.2.2	Ping the SEL 487B from station unit 2.	Verify ping is successful.				
SYS.SCMS.FAT006:1.2.3	Ping the SEL 452-5 from station unit 2.	Verify ping is successful.				
SYS.SCMS.FAT006:1.2.4	Ping the SEL 752A from station unit 2.	Verify ping is successful.				
SYS.SCMS.FAT006:1.2.5	Ping the A-Eberle Tap Changer from station unit 2.	Verify ping is successful.				
SYS.SCMS.FAT006:1.2.6	Ping the Rugged-SH2 from station unit 2.	Verify ping is successful.				
SYS.SCMS.FAT006:1.2.7	Ping the Rugged-SH2 from station unit 2.	Verify ping is successful.				
SYS.SCMS.FAT006:1.2.8	Ping the Rugged-SH3 from station unit 2.	Verify ping is successful.				
SYS.SCMS.FAT006:1.2.9	Ping the Rugged-SH4 from station unit 2.	Verify ping is successful.				
SYS.SCMS.FAT006:1.2.10	Ping the Rugged-CH2 from station unit 2.	Verify ping is successful.				
SYS.SCMS.FAT006:1.2.11	Ping the Cisco-SH2 from station unit 2.	Verify ping is successful.				
SYS.SCMS.FAT006:1.2.12	Ping the Cisco-SH2 from station unit 2.	Verify ping is successful.				
SYS.SCMS.FAT006:1.2.13	Ping the Cisco-SH3 from station unit 2.	Verify ping is successful.				
SYS.SCMS.FAT006:1.2.14	Ping the Cisco-SH4 from station unit 2.	Verify ping is successful.				
SYS.SCMS.FAT006:1.2.15	Ping the Cisco-CH2 from station unit 2.	Verify ping is successful.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.FAT006:2.1	Verify that Relays are available and in "running mode" (Green Play Button) mode on SICAM PAS UI Operation.	N/A				
SYS.SCMS.FAT006:2.2.1	Disconnect the SEL751A from the network.	Verify that the disconnected relay changes mode to "pending up" (Blue Up Arrow) on SICAM PAS UI Operation.				
SYS.SCMS.FAT006:2.2.2	Disconnect the SEL 451-5 from the network.	Verify that the disconnected relay changes mode to "pending up" (Blue Up Arrow) on SICAM PAS UI Operation.				
SYS.SCMS.FAT006:2.2.3	Disconnect the SEL 487B from the network.	Verify that the disconnected relay changes mode to "pending up" (Blue Up Arrow) on SICAM PAS UI Operation.				
SYS.SCMS.FAT006:2.2.4	Disconnect the SEL 487E from the network.	Verify that the disconnected relay changes mode to "pending up" (Blue Up Arrow) on SICAM PAS UI Operation.				
SYS.SCMS.FAT006:2.2.5	Disconnect the REG-DA from the network.	Verify that the disconnected relay changes mode to "pending up" (Blue Up Arrow) on SICAM PAS UI Operation.				
SYS.SCMS.FAT006:2.3.1	Reconnect the SEL751A from the network.	Verify that the reconnected relay changes mode to "Running" (Green Play Button) on SICAM PAS UI Operation.				
SYS.SCMS.FAT006:2.3.2	Reconnect the SEL 451-5 from the network.	Verify that the reconnected relay changes mode to "Running" (Green Play Button) on SICAM PAS UI Operation.				
SYS.SCMS.FAT006:2.3.3	Reconnect the SEL 487B from the network.	Verify that the reconnected relay changes mode to "Running" (Green Play Button) on SICAM PAS UI Operation.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.FAT006:2.3.4	Reconnect the SEL 487E from the network.	Verify that the reconnected relay changes mode to "Running" (Green Play Button) on SICAM PAS UI Operation.				
SYS.SCMS.FAT006:2.3.5	Reconnect the REG-DA from the network.	Verify that the reconnected relay changes mode to "Running" (Green Play Button) on SICAM PAS UI Operation.				
SYS.SCMS.FAT006:3.1.1	Unplug one cable from any active port of switch Ruggedcom-SH1	Verify the status of that port in the value viewer.				
SYS.SCMS.FAT006:3.1.2	Unplug one cable from any active port of switch Ruggedcom-SH2	Verify the status of that port in the value viewer.				
SYS.SCMS.FAT006:3.1.3	Unplug one cable from any active port of switch Ruggedcom-SH3	Verify the status of that port in the value viewer.				
SYS.SCMS.FAT006:3.1.4	Unplug one cable from any active port of switch Ruggedcom-SH4	Verify the status of that port in the value viewer.				
SYS.SCMS.FAT006:3.1.5	Unplug one cable from any active port of switch Ruggedcom-CH1	Verify the status of that port in the value viewer.				
SYS.SCMS.FAT006:3.2.1	Unplug one cable from any active port of switch Cisco-SH1	Verify the status of that port in the value viewer.				
SYS.SCMS.FAT006:3.2.2	Unplug one cable from any active port of switch Cisco-SH2	Verify the status of that port in the value viewer.				
SYS.SCMS.FAT006:3.2.3	Unplug one cable from any active port of switch Cisco-SH3	Verify the status of that port in the value viewer.				
SYS.SCMS.FAT006:3.2.4	Unplug one cable from any active port of switch Cisco-SH4	Verify the status of that port in the value viewer.				
SYS.SCMS.FAT006:3.2.5	Unplug one cable from any active port of switch Cisco-CH1	Verify the status of that port in the value viewer.				
System Test Book - SICAM FAT: Signal Test						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.FAT007:1.1.1	Trigger each indication, as per the signal list, from the 487B.	Verify that the triggered signal changed status in the SICAM Value Viewer.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.FAT007:1.1.2	Inject the measurement signal, as per the signal list, into the 487B using Omicron test set.	Verify that the measurement signal was recognized by the 487B, and that the value in the SICAM Value Viewer matches.				
SYS.SCMS.FAT007:1.1.3	Issue a command from SICAM Value Viewer as per the signal list or from the DCADA system.	Verify the 487B received the command and performs the designated action.				
SYS.SCMS.FAT007:1.2.1	Trigger each indication, as per the signal list, from the 487E.	Verify that the triggered signal changed status in the SICAM Value Viewer.				
SYS.SCMS.FAT007:1.2.2	Inject the measurement signal, as per the signal list, into the 487E using Omicron test set.	Verify that the measurement signal was recognized by the 487E, and that the value in the SICAM Value Viewer matches.				
SYS.SCMS.FAT007:1.2.3	Issue a command from SICAM Value Viewer as per the signal list or from the DCADA system.	Verify the 487E received the command and performs the designated action.				
SYS.SCMS.FAT007:1.3.1	Trigger each indication, as per the signal list, from the 751A.	Verify that the triggered signal changed status in the SICAM Value Viewer.				
SYS.SCMS.FAT007:1.3.2	Inject the measurement signal, as per the signal list, into the 751A using Omicron test set.	Verify that the measurement signal was recognized by the 751A, and that the value in the SICAM Value Viewer matches.				
SYS.SCMS.FAT007:1.3.3	Issue a command from SICAM Value Viewer as per the signal list or from the DCADA system.	Verify the 751A received the command and performs the designated action.				
SYS.SCMS.FAT007:1.4.1	Trigger each indication, as per the signal list, from the 451.	Verify that the triggered signal changed status in the SICAM Value Viewer.				
SYS.SCMS.FAT007:1.4.2	Inject the measurement signal, as per the signal list, into the 451 using Omicron test set.	Verify that the measurement signal was recognized by the 451, and that the value in the SICAM Value Viewer matches.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.FAT007:1.4.3	Issue a command from SICAM Value Viewer as per the signal list or from the DCADA system.	Verify the 451 received the command and performs the designated action.				
SYS.SCMS.FAT007:1.5.1	Trigger each indication, as per the signal list, from the REG-DA.	Verify that the triggered signal changed status in the SICAM Value Viewer.				
SYS.SCMS.FAT007:1.5.2	Inject the measurement signal, as per the signal list, into the REG-DA using Omicron test set.	Verify that the measurement signal was recognized by the REG-DA, and that the value in the SICAM Value Viewer matches.				
SYS.SCMS.FAT007:1.5.3	Issue a command from SICAM Value Viewer as per the signal list or from the DCADA system.	Verify the REG-DA received the command and performs the designated action.				
System Test Book - SICAM FAT: Time Synchronization Test						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.FAT008:1.1.1	Disconnect the network cables from the GPS Clocks.	NTP-Trace on Station Unit - check that the actual time server gets timed out. This can take 3-5 min.				
SYS.SCMS.FAT008:1.1.2	Check that the stratum of the SICAM PAS Station Unit 1 changes from 1 to 11 (10+1).	N/A				
SYS.SCMS.FAT008:1.1.3	Reconnect network cables.	NTP-Trace on Station Unit - check that the stratum of the station controllers changes to 2.				
SYS.SCMS.FAT008:1.1.4	Disconnect the network cables from the GPS Clocks.	N/A				
SYS.SCMS.FAT008:1.2.1	Disconnect the network cables from the GPS Clocks.	NTP-Trace on Station Unit - check that the actual time server gets timed out. This can take 3-5 min.				
SYS.SCMS.FAT008:1.2.2	Check that the stratum of the SICAM PAS Station Unit 2 changes from 1 to 11 (10+1).	N/A				
SYS.SCMS.FAT008:1.2.3	Reconnect network cables.	NTP-Trace on Station Unit - check that the stratum of the station controllers changes to 2.				
SYS.SCMS.FAT008:1.2.4	Disconnect the network cables from the GPS Clocks.	N/A				
SYS.SCMS.FAT008:1.3.1	Stop the NTP service from Station unit 1, and run ntptrace.	Verify the connection is timed.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.FAT008:1.3.2	Run ntptrace-sag on station unit 2.	Check that the stratum of the station controller is 11.				
SYS.SCMS.FAT008:1.4.1	Run the "ntpq-sag -p" command in the command shell. Keep running the command for about 7 to 10 minutes.	Verify that you get "*" mark on the left of the IP address of the clock. This verifies that the station unit is synchronized with the clock.				
SYS.SCMS.FAT008:1.4.2	Run the ntpq-sag -p command in station unit 2.	Verify that it was already synchronized with the clock.				
SYS.SCMS.FAT008:1.4.3	Run the ntpq-sag -p command in the command shell. Keep running the command for about 7 to 10 minutes.	Verify that you get "*" mark on the left of the IP address of the clock. This verifies that the station unit is synchronized with the clock.				
SYS.SCMS.FAT008:1.4.4	Run the ntpq-sag -p command in station unit 1.	Verify that it was already synchronized with the clock.				
SYS.SCMS.FAT008:2.1	Remove the IRIG-B connection from behind the relay	In the Value viewer, verify that IRIG status MMS message signal is changes value from 1 to 0.				
SYS.SCMS.FAT008:2.2	Plug the IRIG-B connection back onto the relay.	In the ValueViewer, verify that IRIG status MMS message signal changes from 0 to 1.				

Supplemental SICAM SAT Test Book: SAT-003						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.SAT.SAT003.1	Verify system management and configuration displays and tools	N/A				
Supplemental SICAM SAT Test Book: SAT-004						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.SAT.SAT004.1	Verify SICAM status changes are reported and logged at the CC and HMI	N/A				
SYS.SCMS.SAT.SAT004.2	Verify that IED scanning is happening and data is correct not only that the application is running	N/A				
SYS.SCMS.SAT.SAT004.3	Verify correct operation of the system components (system configuration overview, servers status, communications status, applications running,....)	N/A				
SYS.SCMS.SAT.SAT004.4	Verify data consistency at all levels starting at the HMI and InService	N/A				
SYS.SCMS.SAT.SAT004.5	Verify users log on and log off	N/A				
SYS.SCMS.SAT.SAT004.6	Verify only defined users can log on	N/A				
SYS.SCMS.SAT.SAT004.7	Verify configuration of AORs and permissions for different users	N/A				
Supplemental SICAM SAT Test Book: SAT-005						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.SAT.SAT005.1	Verify LAN failure recovery for SICAM	N/A				
SYS.SCMS.SAT.SAT005.2	Verify system behavior during individual servers power failures	N/A				
SYS.SCMS.SAT.SAT005.3	Verify SICAM status changes are reported and logged at the CC and HMI	N/A				
SYS.SCMS.SAT.SAT005.4	After Power Failure, verify that IED scanning is happening and data is correct not only that the application is running	N/A				
SYS.SCMS.SAT.SAT005.5	Verify data is correct after failover at all levels of redundancy	N/A				
Supplemental SICAM SAT Test Book: SAT-006						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.SAT.SAT006.1	Verify that all error conditions detected in the communication with the IEDs, are reported upstream. (change signal from 61850 to dnp for instance)	N/A				
SYS.SCMS.SAT.SAT006.2	Verify communication error reporting and logging at the Control Center	N/A				
SYS.SCMS.SAT.SAT006.3	Verify IED and SICAM communication management at the Control Center	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.SAT.SAT006.4	Verify communication management capabilities at the CC	N/A				
SYS.SCMS.SAT.SAT006.5	Verify communication failover and redundancy for communication or application errors/problems.	N/A				
SYS.SCMS.SAT.SAT006.6	Verify SICAM redundancy at the application level (caused by SW decisions, problems or errors)	N/A				
SYS.SCMS.SAT.SAT006.7	Verification of communication redundancy at the protocol level. Failover caused by protocol errors like number of fail attempts, IED reporting errors,....	N/A				
SYS.SCMS.SAT.SAT006.8	Verify system response to communication failure at the IED side (port unavailable, tropos router down,....)	N/A				
SYS.SCMS.SAT.SAT006.9	Verify communication management capabilities like force DNP3 scan, force alternative communication path,....	N/A				
SYS.SCMS.SAT.SAT006.10	Verify IED configuration related to port, protocol, profile,....	N/A				
Supplemental SICAM SAT Test Book: SAT-007						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
IEC61850 - SEL487B (Values)						
SYS.SCMS.SAT.SAT007.1.1	Verify analog data deadband defined in the devices by checking the reported values in HMI. This will verify that there is no deadband defined at the SICAM level	N/A				
IEC61850 - SEL487B Controls)						
SYS.SCMS.SAT.SAT007.1.2	Verify analog controls (set points), raise/lower (no return),...	N/A				
SYS.SCMS.SAT.SAT007.1.3	Verify control action propagation in all modules and that execution is synchronized	N/A				
SYS.SCMS.SAT.SAT007.1.4	Verify control command failures	N/A				
IEC61850 - SEL487E (Values)						
SYS.SCMS.SAT.SAT007.2.1	Verify analog data deadband defined in the devices by checking the reported values in HMI. This will verify that there is no deadband defined at the SICAM level	N/A				
IEC61850 - SEL487E Controls)						
SYS.SCMS.SAT.SAT007.2.2	Verify analog controls (set points), raise/lower (no return),...	N/A				
SYS.SCMS.SAT.SAT007.2.3	Verify control action propagation in all modules and that execution is synchronized	N/A				
SYS.SCMS.SAT.SAT007.2.4	Verify control command failures	N/A				
IEC61850 - SEL751A (Values)						

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.SCMS.SAT.SAT007.3.1	Verify analog data deadband defined in the devices by checking the reported values in HMI. This will verify that there is no deadband defined at the SICAM level	N/A				
IEC61850 - SEL751A Controls						
SYS.SCMS.SAT.SAT007.3.2	Verify analog controls (set points), raise/lower (no return),...	N/A				
SYS.SCMS.SAT.SAT007.3.3	Verify control action propagation in all modules and that execution is synchronized	N/A				
SYS.SCMS.SAT.SAT007.3.4	Verify control command failures	N/A				
IEC61850 - SEL451 (Values)						
SYS.SCMS.SAT.SAT007.4.1	Verify analog data deadband defined in the devices by checking the reported values in HMI. This will verify that there is no deadband defined at the SICAM level	N/A				
IEC61850 - SEL451 Controls						
SYS.SCMS.SAT.SAT007.4.2	Verify analog controls (set points), raise/lower (no return),...	N/A				
SYS.SCMS.SAT.SAT007.4.3	Verify control action propagation in all modules and that execution is synchronized	N/A				
SYS.SCMS.SAT.SAT007.4.4	Verify control command failures	N/A				
IEC61850 - REG-DA (Values)						
SYS.SCMS.SAT.SAT007.5.1	Verify analog data deadband defined in the devices by checking the reported values in HMI. This will verify that there is no deadband defined at the SICAM level	N/A				
IEC61850 - REG-DA Controls						
SYS.SCMS.SAT.SAT007.5.2	Verify analog controls (set points), raise/lower (no return),...	N/A				
SYS.SCMS.SAT.SAT007.5.3	Verify control action propagation in all modules and that execution is synchronized	N/A				
SYS.SCMS.SAT.SAT007.5.4	Verify control command failures	N/A				
SYS.SCMS.SAT.SAT007.5.5	Verify error reporting and logging. Some error conditions need to be generated.	N/A				
SYS.SCMS.SAT.SAT007.5.6	Verify all the alarm types and event reporting caused by data processing	N/A				
SYS.SCMS.SAT.SAT007.5.7	Verify time needed for data presentation and control execution to and from the Control Center	N/A				
Supplemental SICAM SAT Test Book: SAT-009						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
DNP3 - Intellicap (Values)						
SYS.SCMS.SAT.SAT009.1.1	Verify analog data deadband defined in the devices by checking the reported values in HMI. This will verify that there is no deadband defined at the SICAM level	N/A				
DNP3 - Intellicap (Commands)						
SYS.SCMS.SAT.SAT009.1.2	Verify analog controls (set points), raise/lower (no return),...	N/A				
SYS.SCMS.SAT.SAT009.1.3	Verify control action propagation in all modules and that execution is synchronized	N/A				
SYS.SCMS.SAT.SAT009.1.4	Verify control command failures	N/A				
DNP3 - FCI (Values)						
SYS.SCMS.SAT.SAT009.2.1	Verify analog data deadband defined in the devices by checking the reported values in HMI. This will verify that there is no deadband defined at the SICAM level	N/A				
DNP3 - FCI (Commands)						
SYS.SCMS.SAT.SAT009.2.2	Verify analog controls (set points), raise/lower (no return),...	N/A				
SYS.SCMS.SAT.SAT009.2.3	Verify control action propagation in all modules and that execution is synchronized	N/A				
SYS.SCMS.SAT.SAT009.2.4	Verify control command failures	N/A				
DNP3 - Recloser (Values)						
SYS.SCMS.SAT.SAT009.3.1	Verify analog data deadband defined in the devices by checking the reported values in HMI. This will verify that there is no deadband defined at the SICAM level	N/A				
DNP3 - Recloser (Commands)						
SYS.SCMS.SAT.SAT009.3.2	Verify analog controls (set points), raise/lower (no return),...	N/A				
SYS.SCMS.SAT.SAT009.3.3	Verify control action propagation in all modules and that execution is synchronized	N/A				
SYS.SCMS.SAT.SAT009.3.4	Verify control command failures	N/A				
DNP3 - Recloser (Counters)						
SYS.SCMS.SAT.SAT009.3.5	Verify error reporting and logging	N/A				
SYS.SCMS.SAT.SAT009.3.6	Verify all the alarm types and event reporting caused by data processing	N/A				
SYS.SCMS.SAT.SAT009.3.7	Verify time needed for data presentation and control execution to and from the Control Center	N/A				
SYS.SCMS.SAT.SAT009.3.8	Verify that the SICAM can synchronize IEDs using DNP3	N/A				

System Test Book - DCADA (Phase 3 FAT): Control Transfer						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DCADA(P3FAT).TC2.1.1	Starting the UI: Testing the startup sequence of the Control Transfer UI	N/A				
SYS.DCADA(P3FAT).TC2.1.2	Mastership at DMS: Test that UI can transfer mastership at DMS	N/A				
SYS.DCADA(P3FAT).TC2.1.3	Mastership at DCADA: Test that UI can transfer mastership to DCADA	N/A				
SYS.DCADA(P3FAT).TC2.2.1	Transfer Control – DCADA Closed Loop: Verify that Control (mastership) is transferred back to DMS when problems arise when DCADA is in closed loop control for a region.	N/A				
SYS.DCADA(P3FAT).TC2.2.2	Transfer Control – Exit Closed Loop at DMS: Verify that Closed Loop Operation is suspended when problem is encountered while applications are running in closed loop in DMS.	N/A				
SYS.DCADA(P3FAT).TC2.3.1	Verification – DCADA Closed Loop: Verify that DMS Operator is able to perform all actions besides 'Control' when mastership is at DCADA.	N/A				
SYS.DCADA(P3FAT).TC2.3.2	Verification – DMS Manual: Verify that DMS Operator is able to perform all actions including 'Control' when mastership is at DMS with control type of Manual Control.	N/A				
SYS.DCADA(P3FAT).TC2.3.3	Verification – DMS Closed Loop: Verify that DMS Operator is able to perform all actions besides 'Control' when Mastership is at DMS with Control Type of Closed Loop Control.	N/A				
System Test Book - DCADA (Phase 3 FAT): Closed Loop Operation						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DCADA(P3FAT).TC3.1.1	Receiving Messages at DMS sent by DMS applications: Testing message propagation at DMS location sent by DMS applications when DMS has mastership and run in Close Loop or Advisory (manual) operation mode.	N/A				
SYS.DCADA(P3FAT).TC3.1.2	Messages at DMS sent by DCADA applications: Testing propagation of messages to DMS location sent by DCADA applications when DCADA has mastership and operates in Closed Loop control mode	N/A				
SYS.DCADA(P3FAT).TC3.2.1	FDIR – normal operation at DCADA master: Testing of the FDIR operation at DCADA with mastership in closed loop control mode.	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DCADA(P3FAT).TC3.2.2	VVC – normal operation at DCADA master: Testing of the VVC operation at DCADA with mastership in closed loop control mode.	N/A				
SYS.DCADA(P3FAT).TC3.2.3	FLT – normal operation at DCADA master: Testing of the FLT operation at DCADA with mastership in closed loop control mode.	N/A				
SYS.DCADA(P3FAT).TC3.3.1	FDIR – normal operation at DMS master: Testing of the FDIR operation at DMS with mastership in closed loop control mode.	N/A				
SYS.DCADA(P3FAT).TC3.3.2	VVC – normal operation at DMS master: Testing of the VVC operation at DMS with mastership in closed loop control mode.	N/A				
SYS.DCADA(P3FAT).TC3.3.3	FLT – normal operation at DMS master: Testing of the FLT operation at DMS with mastership in closed loop control mode.	N/A				

System Test Book - DCADA (Phase 3 SAT)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DCADA(P3SAT).62	Verify presentation of the control and application status for the substation and the CC	N/A				
SYS.DCADA(P3SAT).64	Verify Manual transfer of DNA control to DMS	N/A				
SYS.DCADA(P3SAT).64	Verify Manual transfer of DNA control to DCADA	N/A				
SYS.DCADA(P3SAT).419	Verify that the Mastership control UI or status and control operations are accessible in DCADA DNA in case DMS is not accessible	N/A				
SYS.DCADA(P3SAT).420	Verify automatic transfer of control from DCADA close loop to DMS: * Boundary switch closed * Connection between DCADA and SICAM lost * FLT/FISR/VVC error condition in DCADA DNA * Loss of communication between DCADA and DMS	N/A				
SYS.DCADA(P3SAT).421	Verify of automatic control authority removal from DMS close loop when: * Boundary switch closed * Connection between DMS and SICAM is lost * FISR/FLT/VVC error condition in DMS DNA * Loss of communication between DCADA and DMS	N/A				
SYS.DCADA(P3SAT).422	Verify normal operation of DMS except for controls when DCADA is master	N/A				
SYS.DCADA(P3SAT).424	Verify normal operation of DMS including controls when DMS is Master and in manual mode	N/A				
SYS.DCADA(P3SAT).425	Verify normal operation of DMS except controls when DMS is Master in Close Loop	N/A				
SYS.DCADA(P3SAT).426	Verify DCADA can not be set to close loop operation when DMS is Master	N/A				
SYS.DCADA(P3SAT).427	Verify DMS can not be set to close loop operation for Midtown when DCADA is Master	N/A				
SYS.DCADA(P3SAT).428	Verify notification of Control Mastership in DCADA and DMS UIs	N/A				
SYS.DCADA(P3SAT).196	Enable- disable applications independently in DCADA and DMS	N/A				
SYS.DCADA(P3SAT).208	From InService demonstrate access to PowerFlow connecting to the DNA in DCADA	N/A				
SYS.DCADA(P3SAT).219	Run DSSE from DCADA DNA UI and verify results	N/A				
SYS.DCADA(P3SAT).220	Verify DSSE different modes of execution from DCADA	N/A				
SYS.DCADA(P3SAT).221	Verify reporting of execution errors or problems from DCADA	N/A				
SYS.DCADA(P3SAT).222	Verify access to application alarms or program output from DCADA	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DCADA(P3SAT).224	Introduce manual data changes and verify results	N/A				
SYS.DCADA(P3SAT).236	Run Power Flow from DCADA DNA UI and verify results	N/A				
SYS.DCADA(P3SAT).237	Verify PowerFlow different modes of execution from the DCADA	N/A				
SYS.DCADA(P3SAT).241	Introduce manual data changes and verify results from the DCADA	N/A				
SYS.DCADA(P3SAT).243	Verify access to list and summaries using DNA UI in DCADA	N/A				
SYS.DCADA(P3SAT).245	Verify alarms generated in DCADA by Limit violation or other operational conditions like non convergence	N/A				
SYS.DCADA(P3SAT).246	Verify DNA PF simultaneous execution in DMS and DCADA (Event Triggered)	N/A				
SYS.DCADA(P3SAT).247	Verify and compare PF results	N/A				
SYS.DCADA(P3SAT).266	Verify FLT running from DCADA	N/A				
SYS.DCADA(P3SAT).289	Verify authority transfer from DCADA to DMS when a solution is not found	N/A				
SYS.DCADA(P3SAT).316	Verify interaction with application in InService	N/A				
SYS.DCADA(P3SAT).317	Verify interaction with application in DNA UI	N/A				
SYS.DCADA(P3SAT).319	Verify access to application alarms or program output	N/A				
SYS.DCADA(P3SAT).344	Verify notification to Operator in DMS when authority is transferred	N/A				
SYS.DCADA(P3SAT).371	Verification of VVC configuration and Manual execution.	N/A				
SYS.DCADA(P3SAT).375	Verify authority transfer from DCADA to DMS when a solution is not found	N/A				
SYS.DCADA(P3SAT).384	Verify VVC execution triggered by different conditions	N/A				
SYS.DCADA(P3SAT).386	Verify VVC results of the sequence generated and executed	N/A				
SYS.DCADA(P3SAT).389	Verify VVC operation after DCADA failover occurs and stable situation is reestablished	N/A				
SYS.DCADA(P3SAT).402	Verify Close Loop Operation in DCADA	N/A				
SYS.DCADA(P3SAT).407	Verify coordinated Close Loop Operation in DCADA and DMS together	N/A				
SYS.DCADA(P3SAT).408	Verify configuration of close loop in DCADA and DMS together	N/A				
SYS.DCADA(P3SAT).409	Verify Operator's notification in DMS	N/A				
SYS.DCADA(P3SAT).410	Verify authority transfer from DCADA to DMS when a solution is not found	N/A				
SYS.DCADA(P3SAT).411	Verify notification to Operator's in DMS when authority is transferred	N/A				

System Test Book - DMS (Phase 1 Factory Acceptance Test) - SmartSubstation Testing						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1FAT).1	Verify the IEC61850- GOOSE & MMS and DNP/IP Communication between SICAM PAS and the process IEDs. This includes report by exception and periodic verification poll.	N/A				
SYS.DMS(P1FAT).2	Verify SCMS equipments - Hardware & Software	N/A				
SYS.DMS(P1FAT).3	Verify Relay Communication	N/A				
SYS.DMS(P1FAT).4	Verify Signal	N/A				
SYS.DMS(P1FAT).5	Verify Time synchronization	N/A				
System Test Book - DMS (Phase 1 Factory Acceptance Test) -DMS System Testing						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1FAT).6	Identify all the substation devices and data points mapping on D-SCADA, InService and ICCP.	N/A				
SYS.DMS(P1FAT).7	Test communication from IECADA to Substation Devices. - Receive Analog Input data from Devices - Receive Digital Input data from Devices - Simulate devices and measurement. Verify the status/analog data changes. - Verify the supervisory control on devices from IECADA, verify all the alarms generated from operations	N/A				
SYS.DMS(P1FAT).8	Login in as different users and test permissions. Ack/Cancel alarms...etc.	N/A				
SYS.DMS(P1FAT).9	Verify all the Hardware & Software(running processes) of DMS	N/A				

System Test Book - DMS (Phase 1 Site Acceptance Test) - Feeder / Tie Breaker (751A Profile 1) : Status Points						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).1	Verify point "Breaker Status"	Values Displayed: - OPEN - CLOSED				
SYS.DMS(P1SAT-P2P-SUB).2	Verify point "Local Remote"	Values Displayed: - LOCAL - REMOTE				
SYS.DMS(P1SAT-P2P-SUB).3	Verify point "79CO"	Values Displayed: - OFF - ON				
SYS.DMS(P1SAT-P2P-SUB).4	Verify point "50CO"	Values Displayed: - OFF - ON				
SYS.DMS(P1SAT-P2P-SUB).5	Verify point "Close Failure"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).6	Verify point "Under Frequency Trip"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).7	Verify point "High Current Lockout"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).8	Verify point "Slow Breaker Indication"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).9	Verify point "Contact Wear"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).10	Verify point "Feeder Lockout Operated"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).11	Verify point "Trip Coil Monitor"	Values Displayed: - FALSE - TRUE				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).12	Verify point "Latched LED 1"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).13	Verify point "Latched LED 2"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).14	Verify point "Latched LED 3"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).15	Verify point "Latched LED 4"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).16	Verify point "Latched LED 5"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).17	Verify point "Latched LED 6"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).18	Verify point "Hardware Alarm"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).19	Verify point "Software Alarm"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).20	Verify point "FAULT"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).21	Verify point "Synchronism Check Element 1"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).22	Verify point "Synchronism Check Element 2"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).23	Verify point "Healthy Voltage Vp for Synchronism Check"	Values Displayed: - FALSE - TRUE				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).24	Verify point "Healthy Voltage Vs for Synchronism Check"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).25	Verify point "Loss of Potential"	Values Displayed: - FALSE - TRUE				
System Test Book - DMS (Phase 1 Site Acceptance Test) - Feeder / Tie Breaker (751A Profile 1) : Control Points						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).26	Verify point "Breaker Open"	Values Displayed: - N/A - OPEN				
SYS.DMS(P1SAT-P2P-SUB).27	Verify point "Breaker Close"	Values Displayed: - N/A - CLOSE				
SYS.DMS(P1SAT-P2P-SUB).28	Verify point "79CO OFF"	Values Displayed: - N/A - OFF				
SYS.DMS(P1SAT-P2P-SUB).29	Verify point "79CO On"	Values Displayed: - N/A - ON				
SYS.DMS(P1SAT-P2P-SUB).30	Verify point "50CO OFF"	Values Displayed: - N/A - OFF				
SYS.DMS(P1SAT-P2P-SUB).31	Verify point "50CO On"	Values Displayed: - N/A - ON				
System Test Book - DMS (Phase 1 Site Acceptance Test) - Feeder / Tie Breaker (751A Profile 1) : Analog Points						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).32	Verify point "Real Power - 3 Phase "	N/A				
SYS.DMS(P1SAT-P2P-SUB).33	Verify point "Reactive Power - 3 Phase "	N/A				
SYS.DMS(P1SAT-P2P-SUB).34	Verify point "Amps - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).35	Verify point "Amps - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).36	Verify point "Amps - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).37	Verify point "Voltage - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).38	Verify point "Voltage - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).39	Verify point "Voltage - Phase C"	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).40	Verify point "Apparent Power - 3 Phase"	N/A				
SYS.DMS(P1SAT-P2P-SUB).41	Verify point "Power Factor - 3 Phase"	N/A				
SYS.DMS(P1SAT-P2P-SUB).42	Verify point "Frequency"	N/A				
SYS.DMS(P1SAT-P2P-SUB).43	Verify point "Voltage - Angle - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).44	Verify point "Voltage - Angle - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).45	Verify point "Voltage - Angle - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).46	Verify point "Voltage - Residual"	N/A				
SYS.DMS(P1SAT-P2P-SUB).47	Verify point "Voltage - Angle - Neutral"	N/A				
SYS.DMS(P1SAT-P2P-SUB).48	Verify point "Amps - Angle - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).49	Verify point "Amps - Angle - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).50	Verify point "Amps - Angle - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).51	Verify point "Amps - Neutral"	N/A				
SYS.DMS(P1SAT-P2P-SUB).52	Verify point "Amps - Angle - Neutral"	N/A				
SYS.DMS(P1SAT-P2P-SUB).53	Verify point "Amps - Residual"	N/A				
SYS.DMS(P1SAT-P2P-SUB).54	Verify point "Amps - Angle - Residual"	N/A				
SYS.DMS(P1SAT-P2P-SUB).55	Verify point "Real Power - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).56	Verify point "Real Power - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).57	Verify point "Real Power - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).58	Verify point "Reactive Power - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).59	Verify point "Reactive Power - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).60	Verify point "Reactive Power - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).61	Verify point "Apparent Power - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).62	Verify point "Apparent Power - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).63	Verify point "Apparent Power - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).64	Verify point "Power Factor - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).65	Verify point "Power Factor - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).66	Verify point "Power Factor - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).67	Verify point "Amps - Positive Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).68	Verify point "Amps - Angle - Positive Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).69	Verify point "Amps - Negative Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).70	Verify point "Amps - Angle - Negative Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).71	Verify point "Amps - Zero Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).72	Verify point "Amps - Angle - Zero Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).73	Verify point "Voltage - Positive Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).74	Verify point "Voltage - Angle - Positive Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).75	Verify point "Voltage Negative Sequence"	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).76	Verify point "Voltage - Angle - Negative Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).77	Verify point "Voltage - Zero Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).78	Verify point "Voltage - Angle - Zero Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).79	Verify point "Current Imbalance"	N/A				
SYS.DMS(P1SAT-P2P-SUB).80	Verify point "Voltage Imbalance"	N/A				
SYS.DMS(P1SAT-P2P-SUB).81	Verify point "Amps - Average"	N/A				
SYS.DMS(P1SAT-P2P-SUB).82	Verify point "Amps - Max - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).83	Verify point "Amps - Max - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).84	Verify point "Amps - Max - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).85	Verify point "Amps - Max - Neutral"	N/A				
SYS.DMS(P1SAT-P2P-SUB).86	Verify point "Amps - Max - Residual"	N/A				
SYS.DMS(P1SAT-P2P-SUB).87	Verify point "Amps - Min - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).88	Verify point "Amps - Min - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).89	Verify point "Amps - Min - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).90	Verify point "Amps - Min - Neutral"	N/A				
SYS.DMS(P1SAT-P2P-SUB).91	Verify point "Amps - Min - Residual"	N/A				
SYS.DMS(P1SAT-P2P-SUB).92	Verify point "Voltage - Average"	N/A				
SYS.DMS(P1SAT-P2P-SUB).93	Verify point "Voltage - Max - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).94	Verify point "Voltage - Max - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).95	Verify point "Voltage - Max - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).96	Verify point "Voltage - Min - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).97	Verify point "Voltage - Min - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).98	Verify point "Voltage - Min - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).99	Verify point "Apparent Power - Max - 3 Phase"	N/A				
SYS.DMS(P1SAT-P2P-SUB).100	Verify point "Apparent Power - Min - 3 Phase"	N/A				
SYS.DMS(P1SAT-P2P-SUB).101	Verify point "Real Power - Max - 3 Phase"	N/A				
SYS.DMS(P1SAT-P2P-SUB).102	Verify point "Real Power - Min - 3 Phase"	N/A				
SYS.DMS(P1SAT-P2P-SUB).103	Verify point "Reactive Power - Max - 3 Phase"	N/A				
SYS.DMS(P1SAT-P2P-SUB).104	Verify point "Reactive Power - Min - 3 Phase"	N/A				
SYS.DMS(P1SAT-P2P-SUB).105	Verify point "Amps - Demand - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).106	Verify point "Amps - Demand - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).107	Verify point "Amps - Demand - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).108	Verify point "Amps - Demand - Residual"	N/A				
SYS.DMS(P1SAT-P2P-SUB).109	Verify point "Amps - Peak Demand - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).110	Verify point "Amps - Peak Demand - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).111	Verify point "Amps - Peak Demand - Phase C"	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).112	Verify point "Amps - Peak Demand - Residual"	N/A				
System Test Book - DMS (Phase 1 Site Acceptance Test) - Feeder / Tie Breaker (751A Profile 2) : Status Points						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).113	Verify point "Breaker Status"	Values Displayed: - OPEN - CLOSED				
SYS.DMS(P1SAT-P2P-SUB).114	Verify point "Local Remote"	Values Displayed: - LOCAL - REMOTE				
SYS.DMS(P1SAT-P2P-SUB).115	Verify point "Manual Auto"	Values Displayed: - AUTO - MANUAL				
SYS.DMS(P1SAT-P2P-SUB).116	Verify point "Slow Breaker Indication"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).117	Verify point "Contact Wear"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).118	Verify point "86BT Lockout Operated"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).119	Verify point "Trip Coil Monitor"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).120	Verify point "Latched LED 1"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).121	Verify point "Latched LED 2"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).122	Verify point "Latched LED 3"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).123	Verify point "Latched LED 4"	Values Displayed: - FALSE - TRUE				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).124	Verify point "Latched LED 5"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).125	Verify point "Latched LED 6"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).126	Verify point "Hardware Alarm"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).127	Verify point "Software Alarm"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).128	Verify point "FAULT"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).129	Verify point "Synchronism Check Element 1"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).130	Verify point "Synchronism Check Element 2"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).131	Verify point "Healthy Voltage Vp for Synchronism Check"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).132	Verify point "Healthy Voltage Vs for Synchronism Check"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).133	Verify point "Loss of Potential"	Values Displayed: - FALSE - TRUE				
System Test Book - DMS (Phase 1 Site Acceptance Test) - Feeder / Tie Breaker (751A Profile 2): Control Points						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).134	Verify point "Breaker Open"	Values Displayed: - N/A - OPEN				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).135	Verify point "Breaker Close"	Values Displayed: - N/A - CLOSE				
SYS.DMS(P1SAT-P2P-SUB).136	Verify point "Manual"	Values Displayed: - N/A - MANUAL				
SYS.DMS(P1SAT-P2P-SUB).137	Verify point "Auto"	Values Displayed: - N/A - AUTO				
System Test Book - DMS (Phase 1 Site Acceptance Test) - Feeder / Tie Breaker (751A Profile 2) : Analog Points						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).138	Verify point "Real Power - 3 Phase "	N/A				
SYS.DMS(P1SAT-P2P-SUB).139	Verify point "Reactive Power - 3 Phase "	N/A				
SYS.DMS(P1SAT-P2P-SUB).140	Verify point "Amps - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).141	Verify point "Amps - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).142	Verify point "Amps - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).143	Verify point "Voltage - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).144	Verify point "Voltage - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).145	Verify point "Voltage - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).146	Verify point "Apparent Power - 3 Phase"	N/A				
SYS.DMS(P1SAT-P2P-SUB).147	Verify point "Power Factor - 3 Phase"	N/A				
SYS.DMS(P1SAT-P2P-SUB).148	Verify point "Frequency"	N/A				
SYS.DMS(P1SAT-P2P-SUB).149	Verify point "Voltage - Angle - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).150	Verify point "Voltage - Angle - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).151	Verify point "Voltage - Angle - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).152	Verify point "Voltage - Residual"	N/A				
SYS.DMS(P1SAT-P2P-SUB).153	Verify point "Voltage - Angle - Neutral"	N/A				
SYS.DMS(P1SAT-P2P-SUB).154	Verify point "Amps - Angle - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).155	Verify point "Amps - Angle - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).156	Verify point "Amps - Angle - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).157	Verify point "Amps - Neutral"	N/A				
SYS.DMS(P1SAT-P2P-SUB).158	Verify point "Amps - Angle - Neutral"	N/A				
SYS.DMS(P1SAT-P2P-SUB).159	Verify point "Amps - Residual"	N/A				
SYS.DMS(P1SAT-P2P-SUB).160	Verify point "Amps - Angle - Residual"	N/A				
SYS.DMS(P1SAT-P2P-SUB).161	Verify point "Real Power - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).162	Verify point "Real Power - Phase B"	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).163	Verify point "Real Power - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).164	Verify point "Reactive Power - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).165	Verify point "Reactive Power - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).166	Verify point "Reactive Power - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).167	Verify point "Apparent Power - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).168	Verify point "Apparent Power - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).169	Verify point "Apparent Power - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).170	Verify point "Power Factor - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).171	Verify point "Power Factor - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).172	Verify point "Power Factor - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).173	Verify point "Amps - Positive Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).174	Verify point "Amps - Angle - Positive Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).175	Verify point "Amps - Negative Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).176	Verify point "Amps - Angle - Negative Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).177	Verify point "Amps - Zero Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).178	Verify point "Amps - Angle - Zero Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).179	Verify point "Voltage - Positive Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).180	Verify point "Voltage - Angle - Positive Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).181	Verify point "Voltage Negative Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).182	Verify point "Voltage - Angle - Negative Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).183	Verify point "Voltage - Zero Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).184	Verify point "Voltage - Angle - Zero Sequence"	N/A				
SYS.DMS(P1SAT-P2P-SUB).185	Verify point "Current Imbalance"	N/A				
SYS.DMS(P1SAT-P2P-SUB).186	Verify point "Voltage Imbalance"	N/A				
SYS.DMS(P1SAT-P2P-SUB).187	Verify point "Amps - Average"	N/A				
SYS.DMS(P1SAT-P2P-SUB).188	Verify point "Amps - Max - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).189	Verify point "Amps - Max - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).190	Verify point "Amps - Max - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).191	Verify point "Amps - Max - Neutral"	N/A				
SYS.DMS(P1SAT-P2P-SUB).192	Verify point "Amps - Max - Residual"	N/A				
SYS.DMS(P1SAT-P2P-SUB).193	Verify point "Amps - Min - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).194	Verify point "Amps - Min - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).195	Verify point "Amps - Min - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).196	Verify point "Amps - Min - Neutral"	N/A				
SYS.DMS(P1SAT-P2P-SUB).197	Verify point "Amps - Min - Residual"	N/A				
SYS.DMS(P1SAT-P2P-SUB).198	Verify point "Voltage - Average"	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).199	Verify point "Voltage - Max - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).200	Verify point "Voltage - Max - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).201	Verify point "Voltage - Max - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).202	Verify point "Voltage - Min - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).203	Verify point "Voltage - Min - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).204	Verify point "Voltage - Min - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).205	Verify point "Apparent Power - Max - 3 Phase"	N/A				
SYS.DMS(P1SAT-P2P-SUB).206	Verify point "Apparent Power - Min - 3 Phase"	N/A				
SYS.DMS(P1SAT-P2P-SUB).207	Verify point "Real Power - Max - 3 Phase"	N/A				
SYS.DMS(P1SAT-P2P-SUB).208	Verify point "Real Power - Min - 3 Phase"	N/A				
SYS.DMS(P1SAT-P2P-SUB).209	Verify point "Reactive Power - Max - 3 Phase"	N/A				
SYS.DMS(P1SAT-P2P-SUB).210	Verify point "Reactive Power - Min - 3 Phase"	N/A				
SYS.DMS(P1SAT-P2P-SUB).211	Verify point "Amps - Demand - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).212	Verify point "Amps - Demand - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).213	Verify point "Amps - Demand - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).214	Verify point "Amps - Demand - Residual"	N/A				
SYS.DMS(P1SAT-P2P-SUB).215	Verify point "Amps - Peak Demand - Phase A"	N/A				
SYS.DMS(P1SAT-P2P-SUB).216	Verify point "Amps - Peak Demand - Phase B"	N/A				
SYS.DMS(P1SAT-P2P-SUB).217	Verify point "Amps - Peak Demand - Phase C"	N/A				
SYS.DMS(P1SAT-P2P-SUB).218	Verify point "Amps - Peak Demand - Residual"	N/A				
System Test Book - DMS (Phase 1 Site Acceptance Test) - Substation Main Breaker (451-5)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).219	Verify point "Breaker Status"	Values Displayed: - OPEN - CLOSED				
SYS.DMS(P1SAT-P2P-SUB).220	Verify point "Local Remote"	Values Displayed: - LOCAL - REMOTE				
SYS.DMS(P1SAT-P2P-SUB).221	Verify point "86M Lockout Operated"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).222	Verify point "Slow Breaker Indication"	Values Displayed: - FALSE - TRUE				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).223	Verify point "Loss of Potential"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).224	Verify point "Contact Wear"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).225	Verify point "Hardware Alarm"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).226	Verify point "Software Alarm"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).227	Verify point "Healthy Voltage Vs for Synchornism Check"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).228	Verify point "Healthy Voltage Vp for Synchornism Check"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).229	Verify point "Circuit Breaker 1 Angle 1 within Window 1"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).230	Verify point "Circuit Breaker 1 Angle 2 within Window 2"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).231	Verify point "FAULT"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).232	Verify point "Protection Timer Output 1"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).233	Verify point "Trip Coil Monitor"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).234	Verify point "Protection Timer Output 3"	Values Displayed: - FALSE - TRUE				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).235	Verify point "Protection Timer Output 4"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).236	Verify point "Protection Timer Output 5"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).237	Verify point "Protection Timer Output 6"	Values Displayed: - FALSE - TRUE				
System Test Book - DMS (Phase 1 Site Acceptance Test) - Substation Transformer Differential (487E)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).238	Verify point "Breaker Status"	Values Displayed: - OPEN - CLOSED				
SYS.DMS(P1SAT-P2P-SUB).239	Verify point "Real Power - 3 Phase - Terminal T"	N/A				
SYS.DMS(P1SAT-P2P-SUB).240	Verify point "Reactive Power - 3 Phase - Terminal T"	N/A				
SYS.DMS(P1SAT-P2P-SUB).241	Verify point "Real Power - 3 Phase - Terminal U"	N/A				
SYS.DMS(P1SAT-P2P-SUB).242	Verify point "Reactive Power - 3 Phase - Terminal U"	N/A				
SYS.DMS(P1SAT-P2P-SUB).243	Verify point "Voltage - Phase A - V"	N/A				
SYS.DMS(P1SAT-P2P-SUB).244	Verify point "Voltage - Phase B - V"	N/A				
SYS.DMS(P1SAT-P2P-SUB).245	Verify point "Voltage - Phase C - V"	N/A				
SYS.DMS(P1SAT-P2P-SUB).246	Verify point "Voltage - Phase A - Z"	N/A				
SYS.DMS(P1SAT-P2P-SUB).247	Verify point "Voltage - Phase B - Z"	N/A				
SYS.DMS(P1SAT-P2P-SUB).248	Verify point "Voltage - Phase C - Z"	N/A				
System Test Book - DMS (Phase 1 Site Acceptance Test) - Load Tap Changer (REG-DA)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).249	Verify point "Position Value"	Values Displayed: - -16 - -15				
SYS.DMS(P1SAT-P2P-SUB).250	Verify point "Manual Auto"	Values Displayed: - MANUAL - AUTO				
SYS.DMS(P1SAT-P2P-SUB).251	Verify point "Position Control"	Values Displayed: - STOP - LOWER				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).252	Verify point "Manual Auto"	Values Displayed: - MANUAL - AUTO				
System Test Book - DMS (Phase 1 Site Acceptance Test) - Substation Bus Differential (467-B)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P1SAT-P2P-SUB).253	Verify point "86B Lockout Operated"	Values Displayed: - FALSE - TRUE				
SYS.DMS(P1SAT-P2P-SUB).254	Verify point "Software or Hardware Alarm"	Values Displayed: - FALSE - TRUE				

System Test Book – DMS (Phase 2 Factory Acceptance Test): Redundancy - Verify Configuration						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2FAT-REDUNDANCY).1	Verify system Test Environment (HW & SW), including simulation and tools, before starting FAT	N/A				
SYS.DMS(P2FAT-REDUNDANCY).2	Verify system management and configuration displays and tools	N/A				
System Test Book – DMS (Phase 2 Factory Acceptance Test): Redundancy - Verify System Components, Tools, DBs						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2FAT-REDUNDANCY).3	Verify correct operation of the system components (system configuration overview, servers status, communications status, applications running,....)	N/A				
SYS.DMS(P2FAT-REDUNDANCY).4	Verify redundancy in the system network at each level (CC, Substation)	N/A				
System Test Book – DMS (Phase 2 Factory Acceptance Test): Redundancy - Basic UI (Power CC)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2FAT-REDUNDANCY).5	Verify users log on and log off	N/A				
SYS.DMS(P2FAT-REDUNDANCY).6	Verify only defined users can log on	N/A				
SYS.DMS(P2FAT-REDUNDANCY).7	Verify reporting and logging	N/A				
SYS.DMS(P2FAT-REDUNDANCY).8	Verify Tabular displays availability and access	N/A				
SYS.DMS(P2FAT-REDUNDANCY).9	Verify that at least system logging reporting can be defined and activated	N/A				
SYS.DMS(P2FAT-REDUNDANCY).10	Verify queries, filtering and sorting capabilities in logs and lists	N/A				
SYS.DMS(P2FAT-REDUNDANCY).11	Verification of management functionality for logs and lists	N/A				
SYS.DMS(P2FAT-REDUNDANCY).12	Verify that at least system statistics can be defined and activated	N/A				
System Test Book – DMS (Phase 2 Factory Acceptance Test): Redundancy - Spontaneous Reporting of Selected Data Points						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2FAT-REDUNDANCY).13	Verify that there is no dead band defined in DSCADA	N/A				
SYS.DMS(P2FAT-REDUNDANCY).14	Verify time needed for data presentation and control execution to and from the Control Center	N/A				
SYS.DMS(P2FAT-REDUNDANCY).15	Verify data presented in Tabular displays	N/A				
SYS.DMS(P2FAT-REDUNDANCY).16	Verify alarm and event list access	N/A				
System Test Book – DMS (Phase 2 Factory Acceptance Test): Redundancy - Areas of Responsibilities and Controls						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2FAT-REDUNDANCY).17	Verify reporting and logging of AOR issues and management (authorizations and permissions)	N/A				
SYS.DMS(P2FAT-REDUNDANCY).18	Verification of control action cancellation by the operator	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2FAT-REDUNDANCY).19	Verification of control action time-out	N/A				
SYS.DMS(P2FAT-REDUNDANCY).20	Verification of control action failed	N/A				
SYS.DMS(P2FAT-REDUNDANCY).21	Verify control action propagation in all modules and that execution is synchronized	N/A				
SYS.DMS(P2FAT-REDUNDANCY).22	Verify analog controls (set points), raise/lower (no return),....	N/A				
SYS.DMS(P2FAT-REDUNDANCY).23	Verify control command failures	N/A				
SYS.DMS(P2FAT-REDUNDANCY).24	Verification of system behavior in case of control "rejected" or "failed"	N/A				
SYS.DMS(P2FAT-REDUNDANCY).25	Verify interlocking conditions :Raise/Lower Limit reached	N/A				
SYS.DMS(P2FAT-REDUNDANCY).26	Verify interlocking conditions :Control in Progress	N/A				
SYS.DMS(P2FAT-REDUNDANCY).27	Verify interlocking conditions :Multiple user/consoles	N/A				
SYS.DMS(P2FAT-REDUNDANCY).28	Verify reporting and logging of control actions, successful and failed	N/A				
System Test Book – DMS (Phase 2 Factory Acceptance Test): Redundancy - Manual Changes and Tags						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2FAT-REDUNDANCY).29	Verify validity checking for manual entries	N/A				
SYS.DMS(P2FAT-REDUNDANCY).30	Verify manual changes are updated in all modules (data synchronization)	N/A				
SYS.DMS(P2FAT-REDUNDANCY).31	Verify reporting and logging of manual changes, successful and failed	N/A				
SYS.DMS(P2FAT-REDUNDANCY).32	Verify JC&G functionality	N/A				
SYS.DMS(P2FAT-REDUNDANCY).33	Verify reporting and logging of temporary elements in the model	N/A				
SYS.DMS(P2FAT-REDUNDANCY).34	Verification of tagging propagation to the different modules of the system	N/A				
SYS.DMS(P2FAT-REDUNDANCY).35	Verification of locking conditions when tags are set	N/A				
SYS.DMS(P2FAT-REDUNDANCY).36	Verify reporting and logging of tagging actions	N/A				
System Test Book – DMS (Phase 2 Factory Acceptance Test): Redundancy - Time Synchronization						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2FAT-REDUNDANCY).37	Verify time synch reporting and logging when it happens	N/A				
System Test Book – DMS (Phase 2 Factory Acceptance Test): Redundancy - ICCP						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2FAT-REDUNDANCY).38	Verification of the association table definition	N/A				
SYS.DMS(P2FAT-REDUNDANCY).39	Verification of association table definition error's reporting	N/A				
SYS.DMS(P2FAT-REDUNDANCY).40	Verification of the data flow through ICCP link, checking the different types of data in both directions	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2FAT-REDUNDANCY).41	Verification ICCP link status display	N/A				
SYS.DMS(P2FAT-REDUNDANCY).42	Verification of the ICCP link management	N/A				
SYS.DMS(P2FAT-REDUNDANCY).43	Verification of the ICCP link redundancy	N/A				
SYS.DMS(P2FAT-REDUNDANCY).44	Verification communications error reporting	N/A				
System Test Book – DMS (Phase 2 Factory Acceptance Test): Redundancy - Switch Mastership						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2FAT-REDUNDANCY).45	Manually Switch Mastership (switch PowerCC Master and Standby)	N/A				
SYS.DMS(P2FAT-REDUNDANCY).46	DCADA Manually Switch Mastership (switch PowerCC Master and Standby)	N/A				
System Test Book – DMS (Phase 2 Factory Acceptance Test): Redundancy - Communications Failover						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2FAT-REDUNDANCY).47	Verify status reporting and logging at the CC	N/A				
SYS.DMS(P2FAT-REDUNDANCY).48	Verify system response to communication failure at the IED side (port unavailable, tropos router down,....)	N/A				
SYS.DMS(P2FAT-REDUNDANCY).49	Verify communication management capabilities like force DNP3 scan, force alternative communication path	N/A				
SYS.DMS(P2FAT-REDUNDANCY).50	Verify status reporting and logging at the HMI and CC	N/A				
SYS.DMS(P2FAT-REDUNDANCY).51	Verify status reporting and logging at the CC	N/A				
System Test Book – DMS (Phase 2 Factory Acceptance Test): Redundancy - Application Failover						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2FAT-REDUNDANCY).52	Verify data is correct after failover at all levels of redundancy	N/A				
SYS.DMS(P2FAT-REDUNDANCY).53	Verify InService redundancy and failover when problems exist in the application or SW	N/A				
SYS.DMS(P2FAT-REDUNDANCY).54	Verify manual InService failover	N/A				
SYS.DMS(P2FAT-REDUNDANCY).55	Verify alarms availability and retention during and after failovers	N/A				
SYS.DMS(P2FAT-REDUNDANCY).56	Verify error handling and redundancy for reporting function	N/A				
SYS.DMS(P2FAT-REDUNDANCY).57	Verify logging of reporting activities	N/A				
System Test Book – DMS (Phase 2 Factory Acceptance Test): Redundancy - DB Management and Model Propagation						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2FAT-REDUNDANCY).58	Based on the DB generation process defined and provided by Siemens and Intergraph, verify that the data definition and DB generation works across all systems and modules	N/A				
SYS.DMS(P2FAT-REDUNDANCY).59	Verify display management	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2FAT-REDUNDANCY).60	Verify general system DB management tools provided with the system (DB Jobs, DB Job propagation, DB Job roll back)	N/A				
SYS.DMS(P2FAT-REDUNDANCY).61	Verify DB error reporting and logging	N/A				
System Test Book – DMS (Phase 2 Factory Acceptance Test): Redundancy – Backup & Restore						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2FAT-REDUNDANCY).62	Verify DB archiving	N/A				
SYS.DMS(P2FAT-REDUNDANCY).63	Verify system tools to backup and restore SW and data	N/A				
SYS.DMS(P2FAT-REDUNDANCY).64	Verify reporting and logging of archiving and restoration activities	N/A				
SYS.DMS(P2FAT-REDUNDANCY).65	Verify system tools to save reports to external media	N/A				
System Test Book – DMS (Phase 2 Factory Acceptance Test): Redundancy - LAN Failures						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2FAT-REDUNDANCY).66	LAN Failure (single and double)	N/A				
SYS.DMS(P2FAT-REDUNDANCY).67	DCADA LAN Failure (single and double)	N/A				
SYS.DMS(P2FAT-REDUNDANCY).68	Verify SCADA applications operation	N/A				
SYS.DMS(P2FAT-REDUNDANCY).69	Verify communication with SICAM and check correct recovery from LAN failure	N/A				
SYS.DMS(P2FAT-REDUNDANCY).70	Verify operation with InService when LAN fails and after correct recovery	N/A				
SYS.DMS(P2FAT-REDUNDANCY).71	Verify status reporting and logging	N/A				
System Test Book – DMS (Phase 2 Factory Acceptance Test): Redundancy - System Startups						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2FAT-REDUNDANCY).72	Automatic Startup - UI Client (PowerCC starts after restarting windows)	N/A				
SYS.DMS(P2FAT-REDUNDANCY).73	DCADA Manual Startup (Manually start PowerCC server)	N/A				
SYS.DMS(P2FAT-REDUNDANCY).74	DCADA Automatic Startup - DMS Master (PowerCC starts after restarting windows)	N/A				
SYS.DMS(P2FAT-REDUNDANCY).75	DCADA Automatic Startup - DMS Standby (PowerCC starts after restarting windows)	N/A				
System Test Book – DMS (Phase 2 Factory Acceptance Test): Redundancy - Availability : Power Failure						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2FAT-REDUNDANCY).76	Verify system behavior during individual servers power failures	N/A				
SYS.DMS(P2FAT-REDUNDANCY).77	Verify applications run up to operational status without human intervention after power failure	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2FAT-REDUNDANCY).78	After Power Failure, verify that IED scanning is happening and data is correct not only that the application is running.	N/A				
System Test Book – DMS (Phase 2 Factory Acceptance Test): Redundancy - System Cold/Start Up						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2FAT-REDUNDANCY).79	Verify execution of the System Start Up procedure	N/A				
SYS.DMS(P2FAT-REDUNDANCY).80	Verify SCADA applications and InService run up to operational status without human intervention after power failure	N/A				
SYS.DMS(P2FAT-REDUNDANCY).81	Verify SICAM status changes are reported and logged at the CC and HMI	N/A				

System Test Book – DMS (Phase 2 Factory Acceptance Test): Consolidated UI – Digital Indication Change						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS.P2FAT.UI.1	Identify a breaker. Simulate opening of the breaker (status) in IED.	The breaker is shown open in InService Map. An alarm is generated in the iAlarm list showing the breaker OPEN.				
SYS.DMS.P2FAT.UI.2	Simulate closing of the breaker.	Breaker is shown closed in map. An alarm is generated in the iAlarm list showing the breaker CLOSE.				
SYS.DMS.P2FAT.UI.3	Simulate Local/Remote status of the breaker to 'Local'.	Local/Remote Flag is shown 'Local' in the properties window of the Breaker. An alarm is generated in the iAlarm list showing the change in status.				
SYS.DMS.P2FAT.UI.4	Simulate Local/Remote status of the breaker to 'Remote'.	Local/Remote status is shown 'Remote' in the properties window of the Breaker. An alarm is generated in the iAlarm list showing the change in status.				
SYS.DMS.P2FAT.UI.5	Simulate a digital status change such that an alarm such as 'High Current Lockout' is set in IED.	Status is shown 'True' in properties window for the Breaker. An alarm is generated in the iAlarm list showing the alarm condition.				
SYS.DMS.P2FAT.UI.6	Clear the alarm condition in IED.	Status is shown 'False' in properties window for the Breaker. An alarm is generated in the iAlarm list showing the alarm disappear condition.				
SYS.DMS.P2FAT.UI.7	Simulate a change in the Tap Position for a tap changer.	The Tap position is shown in properties window for device.				
SYS.DMS.P2FAT.UI.8	Simulate a change of the Manual/Auto status for a Tap or Breaker to 'Auto'.	Manual/Auto status is shown as 'Auto' in the properties window of the Tap or Breaker. An alarm is generated in the iAlarm list showing the change in status.				
SYS.DMS.P2FAT.UI.9	Simulate a change of the Manual/Auto status for a Tap or Breaker to 'Manual'.	Manual/Auto status is shown as 'Man-ual' in the properties window of the Tap or Breaker. An alarm is generated in the iAlarm list showing the change in status.				
System Test Book – DMS (Phase 2 Factory Acceptance Test): Consolidated UI – Analog Change						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS.P2FAT.UI.10	Identify a device such as a breaker in the InService map. Simulate a change in an analog measurement (eg Amps – Phase A) associated with the device, in the IED associated with the device.	The corresponding measurement is shown in the properties window of the Breaker. The measurement is associated with the correct phase.				
SYS.DMS.P2FAT.UI.11	Simulate a change in the measurement such that the measurement is out of high limit.	The corresponding measurement is shown in the properties window of the Breaker. An alarm is generated showing the limit violation.				
SYS.DMS.P2FAT.UI.12	Change the measurement such that the measurement is within limits.	The corresponding measurement is shown in the properties window of the Breaker. An alarm is generated showing return to limits for the measurement.				
SYS.DMS.P2FAT.UI.13	Simulate a change in the measurement such that the measurement is out of low limit.	The corresponding measurement is shown in the properties window of the Breaker. An alarm is generated showing the limit violation.				
SYS.DMS.P2FAT.UI.14	Change the measurement such that the measurement is within limits.	The corresponding measurement is shown in the properties window of the Breaker. An alarm is generated showing return to limits for the measurement.				
System Test Book – DMS (Phase 2 Factory Acceptance Test): Consolidated UI – Controls						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS.P2FAT.UI.15	Identify a breaker on map that can be remotely operated. Using iDispatcher Open dialog, open the breaker.	Operation is successful. Breaker is shown Open in the UI. A message is generated in the message log.				
SYS.DMS.P2FAT.UI.16	Close the Breaker using Close dialog from InService menu.	Operation is successful. Breaker is shown Closed in the UI. A message is generated in the message log.				
SYS.DMS.P2FAT.UI.17	Configure the IED or SICAM PAS, so that control for Breaker would be rejected. Then try to Open the breaker using InService Open dialog.	Operation is unsuccessful. Breaker still shows Closed. An alarm is generated showing operation failure.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS.P2FAT.UI.18	Identify a device that supports ManualAuto controls. Using InService UI, set the state of the device to Manual.	Operation is successful. ManualAuto status is shown as Manual in the properties window of the device. A message is generated in the message log.				
SYS.DMS.P2FAT.UI.19	Change the ManualAuto from the previous step to Auto.	Operation is successful. ManualAuto status is shown as Auto in the properties window of the device. A message is generated in the message log.				
SYS.DMS.P2FAT.UI.20	Raise Tap position of a Tap.	The Tap position is raised and is reflected in the properties window of the device.				
SYS.DMS.P2FAT.UI.21	Lower Tap position of a Tap.	The Tap position is lowered and is reflected in the properties window of the device.				

System Test Book - DMS (Phase 2 Site Acceptance Test) - Capacitor Bank Point to Point Checkout: Profile 1 - DI						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-P2P-CB).1	Verify point "Device Status"	Values Displayed: - OPEN - CLOSED				
SYS.DMS(P2SAT-P2P-CB).2	Verify point "Auto - Manual Status"	Values Displayed: - MANUAL - AUTO				
SYS.DMS(P2SAT-P2P-CB).3	Verify point "Local - Remote"	Values Displayed: - LOCAL - REMOTE				
SYS.DMS(P2SAT-P2P-CB).4	Verify point "Alarm Summary"	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-CB).5	Verify point "SCADA Override Status"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P2SAT-P2P-CB).6	Verify point "Over Voltage"	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-CB).7	Verify point "Under Voltage"	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-CB).8	Verify point "Emergency Voltage Override"	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-CB).9	Verify point "Reclose Block"	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-CB).10	Verify point "Maximum Daily Cycles"	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-CB).11	Verify point "Load Fuse Blown"	Values Displayed: - OK - ALARM				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-P2P-CB).12	Verify point "Temperature Sensor Error "	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-CB).13	Verify point "Neutral Sensor - Lockout"	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-CB).14	Verify point "Neutral Sensor - Continuous "	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-CB).15	Verify point "Neutral Sensor - Zero "	Values Displayed: - OK - ALARM				
System Test Book - DMS (Phase 2 Site Acceptance Test) - Capacitor Bank Point to Point Checkout: Profile 1 - DO						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-P2P-CB).16	Verify point "Device Operate"	Values Displayed: - OPEN - CLOSED				
SYS.DMS(P2SAT-P2P-CB).17	Verify point "Auto - Manual"	Values Displayed: - MANUAL - AUTO				
SYS.DMS(P2SAT-P2P-CB).18	Verify point "SCADA Override Mode"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P2SAT-P2P-CB).19	Verify point "Reset Neutral Lockout"	Values Displayed: - NA - RESET				
SYS.DMS(P2SAT-P2P-CB).20	Verify point "Reset Alarms"	Values Displayed: - NA - RESET				
SYS.DMS(P2SAT-P2P-CB).21	Verify point "Inhibit Automatic Operation Timer"	Values Displayed: - DISABLED - ENABLED				
System Test Book - DMS (Phase 2 Site Acceptance Test) - Capacitor Bank Point to Point Checkout: Profile 1 - AI						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-P2P-CB).22	Verify point "Control Strategy"	N/A				
SYS.DMS(P2SAT-P2P-CB).23	Verify point "Voltage - Secondary"	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-P2P-CB).24	Verify point "Time Remaining in SCADA Override Mode"	N/A				
SYS.DMS(P2SAT-P2P-CB).25	Verify point "Current - Neutral RMS - Fundamental"	N/A				
SYS.DMS(P2SAT-P2P-CB).26	Verify point "THD - Voltage"	N/A				
SYS.DMS(P2SAT-P2P-CB).27	Verify point "THD - Neutral"	N/A				
SYS.DMS(P2SAT-P2P-CB).28	Verify point "Current - Neutral RMS - Total"	N/A				
SYS.DMS(P2SAT-P2P-CB).29	Verify point "Last Switch Operation Reason"	N/A				
System Test Book - DMS (Phase 2 Site Acceptance Test) - Capacitor Bank Point to Point Checkout: Profile 2 - DI						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-P2P-CB).1	Verify point "Device Status"	Values Displayed: - OPEN - CLOSED				
SYS.DMS(P2SAT-P2P-CB).2	Verify point "Auto - Manual Status"	Values Displayed: - MANUAL - AUTO				
SYS.DMS(P2SAT-P2P-CB).3	Verify point "Local - Remote"	Values Displayed: - LOCAL - REMOTE				
SYS.DMS(P2SAT-P2P-CB).4	Verify point "Alarm Summary"	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-CB).5	Verify point "SCADA Override Status"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P2SAT-P2P-CB).6	Verify point "Over Voltage"	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-CB).7	Verify point "Under Voltage"	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-CB).8	Verify point "Emergency Voltage Override "	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-CB).9	Verify point "Reclose Block"	Values Displayed: - OK - ALARM				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-P2P-CB).10	Verify point "Maximum Daily Cycles"	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-CB).11	Verify point "Load Fuse Blown"	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-CB).12	Verify point "Temperature Sensor Error "	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-CB).13	Verify point "Neutral Sensor - Option"	Values Displayed: - NOT PRESENT - PRESENT				
SYS.DMS(P2SAT-P2P-CB).14	Verify point "Neutral Sensor - Lockout"	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-CB).15	Verify point "Neutral Sensor - Continuous"	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-CB).16	Verify point "Neutral Sensor - Zero "	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-CB).17	Verify point "VAR Option"	Values Displayed: - NOT PRESENT - PRESENT				
SYS.DMS(P2SAT-P2P-CB).18	Verify point "Current Direction"	Values Displayed: - NORMAL - REVERSED				
SYS.DMS(P2SAT-P2P-CB).19	Verify point "Low Switching VAR Delta"	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-CB).20	Verify point "Current Sensor Location"	Values Displayed: - SOURCE - LOAD				
System Test Book - DMS (Phase 2 Site Acceptance Test) - Capacitor Bank Point to Point Checkout: Profile 2 - DO						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-P2P-CB).21	Verify point "Device Operate"	Values Displayed: - OPEN - CLOSED				
SYS.DMS(P2SAT-P2P-CB).22	Verify point "Auto - Manual"	Values Displayed: - MANUAL - AUTO				
SYS.DMS(P2SAT-P2P-CB).23	Verify point "SCADA Override Mode"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P2SAT-P2P-CB).24	Verify point "Reset Neutral Lockout"	Values Displayed: - NA - RESET				
SYS.DMS(P2SAT-P2P-CB).25	Verify point "Reset Alarms"	Values Displayed: - NA - RESET				
SYS.DMS(P2SAT-P2P-CB).26	Verify point "Inhibit Automatic Operation Timer"	Values Displayed: - DISABLED - ENABLED				
System Test Book - DMS (Phase 2 Site Acceptance Test) - Capacitor Bank Point to Point Checkout: Profile 2 - AI						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-P2P-CB).27	Verify point "Control Strategy"	N/A				
SYS.DMS(P2SAT-P2P-CB).28	Verify point "Voltage - Secondary"	N/A				
SYS.DMS(P2SAT-P2P-CB).29	Verify point "Voltage - Primary"	N/A				
SYS.DMS(P2SAT-P2P-CB).30	Verify point "Time Remaining in SCADA Override Mode"	N/A				
SYS.DMS(P2SAT-P2P-CB).31	Verify point "Current - Neutral RMS - Fundamental"	N/A				
SYS.DMS(P2SAT-P2P-CB).32	Verify point "Current - Phase A"	N/A				
SYS.DMS(P2SAT-P2P-CB).33	Verify point "Reactive Power - 3 Phase"	N/A				
SYS.DMS(P2SAT-P2P-CB).34	Verify point "Apparent Power - 3 Phase"	N/A				
SYS.DMS(P2SAT-P2P-CB).35	Verify point "Real Power - 3 Phase"	N/A				
SYS.DMS(P2SAT-P2P-CB).36	Verify point "THD - Voltage"	N/A				
SYS.DMS(P2SAT-P2P-CB).37	Verify point "THD - Current"	N/A				
SYS.DMS(P2SAT-P2P-CB).38	Verify point "THD - Neutral"	N/A				
SYS.DMS(P2SAT-P2P-CB).39	Verify point "Current - Neutral RMS - Total"	N/A				
SYS.DMS(P2SAT-P2P-CB).40	Verify point "Last Switch Operation Reason"	N/A				

System Test Book - DMS (Phase 2 Site Acceptance Test) - FCI Point to Point Checkout: Profile 0 - DI						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-P2P-FCI).1	Verify point "FCI Comm Failure"	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-FCI).2	Verify point "Smart Controller Reporter Operational "	Values Displayed: - OK - ALARM				
SYS.DMS(P2SAT-P2P-FCI).3	Verify point "Voltage - Low DC"	Values Displayed: - OK - ALARM				
System Test Book - DMS (Phase 2 Site Acceptance Test) - FCI Point to Point Checkout: Profile 0 - DO						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-P2P-FCI).4	Verify point "Device Operate"	Values Displayed: - NA - RESET				
SYS.DMS(P2SAT-P2P-FCI).5	Verify point "Auto - Manual"	Values Displayed: - NA - RESET				
SYS.DMS(P2SAT-P2P-FCI).6	Verify point "SCADA Override Mode"	Values Displayed: - NA - RESET				
System Test Book - DMS (Phase 2 Site Acceptance Test) - FCI Point to Point Checkout: Profile 0 - AI						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-P2P-FCI).7	Verify point "Device Status"	N/A				
SYS.DMS(P2SAT-P2P-FCI).8	Verify point "Auto - Manual Status"	N/A				
System Test Book - DMS (Phase 2 Site Acceptance Test) - FCI Point to Point Checkout: Profile 3 - DI						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-P2P-FCI).1	Verify point "Over Current - Phase A"	Values Displayed: - OK - FAULT				
SYS.DMS(P2SAT-P2P-FCI).2	Verify point "Permanent Fault - Phase A"	Values Displayed: - OK - FAULT				
SYS.DMS(P2SAT-P2P-FCI).3	Verify point "Momentary Fault - Phase A"	Values Displayed: - OK - FAULT				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-P2P-FCI).4	Verify point "Overhead Line Current Loss - Phase A"	Values Displayed: - OK - LOSS OF CURRENT				
SYS.DMS(P2SAT-P2P-FCI).5	Verify point "Loss of Voltage - Phase A"	Values Displayed: - OK - LOSS OF VOLTAGE				
SYS.DMS(P2SAT-P2P-FCI).6	Verify point "Over Current - Phase B"	Values Displayed: - OK - FAULT				
SYS.DMS(P2SAT-P2P-FCI).7	Verify point "Permanent Fault - Phase B"	Values Displayed: - OK - FAULT				
SYS.DMS(P2SAT-P2P-FCI).8	Verify point "Momentary Fault - Phase B"	Values Displayed: - OK - FAULT				
SYS.DMS(P2SAT-P2P-FCI).9	Verify point "Overhead Line Current Loss - Phase B"	Values Displayed: - OK - LOSS OF CURRENT				
SYS.DMS(P2SAT-P2P-FCI).10	Verify point "Loss of Voltage - Phase B"	Values Displayed: - OK - LOSS OF VOLTAGE				
SYS.DMS(P2SAT-P2P-FCI).11	Verify point "Over Current - Phase C"	Values Displayed: - OK - FAULT				
SYS.DMS(P2SAT-P2P-FCI).12	Verify point "Permanent Fault - Phase C"	Values Displayed: - OK - FAULT				
SYS.DMS(P2SAT-P2P-FCI).13	Verify point "Momentary Fault - Phase C"	Values Displayed: - OK - FAULT				
SYS.DMS(P2SAT-P2P-FCI).14	Verify point "Overhead Line Current Loss - Phase C"	Values Displayed: - OK - LOSS OF CURRENT				
SYS.DMS(P2SAT-P2P-FCI).15	Verify point "Loss of Voltage - Phase C"	Values Displayed: - OK - LOSS OF VOLTAGE				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
System Test Book - DMS (Phase 2 Site Acceptance Test) - FCI Point to Point Checkout: Profile 3 - CTR						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-P2P-FCI).16	Verify point "Temporary Faults - Phase A"	N/A				
SYS.DMS(P2SAT-P2P-FCI).17	Verify point "Permanent Faults - Phase A"	N/A				
SYS.DMS(P2SAT-P2P-FCI).18	Verify point "Temporary Faults - Phase B"	N/A				
SYS.DMS(P2SAT-P2P-FCI).19	Verify point "Permanent Faults - Phase B"	N/A				
SYS.DMS(P2SAT-P2P-FCI).20	Verify point "Temporary Faults - Phase C"	N/A				
SYS.DMS(P2SAT-P2P-FCI).21	Verify point "Permanent Faults - Phase C"	N/A				
System Test Book - DMS (Phase 2 Site Acceptance Test) - FCI Point to Point Checkout: Profile 3 - AI						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-P2P-FCI).21	Verify point "Fault Current - Phase A"	N/A				
SYS.DMS(P2SAT-P2P-FCI).22	Verify point "Fault Duration - Phase A"	N/A				
SYS.DMS(P2SAT-P2P-FCI).23	Verify point "Last Known Good Current - Phase A"	N/A				
SYS.DMS(P2SAT-P2P-FCI).24	Verify point "Current - Average - Phase A"	N/A				
SYS.DMS(P2SAT-P2P-FCI).25	Verify point "Fault Current - Phase B"	N/A				
SYS.DMS(P2SAT-P2P-FCI).26	Verify point "Fault Duration - Phase B"	N/A				
SYS.DMS(P2SAT-P2P-FCI).27	Verify point "Last Known Good Current - Phase B"	N/A				
SYS.DMS(P2SAT-P2P-FCI).28	Verify point "Current - Average - Phase B"	N/A				
SYS.DMS(P2SAT-P2P-FCI).29	Verify point "Fault Current - Phase C"	N/A				
SYS.DMS(P2SAT-P2P-FCI).30	Verify point "Fault Duration - Phase C"	N/A				
SYS.DMS(P2SAT-P2P-FCI).31	Verify point "Last Known Good Current - Phase C"	N/A				
SYS.DMS(P2SAT-P2P-FCI).32	Verify point "Current - Average - Phase C"	N/A				

System Test Book – DMS (Phase 2 Site Acceptance Test): Redundancy - Verify Configuration						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-REDUNDANCY).1	Verify system Test Environment (HW & SW), including simulation and tools, before starting FAT	N/A				
SYS.DMS(P2SAT-REDUNDANCY).2	Verify system management and configuration displays and tools	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Redundancy - Verify System Components, Tools, DBs						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-REDUNDANCY).3	Verify correct operation of the system components (system configuration overview, servers status, communications status, applications running)	N/A				
SYS.DMS(P2SAT-REDUNDANCY).4	Verify redundancy in the system network at each level (CC, Substation)	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Redundancy - Basic UI (Power CC)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-REDUNDANCY).5	Verify users log on and log off	N/A				
SYS.DMS(P2SAT-REDUNDANCY).6	Verify only defined users can log on	N/A				
SYS.DMS(P2SAT-REDUNDANCY).7	Verify reporting and logging	N/A				
SYS.DMS(P2SAT-REDUNDANCY).8	Verify Tabular displays availability and access	N/A				
SYS.DMS(P2SAT-REDUNDANCY).9	Verify that at least system logging reporting can be defined and activated	N/A				
SYS.DMS(P2SAT-REDUNDANCY).10	Verify queries, filtering and sorting capabilities in logs and lists	N/A				
SYS.DMS(P2SAT-REDUNDANCY).11	Verification of management functionality for logs and lists	N/A				
SYS.DMS(P2SAT-REDUNDANCY).12	Verify that at least system statistics can be defined and activated	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Redundancy - Spontaneous Reporting of Selected Data Points						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-REDUNDANCY).13	Verify that there is no dead band defined in DSCADA	N/A				
SYS.DMS(P2SAT-REDUNDANCY).14	Verify time needed for data presentation and control execution to and from the Control Center	N/A				
SYS.DMS(P2SAT-REDUNDANCY).15	Verify data presented in Tabular displays	N/A				
SYS.DMS(P2SAT-REDUNDANCY).16	Verify alarm and event list access	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Redundancy - Areas of Responsibilities and Controls						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-REDUNDANCY).17	Verify reporting and logging of AOR issues and management (authorizations and permissions)	N/A				
SYS.DMS(P2SAT-REDUNDANCY).18	Verification of control action cancellation by the operator	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-REDUNDANCY).19	Verification of control action time-out	N/A				
SYS.DMS(P2SAT-REDUNDANCY).20	Verification of control action failed	N/A				
SYS.DMS(P2SAT-REDUNDANCY).21	Verify control action propagation in all modules and that execution is synchronized	N/A				
SYS.DMS(P2SAT-REDUNDANCY).22	Verify analog controls (set points), raise/lower (no return)	N/A				
SYS.DMS(P2SAT-REDUNDANCY).23	Verify control command failures	N/A				
SYS.DMS(P2SAT-REDUNDANCY).24	Verification of system behavior in case of control "rejected" or "failed"	N/A				
SYS.DMS(P2SAT-REDUNDANCY).25	Verify interlocking conditions: Raise/Lower Limit reached	N/A				
SYS.DMS(P2SAT-REDUNDANCY).26	Verify interlocking conditions: Control in Progress	N/A				
SYS.DMS(P2SAT-REDUNDANCY).27	Verify interlocking conditions: Multiple user/consoles	N/A				
SYS.DMS(P2SAT-REDUNDANCY).28	Verify reporting and logging of control actions, successful and failed	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Redundancy - Manual Changes and Tags						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-REDUNDANCY).29	Verify validity checking for manual entries	N/A				
SYS.DMS(P2SAT-REDUNDANCY).30	Verify manual changes are updated in all modules (data synchronization)	N/A				
SYS.DMS(P2SAT-REDUNDANCY).31	Verify reporting and logging of manual changes, successful and failed	N/A				
SYS.DMS(P2SAT-REDUNDANCY).32	Verify JC&G functionality	N/A				
SYS.DMS(P2SAT-REDUNDANCY).33	Verify reporting and logging of temporary elements in the model	N/A				
SYS.DMS(P2SAT-REDUNDANCY).34	Verification of tagging propagation to the different modules of the system	N/A				
SYS.DMS(P2SAT-REDUNDANCY).35	Verification of locking conditions when tags are set	N/A				
SYS.DMS(P2SAT-REDUNDANCY).36	Verify reporting and logging of tagging actions	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Redundancy - Time Synchronization						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-REDUNDANCY).37	Verify time synch reporting and logging when it happens	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Redundancy - ICCP						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-REDUNDANCY).38	Verification of the association table definition	N/A				
SYS.DMS(P2SAT-REDUNDANCY).39	Verification of association table definition error's reporting	N/A				
SYS.DMS(P2SAT-REDUNDANCY).40	Verification of the data flow through ICCP link, checking the different types of data in both directions.	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-REDUNDANCY).41	Verification ICCP link status display	N/A				
SYS.DMS(P2SAT-REDUNDANCY).42	Verification of the ICCP link management	N/A				
SYS.DMS(P2SAT-REDUNDANCY).43	Verification of the ICCP link redundancy	N/A				
SYS.DMS(P2SAT-REDUNDANCY).44	Verification communications error reporting	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Redundancy - Switch Mastership						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-REDUNDANCY).45	Manually Switch Mastership (switch PowerCC Master and Standby)	N/A				
SYS.DMS(P2SAT-REDUNDANCY).46	DCADA Manually Switch Mastership (switch PowerCC Master and Standby)	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Redundancy - Communications Failover						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-REDUNDANCY).47	Verify status reporting and logging at the CC	N/A				
SYS.DMS(P2SAT-REDUNDANCY).48	Verify system response to communication failure at the IED side (port unavailable, tropos router down)	N/A				
SYS.DMS(P2SAT-REDUNDANCY).49	Verify communication management capabilities like force DNP3 scan, force alternative communication path	N/A				
SYS.DMS(P2SAT-REDUNDANCY).50	Verify status reporting and logging at the HMI and CC	N/A				
SYS.DMS(P2SAT-REDUNDANCY).51	Verify status reporting and logging at the CC	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Redundancy - Application Failover						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-REDUNDANCY).52	Verify data is correct after failover at all levels of redundancy	N/A				
SYS.DMS(P2SAT-REDUNDANCY).53	Verify InService redundancy and failover when problems exist in the application or SW	N/A				
SYS.DMS(P2SAT-REDUNDANCY).54	Verify manual InService failover	N/A				
SYS.DMS(P2SAT-REDUNDANCY).55	Verify alarms availability and retention during and after failovers	N/A				
SYS.DMS(P2SAT-REDUNDANCY).56	Verify error handling and redundancy for reporting function	N/A				
SYS.DMS(P2SAT-REDUNDANCY).57	Verify logging of reporting activities	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Redundancy - DB Management and Model Propagation						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-REDUNDANCY).58	Based on the DB generation process defined and provided by Siemens and Intergraph, verify that the data definition and DB generation works across all systems and modules	N/A				
SYS.DMS(P2SAT-REDUNDANCY).59	Verify display management	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-REDUNDANCY).60	Verify general system DB management tools provided with the system (DB Jobs, DB Job propagation, DB Job roll back)	N/A				
SYS.DMS(P2SAT-REDUNDANCY).61	Verify DB error reporting and logging	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Redundancy - Backup & Restore						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-REDUNDANCY).62	Verify DB archiving	N/A				
SYS.DMS(P2SAT-REDUNDANCY).63	Verify system tools to backup and restore SW and data	N/A				
SYS.DMS(P2SAT-REDUNDANCY).64	Verify reporting and logging of archiving and restoration activities	N/A				
SYS.DMS(P2SAT-REDUNDANCY).65	Verify system tools to save reports to external media	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Redundancy - LAN Failures						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-REDUNDANCY).66	LAN Failure (single and double)	N/A				
SYS.DMS(P2SAT-REDUNDANCY).67	DCADA LAN Failure (single and double)	N/A				
SYS.DMS(P2SAT-REDUNDANCY).68	Verify SCADA applications operation	N/A				
SYS.DMS(P2SAT-REDUNDANCY).69	Verify communication with SICAM and check correct recovery from LAN failure	N/A				
SYS.DMS(P2SAT-REDUNDANCY).70	Verify operation with InService when LAN fails and after correct recovery	N/A				
SYS.DMS(P2SAT-REDUNDANCY).71	Verify status reporting and logging	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Redundancy - System Startups						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-REDUNDANCY).72	Automatic Startup - UI Client (PowerCC starts after restarting windows)	N/A				
SYS.DMS(P2SAT-REDUNDANCY).73	DCADA Manual Startup (Manually start PowerCC server)	N/A				
SYS.DMS(P2SAT-REDUNDANCY).74	DCADA Automatic Startup - DMS Master (PowerCC starts after restarting windows)	N/A				
SYS.DMS(P2SAT-REDUNDANCY).75	DCADA Automatic Startup - DMS Standby (PowerCC starts after restarting windows)	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Redundancy - Availability : Power Failure						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-REDUNDANCY).76	Verify system behavior during individual servers power failures	N/A				
SYS.DMS(P2SAT-REDUNDANCY).77	Verify applications run up to operational status without human intervention after power failure	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-REDUNDANCY).78	After Power Failure, verify that IED scanning is happening and data is correct not only that the application is running	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Redundancy - System Cold/Start Up						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-REDUNDANCY).79	Verify execution of the System Start Up procedure	N/A				
SYS.DMS(P2SAT-REDUNDANCY).80	Verify SCADA applications and InService run up to operational status without human intervention after power failure	N/A				
SYS.DMS(P2SAT-REDUNDANCY).81	Verify SICAM status changes are reported and logged at the CC and HMI	N/A				

System Test Book – DMS (Phase 2 Site Acceptance Test): Integrated UI – Verify System Components, Tools, DBs						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-UI).1	Verify correct operation of the system components (servers status, system configuration overview, communications status, applications running)	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Integrated UI – Basic UI						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-UI).2	Verify navigational functions in InService	N/A				
SYS.DMS(P2SAT-UI).3	Verify Tabular displays availability and access	N/A				
SYS.DMS(P2SAT-UI).4	Verify geographical queries in InService	N/A				
SYS.DMS(P2SAT-UI).5	Verify alarm list functions like filtering, queries, paging	N/A				
SYS.DMS(P2SAT-UI).6	Verify definition and use of KCPL defined help screens	N/A				
SYS.DMS(P2SAT-UI).7	Verify queries, filtering and sorting capabilities in logs and lists	N/A				
SYS.DMS(P2SAT-UI).8	Digital Indication Change	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Integrated UI – Spontaneous Reporting of Selected Data Points						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-UI).9	Verify status reporting and logging at the HMI and CC	N/A				
SYS.DMS(P2SAT-UI).10	Verify all the alarm types and event reporting caused by data processing	N/A				
SYS.DMS(P2SAT-UI).11	Verify alarm events	N/A				
SYS.DMS(P2SAT-UI).12	Verify time needed for data presentation and control execution to and from the Control Center	N/A				
SYS.DMS(P2SAT-UI).13	Verify value representation, values and data quality	N/A				
SYS.DMS(P2SAT-UI).14	Verify data presented in Tabular displays	N/A				
SYS.DMS(P2SAT-UI).15	Verify alarm and event list access	N/A				
SYS.DMS(P2SAT-UI).16	Verify different types of alarms and events	N/A				
SYS.DMS(P2SAT-UI).17	Verify alarm management capabilities (acknowledge, deletion)	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Integrated UI – Areas of Responsibilities and Controls						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-UI).19	Verify configuration of AORs and permissions for different users	N/A				
SYS.DMS(P2SAT-UI).20	Verify change in AOR	N/A				
SYS.DMS(P2SAT-UI).21	Verify authorization and permission changes for an AOR	N/A				
SYS.DMS(P2SAT-UI).22	Verify reporting and logging of AOR issues and management (authorizations and permissions)	N/A				
SYS.DMS(P2SAT-UI).23	Verify control action procedure	N/A				
SYS.DMS(P2SAT-UI).24	Verification of control action in progress representation in displays	N/A				
SYS.DMS(P2SAT-UI).25	Verification of control action cancellation by the operator	N/A				
SYS.DMS(P2SAT-UI).26	Verification of control action time-out	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-UI).27	Verification of control action failed	N/A				
SYS.DMS(P2SAT-UI).28	Verify analog controls (set points), raise/lower (no return)	N/A				
SYS.DMS(P2SAT-UI).29	Verify control command failures	N/A				
SYS.DMS(P2SAT-UI).30	Verification of system behavior in case of control "rejected" or "failed"	N/A				
SYS.DMS(P2SAT-UI).31	Verify interlocking conditions: Raise/Lower Limit reached	N/A				
SYS.DMS(P2SAT-UI).32	Verify interlocking conditions: Multiple user/consoles	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Integrated UI – Manual Changes and Tags						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-UI).33	Verify Manual valid substitution function	N/A				
SYS.DMS(P2SAT-UI).34	Verification of manual entries representation in displays	N/A				
SYS.DMS(P2SAT-UI).35	Verify validity checking for manual entries	N/A				
SYS.DMS(P2SAT-UI).36	Verify reporting and logging of manual changes, successful and failed	N/A				
SYS.DMS(P2SAT-UI).37	Verify Jumpers/Cuts/Grounding functionality	N/A				
SYS.DMS(P2SAT-UI).38	Verification of temporary element representation in displays	N/A				
SYS.DMS(P2SAT-UI).39	Verify reporting and logging of temporary elements in the model	N/A				
SYS.DMS(P2SAT-UI).40	Verification of Tag setting, comments, removal	N/A				
SYS.DMS(P2SAT-UI).41	Verification of tagging representation in displays	N/A				
SYS.DMS(P2SAT-UI).42	Verification of multiple tags for the same device and different device types	N/A				
SYS.DMS(P2SAT-UI).43	Verification of tagging lists (system-wise, tag type)	N/A				
SYS.DMS(P2SAT-UI).44	Verification of tagging propagation to the different modules of the system	N/A				
SYS.DMS(P2SAT-UI).45	Verification of locking conditions when tags are set	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Integrated UI – Time Synchronization						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-UI).46	Verify time synch reporting and logging when it happens	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Integrated UI – Alarm List Management						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-UI).47	Verify that alarm error conditions and problems are reported and logged (list full, alarm processing not working)	N/A				
SYS.DMS(P2SAT-UI).48	Verify alarm management special conditions like max number of alarms reached, reduced view	N/A				
SYS.DMS(P2SAT-UI).49	Verify reporting and logging of alarm issues and list management	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Integrated UI – ICCP						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-UI).50	Verification of the data flow through ICCP link, checking the different types of data in both directions	N/A				
SYS.DMS(P2SAT-UI).51	Verification ICCP link status display	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-UI).52	Verification of the ICCP link management	N/A				
SYS.DMS(P2SAT-UI).53	Verification of the ICCP link redundancy	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Integrated UI – Communications Failover/Redundancy						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-UI).54	Verify communication failover and redundancy for communication or application errors/problems	N/A				
System Test Book – DMS (Phase 2 Site Acceptance Test): Integrated UI – Application Failover/Redundancy						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P2SAT-UI).55	Verify data is correct after failover at all levels of redundancy	N/A				
SYS.DMS(P2SAT-UI).56	Verify InService operation	N/A				

System Test Book - DMS (Phase 3 Factory Acceptance Test) - Recloser Points Checkout: Type DI						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT-651R).1	Verify point "Enabled"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3FAT-651R).2	Verify point "Device Status"	Values Displayed: - OPEN - CLOSE				
SYS.DMS(P3FAT-651R).3	Verify point "Loss of Potential"	Values Displayed: - OK - ALARM				
SYS.DMS(P3FAT-651R).4	Verify point "Fault - Phase C"	Values Displayed: - OK - ALARM				
SYS.DMS(P3FAT-651R).5	Verify point "Fault - Phase B"	Values Displayed: - OK - ALARM				
SYS.DMS(P3FAT-651R).6	Verify point "Fault - Phase A"	Values Displayed: - OK - ALARM				
SYS.DMS(P3FAT-651R).7	Verify point "Sync Check Elements - "	Values Displayed: - OK - ALARM				
SYS.DMS(P3FAT-651R).8	Verify point "Cabinet Door"	Values Displayed: - OK - ALARM				
SYS.DMS(P3FAT-651R).9	Verify point "50CO- Ground Overcurrent Status"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3FAT-651R).10	Verify point "79CO- Reclosing Status"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3FAT-651R).11	Verify point "Local - Remote"	Values Displayed: - LOCAL - REMOTE				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT-651R).12	Verify point "Fast Curves Status"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3FAT-651R).13	Verify point "Push Buttons Locked"	Values Displayed: - UNLOCKED - LOCKED				
SYS.DMS(P3FAT-651R).14	Verify point "Hot Line Tag Status"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3FAT-651R).15	Verify point "Aux 1 Status"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3FAT-651R).16	Verify point "Aux 2 Status"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3FAT-651R).17	Verify point "Aux 3 Status"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3FAT-651R).18	Verify point "Battery Failure "	Values Displayed: - OK - ALARM				
SYS.DMS(P3FAT-651R).19	Verify point "External Power"	Values Displayed: - OFF - ON				
SYS.DMS(P3FAT-651R).20	Verify point "Lockout"	Values Displayed: - OK - ALARM				
SYS.DMS(P3FAT-651R).21	Verify point "Current Direction"	Values Displayed: - NORMAL - REVERSED				
SYS.DMS(P3FAT-651R).22	Verify point "Contact Wear - 3 Phase"	Values Displayed: - OK - ALARM				
SYS.DMS(P3FAT-651R).23	Verify point "Clock Present"	Values Displayed: - NOT PRESENT - PRESENT				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT-651R).24	Verify point "Hardware Alarm"	Values Displayed: - OK - ALARM				
SYS.DMS(P3FAT-651R).25	Verify point "Software Alarm"	Values Displayed: - OK - ALARM				
System Test Book - DMS (Phase 3 Factory Acceptance Test) - Recloser Points Checkout: Type DO						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT-651R).26	Verify point "Aux 1"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3FAT-651R).27	Verify point "Aux 2"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3FAT-651R).28	Verify point "Aux 3"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3FAT-651R).29	Verify point "Aux 4"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3FAT-651R).30	Verify point "50CO - Ground Overcurrent"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3FAT-651R).31	Verify point "79CO - Reclosing"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3FAT-651R).32	Verify point "Fast Curves"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3FAT-651R).33	Verify point "Hot Line Tag"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3FAT-651R).34	Verify point "Device Operate"	Values Displayed: - OPEN - CLOSE				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT-651R).35	Verify point "Reset Front Panel Targets"	Values Displayed: - NA - RESET				
System Test Book - DMS (Phase 3 Factory Acceptance Test) - Recloser Points Checkout: Type CTR						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT-651R).36	Verify point "Active Settings Group"	N/A				
SYS.DMS(P3FAT-651R).37	Verify point "Internal Breaker Trips - Phase A "	N/A				
SYS.DMS(P3FAT-651R).38	Verify point "Internal Breaker Trips - Phase B "	N/A				
SYS.DMS(P3FAT-651R).39	Verify point "Internal Breaker Trips - Phase C "	N/A				
SYS.DMS(P3FAT-651R).40	Verify point "External Breaker Trips - Phase A "	N/A				
SYS.DMS(P3FAT-651R).41	Verify point "External Breaker Trips - Phase B"	N/A				
SYS.DMS(P3FAT-651R).42	Verify point "External Breaker Trips - Phase C"	N/A				
System Test Book - DMS (Phase 3 Factory Acceptance Test) - Recloser Points Checkout: Type AI						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT-651R).43	Verify point "Current - Phase A"	N/A				
SYS.DMS(P3FAT-651R).44	Verify point "Current - Phase B"	N/A				
SYS.DMS(P3FAT-651R).45	Verify point "Current - Phase C"	N/A				
SYS.DMS(P3FAT-651R).46	Verify point "Current - Neutral"	N/A				
SYS.DMS(P3FAT-651R).47	Verify point "Current - Ground"	N/A				
SYS.DMS(P3FAT-651R).48	Verify point "Voltage - Phase A - Y"	N/A				
SYS.DMS(P3FAT-651R).49	Verify point "Voltage - Phase B - Y"	N/A				
SYS.DMS(P3FAT-651R).50	Verify point "Voltage - Phase C - Y"	N/A				
SYS.DMS(P3FAT-651R).51	Verify point "Voltage - Phase A - Z"	N/A				
SYS.DMS(P3FAT-651R).52	Verify point "Voltage - Phase B - Z"	N/A				
SYS.DMS(P3FAT-651R).53	Verify point "Voltage - Phase C - Z"	N/A				
SYS.DMS(P3FAT-651R).54	Verify point "Real Power - Phase A"	N/A				
SYS.DMS(P3FAT-651R).55	Verify point "Real Power - Phase B"	N/A				
SYS.DMS(P3FAT-651R).56	Verify point "Real Power - Phase C"	N/A				
SYS.DMS(P3FAT-651R).57	Verify point "Real Power - 3 Phase"	N/A				
SYS.DMS(P3FAT-651R).58	Verify point "Reactive Power - Phase A"	N/A				
SYS.DMS(P3FAT-651R).59	Verify point "Reactive Power - Phase B"	N/A				
SYS.DMS(P3FAT-651R).60	Verify point "Reactive Power - Phase C"	N/A				
SYS.DMS(P3FAT-651R).61	Verify point "Reactive Power - 3 Phase"	N/A				
SYS.DMS(P3FAT-651R).62	Verify point "Frequency"	N/A				
SYS.DMS(P3FAT-651R).63	Verify point "Contact Wear - Phase A"	N/A				
SYS.DMS(P3FAT-651R).64	Verify point "Contact Wear - Phase B"	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT-651R).65	Verify point "Contact Wear - Phase C"	N/A				
SYS.DMS(P3FAT-651R).66	Verify point "Fault Type "	N/A				
SYS.DMS(P3FAT-651R).67	Verify point "Fault Recloser Shot Counter "	N/A				
SYS.DMS(P3FAT-651R).68	Verify point "Fault Time"	N/A				
SYS.DMS(P3FAT-651R).69	Verify point "Fault Current - Phase A"	N/A				
SYS.DMS(P3FAT-651R).70	Verify point "Fault Current - Phase B"	N/A				
SYS.DMS(P3FAT-651R).71	Verify point "Fault Current - Phase C"	N/A				
SYS.DMS(P3FAT-651R).72	Verify point "Fault Current - Ground"	N/A				
SYS.DMS(P3FAT-651R).73	Verify point "Apparent Power - Phase A"	N/A				
SYS.DMS(P3FAT-651R).74	Verify point "Apparent Power - Phase B"	N/A				
SYS.DMS(P3FAT-651R).75	Verify point "Apparent Power - Phase C"	N/A				
SYS.DMS(P3FAT-651R).76	Verify point "Apparent Power - 3 Phase"	N/A				
SYS.DMS(P3FAT-651R).77	Verify point "THD - Current - Phase A"	N/A				
SYS.DMS(P3FAT-651R).78	Verify point "THD - Current - Phase B"	N/A				
SYS.DMS(P3FAT-651R).79	Verify point "THD - Current - Phase C"	N/A				
SYS.DMS(P3FAT-651R).80	Verify point "THD - Current - Neutral"	N/A				
SYS.DMS(P3FAT-651R).81	Verify point "THD - Voltage - Phase A - Y"	N/A				
SYS.DMS(P3FAT-651R).82	Verify point "THD - Voltage - Phase B - Y"	N/A				
SYS.DMS(P3FAT-651R).83	Verify point "THD - Voltage - Phase C - Y"	N/A				
SYS.DMS(P3FAT-651R).84	Verify point "THD - Voltage - Phase A - Z"	N/A				
SYS.DMS(P3FAT-651R).85	Verify point "THD - Voltage - Phase B - Z"	N/A				
SYS.DMS(P3FAT-651R).86	Verify point "THD - Voltage - Phase C - Z"	N/A				
SYS.DMS(P3FAT-651R).87	Verify point "Battery Voltage"	N/A				
SYS.DMS(P3FAT-651R).88	Verify point "Battery Current"	N/A				
System Test Book - DMS (Phase 3 Factory Acceptance Test) - Recloser Points Checkout: Type AD						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT-651R).89	Verify point "Set Active Settings Group"	N/A				

System Test Book - DMS (Phase 3 FAT): Configuration Verification						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).1	Verify FAT system environment diagram	N/A				
SYS.DMS(P3FAT).2	Verify system Test Environment (HW & SW), including simulation and tools, before starting FAT	N/A				
SYS.DMS(P3FAT).3	Verify system management and configuration displays and tools	N/A				
SYS.DMS(P3FAT).4	Verify correct operation of the system components (system configuration overview, servers status, communications status, applications running,....)	N/A				
System Test Book - DMS (Phase 3 FAT): Computer System Management						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).6	Verify that servers and applications synch using NTP	N/A				
SYS.DMS(P3FAT).12	Verify redundancy for DNA modules	N/A				
SYS.DMS(P3FAT).13	Verify communication redundancy between CC and substation	N/A				
SYS.DMS(P3FAT).20	Verify DNA applications operation	N/A				
SYS.DMS(P3FAT).22	Verify communication with SICAM and check correct recovery from LAN failure	N/A				
SYS.DMS(P3FAT).24	Verify operation with InService when LAN fails and after correct recovery	N/A				
SYS.DMS(P3FAT).26	Verify status reporting and logging	N/A				
SYS.DMS(P3FAT).28	Verify data consistency including DNA	N/A				
SYS.DMS(P3FAT).30	Verify data is correct after failover at all levels of redundancy from DNA perspective	N/A				
SYS.DMS(P3FAT).32	Verify system behavior during DNA servers power failures and vice versa	N/A				
SYS.DMS(P3FAT).35	Verify applications run up to operational status without human intervention after power failure	N/A				
SYS.DMS(P3FAT).36	Verify SICAM status status changes are reported and logged at the CC and HMI	N/A				
SYS.DMS(P3FAT).44	Verify DNA applications run up to operational status without human intervention after power failure	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).48	<p>Verify Cyber security rules and conditions for DNA applications (Similar to the ones defined for the rest of the system components)</p> <p>There are basic security requirements for the systems that need to be verified for this solution:</p> <ul style="list-style-type: none"> * Users definition (password hardening, authorities, permissions) * Log On/Off characteristics (allowed attempts, time outs) * Logging of all actions * System users/passwords * Remote log ins and connections 	N/A				
System Test Book - DMS (Phase 3 FAT): Functional Redundancy						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).55	Verify automatic failover at the substation level when DCADA application has problems or the SW detects errors	N/A				
SYS.DMS(P3FAT).56	Verify status reporting and logging at the CC	N/A				
SYS.DMS(P3FAT).59	Verify DSCADA and DNA redundancy and failover caused by application or SW problems	N/A				
SYS.DMS(P3FAT).60	Verify DNA, SCADA functions manual failover	N/A				
SYS.DMS(P3FAT).61	Verify status reporting and logging at the CC	N/A				
SYS.DMS(P3FAT).62	Verify presentation of the control and application status for the substation and the CC	N/A				
SYS.DMS(P3FAT).64	Verify Manual transfer of DNA control	N/A				
SYS.DMS(P3FAT).419	Verify that the Mastership control UI or status and control operations are accessible in DCADA DNA in case DMS is not accessible	N/A				
SYS.DMS(P3FAT).420	<p>Verify automatic transfer of control from DCADA close loop to DMS:</p> <ul style="list-style-type: none"> * Boundary switch closed * Connection between DCADA and SICAM lost * FLT/FISR/VVC error condition in DCADA DNA * Loss of communication between DCADA and DMS 	N/A				
SYS.DMS(P3FAT).421	<p>Verify of automatic control authority removal from DMS close loop when:</p> <ul style="list-style-type: none"> * Boundary switch closed * Connection between DMS and SICAM is lost * FISR/FLT/VVC error condition in DMS DNA * Loss of communication between DCADA and DMS 	N/A				
SYS.DMS(P3FAT).422	Verify normal operation of DMS except for controls when DCADA is master	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).423	Verify normal operation of DMS including controls when DCADA is master for subsystems outside the DCADA area	N/A				
SYS.DMS(P3FAT).424	Verify normal operation of DMS including controls when DMS is Master and in manual mode	N/A				
SYS.DMS(P3FAT).425	Verify normal operation of DMS except controls when DMS is Master in Close Loop	N/A				
SYS.DMS(P3FAT).426	Verify DCADA can not be set to close loop operation when DMS is Master	N/A				
SYS.DMS(P3FAT).427	Verify DMS can not be set to close loop operation for Midtown when DCADA is Master	N/A				
SYS.DMS(P3FAT).428	Verify notification of Control Mastership in DCADA and DMS UIs	N/A				
SYS.DMS(P3FAT).67	Verify status reporting and logging at the CC	N/A				
System Test Book - DMS (Phase 3 FAT): Data Acquisition						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).77	Verify status reporting to the DNA	N/A				
System Test Book - DMS (Phase 3 FAT): Data Propagation						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).93	Verification of the data flow through ICCP link to DNA	N/A				
System Test Book - DMS (Phase 3 FAT): Data Base Management						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).99	Based on the DB generation process defined and provided by Siemens and Intergraph, verify that the data definition and DB generation works for DNA	N/A				
SYS.DMS(P3FAT).103	Verify DB management tools with DNA model (DB Jobs, DB Job propagation, DB Job roll back)	N/A				
SYS.DMS(P3FAT).105	Verify DNA DB archiving	N/A				
SYS.DMS(P3FAT).106	Verify DB error reporting and logging	N/A				
System Test Book - DMS (Phase 3 FAT): User Interface						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).108	Verify users log on and log off in DNA	N/A				
SYS.DMS(P3FAT).110	Verify only defined users can log on in DNA	N/A				
SYS.DMS(P3FAT).111	Verify reporting and logging	N/A				
SYS.DMS(P3FAT).116	Verify Tabular displays availability and access in DNA	N/A				
SYS.DMS(P3FAT).118	Verify data presented in Tabular displays in DNA	N/A				
SYS.DMS(P3FAT).134	Verify configuration of AORs and permissions for different in DNA	N/A				
SYS.DMS(P3FAT).136	Verify change in AOR for DNA	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).138	Verify authorization and permission changes for an AOR in DNA	N/A				
SYS.DMS(P3FAT).139	Verify reporting and logging of AOR issues and management (authorizations and permissions)	N/A				
SYS.DMS(P3FAT).146	Verify control action propagation in all modules and that execution is synchronized starting from DNA	N/A				
SYS.DMS(P3FAT).154	Verify Switching Plan management and execution (Switching sequences module)	N/A				
SYS.DMS(P3FAT).159	Verify manual changes are updated in DNA (data synchronization)	N/A				
SYS.DMS(P3FAT).160	Verify reporting and logging of manual changes, successful and failed	N/A				
SYS.DMS(P3FAT).162	Verify JC&G functionality in DNA	N/A				
SYS.DMS(P3FAT).164	Verify propagation of temporary elements to all affected modules	N/A				
SYS.DMS(P3FAT).165	Verifies DNA execution when setting or removing temporary elements	N/A				
SYS.DMS(P3FAT).166	Verify reporting and logging of temporary elements in the model	N/A				
SYS.DMS(P3FAT).172	Verification of tagging propagation to DNA	N/A				
SYS.DMS(P3FAT).174	Verify reporting and logging of tagging actions	N/A				
System Test Book - DMS (Phase 3 FAT): Data Archive & Backup						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).177	Verify system tools to save event log, system log and specific DNA data to external media	N/A				
SYS.DMS(P3FAT).178	Verify reporting and logging of information archiving activities	N/A				
SYS.DMS(P3FAT).180	Verify system tools to backup and restore SW and data	N/A				
SYS.DMS(P3FAT).181	Verify reporting and logging of archiving and restoration activities	N/A				
System Test Book - DMS (Phase 3 FAT): Reporting						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).193	Verify application statistics displays for VVC, FLT and FISR	N/A				
System Test Book - DMS (Phase 3 FAT): Distribution Network Applications - General DNA System Testing						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).194	Test DNA hierarchical operation: (monitor and control)	N/A				
SYS.DMS(P3FAT).195	Locking conditions to avoid overlaps between DCADA and DMS	N/A				
SYS.DMS(P3FAT).196	Enable - disable applications independently in DCADA and DMS	N/A				
SYS.DMS(P3FAT).197	Verify User Log On to the DNA Web UI in DMS	N/A				
SYS.DMS(P3FAT).198	Verify User Log On to the DNA Web UI in DNA	N/A				
SYS.DMS(P3FAT).199	Verify access denial to undefined users or wrong password	N/A				
SYS.DMS(P3FAT).200	Verify use of permissions for different users	N/A				
SYS.DMS(P3FAT).201	Verify context management	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).202	Verify access to study context and case management	N/A				
SYS.DMS(P3FAT).203	Verify simultaneous use of multiple contexts and cases	N/A				
SYS.DMS(P3FAT).204	Verify reporting and logging	N/A				
System Test Book - DMS (Phase 3 FAT): Distribution Network Applications - State Estimation (DSSE) & Power Flow (DSPF)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).205	From InService demonstrate access to PowerFlow connecting to the DNA in DMS	N/A				
SYS.DMS(P3FAT).206	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).207	Verify access to application alarms or program output	N/A				
SYS.DMS(P3FAT).208	From InService demonstrate access to PowerFlow connecting to the DNA in DCADA	N/A				
SYS.DMS(P3FAT).209	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).210	Verify access to application alarms or program output	N/A				
SYS.DMS(P3FAT).211	Run DSSE from DMS DNA UI and verify results	N/A				
SYS.DMS(P3FAT).212	Verify DSSE different modes of execution in DMS	N/A				
SYS.DMS(P3FAT).213	Verify DNA DSEE operation with multiple users	N/A				
SYS.DMS(P3FAT).214	Verify DNA DSEE operation with simultaneous execution from multiple users	N/A				
SYS.DMS(P3FAT).215	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).216	Verify access to application alarms or program output	N/A				
SYS.DMS(P3FAT).217	Introduce model changes and verify results	N/A				
SYS.DMS(P3FAT).A	Reverse flow verification/alarm	N/A				
SYS.DMS(P3FAT).B	Verify island condition	N/A				
SYS.DMS(P3FAT).218	Introduce manual data changes and verify results	N/A				
SYS.DMS(P3FAT).219	Run DSSE from DCADA DNA UI and verify results	N/A				
SYS.DMS(P3FAT).220	Verify DSSE different modes of execution from DCADA	N/A				
SYS.DMS(P3FAT).221	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).222	Verify access to application alarms or program output	N/A				
SYS.DMS(P3FAT).223	Introduce model changes and verify results	N/A				
SYS.DMS(P3FAT).224	Introduce manual data changes and verify results	N/A				
SYS.DMS(P3FAT).225	Verify DNA DSEE simultaneous execution in DMS and DCADA (Event Triggered)	N/A				
SYS.DMS(P3FAT).226	Verify and compare DSSE results	N/A				
SYS.DMS(P3FAT).227	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).228	Run Power Flow from DMS DNA UI and verify results	N/A				
SYS.DMS(P3FAT).229	Verify PowerFlow different modes of execution from the DMS	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).230	Verify DNA PF operation with multiple users	N/A				
SYS.DMS(P3FAT).231	Verify DNA PF operation with simultaneous execution from multiple users	N/A				
SYS.DMS(P3FAT).232	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).233	Verify access to application alarms or program output	N/A				
SYS.DMS(P3FAT).234	Introduce model changes and verify results	N/A				
SYS.DMS(P3FAT).235	Introduce manual data changes and verify results	N/A				
SYS.DMS(P3FAT).236	Run Power Flow from DCADA DNA UI and verify results	N/A				
SYS.DMS(P3FAT).237	Verify PowerFlow different modes of execution from the DCADA	N/A				
SYS.DMS(P3FAT).238	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).239	Verify access to application alarms or program output	N/A				
SYS.DMS(P3FAT).240	Introduce model changes and verify results	N/A				
SYS.DMS(P3FAT).241	Introduce manual data changes and verify results	N/A				
SYS.DMS(P3FAT).242	Verify access to list and summaries using DNA UI in the DMS	N/A				
SYS.DMS(P3FAT).243	Verify access to list and summaries using DNA UI in DCADA	N/A				
SYS.DMS(P3FAT).244	Verify alarms generated by Limit violation or other oprational conditions like non convergence	N/A				
SYS.DMS(P3FAT).245	Verify alarms generated in DCADA by Limit violation or other oprational conditions like non convergence.	N/A				
SYS.DMS(P3FAT).246	Verify DNA PF simultaneous execution in DMS and DCADA (Event Triggered)	N/A				
SYS.DMS(P3FAT).247	Verify and compare PF results	N/A				
SYS.DMS(P3FAT).248	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).249	Verify alarm notifications	N/A				
SYS.DMS(P3FAT).250	Verify DSSE operation when DNA failover occurs	N/A				
SYS.DMS(P3FAT).251	Verify PF operation when DNA failover occurs	N/A				
SYS.DMS(P3FAT).252	Verify DSSE operation after DNA failover occurs and stable situation is reestablished	N/A				
SYS.DMS(P3FAT).253	Verify PF operation after DNA failover occurs and stable situation is reestablished	N/A				
SYS.DMS(P3FAT).254	Verify DSSE operation when DNA failover occurs	N/A				
SYS.DMS(P3FAT).255	Verify PF operation when DNA failover occurs	N/A				
SYS.DMS(P3FAT).256	Verify DSSE operation after DNA failover occurs and stable situation is reestablished	N/A				
SYS.DMS(P3FAT).257	Verify PF operation after DNA failover occurs and stable situation is reestablished	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).258	Verify Simulation mode	N/A				
SYS.DMS(P3FAT).259	Verify use and options in Simulation mode	N/A				
SYS.DMS(P3FAT).260	Verify visual differentiation of operational mode: Real Time and Simulation	N/A				
SYS.DMS(P3FAT).261	Verify reporting of execution errors or problems in Simulation Mode	N/A				
System Test Book - DMS (Phase 3 FAT): Distribution Network Applications - Feeder Load Transfer (FLT)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).262	Verify access to FLT from InService	N/A				
SYS.DMS(P3FAT).263	Verify FLT running from DMS (Switching Sequence?)	N/A				
SYS.DMS(P3FAT).264	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).265	Verify access to application alarms or program output	N/A				
SYS.DMS(P3FAT).266	Verify FLT running from DCADA (Switching Sequence execution?)	N/A				
SYS.DMS(P3FAT).267	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).268	Verify access to application alarms or program output	N/A				
SYS.DMS(P3FAT).269	Verify FLT execution and sequence interruption in DMS	N/A				
SYS.DMS(P3FAT).270	Verify FLT execution in close loop	N/A				
SYS.DMS(P3FAT).271	Verify Operator's notification (InService ?)	N/A				
SYS.DMS(P3FAT).272	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).273	Verify validation steps	N/A				
SYS.DMS(P3FAT).274	Verify switching failures and/or confirmation of steps' execution	N/A				
SYS.DMS(P3FAT).275	Verify access to application alarms or program output	N/A				
SYS.DMS(P3FAT).276	Verify FLT execution and sequence interruption in DCADA	N/A				
SYS.DMS(P3FAT).277	Verify FLT execution in close loop	N/A				
SYS.DMS(P3FAT).278	Verify Operator's notification (InService ?)	N/A				
SYS.DMS(P3FAT).279	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).280	Verify validation steps	N/A				
SYS.DMS(P3FAT).281	Verify switching failures and/or confirmation of steps's execution	N/A				
SYS.DMS(P3FAT).282	Verify access to application alarms or program output	N/A				
SYS.DMS(P3FAT).283	Access to FLT results and info from InService	N/A				
SYS.DMS(P3FAT).284	Verify FLT operation when DNA failover occurs	N/A				
SYS.DMS(P3FAT).285	Verify FLT operation after DNA failover occurs and stable situation is reestablished	N/A				
SYS.DMS(P3FAT).286	Verify coordinated Close Loop Operation in DCADA and DMS together	N/A				
SYS.DMS(P3FAT).287	Verify configuration of close loop in DCADA and DMS together	N/A				
SYS.DMS(P3FAT).288	Verify Operator's notification in DMS	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).289	Verify authority transfer from DCADA to DMS when a solution is not found	N/A				
SYS.DMS(P3FAT).290	Verify notification to Operator in DMS when authority is transferred	N/A				
SYS.DMS(P3FAT).291	Verify FLT operation when DNA in DMS failover occurs while running. Check authority status and notification	N/A				
SYS.DMS(P3FAT).292	Verify FLT operation and notification after DNA in DMS failover occurs and stable situation is reestablished	N/A				
SYS.DMS(P3FAT).293	Verify FLT operation when DNA in DCADA failover occurs while running. Check authority status and notification	N/A				
SYS.DMS(P3FAT).294	Verify FLT operation and notification after DNA in DCADA failover occurs and stable situation is reestablished	N/A				
SYS.DMS(P3FAT).295	Verify FLT operation when DCADA and DMS get disconnected (communication failure)	N/A				
SYS.DMS(P3FAT).296	Verify FLT operation when DNA in DCADA is stopped or not available: * Automatic transfer of Authority * Operation stability	N/A				
SYS.DMS(P3FAT).297	Verify FLT operation when DNA in DMS is stopped or not available: * Automatic transfer of Authority * Operation stability	N/A				
SYS.DMS(P3FAT).298	Verify FLT running in simulation mode	N/A				
SYS.DMS(P3FAT).299	Verify use and options in Simulation mode	N/A				
SYS.DMS(P3FAT).300	Verify visual differentiation of operational mode: Real Time and Simulation	N/A				
SYS.DMS(P3FAT).301	Verify that generated and tested sequence in simulated mode can be transferred to Real Time	N/A				
SYS.DMS(P3FAT).302	Verify reporting of execution errors or problems in Simulation Mode	N/A				
System Test Book - DMS (Phase 3 FAT): Distribution Network Applications - Fault Location (FLOC)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).303	Verify that FLOC runs and results can be shown in the map	N/A				
SYS.DMS(P3FAT).304	Verify geographical access to results (Navigation)	N/A				
SYS.DMS(P3FAT).305	Verify reporting of execution errors or problems in InService	N/A				
SYS.DMS(P3FAT).306	Verify interaction with application in InService	N/A				
SYS.DMS(P3FAT).307	Verify interaction with application in DNA UI	N/A				
SYS.DMS(P3FAT).308	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).309	Verify access to application alarms or program output	N/A				
SYS.DMS(P3FAT).310	Verify FLOC operation in different conditions	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).311	Verify FLOC when setting temporary elements in InService	N/A				
SYS.DMS(P3FAT).312	Verify FLOC is not trigger by Operator's controls or switching sequence operations	N/A				
SYS.DMS(P3FAT).313	Verify that only permanent reclosure faults triggers FLOC	N/A				
SYS.DMS(P3FAT).314	Verify geographical access to results (Navigation)	N/A				
SYS.DMS(P3FAT).315	Verify reporting of execution errors or problems in InService	N/A				
SYS.DMS(P3FAT).316	Verify interaction with application in InService	N/A				
SYS.DMS(P3FAT).317	Verify interaction with application in DNA UI	N/A				
SYS.DMS(P3FAT).318	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).319	Verify access to application alarms or program output	N/A				
SYS.DMS(P3FAT).320	Verify FLOC application UI displays	N/A				
SYS.DMS(P3FAT).321	Verify FLOC interfaces with FISR and OMS	N/A				
SYS.DMS(P3FAT).322	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).323	Verify FLOC operation when DNA failover occurs	N/A				
SYS.DMS(P3FAT).324	Verify FLOC operation after DNA failover occurs and stable situation is reestablished	N/A				
System Test Book - DMS (Phase 3 FAT): Distribution Network Applications - Fault Isolation and Service Restoration (FISR)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).325	Verify FISR execution and service restoration	N/A				
SYS.DMS(P3FAT).326	Verify Operator's notification (InService ?)	N/A				
SYS.DMS(P3FAT).327	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).328	Verify interaction with application in InService	N/A				
SYS.DMS(P3FAT).329	Verify geographical access to results (Navigation)	N/A				
SYS.DMS(P3FAT).331	Verify FISR execution with multiple faults at the same time <- FLOC Triggered	N/A				
SYS.DMS(P3FAT).332	Verify FISR execution and service restoration in close loop	N/A				
SYS.DMS(P3FAT).333	Verify Operator's notification (InService ?)	N/A				
SYS.DMS(P3FAT).334	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).335	Verify geographical access to results (Navigation)	N/A				
SYS.DMS(P3FAT).336	Verify Switching Procedure export to OMS	N/A				
SYS.DMS(P3FAT).337	Verify Switching Procedure execution in InService	N/A				
SYS.DMS(P3FAT).338	Verify FISR operation when DNA failover occurs	N/A				
SYS.DMS(P3FAT).339	Verify FISR operation after DNA failover occurs and stable situation is reestablished	N/A				
SYS.DMS(P3FAT).340	Verify coordinated Close Loop Operation in DCADA and DMS together	N/A				
SYS.DMS(P3FAT).341	Verify configuration of close loop in DCADA and DMS together	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).342	Verify Operator's notification in DMS	N/A				
SYS.DMS(P3FAT).343	Verify authority transfer from DCADA to DMS when a solution is not found	N/A				
SYS.DMS(P3FAT).344	Verify notification to Operator in DMS when authority is transferred	N/A				
SYS.DMS(P3FAT).345	Verify FISR operation when DNA in DMS failover occurs while running. Check authority status and notification	N/A				
SYS.DMS(P3FAT).346	Verify FISR operation and notification after DNA in DMS failover occurs and stable situation is reestablished	N/A				
SYS.DMS(P3FAT).347	Verify FISR operation when DNA in DCADA failover occurs while running. Check authority status and notification	N/A				
SYS.DMS(P3FAT).348	Verify FISR operation and notification after DNA in DCADA failover occurs and stable situation is reestablished	N/A				
SYS.DMS(P3FAT).349	Verify FISR operation and notification when DCADA and DMS get disconnected (communication failure)	N/A				
SYS.DMS(P3FAT).350	Verify FISR operation when DNA in DCADA is stopped or not available: * Automatic transfer of Authority * Operation stability	N/A				
SYS.DMS(P3FAT).351	Verify FISR operation when DNA in DMS is stopped or not available: * Automatic transfer of Authority * Operation stability	N/A				
SYS.DMS(P3FAT).352	Verify use and management of Study Context (Create, save & restore cases)	N/A				
SYS.DMS(P3FAT).353	Verify use of multiple Study contexts at the same time	N/A				
SYS.DMS(P3FAT).354	Verify FISR results in Study context	N/A				
SYS.DMS(P3FAT).355	Verify FISR operation in case of abnormal situations, user errors,..... in Study context	N/A				
SYS.DMS(P3FAT).356	Verify reporting of execution errors or problems in Study context	N/A				
System Test Book - DMS (Phase 3 FAT)- Distribution Network Applications - Voltage and VAR control (VVC)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).357	Verify VVC execution in Open Loop and access to the Open Loop configuration	N/A				
SYS.DMS(P3FAT).358	Verify VVC application management: * Add and remove devices * Reject proposed switching plan * Adjust configuration and rerun	N/A				
SYS.DMS(P3FAT).359	Verify Operator's notification (InService ?)	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).360	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).361	Verify geographical access to results (Navigation)	N/A				
SYS.DMS(P3FAT).362	Verification of VVC configuration and Manual execution	N/A				
SYS.DMS(P3FAT).363	Verify Operator's notification (InService ?)	N/A				
SYS.DMS(P3FAT).364	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).365	Verify geographical access to results (Navigation)	N/A				
SYS.DMS(P3FAT).366	Verify multiple Study context at the same time	N/A				
SYS.DMS(P3FAT).367	Verify result in Study context (simulation)	N/A				
SYS.DMS(P3FAT).368	Verify result in Study context can be used in real time context	N/A				
SYS.DMS(P3FAT).369	Verify Switching Procedure export to OMS	N/A				
SYS.DMS(P3FAT).370	Verify Switching Procedure execution in InService	N/A				
SYS.DMS(P3FAT).371	Verification of VVC configuration and Manual execution	N/A				
SYS.DMS(P3FAT).372	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).373	Verify Switching Procedure execution	N/A				
SYS.DMS(P3FAT).374	Verify Operator's notification in DMS	N/A				
SYS.DMS(P3FAT).375	Verify authority transfer from DCADA to DMS when a solution is not found	N/A				
SYS.DMS(P3FAT).376	Verify notification to Operator's in DMS when authority is transferred	N/A				
SYS.DMS(P3FAT).377	Verify VVC execution triggered by different conditions	N/A				
SYS.DMS(P3FAT).378	Verify that DDSE will run automatically when needed	N/A				
SYS.DMS(P3FAT).379	Verify VVC results of the sequence generated and executed	N/A				
SYS.DMS(P3FAT).380	Verify VVC reaction multiple trigger actions at the same time	N/A				
SYS.DMS(P3FAT).381	Verify VVC operation when DNA failover occurs while running	N/A				
SYS.DMS(P3FAT).382	Verify VVC operation after DNA failover occurs and stable situation is reestablished	N/A				
SYS.DMS(P3FAT).383	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).384	Verify VVC execution triggered by different conditions	N/A				
SYS.DMS(P3FAT).385	Verify that DDSE will run automatically when needed	N/A				
SYS.DMS(P3FAT).386	Verify VVC results of the sequence generated and executed	N/A				
SYS.DMS(P3FAT).387	Verify VVC reaction multiple trigger actions at the same time	N/A				
SYS.DMS(P3FAT).388	Verify VVC operation when DNA failover occurs while running	N/A				
SYS.DMS(P3FAT).389	Verify VVC operation after DNA failover occurs and stable situation is reestablished	N/A				
SYS.DMS(P3FAT).390	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).391	Verify VVC execution defining different objectives.	N/A				
SYS.DMS(P3FAT).392	Verify VVC execution using only controllable devices	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).	Verify VVC execution after transferring capacitors to another circuit	N/A				
SYS.DMS(P3FAT).393	Verify VVC execution with tagged devices	N/A				
SYS.DMS(P3FAT).394	Verify VVC execution of control sequence when control fails	N/A				
SYS.DMS(P3FAT).395	Verify VVC reaction to a situation with no controllable devices	N/A				
SYS.DMS(P3FAT).396	Verify VVC reaction to topology changes between calculation and execution	N/A				
SYS.DMS(P3FAT).397	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3FAT).398	Verify Close Loop Operation in DMS	N/A				
SYS.DMS(P3FAT).399	Verify that DDSE will run automatically when needed as part of the VVC close loop execution	N/A				
SYS.DMS(P3FAT).400	Verify Close Loop execution failures and system reaction: * Control fails * Device Tagging * Device already in requested position	N/A				
SYS.DMS(P3FAT).401	Verify Close Loop execution with limit conditions: * Max number of daily operations * Usability Time runs out * Control values out of range	N/A				
SYS.DMS(P3FAT).402	Verify Close Loop Operation in DCADA	N/A				
SYS.DMS(P3FAT).403	Verify that DDSE will run automatically when needed as part of the VVC close loop execution	N/A				
SYS.DMS(P3FAT).404	Verify Close Loop execution failures and system reaction: * Control fails * Device Tagging * Device already in requested position	N/A				
SYS.DMS(P3FAT).405	Verify Close Loop execution with limit conditions: * Max number of daily operations * Usability Time runs out * Control values out of range	N/A				
SYS.DMS(P3FAT).406	Verify Operator's notification (InService ?)	N/A				
SYS.DMS(P3FAT).407	Verify coordinated Close Loop Operation in DCADA and DMS together	N/A				
SYS.DMS(P3FAT).408	Verify configuration of close loop in DCADA and DMS together	N/A				
SYS.DMS(P3FAT).409	Verify Operator's notification in DMS	N/A				
SYS.DMS(P3FAT).410	Verify authority transfer from DCADA to DMS when a solution is not found	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT).411	Verify notification to Operator's in DMS when authority is transferred	N/A				
SYS.DMS(P3FAT).412	Verify VVC operation when DNA in DMS failover occurs while running. Check authority status and notification	N/A				
SYS.DMS(P3FAT).413	Verify VVC operation and notification after DNA in DMS failover occurs and stable situation is reestablished	N/A				
SYS.DMS(P3FAT).414	Verify VVC operation when DNA in DCADA failover occurs while running. Check authority status and notification	N/A				
SYS.DMS(P3FAT).415	Verify VVC operation and notification after DNA in DCADA failover occurs and stable situation is reestablished	N/A				
SYS.DMS(P3FAT).416	Verify VVC operation when DCADA and DMS get disconnected (communication failure)	N/A				
SYS.DMS(P3FAT).417	Verify VVC operation when DNA in DCADA is stopped or not available: * Automatic transfer of Authority * Operation stability	N/A				
SYS.DMS(P3FAT).418	Verify VVC operation when DNA in DMS is stopped or not available: * Automatic transfer of Authority * Operation stability	N/A				

System Test Book - DMS (Phase 3 Factory Acceptance Test) - Battery Points Checkout - User Interface (Graphical Display)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT-RTAC).1	Verify battery representation and data presented in UI (Device ID, Active Power Mode, Active Reactive Mode, Active Charge Mode, Active State, Active Status)	N/A				
SYS.DMS(P3FAT-RTAC).2	Verify Change in symbol and tag color based on active status	N/A				
System Test Book - DMS (Phase 3 Factory Acceptance Test) - Battery Points Checkout - User Interface (BESS - HMI Application)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT-RTAC).3	Verify access to BESS from InService	N/A				
SYS.DMS(P3FAT-RTAC).4	Verify BESS basic functions (One-Line Screen, System Status Screen, Snapshot Screen, Trend Data Screens, Stopping the BESS Remotely and Starting the BESS Remotely)	N/A				
System Test Book - DMS (Phase 3 Factory Acceptance Test) - Battery Points Checkout - Status Points : Indicators (DI)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT-RTAC).5	Verify P-to-P check for all indicator points (Active State, Active Status, Energy Available, et.)	N/A				
SYS.DMS(P3FAT-RTAC).6	Verify status point propagation in all modules is synchronized (InService > SCADA -> SICAM -> Battery Automation Controller RTAC)	N/A				
SYS.DMS(P3FAT-RTAC).7	Verify value representation, values and data quality	N/A				
SYS.DMS(P3FAT-RTAC).8	Verify data presented in Tabular displays	N/A				
SYS.DMS(P3FAT-RTAC).9	Verify all the alarm types and event reporting	N/A				
SYS.DMS(P3FAT-RTAC).10	Verify alarm and event list access	N/A				
System Test Book - DMS (Phase 3 Factory Acceptance Test) - Battery Points Checkout - Value Points (AI)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT-RTAC).10	Verify P-to-P check for all value points (Analog values reporting from the battery controller)	N/A				
SYS.DMS(P3FAT-RTAC).11	Verify value representation, values and data quality	N/A				
SYS.DMS(P3FAT-RTAC).12	Verify data presented in Tabular displays	N/A				
SYS.DMS(P3FAT-RTAC).13	Verify all the alarm types and event reporting	N/A				
SYS.DMS(P3FAT-RTAC).14	Verify alarm and event list access	N/A				
System Test Book - DMS (Phase 3 Factory Acceptance Test) - Battery Points Checkout - Operational Control Points (CO)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT-RTAC).15	Verify P-to-P check for all control points (BESS Operation ENABLE/DISABLE, Schedule Override, Reset BESS Alarms)	N/A				
SYS.DMS(P3FAT-RTAC).16	Verify control action procedure	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT-RTAC).17	Verification of control action time-out	N/A				
SYS.DMS(P3FAT-RTAC).18	Verification of control action failed	N/A				
SYS.DMS(P3FAT-RTAC).19	Verify control command failures (e.g when Active Power Mode, Set KVAR discharged rate)	N/A				
SYS.DMS(P3FAT-RTAC).20	Verification of system behavior in case of control "rejected" or "failed"	N/A				
SYS.DMS(P3FAT-RTAC).21	Verify reporting and logging of control actions, successful and failed	N/A				
SYS.DMS(P3FAT-RTAC).22	Verify error reporting and logging (Some error conditions need to be generated)	N/A				
System Test Book - DMS (Phase 3 Factory Acceptance Test) - Battery Points Checkout - Operational Mode Set Points						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT-RTAC).22	Verify that the BESS must be "ENABLED" to accept Operator's controls	N/A				
SYS.DMS(P3FAT-RTAC).23	Verify analog controls set points: Operational Modes Set Points (Power, Reactive, Charge)	N/A				
SYS.DMS(P3FAT-RTAC).24	Verify Power Mode set points: 0 = OFF 1 = Fixed kW 2 = Load Following (Circuit) 3 = Load Following (Bus) 4 = Load Following (Transformer) 5 = DERM (Not part of scope at the moment) 6 = Islanding (Not part of scope at the moment)	N/A				
SYS.DMS(P3FAT-RTAC).25	Verify control completion (returned value/point)	N/A				
SYS.DMS(P3FAT-RTAC).26	Verify set control failures	N/A				
SYS.DMS(P3FAT-RTAC).27	Verification of system behavior in case of set points are "rejected" or "failed"	N/A				
SYS.DMS(P3FAT-RTAC).28	Verify interlocking conditions: Check for set point limits and values out of range as invalid input	N/A				
SYS.DMS(P3FAT-RTAC).29	Verify interlocking conditions: Multiple user/consoles	N/A				
SYS.DMS(P3FAT-RTAC).30	Verify reporting and logging of control actions, successful and failed	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT-RTAC).31	Verify error reporting and logging (Some error conditions need to be generated)	N/A				
SYS.DMS(P3FAT-RTAC).32	Verify Reactive Mode set points: 0 = OFF 1 = Fixed kVAR 2 = Fixed Power Factor (Circuit) 3 = Fixed Power Factor (Bus) 4 = Fixed Power Factor (Transformer)	N/A				
SYS.DMS(P3FAT-RTAC).33	Verify control completion (returned value/point)	N/A				
SYS.DMS(P3FAT-RTAC).34	Verify set contol failures	N/A				
SYS.DMS(P3FAT-RTAC).35	Verification of system behavior in case of set points are "rejected" or "failed"	N/A				
SYS.DMS(P3FAT-RTAC).36	Verify intelocking conditions: Check for set point limits and alues out of range as invalid input	N/A				
SYS.DMS(P3FAT-RTAC).37	Verify intelocking conditions: Multiple user/consoles	N/A				
SYS.DMS(P3FAT-RTAC).38	Verify reporting and logging of control actions, successful and failed	N/A				
SYS.DMS(P3FAT-RTAC).39	Verify error reporting and logging (Some error conditions need to be generated)	N/A				
SYS.DMS(P3FAT-RTAC).40	Verify Charge Mode set points: 0 = OFF 1 = Fixed kW 2 = Load Following Circuit (Circuit) 3 = Load Following (Bus) 4 = Load Following (Transformer) 5 = DERM (Not part of scope at the moment)	N/A				
SYS.DMS(P3FAT-RTAC).41	Verify control completion (returned value/point)	N/A				
SYS.DMS(P3FAT-RTAC).42	Verify set contol failures	N/A				
SYS.DMS(P3FAT-RTAC).43	Verification of system behavior in case of set points are "rejected" or "failed"	N/A				
SYS.DMS(P3FAT-RTAC).44	Verify intelocking conditions: Check for set point limits and alues out of range as invalid input	N/A				
SYS.DMS(P3FAT-RTAC).45	Verify intelocking conditions: Multiple user/consoles	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT-RTAC).46	Verify reporting and logging of control actions, successful and failed	N/A				
SYS.DMS(P3FAT-RTAC).47	Verify error reporting and logging (Some error conditions need to be generated)	N/A				
System Test Book - DMS (Phase 3 Factory Acceptance Test) - Battery Points Checkout - Value Set Points (AD)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3FAT-RTAC).48	Verify analog value controls (set points): Operator Keyed Set Points (Max Charge rate, LF, Discharge time, duration, etc.)	N/A				
SYS.DMS(P3FAT-RTAC).49	Verify control completion (value change)	N/A				
SYS.DMS(P3FAT-RTAC).50	Verify set control failures	N/A				
SYS.DMS(P3FAT-RTAC).51	Verification of system behavior in case of set points are "rejected" or "failed"	N/A				
SYS.DMS(P3FAT-RTAC).52	Verify interlocking conditions: Check for set point limits	N/A				
SYS.DMS(P3FAT-RTAC).53	Verify interlocking conditions: Multiple user/consoles	N/A				
SYS.DMS(P3FAT-RTAC).54	Verify reporting and logging of control actions, successful and failed	N/A				
SYS.DMS(P3FAT-RTAC).55	Verify error reporting and logging (Some error conditions need to be generated)	N/A				

System Test Book – DMS (Phase 3 Site Acceptance Test): DNA – System Test						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3SAT).48	Verify Cyber security rules and conditions for DNA applications (Similar to the ones defined for the rest of the system components) There are basic security requirements for the systems that need to be verified for this solution: * Users definition (password hardening, authorities, permissions) * Log On/Off characteristics (allowed attempts, time outs) * Logging of all actions * System users/passwords * Remote log ins and connections	N/A				
SYS.DMS(P3SAT).55	Verify automatic failover at the substation level when DCADA application has problems or the SW detects errors	N/A				
SYS.DMS(P3SAT).59	Verify DSCADA and DNA redundancy and failover caused by application or SW problems	N/A				
SYS.DMS(P3SAT).60	Verify DNA, SCADA functions manual failover	N/A				
SYS.DMS(P3SAT).177	Verify system tools to save event log, system log and specific DNA data to external media	N/A				
SYS.DMS(P3SAT).416	Verify VVC operation when DCADA and DMS get disconnected (communication failure)	N/A				
System Test Book – DMS (Phase 3 Site Acceptance Test): DNA – Core Distribution Management System						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3SAT).162	Verify JC&G functionality in DNA	N/A				
SYS.DMS(P3SAT).165	Verifies DNA execution when setting or removing temporary elements	N/A				
SYS.DMS(P3SAT).172	Verification of tagging propagation to DNA	N/A				
SYS.DMS(P3SAT).199	Verify access denial to undefined users or wrong password	N/A				
SYS.DMS(P3SAT).200	Verify use of permissions for different users	N/A				
SYS.DMS(P3SAT).201	Verify context management	N/A				
SYS.DMS(P3SAT).202	Verify access to study context and case management	N/A				
SYS.DMS(P3SAT).203	Verify simultaneous use of multiple contexts and cases	N/A				
System Test Book – DMS (Phase 3 Factory Acceptance Test): DNA - Distribution System Power Flow (DSPF)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3SAT).205	From InService demonstrate access to PowerFlow connecting to the DNA in DMS	N/A				
SYS.DMS(P3SAT).207	Verify access to application alarms or program output	N/A				
SYS.DMS(P3SAT).228	Run Power Flow from DMS DNA UI and verify results	N/A				
SYS.DMS(P3SAT).242	Verify access to list and summaries using DNA UI in the DMS	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3SAT).229	Verify PowerFlow execution "on demand"	N/A				
SYS.DMS(P3SAT).229a	Verify PowerFlow execution in loop	N/A				
SYS.DMS(P3SAT).230	Verify DNA PF operation with multiple users	N/A				
SYS.DMS(P3SAT).231	Verify DNA PF operation with simultaneous execution from multiple users	N/A				
SYS.DMS(P3SAT).235	Introduce manual data changes (JC&G) and verify results	N/A				
SYS.DMS(P3SAT).244	Verify alarms generated by Limit violation or other operational conditions like non convergence	N/A				
SYS.DMS(P3SAT).258	Verify Simulation mode	N/A				
SYS.DMS(P3SAT).259	Verify use and options in Simulation mode	N/A				
SYS.DMS(P3SAT).260	Verify visual differentiation of operational mode: Real Time and Simulation	N/A				
System Test Book – DMS (Phase 3 Site Acceptance Test): DNA - Distribution System State Estimation (DSSE)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3SAT).211	Run DSSE from DMS DNA UI and verify results * On Demand	N/A				
SYS.DMS(P3SAT).212	Verify DSSE different modes of execution in DMS: * Periodic * Measurements validation display	N/A				
SYS.DMS(P3SAT).212a	Verify DSSE execution triggered by Event	N/A				
SYS.DMS(P3SAT).216	Verify access to application alarms or program output	N/A				
SYS.DMS(P3SAT).212b	Verify DSSE execution triggered by Overload	N/A				
SYS.DMS(P3SAT).212c	Verify DSSE execution triggered by Over/Under Voltage	N/A				
SYS.DMS(P3SAT).213	Verify DNA DSSE operation with multiples execution types (cyclic, spontaneous, on demand)	N/A				
SYS.DMS(P3SAT).214	Verify DNA DSSE operation with simultaneous execution from multiple users	N/A				
SYS.DMS(P3SAT).217a	Reverse flow verification/alarm	N/A				
SYS.DMS(P3SAT).217b	Verify island condition	N/A				
SYS.DMS(P3SAT).218	Introduce manual data changes and verify results	N/A				
System Test Book – DMS (Phase 3 Site Acceptance Test): DNA - Fault Isolation & Service Restoration (FISR)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3SAT).331i	Verify FISR execution in Restore to Normal mode	N/A				
SYS.DMS(P3SAT).331n	Verify FISR execution in Look Ahead Mode	N/A				
SYS.DMS(P3SAT).352	Verify use and management of Study Context (Create, save & restore cases)	N/A				
SYS.DMS(P3SAT).353	Verify use of multiple Study contexts at the same time	N/A				
SYS.DMS(P3SAT).354	Verify FISR results in Study context.	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3SAT).355	Verify FISR operation in case of abnormal situations, user errors,.... in Study context	N/A				
SYS.DMS(P3SAT).330	Verify FISR execution manually	N/A				
SYS.DMS(P3SAT).330a	Verify FISR execution to isolate a device	N/A				
SYS.DMS(P3SAT).330b	Verify FISR execution triggered by FLOC.	N/A				
System Test Book – DMS (Phase 3 Site Acceptance Test): DNA - Fault Location (FLOC)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3SAT).320	Verify FLOC application UI displays	N/A				
SYS.DMS(P3SAT).303a	Verify that FLOC runs when fault detected in between reclosers	N/A				
SYS.DMS(P3SAT).303b	Verify that FLOC runs when recloser open	N/A				
SYS.DMS(P3SAT).303c	Verify that FLOC runs substation switch open	N/A				
SYS.DMS(P3SAT).303d	Verify that FLOC runs when fault detected	N/A				
SYS.DMS(P3SAT).303e	Verify that FLOC runs when fault detected in between reclosers away from the FI	N/A				
SYS.DMS(P3SAT).306	Verify interaction with application in InService	N/A				
SYS.DMS(P3SAT).307	Verify interaction with application in DNA UI	N/A				
SYS.DMS(P3SAT).309	Verify access to application alarms or program output	N/A				
SYS.DMS(P3SAT).310a	Verify FLOC operation with multiple simultaneous faults	N/A				
SYS.DMS(P3SAT).310f	Verify FLOC provides correct pre-Fault status	N/A				
SYS.DMS(P3SAT).313	Verify that only permanent reclosure faults triggers FLOC	N/A				
SYS.DMS(P3SAT).321	Verify FLOC interfaces with FISR and OMS	N/A				
System Test Book – DMS (Phase 3 Site Acceptance Test): DNA - Feeder Load Transfer (FLT)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3SAT).262	Verify access to FLT from InService	N/A				
SYS.DMS(P3SAT).263	Verify FLT running from DMS	N/A				
SYS.DMS(P3SAT).275	Verify access to application alarms or program output	N/A				
SYS.DMS(P3SAT).283	Access to FLT results and info from InService	N/A				
SYS.DMS(P3SAT).298	Verify FLT running in simulation mode	N/A				
SYS.DMS(P3SAT).299	Verify use and options in Simulation mode	N/A				
SYS.DMS(P3SAT).300	Verify visual differentiation of operational mode: Real Time and Simulation	N/A				
SYS.DMS(P3SAT).302	Verify reporting of execution errors or problems in Simulation Mode	N/A				
System Test Book – DMS (Phase 3 Site Acceptance Test): DNA – Volt Var Control (VVC)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3SAT).357	Verify VVC execution in Open Loop and access to the Open Loop configuration from Inservice UI	N/A				
SYS.DMS(P3SAT).358	Verify VVC application management from Inservice UI	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3SAT).362	Verification of VVC configuration and parameters from DNA UI	N/A				
SYS.DMS(P3SAT).362a	VVC Manual execution	N/A				
SYS.DMS(P3SAT).362	Verification of VVC parameters in Study Context	N/A				
SYS.DMS(P3SAT).366	Verify multiple Study context at the same time	N/A				
SYS.DMS(P3SAT).367	Verify result in Study context (simulation)	N/A				
SYS.DMS(P3SAT).377	Verify VVC execution triggered by high/low limit violations	N/A				
SYS.DMS(P3SAT).377a	Verify VVC execution triggered by topology change	N/A				
SYS.DMS(P3SAT).377b	Verify VVC execution cyclic triggering	N/A				
SYS.DMS(P3SAT).377c	Verify VVC execution triggered by event while cyclic execution enabled	N/A				
SYS.DMS(P3SAT).378	Verify that DDSE will run automatically when needed	N/A				
SYS.DMS(P3SAT).379	Verify VVC results of the sequence generated and executed	N/A				
SYS.DMS(P3SAT).380	Verify VVC reaction multiple trigger actions at the same time	N/A				
SYS.DMS(P3SAT).391	Verify VVC execution defining Remove/Mitigate limit violation objective	N/A				
SYS.DMS(P3SAT).391a	Verify VVC execution defining Power Loss minimization without limit violations	N/A				
SYS.DMS(P3SAT).391b	Verify VVC execution defining Minimization of Active load consumption objective	N/A				
SYS.DMS(P3SAT).391c	Verify VVC execution defining Minimization of Reactive load consumption objective	N/A				
SYS.DMS(P3SAT).391e	Verify VVC execution defining Power Loss Minimization with limit violations	N/A				
SYS.DMS(P3SAT).392	Verify VVC execution using only controllable devices	N/A				
SYS.DMS(P3SAT).392g	Verify that VVC considers Power Factor limits at the feeder head	N/A				
SYS.DMS(P3SAT).392h	Constrains relaxation	N/A				
SYS.DMS(P3SAT).393	Verify VVC execution with tagged devices	N/A				
SYS.DMS(P3SAT).394	Verify VVC execution of control sequence when control fails	N/A				
SYS.DMS(P3SAT).395	Verify VVC reaction to a situation with no controllable devices	N/A				
SYS.DMS(P3SAT).396	Verify VVC reaction to topology changes between calculation and execution	N/A				
SYS.DMS(P3SAT).397	Verify reporting of execution errors or problems	N/A				
SYS.DMS(P3SAT).398	Verify Close Loop Operation in DMS	N/A				
SYS.DMS(P3SAT).399	Verify that DDSE will run automatically when needed as part of the VVC close loop execution	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3SAT).400	Verify Close Loop execution failures and system reaction: * Control fails * Device Tagging * Device already in requested position	N/A				
SYS.DMS(P3SAT).401	Verify Close Loop execution with limit conditions: * Max number of daily operations * Usability Time runs out * Control values out of range	N/A				
SYS.DMS(P3SAT).420	Verify that VVC sends a SCADA Override signal to Cap Banks in Manual and Remote in the selected injection area	N/A				
SYS.DMS(P3SAT).421	Verify that VVC sends a SCADA Override signal to Cap Banks in Manual and Remote in the selected area	N/A				
SYS.DMS(P3SAT).422	Verify that the Heart Beat signal is sent every 45 minutes	N/A				
SYS.DMS(P3SAT).424	Leave Open Loop mode	N/A				
SYS.DMS(P3SAT).426	Enter VVC Closed Loop	N/A				
SYS.DMS(P3SAT).427	Run VVC Closed Loop Mode with excluded injections	N/A				
SYS.DMS(P3SAT).428	Leave VVC Closed Loop Mode for All Injections (Master Settings)	N/A				

System Test Book - DMS (Phase 3 Site Acceptance Test) - Recloser Point to Point Checkout: Type DI						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3SAT-P2P-651R).1	Verify point "Enabled"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3SAT-P2P-651R).2	Verify point "Device Status"	Values Displayed: - OPEN - CLOSE				
SYS.DMS(P3SAT-P2P-651R).3	Verify point "Loss of Potential"	Values Displayed: - OK - ALARM				
SYS.DMS(P3SAT-P2P-651R).4	Verify point "Fault - Phase C"	Values Displayed: - OK - ALARM				
SYS.DMS(P3SAT-P2P-651R).5	Verify point "Fault - Phase B"	Values Displayed: - OK - ALARM				
SYS.DMS(P3SAT-P2P-651R).6	Verify point "Fault - Phase A"	Values Displayed: - OK - ALARM				
SYS.DMS(P3SAT-P2P-651R).7	Verify point "Sync Check Elements "	Values Displayed: - OK - ALARM				
SYS.DMS(P3SAT-P2P-651R).8	Verify point "Cabinet Door"	Values Displayed: - OK - ALARM				
SYS.DMS(P3SAT-P2P-651R).9	Verify point "50CO - Ground Overcurrent Status"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3SAT-P2P-651R).10	Verify point "79CO - Reclosing Status"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3SAT-P2P-651R).11	Verify point "Local - Remote"	Values Displayed: - LOCAL - REMOTE				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3SAT-P2P-651R).12	Verify point "Fast Curves Status"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3SAT-P2P-651R).13	Verify point "Push Buttons Locked"	Values Displayed: - UNLOCKED - LOCKED				
SYS.DMS(P3SAT-P2P-651R).14	Verify point "Hot Line Tag Status"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3SAT-P2P-651R).15	Verify point "Aux 1 Status"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3SAT-P2P-651R).16	Verify point "Aux 2 Status"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3SAT-P2P-651R).17	Verify point "Aux 3 Status"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3SAT-P2P-651R).18	Verify point "Battery Failure "	Values Displayed: - OK - ALARM				
SYS.DMS(P3SAT-P2P-651R).19	Verify point "External Power"	Values Displayed: - OFF - ON				
SYS.DMS(P3SAT-P2P-651R).20	Verify point "Lockout"	Values Displayed: - OK - ALARM				
SYS.DMS(P3SAT-P2P-651R).21	Verify point "Current Direction"	Values Displayed: - NORMAL - REVERSED				
SYS.DMS(P3SAT-P2P-651R).22	Verify point "Contact Wear - 3 Phase"	Values Displayed: - OK - ALARM				
SYS.DMS(P3SAT-P2P-651R).23	Verify point "Clock Present"	Values Displayed: - NOT PRESENT - PRESENT				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3SAT-P2P-651R).24	Verify point "Hardware Alarm"	Values Displayed: - OK - ALARM				
SYS.DMS(P3SAT-P2P-651R).25	Verify point "Software Alarm"	Values Displayed: - OK - ALARM				
System Test Book - DMS (Phase 3 Site Acceptance Test) - Recloser Point to Point Checkout: Type DO						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3SAT-P2P-651R).26	Verify point "Aux 1"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3SAT-P2P-651R).27	Verify point "Aux 2"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3SAT-P2P-651R).28	Verify point "Aux 3"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3SAT-P2P-651R).29	Verify point "Aux 4"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3SAT-P2P-651R).30	Verify point "50CD - Ground Overcurrent"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3SAT-P2P-651R).31	Verify point "79CD - Reclosing"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3SAT-P2P-651R).32	Verify point "Fast Curves"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3SAT-P2P-651R).33	Verify point "Hot Line Tag"	Values Displayed: - DISABLED - ENABLED				
SYS.DMS(P3SAT-P2P-651R).34	Verify point "Device Operate"	Values Displayed: - OPEN - CLOSE				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3SAT-P2P-651R).35	Verify point "Reset Front Panel Targets"	Values Displayed: - NA - RESET				
System Test Book - DMS (Phase 3 Site Acceptance Test) - Recloser Point to Point Checkout: Type CTR						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3SAT-P2P-651R).36	Verify point "Active Settings Group"	N/A				
SYS.DMS(P3SAT-P2P-651R).37	Verify point "Internal Breaker Trips - Phase A "	N/A				
SYS.DMS(P3SAT-P2P-651R).38	Verify point "Internal Breaker Trips - Phase B "	N/A				
SYS.DMS(P3SAT-P2P-651R).39	Verify point "Internal Breaker Trips - Phase C "	N/A				
SYS.DMS(P3SAT-P2P-651R).40	Verify point "External Breaker Trips - Phase A "	N/A				
SYS.DMS(P3SAT-P2P-651R).41	Verify point "External Breaker Trips - Phase B"	N/A				
SYS.DMS(P3SAT-P2P-651R).42	Verify point "External Breaker Trips - Phase C"	N/A				
System Test Book - DMS (Phase 3 Site Acceptance Test) - Recloser Point to Point Checkout: Type AI						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3SAT-P2P-651R).43	Verify point "Current - Phase A"	N/A				
SYS.DMS(P3SAT-P2P-651R).44	Verify point "Current - Phase B"	N/A				
SYS.DMS(P3SAT-P2P-651R).45	Verify point "Current - Phase C"	N/A				
SYS.DMS(P3SAT-P2P-651R).46	Verify point "Current - Neutral"	N/A				
SYS.DMS(P3SAT-P2P-651R).47	Verify point "Current - Ground"	N/A				
SYS.DMS(P3SAT-P2P-651R).48	Verify point "Voltage - Phase A - Y"	N/A				
SYS.DMS(P3SAT-P2P-651R).49	Verify point "Voltage - Phase B - Y"	N/A				
SYS.DMS(P3SAT-P2P-651R).50	Verify point "Voltage - Phase C - Y"	N/A				
SYS.DMS(P3SAT-P2P-651R).51	Verify point "Voltage - Phase A - Z"	N/A				
SYS.DMS(P3SAT-P2P-651R).52	Verify point "Voltage - Phase B - Z"	N/A				
SYS.DMS(P3SAT-P2P-651R).53	Verify point "Voltage - Phase C - Z"	N/A				
SYS.DMS(P3SAT-P2P-651R).54	Verify point "Real Power - Phase A"	N/A				
SYS.DMS(P3SAT-P2P-651R).55	Verify point "Real Power - Phase B"	N/A				
SYS.DMS(P3SAT-P2P-651R).56	Verify point "Real Power - Phase C"	N/A				
SYS.DMS(P3SAT-P2P-651R).57	Verify point "Real Power - 3 Phase"	N/A				
SYS.DMS(P3SAT-P2P-651R).58	Verify point "Reactive Power - Phase A"	N/A				
SYS.DMS(P3SAT-P2P-651R).59	Verify point "Reactive Power - Phase B"	N/A				
SYS.DMS(P3SAT-P2P-651R).60	Verify point "Reactive Power - Phase C"	N/A				
SYS.DMS(P3SAT-P2P-651R).61	Verify point "Reactive Power - 3 Phase"	N/A				
SYS.DMS(P3SAT-P2P-651R).62	Verify point "Frequency"	N/A				
SYS.DMS(P3SAT-P2P-651R).63	Verify point "Contact Wear - Phase A"	N/A				
SYS.DMS(P3SAT-P2P-651R).64	Verify point "Contact Wear - Phase B"	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3SAT-P2P-651R).65	Verify point "Contact Wear - Phase C"	N/A				
SYS.DMS(P3SAT-P2P-651R).66	Verify point "Fault Type "	N/A				
SYS.DMS(P3SAT-P2P-651R).67	Verify point "Fault Recloser Shot Counter "	N/A				
SYS.DMS(P3SAT-P2P-651R).68	Verify point "Fault Time"	N/A				
SYS.DMS(P3SAT-P2P-651R).69	Verify point "Fault Current - Phase A"	N/A				
SYS.DMS(P3SAT-P2P-651R).70	Verify point "Fault Current - Phase B"	N/A				
SYS.DMS(P3SAT-P2P-651R).71	Verify point "Fault Current - Phase C"	N/A				
SYS.DMS(P3SAT-P2P-651R).72	Verify point "Fault Current - Ground"	N/A				
SYS.DMS(P3SAT-P2P-651R).73	Verify point "Apparent Power - Phase A"	N/A				
SYS.DMS(P3SAT-P2P-651R).74	Verify point "Apparent Power - Phase B"	N/A				
SYS.DMS(P3SAT-P2P-651R).75	Verify point "Apparent Power - Phase C"	N/A				
SYS.DMS(P3SAT-P2P-651R).76	Verify point "Apparent Power - 3 Phase"	N/A				
SYS.DMS(P3SAT-P2P-651R).77	Verify point "THD - Current - Phase A"	N/A				
SYS.DMS(P3SAT-P2P-651R).78	Verify point "THD - Current - Phase B"	N/A				
SYS.DMS(P3SAT-P2P-651R).79	Verify point "THD - Current - Phase C"	N/A				
SYS.DMS(P3SAT-P2P-651R).80	Verify point "THD - Current - Neutral"	N/A				
SYS.DMS(P3SAT-P2P-651R).81	Verify point "THD - Voltage - Phase A - Y"	N/A				
SYS.DMS(P3SAT-P2P-651R).82	Verify point "THD - Voltage - Phase B - Y"	N/A				
SYS.DMS(P3SAT-P2P-651R).83	Verify point "THD - Voltage - Phase C - Y"	N/A				
SYS.DMS(P3SAT-P2P-651R).84	Verify point "THD - Voltage - Phase A - Z"	N/A				
SYS.DMS(P3SAT-P2P-651R).85	Verify point "THD - Voltage - Phase B - Z"	N/A				
SYS.DMS(P3SAT-P2P-651R).86	Verify point "THD - Voltage - Phase C - Z"	N/A				
SYS.DMS(P3SAT-P2P-651R).87	Verify point "Battery Voltage"	N/A				
SYS.DMS(P3SAT-P2P-651R).88	Verify point "Battery Current"	N/A				
System Test Book - DMS (Phase 3 Site Acceptance Test) - Recloser Point to Point Checkout: Type AO						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DMS(P3SAT-P2P-651R).89	Verify point "Set Active Settings Group"	N/A				

System Test Book - HIS (Phase 3 SAT)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HIS(P3SAT).1	User Access Right: Verify user access to HIS based on defined authorization	N/A				
SYS.HIS(P3SAT).2	User Access Right: Verify valid user access denied because of authorization	N/A				
SYS.HIS(P3SAT).3	User Access Right: Verify change of permissions while user connected	N/A				
SYS.HIS(P3SAT).5	Chart Data: Verify that User views can be saved (Public and Private)	N/A				
SYS.HIS(P3SAT).6	Export Data: Verify charting capabilities of the HIS	N/A				
SYS.HIS(P3SAT).7	Print Data: Verify HIS data exporting capabilities	N/A				
SYS.HIS(P3SAT).8	Filter Data: Verify HIS printing capabilities	N/A				
SYS.HIS(P3SAT).9	SCADA Data collection: Demonstrate filtering capabilities of the HIS UI	N/A				
SYS.HIS(P3SAT).10	SCADA Data collection: Verify that SCADA data is collected properly in HIS for Status	N/A				
SYS.HIS(P3SAT).11	SCADA Data collection: Verify that SCADA data is collected properly in HIS for Analog Values	N/A				
SYS.HIS(P3SAT).12	SCADA Data collection: Verify that SCADA data is collected properly in HIS for Accumulators	N/A				
SYS.HIS(P3SAT).13	SCADA Data collection; Verify that "Archive" flag in DB "True" or "False" change point archiving in HIS	N/A				
SYS.HIS(P3SAT).14	SCADA Data collection: Verify that Manual changes in InService are stored in HIS	N/A				
SYS.HIS(P3SAT).16	SCADA Data collection: Verify that Data Quality is archived with the values	N/A				
SYS.HIS(P3SAT).17	Collection Rates: Change collection rates for SCADA points and verify archiving in HIS	N/A				
SYS.HIS(P3SAT).19	Formula Calculations: Define a new calculation and verify values	N/A				
SYS.HIS(P3SAT).20	Data compression: Verify that data compression works according to user definition	N/A				
SYS.HIS(P3SAT).21	Aggregation Calculations: Verify correct calculation of Min, Max, Average and integrals (15m, 1 hour)	N/A				
SYS.HIS(P3SAT).22	Data Modification: Verify editing and logging of manual changes	N/A				
SYS.HIS(P3SAT).23	Data Modification: Verify recalculation of formulas and past values when historic value is changed	N/A				
SYS.HIS(P3SAT).24	Data Modification: Verify that HIS data remain in the archive after deleting a point in SCADA	N/A				
SYS.HIS(P3SAT).25	DMS failover: Verify that no data is lost in HIS when a failover occurs	N/A				
SYS.HIS(P3SAT).27	DMS failover: Verify that system buffer store data while HIS(ORACLE) is not available and that data is archived when available	N/A				
SYS.HIS(P3SAT).28	DMS failover: Verify HIS function/application redundancy	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HIS(P3SAT).30	DMS failover: Verify that HIS report "information", "warning" or "error" conditions	N/A				
SYS.HIS(P3SAT).31	Health Monitor Tool: Data Collection	N/A				
SYS.HIS(P3SAT).32	SQL Plus: Compression and aggregation	N/A				
SYS.HIS(P3SAT).33	SQL Plus: Demonstrate access to HIS data using SQL	N/A				

System Test Book - DERM: Base Data (BD)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DERM.BD4	Tariff and rate definition: Verify user can create tariff and rate and all objects and associated attributes.	User can create and maintain all objects and attributes associated with a specific tariff and rate.				
SYS.DERM.BD5	Grid Model Administration: Verify user can create and view Grid Model data.	User can view all objects and attributes associated with a specific Grid Model.				
SYS.DERM.BD6	Controls Administration: Verify user can create, modify and delete a device control.	User can create, modify and delete a control.				
SYS.DERM.BD7	Wholesale Product Administration: Verify that user can add, modify, and delete Wholesale Product.	N/A.				
SYS.DERM.BD8	Calendar Administration: Verify that user can view the Holidays and Season and update the dates.	N/A.				
SYS.DERM.BD9	Region Administration: Verify that user can view, create, modify, and delete the Region.	N/A.				
SYS.DERM.BD10	Weather Summary: Verify that user can view the weather Forecast and change the weather zone and weather station.	N/A.				
System Test Book - DERM: Enrollment and Contract Management (ENR)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DERM.ENR5	Customer Asset Enrollment: Verify user can create and maintain all objects and attributes associated with a specific end use customer asset.	User can create and maintain all objects and attributes associated with a specific end use customer.				
SYS.DERM.ENR3	Asset Administration: Verify user can view Asset data associated with a customer.	User can view Asset attributes				
SYS.DERM.ENR10	Meter Summary Interface: Verify user can view list of all meters with key attributes.	User can view list of all meters with key attributes.				
System Test Book - DERM: DR Program Creation and Administration (PCA)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DERM.PCA4.1	Program Entry/Modification: Verify user can view display allowing creation of a new DR Program, and modification of an existing DR Program attributes.	User can view display allowing entry and modification of Program attributes.				
SYS.DERM.PCA4.2	Program Summary: Verify user can view display listing available programs and their major attributes.	User can view display listing available programs and their major attributes.				
SYS.DERM.PCA4.3	Program Category: Verify user can view display listing all Programs according to their correct Category, Class and Type.	User can view display listing all Programs according to their correct Category, Class and Type.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DERM.PCA4.4	Tariff Entry/Modification: Verify user can view display allowing entry of tariff with its multiple attributes.	User can view display allowing entry of Tariff with its multiple attributes.				
SYS.DERM.PCA4.5	Tariff Summary: Verify user can view display listing all available Tariffs and their attributes.	User can view display listing all available Tariffs and their attributes.				
System Test Book - DERM: Customer Baseline Load Calculation (CBL)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DERM.CBL1	Definition: Verify user can select the following CBL types: Similar Day Statistical Average and NAESB/FERC.	User can select the following CBL types: Similar Day Statistical Average and NAESB/FERC.				
SYS.DERM.CBL2	Attributes: Verify user can specify the following parameter for each CBL type: Statistical Average (Number of days, smoothing factor, morning adjustment – number of hours before DR Event and NAESB/FERC (highest energy usage days, past non-event days, number of hours before DR to be used for Adjustment).	User can specify each of the listed parameters for each CBL type.				
SYS.DERM.CBL3	Similar Day Statistic: Verify user can calculate Similar Day Statistic Average using average consumption values from non-event days in the recent past.	User can calculate Similar Day Statistic Average using average consumption values from non-event days in the recent past.				
SYS.DERM.CBL6	X out of Y – NAESB/FERC CBL Calculation: Verify user can make NAESB/FERC CBL calculations.	User can make NAESB/FERC CBL calculations.				
SYS.DERM.CBL8	Definition Display: Verify user can view display allowing user to review/modify existing CBLs and/or create new CBLs.	User can view display allowing user to review/modify existing CBLs and/or create new CBLs.				
SYS.DERM.CBL9	Summary Display: Verify user can view display allowing the user to view CBL summary data or select a baseline to view and update.	User can view display allowing the user to view CBL summary data or select a baseline to view and update.				
System Test Book - DERM: Aggregation and Virtual Power Plant Creation (AVP)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DERM.AVP1-3	Axes of Aggregation: Verify user can create DR Resources based on asset type, customer category/class/type, demand response programs, and grid location.	User can create DR Resources based on asset type, customer category/class/type, demand response programs, and grid location.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DERM.AVP2	Multiple Program Enrollments: Verify user can register an asset under more than one program, and be part of more than one aggregated Resource.	User can register an asset under more than one program and can be part of more than one aggregated Resource.				
SYS.DERM.AVP4	Dynamic Resource: Verify user can create a resource as a Dynamic Resource by specifying filters.	User can create a resource as a Dynamic Resource by specifying filters.				
SYS.DERM.AVP5	Static Resource: Verify user can create a resource as a Static Resource consisting of all assets that are assigned to the resource.	User can create a resource as a Static Resource consisting of all assets that are assigned to the resource.				
SYS.DERM.AVP7	Asset to Resource Re-assignment: Verify user can update the list of Assets within the Program Default Resource on demand.	User can update the list of Assets within the Program Default Resource on demand.				
SYS.DERM.AVP13	Modify Existing Resource: Verify user can call up an existing Static or Dynamic Resource and modify its definition.	User can call up an existing Static or Dynamic Resource and modify its definition.				
SYS.DERM.AVP16	Resource Summary: Verify that the Resource Summary display shows the list of all the Resources created in the system with the corresponding attributes.	Resource Summary display shows the list of all the Resources created in the system with the corresponding attributes.				
System Test Book - DERM: DR Availability Assessment and Forecasting (AVF)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DERM.AVF1	Assets and DR Programs Constraint: Verify user can determine available DR capabilities for the current time as well as a time period in the future at different locations, DR program(s), Product, Asset Type, Customer Type, or for an existing Resource.	User can determine available DR capabilities for the current time as well as a time period in the future at different locations, DR program(s), Product, Asset Type, Customer Type, or for an existing Resource.				
SYS.DERM.AVF2+3	Availability Factor Profile: Verify user can view the availability factor profile and can specify the hourly availability factor.	User can view the various defined availability factor profile and can specify the hourly availability factor as a function of heat index.				
SYS.DERM.AVF4+5	Availability Factor Dependency and Availability factor Assignment: Verify that the Availability Factor of an asset can be a function of time (time of the day) and heat index.	The Availability Factor of an asset can be a function of time (time of the day) and heat index.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DERM.AVF8	DR Program Constraints: Verify that the availability assessment takes into account all the constraints related to selected DR Program.	Availability assessment takes into account all the constraints related to selected DR Program.				
System Test Book - DERM: DR Scheduling and Optimization (SCH)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DERM.SCH1-20+26	OATI webDistribute Schedule - General Requirements: Verify user can create a DR Schedule.	User can create a DR Schedule				
SYS.DERM.SCH21	OATI webDistribute Schedule - General Requirements: Verify that user can view the list of all DR Schedules that have been entered in webDistribute through Schedule Summary display.	User can view the list of all DR Schedules that have been entered in webDistribute through the Schedule Summary display.				
SYS.DERM.SCH27	User Interface: Verify that a display is provided to allow user to create a DR Schedule by specifying a DR Schedule Period (Start and End date/time).	Display is provided to allow user to create a DR Schedule by specifying a DR Schedule Period (Start and End date/time).				
SYS.DERM.SCH28	User Interface: Verify that a display is provided to show a summary of available DR Schedules with the specified profile and status.	A display is provided to show a summary of available DR Schedules with the specified profile and status.				
System Test Book - DERM: Distribution Grid Management (DGM)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DERM.DGM1	Distribution Grid Overloads: The DMS operator will send information on grid overloads. webDistribute will use measured voltages, current, and flow, and using the ratings of equipment will determine the amount of DR required.	User can monitor the information received from DMS and verify the calculated DR requested.				
SYS.DERM.DGM2	Determination of the required DR to alleviate overloads and the availability of DR for the same: Verify that the program has the capability to determine the amount of DR required to alleviate the overloads and its capability to determine the amount of DR that is available.	The level of KW overload can be calculated based on the calculated Voltage and ampere measurements, and the amount of DR available to deal with the overload can be calculated.				
SYS.DERM.DGM3	Selection of level of DR and Scheduling DR Events: Verify that that the user can select the amount of DR and schedule resources to deal with the selected overloads.	The use can select all or some portion of the available DR capability and schedule DR events.				
System Test Book - DERM: DR Performance Monitoring (PFM)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DERM.PFM1	Real-Time Performance Monitoring: Using Real-Time DR monitoring, verify user can monitor DR performance using the latest energy meter readings and/or telemetry (RTU) measurements received through SCADA.	User can monitor DR values using the latest energy meter readings and/or telemetry (RTU) measurements received through SCADA.				
SYS.DERM.PFM2	After-the-Fact PFM for DR Event, Program, Zone, UDC: Verify that After-the-Fact PFM can be calculated by comparing the metered energy consumption of each participating DR customer and corresponding adjusted CBL values.	After-the-Fact PFM can be calculated by comparing the metered energy consumption of each participating DR customer and corresponding adjusted CBL values.				
SYS.DERM.PFM3	After-the-Fact Grid Topology Based DR PFM: Verify that by using a combination of DMS/D-SCADA historical archived data together with AMI energy meters, user can monitor DR performance per distribution grid topology (feeder/substation).	User can monitor DR performance per distribution grid topology (feeder/substation).				
SYS.DERM.PFM4	PFM User Interface: Verify that PFM User interface (UI) is presented in the form of tables and graphs.	PFM User Interface (UI) is presented in the form of tables and graphs.				
System Test Book - DERM: Customer Configuration (KCPL)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DERM.KCPL1	Asset Type Configuration: Verify KCP&L asset classifications are defined to correspond to the requested KCP&L Program types.	KCP&L asset classifications are defined to correspond to the requested KCP&L Program types.				
SYS.DERM.KCPL2	Asset Grouping Configuration: Verify asset groups are created to balance across phases, transformers and feeders.	Asset groups are created to balance across phases, transformers and feeders.				
SYS.DERM.KCPL3	Program Type Configuration: Verify configuration of KCP&L required program types.	KCP&L required program types are configured.				
SYS.DERM.KCPL4	Customer Class Configuration: Verify KCP&L's customer class name is the default customer type name for the class.	KCP&L's customer class name is the default customer type name for the class.				
SYS.DERM.KCPL5	Product Configuration: Verify that only one KCP&L products is configured: Energy.	Only one KCP&L products is configured: Energy.				
SYS.DERM.KCPL7	Weather Station Configuration: Verify that only a single weather station will be used for creating the Load Forecast and for calculating asset availability assessments.	A single weather station will be used for creating the Load Forecast and for calculating asset availability assessments.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.DERM.KCPL8	Contract and Rate Configuration: Verify implementation of KCP&L contract parameters, program parameters and performance metrics.	KCP&L contract parameters, program parameters and performance metrics are implemented.				

System Test Book – Meter Data Management (MDM): MDM Setup & Configuration						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.MDM.INT.SETUP.1	Access EnergyIP (EIP) web based user interface	N/A				
SYS.MDM.INT.SETUP.2	Access EnergyIP (EIP) SFTP server - Push Billing Account	N/A				
SYS.MDM.INT.SETUP.3	Access EnergyIP (EIP) SFTP server - Meter Reads Account	N/A				
SYS.MDM.INT.SETUP.4	Access EnergyIP (EIP) web services server	N/A				
SYS.MDM.INT.SETUP.5	Access EnergyIP (EIP) web service for MDM FlexSync interface	N/A				
SYS.MDM.INT.SETUP.6	Access EnergyIP (EIP) web service for MDM Pull Billing Interface	N/A				
System Test Book – Meter Data Management (MDM): Role Based Access Control						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.MDM.INT.RBAC.1	Validate capabilities of the PIPEOP operational user role	N/A				
SYS.MDM.INT.RBAC.2	Validate capabilities of the PIPEMGR data manager role	N/A				
SYS.MDM.INT.RBAC.3	Validate capabilities of the PIPEADMIN data manager role	N/A				
SYS.MDM.INT.RBAC.4	Validate user / role assignments for Test environment	N/A				
System Test Book – Meter Data Management (MDM): General User Interface Functionality						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.MDM.INT.UI.1	Shakeout basic functionality using the "operational user" account	N/A				
SYS.MDM.INT.UI.2	Shakeout basic functionality using the "data manager" account	N/A				
SYS.MDM.INT.UI.3	Shakeout basic functionality using the "systems administrator" account	N/A				
System Test Book – Meter Data Management (MDM): Monthly Meter Read Schedule Setup						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.MDM.INT.MMRS.1	Validate Monthly Meter Read Schedule file format	N/A				
SYS.MDM.INT.MMRS.2	Validate that the Monthly Meter Read Schedule has been loaded successfully in MDM	N/A				
System Test Book – Meter Data Management (MDM): MDM Validation, Estimation, Editing (VEE) Functionality						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.MDM.INT.VEE.1	Validate Manual VEE Capabilities	N/A				
SYS.MDM.INT.VEE.2	MDM Register Read Estimator will perform "Extrapolation" on missing interval reads	N/A				
SYS.MDM.INT.VEE.3	MDM Register Read Estimator will replace "Extrapolated" values with actual values when received	N/A				
SYS.MDM.INT.VEE.4	MDM Register Read Estimator will perform "Interpolation" on missing interval reads	N/A				
SYS.MDM.INT.VEE.5	MDM Register Read Estimator will replace "Interpolated" values with actual values when received	N/A				
SYS.MDM.INT.VEE.6	MDM Register Read Estimator will perform "Extrapolation" on missing register reads	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.MDM.INT.VEE.7	MDM Register Read Estimator will replace "Extrapolated" register read values with actual values when received	N/A				
SYS.MDM.INT.VEE.8	MDM Register Read Estimator will perform "Interpolation" on missing register reads	N/A				
SYS.MDM.INT.VEE.8	MDM Register Read Estimator will replace "Interpolated" register read values with actual values when received	N/A				
System Test Book – Meter Data Management (MDM): MDM Reports						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.MDM.INT.RPTS.1	Validate the following EIP report: AMR Installation Status	N/A				
SYS.MDM.INT.RPTS.2	Validate the following EIP report: Billing Data Change Report	N/A				
SYS.MDM.INT.RPTS.3	Validate the following EIP report: Billing No Reads Report	N/A				
SYS.MDM.INT.RPTS.4	Validate the following EIP report: Billing Service Summary Report	N/A				
SYS.MDM.INT.RPTS.5	Validate the following EIP report: DBSync Exception Report	N/A				
SYS.MDM.INT.RPTS.6	Validate the following EIP report: Estimation Failure Detail Report	N/A				
SYS.MDM.INT.RPTS.7	Validate the following EIP report: Excessive Missing Reads Report	N/A				
SYS.MDM.INT.RPTS.8	Validate the following EIP report: Frammer Exception Report	N/A				
SYS.MDM.INT.RPTS.9	Validate the following EIP report: Frammer Exception Report	N/A				
SYS.MDM.INT.RPTS.10	Validate the following EIP report: Missing Reads Report	N/A				
SYS.MDM.INT.RPTS.11	Validate the following EIP report: Service Request Summary Report	N/A				
SYS.MDM.INT.RPTS.12	Validate the following EIP report: Unauthorized Usage Report	N/A				
SYS.MDM.INT.RPTS.13	Validate the following EIP report: Validation Failure Detail Report	N/A				
SYS.MDM.INT.RPTS.14	Validate the following EIP report: VEE Summary Report	N/A				
System Test Book – Meter Data Management (MDM): MDM – Other						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.MDM.INT.OTHER.1	Validate creation and retrieval of the Push Billing File by MDM to KCP&L	N/A				
SYS.MDM.INT.OTHER.2	Validate that CT/PT was applied to meter read data to calculate proper kWh usage values	N/A				

System Test Book – AMI Head End (AHE): Core Capability - Command Center Initial Configuration						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.AHE(Core).1	Command Center Installation and Verification	Collector in NORMAL Mode, with ability to PING the Collector				
SYS.AHE(Core).2	Configure Users	Create a NEW User				
System Test Book – AMI Head End (AHE): Core Capability - Meter Manufacturing File Import						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.AHE(Core).3	Import MMF file	Upload MMF successfully, and meters transition to Discovered state				
System Test Book – AMI Head End (AHE): Core Capability - Installation File Import						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.AHE(Core).4	Import Meter Installation File	Import IIF file, with proper Meter LAT/LONGs. Meters should appear with full 13 digit meter number, with SP ID, and transition to Normal mode				
System Test Book – AMI Head End (AHE): Core Capability - Customer File Import						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.AHE(Core).5	Import Customer file in CSV format	N/A				
System Test Book – AMI Head End (AHE): Core Capability - Send Command to Meter						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.AHE(Core).6	Ability to send PING command to meter	Send PING and On-Demand read				
System Test Book – AMI Head End (AHE): Core Capability - EMED Meter Read File Export						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.AHE(Core).7	Export EMED (Every Meter Every Day) meter file (KCPL-custom EMED format)	Created customized KCPL EMED file format, Extract Spec, and verify file save to destination target with expected content				
SYS.AHE(Core).8	Export EMED (Every Meter Every Day) meter file (eMeter EnergyIP MDM-custom EMED format)	Created customized EMED file format, "emed_mdm", for use with the eMeter EnergyIP Meter Data Management (MDM) system and verify file save to destination target with expected content				
System Test Book – AMI Head End (AHE): Core Capability - Interval Reads File Export						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.AHE(Core).9	California Meter Exchange Protocol (CMEP)	Generate Interval read file in CMEP format				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.AHE(Core).10	MV90 - Handheld Reader File Format (HHF)	Generate Interval read file in HHF format				
System Test Book – AMI Head End (AHE): Core Capability - EVENTS File Export						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.AHE(Core).11	Export meter read Events File to file path destination	Generate Events File extract				
System Test Book – AMI Head End (AHE): Core Capability - HAN Extract File Export						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.AHE(Core).12	Create manual HAN extract file from Command Center	Generate list of HAN devices with current HAN Status in Excel, CSV format				
System Test Book – AMI Head End (AHE): Core Capability - Meter Extract File Export						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.AHE(Core).13	Create scheduled Meter Extract file	Generate list of Meter devices with current Status in CSV format				
System Test Book – AMI Head End (AHE): Core Capability - External Integration Testing						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.AHE(Core).14	Outage Management Integration – Web Service Based	Outage Management Integration – Web Service Based				
SYS.AHE(Core).15	Customer Information System Integration - Web Service Based	Setup and verify MQ Broker integration with CIS				
SYS.AHE(Core).16	MDM Integration - SFTP Based	Custom EMED_MDM and standard CMEP Interval files load successfully to Siemens-hosted eMeter EnergyIP Meter Data Management				
System Test Book – AMI Head End (AHE): Core Capability - CIM-based Web Service Commands						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.AHE(Core).17	Validate that commands can successfully be sent via HAN CIM Interface to meter	Successful commands sent to meter via the CIM interfaces				
System Test Book – AMI Head End (AHE): Core Capability - Layered Routing Change						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.AHE(Core).18	Validate that metered endpoints are showing good reads	Recent midnight read dates observed in Enpoint Information screen for all normal mode meters				
SYS.AHE(Core).19	Validate successful Meter Command Reports – post Layered routing	Verify successful commands sent after layered routing was configured				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.AHE(Core).20	Verify meter file extract receipt – post Layered routing	2 meter files per day between chosen testing dates				
SYS.AHE(Core).21	Verify meter reads – post Layered routing	Normal Meters show read data, with current meter read date/time				
SYS.AHE(Core).22	Verify interval reads – post Layered routing	Normal Meters show interval data, with current meter read date/time				
SYS.AHE(Core).23	Meter read consistency - post Layered routing	Verify meter read consistency over multiple days, with no major meter read spikes				

System Test Book – AMI Head End (AHE): Basic Commands for Integrated Focus AX Meters						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.AHE(Meter).1	HAN: Register Device	N/A				
SYS.AHE(Meter).2	HAN: Get Network Info	N/A				
SYS.AHE(Meter).3	HAN: Get Device Info	N/A				
SYS.AHE(Meter).4	HAN: Get All Devices Info	N/A				
SYS.AHE(Meter).5	HAN: Get Firmware	N/A				
SYS.AHE(Meter).6	HAN: Ping Device	N/A				
SYS.AHE(Meter).7	HAN: Send Message	N/A				
SYS.AHE(Meter).8	HAN: Delete Device	N/A				
SYS.AHE(Meter).9	HAN: Clear Devices	N/A				
SYS.AHE(Meter).10	HAN: Decommission Network	N/A				
System Test Book – AMI Head End (AHE): Basic Commands for Enhanced S4e Meters						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.AHE(Meter).11	HAN: Register Device	N/A				
SYS.AHE(Meter).12	HAN: Get Network Info	N/A				
SYS.AHE(Meter).13	HAN: Get Device Info	N/A				
SYS.AHE(Meter).14	HAN: Get All Devices Info	N/A				
SYS.AHE(Meter).15	HAN: Get Firmware	N/A				
SYS.AHE(Meter).16	HAN: Ping Device	N/A				
SYS.AHE(Meter).17	HAN: Send Message	N/A				
SYS.AHE(Meter).18	HAN: Delete Device	N/A				
SYS.AHE(Meter).19	HAN: Clear Devices	N/A				
SYS.AHE(Meter).20	HAN: Decommission Network	N/A				
System Test Book – AMI Head End (AHE): Broadcast Commands for Integrated Focus AX Meters						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.AHE(Meter).21	HAN: Firmware Download	N/A				
SYS.AHE(Meter).22	HAN: Get All Devices Info	N/A				
SYS.AHE(Meter).23	HAN: Get Firmware	N/A				
SYS.AHE(Meter).24	HAN: Get Network Info	N/A				
SYS.AHE(Meter).25	HAN: Send Message	N/A				
System Test Book – AMI Head End (AHE): Broadcast Commands for Enhanced S4e Meters						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.AHE(Meter).26	HAN: Firmware Download	N/A				
SYS.AHE(Meter).27	HAN: Get All Devices Info	N/A				
SYS.AHE(Meter).28	HAN: Get Firmware	N/A				
SYS.AHE(Meter).29	HAN: Get Network Info	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS,AHE(Meter).30	HAN: Send Message	N/A				

System Test Book – Home Energy Management Portal (HEMP): Web Portal SSO Functionality						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HEMP.PRTL_01_A	Verify SSO process is working properly	N/A				
System Test Book – Home Energy Management Portal (HEMP): Web Portal Energy Usage Data Presentation						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HEMP.PRTL_02_A	Verify that Web Portal dashboard is accumulating usage information	N/A				
SYS.HEMP.PRTL_02_B	Verify that graphs are accumulating usage cost information	N/A				
SYS.HEMP.PRTL_02_C	Verify that instantaneous consumption is displayed and updated regularly for HAN users	N/A				
System Test Book – Home Energy Management Portal (HEMP): Web Portal Pricing Information						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HEMP.PRTL_03_A	Verify accurate pricing information is received and displayed by Web Portal	N/A				
System Test Book – Home Energy Management Portal (HEMP): Web Portal (Estimated) Billing Information						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HEMP.PRTL_04_A	Verify Bill TrueUps are received by Web Portal and displayed properly	N/A				
SYS.HEMP.PRTL_04_B	"Soak" test Web Portal for a week to verify accuracy of estimated billing information	N/A				
System Test Book – Home Energy Management Portal (HEMP): HAN Device Registration						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HEMP.PRTL_05_A	HAN Gateway can be registered to HAN user account via Web Portal	N/A				
System Test Book – Home Energy Management Portal (HEMP): HAN Device Connectivity Status						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HEMP.PRTL_06_A	HAN Device current status appears in Web Portal	N/A				
System Test Book – Home Energy Management Portal (HEMP): HAN Device Information						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HEMP.PRTL_07_A	HAN Device MAC Address appears in Web Portal	N/A				
SYS.HEMP.PRTL_07_B	HAN Device can be renamed by user in Web Portal	N/A				
System Test Book – Home Energy Management Portal (HEMP): HAN Device Monitoring and Control						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HEMP.PRTL_08_A	Real-time usage instantaneous demand information is displayed in Web Portal	N/A				
SYS.HEMP.PRTL_08_B	PCT set point and schedule can be set via Web Portal	N/A				
SYS.HEMP.PRTL_08_C	LCs can be switched on/off via Web Portal	N/A				
System Test Book – Home Energy Management Portal (HEMP): HAN Device Text Messaging						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HEMP.PRTL_09_A	HAN Devices receive text messages sent via administrative Web Portal	N/A				
System Test Book – Home Energy Management Portal (HEMP): Demand Response Notification						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HEMP.PRTL_10_A	DR event notification is received and displayed in Web Portal	N/A				
SYS.HEMP.PRTL_10_B	DR event details are displayed in Web Portal	N/A				
System Test Book – Home Energy Management Portal (HEMP): Demand Response Opt Out						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HEMP.PRTL_11_A	PCT/HAN user DR event participation status is displayed in Web Portal	N/A				
SYS.HEMP.PRTL_11_B	PCT/HAN user can opt out/in for DR event participation via Web Portal	N/A				
System Test Book – Home Energy Management Portal (HEMP): HAN Device Unregistration						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HEMP.PRTL_12_A	HAN Gateway can be unregistered from HAN user account via administrative Web Portal	N/A				

System Test Book – Home Area Network (HAN): In Home Displays (IHD)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HAN.1	Monitor IHD during entire CC 5.6 upgrade process to make sure it "makes the trip"	N/A				
SYS.HAN.2	Provision IHD from 'HAN' tab	N/A				
SYS.HAN.3	Provision IHD using HAN: Register Device command	N/A				
SYS.HAN.4	Send 'HAN: Get Device Info' command to IHD	N/A				
SYS.HAN.5	Send 'HAN: Ping Device' command to IHD	N/A				
SYS.HAN.6	Send 'HAN: Send Message' command to IHD	N/A				
SYS.HAN.7	Broadcast 'HAN: Send Message' command to all meters	N/A				
SYS.HAN.8	Verify that IHD appears as "Normal" in the 'HAN' tab	N/A				
SYS.HAN.9	Verify that IHD is accumulating usage information on 'Home Screen'	N/A				
SYS.HAN.10	Verify pricing information is received by IHD	N/A				
SYS.HAN.11	Verify that graphs in 'Daily Cost' box are accumulating cost information	N/A				
SYS.HAN.12	Verify that instantaneous consumption is displayed and updated regularly	N/A				
SYS.HAN.13	Verify Bill TrueUps are received by IHD when data is processed and sent by IT	N/A				
SYS.HAN.14	"Soak" test IHD(s) for a week to verify accuracy of estimated billing information (use IHD Soak Test Spreadsheet)	N/A				
SYS.HAN.15	Monitor Error Log in Command Center to verify that no ZigBee communications errors occur on any meter	N/A				
SYS.HAN.16	De-provision IHD from 'HAN' tab	N/A				
SYS.HAN.17	Power cycle IHD and make sure it stay on network	N/A				
SYS.HAN.18	De-provision IHD using 'HAN: Delete Device' command	N/A				
SYS.HAN.19	De-provision IHD using 'HAN: Clear Devices' command	N/A				
SYS.HAN.20	De-provision IHD using 'HAN: Decommission Network' command	N/A				
System Test Book – Home Area Network (HAN): Tendril Set Point 218 Thermostat (TSTAT)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HAN.21	Monitor TSTAT during entire CC 5.6 upgrade process to make sure it "makes the trip"	N/A				
SYS.HAN.22	Provision TSTAT from 'HAN' tab	N/A				
SYS.HAN.23	Provision TSTAT using HAN: Register Device command	N/A				
SYS.HAN.24	Send 'HAN: Get Device Info' command to TSTAT	N/A				
SYS.HAN.25	Send 'HAN: Ping Device' command to TSTAT	N/A				
SYS.HAN.26	Send 'HAN: Send Message' command to TSTAT	N/A				
SYS.HAN.27	Broadcast 'HAN: Send Message' command to all meters	N/A				
SYS.HAN.28	Verify that TSTAT appears as "Normal" in the 'HAN' tab	N/A				
SYS.HAN.29	Verify pricing information is received by TSTAT	N/A				
SYS.HAN.30	Verify that Text Messages can be sent to TSTAT from Command Center	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HAN.31	Monitor Error Log in Command Center to verify that no ZigBee communications errors occur on any meter	N/A				
SYS.HAN.32	De-provision TSTAT from 'HAN' tab	N/A				
SYS.HAN.33	Power cycle TSTAT and make sure it stay on network	N/A				
SYS.HAN.34	De-provision TSTAT using 'HAN: Delete Device' command	N/A				
SYS.HAN.35	De-provision TSTAT using 'HAN: Clear Devices' command	N/A				
SYS.HAN.36	De-provision TSTAT using 'HAN: Decommission Network' command	N/A				
System Test Book – Home Area Network (HAN): HAN Gateway						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HAN.37	Monitor HAN devices during entire CC 5.6 upgrade process to make sure they all "makes the trip"	N/A				
SYS.HAN.38	Provision HAN devices from 'HAN' tab	N/A				
SYS.HAN.39	Provision HAN devices using HAN: Register Device command	N/A				
SYS.HAN.40	Send 'HAN: Get Device Info' command to HAN devices	N/A				
SYS.HAN.41	Send 'HAN: Ping Device' command to HAN devices	N/A				
SYS.HAN.42	Send 'HAN: Send Message' command to GW and see if TSTAT gets it	N/A				
SYS.HAN.43	Send 'HAN: Send Message' command to TSTAT	N/A				
SYS.HAN.44	Broadcast 'HAN: Send Message' command to all meters	N/A				
SYS.HAN.45	Verify that all HAN devices appear as "Normal" in the 'HAN' tab	N/A				
SYS.HAN.46	Verify that GW is accumulating usage information in Energize portal	N/A				
SYS.HAN.47	Verify pricing information is received by TSTAT	N/A				
SYS.HAN.48	Monitor Error Log in Command Center to verify that no ZigBee communications errors occur on any meter	N/A				
SYS.HAN.49	De-provision HAN devices from 'HAN' tab	N/A				
SYS.HAN.50	Power cycle HAN devices and make sure it stay on network	N/A				
SYS.HAN.51	De-provision HAN devices using 'HAN: Delete Device' command	N/A				
SYS.HAN.52	De-provision HAN devices using 'HAN: Clear Devices' command	N/A				
SYS.HAN.53	De-provision HAN devices using 'HAN: Decommission Network' command	N/A				

System Test Book – Home Area Network (HAN) Additional Tests: In-Home Display (IHD) Test Cases- Network Commissioning and IHD Provisioning						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.IHD_01_A	Provision IHD from 'HAN' tab	N/A				
SYS.HANXTRA.IHD_01_B	Provision IHD using 'HAN Register Device' command	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: In-Home Display (IHD) Test Cases- IHD Connectivity Status						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.IHD_02_A	Monitor IHD during entire CC upgrade process to make sure it "makes the trip"	N/A				
SYS.HANXTRA.IHD_02_B	Send 'HAN: Get Device Info' command to IHD	N/A				
SYS.HANXTRA.IHD_02_C	Send 'HAN: Ping Device' command to IHD	N/A				
SYS.HANXTRA.IHD_02_D	Verify that IHD appears as "Normal" in the 'HAN' tab	N/A				
SYS.HANXTRA.IHD_02_E	Monitor Error Log in Command Center to verify that no ZigBee communications errors occur on any meter	N/A				
SYS.HANXTRA.IHD_02_F	Power cycle IHD and make sure it remains communicating with the HAN network	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: In-Home Display (IHD) Test Cases- IHD Device Information						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.IHD_03_A	Verify that device appears as "In Premise Display" in Command Center	N/A				
SYS.HANXTRA.IHD_03_B	Send 'HAN: Get Device Info' command to IHD	N/A				
SYS.HANXTRA.IHD_03_C	Send 'HAN: Get All Devices Info' command to IHD	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: In-Home Display (IHD) Test Cases- IHD Energy Usage Data Presentation						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.IHD_04_A	Verify that IHD is accumulating usage information on 'Home Screen'	N/A				
SYS.HANXTRA.IHD_04_B	Verify that graphs in 'Daily Cost' box are accumulating cost information	N/A				
SYS.HANXTRA.IHD_04_C	Verify that instantaneous consumption is displayed and updated regularly	N/A				
SYS.HANXTRA.IHD_04_D	Verify Bill TrueUps are received by IHD when data is processed and sent by IT	N/A				
SYS.HANXTRA.IHD_04_E	"Soak" test IHD(s) for a week to verify accuracy of estimated billing information (use IHD Soak Test Spreadsheet)	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: In-Home Display (IHD) Test Cases- IHD Pricing Information						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.IHD_05_A	Verify accurate pricing information is received by IHD (should match Web Portal pricing information)	N/A				
SYS.HANXTRA.IHD_05_B	Verify that graphs in 'Daily Cost' box are accumulating cost information	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: In-Home Display (IHD) Test Cases- IHD (Estimated) Billing Information						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.IHD_06_A	Verify Bill TrueUps are received by IHD when data is processed and sent by IT	N/A				
SYS.HANXTRA.IHD_06_B	"Soak" test IHD(s) for a week to verify accuracy of estimated billing information (use IHD Soak Test Spreadsheet)	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: In-Home Display (IHD) Test Cases- IHD Text Messaging						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.IHD_07_A	Send 'HAN: Send Message' command to IHD	N/A				
SYS.HANXTRA.IHD_07_B	Broadcast 'HAN: Send Message' command to multiple meters	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: In-Home Display (IHD) Test Cases- IHD Monitoring						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.IHD_08_A	"Soak" test IHD(s) for a week to verify accuracy of estimated billing information (use IHD Soak Test Spreadsheet)	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: In-Home Display (IHD) Test Cases- Network De-Commissioning and IHD De-Provisioning						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.IHD_09_A	De-provision IHD from 'HAN' tab	N/A				
SYS.HANXTRA.IHD_09_B	De-provision IHD using 'HAN: Delete Device' command	N/A				
SYS.HANXTRA.IHD_09_C	De-provision IHD using 'HAN: Clear Devices' command	N/A				
SYS.HANXTRA.IHD_09_D	De-provision IHD using 'HAN: Decommission Network' command	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: Standalone Thermostat (PCT)- Network Commissioning and PCT Provisioning						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.PCT_01_A	Provision PCT from 'HAN' tab	N/A				
SYS.HANXTRA.PCT_01_B	Provision PCT using 'HAN: Register Device' command	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: Standalone Thermostat (PCT)- PCT Portal Registration						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.PCT_02_A	Click 'Scan for More Devices' and verify that remaining PCT appears in the device list	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: Standalone Thermostat (PCT)- PCT Connectivity Status						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.PCT_03_A	Monitor PCT during entire CC upgrade process to make sure it "makes the trip"	N/A				
SYS.HANXTRA.PCT_03_B	Send 'HAN: Get Device Info' command to PCT	N/A				
SYS.HANXTRA.PCT_03_C	Send 'HAN: Ping Device' command to PCT	N/A				
SYS.HANXTRA.PCT_03_D	Verify that PCT appears as "Normal" in the 'HAN' tab	N/A				
SYS.HANXTRA.PCT_03_E	Monitor Error Log in Command Center to verify that no ZigBee communications errors occur on any meter	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.PCT_03_F	Power cycle PCT and make sure it remains communicating with the HAN network	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: Standalone Thermostat (PCT)- PCT Device Information						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.PCT_04_A	Verify that device appears as "PCT" in Command Center	N/A				
SYS.HANXTRA.PCT_04_B	Send 'HAN: Get Device Info' command to PCT	N/A				
SYS.HANXTRA.PCT_04_C	Send 'HAN: Get All Devices Info' command to PCT	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: Standalone Thermostat (PCT)- PCT Pricing Information						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.PCT_05_A	Verify accurate pricing information is received by PCT (should match Web Portal pricing information)	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: Standalone Thermostat (PCT)- PCT Monitoring and Control						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.PCT_06_A	"Soak" test PCT for a week to verify functionality and network connectivity	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: Standalone Thermostat (PCT)- PCT Demand Response Notification						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.PCT_07_A	Verify PCT receives Demand Response event request	N/A				
SYS.HANXTRA.PCT_07_B	Verify PCT starts Demand Response event at expected 'start time'	N/A				
SYS.HANXTRA.PCT_07_C	Verify PCT ends Demand Response event at expected 'end time'	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: Standalone Thermostat (PCT)- PCT Demand Response Opt Out						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.PCT_08_A	Verify that PCT opt-in to Demand Response events automatically	N/A				
SYS.HANXTRA.PCT_08_B	Verify that PCT respond appropriately when Demand Response event opt-out is performed	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: Standalone Thermostat (PCT)- PCT Text Messaging						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.PCT_09_A	Send 'HAN: Send Message' command to PCT	N/A				
SYS.HANXTRA.PCT_09_B	Broadcast 'HAN: Send Message' command to multiple meters	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: Standalone Thermostat (PCT)- PCT Unregistration						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.PCT_10_A	Provision PCT from 'HAN' tab	N/A				
SYS.HANXTRA.PCT_10_B	Provision PCT using 'HAN: Register Device' command	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: Standalone Thermostat (PCT)- Network De-Commissioning and PCT De-Provisioning						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.PCT_11_A	De-provision PCT from 'HAN' tab	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.PCT_11_B	De-provision PCT using 'HAN: Delete Device' command	N/A				
SYS.HANXTRA.PCT_11_C	De-provision PCT using 'HAN: Clear Devices' command	N/A				
SYS.HANXTRA.PCT_11_D	De-provision PCT using 'HAN: Decommission Network' command	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: Home Area Network (HAN) Devices - Network Commissioning and HAN Device Provisioning						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.HAN_01_A	Provision HAN devices from 'HAN' tab	N/A				
SYS.HANXTRA.HAN_01_B	Provision HAN devices using 'HAN: Register Device' command	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: Home Area Network (HAN) Devices - HAN Device Portal Registration						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.HAN_02_A	Input HAN Gateway ID on 'Device Settings' page in Portal and verify that the HAN Gateway appears in the device list	N/A				
SYS.HANXTRA.HAN_02_B	Click 'Scan for More Devices' and verify that remaining HAN devices appear in the device list	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: Home Area Network (HAN) Devices - HAN Device Connectivity Status						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.HAN_03_A	Monitor HAN devices during entire CC upgrade process to make sure it "makes the trip"	N/A				
SYS.HANXTRA.HAN_03_B	Send 'HAN: Ping Device' command to HAN devices	N/A				
SYS.HANXTRA.HAN_03_C	Verify that HAN devices appears as "Normal" in the 'HAN' tab	N/A				
SYS.HANXTRA.HAN_03_D	Monitor Error Log in Command Center to verify that no ZigBee communications errors occur on any meter	N/A				
SYS.HANXTRA.HAN_03_E	Power cycle HAN devices and make sure they remains communicating with the HAN network	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: Home Area Network (HAN) Devices - HAN Device Information						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.HAN_04_A	Verify that HAN devices appears as "Energy Service Portal", "PCT", and "Load Control Device" in Command Center	N/A				
SYS.HANXTRA.HAN_04_B	Send 'HAN: Get Device Info' command to HAN devices	N/A				
SYS.HANXTRA.HAN_04_C	Send 'HAN: Get All Devices Info' command to HAN devices	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: Home Area Network (HAN) Devices - HAN Device Pricing Information						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.HAN_05_A	Verify accurate pricing information is received by HAN devices	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: Home Area Network (HAN) Devices - HAN Device Monitoring and Control						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.HAN_06_A	"Soak" test HAN devices for a week to verify functionality and network connectivity	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
System Test Book – Home Area Network (HAN) Additional Tests: Home Area Network (HAN) Devices - HAN Device Demand Response Notification						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.HAN_07_A	Verify HAN devices receives Demand Response event request	N/A				
SYS.HANXTRA.HAN_07_B	Verify HAN devices starts Demand Response event at expected 'start time'	N/A				
SYS.HANXTRA.HAN_07_C	Verify HAN devices ends Demand Response event at expected 'end time'	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: Home Area Network (HAN) Devices - HAN Device Demand Response Opt Out						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.HAN_08_A	Verify that HAN devices opt-in to Demand Response events automatically	N/A				
SYS.HANXTRA.HAN_08_B	Verify that HAN devices respond appropriately when Demand Response	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: Home Area Network (HAN) Devices - HAN Device Text Messaging						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.HAN_09_A	Send 'HAN: Send Message' command to HAN devices	N/A				
SYS.HANXTRA.HAN_09_B	Broadcast 'HAN: Send Message' command to multiple meters	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: Home Area Network (HAN) Devices - HAN Device Unregistration						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.HAN_10_A	Provision HAN devices from 'HAN' tab	N/A				
SYS.HANXTRA.HAN_10_B	Provision HAN devices using 'HAN: Register Device' command	N/A				
System Test Book – Home Area Network (HAN) Additional Tests: Home Area Network (HAN) Devices - Network De-Commissioning and HAN Device De-Provisioning						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
SYS.HANXTRA.HAN_11_A	De-provision HAN devices from 'HAN' tab	N/A				
SYS.HANXTRA.HAN_11_B	De-provision HAN devices using 'HAN: Delete Device' command	N/A				
SYS.HANXTRA.HAN_11_C	De-provision HAN devices using 'HAN: Clear Devices' command	N/A				
SYS.HANXTRA.HAN_11_D	De-provision HAN devices using 'HAN: Decommission Network' command	N/A				

Integration Test Book – DMS Interfaces to DERM (Joint): Configuration Verification						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.DMS-DERM.A1.1	Verify FAT system environment diagram	N/A				
INT.DMS-DERM.A1.2	Verify system Test Environment (HW & SW), including communication infrastructure	N/A				
INT.DMS-DERM.A1.3	Verify system management and configuration displays and tools	N/A				
INT.DMS-DERM.A1.4	Verify users access to the DNA's Interface management tools	N/A				
INT.DMS-DERM.A1.5	Verify users access to the DERM's Interface management tools	N/A				
INT.DMS-DERM.A1.6	Verify correct operation of the system components (system configuration overview, servers status, communications status, applications running)	N/A				
Integration Test Book – DMS Interfaces to DERM (Joint): Computer System Management (Servers, Clients, Functions, Environments)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.DMS-DERM.A1.7	Redundancy (Comms, Networks): Verify communication redundancy	N/A				
INT.DMS-DERM.A1.8	Communications Failure: Verify communication redundancy between DERM and DMS	N/A				
INT.DMS-DERM.A1.9	Communications Failure: Verify DNA LAN failures	N/A				
INT.DMS-DERM.A1.10	Communications Failure: Verify DNA LAN failures restoration	N/A				
INT.DMS-DERM.A1.11	Communications Failure: Verify VPN failure	N/A				
INT.DMS-DERM.A1.12	Communications Failure: Verify that the data model is correct after system is restored	N/A				
INT.DMS-DERM.A1.13	Communications Failure: Verify reporting and logging	N/A				
INT.DMS-DERM.A1.14	Power Failure: Verify interface behavior during DNA servers power failures	N/A				
INT.DMS-DERM.A1.15	Power Failure: Verify interface behavior during DERM power failures	N/A				
INT.DMS-DERM.A1.16	Power Failure: Verify that the data model is correct after system is restored	N/A				
Integration Test Book – DMS Interfaces to DERM (Joint): Functional Redundancy						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.DMS-DERM.A1.17	DNA Failover: Verify interface operation when a failover of the DNA applications occurs	N/A				
INT.DMS-DERM.A1.18	DNA Failover: Verify message exchange interruption caused by DNA failover	N/A				
INT.DMS-DERM.A1.19	DNA Failover: Verify status reporting and logging at the CC	N/A				
INT.DMS-DERM.A1.20	DERM Failover: Verify interface operation when a failover of the DERM applications occurs	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.DMS-DERM.A1.21	DERM Failover: Verify message exchange interruption caused by DERM failover	N/A				
INT.DMS-DERM.A1.22	DERM Failover: Verify status reporting and logging at the CC	N/A				
Integration Test Book – DMS Interfaces to DERM (Joint): Data Base Management						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.DMS-DERM.A1.23	DB Model Management: Verify DB change in DNA is propagated to DERM correctly	N/A				
INT.DMS-DERM.A1.24	Model Export: Verify CIM RDF DB model export from DNA	N/A				
INT.DMS-DERM.A1.25	Model Import: Verify CIM RDF DB model import to DERM	N/A				
INT.DMS-DERM.A1.26	Model Import: Verify behavior when sftp goes down during CIM RDF model transfer	N/A				
INT.DMS-DERM.A1.27	Model Import: Verify behavior when DMS goes down during CIM RDF model transfer	N/A				
INT.DMS-DERM.A1.28	Model Import: Verify behavior when DERM goes down during CIM RDF model transfer	N/A				
INT.DMS-DERM.A1.29	Model Import: Verify DB Synch monitoring or mismatch reporting	N/A				
INT.DMS-DERM.A1.30	Model Import: Interrupt DB synchronization and verify reporting error	N/A				
INT.DMS-DERM.A1.31	Model Import: Verify model archiving and management	N/A				
INT.DMS-DERM.A1.32	Model Import: Verify reporting and logging of DB synchronization and errors	N/A				
Integration Test Book – DMS Interfaces to DERM (Joint): User Interface						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.DMS-DERM.A1.33	Interface Management: Verify control enable/disable interface in DNA	N/A				
INT.DMS-DERM.A1.34	Interface Management: Verify control enable/disable interface in DERM	N/A				
INT.DMS-DERM.A1.35	Interface Management: Verify reporting and logging of Interface Status	N/A				
INT.DMS-DERM.A1.36	Simultaneous Operation: Verify simultaneous operation of the requests from DNA and user operation in DERM	N/A				
Integration Test Book – DMS Interfaces to DERM (Joint): Message Transfer						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.DMS-DERM.A1.37	Interface handshaking: Verify interface status	N/A				
INT.DMS-DERM.A1.38	Interface handshaking: Verify system behavior on error or negative handshaking conditions from DERM	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.DMS-DERM.A1.39	Interface handshaking: Verify system behavior on error or negative handshaking conditions from DNA	N/A				
INT.DMS-DERM.A1.40	Interface handshaking: Verify reporting and logging	N/A				
INT.DMS-DERM.A1.41	Interface handshaking: Verify behavior when JMS Adapter goes down during message exchange	N/A				
INT.DMS-DERM.A1.42	Interface handshaking: Verify behavior when ESB goes down during message exchange	N/A				
INT.DMS-DERM.A1.43	Interface handshaking: Verify behavior when DMS goes down during message exchange	N/A				
INT.DMS-DERM.A1.44	Interface handshaking: Verify behavior when DERM goes down during message exchange	N/A				
INT.DMS-DERM.A1.45	GetDiscreteMeasurements: Verify requests from DERM	N/A				
INT.DMS-DERM.A1.46	GetDiscreteMeasurements: Verify requests from DERM (multiple users)	N/A				
INT.DMS-DERM.A1.47	GetDiscreteMeasurements: Verify incorrect Interface handshaking	N/A				
INT.DMS-DERM.A1.48	GetDiscreteMeasurements: Verify correct response	N/A				
INT.DMS-DERM.A1.49	GetDiscreteMeasurements: Verify incorrect response (data mapping errors, model mismatch,...)	N/A				
INT.DMS-DERM.A1.50	GetDiscreteMeasurements: Verify no response - Time out	N/A				
INT.DMS-DERM.A1.51	GetDiscreteMeasurements: Verify reporting and logging	N/A				
INT.DMS-DERM.A1.52	Report spontaneous switch changes: Verify change of status is sent from DNA to DERM	N/A				
INT.DMS-DERM.A1.53	Report spontaneous switch changes: Verify incorrect response (no-ack)	N/A				
INT.DMS-DERM.A1.54	Report spontaneous switch changes: Verify no response (ack) - Time out	N/A				
INT.DMS-DERM.A1.55	Report spontaneous switch changes: Verify incorrect Interface handshaking	N/A				
INT.DMS-DERM.A1.56	Report spontaneous switch changes: Verify correct status change and new measure values	N/A				
INT.DMS-DERM.A1.57	Report spontaneous switch changes: Verify multiple consecutive status changes from DNA (1 or several messages)	N/A				
INT.DMS-DERM.A1.58	Report spontaneous switch changes: Verify erroneous switch reporting (not in the model or incorrect mapping)	N/A				
INT.DMS-DERM.A1.59	Report spontaneous switch changes: Verify reporting and logging	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.DMS-DERM.A1.60	Power Flow limit violations: Verify PF limit violations are sent from DNA to DERM	N/A				
INT.DMS-DERM.A1.61	Power Flow limit violations: Verify incorrect response (no-ack)	N/A				
INT.DMS-DERM.A1.62	Power Flow limit violations: Verify no response (ack) - Time out	N/A				
INT.DMS-DERM.A1.63	Power Flow limit violations : Verify limit violations are created, changed and deleted : * ChangedDistributionPowerFlowLimitViolation * CreatedDistributionPowerFlowLimitViolation * DeleteDistributionPowerFlowLimitViolation	N/A				
INT.DMS-DERM.A1.64	Power Flow limit violations: Verify erroneous message sequence (delete a violation that was not previously created)	N/A				
INT.DMS-DERM.A1.65	Power Flow limit violations: Verify incorrect Interface handshaking	N/A				
INT.DMS-DERM.A1.66	Power Flow limit violations: Verify reporting and logging	N/A				
INT.DMS-DERM.A1.67	CreatedDemandResourceControls: Verify requests from DERM	N/A				
INT.DMS-DERM.A1.68	CreatedDemandResourceControls: Verify incorrect response (no-ack)	N/A				
INT.DMS-DERM.A1.69	CreatedDemandResourceControls: Verify no response - Time out	N/A				
INT.DMS-DERM.A1.70	CreatedDemandResourceControls: Verify correct information is received in DNA	N/A				
INT.DMS-DERM.A1.71	CreatedDemandResourceControls: Verify the rest of DR event sequence: Event start when time arrives, notification, information about action taken, completion	N/A				
INT.DMS-DERM.A1.72	CreatedDemandResourceControls: Verify incorrect Interface handshaking	N/A				
INT.DMS-DERM.A1.73	CreatedDemandResourceControls: Verify reporting and logging	N/A				
INT.DMS-DERM.A1.74	DeleteDemandResourceControls: Verify requests from DERM	N/A				
INT.DMS-DERM.A1.75	DeleteDemandResourceControls: Verify incorrect response (no-ack)	N/A				
INT.DMS-DERM.A1.76	DeleteDemandResourceControls: Verify no response - Time out	N/A				
INT.DMS-DERM.A1.77	DeleteDemandResourceControls: Verify incorrect Interface handshaking	N/A				
INT.DMS-DERM.A1.78	DeleteDemandResourceControls: Verify correct information is received in DNA	N/A				
INT.DMS-DERM.A1.79	DeleteDemandResourceControls: Verify reporting and logging	N/A				
INT.DMS-DERM.A1.80	GetDemandResourceControls ReplyResourceControls: Verify requests from DNA	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.DMS-DERM.A1.81	GetDemandResourceControls ReplyResourceControls: Verify incorrect response (no-ack)	N/A				
INT.DMS-DERM.A1.82	GetDemandResourceControls ReplyResourceControls: Verify no response - Time out	N/A				
INT.DMS-DERM.A1.83	GetDemandResourceControls ReplyResourceControls: Verify incorrect Interface handshaking	N/A				
INT.DMS-DERM.A1.84	GetDemandResourceControls ReplyResourceControls: Verify correct information is received in DNA	N/A				
INT.DMS-DERM.A1.85	GetDemandResourceControls ReplyResourceControls: Verify behavior when incorrect data reported as part of events(not in the model or incorrect mapping)	N/A				
INT.DMS-DERM.A1.86	GetDemandResourceControls ReplyResourceControls: Verify reporting and logging	N/A				
Integration Test Book – DMS Interfaces to DERM (Joint): Full Scenario Tests						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.DMS-DERM.A1.87	DERM Initialization Base Case: Verify that CIM RDF data file can be loaded in DERM	N/A				
INT.DMS-DERM.A1.88	DERM Initialization Base Case: Request synchronization of device statuses from DERM GUI and verify receipt via consistent DMS and DERM Uis.	N/A				
INT.DMS-DERM.A1.89	DERM Initialization Base Case: Simulate a device status change in the DMS and verify that the device status change appears in the DERM UI.	N/A				
INT.DMS-DERM.A1.90	Feeder Load Management Base Case: Create study case in DMS with specific time period and verify that the study case is published to DERM	N/A				
INT.DMS-DERM.A1.91	Feeder Load Management Base Case: Verify behavior when DERM study case is not properly created	N/A				
INT.DMS-DERM.A1.92	Feeder Load Management Base Case: Input study case injection correction factor into DMS GUI and verify behavior on DMS study case	N/A				
INT.DMS-DERM.A1.93	Feeder Load Management Base Case: Set target network topology in DMS GUI by hand	N/A				
INT.DMS-DERM.A1.94	Feeder Load Management Base Case: Set target network topology in DMS GUI from InService switching orders	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.DMS-DERM.A1.95	Feeder Load Management Base Case: Verify that both types of network topology updates have been applied in the DMS GUI	N/A				
INT.DMS-DERM.A1.96	Feeder Load Management Base Case: Verify that the network topology updates have been sent to the DERM (via DERM GUI? How will we verify?)	N/A				
INT.DMS-DERM.A1.97	Feeder Load Management Base Case: Invoke Power Flow on study case from DMS and verify that line overloads for hourly peak are displayed on the DMS UI	N/A				
INT.DMS-DERM.A1.98	Feeder Load Management Base Case: Run FLT to mitigate overload in study case and verify that switching procedures are displayed on the DMS UI	N/A				
INT.DMS-DERM.A1.99	Feeder Load Management Base Case: Execute switching procedure steps in the study case using SPM and verify that remaining overloads for the peak hour of study case are displayed on the DMS UI	N/A				
INT.DMS-DERM.A1.100	Feeder Load Management Base Case: Verify that switch changes from switching procedure are sent from DMS to DERM and are applied to the DERM network model	N/A				
INT.DMS-DERM.A1.101	Feeder Load Management Base Case: Initiate PF simulation scheduler (for hourly PF) from DMS GUI and verify that DMS runs the hourly PF	N/A				
INT.DMS-DERM.A1.102	Feeder Load Management Base Case: Verify that hourly PF violations are sent from DMS to DERM and that results are displayed on DERM UI	N/A				
INT.DMS-DERM.A1.103	Feeder Load Management Base Case: Verify that user can select feeder/section requiring load reduction and that DERM returns DR/DER available on the DERM UI	N/A				
INT.DMS-DERM.A1.104	Feeder Load Management Base Case: Select DR/DER to apply and verify that message is sent to DMS with load reductions per transformer/node/hour	N/A				
INT.DMS-DERM.A1.105	Feeder Load Management Base Case: Verify that DR/DER load reduction applied notification is displayed on the DMS UI	N/A				
INT.DMS-DERM.A1.106	Feeder Load Management Base Case: Request PF re-run from the DMS UI and verify that DMS takes proposed DR reductions into account	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.DMS-DERM.A1.107	Feeder Load Management Base Case: Verify that updated line overloads per hour are displayed on the DMS UI and that these overloads are sent to the DERM to continue applying DR/DER to resolve	N/A				
INT.DMS-DERM.A1.108	Feeder Load Management Base Case: If there are no additional line overloads, verify that none are displayed on DMS UI	N/A				
INT.DMS-DERM.A1.109	Feeder Load Management Base Case: From DERM UI, request that proposed DR/DER is scheduled and verify that event schedule is returned to user via DERM UI	N/A				
INT.DMS-DERM.A1.110	Feeder Load Management Base Case: Approve and commit DR/DER in DERM UI and verify that message is sent to DMS	N/A				
INT.DMS-DERM.A1.111	Feeder Load Management Base Case: At event time, confirm that DMS UI notifies user that there are FLT switching procedures to be executed	N/A				
INT.DMS-DERM.A1.112	Feeder Load Management Base Case: Execute the switching procedures and verify that the feeder is reconfigured	N/A				
INT.DMS-DERM.A1.113	Feeder Load Management Base Case: Verify that DERM dispatches DR at the scheduled time	N/A				
INT.DMS-DERM.A1.114	Feeder Load Management Follow-Up Tests: Create second study case during same time period as first, and verify that study case starts from nominal network state and includes the previously committed DR/DER from study case #1	N/A				
INT.DMS-DERM.A1.115	Feeder Load Management Follow-Up Tests: Invoke Power Flow on study case #2 from DMS and verify that PF incorporates previously committed DR/DER from study case #1	N/A				
INT.DMS-DERM.A1.116	Feeder Load Management Follow-Up Tests: Verify behavior in DMS and DERM when conditions change between time when study case was created and time when study case execution is to occur	N/A				
INT.DMS-DERM.A1.117	Feeder Load Management Follow-Up Tests: Verify behavior when two study cases are created simultaneously with an overlapping time frame	N/A				
INT.DMS-DERM.A1.118	Feeder Load Management Follow-Up Tests: Verify that DERM can schedule VVC for planning purposes	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.DMS-DERM.A1.119	Feeder Load Shed Base Case: Simulate a feeder overload condition and verify that: PF detects it and creates an alert FLT is invoked to mitigate FLT recommended switching procedures are displayed on the DMS UI Switching procedures are executed Loads are transferred Next iteration of DSSE runs and results are displayed	N/A				
INT.DMS-DERM.A1.120	Feeder Load Shed Base Case: Verify that DSSE remaining overload results are sent to DERM and displayed on DERM UI	N/A				
INT.DMS-DERM.A1.121	Feeder Load Shed Base Case: Verify that user can select feeder/section requiring load reduction and that DERM returns DR/DER available on the DERM UI	N/A				
INT.DMS-DERM.A1.122	Feeder Load Shed Base Case: Select DR/DER to apply and verify that commit messages are sent to relevant DR control authorities	N/A				
INT.DMS-DERM.A1.123	Feeder Load Shed Base Case: Verify that DR/DER applied in DERM UI is sent to DMS and used to update real time load model	N/A				
INT.DMS-DERM.A1.124	Feeder Load Shed Base Case: Wait for 5 minutes and verify that load reduction has occurred via next DSSE run	N/A				
INT.DMS-DERM.A1.125	Feeder Load Shed Base Case: Verify that remaining overloads are displayed on DMS UI and that these overloads are sent to the DERM to continue applying DR/DER to resolve	N/A				
INT.DMS-DERM.A1.126	Feeder Load Shed Base Case: If there are no additional line overloads, verify that none are displayed on DMS UI.	N/A				
INT.DMS-DERM.A1.127	Feeder Load Shed Follow-Up Tests: Verify behavior when two operators simultaneously try to solve an overload	N/A				

Integration Test Book – DMS Interfaces to DERM (DERM Focus); XML Verification						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.DMS-DERM.A2.1	GetDiscreteMeasurements: Verify that the user can synchronize the dynamic network model with the DMS system that can be synchronizing with RT, after re-start of the DERM system of synchronization with a study case when a new study is created or a different data set of dynamic data has been loaded.	User synchronized the DERM network with the DMS data.				
INT.DMS-DERM.A2.2	Opening/Closing a switch (ChangedDiscreteMeasurements): Broadcasts all spontaneous switch status changes.	The state of the selected switch status has been changed.				
INT.DMS-DERM.A2.3	Receive Power Flow Limit Violation Results: The event messages ChangedDistributionPowerFlowLimitViolation, CreatedDistributionPowerFlowLimitViolation and DeletedDistributionPowerFlowLimitViolation are used to report when a violation occurs, disappears, or changes in value. Like all event messages, they have a header and a payload.	Verify that DMS sends power flow violation results back to DERM.				
INT.DMS-DERM.A2.4	CreatedDemandResourceControls: Verify that DERM can send a message to SCADA/DMS that the DR event has been scheduled.	User can create and schedule DR Load Control event. The message will be sent to the DMS.				
INT.DMS-DERM.A2.5	DeletedDemandResourceControls: Verify that DERM can send a message to SCADA/DMS that the DR event has been un-scheduled.	User can un-schedule DR Load Control event. The message will be sent to the DMS.				
INT.DMS-DERM.A2.6	GetDemandResourceControls/ReplyResourceControl: This message GetDemandResourceControls enables DMS to request all Demand Response (DR) events that are currently scheduled. The response message from DERM to DMS is ReplyDemandResourceControls.	All requested DR events were sent by DERM and received by DMS.				

Integration Test Book – ESB Interfaces to Misc Systems: Simulated Outage/Restoration Event						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.B1.OUT.1	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the ESB Logs and MDM.				
INT.ESB-MISC.B1.OUT.2	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the ESB Logs and MDM.				
INT.ESB-MISC.B1.RES.1	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the ESB Logs and MDM.				
INT.ESB-MISC.B1.RES.2	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the ESB Logs and MDM.				
Integration Test Book – ESB Interfaces to Misc Systems: Meter Lab Outage/Restoration Event (w/o OMS)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.B1.OUT.3	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the AHE and MDM.				
INT.ESB-MISC.B1.RES.3	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the AHE and MDM.				
Integration Test Book – ESB Interfaces to Misc Systems: Meter Lab Outage/Restoration Event (w/OMS)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.B1.OUT.4	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the AHE, MDM and OMS.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.B1.RES.4	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the AHE, MDM and OMS.				

Integration Test Book – ESB Interfaces to Misc Systems: Outage Derivation in MDM via FlexSync						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.B2.FS.1	Generate a single FlexSync Message from CIS test environment via ESB to the MDM with the modified SDP-Meter Association date and verify the results.	(1) Confirm that FlexSync message is sent to MDM with modified SDP-Meter Association date (2) Verify that MDM processes the message (3) Verify that MDM derives the Outage Service for the SDP				
INT.ESB-MISC.B2.FS.2	Generate a multiple FlexSync Message from CIS test environment via ESB to the MDM with the modified SDP-Meter Association date and verify the results.	(1) Confirm that FlexSync message is sent to MDM with modified SDP-Meter Association date (2) Verify that MDM processes the message (3) Verify that MDM derives the Outage Service for the SDP				
INT.ESB-MISC.B2.FS.3	Generate a single FlexSync Message from CIS test environment via ESB to the MDM with the modified SDP-Meter Association date and verify the results.	(1) Confirm that FlexSync message is sent to MDM with modified SDP-Meter Association date (2) Verify that MDM processes the message (3) Verify that MDM derives the Outage Service for the SDP				

Integration Test Book – ESB Interfaces to Misc Systems: Power Status Verification – Unit Testing						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.C.3	Validate setup and configuration of the OMS, ESB, MDM, and AHE to support Power Status Verification	A) Verify that the OMS is configured to write PSV request messages to the OMS_AMI_REPLY queue and read PSV reply messages from the OMS_AMI_INPUT_PSV queue B) Verify that the ESB is configured to read PSV request messages from the OMS_AMI_REPLY queue, send PSV request messages to the MDM, and write PSV reply messages to the OMS_AMI_INPUT_PSV queue C) Verify that the MDM is configured to send PSV request and reply messages to the ESB D) Verify that the AHE is configured to send PSV reply messages to the ESB				
INT.ESB-MISC.C.4	Confirm that the OMS is generating the appropriate outbound PSV request message to the MDM via the ESB	A) Verify that the OMS generates the appropriate outbound PSV request message and sends it to the ESB on the OMS_AMI_REPLY queue to be transformed and sent to the MDM				
INT.ESB-MISC.C.5	Confirm that the ESB is properly transforming PSV request message from the OMS to the MDM	A) Verify that the ESB reads the PSV request message from the OMS_AMI_REPLY queue B) Verify that the ESB makes Webservice call to the CIS to check for 'MeterEnergized' status C) Verify that the ESB transforms the PSV request message to the proper format for the MDM to process D) Verify that the ESB sends the transformed PSV request message to the MDM				
INT.ESB-MISC.C.6	Confirm that the MDM is generating the appropriate outbound PSV request message to the AHE via the ESB	A) Verify that the MDM receives the PSV request message from the ESB B) Verify that the MDM generates the appropriate outbound PSV request message (endpoint on-demand read request) and sends it to the AHE via the ESB				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.C.7	Confirm that the AHE receives the PSV request message from the MDM via the ESB	A) Verify that the AHE receives the PSV request message (endpoint on-demand read request) from the MDM via the ESB and sends the PSV request message to the target AMI meter				
INT.ESB-MISC.C.8	Confirm that the AHE is processing the PSV request message and generating the appropriate outbound PSV reply message to the MDM via the ESB	A) Verify that the AHE receives PSV reply message from the target AMI meter and generates the appropriate outbound PSV reply message (endpoint on-demand read reply) and sends it to the MDM via the ESB				
INT.ESB-MISC.C.9	Confirm that the MDM is generating the appropriate outbound PSV reply message to the OMS via the ESB	A) MDM generates a 'meter on' PSV reply message and sends it to the ESB				
INT.ESB-MISC.C.10	Confirm that the ESB is properly transforming the PSV reply message from the MDM to the OMS	A) Verify that the ESB receives the PSV reply message from the MDM B) Verify that the ESB transforms the PSV reply message to the proper format for the OMS to process C) Verify that ESB sends the transformed PSV reply message to the OMS_AMI_INPUT_PSV queue				
INT.ESB-MISC.C.11	Confirm that the OMS is processing the PSV reply message	A) Verify that OMS reads the PSV reply message from the OMS_AMI_INPUT_PSV queue				
INT.ESB-MISC.C.12	Test Plan review	Review test plan PRIOR TO testing. Consult your PA to determine attendees. Review unit test results if necessary				
INT.ESB-MISC.C.13	Code review – include diffs'	Repeat code review if changes were made during unit testing				
Integration Test Book - ESB Interfaces to Misc Systems: Power Status Verification - System/Scenario Testing						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.C.14	PSV is manually initiated from the OMS to a target meter that is powered ON	N/A				
INT.ESB-MISC.C.15	PSV is manually initiated from the OMS to a target meter that is powered OFF	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.C.16	PSV is manually initiated from the OMS to a target meter that is not "energized" in CIS (service disconnected)	A) Verify that the OMS generates the appropriate outbound PSV request message and sends it to the ESB on the OMS_AMI_REPLY queue to be transformed and sent to the MDM B) Verify that the ESB reads the PSV request message from the OMS_AMI_REPLY queue, makes WebService call to the CIS to check for 'MeterEnergized=N' status, creates the appropriate PSV reply message in the proper format for the OMS to process, and sends the created PSV reply message to the OMS_AMI_INPUT_PSV queue C) Verify that OMS reads the PSV reply message from the OMS_AMI_INPUT_PSV queue				

Integration Test Book – DERM Interfaces to HEMP (DERM Focus): XML Verification						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.DERM-HEMP.D.1	DR Schedule - Load Control Switch message: Verify user can create and maintain all objects and attributes associated with a specific schedule that involves the load control switch operation.	User can create and schedule DR Load Control Switch event. The message will be sent to the HEMP devices. It will be verified that the devices operate properly. (Two venIDs)				
INT.DERM-HEMP.D.2	DR Schedule - Thermostat delta value: Verify user can create and maintain all objects and attributes associated with a specific schedule that involves the thermostat operation.	User can create and schedule DR Thermostat event. The message will be sent to the HEMP device. It will be verified that the devices operate properly. (Temperature changes by delta value - two venIDs).				
INT.DERM-HEMP.D.3	Load Control sent to invalid Network ID: Verify user can create and maintain all objects and attributes associated with a specific schedule that involves the load control switch operation.	User can create and schedule DR Load Control event. The message will be sent to the invalid HEMP device. It will be verified that HEMP responds with an error message.				
INT.DERM-HEMP.D.4	Load Control with customer OptOut option: Verify user can create and maintain all objects and attributes associated with a specific schedule that involves the load control switch with customer OptOut operation.	User can create and schedule DR Load Control event. The message will be sent to the HEMP devices. The second end user will OptOut from this operation. It will be verified that the device operates properly and the OptOut message is sent back to DERM. (Two venIDs)				
INT.DERM-HEMP.D.5	Thermostat delta value schedule with OptOut option: Verify user can create and maintain all objects and attributes associated with a specific schedule that involves the thermostat and OptOut operation.	User can create and schedule DR Thermostat event. The message will be sent to the HEMP devices. The second end user will OptOut from this operation. It will be verified that the device operates properly and the OptOut message is sent back to DERM (Two venIDs).				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.DERM-HEMP.D.6	SIMPLE schedule (LOW): Verify user can create and maintain all objects and attributes associated with a SIMPLE schedule.	User can create a SIMPLE schedule. The message will be sent to the HEMP device. It will be verified that the devices operate properly and the response message is sent back to DERM.				
INT.DERM-HEMP.D.7	SIMPLE schedule (MEDIUM): Verify user can create and maintain all objects and attributes associated with a SIMPLE schedule.	User can create a SIMPLE schedule. The message will be sent to the HEMP device. It will be verified that the devices operate properly and the response message is sent back to DERM.				
INT.DERM-HEMP.D.8	SIMPLE schedule (HIGH): Verify user can create and maintain all objects and attributes associated with a SIMPLE schedule.	User can create a SIMPLE schedule. The message will be sent to the HEMP device. It will be verified that the devices operate properly and the response message is sent back to DERM.				
INT.DERM-HEMP.D.9	CYCLING-LCS schedule: Verify user can create and maintain all objects and attributes associated with a CYCLING-LCS schedule.	User can create a CYCLING schedule. The message will be sent to the HEMP device. It will be verified that the devices operate properly and the response message is sent back to DERM.				
INT.DERM-HEMP.D.10	DR schedule - modified: Verify user can modify and maintain all objects and attributes associated with a CYCLING-LCS schedule.	User can modify a schedule (INT 1). The message will be sent to the HEMP device. It will be verified that the devices operate properly and the response message is sent back to DERM.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.DERM-HEMP.D.11	DR schedule - cancelled: Verify user can cancel a CYCLING-LCS schedule.	User can cancel a schedule (INT 10). The message will be sent to the HEMP device. It will be verified that the devices operate properly and the response message is sent back to DERM.				
INT.DERM-HEMP.D.12	DR Schedule - Load Control Switch message: Verify user can create and maintain all objects and attributes associated with a specific schedule that involves the load control switch operation.	User can create and schedule DR Load Control Switch event. The message will be sent to the HEMP devices. It will be verified that the devices operate properly (OptIn – OptOut - OptIn).				

Integration Test Book – MDM Interfaces to FlexSync: MDM General User Functionality Regression Testing						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.FS-MDM.E1.USER.1	Confirm that KCP&L personnel may access the EIP user interface and browse through various screens. This is not intended to test any specific functionality of the EIP system.	KCP&L personnel are able to access the EIP user interface, successfully log in and browse through the system.				
INT.FS-MDM.E1.USER.2	Confirm that KCP&L personnel may access the EIP SFTP server using the Push Billing account and post/retrieve files.	KCP&L personnel are able to access the EIP SFTP server and then post and retrieve files successfully.				
INT.FS-MDM.E1.USER.3	Confirm that KCP&L personnel may access the EIP SFTP server using the Meter Reads account and post/retrieve files.	KCP&L personnel are able to access the EIP SFTP server and then post and retrieve files successfully.				
INT.FS-MDM.E1.USER.4	Confirm that KCP&L personnel may access the EIP server which runs EIP web services.	KCP&L personnel are able to access the EIP web server.				
INT.FS-MDM.E1.USER.5	Confirm that KCP&L is able to access the MDM FlexSync web service.	KCP&L MQ Broker interface is able to access the MDM FlexSync web service and get a response - either valid or error is acceptable as the purpose is to confirm that we have connectivity.				
INT.FS-MDM.E1.USER.6	Confirm that KCP&L is able to access the MDM FlexSync web service.	KCP&L MQ Broker interface is able to access the MDM FlexSync web service and get a response - either valid or error is acceptable as the purpose is to confirm that we have connectivity.				
INT.FS-MDM.E1.USER.7	Tester will log in to the EIP UI using the "systems administrator" account and visit each of the major screens and links. Errors or other non-functional links/pages will be logged for report back to Siemens.	Tester can log into the EIP UI and visit all of the pages noted below. The tester may click on additional links buttons as desired to further review the UI.				
INT.FS-MDM.E1.USER.8	Ensure that the specified report is generated by the MDM system and if appropriate distributed by email to the KCP&L report distribution list.	The named report is generated by EIP and viewable in the EIP UI. The named report is automatically sent via email to the KCP&L report distribution list.				
Integration Test Book – MDM Interfaces to FlexSync: MDM System Interface Regression Testing						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.FS-MDM.E1.IF.1	FlexSync Batch Jobs will populate FlexSync staging tables with a limited number of records per test case requirements. The FlexSync MQ Broker interface will select these records from the staging tables, create an XML message per the MDM Functional/Technical Specification and then send the XML message to the Siemens hosted eMeter EnergyIP MDM system web service using SOAP. The MDM web service will reply with a success or failure message as appropriate and this reply message will be logged.	(1) MDM FlexSync UCA Process and corresponding jobs will run to select Account/SDP changes from CISPROD for submission to the MDM. NOTE: The appropriate changes must have been made to accounts (i.e. rate changes, move-in/out, etc.) to trigger their appearance in the selection query (2) MQ Broker will successfully generate and send a SOAP message to MDM with valid data and receive a valid "success" response which is logged. The record will be updated correctly in MDM. (3) MQ Broker will successfully generate and send a SOAP message to MDM with invalid data and receive a valid "error" response which is logged. The record will not be updated in MDM.				
INT.FS-MDM.E1.IF.2	On a daily basis, KCP&L will transfer an MDM specific formatted EMED file generated by L+G Command Center 5.1 via the MQ File Mover Interface to the Siemens hosted server via SFTP. The TEST EMED file contains daily register reads for 4 SmartGrid Lab meters. The PROD EMED file contains daily register reads for the previous day for all SmartGrid meters (~14,000).	Command Center will generate the file in the specified format. MQ File Mover will find the daily file in the specified location and successfully move it to Siemens via SFTP. EIP adapter will pick up the file and load it into the MDM system. Meter data values from the file will be viewable in the EIP UI.				
INT.FS-MDM.E1.IF.3	On a daily basis, KCP&L will transfer an standard formatted intervals file generated by L+G Command Center 5.1 via the MQ File Mover Interface to the Siemens hosted server via SFTP.	Command Center will generate the file in the specified format. MQ File Mover will find the daily file in the specified location and successfully move it to Siemens via SFTP. EIP adapter will pick up the file and load it into the MDM system. Meter data values from the file will be viewable in the EIP UI.				
Integration Test Book – MDM Interfaces to FlexSync: MDM Validation, Estimation, Editing (VEE) Functionality						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.FS-MDM.E1.VEE.1	Test user can perform manual validation, estimation and editing in the MDM GUI in the Data Administration module and specifically the "Interval Editing" function.	Test user can view, validate, edit and create values using the EIP UI.				
INT.FS-MDM.E1.VEE.2	MDM will estimate any gaps in interval reads that it encounters. It will only estimate these values if it has both a read prior to and following the gap; open-ended gaps will not be estimated. 90 days of meter read history are desirable to produce a more accurate estimated value.	MDM will fill the gaps in the interval read values.				
INT.FS-MDM.E1.VEE.3	If the MDM receives actual values for a slot where it had previously Estimated a value, it will replace the estimated value with the actual value.	If a valid read is then received for a specific slot, the actual read will replace either an extrapolated or interpolated read.				
INT.FS-MDM.E1.VEE.4	If the MDM determines it is missing the most recent meter read value, it will extrapolate a value based on prior reads. This includes both daily register reads and 15 minute interval reads.	MDM populates the most recent "empty" read slot with an extrapolated value that makes sense based on prior data.				
INT.FS-MDM.E1.VEE.5	If the MDM receives actual values for a slot where it had previously either Extrapolated or Interpolated a value, it will replace the estimated value with the actual value.	If a valid read is then received for a specific slot, the actual read will replace either an extrapolated or interpolated read.				
INT.FS-MDM.E1.VEE.6	If the MDM determines it is missing the most recent meter read value, it will extrapolate a value based on prior reads. This includes both daily register reads and 15 minute interval reads. If MDM then receives valid reads after the gap period, it will re-estimate the original missing reads using interpolation.	MDM will re-estimate previously extrapolated reads by interpolation.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.FS-MDM.E1.VEE.7	If the MDM receives actual values for a slot where it had previously either Extrapolated or Interpolated a value, it will replace the estimated value with the actual value.	If a valid read is then received for a specific slot, the actual read will replace either an extrapolated or interpolated read.				
Integration Test Book – MDM Interfaces to FlexSync: MDM TOU Setup & Usage Framing						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.FS-MDM.E1.TOU.1	Regular rate setup process will be followed in MDM.	1TOUA and 1TOAA rates in MDM will be available for mapping SDP/account to the corresponding TOU calendar.				
INT.FS-MDM.E1.TOU.2	This scenario covers the TOU Calendar setup – Seasons, Day Type, Peak/Off-Peak Times – in each of the key systems.	For testing, the 2011 TOU Test calendar will be set up with November 2011 as a “Summer” month and December 2011 as a “Winter” month for 1TOUA and with November 2011 as a “Winter” month and December 2011 as a “Summer” month for 1TOAA. This may be modified depending on the actual date of the testing to ensure that both seasons are validated.				
INT.FS-MDM.E1.TOU.3	Customers who enroll in TOU will be framed per the TOU calendar beginning on their TOU effective date as communicated from CIS to MDM. Assumption is that 1TOUA and 1TOAA frame consistently, so the regression test only requires validation of the more common 1TOUA rate.	MDM will correctly frame usage for all customers enrolled in the 1TOUA rate.				
INT.FS-MDM.E1.TOU.4	KCP&L will use MQ Broker to request and retrieve usage data from MDM on a daily basis for all TOU customers. This usage data will be written to a staging table for further processing outside this test case.	TOU Calculator staging table is populated with usage data for 1TOUA customers.				

Integration Test Book – MDM Interfaces via VPN: MDM General User Functionality Regression Testing						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-VPN.E2.USER.1	Confirm that KCP&L personnel may access the EIP user interface and browse through various screens. This is not intended to test any specific functionality of the EIP system.	KCP&L personnel are able to access the EIP user interface, successfully log in and browse through the system.				
INT.MDM-VPN.E2.USER.2	Confirm that KCP&L personnel may access the EIP SFTP server using the Push Billing account and post/retrieve files.	KCP&L personnel are able to access the EIP SFTP server and then post and retrieve files successfully.				
INT.MDM-VPN.E2.USER.3	Confirm that KCP&L personnel may access the EIP SFTP server using the Meter Reads account and post/retrieve files.	KCP&L personnel are able to access the EIP SFTP server and then post and retrieve files successfully.				
INT.MDM-VPN.E2.USER.4	Confirm that KCP&L personnel may access the EIP server which runs EIP web services.	KCP&L personnel are able to access the EIP web server.				
INT.MDM-VPN.E2.USER.5	Confirm that KCP&L is able to access the MDM FlexSync web service.	KCP&L MQ Broker interface is able to access the MDM FlexSync web service and get a response - either valid or error is acceptable as the purpose is to confirm that we have connectivity.				
INT.MDM-VPN.E2.USER.6	Confirm that KCP&L is able to access the MDM FlexSync web service.	KCP&L MQ Broker interface is able to access the MDM flexSync web service and get a response - either valid or error is acceptable as the purpose is to confirm that we have connectivity.				
INT.MDM-VPN.E2.USER.7	Tester will log in to the EIP UI using the "systems administrator" account and visit each of the major screens and links. Errors or other non-functional links/pages will be logged for report back to Siemens.	Tester can log into the EIP UI and visit all of the pages noted below. The tester may click on additional links buttons as desired to further review the UI.				
INT.MDM-VPN.E2.USER.8	Ensure that the specified report is generated by the MDM system and if appropriate distributed by email to the KCP&L report distribution list.	The named report is generated by EIP and viewable in the EIP UI. The named report is automatically sent via email to the KCP&L report distribution list.				
Integration Test Book – MDM Interfaces via VPN: MDM System Interface Regression Testing						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-VPN.E2.IF.1	Confirm that FlexSync process is able to access the new kcp1testeip1.mdmhosting.com domain within the VPN.	(1) FlexSync flows are able to access the new domain name.				
INT.MDM-VPN.E2.IF.2	Confirm that Pull Billing process is able to access the new kcp1testeip1.mdmhosting.com domain within the VPN.	(1) Pull Billing flows are able to access the new domain name.				
INT.MDM-VPN.E2.IF.3	On a daily basis, KCP&L will transfer an MDM specific formatted EMED file generated by L+G Command Center 5.1 via the MQ File Mover Interface to the Siemens hosted server via SFTP. The TEST EMED file contains daily register reads for 4 SmartGrid Lab meters. The PROD EMED file contains daily register reads for the previous day for all SmartGrid meters (~14,000).	Command Center will generate the file in the specified format. MQ File Mover will find the daily file in the specified location and successfully move it to Siemens via SFTP. EIP adapter will pick up the file and load it into the MDM system. Meter data values from the file will be viewable in the EIP UI.				
INT.MDM-VPN.E2.IF.4	On a daily basis, KCP&L will transfer an standard formatted Intervals file generated by L+G Command Center 5.1 via the MQ File Mover Interface to the Siemens hosted server via SFTP.	Command Center will generate the file in the specified format. MQ File Mover will find the daily file in the specified location and successfully move it to Siemens via SFTP. EIP adapter will pick up the file and load it into the MDM system. Meter data values from the file will be viewable in the EIP UI.				
Integration Test Book – MDM Interfaces via VPN: MDM Validation, Estimation, Editing (VEE) Functionality						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-VPN.E2.VEE.1	MDM will estimate any gaps in interval reads that it encounters. It will only estimate these values if it has both a read prior to and following the gap; open-ended gaps will not be estimated. 90 days of meter read history are desirable to produce a more accurate estimated value.	MDM will fill the gaps in the interval read values.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-VPN.E2.VEE.2	If the MDM receives actual values for a slot where it had previously Estimated a value, it will replace the estimated value with the actual value.	If a valid read is then received for a specific slot, the actual read will replace either an extrapolated or interpolated read.				
INT.MDM-VPN.E2.VEE.3	If the MDM determines it is missing the most recent meter read value, it will extrapolate a value based on prior reads.	MDM populates the most recent "empty" read slot with an extrapolated value that makes sense based on prior data.				
INT.MDM-VPN.E2.VEE.4	If the MDM receives actual values for a slot where it had previously either Extrapolated or Interpolated a value, it will replace the estimated value with the actual value.	If a valid read is then received for a specific slot, the actual read will replace either an extrapolated or interpolated read.				
INT.MDM-VPN.E2.VEE.5	If the MDM determines it is missing the most recent meter read value, it will extrapolate a value based on prior reads. This includes both daily register reads and 15 minute interval reads. If MDM then receives valid reads after the gap period, it will re-estimate the original missing reads using interpolation.	MDM will re-estimate previously extrapolated reads by interpolation.				
INT.MDM-VPN.E2.VEE.6	If the MDM receives actual values for a slot where it had previously either Extrapolated or Interpolated a value, it will replace the estimated value with the actual value.	If a valid read is then received for a specific slot, the actual read will replace either an extrapolated or interpolated read.				
Integration Test Book - MDM Interfaces via VPN: MDM TOU Functionality						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-VPN.E2.TOU.1	Customers who enroll in TOU will be framed per the TOU calendar beginning on their TOU effective date as communicated from CIS to MDM. Assumption is that 1TOUA and 1TOAA frame consistently, so the regression test only requires validation of the more common 1TOUA rate.	MDM will correctly frame usage for all customers enrolled in the 1TOUA rate.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-VPN.E2.TOU.2	KCP&L will use manually generate a billing request via the MDM GUI and verify that the file is exported for processing by KCP&L.	Billing request is successfully generated and "billing determinants" file is created for retrieval by KCP&L.				

Integration Test Book – AHE Interfaces to Meter: End Point Processing Checks						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.AHE-MTR.E3.1	Validate AMI meter is switched off for Remote Disconnect Order – AHE Status	Cross-reference screenshots in supplemental documentation.				
INT.AHE-MTR.E3.2	Validate AMI meter is switched off for Remote Disconnect Order – Meter Status	Cross-reference screenshots in supplemental documentation.				
INT.AHE-MTR.E3.3	Validate that ODR is returned for Remote Disconnect Order – AHE Status	Cross-reference screenshots in supplemental documentation.				
INT.AHE-MTR.E3.4	Validate AMI meter is switched on for Remote Connect Order – AHE Status	Cross-reference screenshots in supplemental documentation.				
INT.AHE-MTR.E3.5	Validate AMI meter is switched on for Remote Connect Order – Meter Status	Cross-reference screenshots in supplemental documentation.				
INT.AHE-MTR.E3.6	Validate that ODR is returned for Remote Connect Order – AHE Status	Cross-reference screenshots in supplemental documentation.				

Integration Test Book – AHE Interfaces to MDM: MDM- AHE For EndDeviceControls Request						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.AHE-MDM.E4.GROUP1.1	Validate to get the synchronous Request (CreateEndDeviceControls) from MDM Via Soap.	N/A				
INT.AHE-MDM.E4.GROUP1.2	Check whether we receive both incoming synchronous messages in IEC-61968 format.	N/A				
INT.AHE-MDM.E4.GROUP1.3	Verify the Audit logs whether we are logging the incoming message properly or not.	N/A				
INT.AHE-MDM.E4.GROUP1.4	Route the message to ESB based on the incoming messageType. A) KCPLHeader.MessageType = 'createEndDeviceControls' Then send the message to ESB_ROUTE_ENDDEVICECONTROLS queue. B) KCPLHeader.MessageType = 'getMeterReadings' Then send the message to ESB_ROUTE_METERREADINGS queue.	N/A				
INT.AHE-MDM.E4.GROUP1.5	Check whether we added Kcpl Header before sending to ESB.	N/A				
INT.AHE-MDM.E4.GROUP1.6	Verify the audit table whether we are logging every thing to log table for every adapter.	N/A				
INT.AHE-MDM.E4.GROUP1.7	Validate the incoming Message from the ESB queue have the kcpl header and that includes request message or not.	N/A				
INT.AHE-MDM.E4.GROUP1.8	Verify whether the environment variables set properly in order to determine whether the incoming message is request or reply message.	N/A				
INT.AHE-MDM.E4.GROUP1.9	Route the Request message (If createEndDeviceControls) To AHE inbound queue (AHE_ADAPTER_CREATEENDDEVICECONTROLS_INBOUND) by deleting the Kcpl Header.	N/A				
INT.AHE-MDM.E4.GROUP1.10	Verify whether we send the proper request message to the AHE Inbound queue or not.	N/A				
INT.AHE-MDM.E4.GROUP1.11	Check whether we are making proper web service call (AHE)	N/A				
INT.AHE-MDM.E4.GROUP1.12	Make sure to add Kcpl Header to the response before sending to ESB (ESB_ROUTE_ENDDEVICECONTROLS) queue.	N/A				
INT.AHE-MDM.E4.GROUP1.13	Check whether we receive the proper response with Kcpl Header.	N/A				
INT.AHE-MDM.E4.GROUP1.14	Route the Response message (If replyEndDeviceControls) MDM_ADAPTER_REPLYENDDEVICECONTROLS_INBOUND queue.	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.AHE-MDM.E4.GROUP1.15	Verify to send the Asynchronous response (EndDeviceEvents) back to MDM.	N/A				
INT.AHE-MDM.E4.GROUP1.17	Test whether we added the reply Identifier before sending reply.	N/A				
Integration Test Book – AHE Interfaces to MDM: MDM- AHE For GetMeterReadings Request						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.AHE-MDM.E4.GROUP2.1	Validate to get the synchronous Request (getMeterReadings) from MDM Via Soap.	N/A				
INT.AHE-MDM.E4.GROUP2.2	Check whether we receive both incoming synchronous messages in IEC-61968 format.	N/A				
INT.AHE-MDM.E4.GROUP2.3	Verify the Audit logs whether we are logging the incoming message properly or not.	N/A				
INT.AHE-MDM.E4.GROUP2.4	Route the message to ESB based on the incoming messageType. A) KcplHeader.MessageType = 'getMeterReadings' Then send the message to ESB_ROUTE_METERREADINGS queue.	N/A				
INT.AHE-MDM.E4.GROUP2.5	Check whether we added Kcpl Header before sending to ESB.	N/A				
INT.AHE-MDM.E4.GROUP2.6	Verify the audit table whether we are logging every thing to log table for every adapter.	N/A				
INT.AHE-MDM.E4.GROUP2.7	Validate the incoming Message from the ESB queue have the kcpl header and that includes request message or not.	N/A				
INT.AHE-MDM.E4.GROUP2.8	Verify whether the environment variables set properly in order to determine whether the incoming message is request or reply message.	N/A				
INT.AHE-MDM.E4.GROUP2.9	Route the Request message (If createEndDeviceControls) To AHE inbound queue (AHE_ADAPTER_GETMETERREADINGS_INBOUND) by deleting the Kcpl Header.	N/A				
INT.AHE-MDM.E4.GROUP2.10	Verify whether we send the proper request message to the AHE Inbound queue or not.	N/A				
INT.AHE-MDM.E4.GROUP2.11	Check whether we are making proper web service call (AHE)	N/A				
INT.AHE-MDM.E4.GROUP2.12	Make sure to add Kcpl Header to the response before sending to ESB (ESB_ROUTE_METERREADINGS) queue.	N/A				
INT.AHE-MDM.E4.GROUP2.13	Check whether we receive the proper response with Kcpl Header	N/A				
INT.AHE-MDM.E4.GROUP2.14	Route the Response message (If replyMeterReadings) MDM_ADAPTER_REPLYMETERREADINGS_INBOUND queue	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.AHE-MDM.E4.GROUP2.15	Verify to send the Asynchronous response (MeterReadings) back to MDM.	N/A				
INT.AHE-MDM.E4.GROUP2.16	Verify AHE generates the Asynchronous response for the given MeterReadings Request.	N/A				
INT.AHE-MDM.E4.GROUP2.17	Check for the audit logs whether we log everything to the table.	N/A				
INT.AHE-MDM.E4.GROUP2.18	Test whether we are logging proper payload message and related response to the ESB Log table (KCPL_ESB_AUDIT).	N/A				

Integration Test Book – ESB Interfaces to Misc Systems: Simulated Outage/Restoration Event						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.B1.OUT.1	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the ESB Logs and MDM.				
INT.ESB-MISC.B1.OUT.2	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the ESB Logs and MDM.				
INT.ESB-MISC.B1.RES.1	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the ESB Logs and MDM.				
INT.ESB-MISC.B1.RES.2	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the ESB Logs and MDM.				
Integration Test Book – ESB Interfaces to Misc Systems: Meter Lab Outage/Restoration Event (w/o OMS)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.B1.OUT.3	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the AHE and MDM.				
INT.ESB-MISC.B1.RES.3	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the AHE and MDM.				
Integration Test Book – ESB Interfaces to Misc Systems: Meter Lab Outage/Restoration Event (w/OMS)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.B1.OUT.4	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the AHE, MDM and OMS.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.B1.RES.4	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the AHE, MDM and OMS.				

Integration Test Book – ESB Interfaces to Misc Systems: Outage Derivation in MDM via FlexSync						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.B2.FS.1	Generate a single FlexSync Message from CIS test environment via ESB to the MDM with the modified SDP-Meter Association date and verify the results.	(1) Confirm that FlexSync message is sent to MDM with modified SDP-Meter Association date (2) Verify that MDM processes the message (3) Verify that MDM derives the Outage Service for the SDP				
INT.ESB-MISC.B2.FS.2	Generate a multiple FlexSync Message from CIS test environment via ESB to the MDM with the modified SDP-Meter Association date and verify the results.	(1) Confirm that FlexSync message is sent to MDM with modified SDP-Meter Association date (2) Verify that MDM processes the message (3) Verify that MDM derives the Outage Service for the SDP				
INT.ESB-MISC.B2.FS.3	Generate a single FlexSync Message from CIS test environment via ESB to the MDM with the modified SDP-Meter Association date and verify the results.	(1) Confirm that FlexSync message is sent to MDM with modified SDP-Meter Association date (2) Verify that MDM processes the message (3) Verify that MDM derives the Outage Service for the SDP				

Integration Test Book – ESB Interfaces to Misc Systems: Power Status Verification – Unit Testing						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.C.3	Validate setup and configuration of the OMS, ESB, MDM, and AHE to support Power Status Verification	A) Verify that the OMS is configured to write PSV request messages to the OMS_AMI_REPLY queue and read PSV reply messages from the OMS_AMI_INPUT_PSV queue B) Verify that the ESB is configured to read PSV request messages from the OMS_AMI_REPLY queue, send PSV request messages to the MDM, and write PSV reply messages to the OMS_AMI_INPUT_PSV queue C) Verify that the MDM is configured to send PSV request and reply messages to the ESB D) Verify that the AHE is configured to send PSV reply messages to the ESB				
INT.ESB-MISC.C.4	Confirm that the OMS is generating the appropriate outbound PSV request message to the MDM via the ESB	A) Verify that the OMS generates the appropriate outbound PSV request message and sends it to the ESB on the OMS_AMI_REPLY queue to be transformed and sent to the MDM				
INT.ESB-MISC.C.5	Confirm that the ESB is properly transforming PSV request message from the OMS to the MDM	A) Verify that the ESB reads the PSV request message from the OMS_AMI_REPLY queue B) Verify that the ESB makes WebService call to the CIS to check for 'MeterEnergized' status C) Verify that the ESB transforms the PSV request message to the proper format for the MDM to process D) Verify that the ESB sends the transformed PSV request message to the MDM				
INT.ESB-MISC.C.6	Confirm that the MDM is generating the appropriate outbound PSV request message to the AHE via the ESB	A) Verify that the MDM receives the PSV request message from the ESB B) Verify that the MDM generates the appropriate outbound PSV request message (endpoint on-demand read request) and sends it to the AHE via the ESB				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.C.7	Confirm that the AHE receives the PSV request message from the MDM via the ESB	A) Verify that the AHE receives the PSV request message (endpoint on-demand read request) from the MDM via the ESB and sends the PSV request message to the target AMI meter				
INT.ESB-MISC.C.8	Confirm that the AHE is processing the PSV request message and generating the appropriate outbound PSV reply message to the MDM via the ESB	A) Verify that the AHE receives PSV reply message from the target AMI meter and generates the appropriate outbound PSV reply message (endpoint on-demand read reply) and sends it to the MDM via the ESB				
INT.ESB-MISC.C.9	Confirm that the MDM is generating the appropriate outbound PSV reply message to the OMS via the ESB	A) MDM generates a 'meter on' PSV reply message and sends it to the ESB				
INT.ESB-MISC.C.10	Confirm that the ESB is properly transforming the PSV reply message from the MDM to the OMS	A) Verify that the ESB receives the PSV reply message from the MDM B) Verify that the ESB transforms the PSV reply message to the proper format for the OMS to process C) Verify that ESB sends the transformed PSV reply message to the OMS_AMI_INPUT_PSV queue				
INT.ESB-MISC.C.11	Confirm that the OMS is processing the PSV reply message	A) Verify that OMS reads the PSV reply message from the OMS_AMI_INPUT_PSV queue				
INT.ESB-MISC.C.12	Test Plan review	Review test plan PRIOR TO testing. Consult your PA to determine attendees. Review unit test results if necessary				
INT.ESB-MISC.C.13	Code review – include diffs'	Repeat code review if changes were made during unit testing				
Integration Test Book - ESB Interfaces to Misc Systems: Power Status Verification - System/Scenario Testing						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.C.14	PSV is manually initiated from the OMS to a target meter that is powered ON	N/A				
INT.ESB-MISC.C.15	PSV is manually initiated from the OMS to a target meter that is powered OFF	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.C.16	PSV is manually initiated from the OMS to a target meter that is not "energized" in CIS (service disconnected)	A) Verify that the OMS generates the appropriate outbound PSV request message and sends it to the ESB on the OMS_AMI_REPLY queue to be transformed and sent to the MDM B) Verify that the ESB reads the PSV request message from the OMS_AMI_REPLY queue, makes WebService call to the CIS to check for 'MeterEnergized=N' status, creates the appropriate PSV reply message in the proper format for the OMS to process, and sends the created PSV reply message to the OMS_AMI_INPUT_PSV queue C) Verify that OMS reads the PSV reply message from the OMS_AMI_INPUT_PSV queue				

Integration Test Book – MDM Interfaces to CIS: Request 55443R MDM Aggregation						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-CIS.F1.4	SGD301 – Get parameters for service points, meters.	Verify SQL per supplemental documentation.				
INT.MDM-CIS.F1.5	sg_sp_param_assoc_master_t BEFORE master table was updated. Shows old values from CIS.	Verify SQL per supplemental documentation.				
INT.MDM-CIS.F1.6	sg_sp_param_assoc_today_t Shows new values from GIS. Circuit ID is no longer all 9s.	Verify SQL per supplemental documentation.				
INT.MDM-CIS.F1.7	sg_sp_list_prev_t	Verify SQL per supplemental documentation.				
INT.MDM-CIS.F1.8	sg_sp_list_today_t	Verify SQL per supplemental documentation.				
INT.MDM-CIS.F1.9	sg_sp_compare_list_t	Verify SQL per supplemental documentation.				
INT.MDM-CIS.F1.10	mdm_sdp_t NOTE: MRID = SP ID The ID fields are all defined as 50 characters (even though we don't use that many) because that is the field size used by the vendor. The extra size causes blank space to appear when selecting the columns for display.	Verify SQL per supplemental documentation.				

Integration Test Book – MDM Interfaces to CIS: Remote Service Order						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-CIS.F2.4	Validate adding a new meter model without a Remote Disconnect Switch (RDS) flag produces an error message "Remote Disconnect Switch Flag must be Y or N"	N/A				
INT.MDM-CIS.F2.5	Validate adding a new meter model with an RDS flag not equal to 'N' or 'Y' produces error message "Remote Disconnect Switch Flag must be Y or N"	N/A				
INT.MDM-CIS.F2.6	Validate able to successfully add a new meter model with RDS flag equal to 'N'	N/A				
INT.MDM-CIS.F2.7	Validate audit trail entry (CTCMODE) shows added entry with RDS = 'N'	N/A				
INT.MDM-CIS.F2.8	Validate audit trail by time (CTCMODT) shows added entry with RDS = 'N'	N/A				
INT.MDM-CIS.F2.9	Validate able to successfully add a new meter model with RDS flag equal to 'Y'	N/A				
INT.MDM-CIS.F2.10	Validate audit trail entry (CTCMODE) shows added entry with RDS = 'Y'	N/A				
INT.MDM-CIS.F2.11	Validate audit trail by time (CTCMODT) shows added entry with RDS = 'Y'	N/A				
INT.MDM-CIS.F2.12	Change existing model's RDS flag from 'N' to '' and validate error message received stating "Remote Disconnect Switch Flag must be Y or N"	N/A				
INT.MDM-CIS.F2.13	Change an existing model's RDS flag from 'N' to a non-'Y' value and validate error message received stating "Remote Disconnect Switch Flag must be Y or N"	N/A				
INT.MDM-CIS.F2.14	Validate able to successfully change existing model's RDS flag from 'N' to 'Y'	N/A				
INT.MDM-CIS.F2.15	Validate audit trail entry (CTCMODE) shows changed entry with RDS = 'Y'	N/A				
INT.MDM-CIS.F2.16	Validate audit trail by time (CTCMODT) shows changed entry with RDS = 'Y'	N/A				
INT.MDM-CIS.F2.17	Change existing model's RDS flag from 'Y' to '' and validate error message received stating RDS value is required	N/A				
INT.MDM-CIS.F2.18	Change an existing model's RDS flag from 'Y' to a non-'N' value and validate error message received stating invalid RDS value	N/A				
INT.MDM-CIS.F2.19	Validate able to successfully change existing model's RDS flag from 'Y' to 'N'	N/A				
INT.MDM-CIS.F2.20	Validate audit trail entry (CTCMODE) shows changed entry with RDS = 'N'	N/A				
INT.MDM-CIS.F2.21	Validate audit trail by time (CTCMODT) shows changed entry with RDS = 'N'	N/A				
INT.MDM-CIS.F2.22	Validate model listing includes RDS column with valid values	N/A				
INT.MDM-CIS.F2.23	Validate the Service Order Auto Completion skips RSO orders	N/A				
INT.MDM-CIS.F2.24	Validate MOBILE Extract does not select RSO eligible orders	N/A				
INT.MDM-CIS.F2.25	Confirm that CIS+ does not send multiple/duplicate RSO requests	N/A				
INT.MDM-CIS.F2.26	Validate that the RSO Service Order Auto Completion only includes connects and disconnects scheduled to be processed on that day (Request)	N/A				
INT.MDM-CIS.F2.27	Validate that CIS+ can process and post the final meter reading as appropriate Completed order	N/A				

Integration Test Book – MDM Interfaces to CIS: Remote Service Order End to End (Turn On Read Orders)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-CIS.F3.3	Turn On-Read: Meter @ SP Status = OFFS	Received error message "Invalid Turn On SubType"				
INT.MDM-CIS.F3.4	Turn On-Read: RSO Ineligible – CellNet Meter – Succession Orders (ON-R #1)	Neither Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.5	Turn On-Read: RSO Ineligible – CellNet Meter (ON-R #1)	Account (ID)/Order Control ID are not selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.6	Turn On-Read: RSO Eligible Meter – Succession Orders (ON-R #1)	- Showing meter XXXXXXXXXX has a disconnect switch (indicated by the 'G') - Remaining 7/31 pending orders for meters with a disconnect switch after SOAUTC and Mobile Extract ACCOUNT_ID SO_ID PREMISE_ID SO_T XXXXXXXX (Removed in TPR to to confidentiality) - ON-R account XXXXXXXX is selected for new RSO batch and OFF-J account XXXXXXXX is not (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.7	Turn On-Read: RSO Eligible Meter – Succession Orders & LL Revert (ON-R #1)	N/A				
INT.MDM-CIS.F3.8	Turn On-Read: RSO Eligible Meter – TOU Rates (ON-R #1)	- Time of Use Rate (TOUA) on a meter with remote disconnect switch - Neither Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.9	Turn On-Read: RSO Ineligible – Field Order – Succession Orders (ON-R#2)	- District Area 7 – No Mobile, only paper orders; Pending ON-R order - Neither Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.10	Turn On-Read: RSO Eligible Meter – SP Status is 'OFFP' (ON-R #2)	- Meter @ SP Status has been changed to 'OffP' - Account (ID)/Order Control ID are not selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-CIS.F3.11	Turn On-Read: RSO & Switch Eligible (ON-R#3)	- Meter @ SP Status is 'Conn On' at time ON-R order is entered - Meter @ SP Status has changed to 'Conn Offs' before order date. No pending Off order. Off Read manually completed with a 7/30 date - Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.12	Turn On-Read: RSO Eligible but Not Switch Eligible (ON-R#24)	- Pending ON-R and completed OFF-J (dated 8/2 originally but changed to end date of 7/25 in green screens) - Meter @ SP Status is 'Conn On' but not linked to a customer - Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.13	Turn On-Read: RSO & Switch Eligible	- No pending same day off order - Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.14	Turn On-Read: RSO Eligible but Not Switch Eligible – Reads don't exist (ON-R#26)	N/A				
INT.MDM-CIS.F3.15	Turn On-Read: RSO & Switch Eligible – Switch Unknown (ON-R #9)	N/A				
INT.MDM-CIS.F3.16	Turn On-Read: RSO & Switch Eligible – Switch Fails (ON-R #16)	N/A				
INT.MDM-CIS.F3.17	Turn On-Read: RSO & Switch Eligible – Change Date	Remaining RSO order (After SOAUTC ran) SO_T ACCOUNT_ID METER_ID STD_FORM_ADDR ON R XXXXXXXX (Removed in TPR to to confidentiality) Mobile Extract Skipped Orders KMDFSRB_push_rep08:XXXXXXXXXXXXX Skipping RSO eligible OC (XXXXXXXXXX) Type (ON R)				
INT.MDM-CIS.F3.18	Cancel Turn On-Read: RSO Eligible Meter	Account (ID)/Order Control ID are not selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
Integration Test Book – MDM Interfaces to CIS: Remote Service Order End to End (Turn Off Read Orders)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-CIS.F3.19	Turn Off-Read: RSO Ineligible – CellNet Meter (OFF-R #1)	Account (ID)/Order Control ID are not selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.20	Turn Off-Read: RSO Ineligible – CellNet Meter – LL Revert (OFF-R #1)	Neither Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order).				
INT.MDM-CIS.F3.21	Turn Off-Read: RSO Ineligible – Mobile – LL Revert (OFF-R #2)	- South District works off paper orders which are printed in the office - Account (ID)/Order Control ID are not selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.22	Turn Off-Read: RSO Ineligible – Mobile (OFF-R #2)	- East District works off paper orders which are printed in the office - Account (ID)/Order Control ID are not selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.23	Turn Off-Read: RSO & Switch Eligible (OFF-R #3)	- No LL revert, life support or sensitive load. No pending same day On order - Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.24	Turn Off-Read: RSO & Switch Eligible – Pending ON-R in the future (OFF-R #3)	- Pending ON-R and OFF-J for 8/2/12. Changed OFF-J to OFF-R and 7/31/12 - No LL revert, life support or sensitive load. - Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.25	Turn Off-Read: RSO but Not Switch Eligible – LL Revert (OFF-R #23)	Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.26	Turn Off-Read: RSO Eligible but Not Switch Eligible – Premise has Life Support (OFF-R #23)	Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-CIS.F3.27	Turn Off-Read: RSO Eligible but Not Switch Eligible – Person has Life Support (OFF-R #23)	Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.28	Turn Off-Read: RSO Eligible but Not Switch Eligible – Premise has Sensitive Load (OFF-R #23)	Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.29	Turn Off-Read: RSO Eligible but Not Switch Eligible – Person has Sensitive Load (OFF-R #23)	- Mobile Data Extract Skipped Orders: KMDFSRB_push_rep08: XXXXXXXX Skipping RSO eligible OC (XXXXXXXX) Type (OFFR) - Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.30	Turn Off-Read: RSO & Switch Eligible – Switch Unknown – Resubmit Switch Successful (OFF-R #9)	N/A				
INT.MDM-CIS.F3.31	Turn Off-Read: RSO & Switch Eligible – Switch Unknown – Resubmit On-Demand Read (OFF-R #14)	N/A				
INT.MDM-CIS.F3.32	Turn Off-Read: RSO & Switch Eligible – Switch Fails – Resubmit On-Demand Read (OFF-R #20)	N/A				
INT.MDM-CIS.F3.33	Turn Off-Read: RSO & Switch Eligible – Change Date #1	- Original order date is 8/15/12. Order changed to 7/31/12 - No LL revert, life support or sensitive load. - Account (ID)/Order Control ID are selected for new RSO batch on 7/31/12 (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-CIS.F3.34	Turn Off-Read: RSO & Switch Eligible - Change Date #2	- Original order date is 7/31/12. Change order date to 8/1/12 - No LL revert, life support or sensitive load. No same day pending On order - Mobile Data Extract Skipped Orders: KMDFSRB_push_rep08: XXXXXXXXX Skipping RSO eligible OC (XXXXXXXXX) Type (OFFR) - Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.35	Cancel Turn Off-Read: RSO Eligible Meter	- Order voided 1 day prior to the order date - Account (ID)/Order Control ID are not selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
Integration Test Book – MDM Interfaces to CIS: Remote Service Order End to End (Turn On At Meter Orders)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-CIS.F3.36	Turn On-At Meter: RSO Ineligible – CellNet Meter (ON-A #1)	Account (ID)/Order Control ID are not selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.37	Turn On-At Meter: RSO Ineligible – Itron Meter (ON-A #1)	Account (ID)/Order Control ID are not selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.38	Turn On-At Meter: RSO Eligible Meter – SP Status is not 'OFFS' (ON-A #1)	Account (ID)/Order Control ID are not selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.39	Turn On-At Meter: RSO Eligible Meter – Previously CNP'd (ON-A #1)	Account (ID)/Order Control ID are not selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.40	Turn On-At Meter: RSO & Switch Eligible (ON-A #2)	- No pending same day Off order - Mobile Data Extract Skipped Order: KMDFSRB_push_rep08: XXXXXXXXX Skipping RSO eligible OC (XXXXXXXXX) Type (ON A)				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-CIS.F3.41	Turn On-At Meter: RSO Eligible Meter – Sensitive Load (ON-A #2)	- Premise is designated as Sensitive Load. This should not affect RSO eligibility. - No pending same day Off order - Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.42	Turn On-At Meter: RSO Eligible but Not Switch Eligible (ON-A #23)	- No pending same day Off order - Need to change to "Conn On" after Mobile Extract				
INT.MDM-CIS.F3.43	Turn On-At Meter: RSO & Switch Eligible – Switch Fails (ON-A #16)	N/A				
INT.MDM-CIS.F3.44	Turn On-At Meter: RSO & Switch Eligible – Change Date #1	- Original order date is 8/10/12. Order date changed to 7/31/12 - No pending same day Off order - Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.45	Turn On-At Meter: RSO & Switch Eligible – Change Date #2	- Original order date 7/31/12. Change to 8/2/12 - Account (ID)/Order Control ID are not selected for new RSO batch on 7/31/12 (Query below shows accounts that are selected for RSO batch and are listed in numerical order) - No pending same day Off order				
INT.MDM-CIS.F3.46	Cancel Turn On-At Meter: RSO Eligible Meter	N/A				
Integration Test Book – MDM Interfaces to CIS: Remote Service Order End to End (Turn Off at Meter Orders)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-CIS.F3.47	Turn Off-Off at Meter: RSO Ineligible – CellNet Meter (OFF-O #1)	Account (ID)/Order Control ID are not selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.48	Turn Off-Off at Meter: RSO Ineligible – CellNet Meter – LL Revert (OFF-O #1)	- Landlord revert information for premise - Account (ID)/Order Control ID are not selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-CIS.F3.49	Turn Off-Off at Meter: RSO Ineligible – Mobile (OFF-O #1)	- Reference Test #10 for XXXXXXXXX, KS after this test is complete - District Area 7 – No Mobile, only paper orders - Account (ID)/Order Control ID are not selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.50	Turn Off-Off at Meter: RSO & Switch Eligible (OFF-O #2)	- No pending same day On order - Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.51	Turn Off-Off at Meter: RSO & Switch Eligible – LL Revert #1 (OFF-O #2)	- Premise has a landlord revert - No same day On order - Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.52	Turn Off-Off at Meter: RSO & Switch Eligible – LL Revert #2 (OFF-O #2)	- Landlord revert information (below) is the same acct that the electric service is currently linked to (above) - No pending same day On order - Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.53	Turn Off-Off at Meter: RSO & Switch Eligible – Premise has Life Support (OFF-O #2)	- Premise has life support - No pending same day On order - Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.54	Turn Off-Off at Meter: RSO & Switch Eligible – Premise has Sensitive Load (OFF-O #2)	- Premise has sensitive load - No pending same day On order - Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.55	Turn Off-Off at Meter: RSO & Switch Eligible – Person has Life Support (OFF-O #2)	- Person has life support - No pending same day On order - Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-CIS.F3.56	Turn Off-Off at Meter: RSO & Switch Eligible – Person has Sensitive Load (OFF-O #2)	- Person is marked as sensitive load - No pending same day On order - Account (ID)/Order Control ID are selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.57	Turn Off-Off at Meter: RSO & Switch Eligible – CIS+ Fails (OFF-O #3)	No pending same day On order				
INT.MDM-CIS.F3.58	Turn Off-Off at Meter: RSO Eligible but Not Switch Eligible (OFF-O #22)	Mobile Data Extract Skipped Orders KMDFSRB_push_rep08: XXXXXXXXXX Skipping RSO eligible OC (XXXXXXXXXX) Type (OFFO) KMDFSRB_push_rep08: XXXXXXXXXX Skipping RSO eligible OC (XXXXXXXXXX) Type (ON R)				
INT.MDM-CIS.F3.59	Turn Off-Off at Meter: RSO & Switch Eligible – Change Date	- Order originally dated for 8/17/12 - No pending same day On order - Mobile Data Extract Skipped Order: KMDFSRB_push_rep08: XXXXXXXXXX Skipping RSO eligible OC (XXXXXXXXXX) Type (OFFO)				
INT.MDM-CIS.F3.60	Cancel Turn Off-Off at Meter: RSO Eligible Meter	- Pending OFF-O order. Order is now voided - Account (ID)/Order Control ID are not selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
Integration Test Book – MDM Interfaces to CIS: Remote Service Order End to End (Miscellaneous)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-CIS.F3.61	Turn On-Install Meter: RSO Ineligible	Account (ID)/Order Control ID are not selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.62	Turn Off-Remove Meter	Account (ID)/Order Control ID are not selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.63	Turn Off-Remove Service	Account (ID)/Order Control ID are not selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-CIS.F3.64	Pending ON-J & OFF-J (Same Day) Orders: RSO Ineligible	- Pending OFF-J. Pending ON-J - Error report after SO Auto-completion. - Account (ID)/Order Control ID are not selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				
INT.MDM-CIS.F3.65	Service Investigation Order: Install Medical Seal	N/A				
INT.MDM-CIS.F3.66	RSO Eligible Meter: Meter Exchange	Account (ID)/Order Control ID are not selected for new RSO batch (Query below shows accounts that are selected for RSO batch and are listed in numerical order)				

Integration Test Book – MDM Interfaces to CIS: Remote Service Order Online GUI						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-CIS.F4.3	Validate able to enter ON-A for a meter with a Meter Disconnect Switch (MDS)	Added Successfully				
INT.MDM-CIS.F4.4	Validate able to enter ON-R for a meter with a MDS	N/A				
INT.MDM-CIS.F4.5	Validate not able to enter ON-R for a meter with a MDS where the Service Point is 'Offp' after a CNP	N/A				
INT.MDM-CIS.F4.6	Validate able to enter OFF-O for a meter with a MDS	N/A				
INT.MDM-CIS.F4.7	Validate able to enter OFF-R for a meter with a MDS	N/A				
INT.MDM-CIS.F4.8	Validate able to enter OFF-J for a meter with a MDS	N/A				
INT.MDM-CIS.F4.9	Validate able to enter ON-A for a meter without a MDS	N/A				
INT.MDM-CIS.F4.10	Validate able to enter ON-R for a meter without a MDS	N/A				
INT.MDM-CIS.F4.11	Validate able to enter OFF-O for a meter without a MDS	N/A				
INT.MDM-CIS.F4.12	Validate able to enter OFF-R for a meter without a MDS	N/A				
INT.MDM-CIS.F4.13	Validate able to delete pending order for a meter without a MDS	N/A				
INT.MDM-CIS.F4.14	Validate able to enter OFF-J for a meter without a MDS	N/A				
INT.MDM-CIS.F4.15	Validate able to void order for a meter without a MDS	N/A				
INT.MDM-CIS.F4.16	Validate able to manually change Meter @ SP Status to 'Meter Off Switched' for a SP with a MDS meter	N/A				
INT.MDM-CIS.F4.17	Validate SP audit log (SPAEL) captures changes to/from 'Meter Off Switched' status	(See previous test) Shows Meter At SP Status for Service Point XXXXXXXXX changed to 'S' and then back to 'O'				
INT.MDM-CIS.F4.18	Validate not able to manually change Meter @ SP Status to 'Meter Off Switched' for a SP without a MDS meter	N/A				
INT.MDM-CIS.F4.19	Validate Service Point Status is 'Conn OffS' when meter has been remotely disconnected	N/A				
INT.MDM-CIS.F4.20	Validate '**Remotely Disconnected**' appears in letSearch when meter has been remotely disconnected	N/A				

Integration Test Book – MDM Interfaces to CIS: Remote Service Order Web Services						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-CIS.F5.3	ON-A Remote Service Order	N/A				
INT.MDM-CIS.F5.4	ON-R Remote Service Order	N/A				
INT.MDM-CIS.F5.5	OFF-O Remote Service Order	N/A				
INT.MDM-CIS.F5.6	OFF-R Remote Service Order	N/A				

Integration Test Book – MDM Interfaces to FlexSync: MDM General User Functionality Regression Testing						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.FS-MDM.E1.USER.1	Confirm that KCP&L personnel may access the EIP user interface and browse through various screens. This is not intended to test any specific functionality of the EIP system.	KCP&L personnel are able to access the EIP user interface, successfully log in and browse through the system.				
INT.FS-MDM.E1.USER.2	Confirm that KCP&L personnel may access the EIP SFTP server using the Push Billing account and post/retrieve files.	KCP&L personnel are able to access the EIP SFTP server and then post and retrieve files successfully.				
INT.FS-MDM.E1.USER.3	Confirm that KCP&L personnel may access the EIP SFTP server using the Meter Reads account and post/retrieve files.	KCP&L personnel are able to access the EIP SFTP server and then post and retrieve files successfully.				
INT.FS-MDM.E1.USER.4	Confirm that KCP&L personnel may access the EIP server which runs EIP web services.	KCP&L personnel are able to access the EIP web server.				
INT.FS-MDM.E1.USER.5	Confirm that KCP&L is able to access the MDM FlexSync web service.	KCP&L MQ Broker interface is able to access the MDM FlexSync web service and get a response - either valid or error is acceptable as the purpose is to confirm that we have connectivity.				
INT.FS-MDM.E1.USER.6	Confirm that KCP&L is able to access the MDM FlexSync web service.	KCP&L MQ Broker interface is able to access the MDM FlexSync web service and get a response - either valid or error is acceptable as the purpose is to confirm that we have connectivity.				
INT.FS-MDM.E1.USER.7	Tester will log in to the EIP UI using the "systems administrator" account and visit each of the major screens and links. Errors or other non-functional links/pages will be logged for report back to Siemens.	Tester can log into the EIP UI and visit all of the pages noted below. The tester may click on additional links buttons as desired to further review the UI.				
INT.FS-MDM.E1.USER.8	Ensure that the specified report is generated by the MDM system and if appropriate distributed by email to the KCP&L report distribution list.	The named report is generated by EIP and viewable in the EIP UI. The named report is automatically sent via email to the KCP&L report distribution list.				
Integration Test Book – MDM Interfaces to FlexSync: MDM System Interface Regression Testing						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.FS-MDM.E1.IF.1	FlexSync Batch Jobs will populate FlexSync staging tables with a limited number of records per test case requirements. The FlexSync MQ Broker interface will select these records from the staging tables, create an XML message per the MDM Functional/Technical Specification and then send the XML message to the Siemens hosted eMeter EnergyIP MDM system web service using SOAP. The MDM web service will reply with a success or failure message as appropriate and this reply message will be logged.	(1) MDM FlexSync UCA Process and corresponding jobs will run to select Account/SDP changes from CISPROD for submission to the MDM. NOTE: The appropriate changes must have been made to accounts (i.e. rate changes, move-in/out, etc.) to trigger their appearance in the selection query (2) MQ Broker will successfully generate and send a SOAP message to MDM with valid data and receive a valid "success" response which is logged. The record will be updated correctly in MDM. (3) MQ Broker will successfully generate and send a SOAP message to MDM with invalid data and receive a valid "error" response which is logged. The record will not be updated in MDM.				
INT.FS-MDM.E1.IF.2	On a daily basis, KCP&L will transfer an MDM specific formatted EMED file generated by L+G Command Center 5.1 via the MQ File Mover Interface to the Siemens hosted server via SFTP. The TEST EMED file contains daily register reads for 4 SmartGrid Lab meters. The PROD EMED file contains daily register reads for the previous day for all SmartGrid meters (~14,000).	Command Center will generate the file in the specified format. MQ File Mover will find the daily file in the specified location and successfully move it to Siemens via SFTP. EIP adapter will pick up the file and load it into the MDM system. Meter data values from the file will be viewable in the EIP UI.				
INT.FS-MDM.E1.IF.3	On a daily basis, KCP&L will transfer an standard formatted intervals file generated by L+G Command Center 5.1 via the MQ File Mover Interface to the Siemens hosted server via SFTP.	Command Center will generate the file in the specified format. MQ File Mover will find the daily file in the specified location and successfully move it to Siemens via SFTP. EIP adapter will pick up the file and load it into the MDM system. Meter data values from the file will be viewable in the EIP UI.				
Integration Test Book – MDM Interfaces to FlexSync: MDM Validation, Estimation, Editing (VEE) Functionality						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.FS-MDM.E1.VEE.1	Test user can perform manual validation, estimation and editing in the MDM GUI in the Data Administration module and specifically the "Interval Editing" function.	Test user can view, validate, edit and create values using the EIP UI.				
INT.FS-MDM.E1.VEE.2	MDM will estimate any gaps in interval reads that it encounters. It will only estimate these values if it has both a read prior to and following the gap; open-ended gaps will not be estimated. 90 days of meter read history are desirable to produce a more accurate estimated value.	MDM will fill the gaps in the interval read values.				
INT.FS-MDM.E1.VEE.3	If the MDM receives actual values for a slot where it had previously Estimated a value, it will replace the estimated value with the actual value.	If a valid read is then received for a specific slot, the actual read will replace either an extrapolated or interpolated read.				
INT.FS-MDM.E1.VEE.4	If the MDM determines it is missing the most recent meter read value, it will extrapolate a value based on prior reads. This includes both daily register reads and 15 minute interval reads.	MDM populates the most recent "empty" read slot with an extrapolated value that makes sense based on prior data.				
INT.FS-MDM.E1.VEE.5	If the MDM receives actual values for a slot where it had previously either Extrapolated or Interpolated a value, it will replace the estimated value with the actual value.	If a valid read is then received for a specific slot, the actual read will replace either an extrapolated or interpolated read.				
INT.FS-MDM.E1.VEE.6	If the MDM determines it is missing the most recent meter read value, it will extrapolate a value based on prior reads. This includes both daily register reads and 15 minute interval reads. If MDM then receives valid reads after the gap period, it will re-estimate the original missing reads using interpolation.	MDM will re-estimate previously extrapolated reads by interpolation.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.FS-MDM.E1.VEE.7	If the MDM receives actual values for a slot where it had previously either Extrapolated or Interpolated a value, it will replace the estimated value with the actual value.	If a valid read is then received for a specific slot, the actual read will replace either an extrapolated or interpolated read.				
Integration Test Book – MDM Interfaces to FlexSync: MDM TOU Setup & Usage Framing						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.FS-MDM.E1.TOU.1	Regular rate setup process will be followed in MDM.	1TOUA and 1TOAA rates in MDM will be available for mapping SDP/account to the corresponding TOU calendar.				
INT.FS-MDM.E1.TOU.2	This scenario covers the TOU Calendar setup – Seasons, Day Type, Peak/Off-Peak Times – in each of the key systems.	For testing, the 2011 TOU Test calendar will be set up with November 2011 as a “Summer” month and December 2011 as a “Winter” month for 1TOUA and with November 2011 as a “Winter” month and December 2011 as a “Summer” month for 1TOAA. This may be modified depending on the actual date of the testing to ensure that both seasons are validated.				
INT.FS-MDM.E1.TOU.3	Customers who enroll in TOU will be framed per the TOU calendar beginning on their TOU effective date as communicated from CIS to MDM. Assumption is that 1TOUA and 1TOAA frame consistently, so the regression test only requires validation of the more common 1TOUA rate.	MDM will correctly frame usage for all customers enrolled in the 1TOUA rate.				
INT.FS-MDM.E1.TOU.4	KCP&L will use MQ Broker to request and retrieve usage data from MDM on a daily basis for all TOU customers. This usage data will be written to a staging table for further processing outside this test case.	TOU Calculator staging table is populated with usage data for 1TOUA customers.				

Integration Test Book – MDM Interfaces via VPN: MDM General User Functionality Regression Testing						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-VPN.E2.USER.1	Confirm that KCP&L personnel may access the EIP user interface and browse through various screens. This is not intended to test any specific functionality of the EIP system.	KCP&L personnel are able to access the EIP user interface, successfully log in and browse through the system.				
INT.MDM-VPN.E2.USER.2	Confirm that KCP&L personnel may access the EIP SFTP server using the Push Billing account and post/retrieve files.	KCP&L personnel are able to access the EIP SFTP server and then post and retrieve files successfully.				
INT.MDM-VPN.E2.USER.3	Confirm that KCP&L personnel may access the EIP SFTP server using the Meter Reads account and post/retrieve files.	KCP&L personnel are able to access the EIP SFTP server and then post and retrieve files successfully.				
INT.MDM-VPN.E2.USER.4	Confirm that KCP&L personnel may access the EIP server which runs EIP web services.	KCP&L personnel are able to access the EIP web server.				
INT.MDM-VPN.E2.USER.5	Confirm that KCP&L is able to access the MDM FlexSync web service.	KCP&L MQ Broker interface is able to access the MDM FlexSync web service and get a response - either valid or error is acceptable as the purpose is to confirm that we have connectivity.				
INT.MDM-VPN.E2.USER.6	Confirm that KCP&L is able to access the MDM FlexSync web service.	KCP&L MQ Broker interface is able to access the MDM flexSync web service and get a response - either valid or error is acceptable as the purpose is to confirm that we have connectivity.				
INT.MDM-VPN.E2.USER.7	Tester will log in to the EIP UI using the "systems administrator" account and visit each of the major screens and links. Errors or other non-functional links/pages will be logged for report back to Siemens.	Tester can log into the EIP UI and visit all of the pages noted below. The tester may click on additional links buttons as desired to further review the UI.				
INT.MDM-VPN.E2.USER.8	Ensure that the specified report is generated by the MDM system and if appropriate distributed by email to the KCP&L report distribution list.	The named report is generated by EIP and viewable in the EIP UI. The named report is automatically sent via email to the KCP&L report distribution list.				
Integration Test Book – MDM Interfaces via VPN: MDM System Interface Regression Testing						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-VPN.E2.IF.1	Confirm that FlexSync process is able to access the new kcp1testeip1.mdmhosting.com domain within the VPN.	(1) FlexSync flows are able to access the new domain name.				
INT.MDM-VPN.E2.IF.2	Confirm that Pull Billing process is able to access the new kcp1testeip1.mdmhosting.com domain within the VPN.	(1) Pull Billing flows are able to access the new domain name.				
INT.MDM-VPN.E2.IF.3	On a daily basis, KCP&L will transfer an MDM specific formatted EMED file generated by L+G Command Center 5.1 via the MQ File Mover Interface to the Siemens hosted server via SFTP. The TEST EMED file contains daily register reads for 4 SmartGrid Lab meters. The PROD EMED file contains daily register reads for the previous day for all SmartGrid meters (~14,000).	Command Center will generate the file in the specified format. MQ File Mover will find the daily file in the specified location and successfully move it to Siemens via SFTP. EIP adapter will pick up the file and load it into the MDM system. Meter data values from the file will be viewable in the EIP UI.				
INT.MDM-VPN.E2.IF.4	On a daily basis, KCP&L will transfer an standard formatted Intervals file generated by L+G Command Center 5.1 via the MQ File Mover Interface to the Siemens hosted server via SFTP.	Command Center will generate the file in the specified format. MQ File Mover will find the daily file in the specified location and successfully move it to Siemens via SFTP. EIP adapter will pick up the file and load it into the MDM system. Meter data values from the file will be viewable in the EIP UI.				
Integration Test Book – MDM Interfaces via VPN: MDM Validation, Estimation, Editing (VEE) Functionality						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-VPN.E2.VEE.1	MDM will estimate any gaps in interval reads that it encounters. It will only estimate these values if it has both a read prior to and following the gap; open-ended gaps will not be estimated. 90 days of meter read history are desirable to produce a more accurate estimated value.	MDM will fill the gaps in the interval read values.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-VPN.E2.VEE.2	If the MDM receives actual values for a slot where it had previously Estimated a value, it will replace the estimated value with the actual value.	If a valid read is then received for a specific slot, the actual read will replace either an extrapolated or interpolated read.				
INT.MDM-VPN.E2.VEE.3	If the MDM determines it is missing the most recent meter read value, it will extrapolate a value based on prior reads.	MDM populates the most recent "empty" read slot with an extrapolated value that makes sense based on prior data.				
INT.MDM-VPN.E2.VEE.4	If the MDM receives actual values for a slot where it had previously either Extrapolated or Interpolated a value, it will replace the estimated value with the actual value.	If a valid read is then received for a specific slot, the actual read will replace either an extrapolated or interpolated read.				
INT.MDM-VPN.E2.VEE.5	If the MDM determines it is missing the most recent meter read value, it will extrapolate a value based on prior reads. This includes both daily register reads and 15 minute interval reads. If MDM then receives valid reads after the gap period, it will re-estimate the original missing reads using interpolation.	MDM will re-estimate previously extrapolated reads by interpolation.				
INT.MDM-VPN.E2.VEE.6	If the MDM receives actual values for a slot where it had previously either Extrapolated or Interpolated a value, it will replace the estimated value with the actual value.	If a valid read is then received for a specific slot, the actual read will replace either an extrapolated or interpolated read.				
Integration Test Book - MDM Interfaces via VPN: MDM TOU Functionality						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-VPN.E2.TOU.1	Customers who enroll in TOU will be framed per the TOU calendar beginning on their TOU effective date as communicated from CIS to MDM. Assumption is that 1TOUA and 1TOAA frame consistently, so the regression test only requires validation of the more common 1TOUA rate.	MDM will correctly frame usage for all customers enrolled in the 1TOUA rate.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.MDM-VPN.E2.TOU.2	KCP&L will use manually generate a billing request via the MDM GUI and verify that the file is exported for processing by KCP&L.	Billing request is successfully generated and "billing determinants" file is created for retrieval by KCP&L.				

Integration Test Book – ESB Interfaces to Misc Systems: Simulated Outage/Restoration Event						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.B1.OUT.1	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the ESB Logs and MDM.				
INT.ESB-MISC.B1.OUT.2	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the ESB Logs and MDM.				
INT.ESB-MISC.B1.RES.1	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the ESB Logs and MDM.				
INT.ESB-MISC.B1.RES.2	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the ESB Logs and MDM.				
Integration Test Book – ESB Interfaces to Misc Systems: Meter Lab Outage/Restoration Event (w/o OMS)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.B1.OUT.3	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the AHE and MDM.				
INT.ESB-MISC.B1.RES.3	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the AHE and MDM.				
Integration Test Book – ESB Interfaces to Misc Systems: Meter Lab Outage/Restoration Event (w/OMS)						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.B1.OUT.4	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the AHE, MDM and OMS.				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.B1.RES.4	Confirm that the specified event scenario is transmitted from the AMI/AHE infrastructure through the KCP&L ESB to the MDM (via the eMeter EIP L+G 5.1 Adapter) and then from the MDM via ESB to the OMS system.	Specified event is visible in the AHE, MDM and OMS.				

Integration Test Book – ESB Interfaces to Misc Systems: Power Status Verification – Unit Testing						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.C.3	Validate setup and configuration of the OMS, ESB, MDM, and AHE to support Power Status Verification	A) Verify that the OMS is configured to write PSV request messages to the OMS_AMI_REPLY queue and read PSV reply messages from the OMS_AMI_INPUT_PSV queue B) Verify that the ESB is configured to read PSV request messages from the OMS_AMI_REPLY queue, send PSV request messages to the MDM, and write PSV reply messages to the OMS_AMI_INPUT_PSV queue C) Verify that the MDM is configured to send PSV request and reply messages to the ESB D) Verify that the AHE is configured to send PSV reply messages to the ESB				
INT.ESB-MISC.C.4	Confirm that the OMS is generating the appropriate outbound PSV request message to the MDM via the ESB	A) Verify that the OMS generates the appropriate outbound PSV request message and sends it to the ESB on the OMS_AMI_REPLY queue to be transformed and sent to the MDM				
INT.ESB-MISC.C.5	Confirm that the ESB is properly transforming PSV request message from the OMS to the MDM	A) Verify that the ESB reads the PSV request message from the OMS_AMI_REPLY queue B) Verify that the ESB makes Webservice call to the CIS to check for 'MeterEnergized' status C) Verify that the ESB transforms the PSV request message to the proper format for the MDM to process D) Verify that the ESB sends the transformed PSV request message to the MDM				
INT.ESB-MISC.C.6	Confirm that the MDM is generating the appropriate outbound PSV request message to the AHE via the ESB	A) Verify that the MDM receives the PSV request message from the ESB B) Verify that the MDM generates the appropriate outbound PSV request message (endpoint on-demand read request) and sends it to the AHE via the ESB				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.C.7	Confirm that the AHE receives the PSV request message from the MDM via the ESB	A) Verify that the AHE receives the PSV request message (endpoint on-demand read request) from the MDM via the ESB and sends the PSV request message to the target AMI meter				
INT.ESB-MISC.C.8	Confirm that the AHE is processing the PSV request message and generating the appropriate outbound PSV reply message to the MDM via the ESB	A) Verify that the AHE receives PSV reply message from the target AMI meter and generates the appropriate outbound PSV reply message (endpoint on-demand read reply) and sends it to the MDM via the ESB				
INT.ESB-MISC.C.9	Confirm that the MDM is generating the appropriate outbound PSV reply message to the OMS via the ESB	A) MDM generates a 'meter on' PSV reply message and sends it to the ESB				
INT.ESB-MISC.C.10	Confirm that the ESB is properly transforming the PSV reply message from the MDM to the OMS	A) Verify that the ESB receives the PSV reply message from the MDM B) Verify that the ESB transforms the PSV reply message to the proper format for the OMS to process C) Verify that ESB sends the transformed PSV reply message to the OMS_AMI_INPUT_PSV queue				
INT.ESB-MISC.C.11	Confirm that the OMS is processing the PSV reply message	A) Verify that OMS reads the PSV reply message from the OMS_AMI_INPUT_PSV queue				
INT.ESB-MISC.C.12	Test Plan review	Review test plan PRIOR TO testing. Consult your PA to determine attendees. Review unit test results if necessary				
INT.ESB-MISC.C.13	Code review – include diffs'	Repeat code review if changes were made during unit testing				
Integration Test Book - ESB Interfaces to Misc Systems: Power Status Verification - System/Scenario Testing						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.C.14	PSV is manually initiated from the OMS to a target meter that is powered ON	N/A				
INT.ESB-MISC.C.15	PSV is manually initiated from the OMS to a target meter that is powered OFF	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.ESB-MISC.C.16	PSV is manually initiated from the OMS to a target meter that is not "energized" in CIS (service disconnected)	A) Verify that the OMS generates the appropriate outbound PSV request message and sends it to the ESB on the OMS_AMI_REPLY queue to be transformed and sent to the MDM B) Verify that the ESB reads the PSV request message from the OMS_AMI_REPLY queue, makes WebService call to the CIS to check for 'MeterEnergized=N' status, creates the appropriate PSV reply message in the proper format for the OMS to process, and sends the created PSV reply message to the OMS_AMI_INPUT_PSV queue C) Verify that OMS reads the PSV reply message from the OMS_AMI_INPUT_PSV queue				

Integration Test Book – HEMP Interfaces to AHE: Meter ESI to Device Communication						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.HEMP-AHE.G.1	Device Commissioning/Joining: Devices commissioned to meter utilizing ETM tool and verify device joining at device and with ETM tool.	N/A				
INT.HEMP-AHE.G.2	Device Commissioning/Joining: Devices commissioned to meter utilizing ETM tool. After verification of joining, devices are removed utilizing ETM tool and network leave verified.	N/A				
INT.HEMP-AHE.G.3	Device Commissioning/Joining: Device is commissioned to meter without previously creating HAN.	N/A				
INT.HEMP-AHE.G.4	Device Commissioning/Joining: After joining device to meter messages initiated with past and future effective date/time received properly by device and verified with ZigBee "sniffer" capture.	N/A				
INT.HEMP-AHE.G.5	Device Commissioning/Joining: After joining device to meter and message having been sent, power cycling of meter then device should result in GetLastMessage command visible by ZigBee "sniffer".	N/A				
INT.HEMP-AHE.G.6	Device Commissioning/Joining: After joining device to meter send two messages with start time of now. Second message should replace first.	N/A				
INT.HEMP-AHE.G.7	Messaging/HAN Notifications: After joining a device to the meter, verify messages can be received to device from meter ESI.	N/A				
INT.HEMP-AHE.G.8	Messaging/HAN Notifications: After joining device to meter and message having been received by device, issue cancelation and verify message removal.	N/A				
INT.HEMP-AHE.G.9	Messaging/HAN Notifications: After joining device to meter and message having been received by the device, the device is power-cycled for verification that message remaining time is accurate.	N/A				
Integration Test Book – HEMP Interfaces to AHE: Broadband Network Communication						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.HEMP-AHE.G.10	Device Commissioning/Joining: Devices commissioning to meter in meterformed HAN with Gateway. Device registration confirmed in Command Center and Tendril user portal.	N/A				
INT.HEMP-AHE.G.11	Device Commissioning/Joining: After joining devices to HAN, devices are removed from Han and removal is confirmed at device UI, Command center and in Tendril User Portal.	N/A				
INT.HEMP-AHE.G.12	Device Commissioning/Joining: After joining devices to meter, devices are removed with confirmation of removal and rejoined confirmed in Command Center and Tendril user portal.	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.HEMP-AHE.G.13	Device Commissioning/Joining: After joining a device to the HAN, Test the joining of a second device joining by means of communication through the previously joined device.	N/A				
INT.HEMP-AHE.G.14	After joining the HAN a device receives and displays the correct date and time.	N/A				
INT.HEMP-AHE.G.15	Messaging: Text message sent with a start time of now and in the future without request for user acknowledgement, confirming messages are displayed correctly at the proper time with the popper duration, at the correct importance level.	N/A				
INT.HEMP-AHE.G.16	Messaging: Text messages sent with start times of now and in the future with requests for customer acknowledgement, verifying messages display properly, at the proper time for the proper duration, at the proper importance level and user acknowledgments are communicated properly.	N/A				
INT.HEMP-AHE.G.17	Messaging: Text message sent with a start time of now and in the future without request for user acknowledgement and devices powered off at the time of the message being sent but powered on within the message active window, confirming messages are displayed correctly at the proper time with the popper duration, at the correct importance level.	N/A				
INT.HEMP-AHE.G.18	Text messages sent with start times of now and in the future with requests for customer acknowledgement and the devices powered off at the time of message initiation but powered on during the message active window, verifying messages display properly, at the proper time for the proper duration, at the proper importance level and user acknowledgments are communicated.	N/A				
INT.HEMP-AHE.G.19	Load Control: LC events for varying criticality levels imitated for HVAC device class with specified offset, start time and duration verifying correct start and duration and events appearing properly in UI and participation reporting appearing properly in Tendril admin portal.	N/A				
INT.HEMP-AHE.G.20	Load Control: LC event initiated for HVAC and simple misc. LC devices with specified offset, start time and duration verifying correct start and duration and events appearing properly in UI and participation reporting appearing properly in Tendril admin portal.	N/A				
INT.HEMP-AHE.G.21	Load Control: LC event initiated for simple misc. LC devices with start time and duration verifying thermostats do not participate.	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.HEMP-AHE.G.22	Load Control: LC event initiated for HVAC device class with specified offset, start time and duration. Opting out of event from thermostat after start of event verifying opt-out is reported properly and participation is reported properly "partial opt-out".	N/A				
INT.HEMP-AHE.G.23	Load Control: LC event initiated for HVAC device class with specified offset, start time and duration. Opting out of event from thermostat after start of event and back in prior to conclusion of event verifying participation is reported properly "partial opt-in".	N/A				
INT.HEMP-AHE.G.24	Load Control: LC event scheduled and canceled prior to the scheduled start time. Verification that prior to cancellation the event appears properly in the user and admin interfaces for scheduled events and after cancellation the event does not start at the device and appears properly as canceled in the event status.	N/A				
INT.HEMP-AHE.G.25	Load Control: LC event initiated and properly initiated on the device and canceled within the active period and canceled from the Tendril admin portal, verifying the event is terminated properly on the device and displayed properly at the device, user portal and reported properly.	N/A				
INT.HEMP-AHE.G.26	Load Control: Initiate device embedded software/firmware update by means of Over the Air update (OTA) from the Tendril admin portal. Verify successful delivery and installation of OTA image on device.	N/A				
INT.HEMP-AHE.G.27	Load Control: Initiate gateway embedded software/firmware update by means of Over the Internet update (OTI) from the tendril admin interface. Verify the successful delivery and installation of the OTI image on the gateway.	N/A				
Integration Test Book – HEMP Interfaces to AHE: AMI Network Communication						
ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.HEMP-AHE.G.28	Device Commissioning/Joining: Devices commissioning to meter in meterformed HAN without a gateway. Device registration confirmed in Command Center and device find control successfully associates device on AMI network to user's account Tendril connect Database and devices appear on User portal.	N/A				
INT.HEMP-AHE.G.29	Device Commissioning/Joining: After joining devices to HAN, devices are removed from Han and removal is confirmed at device UI, Command center and in the Tendril User portal.	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.HEMP-AHE.G.30	Device Commissioning/Joining: After joining devices to meter, devices are removed with confirmation of removal and rejoined to the HAN. Device leave and re-joining confirmed in Command Center and Tendril user portal.	N/A				
INT.HEMP-AHE.G.31	Device Commissioning/Joining: After joining a device to the HAN, Test the joining of a second device joining by means of communication through the previously joined device.	N/A				
INT.HEMP-AHE.G.32	Device Commissioning/Joining: After Joining the HAN a device receives and displays the correct data and time.	N/A				
INT.HEMP-AHE.G.33	Messaging: Text message sent with a start time of now and in the future without request for user acknowledgement, confirming messages are displayed correctly at the proper time with the popper duration, at the correct importance level.	N/A				
INT.HEMP-AHE.G.34	Messaging: Text messages sent with start times of now and in the future with requests for customer acknowledgement, verifying messages display properly, at the proper time for the proper duration, at the proper importance level and user acknowledgments are communicated properly.	N/A				
INT.HEMP-AHE.G.35	Messaging: Text message sent with a start time of now and in the future without request for user acknowledgement and devices powered off at the time of the message being sent but powered on within the message active window, confirming messages are displayed correctly at the proper time with the popper duration, at the correct importance level.	N/A				
INT.HEMP-AHE.G.36	Messaging: Text messages sent with start times of now and in the future with requests for customer acknowledgement and the devices powered off at the time of message initiation but powered on during the message active window, verifying messages display properly, at the proper time for the proper duration, at the proper importance level and user acknowledgements are communicated properly.	N/A				
INT.HEMP-AHE.G.37	Load Control: LC events for varying criticality levels imitated for HVAC device class with specified offset, start time and duration verifying correct start and duration and events appearing properly in UI and participation reporting appearing properly in Tendril admin portal.	N/A				

ID	Test Description	Expected Result	Status	Actual Result	Test Date	Tested By
INT.HEMP-AHE.G.38	Load Control: LC event initiated for HVAC and simple misc. LC devices with specified offset, start time and duration verifying correct start and duration and events appearing properly in UI and participation reporting appearing properly in Tendril admin portal.	N/A				
INT.HEMP-AHE.G.39	Load Control: LC event initiated for simple misc. LC devices with start time and duration verifying thermostats do not participate.	N/A				
INT.HEMP-AHE.G.40	Load Control: LC event initiated for HVAC device class with specified offset, start time and duration. Opting out of event from thermostat after start of event verifying opt-out is reported properly and participation is reported properly.	N/A				
INT.HEMP-AHE.G.41	Load Control: LC event initiated for HVAC device class with specified offset, start time and duration. Opting out of event from thermostat after start of event and back in prior to conclusion of event verifying participation is reported properly "partial opt-in".	N/A				
INT.HEMP-AHE.G.42	Load Control: LC event scheduled and canceled prior to the scheduled start time. Verification that prior to cancelation the event appears properly in the user and admin interfaces for scheduled events and after cancelation the event does not start at the device and appears properly as canceled in the event status.	N/A				
INT.HEMP-AHE.G.43	Load Control: LC event initiated and properly initiated on the device and canceled within the active period and canceled from the Tendril admin portal, verifying the event is terminated properly on the device and displayed properly at the device, user portal and reported properly.	N/A				

This page intentionally blank.

Appendix J End-to-End Interoperability Testing Documentation

J.1	Remote Connect and Disconnect	J-3
J.2	Demand Response – AMI Thermostat.....	J-25
J.3	Demand Response – HAN Devices	J-35
J.4	Demand Response - Battery	J-48
J.5	1 st Responder Function – Volt Var Control	J-60
J.6	1 st Responder Function – Feeder Load Transfer.....	J-73
J.7	1 st Responder Function – Fault Location, Isolation and Service Restoration	J-82
J.8	Outage and Restoration Events.....	J-97
J.9	Power Status Verification	J-106
J.10	Battery Grid Operation – Local Control (Discharge).....	J-116
J.11	Battery Grid Operation – Fixed kW (Discharge)	J-123
J.12	Battery Grid Operation – Load Following (Discharge).....	J-132

This page intentionally blank.

Remote Connect and Disconnect





Remote Connect and On-Demand Read

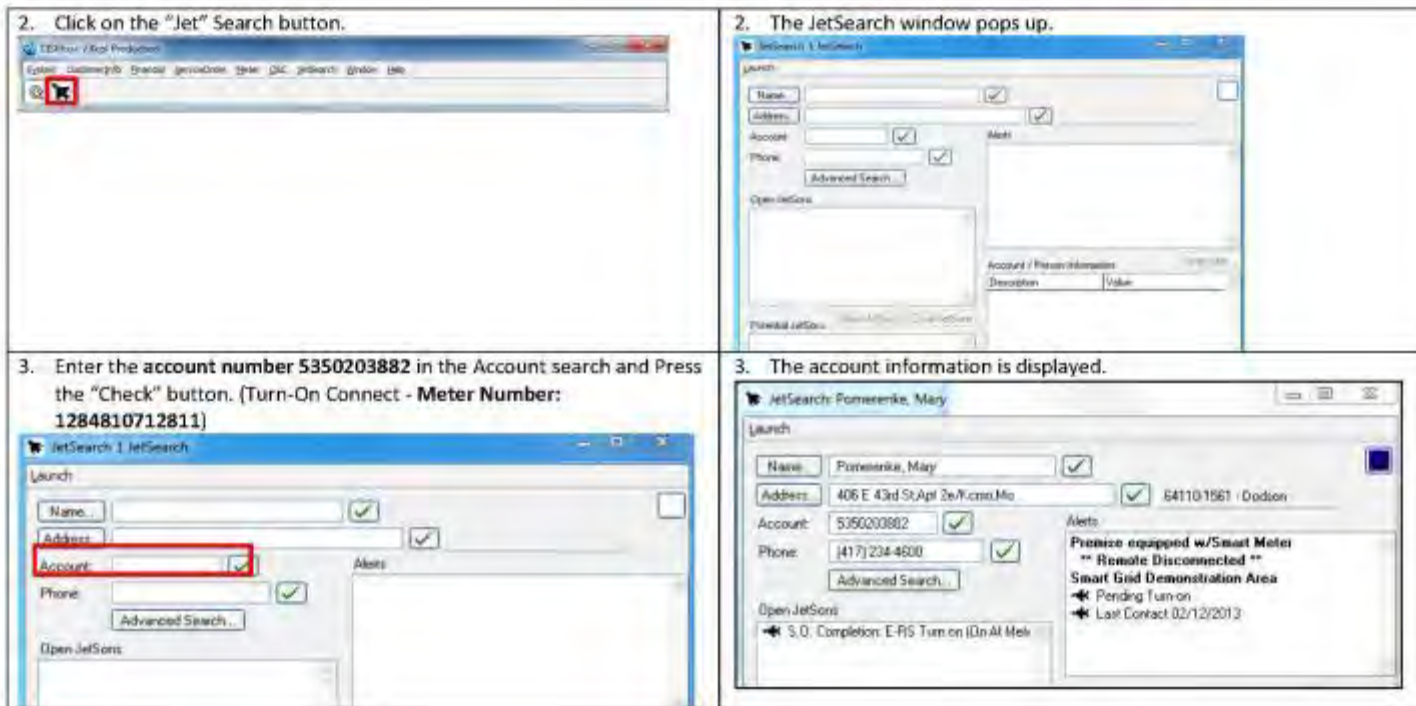
Precondition:

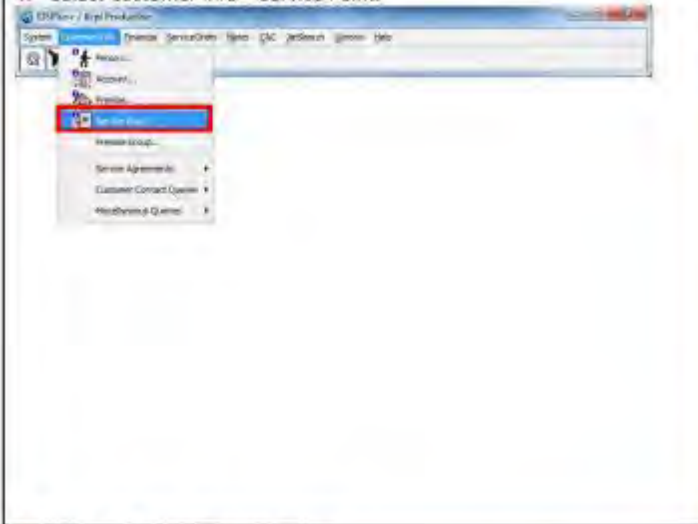


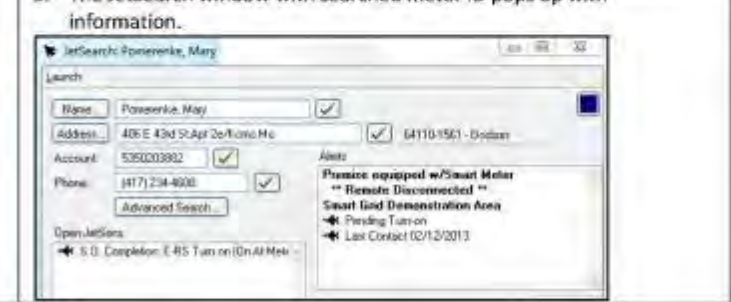
- Prior to entering a turn on order in GUI, make sure to change the Positive ID flag to 'P' in the green screens for each customer. In CIS+, pull up the customer ID on the PER screen (green screen) and panel left once for Positive ID field. Enter a 'C' in the Action field, 'P' in the Positive ID field and press Enter. (This is to verify that customer can open the account and turn on the meter. This has to be done before the meter service request)
- Meter has disconnect switch and Source is connected

Remote Connect Meter Info – Production:

- Meter ID: 1284810439383

<i>Steps</i>	<i>Expected Results</i>
<p>1. Log in to the CIS system.</p> 	<p>1. Successfully logged in to the CIS+ system.</p> 



<p>4. Select Customer Info > Service Point.</p> 	<p>4. A new window "Service Point" pops with detailed information on the entered account number.</p> 
<p>5. Click on the "Jet" Search button.</p> 	<p>5. The JetSearch window with searched meter ID pops up with information.</p> 

<p>6. Click on "Pending Turn-on".</p>	<p>6. A new S. O. Completion window pops up with Service Order "Pending".</p>
<p>7. Wait for the UC4 process to kick off.</p>	<p>7. UC4 process is executed.</p>

8. Select Action > Refresh.

S.D. Completion: E-RS Turn on (On At Meter)			
Action			
Refresh	Alt+R	36527344	Initiated On 02/12/2013 By Ivie, Kelly
Complete	Alt+C	n On	Turn on (On At Meter)
Delete	Alt+D	omplete on 02/14/2013 09:19 by Mdm, System	Fid Order:
Undo	Alt+U	34790610	Conn On E-RS, 1RS1A, 10712811G, ON, PH1
Redo	Alt+R		
Acct/Premise:		5350203882 Pomerleau, May / 406 E 43rd St, Apt 2e/Kamo, Mo	

8. The service order is "acknowledged".

S.D. Maintenance: E-RS Turn on (On At Meter)

Action

Service Order: 36527344 Initiated on 02/12/2013 by Ivie, Kelly

Status: Pending Fid Order: 10712811G, Conn On

Service Point: 5350203882 Conn On E-RS, 1RS1A, 10712811G, ON, PH1 02/08/13

Account Name: 5350203882 Pomerleau, May / 406 E 43rd St, Apt 2e/Kamo, Mo

Order Type: Turn On Date Date: 02/14/2013

Order Subject: Turn on (On At Meter)

Origin: T - Telephone

Deleted By: Empty Service Password:

Dispatch: C - Customer Convenience

Blocked Date:

Comments: on of order: 100246272

Phone Number: (417) 731-4631 Pay at Premise Off to Table

Work Number:

Mailing Address: 406 E 43rd St, St. Louis, Mo 63112-1981

9. Select Action > Refresh.

S.O. Completion: E-RS Turn on (On At Meter)

Action

Refresh Alt+R

96527344 Initiated On 02/12/2013 By Ivie, Kelly

Complete Alt+C n On Turn on (On At Meter)

Cancel Alt+D n On Turn on (On At Meter)

Unblock Alt+U n On Turn on (On At Meter)

Void Alt+V 24790610 Conn On E-RS, 1RS1A, 10712811G, ON, PH1

Acct/Premise: 5350203882 Pomerence, May / 406 E 43rd St Apt 2e/Kcmo,Mo

9. Meter Turn-On Order has been completed with On Demand Meter Read.

S.O. Completion: E-RS Turn on (On At Meter)

Control Order: 360527344 Initiated On 02/12/2013 By Ivie, Kelly

Order Type: Turn On Item on (On At Meter)

Status: Complete on 02/14/2013 09:19 by Mdm, System No Order **1105015258 Complete**

Service Point: 90628600 Conn On E-RS, 1RS1A, 10712811G, ON, PH1

Acct/Premise: 5350203882 Pomerence, May / 406 E 43rd St Apt 2e/Kcmo,Mo

Task Date: 02/14/2013 09:19 Location: CH - Des Moines, IA

Priority Sequence: 02/14/2013 09:19 Task Order: 1105015258

Task Type: 1071-2010 Work: 1

Comments:

Meta:

AM ID: 10712811 ✓ Link: 02000-8/2010

AM ID	Reading	MC Details	Last Read Date/Type	Last Reading
1105015258	1105015258	Power Services, 1071		

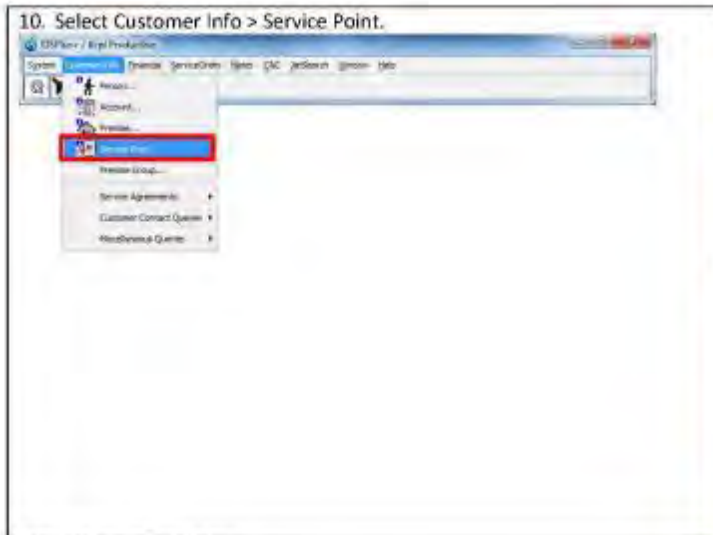
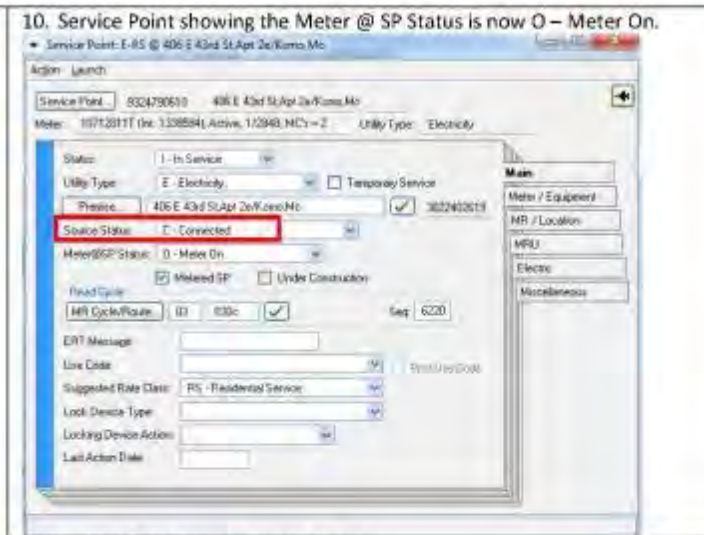


Reading: 1105015258 Power Reading

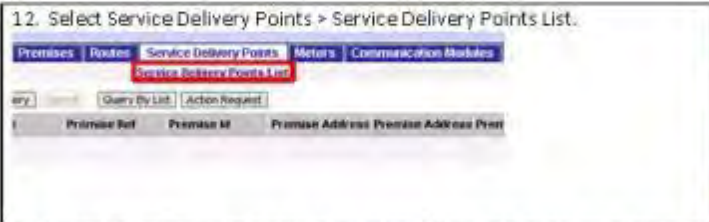

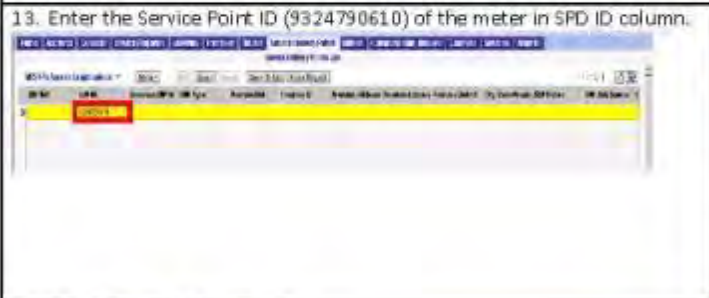
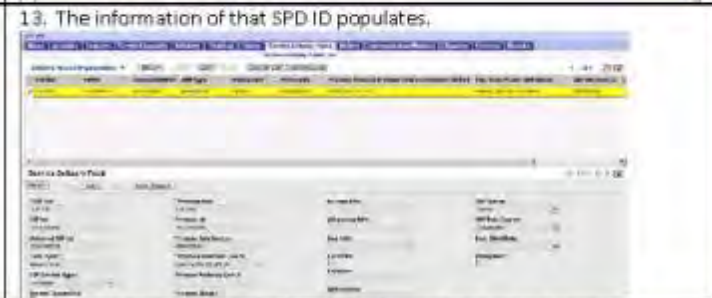

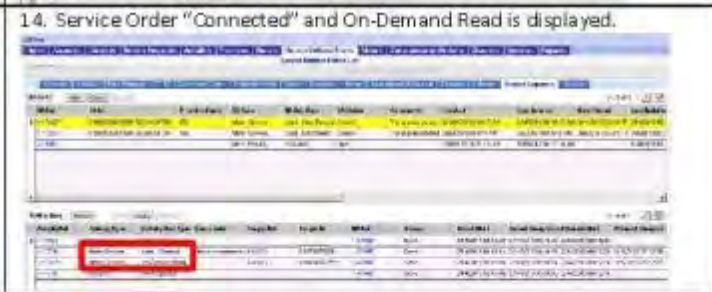
Last Reading Type: Lock Down - Jobs

Last Order Date:

Read Window: Read Code:

USG #0: 02/14/2013 1

<p>10. Select Customer Info > Service Point.</p> 	<p>10. Service Point showing the Meter @ SP Status is now O – Meter On.</p> 
<p>11. Log in to the MDM.</p> 	<p>11. Successfully logged in to the MDM.</p> 

<p>12. Select Service Delivery Points > Service Delivery Points List.</p> 	<p>12. A page opens to search for meter Service Point IDs.</p> 
<p>13. Enter the Service Point ID (9324790610) of the meter in SPD ID column.</p> 	<p>13. The information of that SPD ID populates.</p> 
<p>14. Select Service Requests tab.</p> 	<p>14. Service Order "Connected" and On-Demand Read is displayed.</p> 

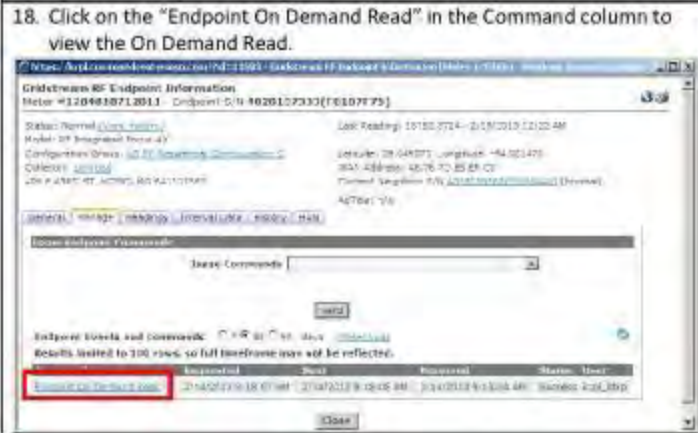
15. Log in to the AHE Command Center.



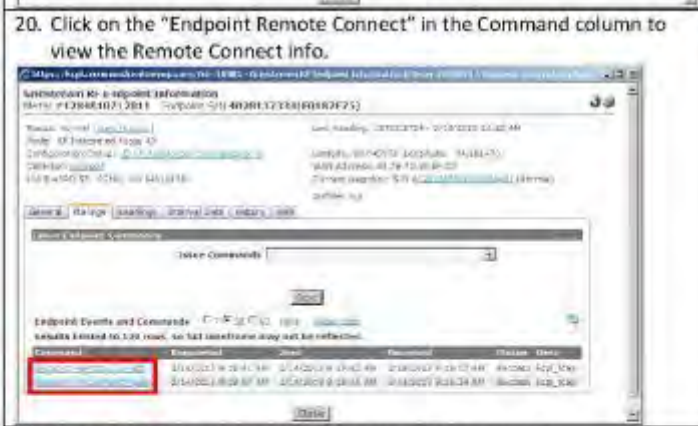
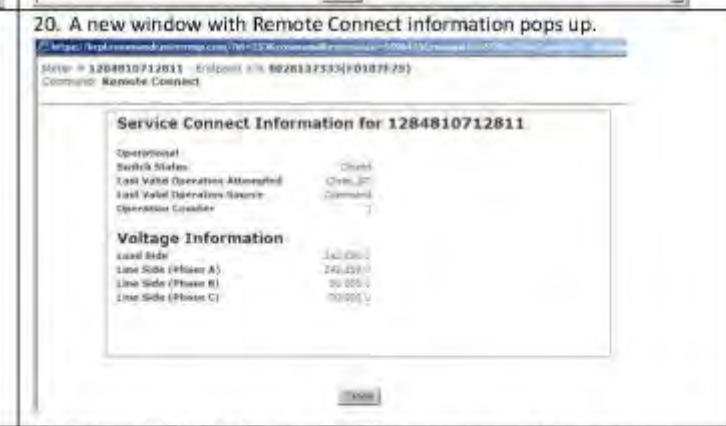
15. Successfully logged in to the AHE Command Center.

16. Enter Meter ID (1284810712811) in the search box and press Search.

16. A new window with the meter information is displayed.

Gridstream RF Endpoint Information																																																																																																																				
Meter #1284810712811 Endpoint S/N 4028137333(F0187F75)																																																																																																																				
Status: Normal	View History	Last Reading: 10899.6200 - 2/18/2013 12:17 AM																																																																																																																		
Model: RF Integrated Focus 4X																																																																																																																				
Configuration Group: US ST SmartGrid_Cof/SmartGrid		Latitude: 38.649575 Longitude: -84.824470																																																																																																																		
Collector: L1284810712811		WiFi Address: 68.76.70.63.6F.C0																																																																																																																		
400 E 43RD ST, KCMO, MO 641110195L		Current Neighbor: S/N 422023843110000000 (Normal)																																																																																																																		
		RgTitle: n/a																																																																																																																		
<table border="1"> <thead> <tr> <th>General</th> <th>Usage</th> <th>Readings</th> <th>Interval Data</th> <th>History</th> <th>Tags</th> </tr> </thead> <tbody> <tr> <td>North State</td> <td>Commodity</td> <td>Multipplier</td> <td colspan="3"></td> </tr> <tr> <td>Demand Multiplier: 1</td> <td></td> <td>Meter Dial Digits / kWh</td> <td colspan="3">5 / 7.2</td> </tr> <tr> <td>Initial/Latest kWh: 0 / 10899.6200</td> <td></td> <td>Module Firmware Version</td> <td colspan="3">051107-03.09</td> </tr> <tr> <td>Meter Firmware Version: 5.33</td> <td></td> <td>ZigBee Firmware Version</td> <td colspan="3">068204-01.07.03</td> </tr> <tr> <td>DCW Version: 1401.01.00</td> <td></td> <td>Tickle %</td> <td colspan="3">20</td> </tr> <tr> <td>Number of Neighbors: 02</td> <td></td> <td>Initial Programming</td> <td colspan="3">10/18/2010 6:01 AM [View Log]</td> </tr> <tr> <td>Last Programming: 1/21/2013 12:00 AM</td> <td></td> <td>Last Good Packet</td> <td colspan="3">2/14/2013 12:17:42 AM</td> </tr> <tr> <td>Firmware Version: 018</td> <td></td> <td>Firmware Download Status</td> <td colspan="3">Success</td> </tr> <tr> <td>Will Be Activated On:</td> <td></td> <td>Next Expected Reset Date</td> <td colspan="3">3/8/2013 11:00:00 AM</td> </tr> <tr> <td>Grid Location</td> <td></td> <td>Custom #1</td> <td colspan="3"></td> </tr> <tr> <td>Pole Number</td> <td></td> <td>Custom #2</td> <td colspan="3"></td> </tr> <tr> <td>Meter Position: 09</td> <td></td> <td>Map Location</td> <td colspan="3"></td> </tr> <tr> <td>Customer ID</td> <td></td> <td>Billing Cycle</td> <td colspan="3">03</td> </tr> <tr> <td>Account Number</td> <td></td> <td>Revenue Class</td> <td colspan="3">10010</td> </tr> <tr> <td>Service Location</td> <td></td> <td></td> <td colspan="3"></td> </tr> <tr> <td>CIS Data</td> <td></td> <td>Billing Address</td> <td colspan="3"></td> </tr> <tr> <td></td> <td>POHESINVE, HXRY</td> <td></td> <td colspan="3"></td> </tr> <tr> <td></td> <td>641702349900</td> <td></td> <td colspan="3"></td> </tr> </tbody> </table>			General	Usage	Readings	Interval Data	History	Tags	North State	Commodity	Multipplier				Demand Multiplier: 1		Meter Dial Digits / kWh	5 / 7.2			Initial/Latest kWh: 0 / 10899.6200		Module Firmware Version	051107-03.09			Meter Firmware Version: 5.33		ZigBee Firmware Version	068204-01.07.03			DCW Version: 1401.01.00		Tickle %	20			Number of Neighbors: 02		Initial Programming	10/18/2010 6:01 AM [View Log]			Last Programming: 1/21/2013 12:00 AM		Last Good Packet	2/14/2013 12:17:42 AM			Firmware Version: 018		Firmware Download Status	Success			Will Be Activated On:		Next Expected Reset Date	3/8/2013 11:00:00 AM			Grid Location		Custom #1				Pole Number		Custom #2				Meter Position: 09		Map Location				Customer ID		Billing Cycle	03			Account Number		Revenue Class	10010			Service Location						CIS Data		Billing Address					POHESINVE, HXRY						641702349900				
General	Usage	Readings	Interval Data	History	Tags																																																																																																															
North State	Commodity	Multipplier																																																																																																																		
Demand Multiplier: 1		Meter Dial Digits / kWh	5 / 7.2																																																																																																																	
Initial/Latest kWh: 0 / 10899.6200		Module Firmware Version	051107-03.09																																																																																																																	
Meter Firmware Version: 5.33		ZigBee Firmware Version	068204-01.07.03																																																																																																																	
DCW Version: 1401.01.00		Tickle %	20																																																																																																																	
Number of Neighbors: 02		Initial Programming	10/18/2010 6:01 AM [View Log]																																																																																																																	
Last Programming: 1/21/2013 12:00 AM		Last Good Packet	2/14/2013 12:17:42 AM																																																																																																																	
Firmware Version: 018		Firmware Download Status	Success																																																																																																																	
Will Be Activated On:		Next Expected Reset Date	3/8/2013 11:00:00 AM																																																																																																																	
Grid Location		Custom #1																																																																																																																		
Pole Number		Custom #2																																																																																																																		
Meter Position: 09		Map Location																																																																																																																		
Customer ID		Billing Cycle	03																																																																																																																	
Account Number		Revenue Class	10010																																																																																																																	
Service Location																																																																																																																				
CIS Data		Billing Address																																																																																																																		
	POHESINVE, HXRY																																																																																																																			
	641702349900																																																																																																																			



<p>19. Press the "Refresh" Button.</p> 	<p>19. "Endpoint Remote Connect" command is displayed in the message log.</p> 
<p>20. Click on the "Endpoint Remote Connect" in the Command column to view the Remote Connect info.</p> 	<p>20. A new window with Remote Connect information pops up.</p> 
<p>21. Check ESB/back end for the verification of the messages. Database: CMB2DEVC. Check Source and Target column in the table "KCPL_ESB_AUDIT".</p>	<p>21. Column REQ_RSP_IND to verify if the message sent is a request or response (REQ or RSP) checked.</p>

Remote Disconnect and On-Demand Read (Demo)

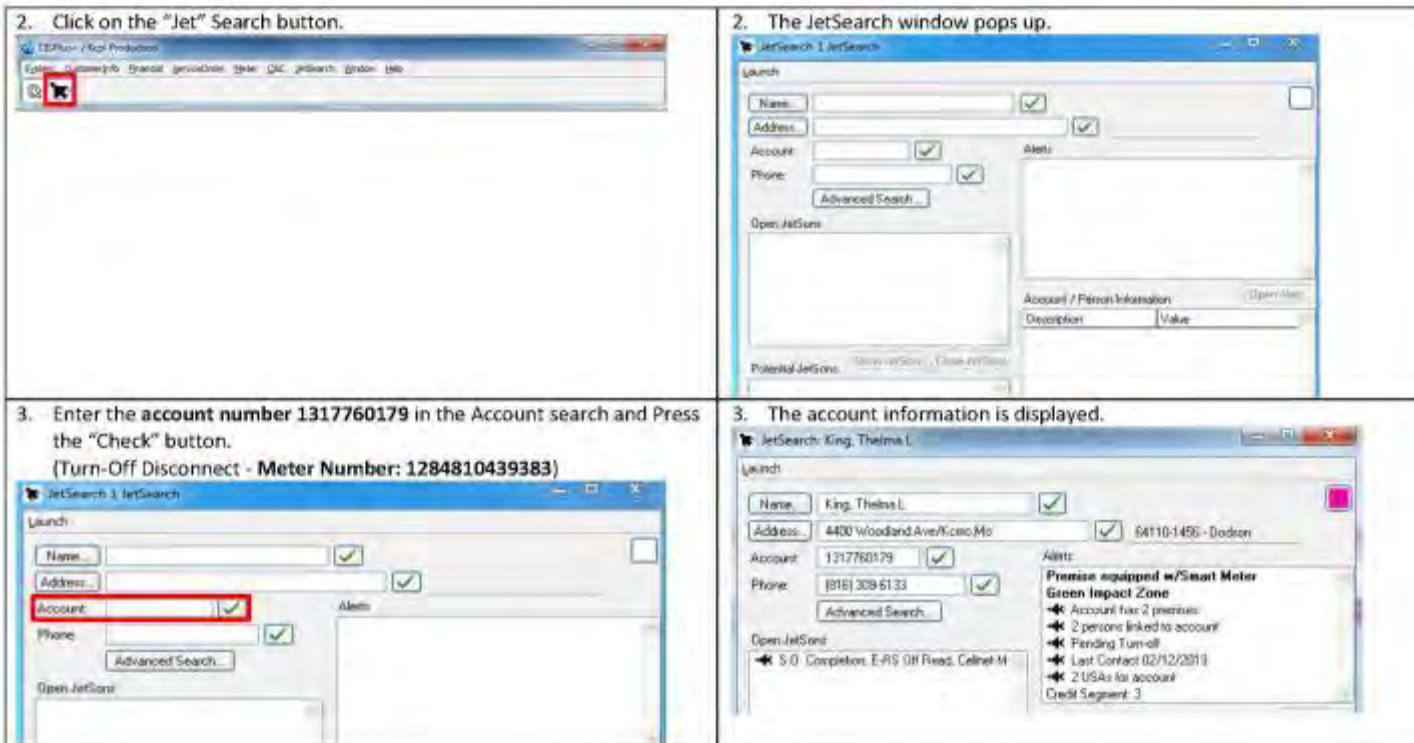
Precondition:

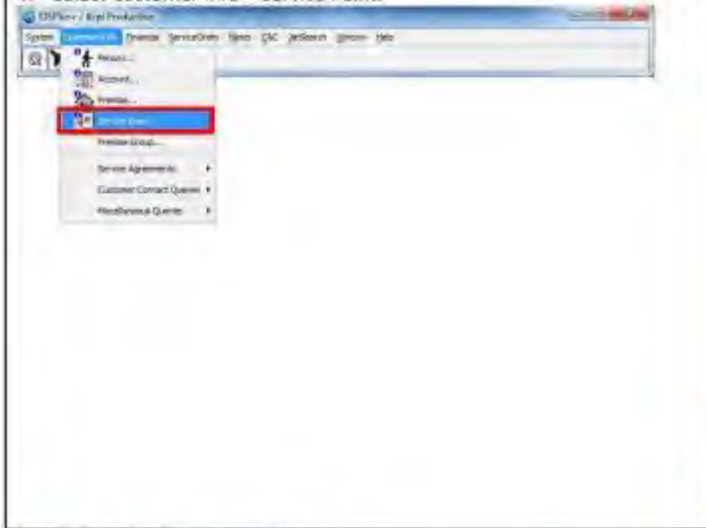
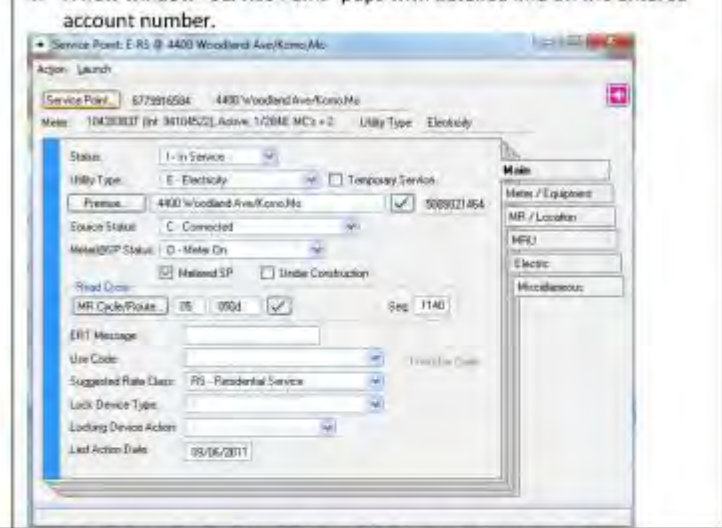

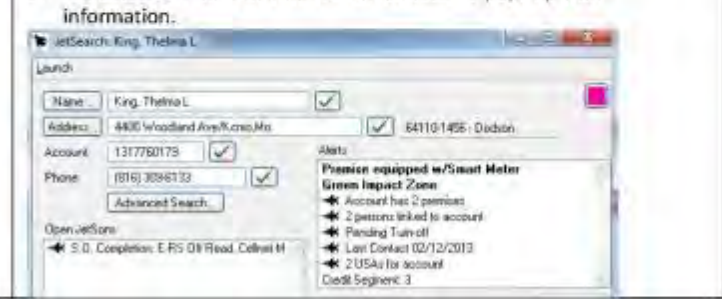
- Assume each scenario does not have a pending turn on, pending turn off, LL revert, current resident at the premise, life support, sensitive load, etc. unless it is noted.
- Meter has disconnect switch and Source is connected
- Meter at SP status = "On"

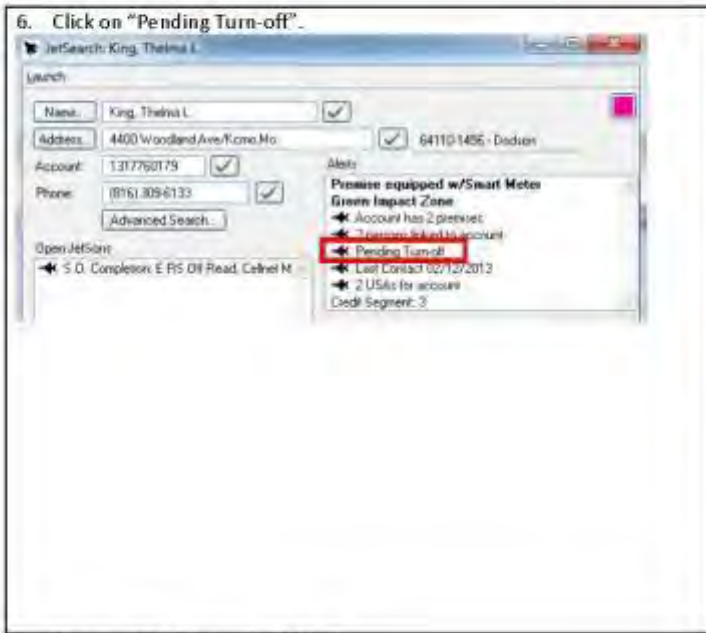
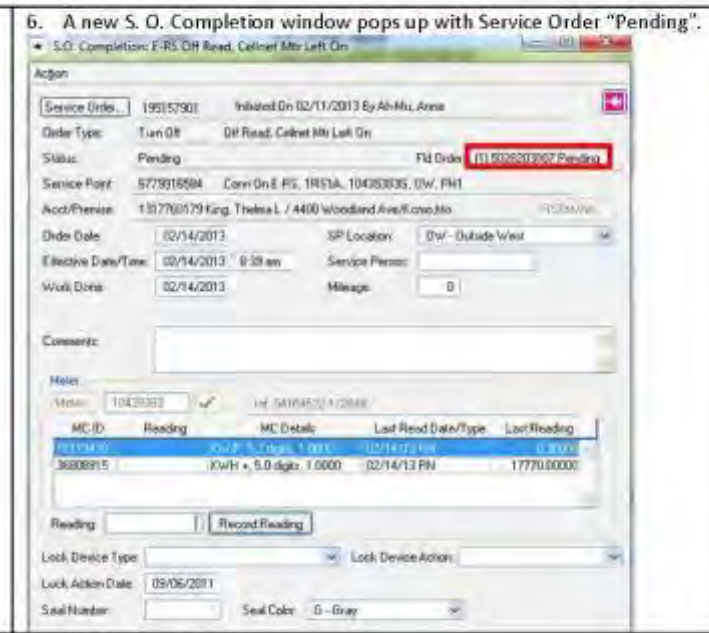
Remote Disconnect Meter Info – Production:

- Meter ID: 1284810439383
- Service Point ID: 6779916584
- Account Number: 1317760179

<i>Steps</i>	<i>Expected Results</i>
<p>1. Log in to the CIS+ system.</p> 	<p>1. Successfully logged in to the CIS+ system.</p> 



<p>4. Select Customer Info > Service Point.</p> 	<p>4. A new window "Service Point" pops with detailed info on the entered account number.</p> 
<p>5. Click on the "Jet" Search button.</p> 	<p>5. The JetSearch window with searched meter ID pops up with information.</p> 

<p>6. Click on "Pending Turn-off".</p> 	<p>6. A new S. O. Completion window pops up with Service Order "Pending".</p> 
<p>7. Wait for UC4 Process to kick off.</p>	<p>7. UC4 Process is executed.</p>

8. Select Action > Refresh.

S.O. Completion: E-R5 Off Read, Cellnet Mtr Left On			
Action			
Refresh Alt+R	5157901	Initiated On 02/11/2013	By Ah-Mu, Anne
Complete Alt+C	n Off	Off Read, Cellnet Mtr Left On	
Delete Alt+D	omplete on 02/14/2013 09:18	by Mdm, System	Fld Ord
Use/Mod Alt+U	79916584	Conn Offs E-R5, 1RS1A, 10439383G, DW, F	
View Alt+V	1317760179	King, Thelma L / 4400 Woodland Ave/Kcmo, Mo	

8. The service order is "acknowledged".

Service Order: 5157901 Initiated on 02/11/2013 by Ah-Mu, Anne

Status: Pending Fld Ord: 1317760179 Acknowledged

Service Order: 67759 1364 Conn Off E-R5, 1RS1A, 10439383G, DW, F

Account: 1317760179 King, Thelma L / 4400 Woodland Ave/Kcmo, Mo

Order Type: Service Order

Order Subtype: Off Read, Cellnet Mtr Left On

Origin: Telephone

Priority: Normal

Category: Emergency

Check Out: Blocked Date:

Location: 1317760179

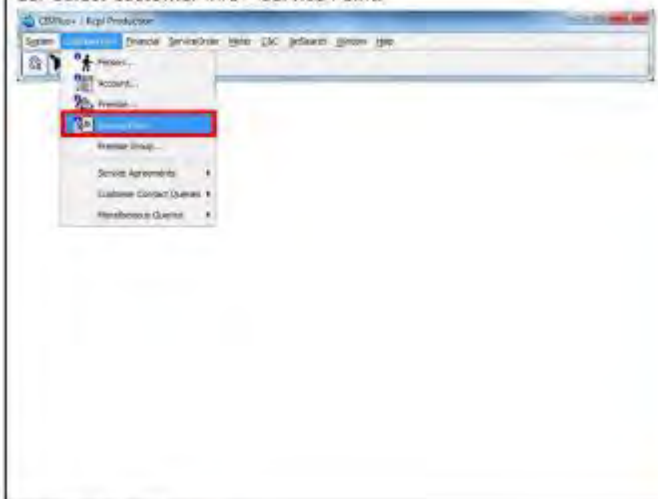
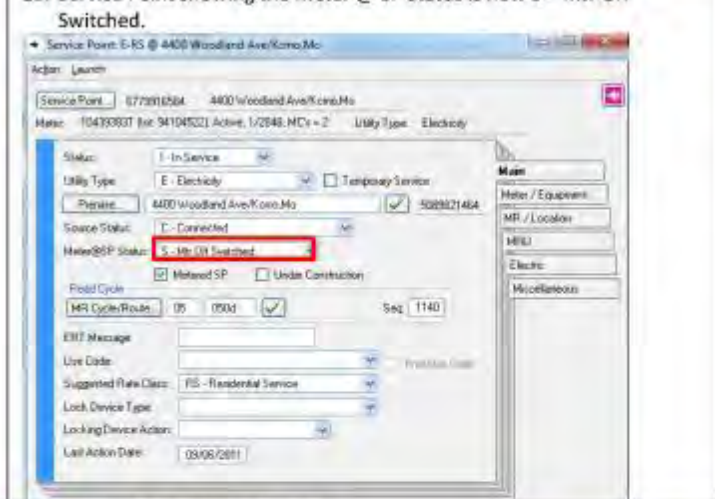


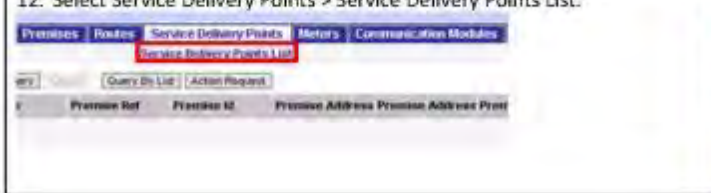

Address: 4011 Maryland Avenue, St. Louis, MO 63108


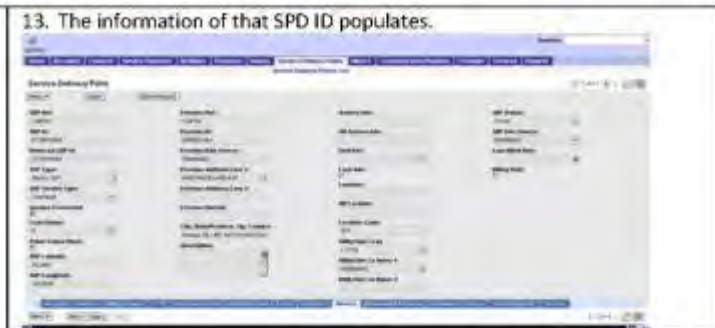

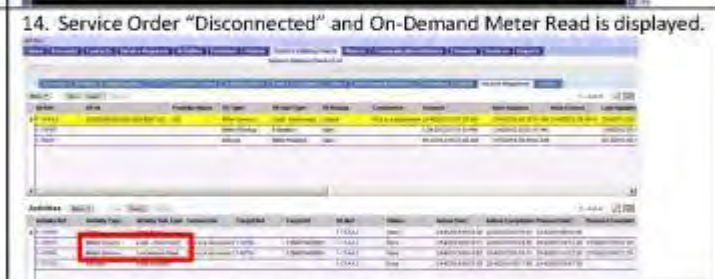


9. Select Action > Refresh.

Action	Account	Initiated On	By
Refresh Alt+R	5157901	02/11/2013	Ah-Mu, Anne
Complete Alt+C	n Off	Off Read, Cellnet Mtr Left On	
Delete Alt+D	Complete on 02/14/2013 09:18	by Mdm, System	Fld Ord
Unblock Alt+U	79916584	Conn Offs E-RS, 1RS1A, 10439383G, DW, F	
View Alt+V	1317760179	King, Thelma L / 4400 Woodland Ave/Kcmo, Mo	

9. Meter Turn-Off Order has been completed with On Demand Meter Reading.

Account: 5157901
 Meter ID: 36803815
 Meter Type: 179E-0032C-RS-4-5.3 cpm.1.3000

<p>10. Select Customer Info > Service Point.</p> 	<p>10. Service Point showing the Meter @ SP Status is now S – Mtr Off Switched.</p> 				
<p>11. Log in to MDM.</p> 	<p>11. Successfully logged in to MDM.</p> 				
<p>12. Select Service Delivery Points > Service Delivery Points List.</p>  <table border="1"> <thead> <tr> <th>Prmsrv Ref</th> <th>Prmsrv ID</th> <th>Prmsrv Address</th> <th>Prmsrv Address Print</th> </tr> </thead> </table>	Prmsrv Ref	Prmsrv ID	Prmsrv Address	Prmsrv Address Print	<p>12. A new page opens to search for meter Service Point IDs.</p> 
Prmsrv Ref	Prmsrv ID	Prmsrv Address	Prmsrv Address Print		

<p>13. Enter the Service Point ID (6779916584) of the meter in SPD ID column.</p> 	<p>13. The information of that SPD ID populates.</p> 
<p>14. Select Service Requests tab.</p> 	<p>14. Service Order "Disconnected" and On-Demand Meter Read is displayed.</p> 
<p>15. Log in to the AHE Command Center.</p> 	<p>15. Successfully logged in to the AHE Command Center.</p> 

16. Enter the Meter ID (1284810439383) in the search box and press Search.



16. A new window with the meter information is displayed.




17. Select the "Manage" tab.



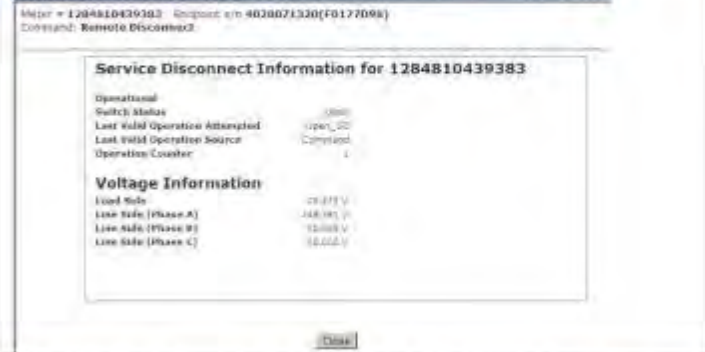
17. "Endpoint Remote Disconnect" command is displayed in the log.



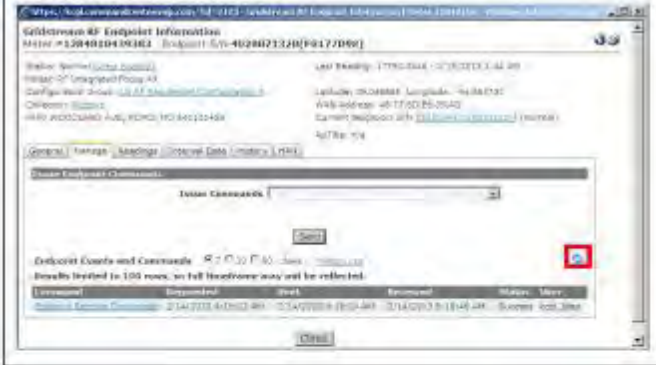
18. Click on the "Endpoint Remote Disconnect" from the Command column to view the Remote Disconnect Info.




18. A new window with Remote Disconnect Information pops up.





19. Press the "Refresh" button.

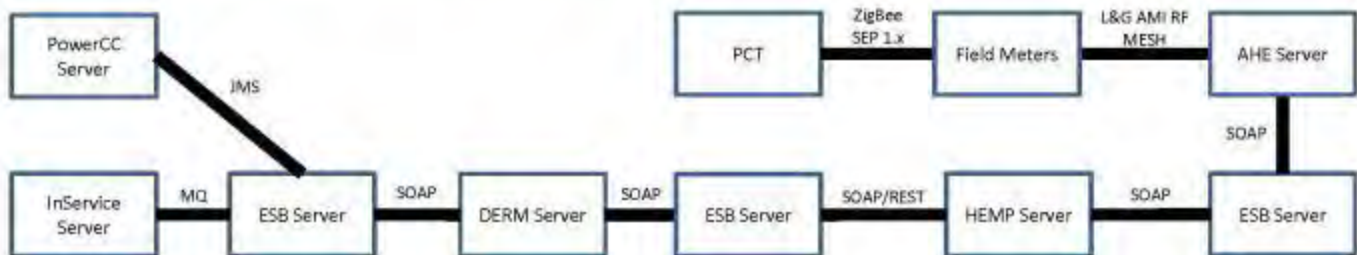


19. "Endpoint On Demand Read" command is displayed in the log.






<p>20. Click on the "Endpoint On Demand Read" from the Command column to view the On Demand Read.</p> 	<p>20. A new window with On Demand Read information pops up.</p>  <table border="1"> <thead> <tr> <th>Name</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Request</td> <td>127512775</td> </tr> <tr> <td>Request On Demand Read Info Data Field Configuration</td> <td>0</td> </tr> <tr> <td>Request ID</td> <td>7</td> </tr> <tr> <td>Req ID</td> <td>127512775</td> </tr> <tr> <td>Completion Time</td> <td>0 seconds</td> </tr> <tr> <td>Completion Time</td> <td>0 seconds</td> </tr> <tr> <td>Total Time</td> <td>11.300000</td> </tr> <tr> <td>Completion Time</td> <td>0</td> </tr> <tr> <td>Completion Time</td> <td>0</td> </tr> <tr> <td>Total Time</td> <td>0</td> </tr> </tbody> </table>	Name	Value	Request	127512775	Request On Demand Read Info Data Field Configuration	0	Request ID	7	Req ID	127512775	Completion Time	0 seconds	Completion Time	0 seconds	Total Time	11.300000	Completion Time	0	Completion Time	0	Total Time	0
Name	Value																						
Request	127512775																						
Request On Demand Read Info Data Field Configuration	0																						
Request ID	7																						
Req ID	127512775																						
Completion Time	0 seconds																						
Completion Time	0 seconds																						
Total Time	11.300000																						
Completion Time	0																						
Completion Time	0																						
Total Time	0																						
<p>21. Check ESB/back end for the verification of the messages. Database: CMB2DEVC Check Source and Target column in the table "KCPL_ESB_AUDIT".</p>	<p>21. Column REQ_RSP_IND to verify if the message sent is a request or response (REQ or RSP) checked.</p>																						

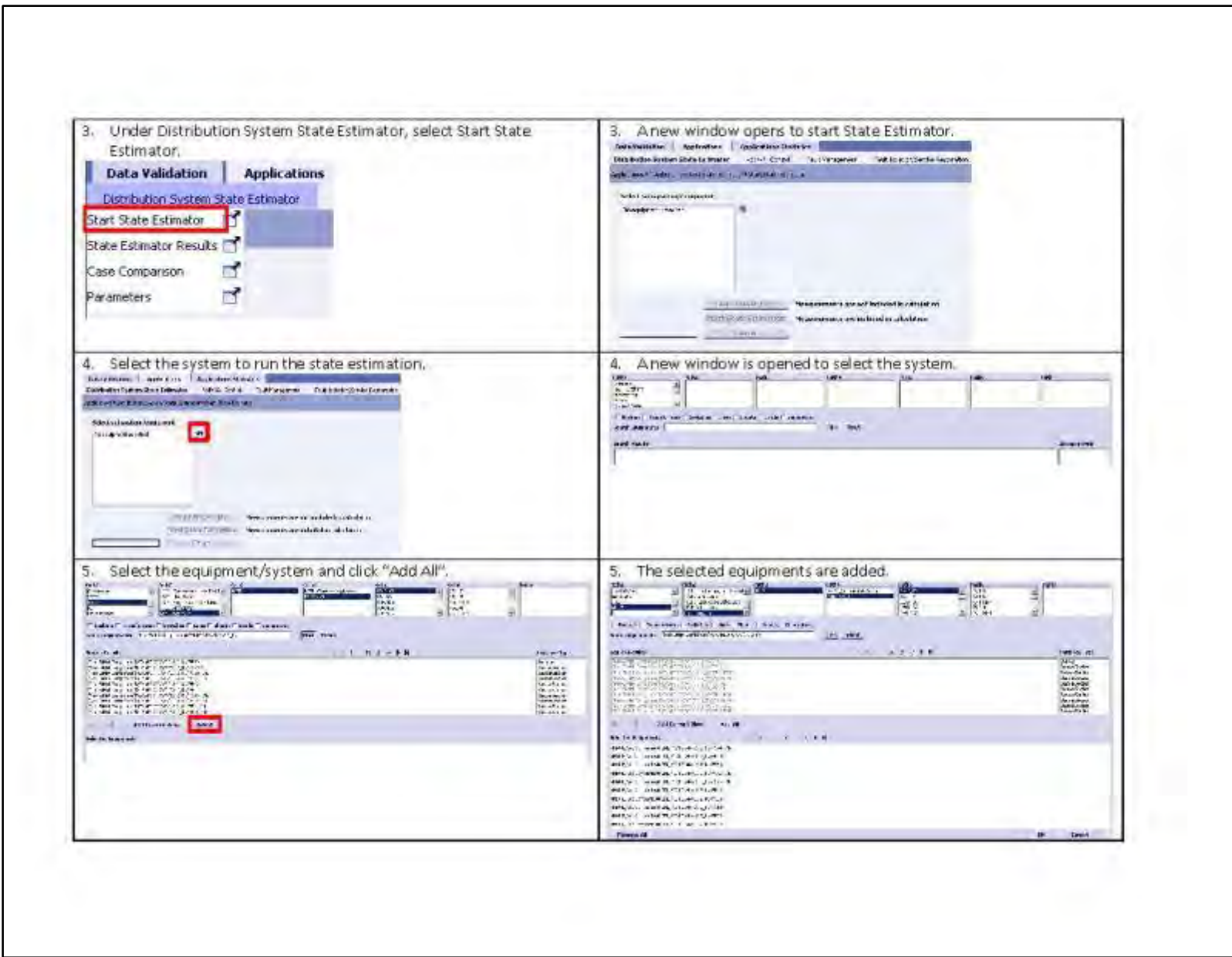
Demand Response – AMI Thermostat







Scheduled Demand Response: AMI Thermostat Operation

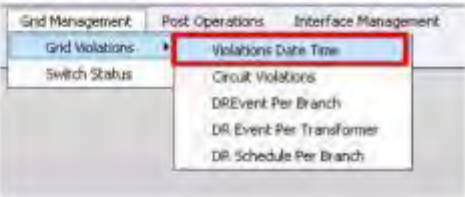
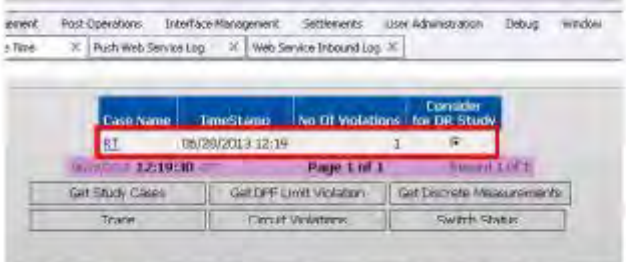
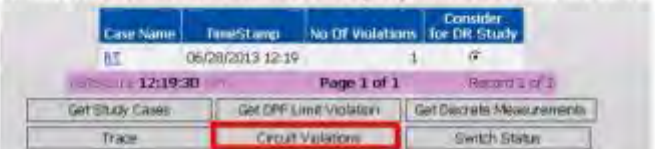





Pre-Condition: An overload is occurred in a feeder.

<p>1. Log in to PowerCC/DMS.</p> 	<p>1. Successfully logged in to PowerCC/DMS.</p> 
<p>2. Select Applications.</p> 	<p>2. WebUI displays the distribution network applications.</p> 





<p>8. Verify in the DMS server log that the message has been sent to DERM. Go to Network > DMS01 > powercc > temp > DERM. And select OUT_RT_MsgCreatedDistributionPowerFlowLimitViolations51.xml with the latest time stamp.</p> 	<p>8. The log file is opened that verified that violations have been sent to DERM.</p> 
<p>9. Log in to the DERM webUI.</p> 	<p>9. Successful log in to DERM webUI.</p> 

<p>10. Under Grid Management, select Grid Violations and then Violations Date Time.</p> 	<p>10. A new window/tab with violations is opened.</p>  <table border="1"> <thead> <tr> <th>Case Name</th> <th>TimeStamp</th> <th>No Of Violations</th> <th>Consider for DR Study</th> </tr> </thead> <tbody> <tr> <td>RT</td> <td>05/28/2013 12:19</td> <td>1</td> <td>Y</td> </tr> </tbody> </table>	Case Name	TimeStamp	No Of Violations	Consider for DR Study	RT	05/28/2013 12:19	1	Y												
Case Name	TimeStamp	No Of Violations	Consider for DR Study																		
RT	05/28/2013 12:19	1	Y																		
<p>11. Press "Circuit Violations" button to query the violations from DMS.</p> 	<p>11. A new tab "Circuit Violations" open with details of violations.</p> 																				
<p>12. Since there is only 1 overload, click "Grid Aggregation".</p> 	<p>12. A new tab "Required\Available DR" opens with required and available DR.</p> 																				
<p>13. Click on "DR Event per Branch".</p> 	<p>13. A new tab "DR Event Per Branch" opens with information.</p>  <table border="1"> <thead> <tr> <th rowspan="2">Equipment Name</th> <th colspan="3">Scheduled LK</th> <th colspan="3">Requested LK</th> </tr> <tr> <th>A [kW]</th> <th>B [kW]</th> <th>F [kW]</th> <th>A [kW]</th> <th>B [kW]</th> <th>F [kW]</th> </tr> </thead> <tbody> <tr> <td>1051021</td> <td>.00</td> <td>.00</td> <td>26.40</td> <td>26.40</td> <td>.00</td> <td>.00</td> </tr> </tbody> </table>	Equipment Name	Scheduled LK			Requested LK			A [kW]	B [kW]	F [kW]	A [kW]	B [kW]	F [kW]	1051021	.00	.00	26.40	26.40	.00	.00
Equipment Name	Scheduled LK			Requested LK																	
	A [kW]	B [kW]	F [kW]	A [kW]	B [kW]	F [kW]															
1051021	.00	.00	26.40	26.40	.00	.00															

14. Click on "DR Event per Transformer".

Equipment Name	Scheduled DR				Requested DR			
	A [kW]	B [kW]	C [kW]	ABC [kW]	A [kW]	B [kW]	C [kW]	ABC [kW]
1061021	.00	.00	26.40	26.40	.00	.00	26.40	26.40

Page 1 of 1 Record 1 of 1

DR Event per Transformer

14. A new tab "DR Event Per Transformer" opens with DR that will be scheduled from each transformer.

Transformer	DR_A [kW]	DR_B [kW]	DR_C [kW]	Total kW
1079322	.00	.00	10.20	10.20
1079323	.00	.00	10.20	10.20
1322676	.00	.00	6.00	6.00
Total	.00	.00	26.40	26.40

Schedule DR Controls | Delete DR Controls | Get DPF Solution

15. Click on "Schedule DR Controls".

Transformer	DR_A [kW]	DR_B [kW]	DR_C [kW]	Total kW
1079322	.00	.00	10.20	10.20
1079323	.00	.00	10.20	10.20
1322676	.00	.00	6.00	6.00
Total	.00	.00	26.40	26.40

Schedule DR Controls | Delete DR Controls | Get DPF Solution

Save for validation | Validate DR Event

15. A schedule DR controls opens and pops up a window to enter schedule information.

Enter Schedule Information

Schedule Name: [transformer_1079322_1079323_1322676]

Schedule Date: 06/28/2013

Start Time: 7:00

End Time: 8:00



Cancel | OK

16. Enter the schedule information and press "create".

16. A new page opens that shows the DR events that were committed as a result of the overload. (notification was sent to the HEMP at 12:21, and the event was scheduled from 12:26 through 1:00).

17. Go to Interface Management > Web Services > Push Web Services > Push Web Service Log.

17. This verifies DR message has been sent to HEMP.

<p>18. Log in to KCP&L portal (HEMP) to verify the devices are off. (DR event is process).</p>	<p>18. The devices connected to the meter ID 1284810711063 are "In Progress".</p>  <p>The screenshot shows the 'Your Account' page with an 'Events' table. The first row is highlighted in yellow and shows a 'Load Control' event for meter ID 1284810711063, starting on 1/23/13 at 10:00 AM and ending at 11:00 AM. The status is 'In Progress'.</p> <table border="1"> <thead> <tr> <th>Event Type</th> <th>Start</th> <th>End</th> <th>Location</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>Load Control</td> <td>1/23/13 10:00 AM</td> <td>1/23/13 11:00 AM</td> <td>1284810711063</td> <td>In Progress</td> </tr> <tr> <td>Load Control</td> <td>1/23/13 10:00 AM</td> <td>1/23/13 11:00 AM</td> <td>1284810711063</td> <td>Completed</td> </tr> <tr> <td>Load Control</td> <td>1/23/13 10:00 AM</td> <td>1/23/13 11:00 AM</td> <td>1284810711063</td> <td>Completed</td> </tr> <tr> <td>Load Control</td> <td>1/23/13 10:00 AM</td> <td>1/23/13 11:00 AM</td> <td>1284810711063</td> <td>Completed</td> </tr> <tr> <td>Load Control</td> <td>1/23/13 10:00 AM</td> <td>1/23/13 11:00 AM</td> <td>1284810711063</td> <td>Completed</td> </tr> </tbody> </table>	Event Type	Start	End	Location	Status	Load Control	1/23/13 10:00 AM	1/23/13 11:00 AM	1284810711063	In Progress	Load Control	1/23/13 10:00 AM	1/23/13 11:00 AM	1284810711063	Completed	Load Control	1/23/13 10:00 AM	1/23/13 11:00 AM	1284810711063	Completed	Load Control	1/23/13 10:00 AM	1/23/13 11:00 AM	1284810711063	Completed	Load Control	1/23/13 10:00 AM	1/23/13 11:00 AM	1284810711063	Completed
Event Type	Start	End	Location	Status																											
Load Control	1/23/13 10:00 AM	1/23/13 11:00 AM	1284810711063	In Progress																											
Load Control	1/23/13 10:00 AM	1/23/13 11:00 AM	1284810711063	Completed																											
Load Control	1/23/13 10:00 AM	1/23/13 11:00 AM	1284810711063	Completed																											
Load Control	1/23/13 10:00 AM	1/23/13 11:00 AM	1284810711063	Completed																											
Load Control	1/23/13 10:00 AM	1/23/13 11:00 AM	1284810711063	Completed																											
<p>19. Check the portal for the DR event completion. (After – event)</p>	<p>19. The devices connected to the meter ID 1284810711063 are "Completed".</p>  <p>The screenshot shows the 'Your Account' page with an 'Events' table. The first row shows a 'Load Control' event for meter ID 1284810711063, starting on 1/23/13 at 10:00 AM and ending at 11:00 AM. The status is 'Completed'.</p> <table border="1"> <thead> <tr> <th>Event Type</th> <th>Start</th> <th>End</th> <th>Location</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>Load Control</td> <td>1/23/13 10:00 AM</td> <td>1/23/13 11:00 AM</td> <td>1284810711063</td> <td>Completed</td> </tr> <tr> <td>Load Control</td> <td>1/23/13 10:00 AM</td> <td>1/23/13 11:00 AM</td> <td>1284810711063</td> <td>Completed</td> </tr> <tr> <td>Load Control</td> <td>1/23/13 10:00 AM</td> <td>1/23/13 11:00 AM</td> <td>1284810711063</td> <td>Completed</td> </tr> <tr> <td>Load Control</td> <td>1/23/13 10:00 AM</td> <td>1/23/13 11:00 AM</td> <td>1284810711063</td> <td>Completed</td> </tr> <tr> <td>Load Control</td> <td>1/23/13 10:00 AM</td> <td>1/23/13 11:00 AM</td> <td>1284810711063</td> <td>Completed</td> </tr> </tbody> </table>	Event Type	Start	End	Location	Status	Load Control	1/23/13 10:00 AM	1/23/13 11:00 AM	1284810711063	Completed	Load Control	1/23/13 10:00 AM	1/23/13 11:00 AM	1284810711063	Completed	Load Control	1/23/13 10:00 AM	1/23/13 11:00 AM	1284810711063	Completed	Load Control	1/23/13 10:00 AM	1/23/13 11:00 AM	1284810711063	Completed	Load Control	1/23/13 10:00 AM	1/23/13 11:00 AM	1284810711063	Completed
Event Type	Start	End	Location	Status																											
Load Control	1/23/13 10:00 AM	1/23/13 11:00 AM	1284810711063	Completed																											
Load Control	1/23/13 10:00 AM	1/23/13 11:00 AM	1284810711063	Completed																											
Load Control	1/23/13 10:00 AM	1/23/13 11:00 AM	1284810711063	Completed																											
Load Control	1/23/13 10:00 AM	1/23/13 11:00 AM	1284810711063	Completed																											
Load Control	1/23/13 10:00 AM	1/23/13 11:00 AM	1284810711063	Completed																											

<p>20. Log in to AHE Command Center.</p> 	<p>20. Successfully logged in to AHE.</p> 
<p>21. Search the meter number 1284810711063.</p> 	<p>21. Meter search displays the information.</p>  <p>Gridstream RF Endpoint Information Meter # 1284810711063 Endpoint ID: 4028145577(F03B9FA9)</p> <p>Model: Smart [Link] Last Reading: 134 000.1 9/25/2011 2:32 AM Model: RF Integrated Focus AX Latitude: 39.105028 Longitude: -94.375129 Configuration Group: RF Endpoint - Green Impact Zone [Link] Collector: 121.128.1063 - Level 1 WAN Address: 192.168.1.1063 800 CHARLOTTE ST, ATGPO, MD 44208 Street Name: 878-4028145577(F03B9FA9) (Internal) ipTitle: n/a</p> <p>Generic Manage Readings Interval Data History MIB Security</p> <p>View Endpoint Commands</p> <p>Issue Commands [Dropdown]</p>

22. Select the "History" tab.

Gridstream RF Endpoint Information
Meter = 1204010711063 Endpoint S/N 4020145577(FD109FA9)

General | **History** | Readings | Interval Data | NAM | Security

22. The History tab shows that event has started.

Gridstream RF Endpoint Information
Meter = 1204010711063 Endpoint S/N 4020145577(FD109FA9)

General | **History** | Readings | Interval Data | NAM | Security

Event	Description	Received	Collector
Load control event status	WAN Device Smart ID = 5045 Load Control Event ID = 24001 Load Control Event Status Code = 1	12/22/2013 12:26:24	001 G&P Collector
WAN Load Control Received	SendSmartEnergyPackTest=Success	12/22/2013 12:26:24	001 G&P Collector
Load control event received	WAN Device Smart ID = 5045 Load Control Event ID = 24001 Load Control Event Status Code = 1	12/22/2013 12:26:24	001 G&P Collector
WAN Load Control Scheduled	SendSmartEnergyPackTest=Success	12/22/2013 12:26:24	001 G&P Collector
Load control event received	WAN Device Smart ID = 5045 Load Control Event ID = 24001 Load Control Event Status Code = 1	12/22/2013 12:26:24	001 G&P Collector
WAN Load Control All Cancelled	SendSmartEnergyPackTest=Success	12/22/2013 12:26:24	001 G&P Collector
Endpoint Power Restore	Power restore event number 4020145577	12/22/2013 12:26:24	001 G&P Collector

23. Check the History tab for the DR event completion. (After – event)

Gridstream RF Endpoint Information
Meter = 1204010711063 Endpoint S/N 4020145577(FD109FA9)

General | **History** | Readings | Interval Data | NAM | Security

Event	Description	Received	Collector
Load control event completion	WAN Device Smart ID = 5045 Load Control Event ID = 24001 Load Control Event Status Code = 1	12/22/2013 12:26:24	001 G&P Collector
Load control event status	WAN Device Smart ID = 5045 Load Control Event ID = 24001 Load Control Event Status Code = 1	12/22/2013 12:26:24	001 G&P Collector
WAN Load Control Scheduled	SendSmartEnergyPackTest=Success	12/22/2013 12:26:24	001 G&P Collector
Load control event received	WAN Device Smart ID = 5045 Load Control Event ID = 24001 Load Control Event Status Code = 1	12/22/2013 12:26:24	001 G&P Collector
WAN Load Control All Cancelled	SendSmartEnergyPackTest=Success	12/22/2013 12:26:24	001 G&P Collector

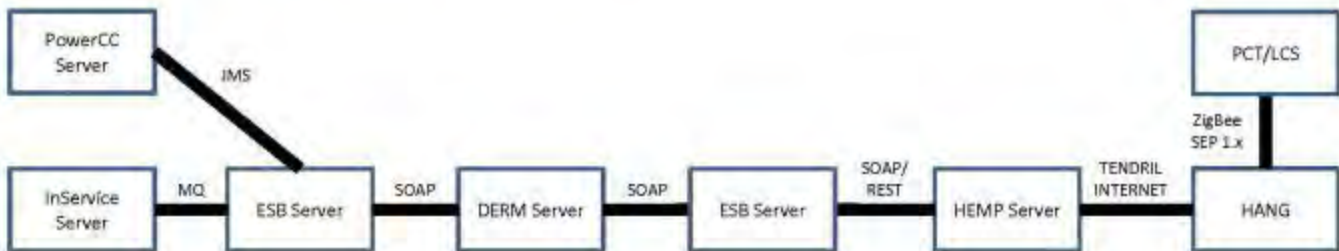
23. The result shows that the event has been successfully completed.

Gridstream RF Endpoint Information
Meter = 1204010711063 Endpoint S/N 4020145577(FD109FA9)

General | **History** | Readings | Interval Data | NAM | Security



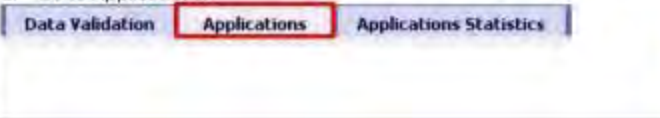

Event	Description	Received	Collector
Load control event completion	WAN Device Smart ID = 5045 Load Control Event ID = 24001 Load Control Event Status Code = 1	12/22/2013 12:26:24	001 G&P Collector
Load control event status	WAN Device Smart ID = 5045 Load Control Event ID = 24001 Load Control Event Status Code = 1	12/22/2013 12:26:24	001 G&P Collector
WAN Load Control Scheduled	SendSmartEnergyPackTest=Success	12/22/2013 12:26:24	001 G&P Collector
Load control event received	WAN Device Smart ID = 5045 Load Control Event ID = 24001 Load Control Event Status Code = 1	12/22/2013 12:26:24	001 G&P Collector
WAN Load Control All Cancelled	SendSmartEnergyPackTest=Success	12/22/2013 12:26:24	001 G&P Collector

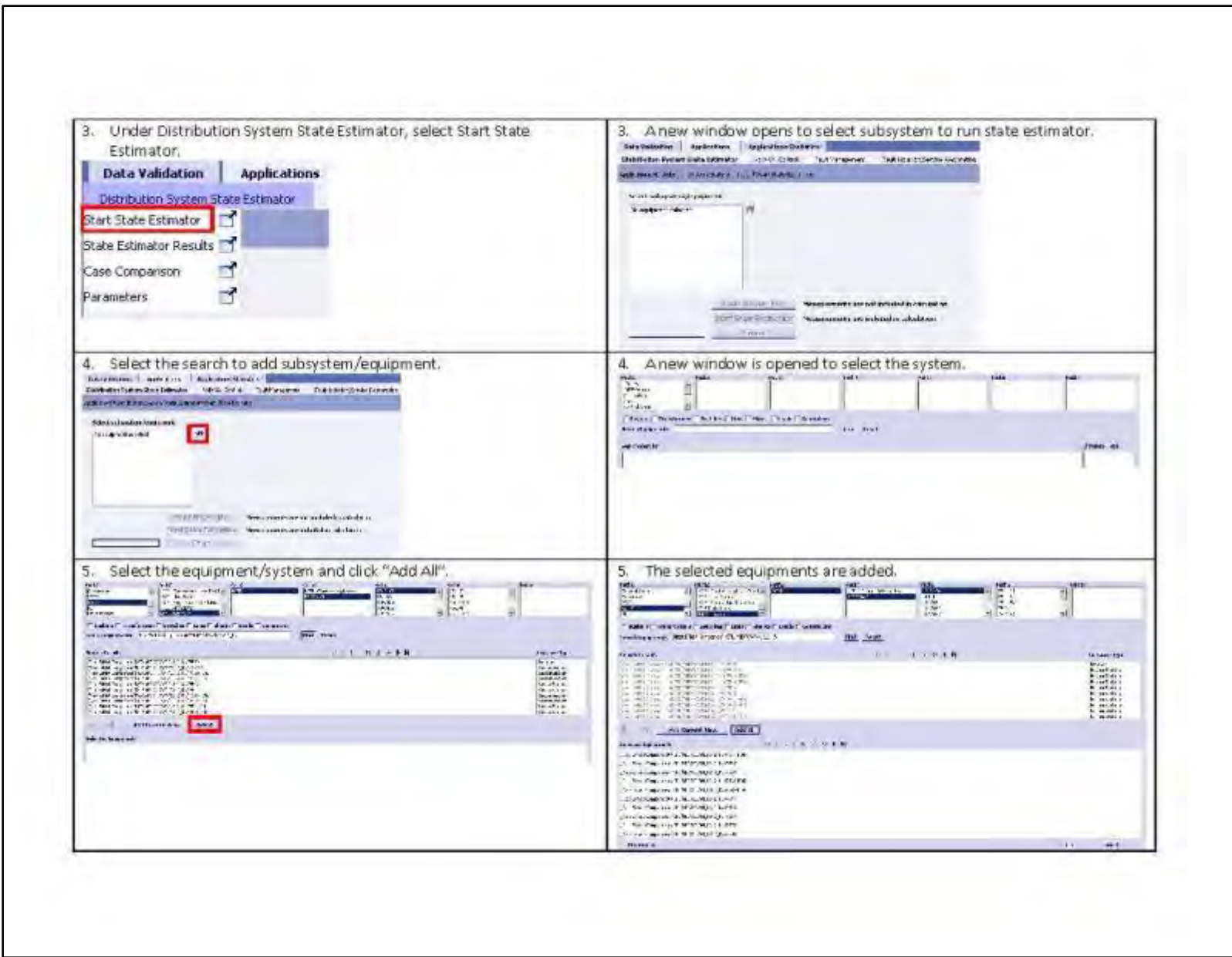
Demand Response – HAN Devices

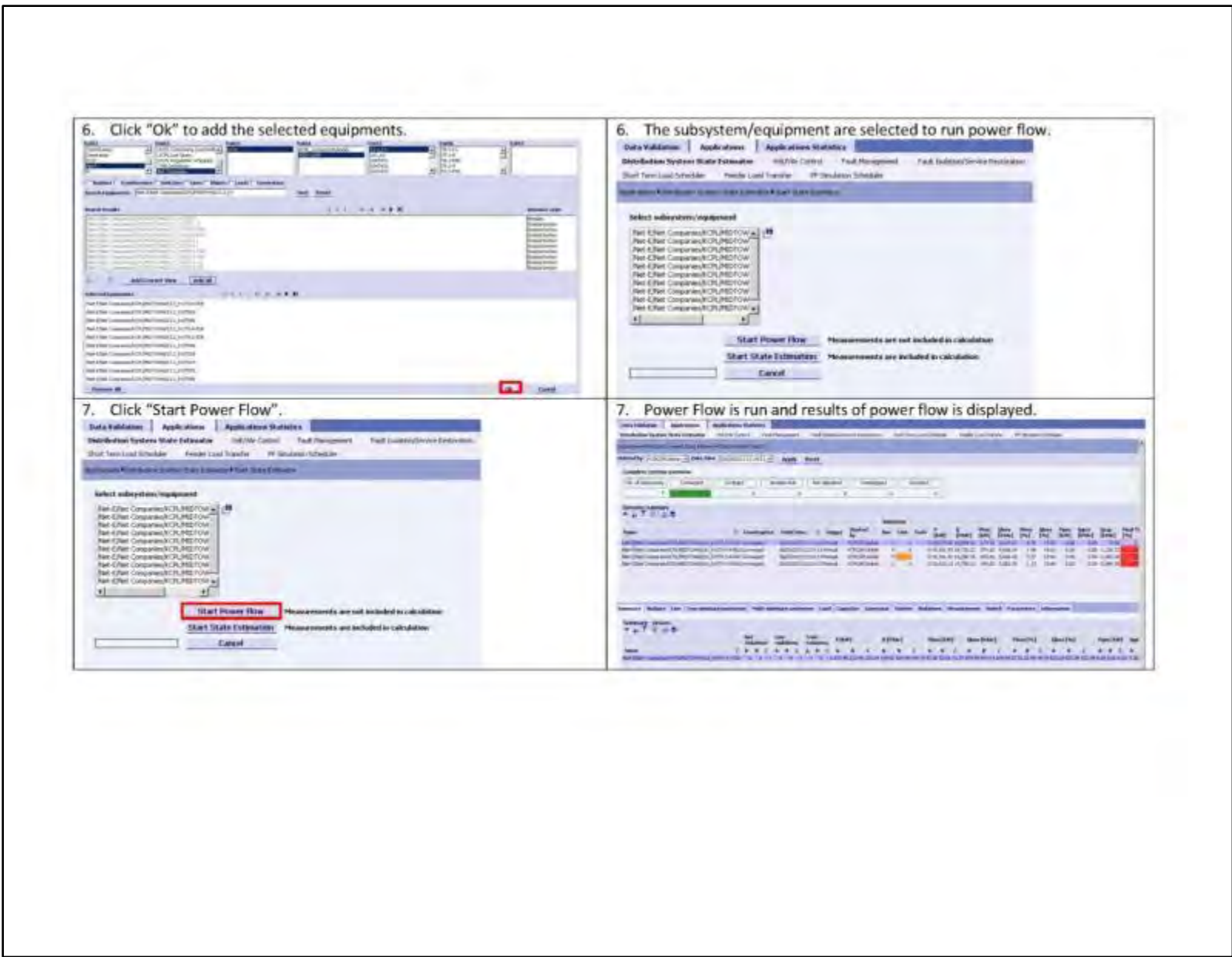


Scheduled Demand Response: HAN Devices Operation

Pre-Condition: An overload is occurred in a feeder.

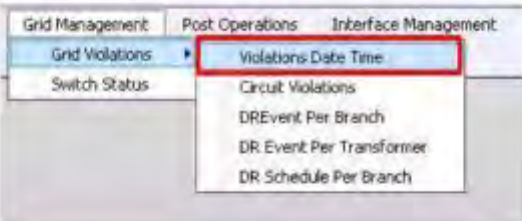
Steps	Expected Result
1. Log in to PowerCC/DMS. 	1. Successfully logged in to PowerCC/DMS. 
2. Go to Applications. 	2. WebUI displays the distribution network applications. 



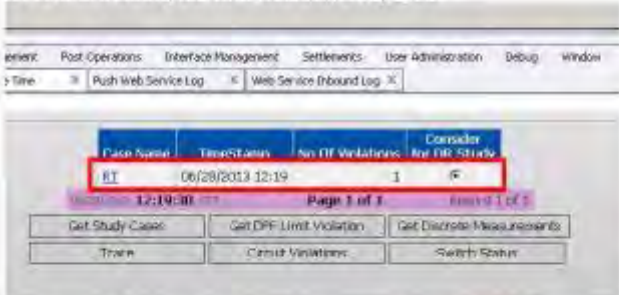


<p>8. Verify in the DMS server log that the message has been sent to DERM. Go to Network > DMS01 > powercc > temp > DERM. And select OUT_RT_MsgCreatedDistributionPowerFlowLimitViolations51.xml with the latest time stamp.</p> 	<p>8. The log file is opened that verified that violations have been sent to DERM.</p> 
<p>9. Log in to the DERM webUI.</p> 	<p>9. Successfully logged in to DERM webUI.</p> 

10. Under Grid Management, select Grid Violations and then Violations Date Time.

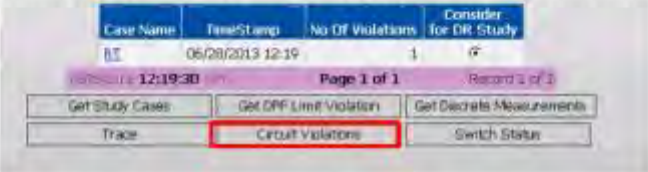


10. A new window/tab with violations is opened.




Case Name	TimeStamp	No. Of Violations	Consider for DR Study
ET	06/28/2013 12:19	1	Y

11. Press "Circuit Violations" button to query the violations from DMS.




11. A new tab "Circuit Violations" open with details of violations.

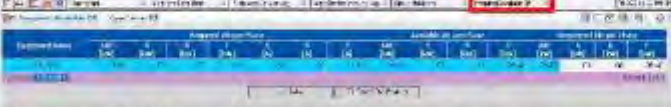


Customer Name	Violation Line No.	Device No.	Line No.	Phase	Phase A	Phase B	Phase C	Unit Type	Equipment	Created On Date
100001	100001	01	001	01	01	01	01	00	000000000000000000	06/28/2013


12. Since there is only 1 overload, click "Grid Aggregation".




12. A new tab "Required/Available DR" opens with required and available DR.



13. Click "DR Event per Branch".



13. A new tab "DR Event Per Branch" opens with information.



Equipment Name	Scheduled DR			Requested DR		
	A [RW]	B [RW]	C [RW]	A [RW]	B [RW]	C [RW]
100001	00	00	00	00	00	00

14. Click "DR Event per Transformer".

Push Web Service Log Web Service Inbound ... Circuit Violations

Equipment Name	Scheduled DR				Requested DR			
	A [kW]	B [kW]	C [kW]	ABC [kW]	A [kW]	B [kW]	C [kW]	ABC [kW]
1061021	.00	.00	26.40	26.40	.00	.00	26.40	26.40
05/28/2013 12:21:11 CPT Page 1 of 1 Record 1 of 1 DR Event per Transformer								

14. A new tab "DR Event Per Transformer" opens with DR that will be scheduled from each transformer.

Push Web Service Log Web Service Inbound ... Circuit Violations ... Required/Validat...

Transformer	Scheduled				Total kW
	DR A [kW]	DR B [kW]	DR C [kW]	DR ABC [kW]	
1079325	.00	.00	10.20	10.20	10.20
1079330	.00	.00	10.20	10.20	10.20
1327679	.00	.00	6.00	6.00	6.00
Total	.00	.00	26.40	26.40	26.40

05/28/2013 12:21:22 CPT Record 1 of 3

back to the dates go date to event

15. Click on "Schedule DR Controls".

Push Web Service Log Web Service Inbound ... Circuit Violations ... Required/Validat...

Transformer	Scheduled				Total kW
	DR A [kW]	DR B [kW]	DR C [kW]	DR ABC [kW]	
1079325	.00	.00	10.20	10.20	10.20
1079330	.00	.00	10.20	10.20	10.20
1327679	.00	.00	6.00	6.00	6.00
Total	.00	.00	26.40	26.40	26.40

05/28/2013 12:21:22 CPT Record 1 of 3

Schedule DR Controls Delete DR Controls Get DFT Solution

save for validation validate DR event

15. A schedule DR controls opens and pops up a window to enter schedule information.

Push Web Service Log Web Service Inbound ... Circuit Violations ... Required/Validat... DR

Transformer	Scheduled				Total kW
	DR A [kW]	DR B [kW]	DR C [kW]	DR ABC [kW]	
1079325	.00	.00	10.20	10.20	10.20
1079330	.00	.00	10.20	10.20	10.20
1327679	.00	.00	6.00	6.00	6.00
Total	.00	.00	26.40	26.40	26.40

05/28/2013 12:21:22 CPT Record 1 of 3

Enter Schedule Information

Schedule Name: [Circuit Violation - 1079325 - 1079330 - 1327679]

Schedule Date: 05/28/2013

Start Time: 12:00

End Time: 12:00



create cancel


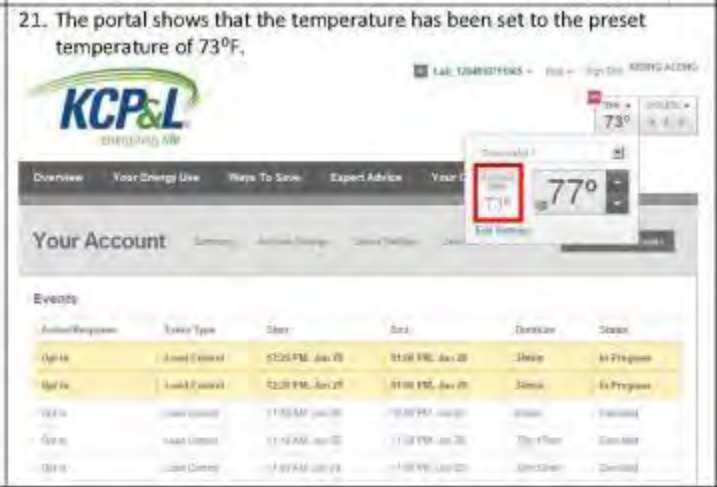
16. Enter the schedule information and press "create".

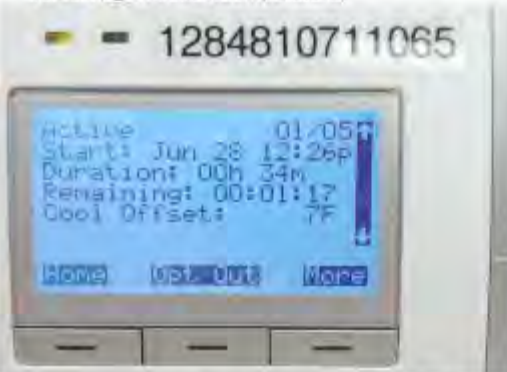

16. A new page opens that shows the DR events that were committed as a result of the overload. (notification was sent to the HEMP at 12:21, and the event was scheduled from 12:26 through 1:00)

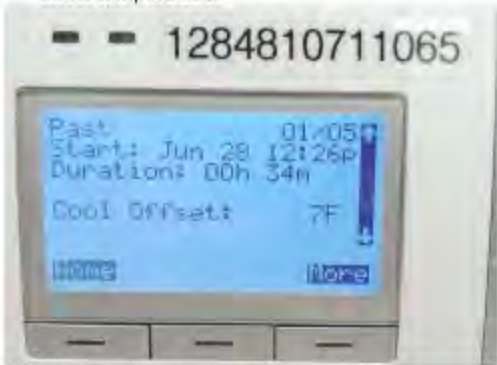

17. Go to Interface Management > Web Services > Push Web Services > Push Web Service Log.



17. This verifies DR message has been sent to HEMP.



<p>18. Verify the DR events in HAN devices. Check the thermostat before the event starts. (Pre-event)</p>	<p>18. The thermostat shows the start date, start time and duration.</p> 
<p>19. Check the thermostat for temperature offset before the event start. (Pre-event)</p>	<p>19. Temperature before the event.</p> 

<p>20. Log in to KCP&L portal (HEMP) to verify the devices are off. (DR event is process)</p>	<p>20. The devices connected to the meter ID 1284810711065 are off.</p>  <table border="1"> <thead> <tr> <th>Actual/Response</th> <th>Event Type</th> <th>Start</th> <th>End</th> <th>Duration</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>Off</td> <td>Load Control</td> <td>12:01 PM, Jun 20</td> <td>01:00 PM, Jun 20</td> <td>59min</td> <td>In Progress</td> </tr> <tr> <td>Off</td> <td>Load Control</td> <td>03:02 PM, Jun 20</td> <td>04:00 PM, Jun 20</td> <td>58min</td> <td>In Progress</td> </tr> <tr> <td>Off</td> <td>Load Control</td> <td>11:28 AM, Jun 20</td> <td>12:00 PM, Jun 20</td> <td>36min</td> <td>Completed</td> </tr> <tr> <td>Off</td> <td>Load Control</td> <td>11:20 AM, Jun 20</td> <td>11:00 AM, Jun 20</td> <td>20min</td> <td>Completed</td> </tr> <tr> <td>Off</td> <td>Load Control</td> <td>11:06 AM, Jun 20</td> <td>11:00 AM, Jun 20</td> <td>5min</td> <td>Completed</td> </tr> </tbody> </table>	Actual/Response	Event Type	Start	End	Duration	Status	Off	Load Control	12:01 PM, Jun 20	01:00 PM, Jun 20	59min	In Progress	Off	Load Control	03:02 PM, Jun 20	04:00 PM, Jun 20	58min	In Progress	Off	Load Control	11:28 AM, Jun 20	12:00 PM, Jun 20	36min	Completed	Off	Load Control	11:20 AM, Jun 20	11:00 AM, Jun 20	20min	Completed	Off	Load Control	11:06 AM, Jun 20	11:00 AM, Jun 20	5min	Completed
Actual/Response	Event Type	Start	End	Duration	Status																																
Off	Load Control	12:01 PM, Jun 20	01:00 PM, Jun 20	59min	In Progress																																
Off	Load Control	03:02 PM, Jun 20	04:00 PM, Jun 20	58min	In Progress																																
Off	Load Control	11:28 AM, Jun 20	12:00 PM, Jun 20	36min	Completed																																
Off	Load Control	11:20 AM, Jun 20	11:00 AM, Jun 20	20min	Completed																																
Off	Load Control	11:06 AM, Jun 20	11:00 AM, Jun 20	5min	Completed																																
<p>21. Log in to the KCP&L Portal to verify the temperature.</p>	<p>21. The portal shows that the temperature has been set to the preset temperature of 73°F.</p>  <table border="1"> <thead> <tr> <th>Actual/Response</th> <th>Event Type</th> <th>Start</th> <th>End</th> <th>Duration</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>Off</td> <td>Load Control</td> <td>03:25 PM, Jun 20</td> <td>04:00 PM, Jun 20</td> <td>35min</td> <td>In Progress</td> </tr> <tr> <td>Off</td> <td>Load Control</td> <td>02:28 PM, Jun 20</td> <td>03:00 PM, Jun 20</td> <td>32min</td> <td>In Progress</td> </tr> <tr> <td>Off</td> <td>Load Control</td> <td>11:58 AM, Jun 20</td> <td>12:00 PM, Jun 20</td> <td>2min</td> <td>Completed</td> </tr> <tr> <td>Off</td> <td>Load Control</td> <td>11:12 AM, Jun 20</td> <td>11:00 AM, Jun 20</td> <td>12min</td> <td>Completed</td> </tr> <tr> <td>Off</td> <td>Load Control</td> <td>11:07 AM, Jun 20</td> <td>11:00 AM, Jun 20</td> <td>7min</td> <td>Completed</td> </tr> </tbody> </table>	Actual/Response	Event Type	Start	End	Duration	Status	Off	Load Control	03:25 PM, Jun 20	04:00 PM, Jun 20	35min	In Progress	Off	Load Control	02:28 PM, Jun 20	03:00 PM, Jun 20	32min	In Progress	Off	Load Control	11:58 AM, Jun 20	12:00 PM, Jun 20	2min	Completed	Off	Load Control	11:12 AM, Jun 20	11:00 AM, Jun 20	12min	Completed	Off	Load Control	11:07 AM, Jun 20	11:00 AM, Jun 20	7min	Completed
Actual/Response	Event Type	Start	End	Duration	Status																																
Off	Load Control	03:25 PM, Jun 20	04:00 PM, Jun 20	35min	In Progress																																
Off	Load Control	02:28 PM, Jun 20	03:00 PM, Jun 20	32min	In Progress																																
Off	Load Control	11:58 AM, Jun 20	12:00 PM, Jun 20	2min	Completed																																
Off	Load Control	11:12 AM, Jun 20	11:00 AM, Jun 20	12min	Completed																																
Off	Load Control	11:07 AM, Jun 20	11:00 AM, Jun 20	7min	Completed																																

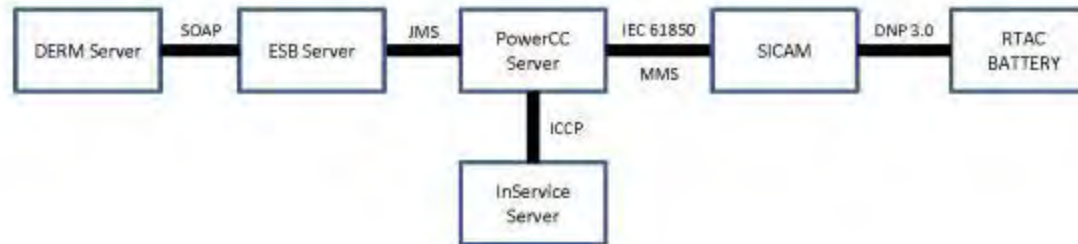
<p>22. Verify the DR events in HAN devices. Check the thermostat before the event starts. (During event)</p>	<p>22. The thermostat shows the DR event start date, time, duration, time remaining and offset temperature.</p> 
<p>23. Check the thermostat for temperature offset during the event. (during-event)</p>	<p>23. Thermostat shows the temperature offset by DR event.</p> 

<p>24. Check the thermostat for the DR event completion. (After – event)</p>	<p>24. The thermostat displays the DR event start date, time, duration and offset temperature.</p>  <p>The image shows a thermostat screen with the following text: "Past", "Start: Jun 28 01:05p", "Duration: 00h 34m", and "Cool Offset: 7F". There are also "HOME" and "MENU" buttons at the bottom of the screen.</p>
<p>25. Check the thermostat for the temperature offset. (After-event)</p>	<p>25. Thermostat shows the temperature offset.</p>  <p>The image shows a thermostat screen with the following text: "Fri Jun 28 1:01p", "73°F", "70°F", "Cool Away", "Auto S2", and "\$0.074/kWh". There are also "HOME", "MENU", and "MESSAGE" buttons at the bottom of the screen.</p>

<p>26. Log in to KCP&L portal to verify the devices are on. (DR event complete)</p>	 <p>26. The devices connected to the meter ID 1284810711065 are on.</p> <table border="1"> <thead> <tr> <th>Account/Response</th> <th>Event Type</th> <th>Start</th> <th>End</th> <th>Location</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>1284810711065</td> <td>Load Control</td> <td>12/21/13 10:00</td> <td>11/30/13 12:00</td> <td>1284810711065</td> <td>Completed</td> </tr> <tr> <td>1284810711065</td> <td>Load Control</td> <td>12/21/13 10:00</td> <td>11/30/13 12:00</td> <td>1284810711065</td> <td>Completed</td> </tr> <tr> <td>1284810711065</td> <td>Load Control</td> <td>12/21/13 10:00</td> <td>11/30/13 12:00</td> <td>1284810711065</td> <td>Completed</td> </tr> <tr> <td>1284810711065</td> <td>Load Control</td> <td>12/21/13 10:00</td> <td>11/30/13 12:00</td> <td>1284810711065</td> <td>Completed</td> </tr> <tr> <td>1284810711065</td> <td>Load Control</td> <td>12/21/13 10:00</td> <td>11/30/13 12:00</td> <td>1284810711065</td> <td>Completed</td> </tr> </tbody> </table>	Account/Response	Event Type	Start	End	Location	Status	1284810711065	Load Control	12/21/13 10:00	11/30/13 12:00	1284810711065	Completed	1284810711065	Load Control	12/21/13 10:00	11/30/13 12:00	1284810711065	Completed	1284810711065	Load Control	12/21/13 10:00	11/30/13 12:00	1284810711065	Completed	1284810711065	Load Control	12/21/13 10:00	11/30/13 12:00	1284810711065	Completed	1284810711065	Load Control	12/21/13 10:00	11/30/13 12:00	1284810711065	Completed
Account/Response	Event Type	Start	End	Location	Status																																
1284810711065	Load Control	12/21/13 10:00	11/30/13 12:00	1284810711065	Completed																																
1284810711065	Load Control	12/21/13 10:00	11/30/13 12:00	1284810711065	Completed																																
1284810711065	Load Control	12/21/13 10:00	11/30/13 12:00	1284810711065	Completed																																
1284810711065	Load Control	12/21/13 10:00	11/30/13 12:00	1284810711065	Completed																																
1284810711065	Load Control	12/21/13 10:00	11/30/13 12:00	1284810711065	Completed																																
<p>27. In the KCP&L Portal, verify the temperature offset. (After event)</p>	 <p>27. The portal shows that the temperature has been set to the preset temperature of 73°F. (After event)</p> <table border="1"> <thead> <tr> <th>Account/Response</th> <th>Event Type</th> <th>Start</th> <th>End</th> <th>Location</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>1284810711065</td> <td>Load Control</td> <td>12/21/13 10:00</td> <td>11/30/13 12:00</td> <td>1284810711065</td> <td>Completed</td> </tr> <tr> <td>1284810711065</td> <td>Load Control</td> <td>12/21/13 10:00</td> <td>11/30/13 12:00</td> <td>1284810711065</td> <td>Completed</td> </tr> <tr> <td>1284810711065</td> <td>Load Control</td> <td>12/21/13 10:00</td> <td>11/30/13 12:00</td> <td>1284810711065</td> <td>Completed</td> </tr> <tr> <td>1284810711065</td> <td>Load Control</td> <td>12/21/13 10:00</td> <td>11/30/13 12:00</td> <td>1284810711065</td> <td>Completed</td> </tr> <tr> <td>1284810711065</td> <td>Load Control</td> <td>12/21/13 10:00</td> <td>11/30/13 12:00</td> <td>1284810711065</td> <td>Completed</td> </tr> </tbody> </table>	Account/Response	Event Type	Start	End	Location	Status	1284810711065	Load Control	12/21/13 10:00	11/30/13 12:00	1284810711065	Completed	1284810711065	Load Control	12/21/13 10:00	11/30/13 12:00	1284810711065	Completed	1284810711065	Load Control	12/21/13 10:00	11/30/13 12:00	1284810711065	Completed	1284810711065	Load Control	12/21/13 10:00	11/30/13 12:00	1284810711065	Completed	1284810711065	Load Control	12/21/13 10:00	11/30/13 12:00	1284810711065	Completed
Account/Response	Event Type	Start	End	Location	Status																																
1284810711065	Load Control	12/21/13 10:00	11/30/13 12:00	1284810711065	Completed																																
1284810711065	Load Control	12/21/13 10:00	11/30/13 12:00	1284810711065	Completed																																
1284810711065	Load Control	12/21/13 10:00	11/30/13 12:00	1284810711065	Completed																																
1284810711065	Load Control	12/21/13 10:00	11/30/13 12:00	1284810711065	Completed																																
1284810711065	Load Control	12/21/13 10:00	11/30/13 12:00	1284810711065	Completed																																

<p>28. Log in to Tendril Utility Load Control to see the DR Event in the Load Control.</p>	<p>28. Load Control summary for the DR Event.</p> 
<p>29. DR event as seen in the load control.</p>	<p>29. DR event summary of the device for the given device ID.</p> 

Demand Response – Battery



Scheduled Demand Response: Battery Operation

Pre-Condition: Battery must be fully charged


1. Log in to OMS I/Dispatcher.




1. Successfully logged in to OMS I/Dispatcher.




2. Open the Feature Information window.



2. A new window is opened.



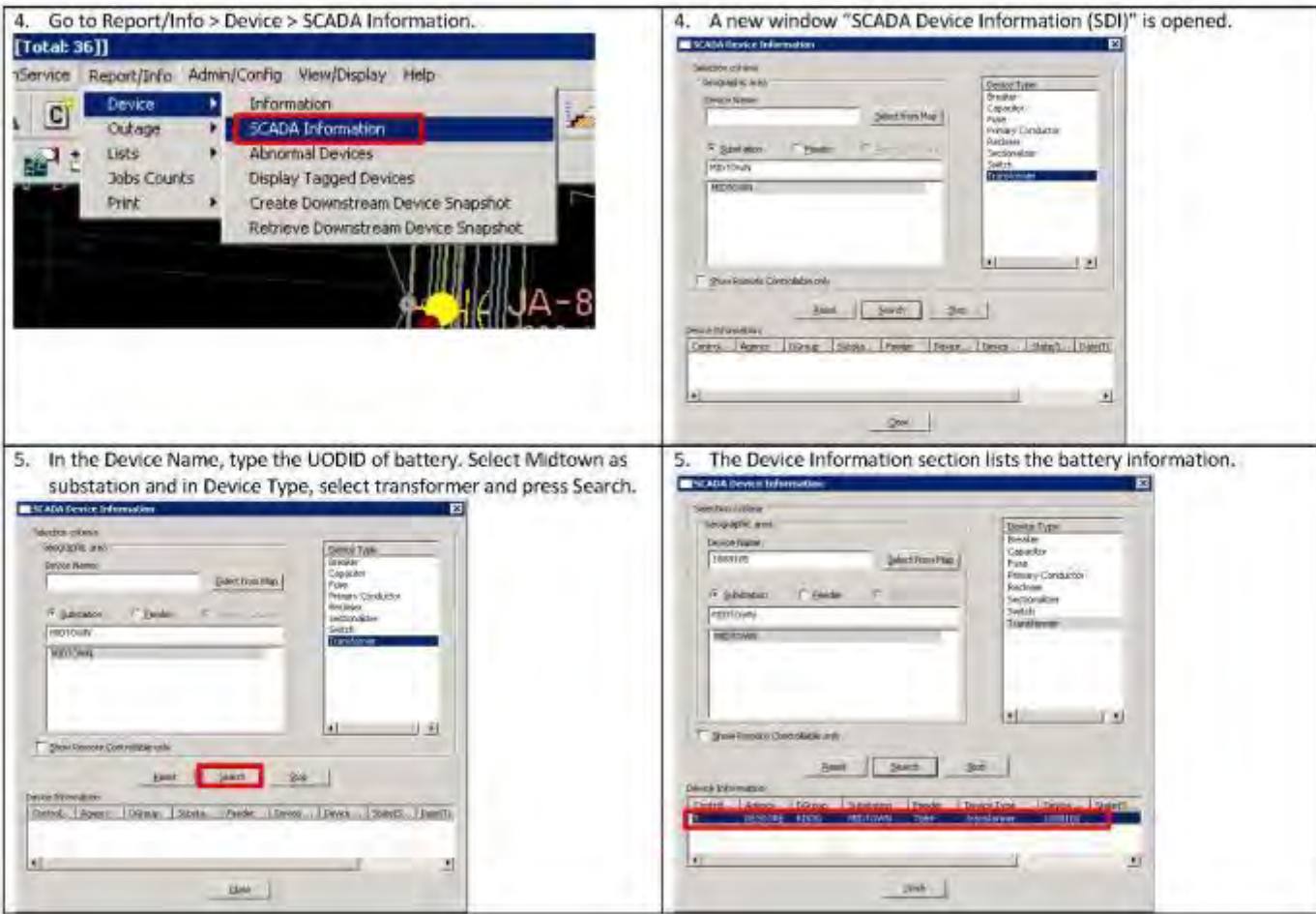
3. In the Feature Information window, enter the battery UODID (1888105).



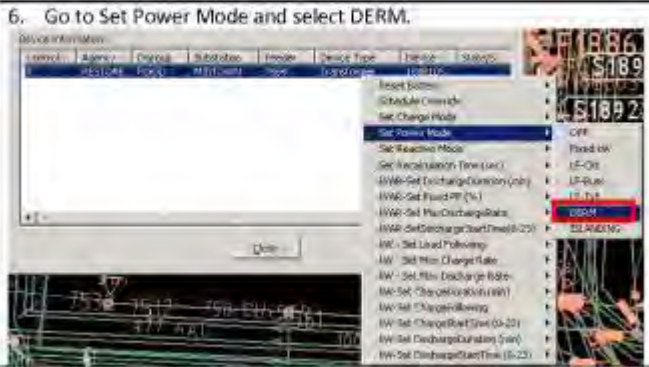
3. The feature information displays the SCADA value for battery.



Item	Value
Active State	Ready
Active Status	unknown
Alarm - 0004	00
Alarm - 0006	00
Alarm - Trip Offlow	00
Alarm - Warning	00
BEC Status	Enabled
Charge Mode	OFF
Energy Available (%)	50
Local - Remote	Remote
Power Mode	OFF
Reserve Mode	OFF
Reproduction Time (sec)	0
SCADA Device Comm Failure	OK
Schedule Charge Status	Disabled
UASC - Discharge Duration (min)	0
UASC - Discharge Start Time (0-23)	0
UASC - Flood RT (min)	0
UASC - Max Discharge Rate	0
UASC - Charge Duration (min)	0
UASC - Charge Following	0
UASC - Charge Start Time (0-23)	0
UASC - Discharge Duration (min)	0
UASC - Discharge Start Time (0-23)	0
UASC - Load Following	0
UASC - Max Charge Rate	0
UASC - Max Discharge Rate	0




6. Go to Set Power Mode and select DERM.



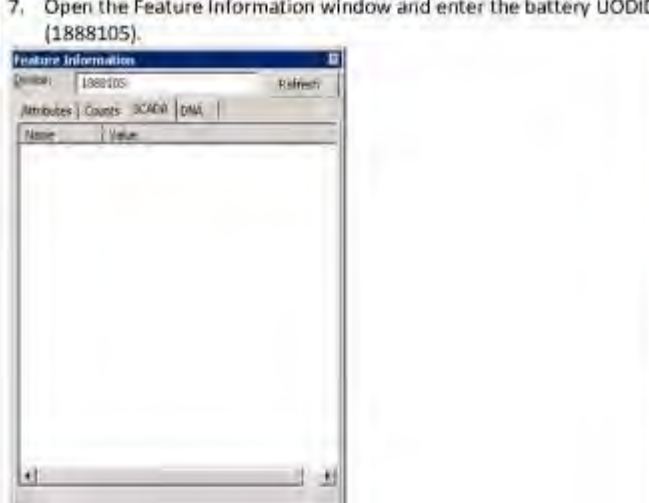
The screenshot shows a 'Device Information' window with a dropdown menu open. The menu items include 'Set Power Mode', 'Set Reactive Mode', 'Set Recirculation Time (sec)', 'AWR-Set [Discharge Duration (min)]', 'AWR-Set Recirculation Rate', 'AWR-Set Discharge Start Time (0-23)', 'AW-Set Load Following', 'AW-Set Min. Charge Rate', 'AW-Set Min. Discharge Rate', 'AW-Set Charge Following', 'AW-Set Charge Start Time (0-23)', 'AW-Set Discharge Duration (min)', and 'AW-Set Discharge Start Time (0-23)'. The 'Set Power Mode' option is highlighted, and a sub-menu is visible with 'DERM' selected.

6. The Battery is now set to DERM mode.



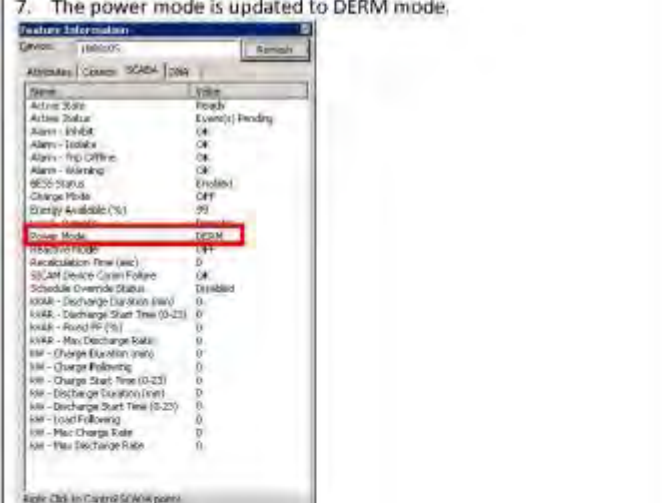
The screenshot shows the 'Device Information' window with the dropdown menu closed. The 'Set Power Mode' is now set to 'DERM'.

7. Open the Feature Information window and enter the battery UODID (1888105).

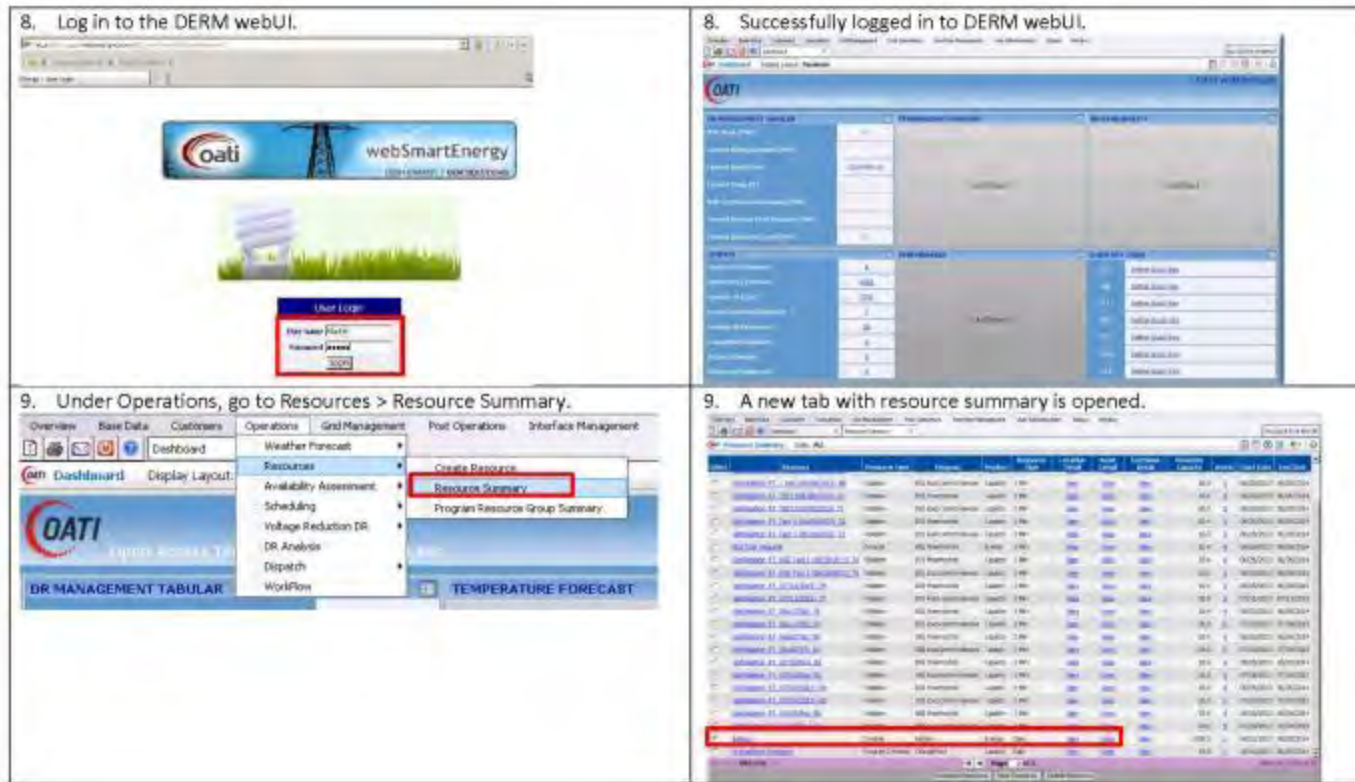


The screenshot shows a 'Feature Information' window. The 'Device' field contains '1888105'. There are tabs for 'Attributes', 'Counts', 'SCADA', and 'DMS'. The 'Attributes' tab is active, showing a table with columns for 'Name' and 'Value'.

7. The power mode is updated to DERM mode.



The screenshot shows the 'Feature Information' window with the 'Power Mode' attribute highlighted in red. The value for 'Power Mode' is 'DERM'. Other attributes listed include 'Active State', 'Active Status', 'Alarm - Inhibit', 'Alarm - Trip Offline', 'Alarm - Warning', 'BEC Status', 'Charge Mode', 'Charge Available (%)', 'Discharge Mode', 'Recirculation Mode', 'Recirculation Time (sec)', 'SCADA Device - Charge Following', 'Schedule Override Status', 'AWR - Discharge Duration (min)', 'AWR - Discharge Start Time (0-23)', 'AWR - Recirculation Rate', 'AWR - Max. Discharge Rate', 'AW - Charge Duration (min)', 'AW - Charge Following', 'AW - Charge Start Time (0-23)', 'AW - Discharge Duration (min)', 'AW - Discharge Start Time (0-23)', 'AW - Load Following', 'AW - Max. Charge Rate', and 'AW - Max. Discharge Rate'.



10. Select the battery from the list of resources and press "Schedule Resource".



10. A new window pops up to enter the schedule information.


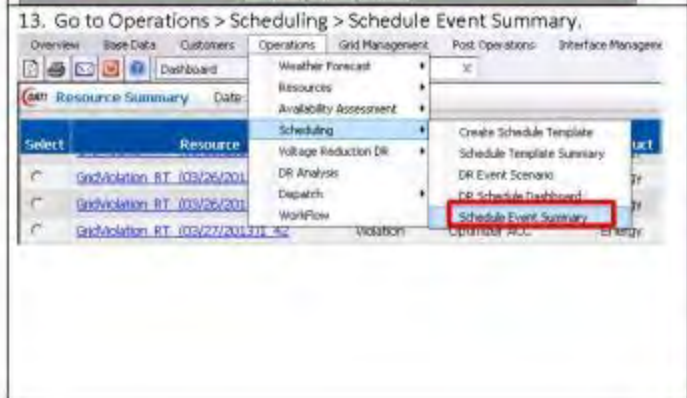
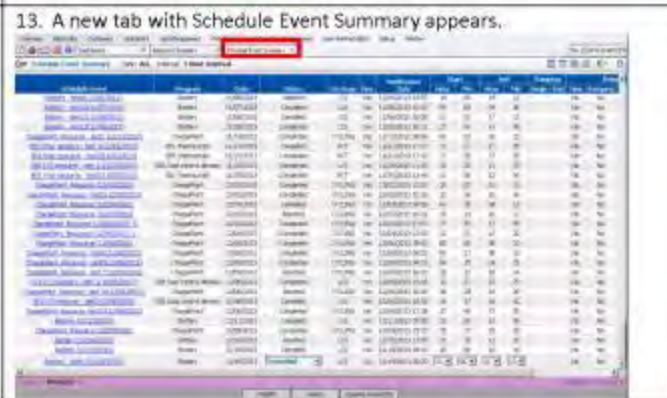


11. Enter the schedule information with name, date, start and end time. Then press Create.

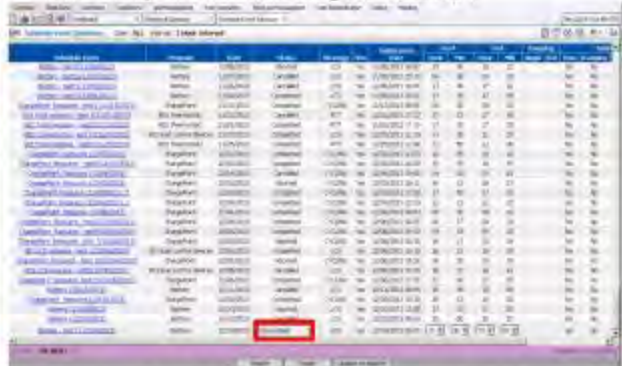


11. A new window pops up that displays the schedule has been created.

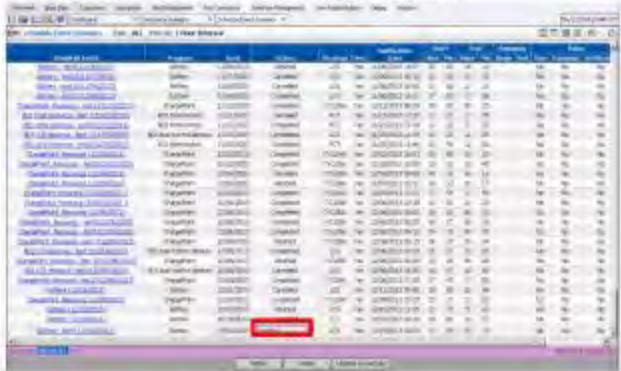


<p>12. Press OK.</p> 	<p>12. The event has been created.</p>
<p>13. Go to Operations > Scheduling > Schedule Event Summary.</p> 	<p>13. A new tab with Schedule Event Summary appears.</p> 

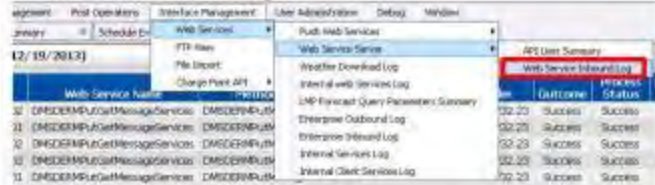
14. Notice that the event is "Committed" now. After the event has been sent to ESB, the status will change to "Notified".




14. Notice that the event has the status "Notified".



15. Go to Interface Management > Web Services > Web Service Server > Web Service Inbound Log.



15. A new tab with Web Service Inbound Log is opened. The oadrCreatedEvent was successful.



Seq	Outcome	Status
10	Success	Success
11	Success	Success
12	Success	Success
13	Success	Success
14	Success	Success
15	Success	Success

16. In I/Dispatcher, press Refresh in the feature information window, to view the DR event sent by DERM.

Feature Information
Device: 1000100
Attributes: Counts: SCADA [OK] Refresh

Name	Value
Active State	Ready
Active Status	Event(s) Pending
Alarm - DMMB	OK
Alarm - Isolate	OK
Alarm - Trip Offline	OK
Alarm - Warning	OK
BESS Status	Enabled
Charge Mode	OFF
Energy Available (%)	99
Local - Remote	Remote
Power Mode	DERM
Relative Mode	OFF
Recalculation Time (sec)	0
SCADA Device Comm Failure	OK
Schedule Override Status	Disabled
KW - Discharge Duration (min)	0
KW - Discharge Start Time (0-23)	0
KW - Fixed PF (%)	0
KW - Max Discharge Rate	0
KW - Charge Duration (min)	0
KW - Charge Following	0
KW - Charge Start Time (0-23)	0
KW - Discharge Duration (min)	0
KW - Discharge Start Time (0-23)	0
KW - Load Following	0
KW - Max Charge Rate	0
KW - Max Discharge Rate	0

Right Click to Control SCADA points

16. The SCADA values are updated after OMS receives the DR event from DERM.

Feature Information
Device: 1000100
Attributes: Counts: SCADA [OK] Refresh

Name	Value
Active State	Event(s) Pending
Active Status	Event(s) Pending
Alarm - Isolate	OK
Alarm - Trip Offline	OK
Alarm - Warning	OK
BESS Status	Enabled
Charge Mode	OFF
Energy Available (%)	98
Local - Remote	Remote
Power Mode	DERM
Relative Mode	OFF
Recalculation Time (sec)	0
SCADA Device Comm Failure	OK
Schedule Override Status	Disabled
KW - Discharge Duration (min)	0
KW - Discharge Start Time (0-23)	0
KW - Fixed PF (%)	0
KW - Max Discharge Rate	0
KW - Charge Duration (min)	0
KW - Charge Following	0
KW - Charge Start Time (0-23)	0
KW - Discharge Duration (min)	10
KW - Discharge Start Time (0-23)	10
KW - Load Following	0
KW - Max Charge Rate	0
KW - Max Discharge Rate	0.71

Right Click to Control SCADA points

17. In the DERM WebUI, go to the Schedule Event Summary tab.

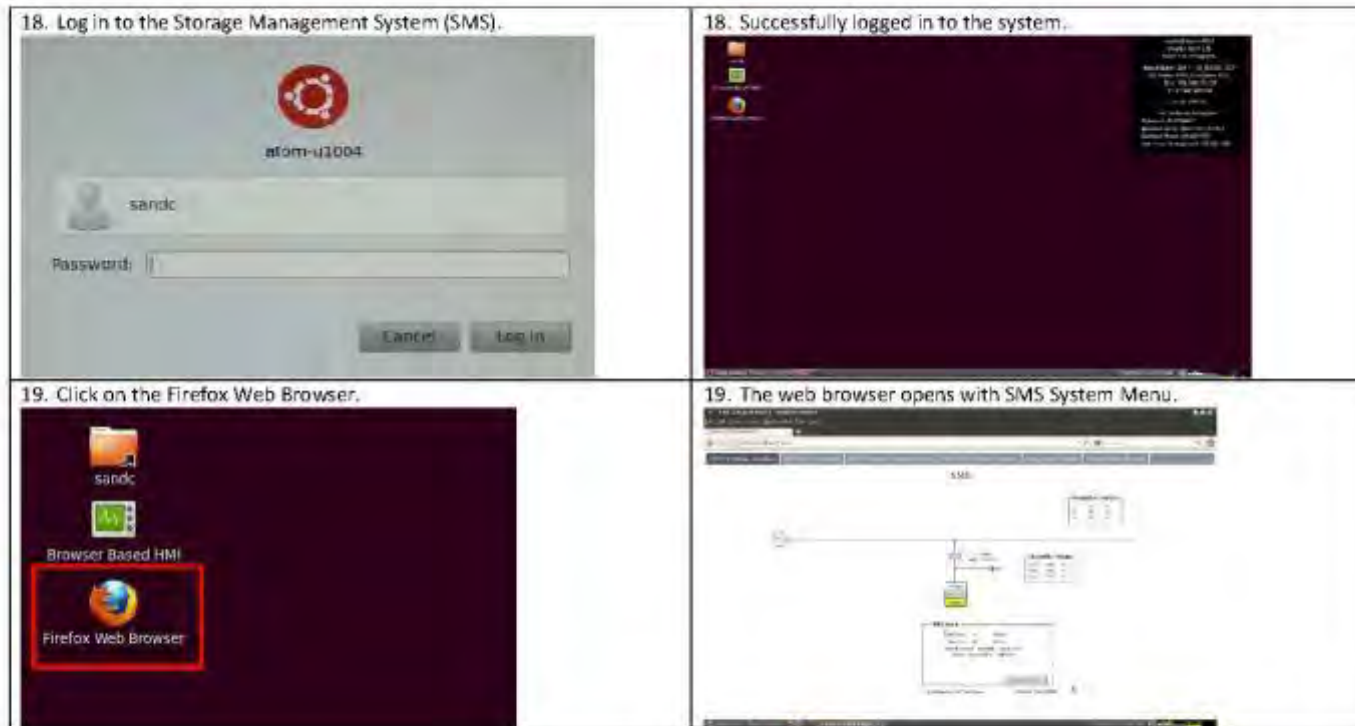
Schedule Event Summary

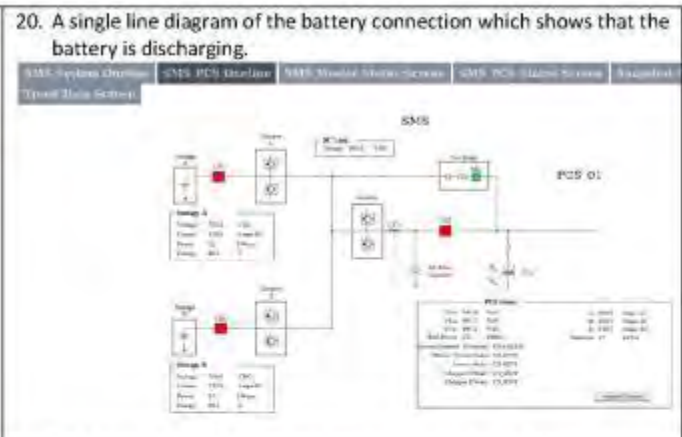
Event ID	Event Name	Status	Start Time	End Time	Priority	Active
1000100-1	DR Event	Active	10/10/2013 10:00:00	10/10/2013 10:10:00	1	Yes
1000100-2	DR Event	Pending	10/10/2013 10:15:00	10/10/2013 10:25:00	1	No
1000100-3	DR Event	Pending	10/10/2013 10:30:00	10/10/2013 10:40:00	1	No

17. In Schedule Event Summary tab, when the DR event has started, the status of event changes to "Active".

Schedule Event Summary

Event ID	Event Name	Status	Start Time	End Time	Priority	Active
1000100-1	DR Event	Active	10/10/2013 10:00:00	10/10/2013 10:10:00	1	Yes
1000100-2	DR Event	Pending	10/10/2013 10:15:00	10/10/2013 10:25:00	1	No
1000100-3	DR Event	Pending	10/10/2013 10:30:00	10/10/2013 10:40:00	1	No





21. In the DERM webUI, go to the Schedule Event Summary tab.

Event ID	Event Name	Event Type	Event Status	Event Start	Event End	Event Duration	Event Location	Event Description
1000000001	Event 1	DR	Completed	1/1/2013 10:00:00	1/1/2013 11:00:00	1:00:00	Location 1	Description 1
1000000002	Event 2	DR	Completed	1/1/2013 12:00:00	1/1/2013 13:00:00	1:00:00	Location 2	Description 2
1000000003	Event 3	DR	Completed	1/1/2013 14:00:00	1/1/2013 15:00:00	1:00:00	Location 3	Description 3
1000000004	Event 4	DR	Completed	1/1/2013 16:00:00	1/1/2013 17:00:00	1:00:00	Location 4	Description 4
1000000005	Event 5	DR	Completed	1/1/2013 18:00:00	1/1/2013 19:00:00	1:00:00	Location 5	Description 5

The screenshot shows a table with columns for Event ID, Event Name, Event Type, Event Status, Event Start, Event End, Event Duration, Event Location, and Event Description. The 'Event Status' column contains the word 'Completed' for several rows. A red box highlights the 'Completed' status in one of the rows.

21. In Schedule Event Summary tab, when the DR event has completed, the status of event changes to "Completed".

Event ID	Event Name	Event Type	Event Status	Event Start	Event End	Event Duration	Event Location	Event Description
1000000001	Event 1	DR	Completed	1/1/2013 10:00:00	1/1/2013 11:00:00	1:00:00	Location 1	Description 1
1000000002	Event 2	DR	Completed	1/1/2013 12:00:00	1/1/2013 13:00:00	1:00:00	Location 2	Description 2
1000000003	Event 3	DR	Completed	1/1/2013 14:00:00	1/1/2013 15:00:00	1:00:00	Location 3	Description 3
1000000004	Event 4	DR	Completed	1/1/2013 16:00:00	1/1/2013 17:00:00	1:00:00	Location 4	Description 4
1000000005	Event 5	DR	Completed	1/1/2013 18:00:00	1/1/2013 19:00:00	1:00:00	Location 5	Description 5

The screenshot shows a table with columns for Event ID, Event Name, Event Type, Event Status, Event Start, Event End, Event Duration, Event Location, and Event Description. The 'Event Status' column contains the word 'Completed' for several rows. A red box highlights the 'Completed' status in one of the rows.

22. In /Dispatcher, after the event has completed, hit refresh in the feature information window.

The screenshot shows a 'Feature Information' window for device '1000105'. The 'Active Status' is highlighted in red and shows the value 'Event(s) Duration'. A red box highlights the 'Refresh' button in the top right corner.

Name	Value
Active Status	Event(s) Duration
Alarm - Inhibit	OK
Alarm - Isolate	OK
Alarm - Trip Offline	OK
Alarm - Warning	OK
BESS Status	Enabled
Charge Mode	OPT
Energy Available (%)	95
Local - Remote	Remote
Power Mode	DERM
Reactive Mode	OFF
Recalculation Time (sec)	0
SCADA Device Conn Failure	OK
Schedule Override Status	Disabled
WAR - Discharge Duration (min)	0
WAR - Discharge Start Time (0-23)	0
WAR - Fixed PF (%)	0
WAR - Max Discharge Rate	0
WAR - Charge Duration (min)	0
WAR - Charge Following	0
WAR - Charge Start Time (0-23)	0
WAR - Discharge Duration (min)	10
WAR - Discharge Start Time (0-23)	10
WAR - Load Following	0
WAR - Max Charge Rate	0
WAR - Max Discharge Rate	1000

Right Click to Control SCADA points

22. The Active status has changed to Event(s) Complete.

The screenshot shows the same 'Feature Information' window after a refresh. The 'Active Status' is now 'Event(s) Complete', highlighted in red. The 'Energy Available (%)' is also highlighted in red and shows a value of 92.


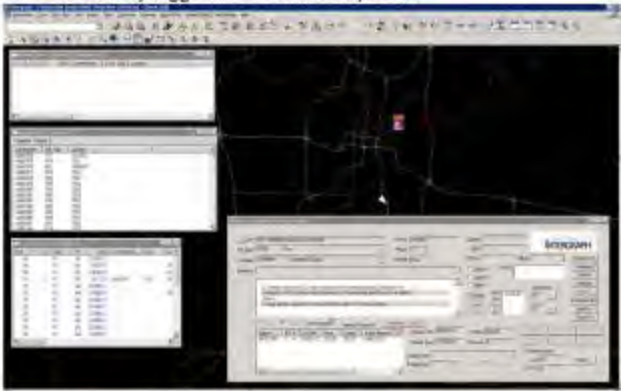
Name	Value
Active Status	Event(s) Complete
Alarm - Inhibit	OK
Alarm - Isolate	OK
Alarm - Trip Offline	OK
Alarm - Warning	OK
BESS Status	Enabled
Charge Mode	OFF
Energy Available (%)	92
Local - Remote	Remote
Power Mode	DERM
Reactive Mode	OFF
Recalculation Time (sec)	0
SCADA Device Conn Failure	OK
Schedule Override Status	Disabled
WAR - Discharge Duration (min)	0
WAR - Discharge Start Time (0-23)	0
WAR - Fixed PF (%)	0
WAR - Max Discharge Rate	0
WAR - Charge Duration (min)	0
WAR - Charge Following	0
WAR - Charge Start Time (0-23)	0
WAR - Discharge Duration (min)	10
WAR - Discharge Start Time (0-23)	10
WAR - Load Following	0
WAR - Max Charge Rate	0
WAR - Max Discharge Rate	1000

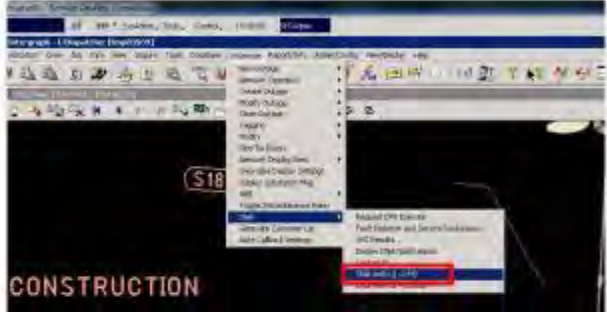




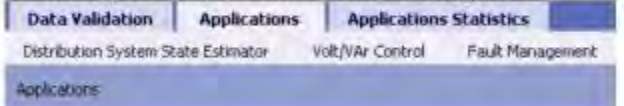
Right Click to Control SCADA points

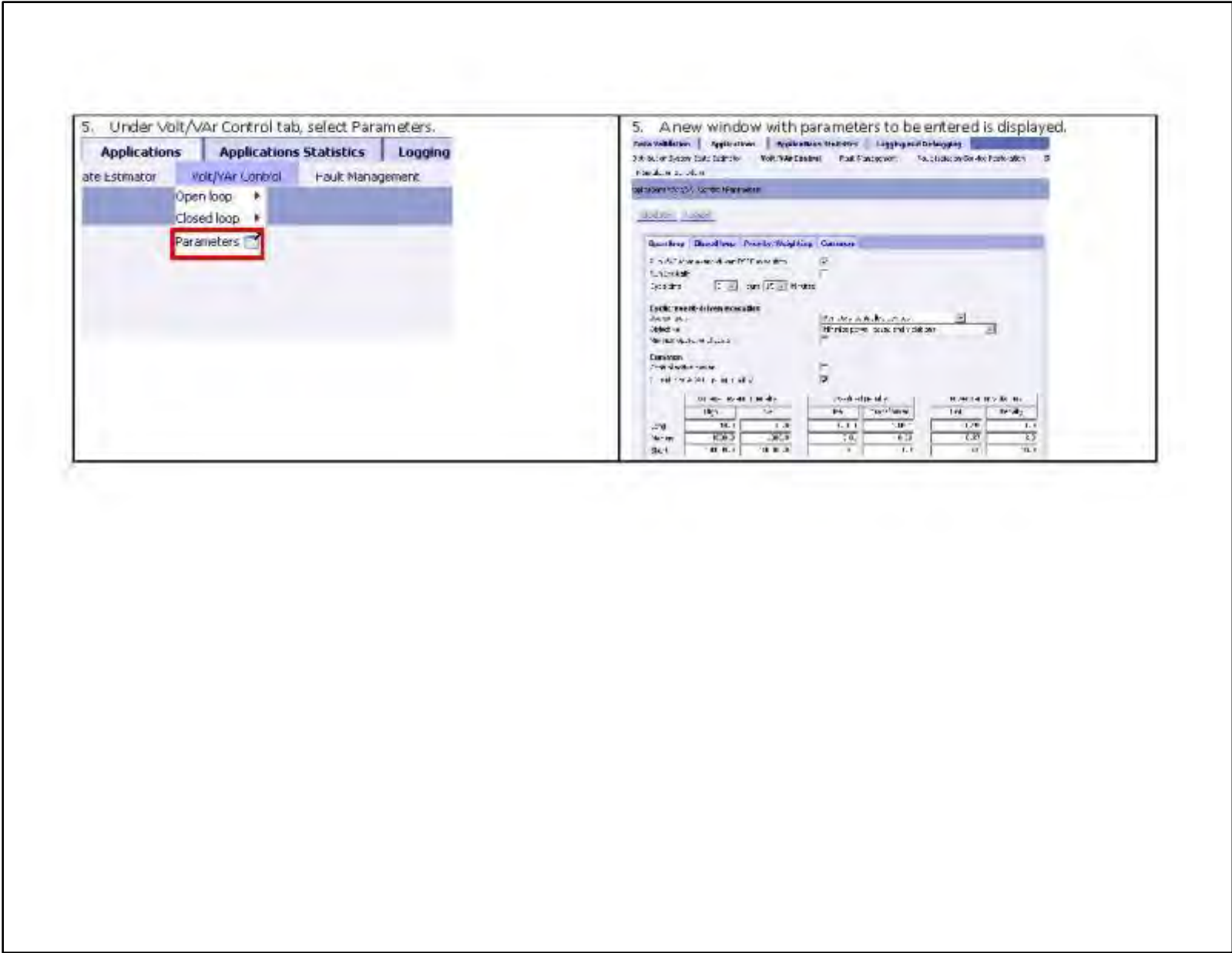
1st Responder Function – Volt/Var Control



VVC in Open Loop Mode

Steps	Expected Results
<p>1. Log in to I/Dispatcher OMS system.</p> 	<p>1. Successfully logged in to the OMS system.</p> 

<p>2. Start WebUI from IDispatcher. Go to InService > DNA > DNA WebUI – DMS.</p>  <p>The screenshot shows a software interface with a menu open. A red box highlights the 'DNA WebUI - DMS' option. A 'CONSTRUCTION' watermark is visible in the bottom left corner.</p>	<p>2. Spectrum PowerCC WebUI opens.</p>  <p>The screenshot shows the Spectrum PowerCC WebUI login page with a title bar that reads 'Distribution Network Applications'.</p>
<p>3. Log in to the Spectrum PowerCC WebUI.</p>  <p>The screenshot shows the Spectrum PowerCC WebUI login page with a title bar that reads 'Distribution Network Applications'.</p>	<p>3. Successfully logged in.</p>  <p>The screenshot shows the Spectrum PowerCC WebUI main dashboard with a title bar that reads 'Distribution Network Applications'.</p>
<p>4. Select "Applications" tab.</p>  <p>The screenshot shows the Spectrum PowerCC WebUI main dashboard with three tabs: 'Data Validation', 'Applications' (highlighted with a red box), and 'Applications Statistics'.</p>	<p>4. The WebUI displays the distribution network applications.</p>  <p>The screenshot shows the Spectrum PowerCC WebUI main dashboard with a title bar that reads 'Distribution Network Applications'. Below the tabs, there are sub-sections for 'Distribution System State Estimator', 'Volt/VAR Control', and 'Fault Management'.</p>



6. Enter the parameters in Open Loop tab and press update button. Verify that the limits and penalty are within the range.

6. Parameters entered are updated and displayed.

7. In Spectrum PowerCC DNA WebUI, under Volt/Var Control tab, select Close loop > Settings.

7. A new page opens to select the injection point.

Injection	Included	Exclusion time	Exclusion reason
Net-E-Net Companies/KCP/MDTC/WA/161_KV75-1-2-312		12/26/2013 16:51:15	Excluded by default
Net-E-Net Companies/KCP/MDTC/WA/161_KV75-3-4-381		12/26/2013 16:51:15	Excluded by default
Net-E-Net Companies/KCP/MDTC/WA/161_KV75-5-6-381		12/11/2013 13:08:38	Excluded by default
Net-E-Net Companies/KCP/MDTC/WA/161_KV75-7-8-381		12/26/2013 16:51:15	Excluded by default

8. Click on the edit button to include the injection point.

Consideration of injections in closed loop calculation

Injection	Included	Exclusion time	Exclusion reason
/Net-E/Net-Companies/KCP/MIDTOWN/161_JV/75-3-2-IND	<input type="checkbox"/>	12/06/2013 16:51:05	Excluded by default
/Net-E/Net-Companies/KCP/MIDTOWN/161_JV/75-3-4-IND	<input checked="" type="checkbox"/>	12/06/2013 16:51:06	Excluded by default
/Net-E/Net-Companies/KCP/MIDTOWN/161_JV/75-5-6-IND	<input type="checkbox"/>	12/13/2013 13:39:38	Excluded by default
/Net-E/Net-Companies/KCP/MIDTOWN/161_JV/75-7-8-IND	<input type="checkbox"/>	12/06/2013 16:51:05	Excluded by default

8. Now you can select the injection points.

Consideration of injections in closed loop calculation

Injection	Included	Exclusion time	Exclusion reason
/Net-E/Net-Companies/KCP/MIDTOWN/161_JV/75-3-2-IND	<input type="checkbox"/>	12/06/2013 16:51:05	Excluded by default
/Net-E/Net-Companies/KCP/MIDTOWN/161_JV/75-3-4-IND	<input checked="" type="checkbox"/>	12/06/2013 16:51:06	Excluded by default
/Net-E/Net-Companies/KCP/MIDTOWN/161_JV/75-5-6-IND	<input type="checkbox"/>	12/13/2013 13:39:38	Excluded by default
/Net-E/Net-Companies/KCP/MIDTOWN/161_JV/75-7-8-IND	<input type="checkbox"/>	12/06/2013 16:51:05	Excluded by default

9. Select the injection point to include. And press Update.

Consideration of injections in closed loop calculation

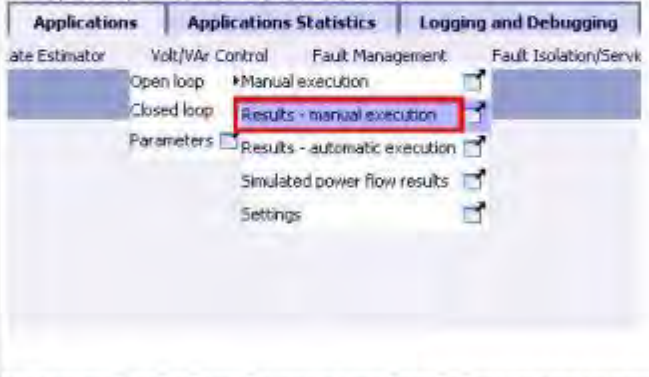
Injection	Included	Exclusion time	Exclusion reason
/Net-E/Net-Companies/KCP/MIDTOWN/161_JV/75-3-2-IND	<input type="checkbox"/>	12/06/2013 16:51:05	Excluded by default
/Net-E/Net-Companies/KCP/MIDTOWN/161_JV/75-3-4-IND	<input checked="" type="checkbox"/>	12/06/2013 16:51:06	Excluded by default
/Net-E/Net-Companies/KCP/MIDTOWN/161_JV/75-5-6-IND	<input type="checkbox"/>	12/13/2013 13:39:38	Excluded by default
/Net-E/Net-Companies/KCP/MIDTOWN/161_JV/75-7-8-IND	<input type="checkbox"/>	12/06/2013 16:51:05	Excluded by default

9. The selected injection point is included in VVC calculation.

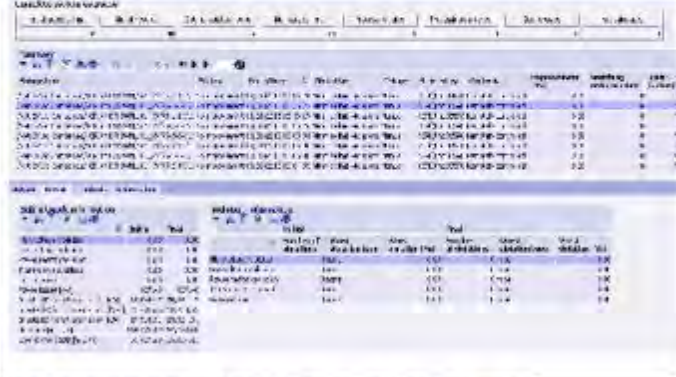
Consideration of injections in closed loop calculation

Injection	Included	Exclusion time	Exclusion reason
/Net-E/Net-Companies/KCP/MIDTOWN/161_JV/75-3-2-IND	<input type="checkbox"/>	12/06/2013 16:51:05	Excluded by default
/Net-E/Net-Companies/KCP/MIDTOWN/161_JV/75-3-4-IND	<input checked="" type="checkbox"/>	12/06/2013 16:51:06	Excluded by default
/Net-E/Net-Companies/KCP/MIDTOWN/161_JV/75-5-6-IND	<input type="checkbox"/>	12/13/2013 13:39:38	Excluded by default
/Net-E/Net-Companies/KCP/MIDTOWN/161_JV/75-7-8-IND	<input type="checkbox"/>	12/06/2013 16:51:05	Excluded by default

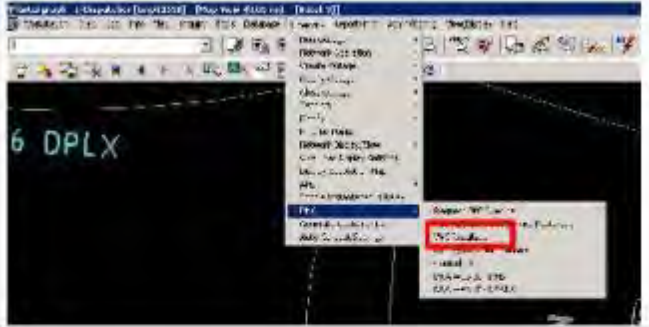
10. In Spectrum PowerCC DNA WebUI, under Volt/Var Control tab, select Open loop > Results – Manual execution.




10. A new window for execution is displayed.

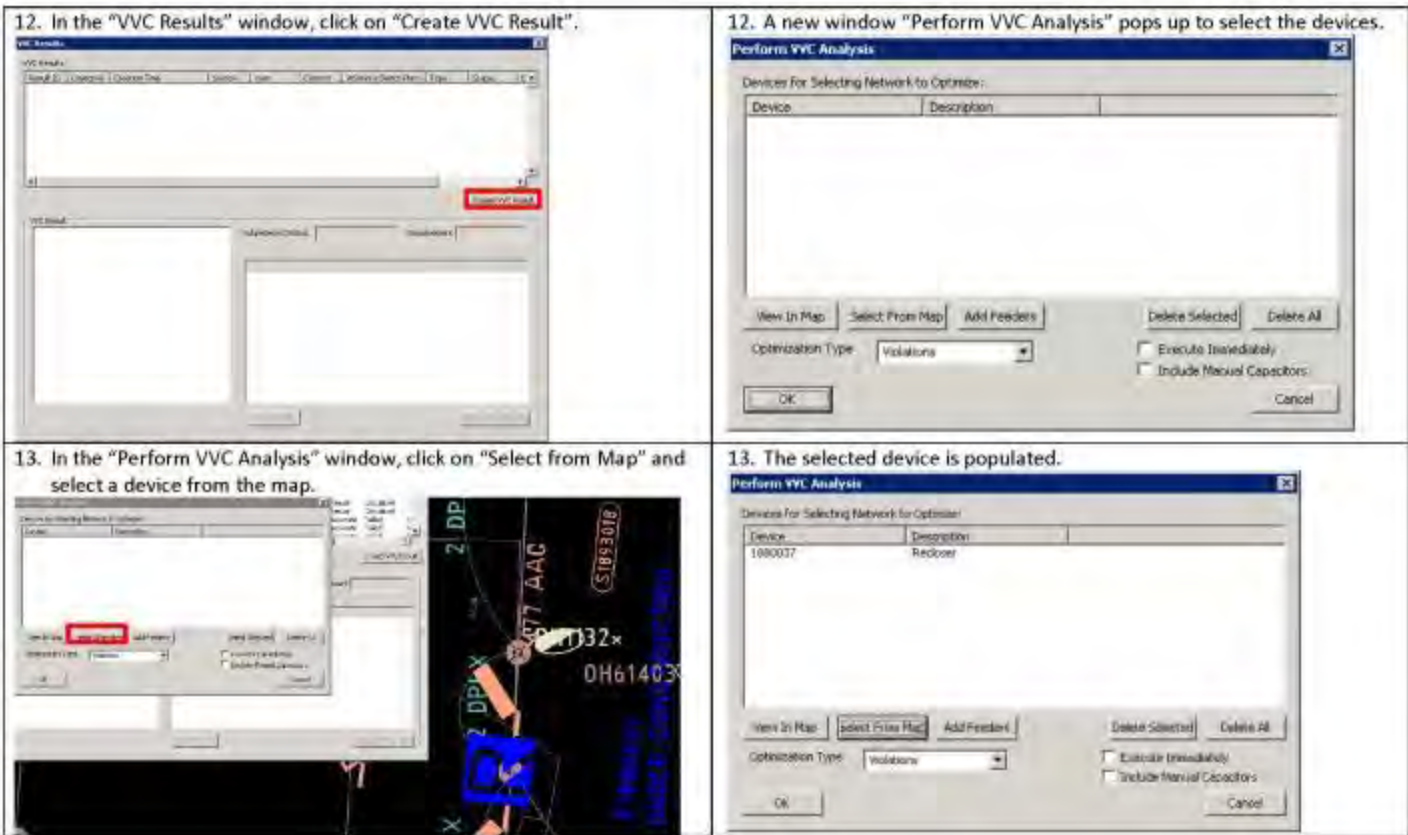


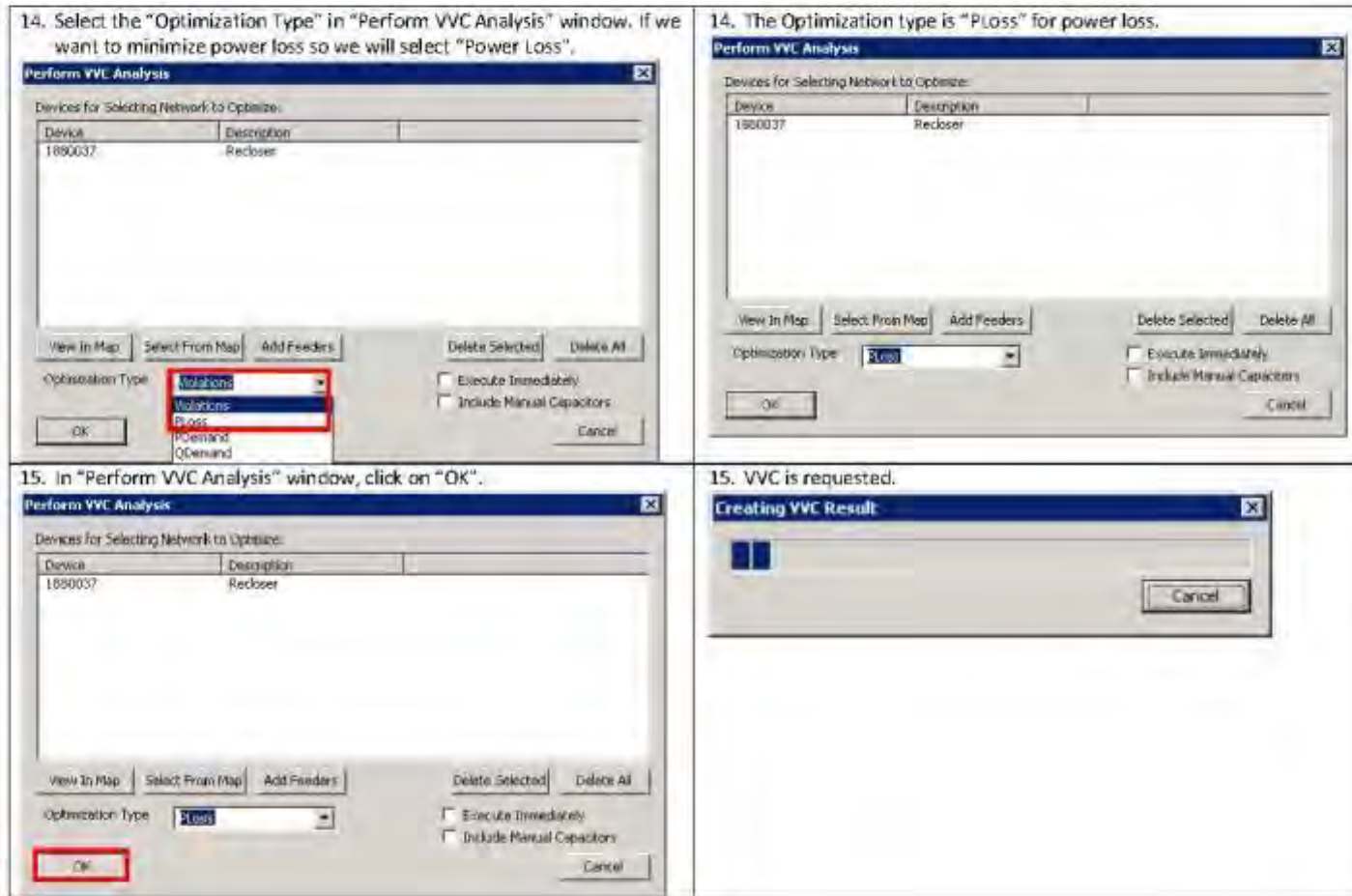
11. Open the OMS I/Dispatcher window. And go to InService > DNA > VVC Results.



11. A new window "VVC Results" pops up to request VVC







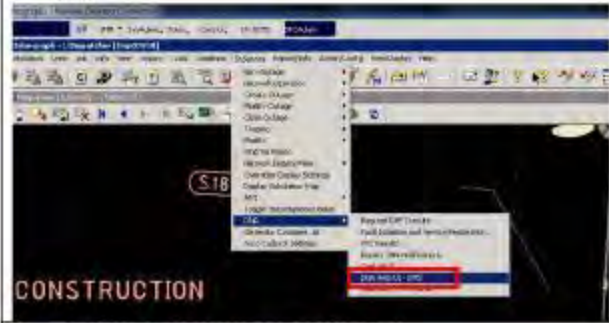





16. Go to the DNA Web UI window, opened with VVC Open Loop Results – Manual Execution and refresh the page.

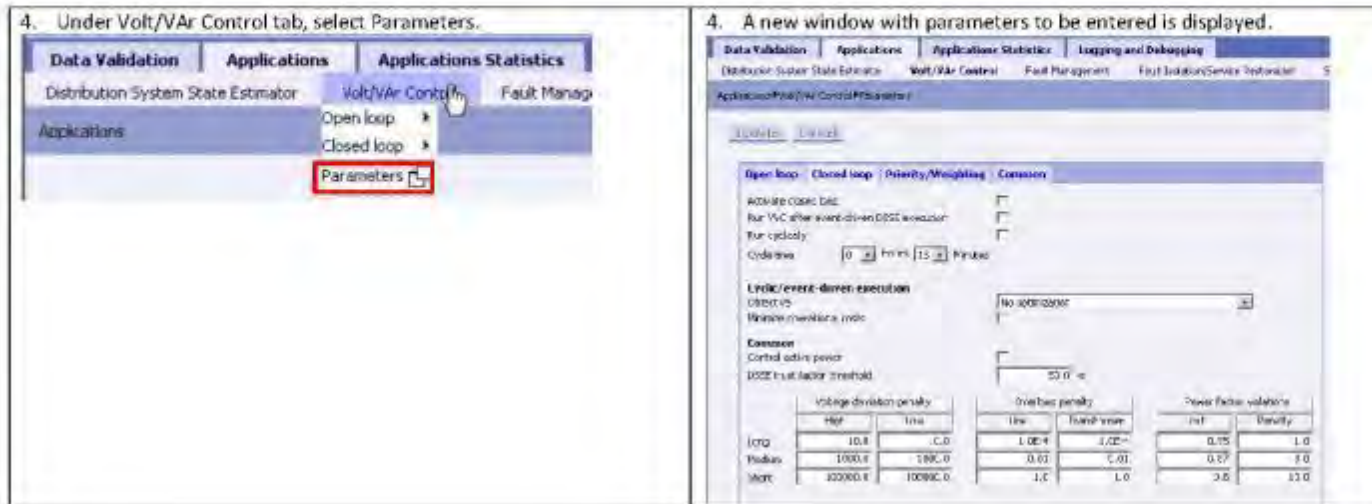
16. The VVC Open Loop Results – Manual Execution page shows the updated VVC result.

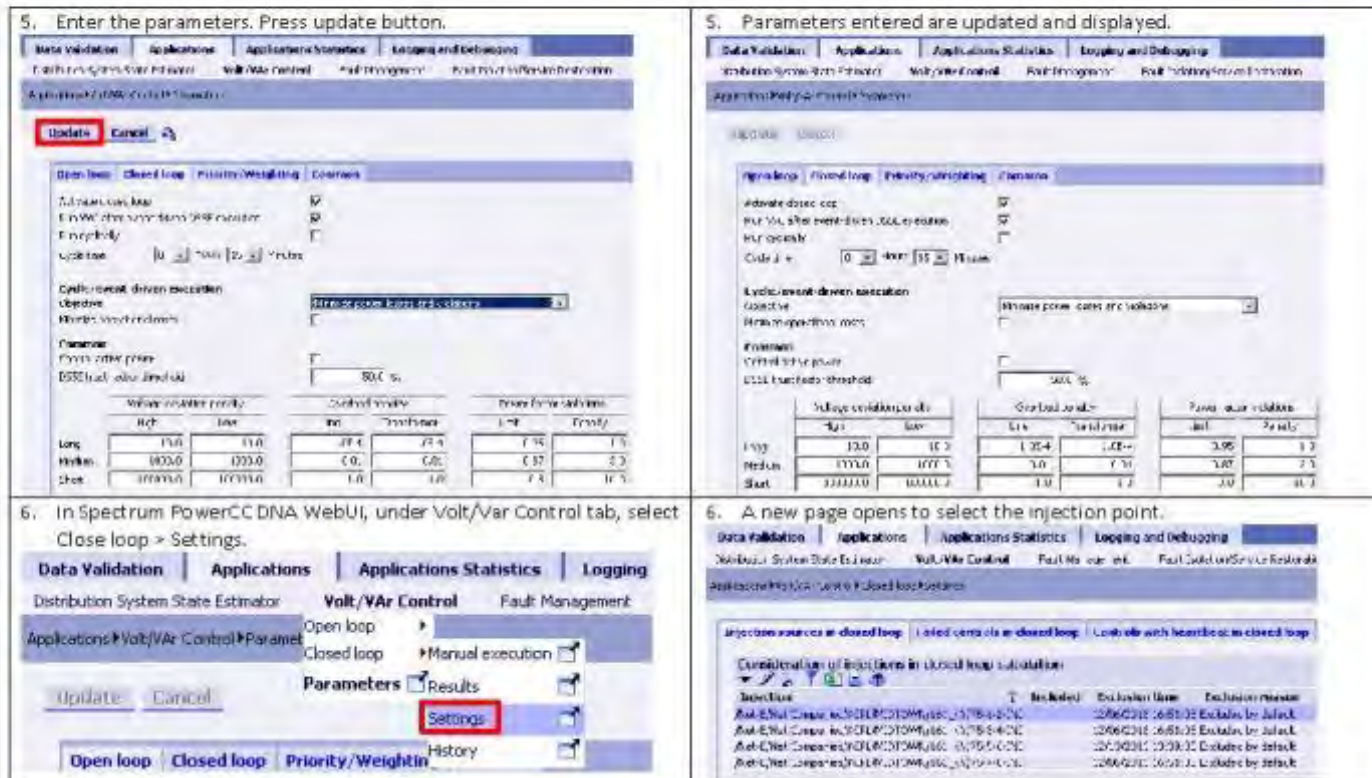
17. In the VVC Open Loop Results – Manual Execution page, go to the details tab. This shows the violations before and after VVC execution.

17. It shows that violations have been decreased after VVC execution.

VVC in Close Loop Mode

Steps	Expected Results
<p>1. Start WebUI from Idispatcher. Go to InService > DNA > DNA WebUI – DMS.</p> 	<p>1. Spectrum PowerCC WebUI opens.</p> 
<p>2. Log in to the Spectrum PowerCC WebUI.</p> 	<p>2. Successfully logged in.</p> 
<p>3. Select "Applications" tab.</p> 	<p>3. The WebUI displays the distribution network applications.</p> 





7. Click on the edit button to include the injection point.

Injection	Included	Exclusion time	Exclusion reason
Net-C/Net-Compans/KCP/MIDTOWN/161_KV75-1-2-IND	<input checked="" type="checkbox"/>	12/06/2013 16:51:05	Excluded by default
Net-C/Net-Compans/KCP/MIDTOWN/161_KV75-3-4-IND	<input type="checkbox"/>	12/06/2013 16:51:05	Excluded by default
Net-C/Net-Compans/KCP/MIDTOWN/161_KV75-5-6-IND	<input type="checkbox"/>	12/13/2013 13:39:38	Excluded by default
Net-C/Net-Compans/KCP/MIDTOWN/161_KV75-7-8-IND	<input type="checkbox"/>	12/06/2013 16:51:05	Excluded by default

7. Now you can select the injection points.

Injection	Included	Exclusion time	Exclusion reason
Net-C/Net-Compans/KCP/MIDTOWN/161_KV75-1-2-IND	<input checked="" type="checkbox"/>	12/06/2013 16:51:05	Excluded by default
Net-C/Net-Compans/KCP/MIDTOWN/161_KV75-3-4-IND	<input type="checkbox"/>	12/06/2013 16:51:05	Excluded by default
Net-C/Net-Compans/KCP/MIDTOWN/161_KV75-5-6-IND	<input type="checkbox"/>	12/13/2013 13:39:38	Excluded by default
Net-C/Net-Compans/KCP/MIDTOWN/161_KV75-7-8-IND	<input type="checkbox"/>	12/06/2013 16:51:05	Excluded by default

8. Select the injection point to include. And press Update.

Injection	Included	Exclusion time	Exclusion reason
Net-C/Net-Compans/KCP/MIDTOWN/161_KV75-1-2-IND	<input checked="" type="checkbox"/>	12/06/2013 16:51:05	Excluded by default
Net-C/Net-Compans/KCP/MIDTOWN/161_KV75-3-4-IND	<input type="checkbox"/>	12/06/2013 16:51:05	Excluded by default
Net-C/Net-Compans/KCP/MIDTOWN/161_KV75-5-6-IND	<input type="checkbox"/>	12/13/2013 13:39:38	Excluded by default
Net-C/Net-Compans/KCP/MIDTOWN/161_KV75-7-8-IND	<input type="checkbox"/>	12/06/2013 16:51:05	Excluded by default

8. The selected injection point is included in VVC calculation.

Injection	Included	Exclusion time	Exclusion reason
Net-C/Net-Compans/KCP/MIDTOWN/161_KV75-1-2-IND	<input checked="" type="checkbox"/>	12/06/2013 16:51:05	Excluded by default
Net-C/Net-Compans/KCP/MIDTOWN/161_KV75-3-4-IND	<input type="checkbox"/>	12/06/2013 16:51:05	Excluded by default
Net-C/Net-Compans/KCP/MIDTOWN/161_KV75-5-6-IND	<input type="checkbox"/>	12/13/2013 13:39:38	Excluded by default
Net-C/Net-Compans/KCP/MIDTOWN/161_KV75-7-8-IND	<input type="checkbox"/>	12/06/2013 16:51:05	Excluded by default

9. In Spectrum PowerCC DNA WebUI, under Volt/Var Control tab, select Close loop > Results.

9. A new window with VVC closed loop results is displayed.

1st Responder Function – Feeder Load Transfer



Feeder Load Transfer in Open Loop or Advisory Mode

Pre-Condition: Overload occurs in one of the feeders in the system.

Steps	Expected Results
1. Log in to the Spectrum PowerCC WebUI. 	1. Successfully logged in. 
2. Select "Applications" tab. 	2. WebUI displays the distribution network applications. 



4. Enter the parameters in Advisory Mode tab and press "update".

Application Preorder Load Transfer Parameters

Update **Cancel**

Advisory mode | Trigger execution | Closed loop mode

Load source: [DSSE] Enable simultaneous supplying from two subsystems

Operation with switches

Operate disconnectors: [yes, under load open first, LBS/CB] Operate fuses: Check capacity of load break switches in branch exchange:

Check overload limits for lines and transformers

Check overload limits in branch exchange: Limit type for line overloads in branch exchange: [Short] Limit type for line overloads in final solution: [Long]

Weighting factors

Line overload: [1.0] Transformer overload: [0.1]

Thresholds

Switching action effect threshold [%]: [0.0] Objective function threshold [%]: [0.0]

4. Updated parameters are displayed.

Application Preorder Load Transfer Parameters

Update **Cancel**

Advisory mode | Trigger execution | Closed loop mode

Load source: [DSSE] Enable simultaneous supplying from two subsystems

Operation with switches

Operate disconnectors: [yes, under load open first, LBS/CB] Operate fuses: Check capacity of load break switches in branch exchange:

Check overload limits for lines and transformers

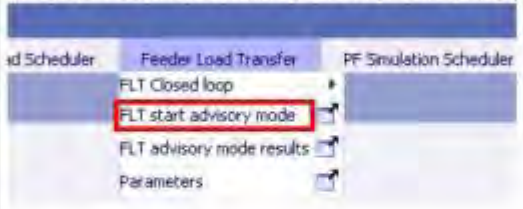



Check overload limits in branch exchange: Limit type for line overloads in branch exchange: [Short] Limit type for line overloads in final solution: [Long]

Weighting factors


Line overload: [1.0] Transformer overload: [0.1]

Thresholds


Switching action effect threshold [%]: [0.0] Objective function threshold [%]: [0.0]

<p>5. Under Feeder Load Transfer, Select FLT start advisory mode</p> 	<p>5. A new page FLT start advisory mode is displayed.</p> 
<p>6. Select the injection source or equipment.</p> 	<p>6. A new window to select system is opened.</p> 


7. Select Net E > Net Companies > KCPL > Midtown > 161kV and select Injection points 75-1-2-INJ, 75-3-4-INJ, 75-5-6-INJ and 75-7-8-INJ. Then click "Find".




7. The Search Results section is populated.

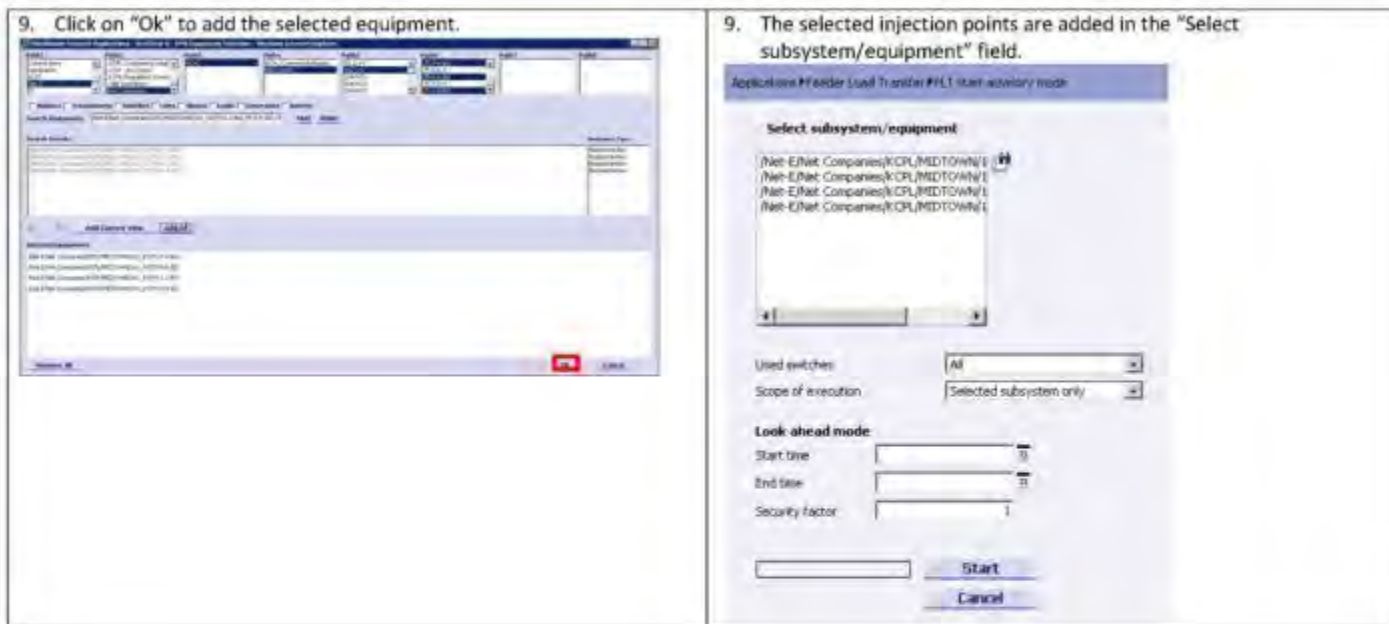


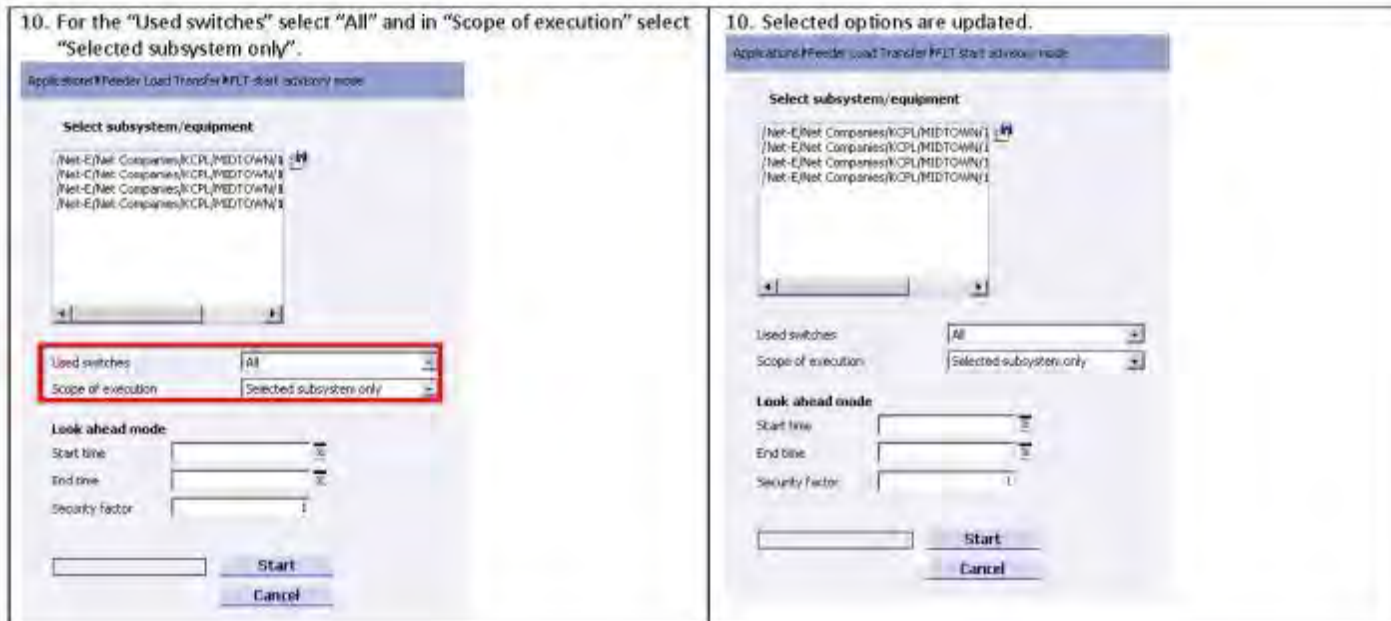
8. Click "Add All".



8. The Selected Equipments section is updated with the added equipment.









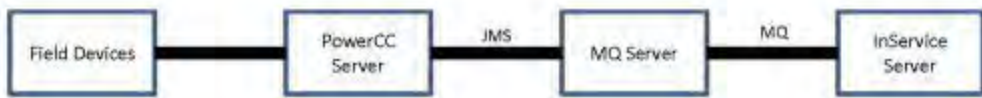
12. Go to the "Violations" tab to see the violations summary.

12. Any violations, if present are displayed.

13. Go to "Initially opened switches" tab.


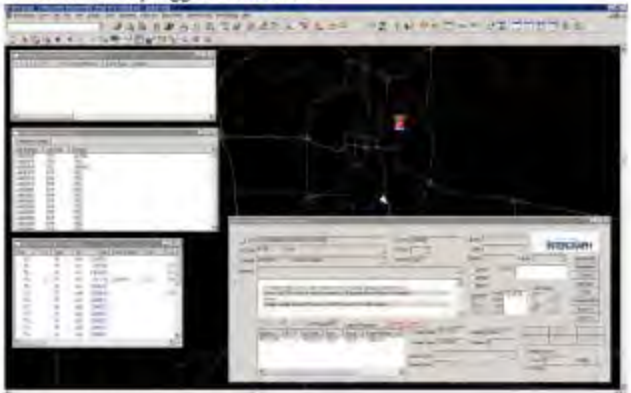
13. Switches used are displayed.

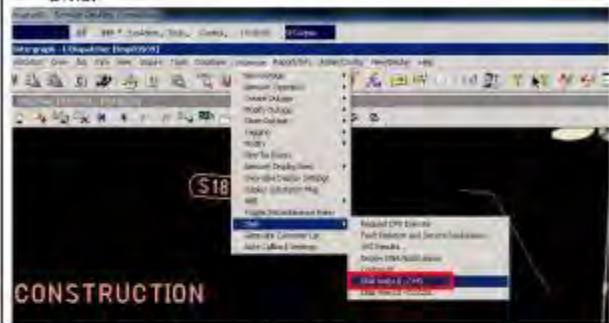

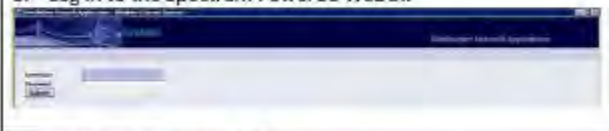

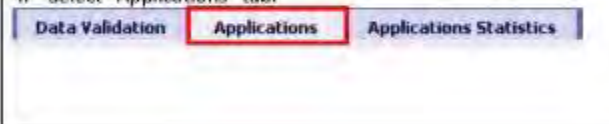

1st Responder Function – Fault Location, Isolation and Service Restoration




FISR Manual Execution in Open Loop Mode

Pre-Condition: A fault occurs in the system.

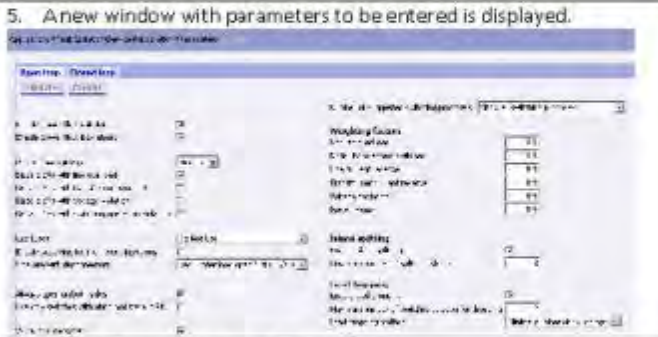
<i>Steps</i>	<i>Expected Results</i>
<p>1. Log in to I/Dispatcher OMS system.</p> 	<p>1. Successfully logged on to OMS.</p> 

<p>2. Start WebUI from IDispatcher. Go to InService > DNA > DNA WebUI – DMS.</p>  A screenshot of the IDispatcher web interface. The 'InService' menu is open, showing a path: InService > DNA > DNA WebUI – DMS. A red box highlights the 'DNA WebUI – DMS' option. A 'CONSTRUCTION' watermark is visible in the bottom left corner.	<p>2. Spectrum PowerCC WebUI opens.</p>  A screenshot of the Spectrum PowerCC WebUI login page. It features a header with the Spectrum logo and 'Spectrum PowerCC' text. Below the header is a large, empty white rectangular area, likely a placeholder for a logo or image.
<p>3. Log in to the Spectrum PowerCC WebUI.</p>  A screenshot of the Spectrum PowerCC WebUI login form. It shows a header with the Spectrum logo and 'Spectrum PowerCC' text. Below the header is a login form with fields for 'Username' and 'Password', and a 'Log In' button.	<p>3. Successfully logged in.</p>  A screenshot of the Spectrum PowerCC WebUI dashboard after successful login. The dashboard displays a header with the Spectrum logo and 'Spectrum PowerCC' text. Below the header is a navigation menu with tabs for 'Data Validation', 'Applications', and 'Applications Statistics'. The 'Applications' tab is selected.
<p>4. Select "Applications" tab.</p>  A screenshot of the Spectrum PowerCC WebUI navigation tabs. The tabs are 'Data Validation', 'Applications', and 'Applications Statistics'. The 'Applications' tab is highlighted with a red box.	<p>4. WebUI displays the distribution network applications.</p>  A screenshot of the Spectrum PowerCC WebUI distribution network applications. The dashboard displays a header with the Spectrum logo and 'Spectrum PowerCC' text. Below the header is a navigation menu with tabs for 'Data Validation', 'Applications', and 'Applications Statistics'. The 'Applications' tab is selected. Below the tabs, there are three sub-tabs: 'Distribution System State Estimator', 'Volt/VAr Control', and 'Fault Management'. The 'Applications' sub-tab is selected.

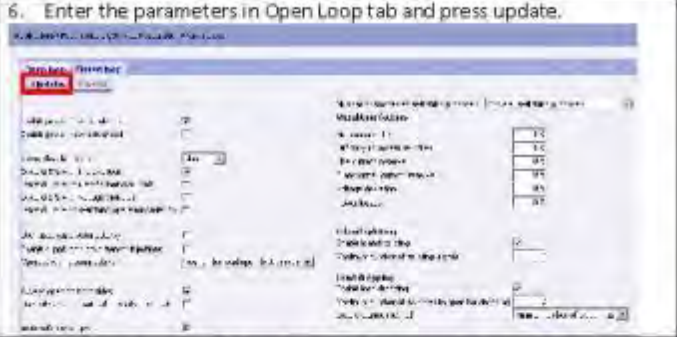
5. Under Fault Isolation/Service Restoration, select Parameters.



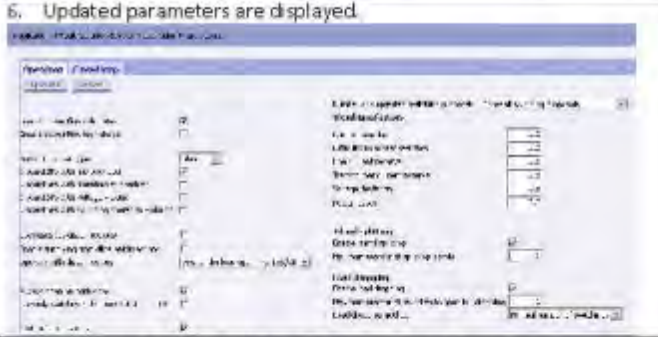
5. A new window with parameters to be entered is displayed.




6. Enter the parameters in Open Loop tab and press update.




6. Updated parameters are displayed.

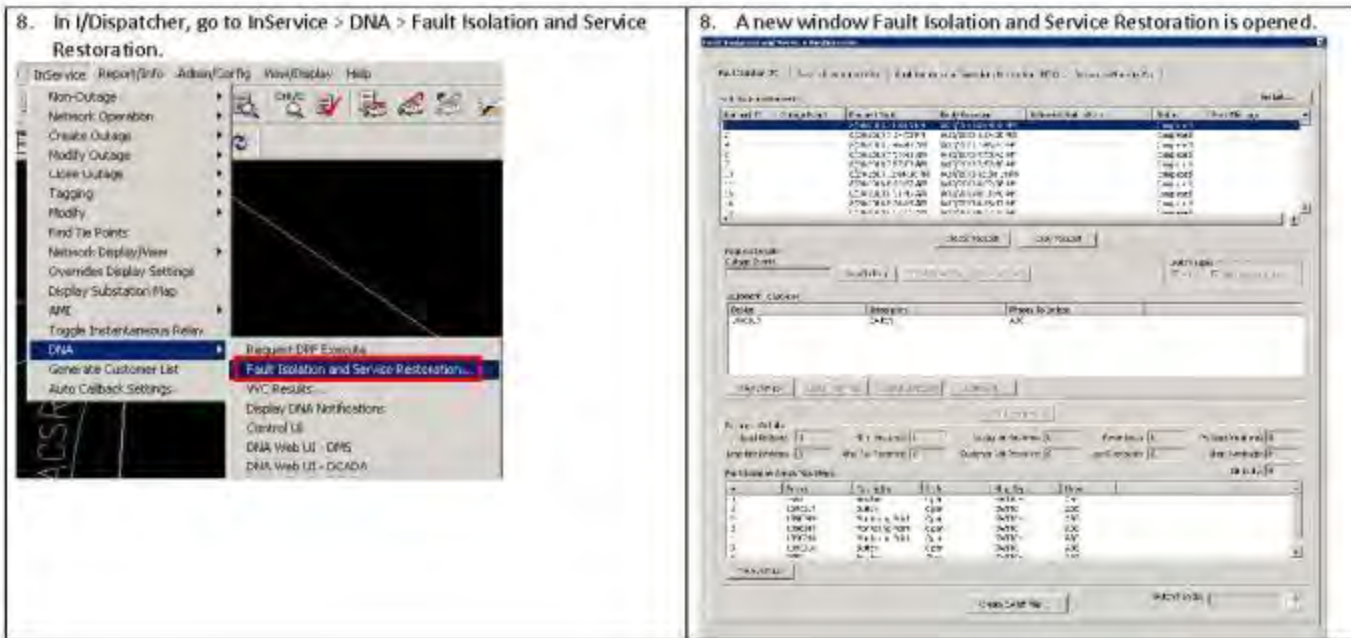


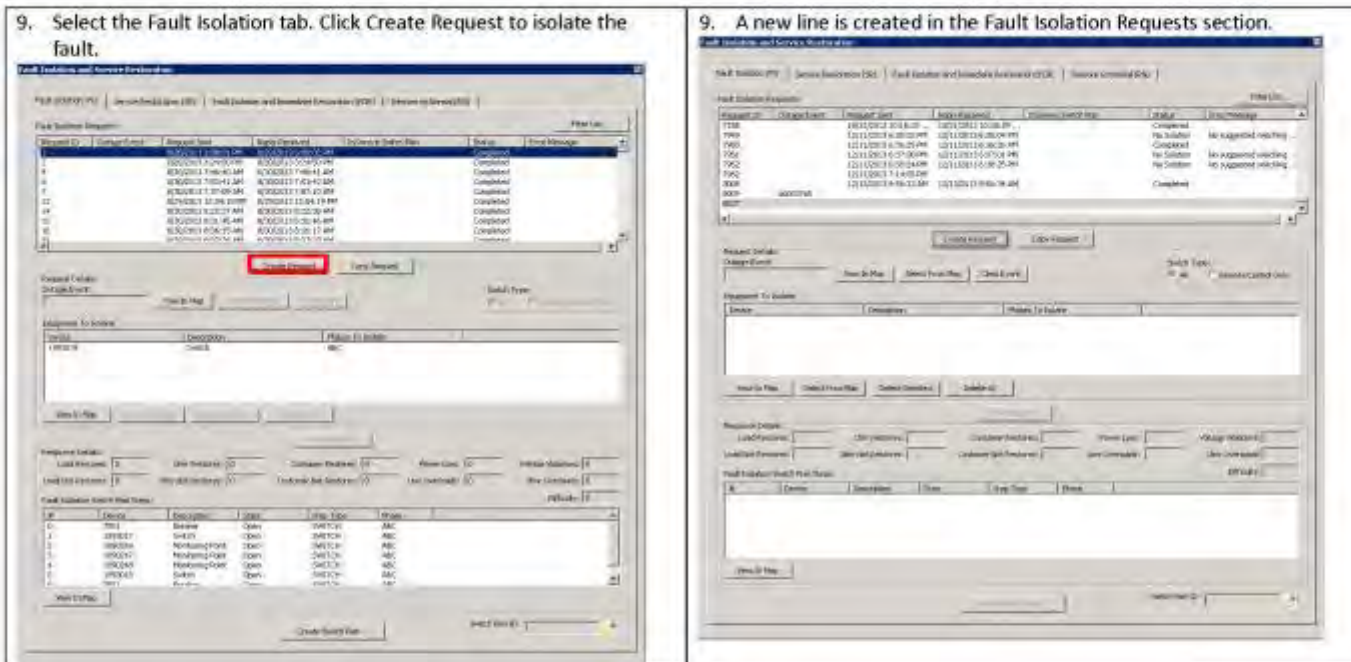
7. Go to Applications tab and in Fault Management tab, select Faults Overview.



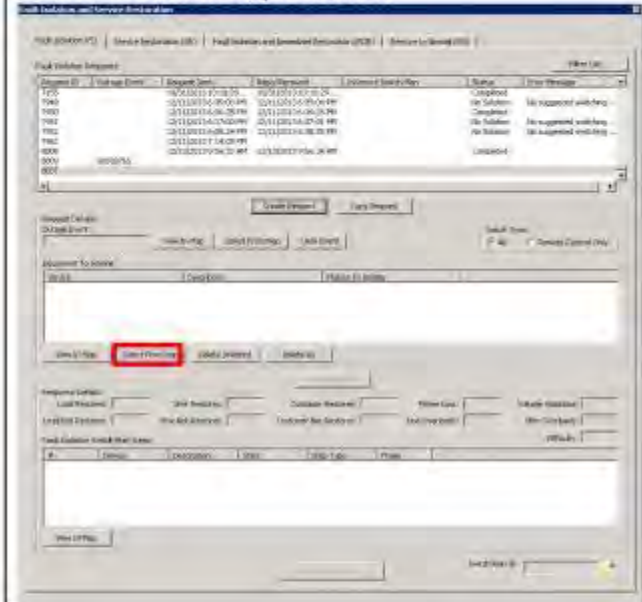
7. A page opens with the latest faults in the system.








10. In the Equipment to Isolation section, click Select from Map to select the device from the map for isolation.




Equipment ID	Equipment Name	Equipment Location	Equipment Status	Equipment Type
1750	10/21/2011 17:18:39	10/21/2011 17:18:39	Unassigned	
1760	10/21/2011 17:18:39	10/21/2011 17:18:39	Unassigned	Unassigned switching
1780	10/21/2011 17:18:39	10/21/2011 17:18:39	Completed	
1782	10/21/2011 17:18:39	10/21/2011 17:18:39	Unassigned	Unassigned switching
1784	10/21/2011 17:18:39	10/21/2011 17:18:39	Unassigned	Unassigned switching
1800	10/21/2011 17:18:39	10/21/2011 17:18:39	Unassigned	
1802	10/21/2011 17:18:39	10/21/2011 17:18:39	Unassigned	

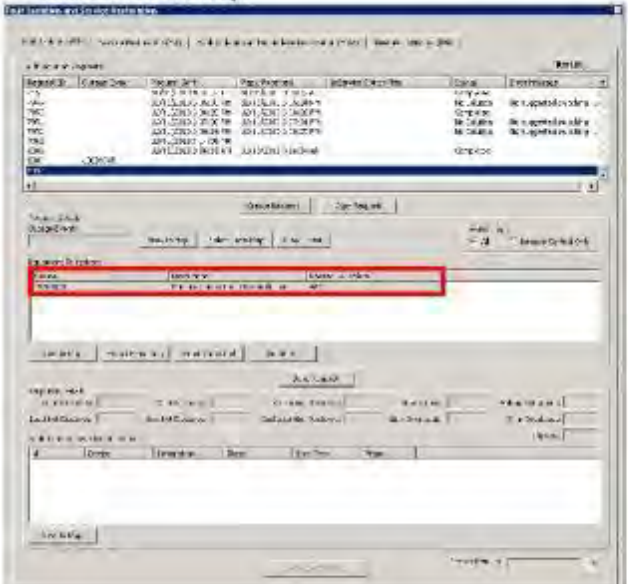
10. In I/Dispatcher map, select the equipment to isolate.



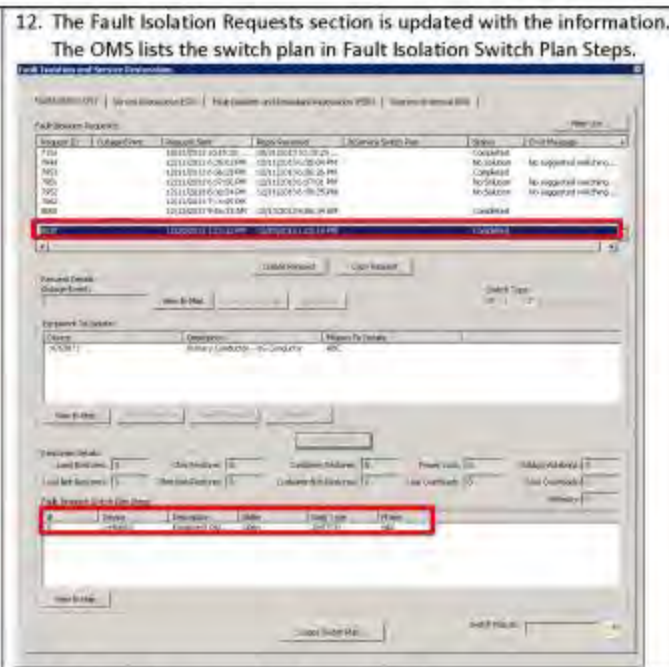
11. Double click the device/line from the map.



11. The Equipment to isolate section is populated with the device selected from the map.

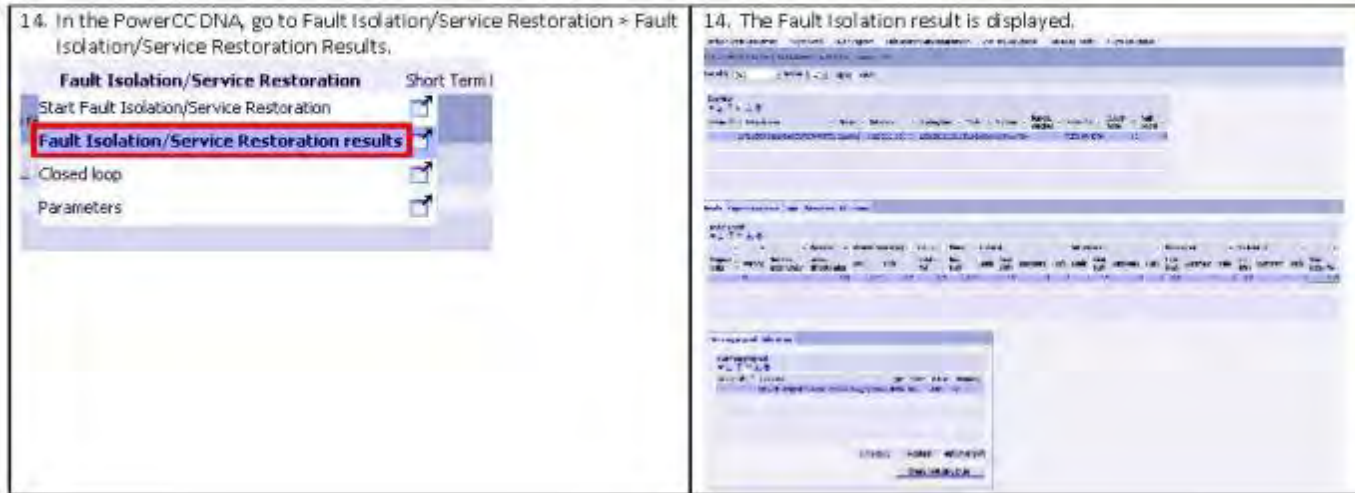


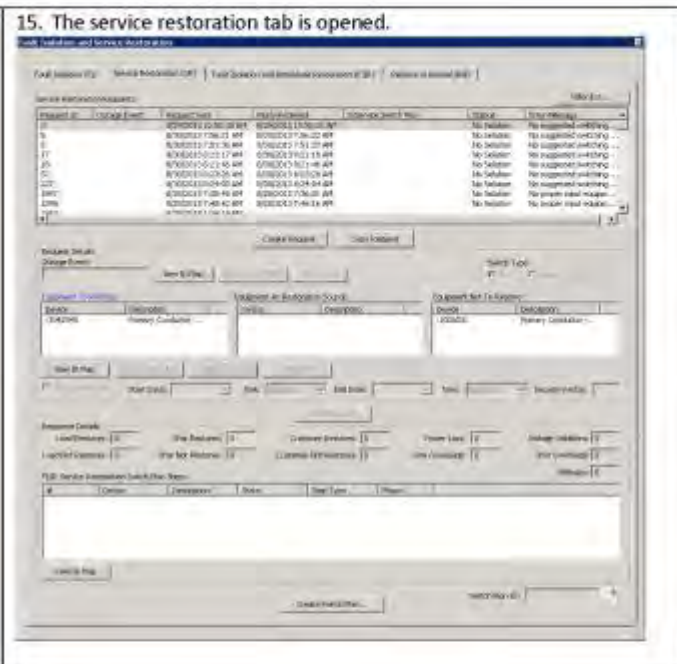
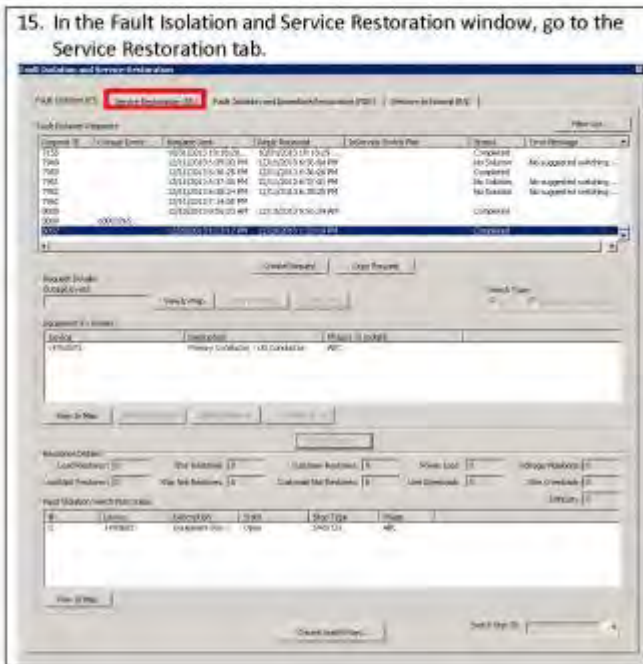
Equipment ID	Equipment Name	Equipment Type	Equipment Description	Status	Equipment Location
001	001	001	001	001	001
002	002	002	002	002	002
003	003	003	003	003	003
004	004	004	004	004	004
005	005	005	005	005	005
006	006	006	006	006	006
007	007	007	007	007	007
008	008	008	008	008	008
009	009	009	009	009	009
010	010	010	010	010	010

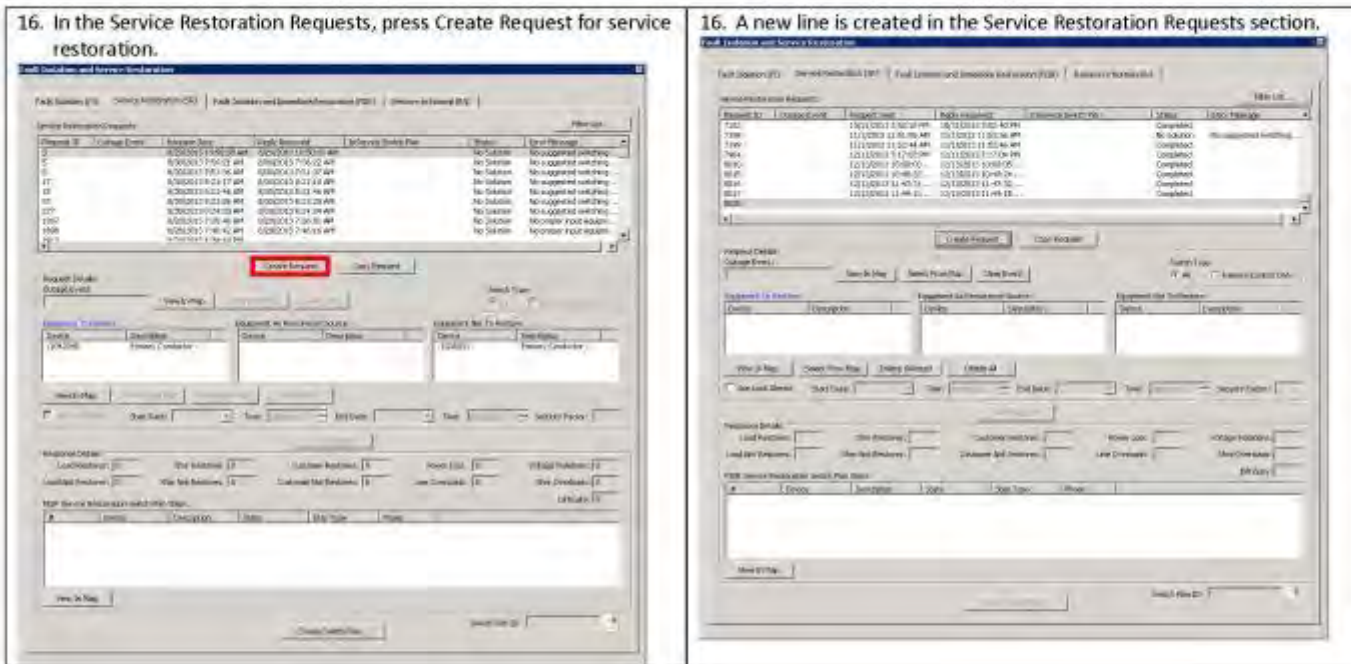


13. The switch plan is executed manually.

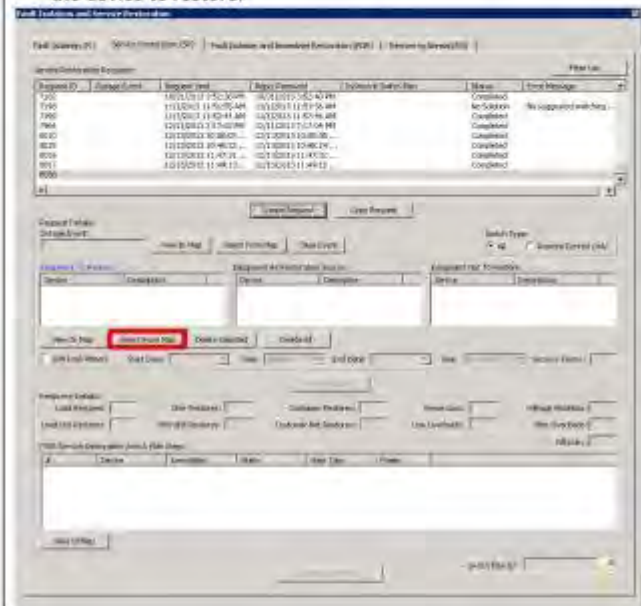
13. The device/equipment has been isolated.





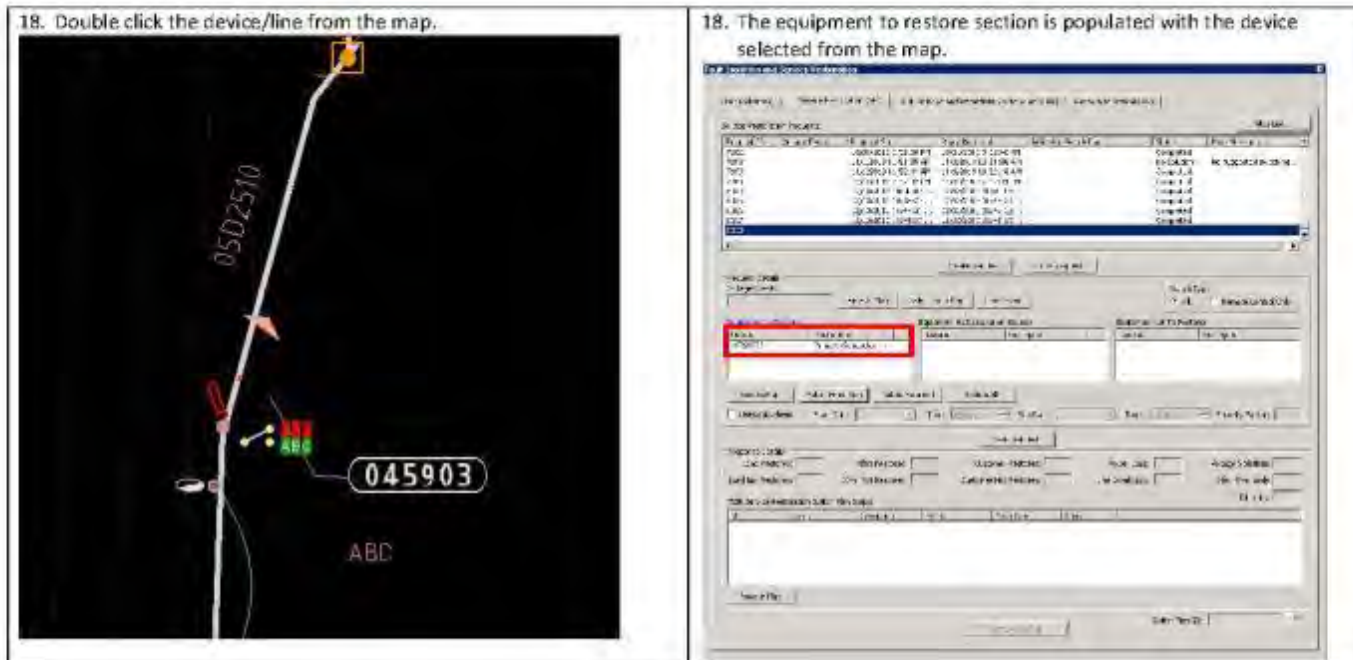


17. In the Equipment to Restore section, click Select from Map to select the device to restore.

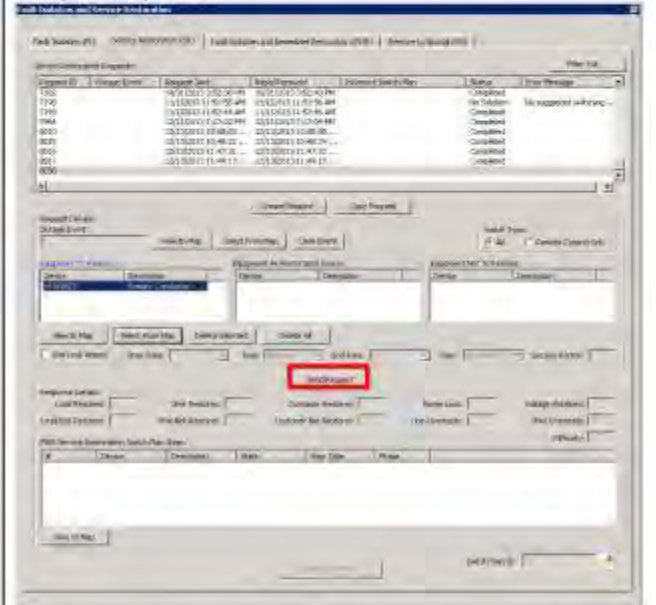


17. In I/Dispatcher map select the device to be restored.



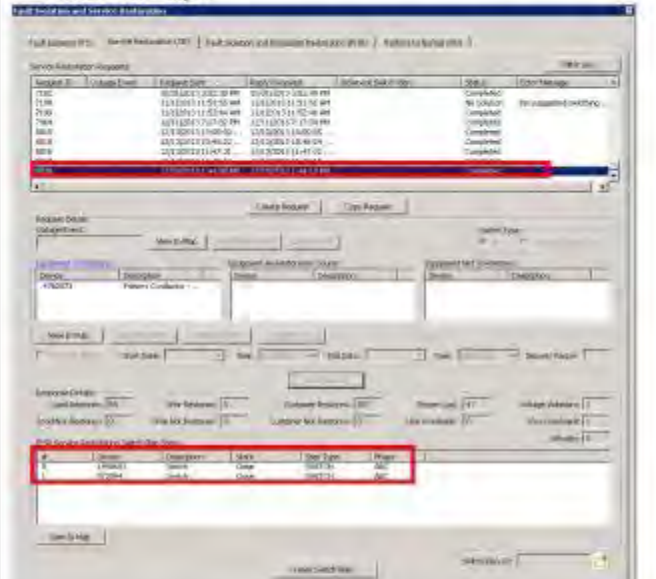


19. Select the device selected to restore and click Send Request for the system to process.



20. The Service Restoration switch plan is executed manually.

19. The Service Restoration Requests is filled with the information and status "Completed", It lists the switch plan in Service Restoration Switch Plan Steps.



20. Service is restored to the devices.





Outage and Restoration Events




Outage event

Precondition: MFR within SmartMeter detects a sustained voltage loss for more than 30 seconds and generates an outage event.


Meter ID: 1284810711062

<i>Steps</i>	<i>Expected Results</i>
<ol style="list-style-type: none"> SmartMeter loses power for more than 30 seconds. Log in to Gridstream Command Center to verify that meter has sent outage event to AHE. 	<ol style="list-style-type: none"> Meter doesn't have power. Successfully logged in to the Gridstream Command Center. 


3. In the Search box, type in the meter ID 1284810711062.




3. A new page opens with Gridstream RF Endpoint Information of the meter ID.








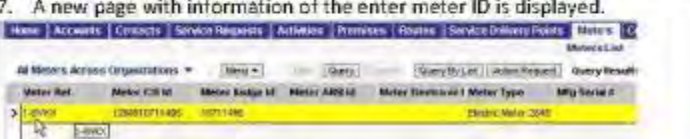

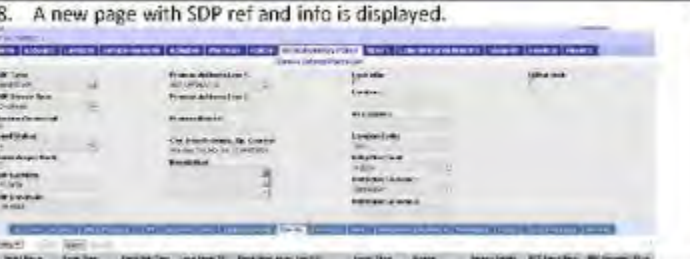
4. Click on the "History" tab to view the outages.




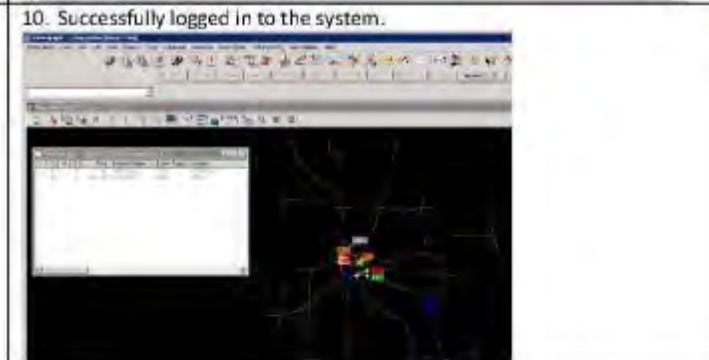


4. The window shows the status and outage event of the meter.

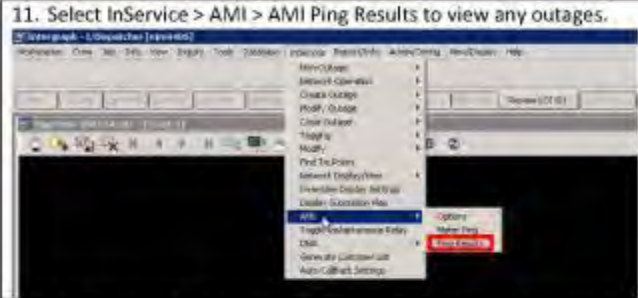


Event	Description	Occurred	Collector
Endpoint Power Outage	Power outage on serial number 4028145549	8/29/2012 4:49 PM	RF GAP Collector
Endpoint Power Restore	Power restore on serial number 4028145549	8/29/2012 5:08 AM	RF GAP Collector
Endpoint Power Outage	Power outage on meter number 4028145549	8/29/2012 5:18 AM	RF GAP Collector
Endpoint Power Restore	Power restore on meter number 4028145549	8/29/2012 5:08 PM	RF GAP Collector
Endpoint Power Outage	Power outage on serial number 4028145549	8/29/2012 5:57 PM	RF GAP Collector
Endpoint Power Restore	Power restore on serial number 4028145549	8/29/2012 5:59 PM	RF GAP Collector


<p>5. Log in to the MDM.</p> 	<p>5. Successful log in to the system.</p> 
<p>6. Select the "Meters" tab to search for Meter ID.</p> 	<p>6. A new page is opened to enter the Meter ID.</p> 
<p>7. Enter the meter ID 1284810711062 in Meter CIS Id column.</p> 	<p>7. A new page with information of the enter meter ID is displayed.</p> 
<p>8. Select the Service Delivery Points tab.</p> 	<p>8. A new page with SDP ref and info is displayed.</p> 

<p>9. Select the events tab.</p> 	<p>9. A new page with meter outage event in the entered meter ID is displayed.</p> 
<p>10. Log in to IDispatcher OMS system.</p> 	<p>10. Successfully logged in to the system.</p> 

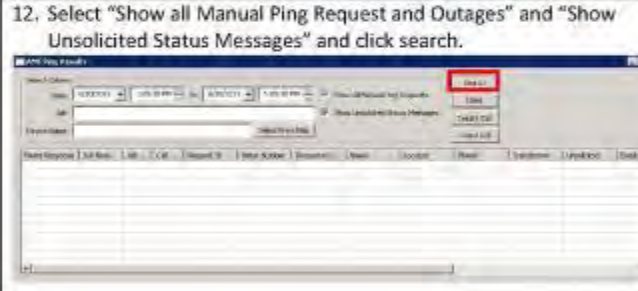
11. Select InService > AMI > AMI Ping Results to view any outages.



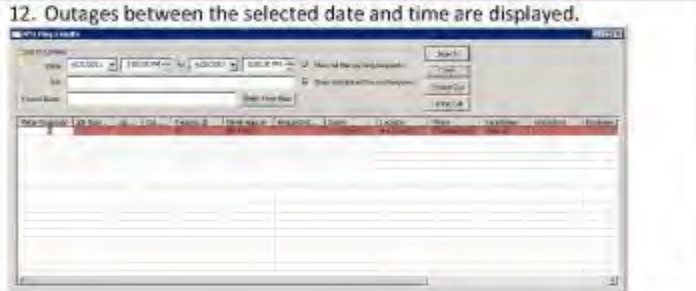
11. AMI Ping Results window pops open.



12. Select "Show all Manual Ping Request and Outages" and "Show Unsolicited Status Messages" and click search.



12. Outages between the selected date and time are displayed.





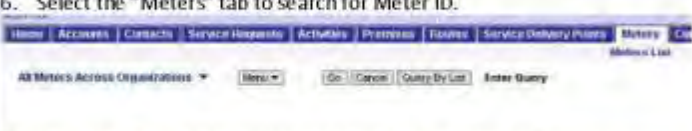

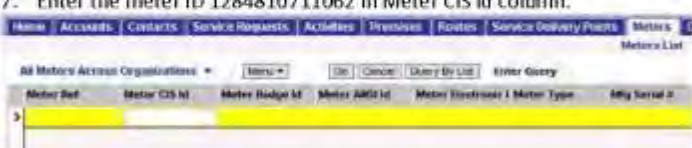
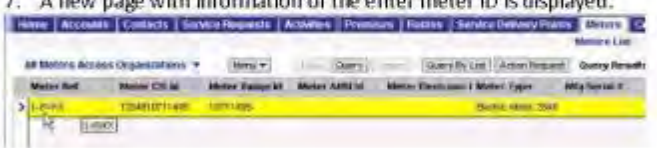


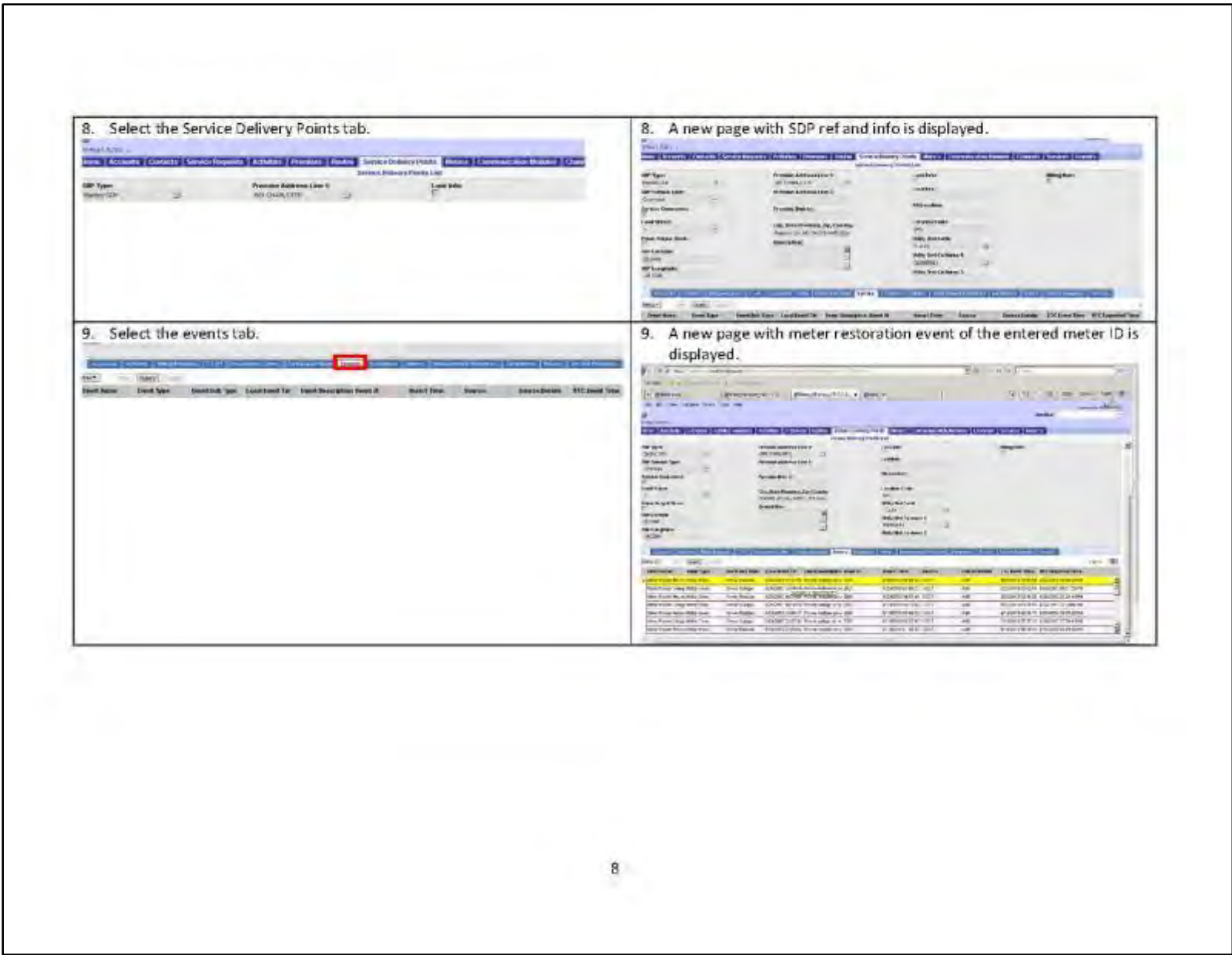
Restoration Event

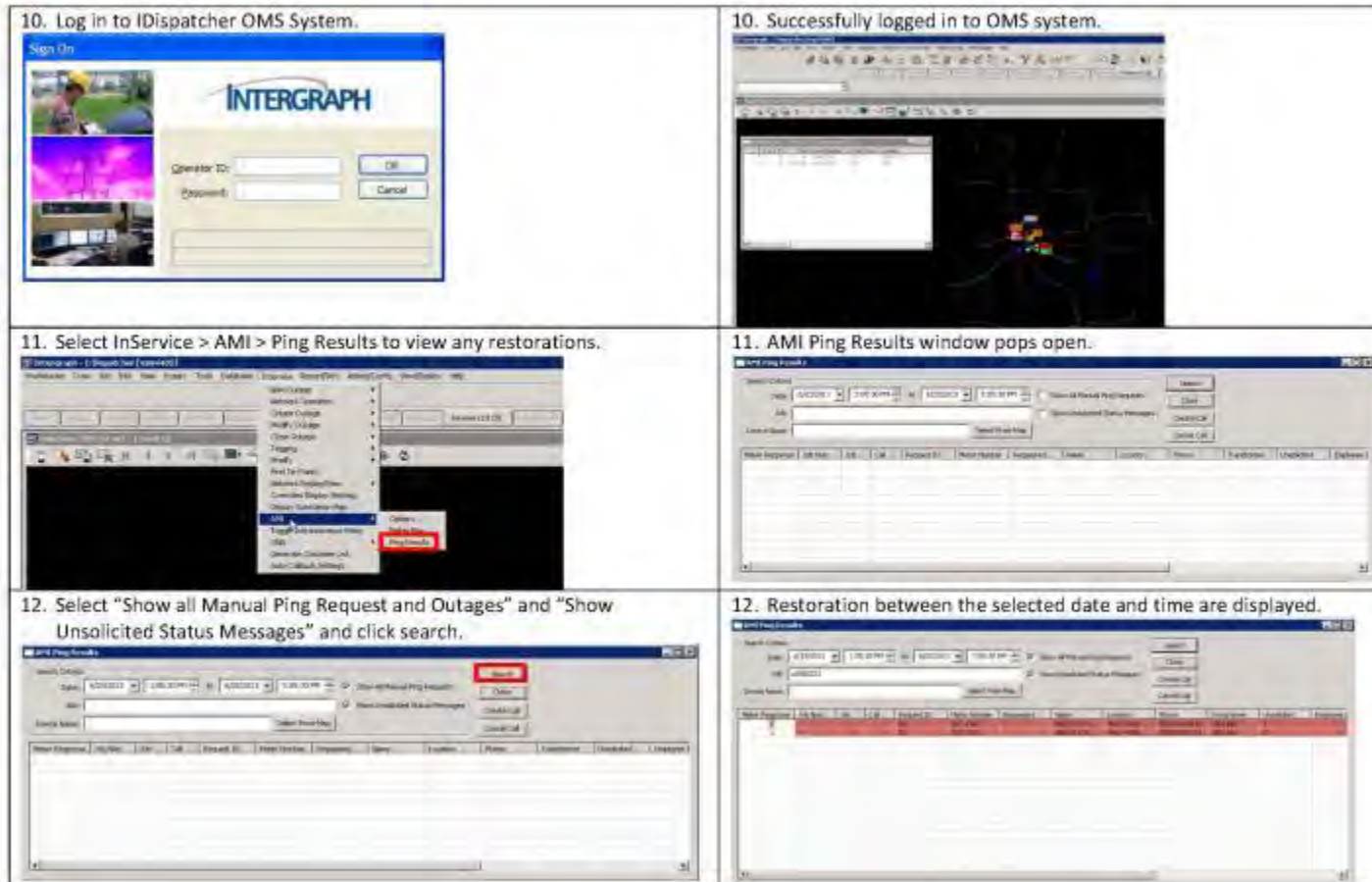
Precondition: MFR within SmartMeter detects a power restoration event following an outage and generates a restoration event.

Meter ID: 1284810711062

Steps	Expected Results										
<p>1. SmartMeter restores power.</p> <p>2. Log in to Gridstream Command Center to verify that meter has sent restoration event to AHE.</p> 	<p>1. Meter has power restored to it.</p> <p>2. Successfully logged in to the Gridstream Command Center.</p> 										
<p>3. In the Search box, type in the meter ID 1284810711062.</p> 	<p>3. A new page opens with Gridstream RF Endpoint Information of the meter ID.</p>  <table border="1"> <caption>Gridstream RF Endpoint Information</caption> <thead> <tr> <th>Parameter</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Switch State</td> <td>Completed</td> </tr> <tr> <td>Number of Meters</td> <td>1</td> </tr> <tr> <td>Mobile Firmware Version</td> <td>23.137-07.35</td> </tr> <tr> <td>Total Programmed</td> <td>23.141-003 8197.00</td> </tr> </tbody> </table>	Parameter	Value	Switch State	Completed	Number of Meters	1	Mobile Firmware Version	23.137-07.35	Total Programmed	23.141-003 8197.00
Parameter	Value										
Switch State	Completed										
Number of Meters	1										
Mobile Firmware Version	23.137-07.35										
Total Programmed	23.141-003 8197.00										

<p>4. Click on the "History" tab to view the restorations.</p> 	<p>4. The window shows the status and restoration event of the meter.</p> 
<p>5. Log in to the MDM.</p> 	<p>5. Successful log in to the system.</p> 
<p>6. Select the "Meters" tab to search for Meter ID.</p> 	<p>6. A new page is opened to enter the Meter ID.</p> 
<p>7. Enter the meter ID 1284810711062 in Meter CIS Id column.</p> 	<p>7. A new page with information of the enter meter ID is displayed.</p> 


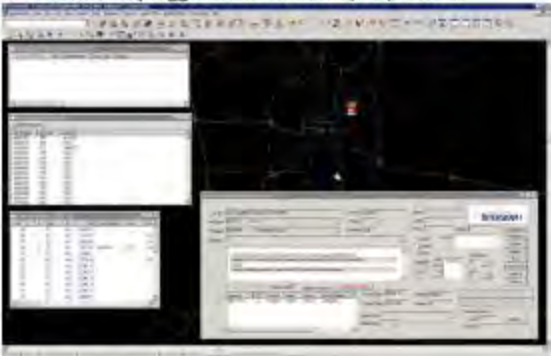




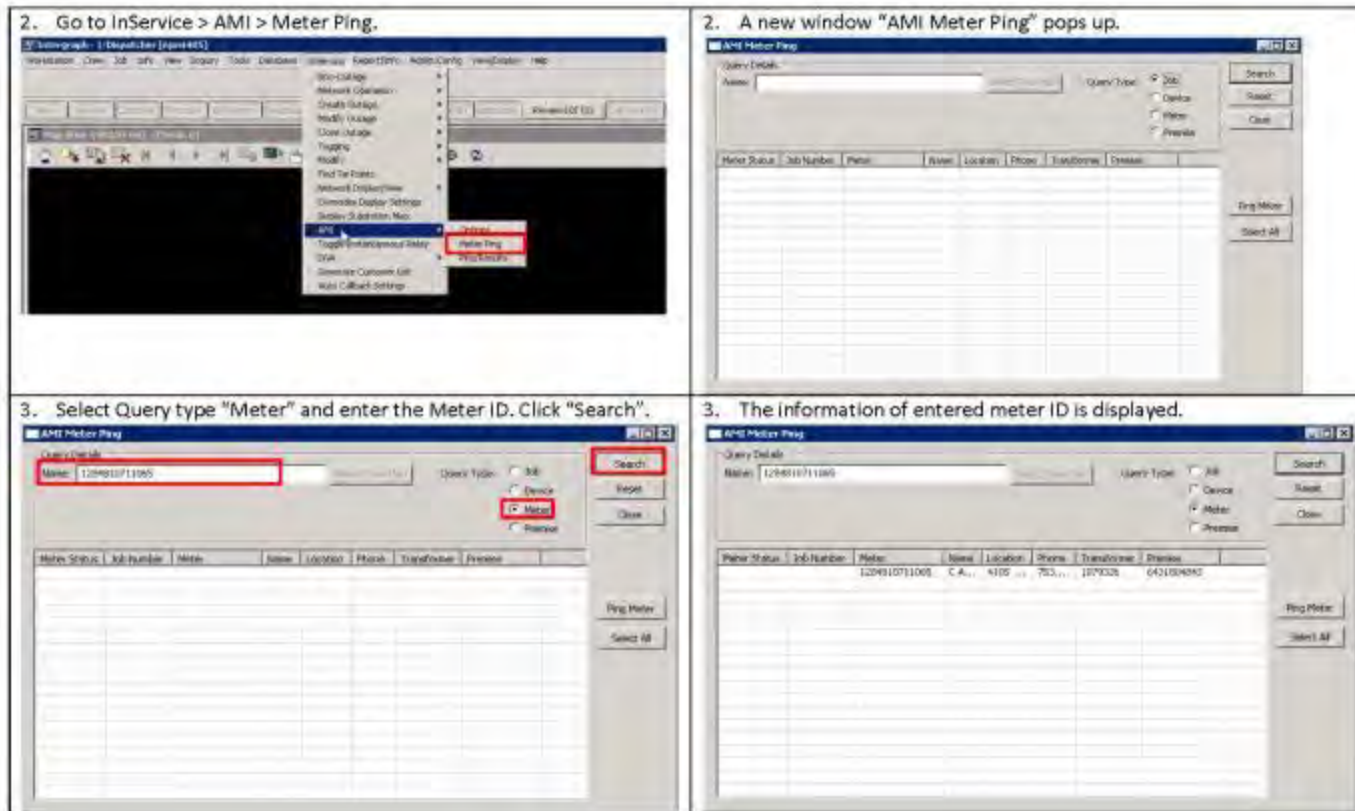
Power Status Verification

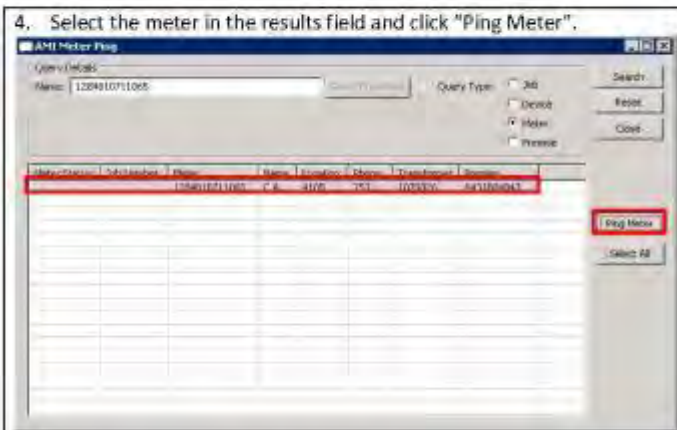


Power Status Verification

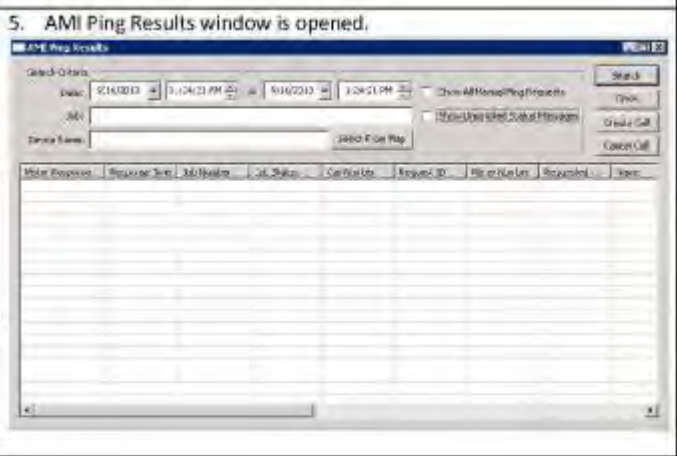
Steps	Expected Results
<p>1. Log in to the OMS I/Dispatcher.</p> 	<p>1. Successfully logged in to the OMS I/Dispatcher.</p> 

1






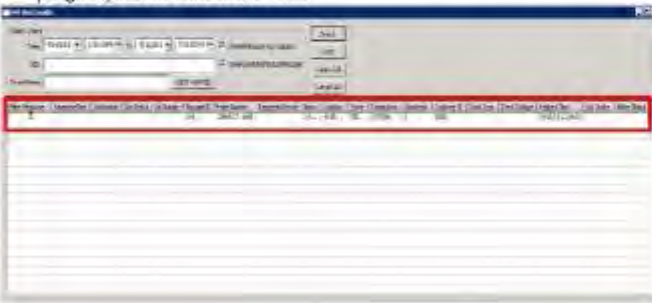
4. The meter ping request is sent to meter via MDM/AHE.




6. Select the Date and Time and check "Show All Manual Ping Request" and "Show Unsolicited Status Messages" and click Search.




6. The Meter Ping Request is displayed in the AMI Ping Results window. The "Hour Glass" in Meter Response column represents that meter ping request is sent from OMS.




7. Log in to MDM to check Power Status Verification.




7. Successfully logged in to the MDM.



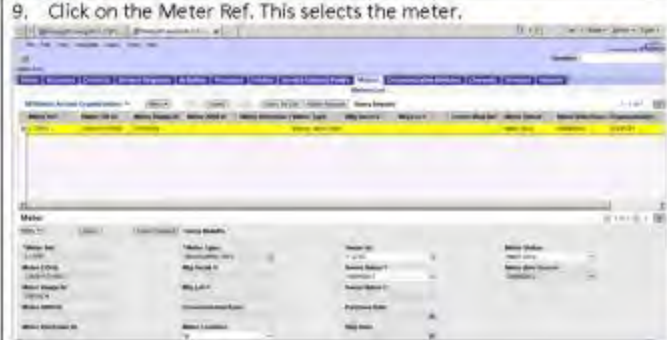
8. Select the "Meters" tab and enter meter number 1284810711065 in Meter CIS id column. Click "Go" to execute the query.




8. The page refreshes with information of the enter meter ID is displayed.







9. Click on the Meter Ref. This selects the meter.



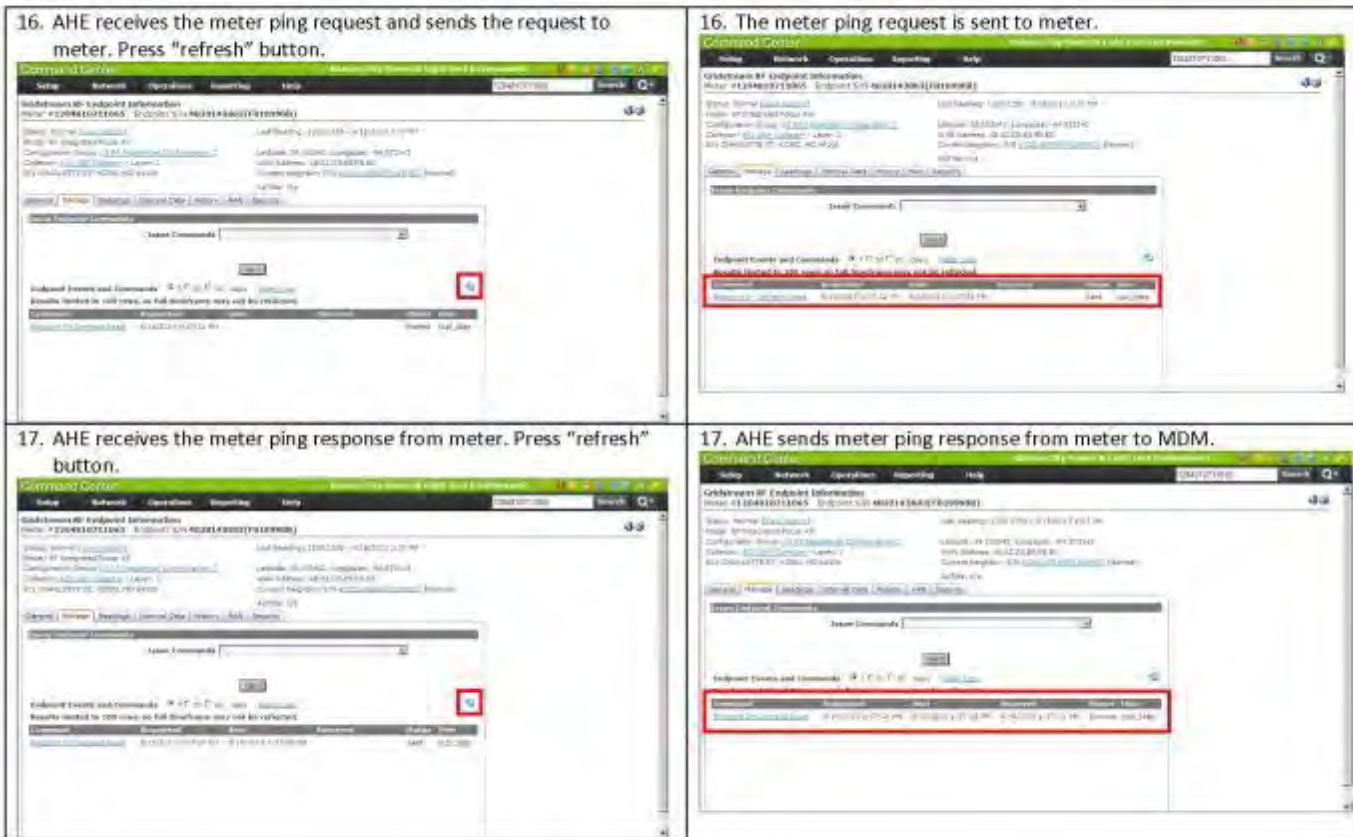
9. The page displays the detailed information on that meter.

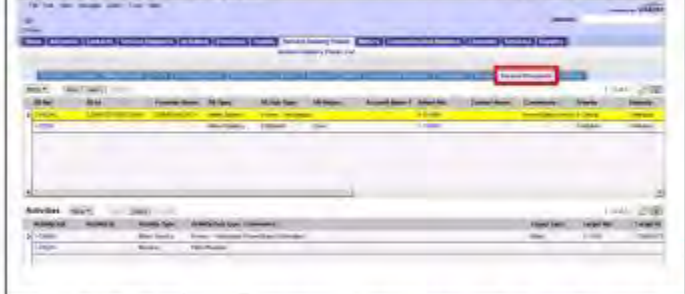
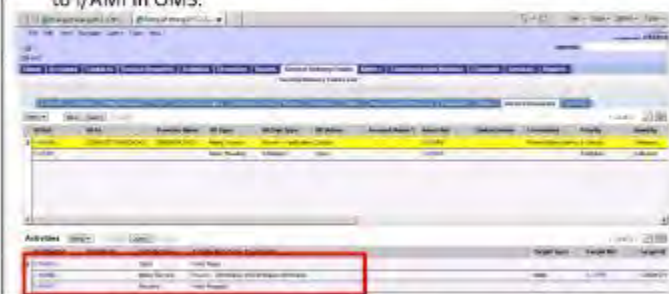
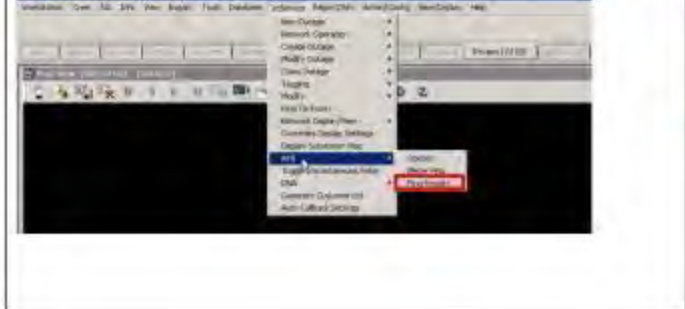
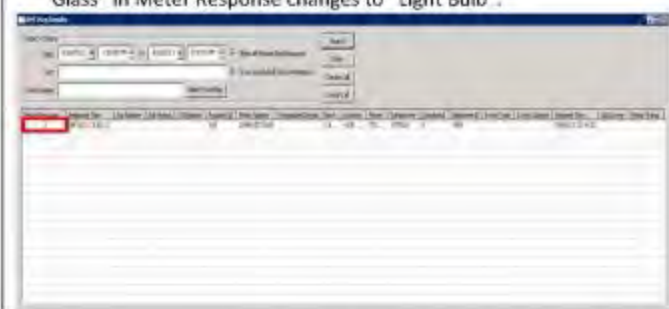


<p>10. Select the "Service Delivery Points" tab. This is the "Meter level service delivery point".</p> 	<p>10. The page displays the SDP ID of the entered meter number.</p> 
<p>11. Select the SDP Ref of the meter to navigate to Service Delivery Points List.</p> 	<p>11. The SDP info of the entered meter is displayed.</p> 

<p>12. Select the "Service Requests" tab.</p> 	<p>12. This displays the PSV request with the transaction level details in the "Activities" portion of the view.</p> 
<p>13. Log in to AHE Command Center.</p> 	<p>13. Successfully logged in to the AHE.</p> 






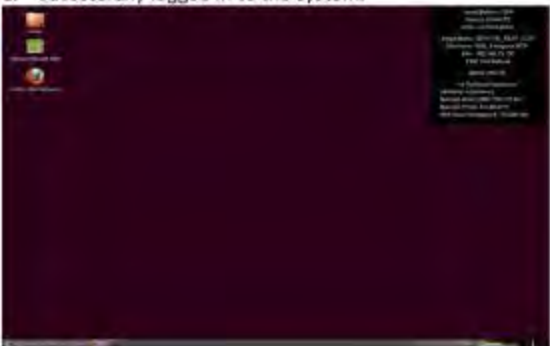
<p>18. In the MDM, navigate to Service Delivery Points > Service Requests.</p>  A screenshot of the MDM (Master Data Management) interface. The page title is "Service Requests". It shows a list of service requests with columns for ID, Name, Status, and Date. A red box highlights a specific entry in the list.	<p>18. The PSV message received from AHE is processed by MDM and sent to I/AMI in OMS.</p>  A screenshot of the MDM interface showing the "I/AMI" (Interim/Advanced Metering Interface) section. It displays a list of data points or messages. A red box highlights a specific entry in the list.
<p>19. In the OMS I/Dispatcher, go to InService > AMI > Ping Results.</p>  A screenshot of the OMS I/Dispatcher interface. The "InService" menu is open, showing options like "AMI", "Ping Results", and "Meter Response". A red box highlights the "AMI" option.	<p>19. "AMI Ping Results" is populated with Ping Response, the "Hour Glass" in Meter Response changes to "Light Bulb".</p>  A screenshot of the OMS I/Dispatcher interface showing the "AMI Ping Results" page. It displays a table of ping results with columns for ID, Name, Status, and Date. A red box highlights a specific entry in the table.

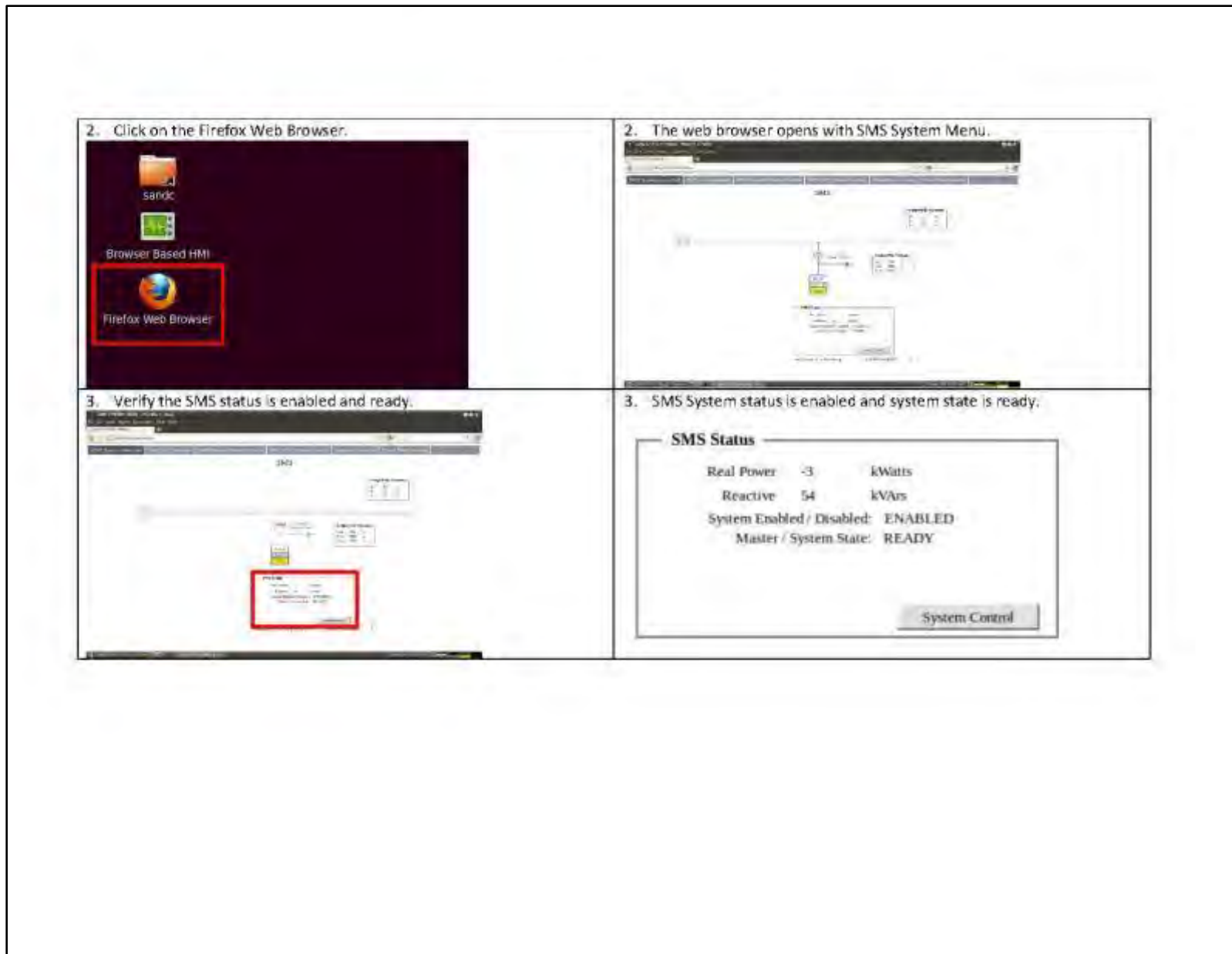
Battery Grid Operation – Local Control (Discharge)




Local Control – Battery Discharging in Power Mode

Precondition: Battery is fully charged.

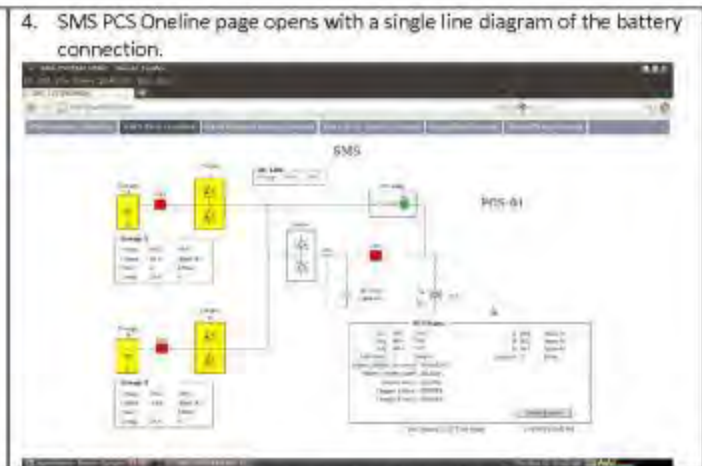
<i>Steps</i>	<i>Expected Results</i>
<p>1. Log in to the S&C SMS for battery.</p> 	<p>1. Successfully logged in to the system.</p> 



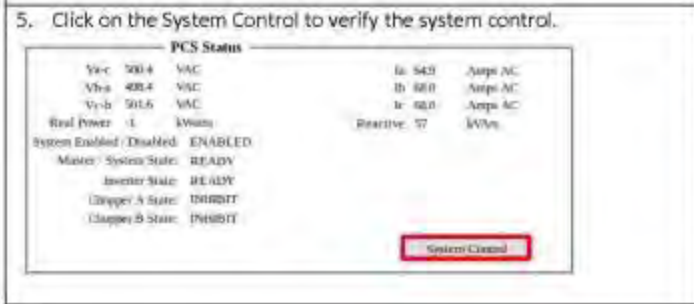
4. Click on the SMS PCS Online tab.



4. SMS PCS Online page opens with a single line diagram of the battery connection.

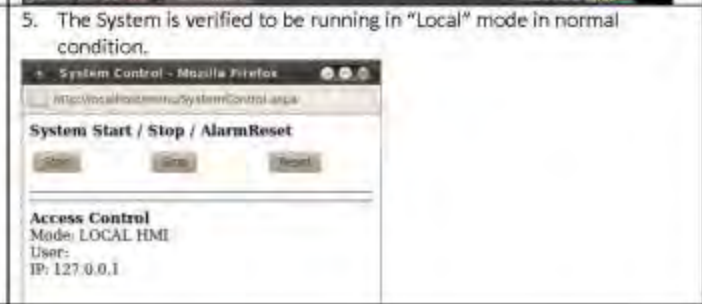


5. Click on the System Control to verify the system control.



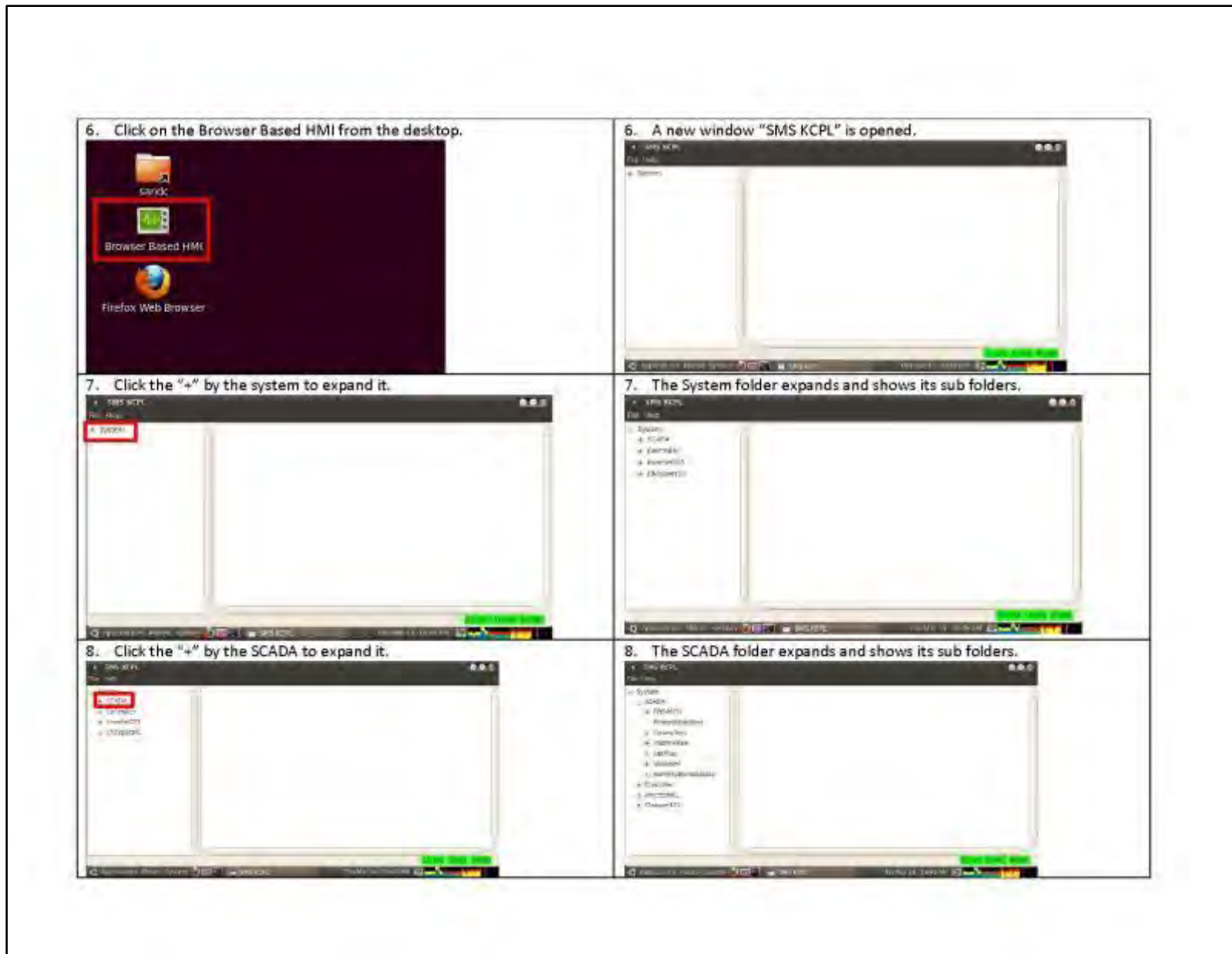
PCS Status			
V _{a-c}	500.4 VAC	I _a	54.9 Amps AC
V _{b-a}	498.4 VAC	I _b	60.0 Amps AC
V _{c-b}	501.6 VAC	I _c	48.0 Amps AC
Real Power	-1 kWatts	Reactive	17 kVAr
System Enabled / Disabled	ENABLED		
Master / System State	READY		
Inverter State	READY		
Charger A State	INHIBIT		
Charger B State	INHIBIT		

5. The System is verified to be running in "Local" mode in normal condition.



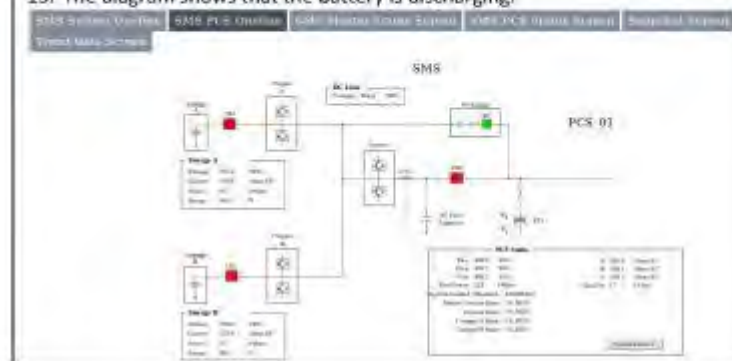


System Start / Stop / AlarmReset

Access Control
 Mode: LOCAL HMI
 User:
 IP: 127.0.0.1






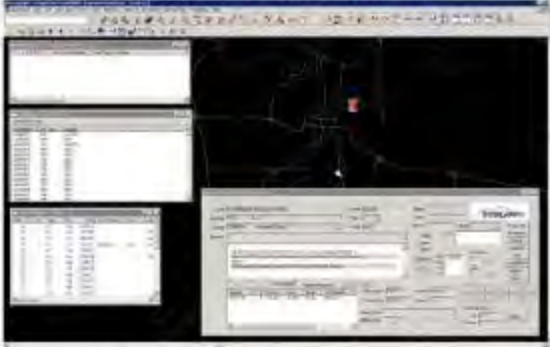
<p>14. Press "Ok" to confirm the changes.</p>  <p>The screenshot shows a software interface with a table of data. A dialog box with 'Confirm' and 'Cancel' buttons is overlaid on the table.</p> <table border="1"><thead><tr><th>Item</th><th>Value</th><th>Unit</th><th>Min</th><th>Max</th><th>Default</th></tr></thead><tbody><tr><td>1. 100%</td><td>100</td><td>%</td><td>0</td><td>100</td><td>100</td></tr><tr><td>2. 100%</td><td>100</td><td>%</td><td>0</td><td>100</td><td>100</td></tr><tr><td>3. 100%</td><td>100</td><td>%</td><td>0</td><td>100</td><td>100</td></tr><tr><td>4. 100%</td><td>100</td><td>%</td><td>0</td><td>100</td><td>100</td></tr><tr><td>5. 100%</td><td>100</td><td>%</td><td>0</td><td>100</td><td>100</td></tr><tr><td>6. 100%</td><td>100</td><td>%</td><td>0</td><td>100</td><td>100</td></tr><tr><td>7. 100%</td><td>100</td><td>%</td><td>0</td><td>100</td><td>100</td></tr><tr><td>8. 100%</td><td>100</td><td>%</td><td>0</td><td>100</td><td>100</td></tr><tr><td>9. 100%</td><td>100</td><td>%</td><td>0</td><td>100</td><td>100</td></tr><tr><td>10. 100%</td><td>100</td><td>%</td><td>0</td><td>100</td><td>100</td></tr></tbody></table>	Item	Value	Unit	Min	Max	Default	1. 100%	100	%	0	100	100	2. 100%	100	%	0	100	100	3. 100%	100	%	0	100	100	4. 100%	100	%	0	100	100	5. 100%	100	%	0	100	100	6. 100%	100	%	0	100	100	7. 100%	100	%	0	100	100	8. 100%	100	%	0	100	100	9. 100%	100	%	0	100	100	10. 100%	100	%	0	100	100	<p>14. The Battery starts to discharge.</p>
Item	Value	Unit	Min	Max	Default																																																														
1. 100%	100	%	0	100	100																																																														
2. 100%	100	%	0	100	100																																																														
3. 100%	100	%	0	100	100																																																														
4. 100%	100	%	0	100	100																																																														
5. 100%	100	%	0	100	100																																																														
6. 100%	100	%	0	100	100																																																														
7. 100%	100	%	0	100	100																																																														
8. 100%	100	%	0	100	100																																																														
9. 100%	100	%	0	100	100																																																														
10. 100%	100	%	0	100	100																																																														
<p>15. Open web browser opens with SMS System Menu.</p>  <p>The screenshot shows a web browser displaying a menu with various options and a diagram of a system.</p>	<p>15. The diagram shows that the battery is discharging.</p>  <p>The diagram shows a power system with a battery and a PCS (Power Conversion System) unit. The battery is labeled 'Battery' and the PCS is labeled 'PCS 01'. The battery is shown with a red arrow pointing away from it, indicating discharge.</p>																																																																		

Battery Grid Operation – Fixed kW (Discharge)

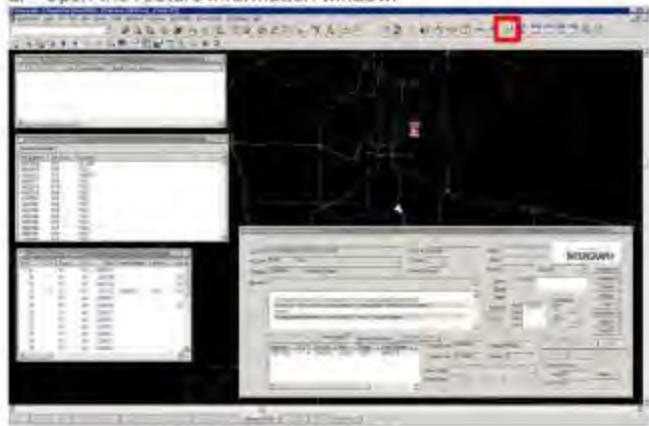


Fixed kW – Battery Discharging in Power Mode


Precondition: Battery is fully charged.

<i>Steps</i>	<i>Expected Results</i>
<p>1. Log in to OMS I/Dispatcher.</p> 	<p>1. Successfully logged in to OMS I/Dispatcher.</p> 


2. Open the Feature Information window.




2. A new window is opened.



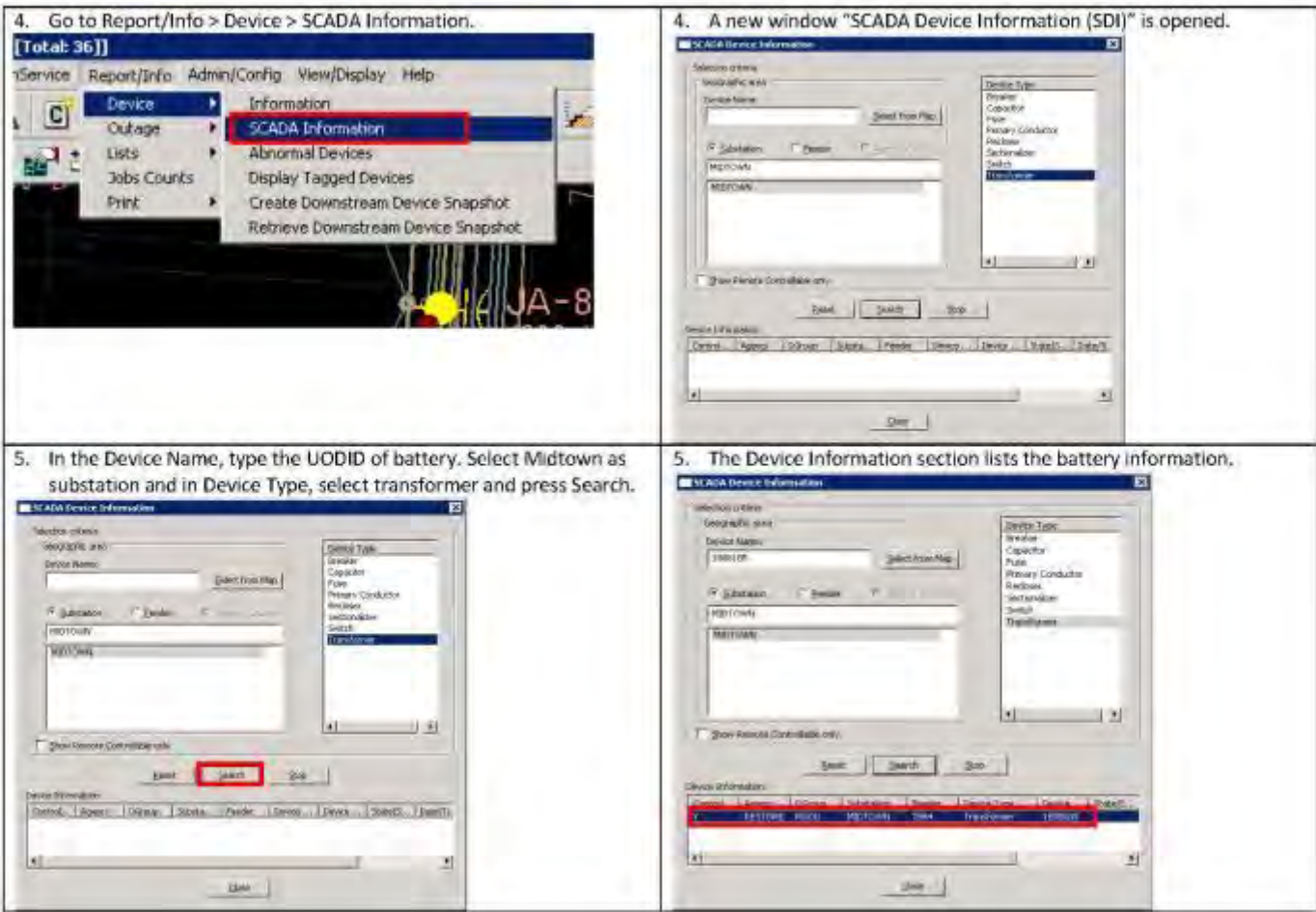
3. In the Feature Information window, enter the battery UODID (1888105).



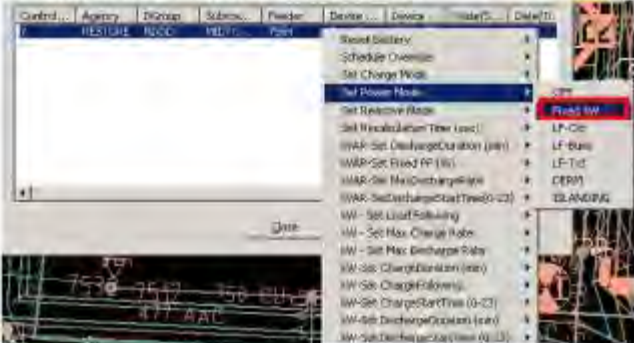
3. The feature information displays the SCADA value for battery.



Attribute	Value
Active State	Ready
Active Status	Unready
Alarm - Inhibit	OK
Alarm - Isolate	OK
Alarm - Trip Offline	OK
Alarm - Warning	OK
BESS Status	Enabled
Charge Mode	OFF
Energy Available (%)	80
Local - Available	Ready
Local - Mode	OFF
Recharge Mode	OFF
Reconciliation Time (Sec)	0
SCADA Error Cause Failure	OK
Schedule Override Status	Disabled
USM - Discharge Overlaid (MWh)	0
USM - Discharge Start Time (H:MM)	0
USM - Forecast Full	0
USM - Max Discharge Rate	0
MP - Charge Duration (Hours)	0
MP - Charge Following	0
MP - Charge Start Time (H:MM)	0
MP - Discharge Duration (Hours)	0
MP - Discharge Start Time (H:MM)	0
MP - Load Following	0
MP - Max Charge Rate	0
MP - Max Discharge Rate	0

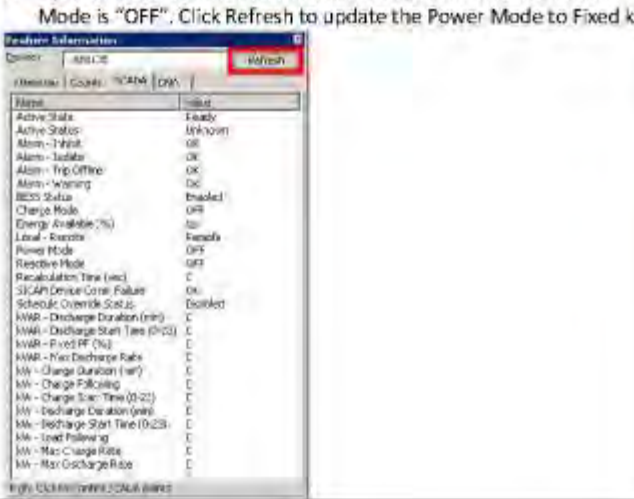


6. Go to Set Power Mode and select Fixed kW.

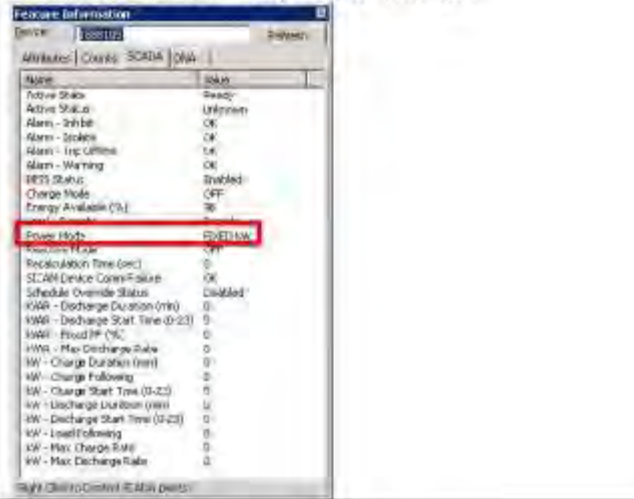


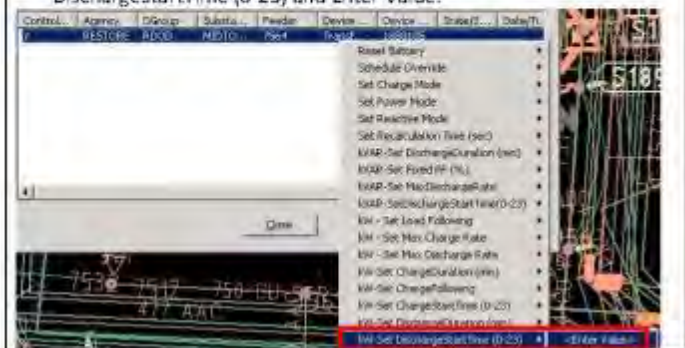
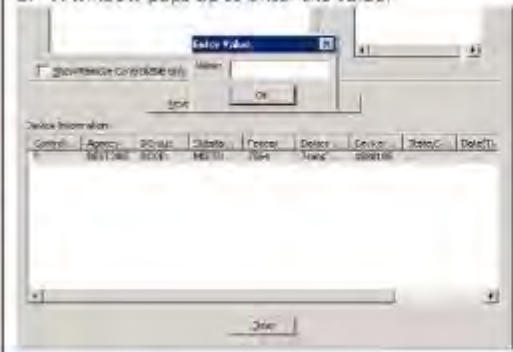
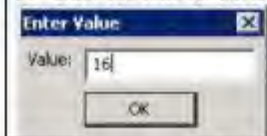
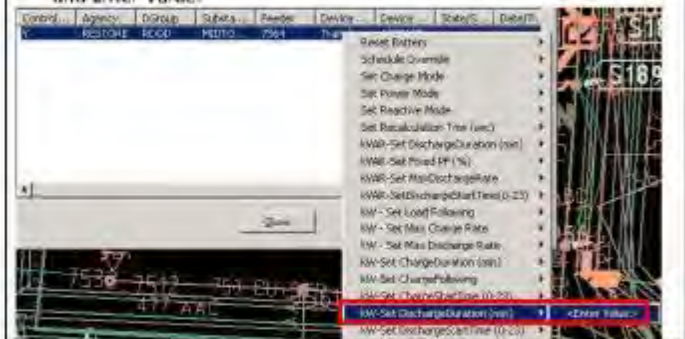
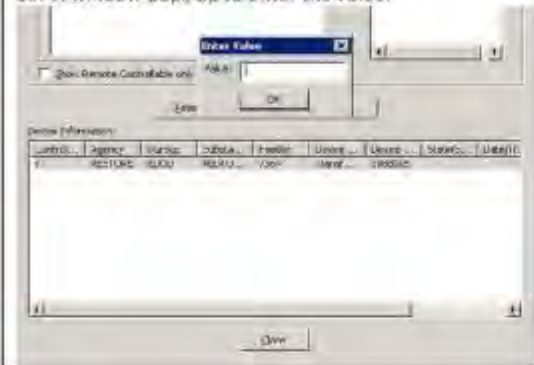
6. The Battery is now set to Fixed kW Discharge mode

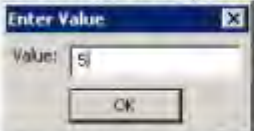
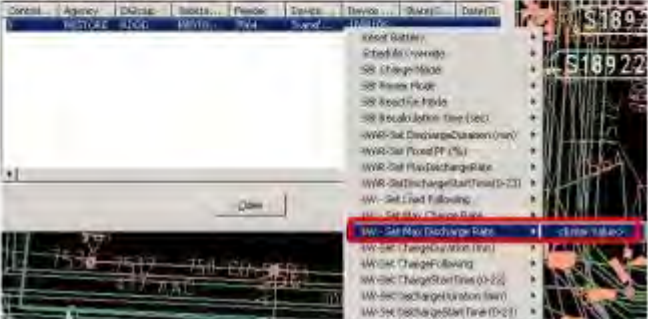
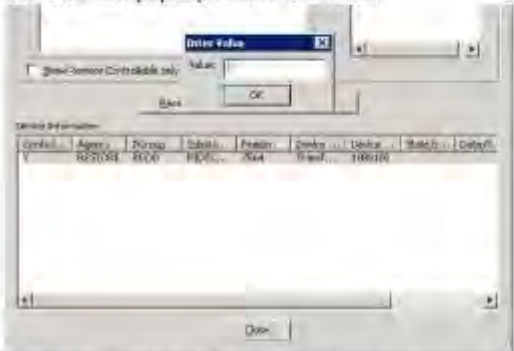
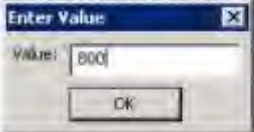
7. Open the Feature Information window and note that the Power Mode is "OFF". Click Refresh to update the Power Mode to Fixed kW.




7. The Power Mode is now updated to "Fixed kW".



<p>8. Open SDI and right click the battery. Select kW-Set DischargeStartTime (0-23) and Enter Value.</p> 	<p>8. A window pops up to enter the value.</p> 
<p>9. Enter the time for battery to start discharging and click OK.</p> 	<p>9. The battery discharge time is set to 16:00.</p>
<p>10. In SDI, right click the battery. Select kW-Set DischargeDuration (min) and Enter Value.</p> 	<p>10. A window pops up to enter the value.</p> 

<p>11. Enter the discharge duration for battery and click OK.</p> 	<p>11. The battery discharge duration is set to 5 minutes.</p>
<p>12. In SDI, right click the battery. Select kW-Set Max Discharge Rate and Enter Value.</p> 	<p>12. A window pops up to enter the value.</p> 
<p>13. Enter the maximum discharge rate for battery and click OK.</p> 	<p>13. The battery discharge rate is set to 800kW.</p>

14. Open the feature information window and verify that the values entered above are reflected in the SCADA tab. Press Refresh.




Name	Value
Active State	Ready
Active Status	Unknown
Alarm - Inhibit	OK
Alarm - Isolate	OK
Alarm - Trip Offline	OK
Alarm - Warning	OK
BESS Status	Enabled
Charge Mode	OFF
Energy Available (%)	95
Local - Remote	Remote
Power Mode	FIXED kW
Reactive Mode	OFF
Recalculation Time (sec)	0
SCADA Device Comm Failure	OK
Schedule Override Status	Disabled
kVAR - Discharge Duration (min)	0
kVAR - Discharge Start Time (0-23)	0
kVAR - Fixed PF (%)	0
kVAR - Max Discharge Rate	0
kW - Charge Duration (min)	0
kW - Charge Following	0
kW - Charge Start Time (0-23)	0
kW - Discharge Duration (min)	5
kW - Discharge Start Time (0-23)	16
kW - Load Following	0
kW - Max Charge Rate	0
kW - Max Discharge Rate	0

14. Note that the kW – Discharge Duration is 5 min, kW – Discharge time is 16:00 and kW – Max Discharge Rate is 800kW.




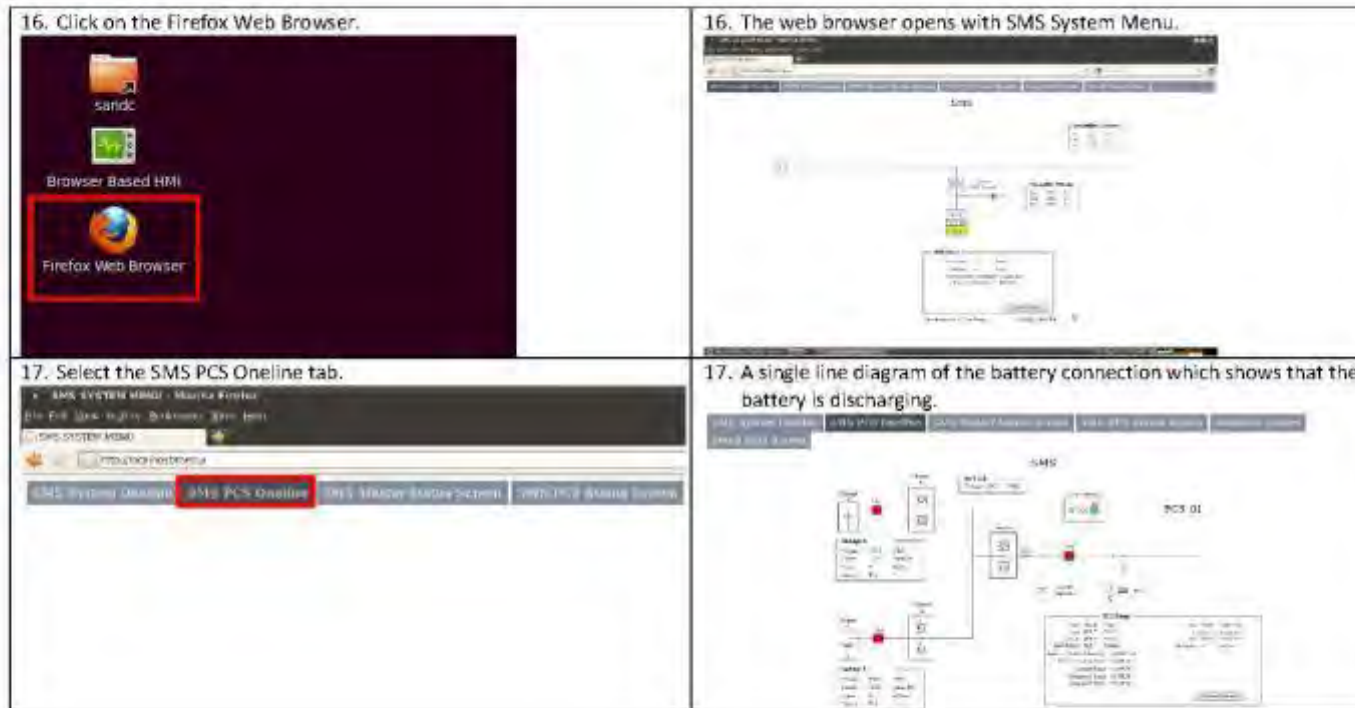
Name	Value
Active State	Ready
Active Status	Unknown
Alarm - Inhibit	OK
Alarm - Isolate	OK
Alarm - Trip Offline	OK
Alarm - Warning	OK
BESS Status	Enabled
Charge Mode	OFF
Energy Available (%)	95
Local - Remote	Remote
Power Mode	FIXED kW
Reactive Mode	OFF
Recalculation Time (sec)	0
SCADA Device Comm Failure	OK
Schedule Override Status	Disabled
kVAR - Discharge Duration (min)	0
kVAR - Discharge Start Time (0-23)	0
kVAR - Fixed PF (%)	0
kVAR - Max Discharge Rate	0
kW - Charge Duration (min)	0
kW - Charge Following	0
kW - Charge Start Time (0-23)	0
kW - Discharge Duration (min)	5
kW - Discharge Start Time (0-23)	16
kW - Load Following	0
kW - Max Charge Rate	0
kW - Max Discharge Rate	800

15. Log in to the S&C SMS for battery.

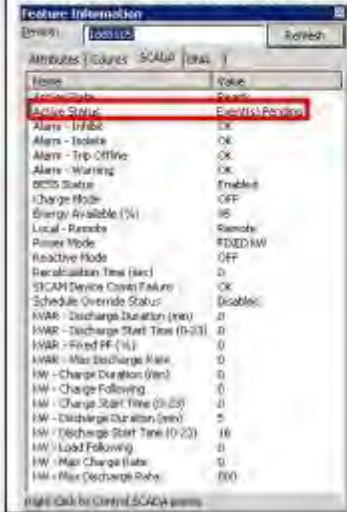


15. Successfully logged in to the system.






18. When the event is in process, open the feature information window in I/Dispatcher. Verify that the Active Status is Event(s) Pending.



The screenshot shows a 'Feature Information' window for device '1000100'. The 'Active Status' is highlighted in red and shows 'Event(s) Pending'. Other attributes include 'Alarm - Inhibit' (OK), 'Alarm - Isolate' (OK), 'Alarm - Trip Offline' (OK), 'Alarm - Warning' (OK), 'BESS Status' (Enabled), 'Charge Mode' (OFF), 'Energy Available (%)' (95), 'Local - Remote' (Remote), 'Power Mode' (FED MW), 'Reactive Mode' (OFF), 'Recalculation Time (sec)' (0), 'SCADA Device Config Failure' (OK), 'Schedule Override Status' (Disabled), and various IWR and I/W parameters.

18. The Active Status changes from Event(s) Pending to Event(s) Complete once the event duration has occurred.




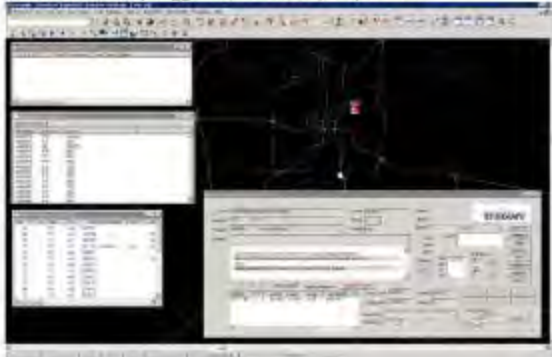
The screenshot shows the same 'Feature Information' window. The 'Active Status' is highlighted in red and now shows 'Event(s) Complete'. All other attributes remain the same as in the previous screenshot.

Battery Grid Operation – Load Following (Discharge)

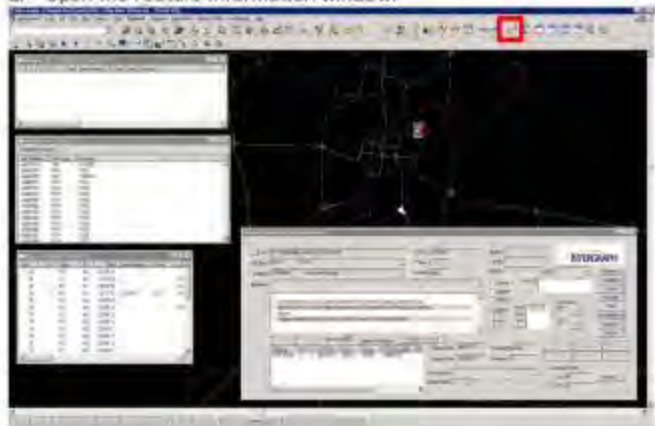


Load Following – Battery Discharging in Power Mode


Precondition: Battery is fully charged.

<i>Steps</i>	<i>Expected Results</i>
<p>1. Log in to OMS I/Dispatcher.</p> 	<p>1. Successfully logged in to OMS I/Dispatcher.</p> 


2. Open the Feature Information window.




2. A new window is opened.



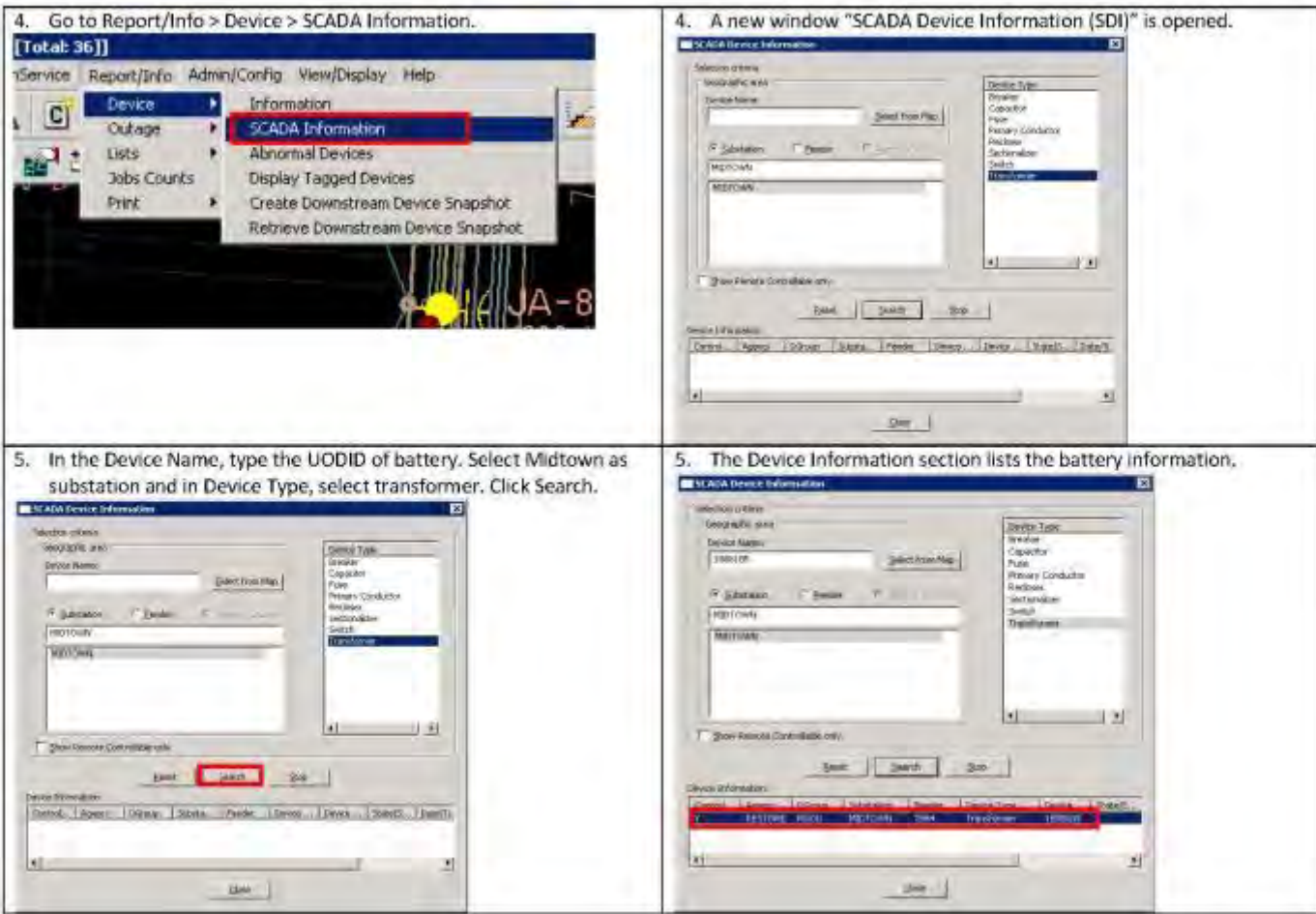
3. In the Feature Information window, enter the battery UODID (1888105).



3. The feature information displays the SCADA value for battery.



Name	Value
Active State	Ready
Active Status	Unknown
Alarm - Inhibit	OK
Alarm - Inhibit	OK
Alarm - Trip Offline	OK
Alarm - Warning	OK
BESS Status	Enabled
Charge Mode	OFF
Energy Available (%)	80
Local - Remote	Function
Mount Mode	OFF
Reaction Mode	OFF
Reconciliation Time (Sec)	0
SCADA Error Cause Failure	OK
Schedule Override Status	Disabled
USM - Discharge Current (A)	0
USM - Discharge Start Time (H:MM)	0
USM - Ready (H:MM)	0
USM - Max Discharge Rate	0
USM - Charge Duration (min)	0
USM - Charge Following	0
USM - Charge Start Time (H:MM)	0
USM - Discharge Duration (min)	0
USM - Discharge Start Time (H:MM)	0
USM - Cool Following	0
USM - Max Charge Rate	0
USM - Max Discharge Rate	0




6. Go to Set Power Mode and select LF-Ckt or LF-Buss or LF-Txf. For this test, LF-Ckt is selected.



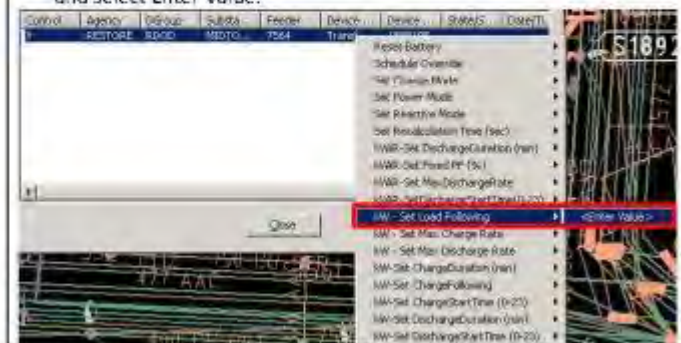
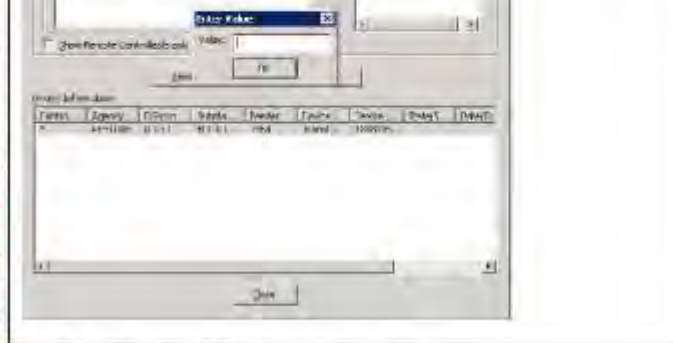

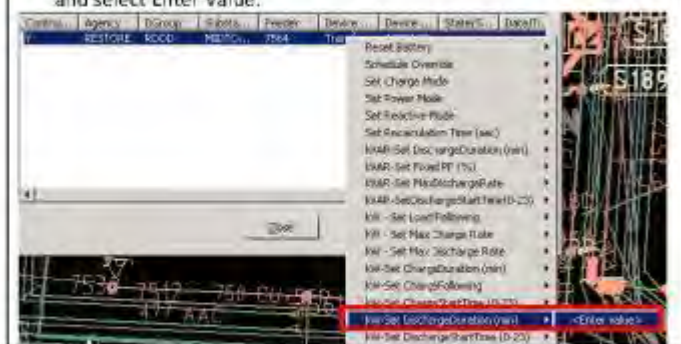
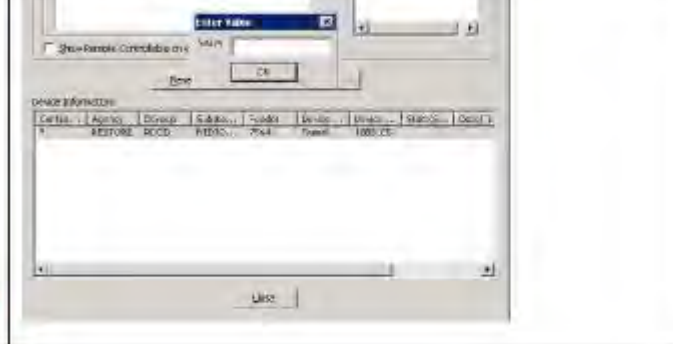
6. The Battery is now set to Load Following - Circuit (LF-Ckt) Discharge mode.

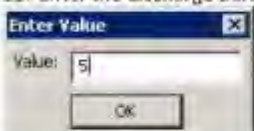
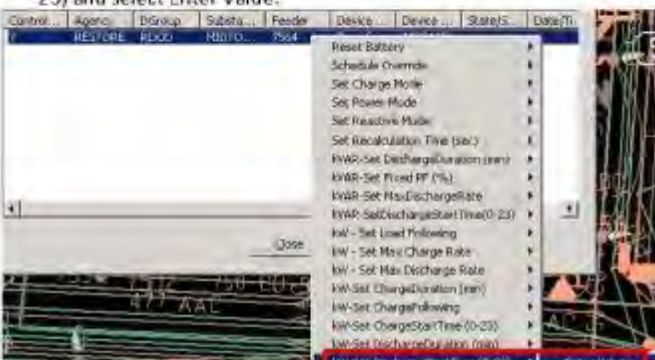
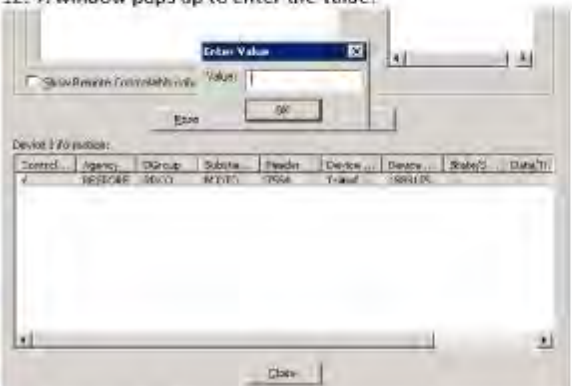
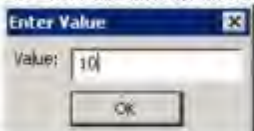
7. Open the Feature Information window and note that the Power Mode is "OFF", Click Refresh to update the Power Mode to Fixed kW.




7. The Power Mode is now updated to "LF-Ckt".



<p>8. Open SDI and right click the battery. Select kW-Set Load Following and select Enter Value.</p> 	<p>8. A window pops up to enter the value.</p> 
<p>9. Enter the value for load following for battery discharge and click OK.</p> 	<p>9. The battery Load Following is set to 200kW.</p>
<p>10. In SDI, right click the battery. Select kW-Set DischargeDuration (min) and select Enter Value.</p> 	<p>10. A window pops up to enter the value.</p> 


<p>11. Enter the discharge duration for battery and click OK.</p> 	<p>11. The battery discharge duration is set to 5 minutes.</p>
<p>12. In SDI, right click the battery. Select kW-Set DischargeStartTime (0-23) and select Enter Value.</p> 	<p>12. A window pops up to enter the value.</p> 
<p>13. Enter the time when battery starts discharging and click OK.</p> 	<p>13. The battery discharge start time is set to 10:00.</p>

14. Open the feature information window and to verify that the values entered above are reflected in the SCADA tab, press Refresh.



Name	Value
Active State	Ready
Active Status	Unknown
Alarm - Inhibit	OK
Alarm - Inhibit	OK
Alarm - Trip Offline	OK
Alarm - Warning	OK
BESS Status	Enabled
Charge Mode	OFF
Energy Available (%)	90
Local - Remote	Remote
Power Mode	IP-OK
Reactive Mode	OFF
Recalculation Time (sec)	0
SCADA Device Comm Failure	OK
Schedule Override Status	Disabled
SWR - Discharge Duration (min)	0
SWR - Discharge Start Time (D-23)	0
SWR - Fixed PF (%)	0
SWR - Max Discharge Rate	0
SW - Charge Duration (min)	0
SW - Charge Following	0
SW - Charge Start Time (D-23)	0
SW - Discharge Duration (min)	0
SW - Discharge Start Time (D-23)	0
SW - Load Following	0
SW - Max Charge Rate	0
SW - Max Discharge Rate	0

14. Note that the kW – Discharge Duration is 5 min, kW – Discharge time is 10:00 and kW – Load Following is 200.



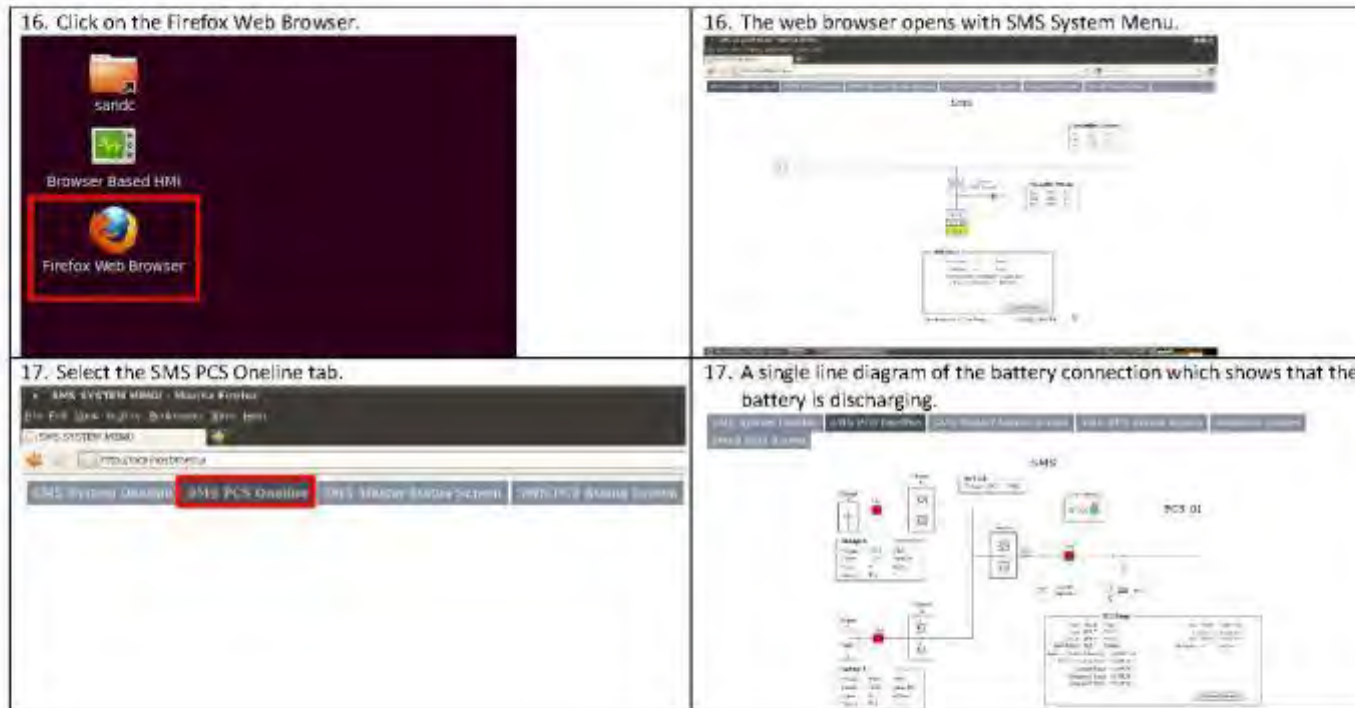
Name	Value
Active State	Ready
Active Status	Event(s) Pending
Alarm - Inhibit	OK
Alarm - Inhibit	OK
Alarm - Trip Offline	OK
Alarm - Warning	OK
BESS Status	Enabled
Charge Mode	OFF
Energy Available (%)	90
Local - Remote	Remote
Power Mode	IP-OK
Reactive Mode	OFF
Recalculation Time (sec)	0
SCADA Device Comm Failure	OK
Schedule Override Status	Disabled
SWR - Discharge Duration (min)	0
SWR - Discharge Start Time (D-23)	0
SWR - Fixed PF (%)	0
SWR - Max Discharge Rate	0
SW - Charge Duration (min)	0
SW - Charge Following	0
SW - Charge Start Time (D-23)	0
kW - Discharge Duration (min)	5
kW - Discharge Start Time (D-23)	10
kW - Load Following	200
SW - Max Charge Rate	0
SW - Max Discharge Rate	0

15. Log in to the S&C SMS for battery.




15. Successfully logged in to the system






18. When the event is in process, open the feature information window in I/Dispatcher. Verify that the Active Status is Event(s) Pending.



The screenshot shows a 'Feature Information' window for device '1100105'. The 'Active Status' is highlighted in red and shows 'Event(s) Pending'. Other parameters include Alarm - Inhibit (OK), Alarm - Lockout (OK), Alarm - Trip Offline (OK), Alarm - Warning (OK), BESS Status (Enabled), Charge Mode (OFF), Energy Available (%) (0), Local - Remote (Remote), Power Mode (FACTS), Reactive Mode (OFF), Recalculation Time (sec) (0), SICAM Device Comm Failure (OK), Schedule Override Status (Disabled), MW - Discharge Duration (min) (0), MW - Discharge Start Time (0-23) (0), MW - Power (%) (0), MW - Max Discharge Rate (0), MW - Charge Duration (min) (0), MW - Charge Following (0), MW - Charge Start Time (0-23) (0), MW - Discharge Duration (min) (0), MW - Discharge Start Time (0-23) (0), MW - Load Following (200), MW - Max Charge Rate (0), and MW - Max Discharge Rate (0).

18. The Active Status changes from Event(s) Pending to Event(s) Complete once the event duration has occurred.



The screenshot shows the same 'Feature Information' window for device '1100105'. The 'Active Status' is highlighted in red and now shows 'Event(s) Complete'. All other parameters remain the same as in the previous screenshot.

Appendix K Interoperability Field Demonstration Scripts

K.1	Remote Connect and Disconnect	K-3
K.2	Demand Response – AMI Thermostat.....	K-31
K.3	Demand Response – HAN Devices	K-51
K.4	Demand Response - Battery.....	K-74
K.5	1 st Responder Volt Var Control.....	K-101
K.6	1 st Responder Feeder Load Transfer	K-114
K.7	1 st Responder Fault Isolation and Service Restoration.....	K-125
K.8	Outage and Restoration Events.....	K-144
K.9	Power Status Verification	K-176
K.10	Battery Operation: Local Control	K-193
K.11	Battery Operation: Fixed kW Discharge	K-213
K.12	Battery Operation: Load Following Discharge.....	K-234

This page intentionally blank.

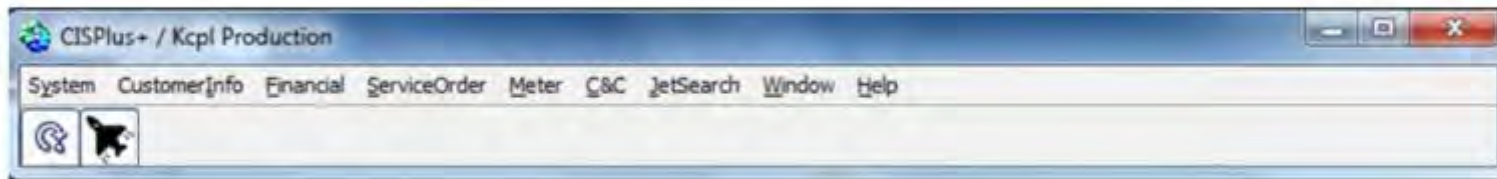


Remote Connect

- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program



Launch GIS

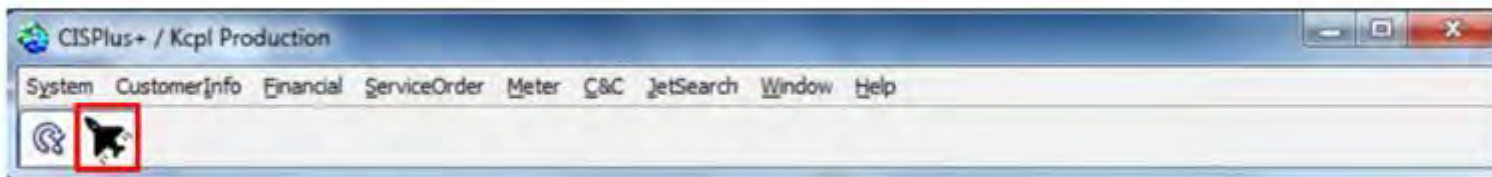


▪2

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Select "Jet" Search Button



3

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Enter Account Information

The screenshot shows a software window titled "JetSearch 1 JetSearch". The window contains a form with the following sections:

- Launch**: Includes input fields for "Name...", "Address...", "Account:", and "Phone:". Each field has a green checkmark icon to its right. There is also an "Advanced Search..." button.
- Alerts**: A large empty text area.
- Open JetSons**: A large empty text area.
- Account / Person Information**: A table with two columns: "Description" and "Value".
- Potential JetSons**: A section with "Show JetSon" and "Close JetSons" buttons.

At the bottom right of the window, there is an "Open Alert..." button.

4

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Account Information is Displayed

The screenshot shows a web application window titled "JetSearch: Pomerence, Mary". The window contains a "Launch" section with several input fields and checkboxes, each with a green checkmark indicating successful validation:

- Name: Pomerence, Mary
- Address: 406 E 43rd St, Apt 2e/Kcmo, Mo
- Account: 5350203882
- Phone: (417) 234-4600

Below these fields is an "Advanced Search..." button. To the right, an "Alerts" section displays the following information:

- Premise equipped w/Smart Meter
- ** Remote Disconnected **
- Smart Grid Demonstration Area
- ⚡ Pending Turn-on
- ⚡ Last Contact 02/12/2013

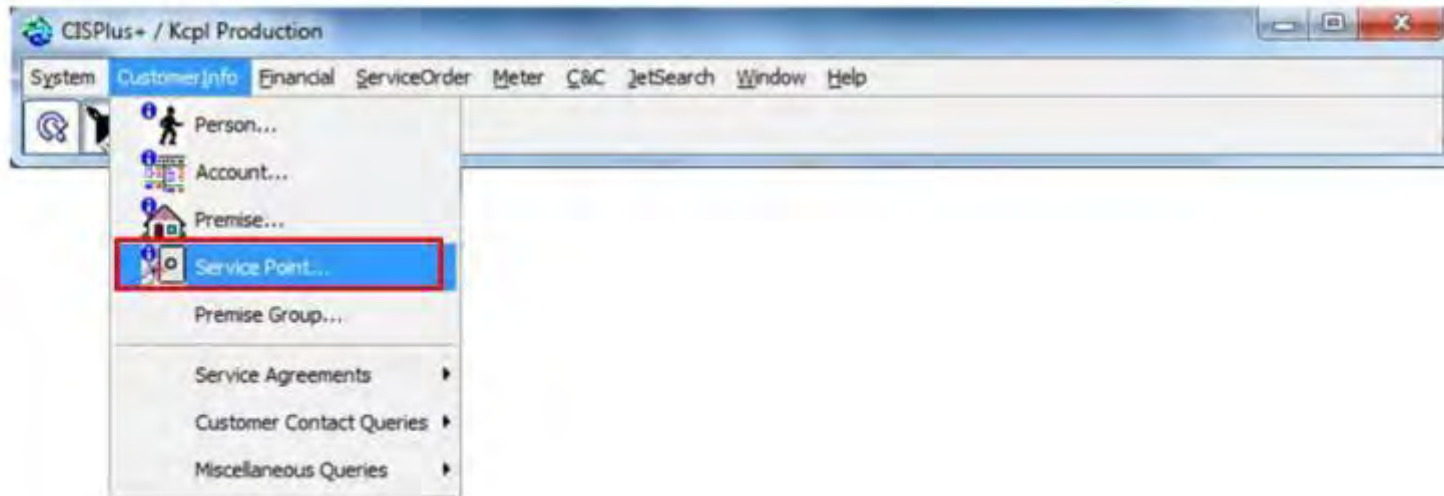
At the bottom left, there is a section for "Open JetSons" with a dropdown menu showing "S.O. Completion: E-RS Turn on (On At Metr...".

5

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Go to Service Point



6

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Service Point Information of Entered Account Number

The screenshot shows a software window titled "Service Point: E-RS @ 406 E 43rd St,Apt 2e/Kcmo,Mo". The interface includes the following fields and controls:

- Action:** Launch
- Service Point:** 9324790610 406 E 43rd St,Apt 2e/Kcmo,Mo
- Meter:** 10712811T (Int: 1338594), Active, 1/2848, MC's = 2
- Utility Type:** Electricity
- Status:** I - In Service
- Utility Type:** E - Electricity Temporary Service
- Premise:** 406 E 43rd St,Apt 2e/Kcmo,Mo 3022402619
- Source Status:** C - Connected
- Meter@SP Status:** S - Mtr Off Switched (highlighted in red)
- Metered SP Under Construction
- Read Cycle:** MR Cycle/Route... 03 030c Seq: 6220
- ERT Message:** [Empty text box]
- Use Code:** [Empty dropdown] Print Use Code
- Suggested Rate Class:** RS - Residential Service
- Lock Device Type:** [Empty dropdown]
- Locking Device Action:** [Empty dropdown]
- Last Action Date:** [Empty text box]

On the right side, there is a sidebar menu with the following items:

- Main
- Meter / Equipment
- MR / Location
- MRU
- Electric
- Miscellaneous

7

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

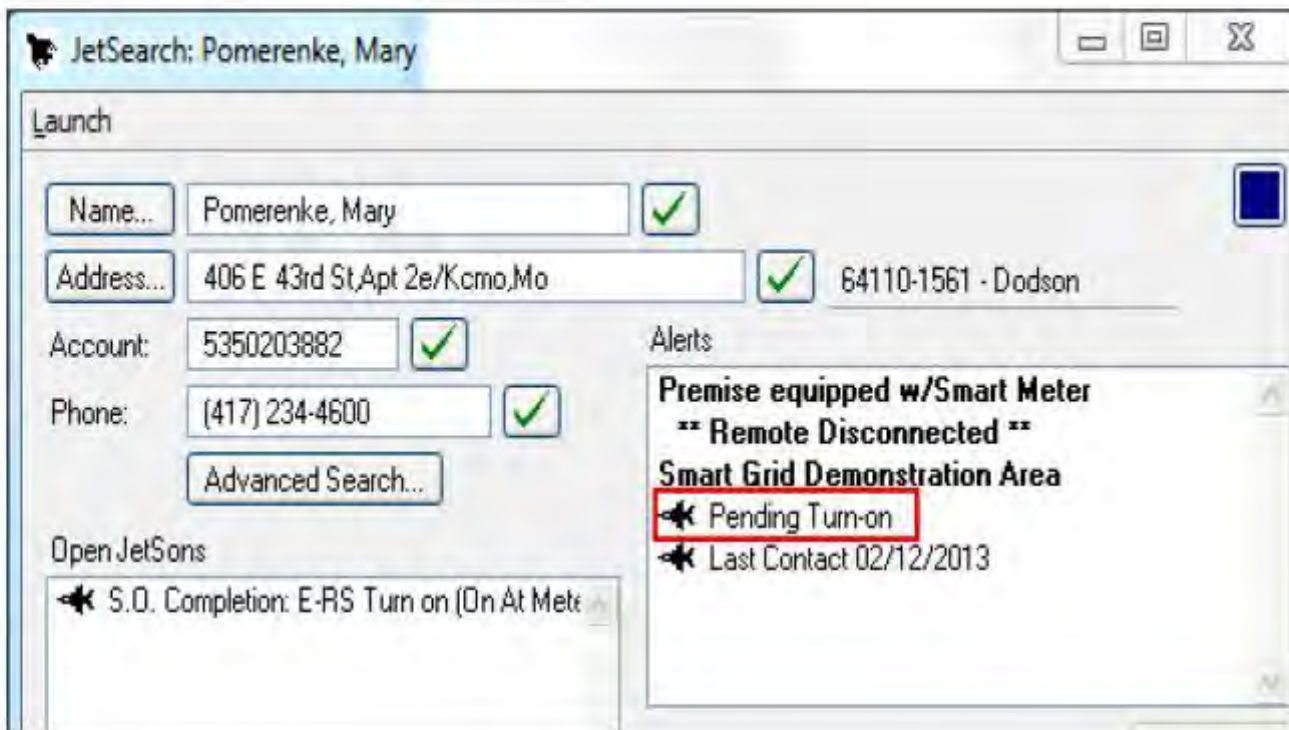


Go to Jet Search Window: Updated Information

The screenshot shows a software window titled "JetSearch: Pomerence, Mary". The window contains several input fields and sections:

- Launch** section:
 - Name: Pomerence, Mary (with a green checkmark)
 - Address: 406 E 43rd St, Apt 2e/Kcmo, Mo (with a green checkmark) and 64110-1561 - Dodson
 - Account: 5350203882 (with a green checkmark)
 - Phone: (417) 234-4600 (with a green checkmark)
 - Advanced Search... button
- Open JetSons** section:
 - S.O. Completion: E-RS Turn on (On At Mete...
- Alerts** section:
 - Premise equipped w/Smart Meter
 - ** Remote Disconnected **
 - Smart Grid Demonstration Area
 - Pending Turn-on
 - Last Contact 02/12/2013

Select "Pending Turn-On"



Status of Service Order "Pending"

S.O. Completion: E-RS Turn on (On At Meter)

Action

Service Order: 5596527344 Initiated On 02/12/2013 By Ivie, Kelly

Order Type: Turn On Turn on (On At Meter)

Status: Pending Fld Order: (1) 8058192598 Pending

Service Point: 9324790610 Conn Difs E-RS, 1RS1A, 10712811G, ON, PH1

Acct/Premise: 5350203882 Pomeranke, May / 406 E 43rd St,Apt 2e/K.cmo,Mo RSSM/AR...

Order Date: 02/14/2013 SP Location: ON - Outside North

Effective Date/Time: 02/14/2013 8:11 am Service Person:

Work Done: 02/14/2013 Mileage: 0

Comments:

Meter

Meter: 10712811 Int: 1338594 1/2848

MC ID	Reading	MC Details	Last Read Date/Type	Last Reading
19704096		KWH = 5.0 digt; 1.0000	02/08/13 RN	10727.00000

Reading: Record Reading

Lock Device Type: Lock Device Action:

Lock Action Date:

Seal Number: Seal Color:

USA Info: ER-RS 1RS1A 1 USA Details...

10

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Status "Acknowledged" After Process is Started

S.O. Maintenance: E-RS Turn on (On At Meter)

Action

Service Order: 5596527344 Initiated on 02/12/2013 by Ivie, Kelly

Status: Pending **Fid Order: (1) 8058192596 Acknowledged**

Service Point: 9324790610 Conn DWS E-RS, 1RS1A, 10712811G, ON, PH1, 02/08/12 RSSM/AK

Acct/Premise: 5350203882 Pomeranke, Mary / 406 E 43rd St Apt 2e/Kcmo,Mo

Order Type: Turn On Order Date: 02/14/2013

Order Subtype: Turn on (On At Meter)

Orig: T - Telephone

Ordered by: Mary Service Person:

Urgency: C - Company's Convenience

Block User: Blocked Date:

Instructions: on at meter 13020467072

Comments:

Turn On Info:

Premise Phone: (417) 234-4600 Key at Premise OK to Enter

Work Phone:

Mailing Address: 406 E 43rd St, 2e/Kansas City, Mo 64110-1561

After Connect, Status of Service Order “Completed”

S.O. Completion: E-RS Turn on (On At Meter)

Action

Service Order: 5596527344 Initiated On 02/12/2013 By Ivie, Kelly

Order Type: Turn On Turn on (On At Meter)

Status: Complete on 02/14/2013 09:19 by Mdm, System **Fld Order: (1) 8058192596 Completed**

Service Point: 9324790610 Conn On E-RS, 1RS1A, 10712811G, DN, PH1

Acct/Premise: 5350203882 Pomeranke, May / 406 E 43rd St Apt 2e/Kcmo,Mo RSM/Alt

Order Date: 02/14/2013 SP Location: DN - Outside North

Effective Date/Time: 02/14/2013 9:19 am Service Person:

Work Done: 02/14/2013 Mileage: 0

Comments:

Meter

Meter: 10712811 Ink: 1338594 1/2848

MC ID	Reading	MC Details	Last Read Date/Type	Last Reading
19704096	18727.00000	KWH = 5.0 dpts, 1.0000		

Reading: 18727.00000 Record Reading

Lock Device Type: Lock Device Action:

Lock Action Date:

Seal Number: Seal Color:

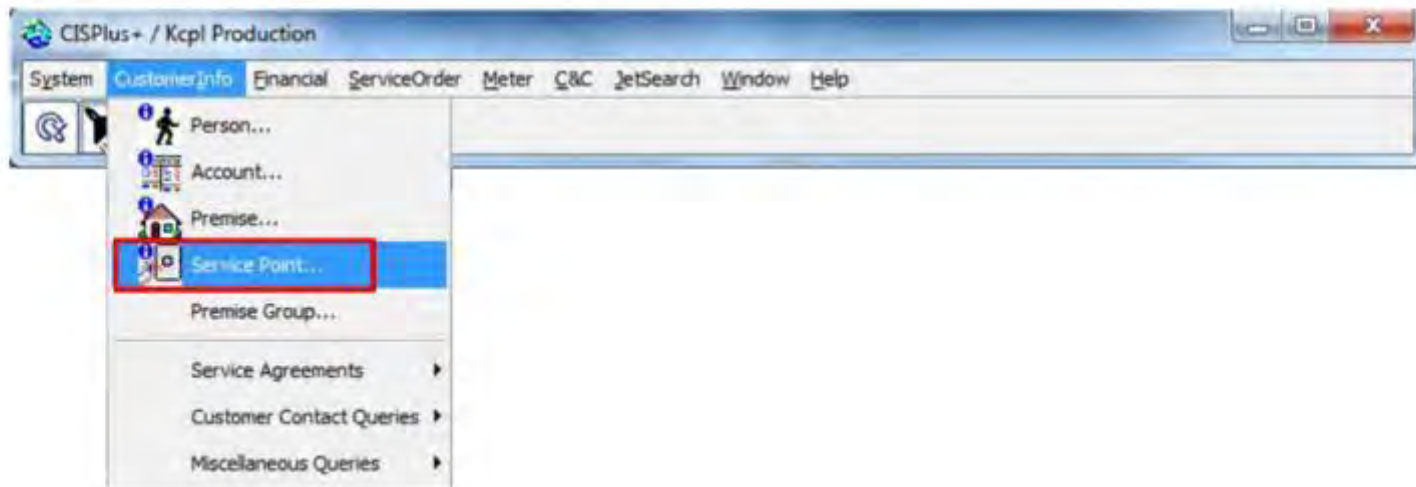
USA Info: ER-RS 1RS1A, 1 USA Detail:

12

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Go to "Service Point"



Service Point Displays “Meter On”

Service Point: E-RS @ 406 E 43rd St,Apt 2e/Kcmo,Mo

Action Launch

Service Point... 9324790610 406 E 43rd St,Apt 2e/Kcmo,Mo

Meter: 10712811T (Int: 1338594), Active, 1/2848, MC's = 2 Utility Type: Electricity

Status: I - In Service

Utility Type: E - Electricity Temporary Service

Premise... 406 E 43rd St,Apt 2e/Kcmo,Mo 3022402619

Source Status: C - Connected

Meter@SP Status: 0 - Meter On

Metered SP Under Construction

Read Cycle

MR Cycle/Route... 03 030c Seq: 6220

ERT Message:

Use Code: Print Use Code

Suggested Rate Class: RS - Residential Service

Lock Device Type:

Locking Device Action:

Last Action Date:

Main

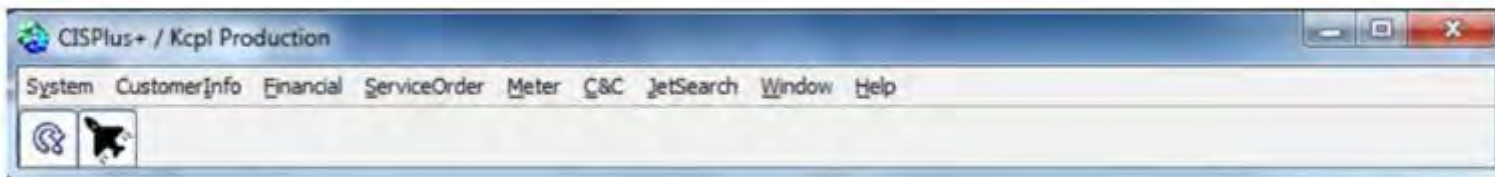
- Meter / Equipment
- MR / Location
- MRU
- Electric
- Miscellaneous

Remote Disconnect

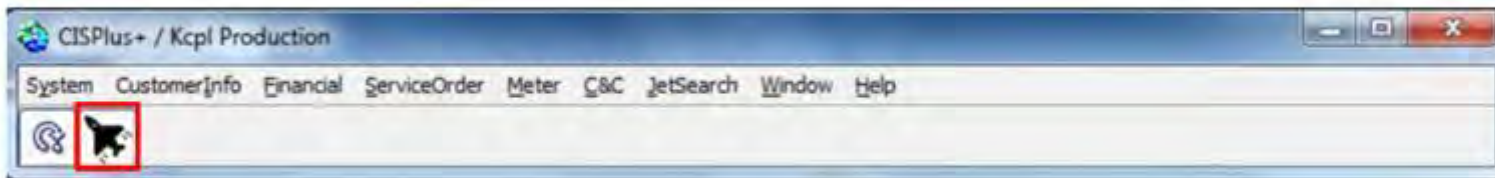
- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program



Launch CIS



Select "Jet" Search Button



Enter Account Information

The screenshot shows a software window titled "JetSearch 1 JetSearch". The window contains several input fields and sections:

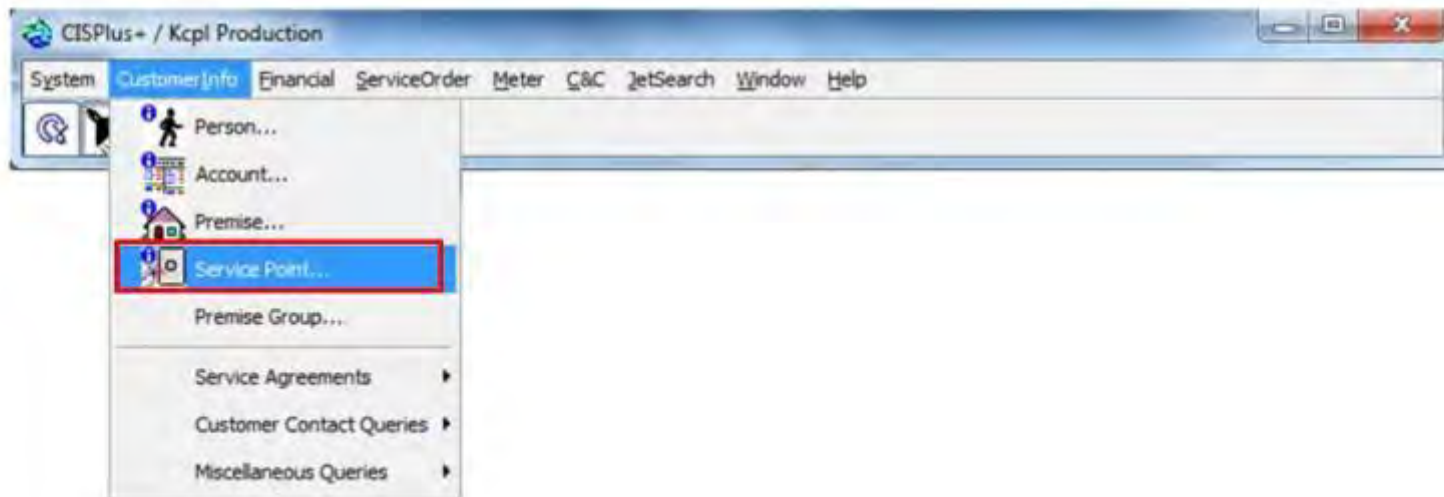
- Launch** section:
 - Name...: with a green checkmark icon.
 - Address...: with a green checkmark icon.
 - Account: with a green checkmark icon.
 - Phone: with a green checkmark icon.
 - Advanced Search...:
- Alerts** section: A large empty text area.
- Open JetSons** section: A large empty text area.
- Account / Person Information** section: A table with two columns: "Description" and "Value".
- Potential JetSons** section: Show JetSon Close JetSons

Account Information is Displayed

The screenshot shows a software window titled "JetSearch: King, Thelma L". The window contains several input fields and sections:

- Name...:** King, Thelma L (with a green checkmark icon)
- Address...:** 4400 Woodland Ave/Kcmo,Mo (with a green checkmark icon) and 64110-1456 - Dodson
- Account:** 1317760179 (with a green checkmark icon)
- Phone:** (816) 309-6133 (with a green checkmark icon)
- Advanced Search...** button
- Alerts:**
 - Premise equipped w/Smart Meter**
 - Green Impact Zone**
 - Account has 2 premises
 - 2 persons linked to account
 - Pending Turn-off
 - Last Contact 02/12/2013
 - 2 USAs for account
 - Credit Segment: 3
- Open JetSons:**
 - S.O. Completion: E-RS Off Read, Cellnet M

Go to Service Point



Service Point Information of Entered Account Number

Service Point: E-RS @ 4400 Woodland Ave/Kcmo,Mo

Action Launch

Service Point: 6779916584 4400 Woodland Ave/Kcmo,Mo

Meter: 10439383T (Int: 94104522), Active, 1/2848, MC's = 2 Utility Type: Electricity

Status: I - In Service

Utility Type: E - Electricity Temporary Service

Premise: 4400 Woodland Ave/Kcmo,Mo 5089821464

Source Status: C - Connected

Meter@SP Status: D - Meter On

Metered SP Under Construction

Read Cycle

MR Cycle/Route: 05 050d Seq: 1140

ERT Message:

Use Code: Print Use Code

Suggested Rate Class: RS - Residential Service

Lock Device Type:

Locking Device Action:

Last Action Date: 09/06/2011

Main

Meter / Equipment

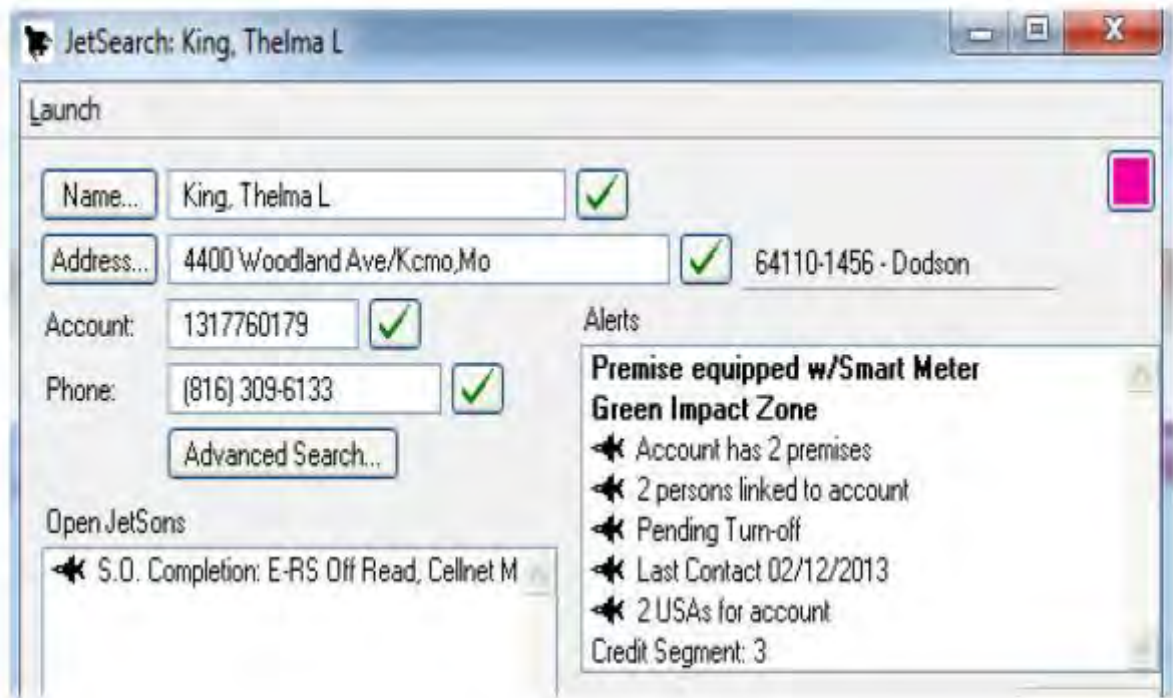
MR / Location

MRU

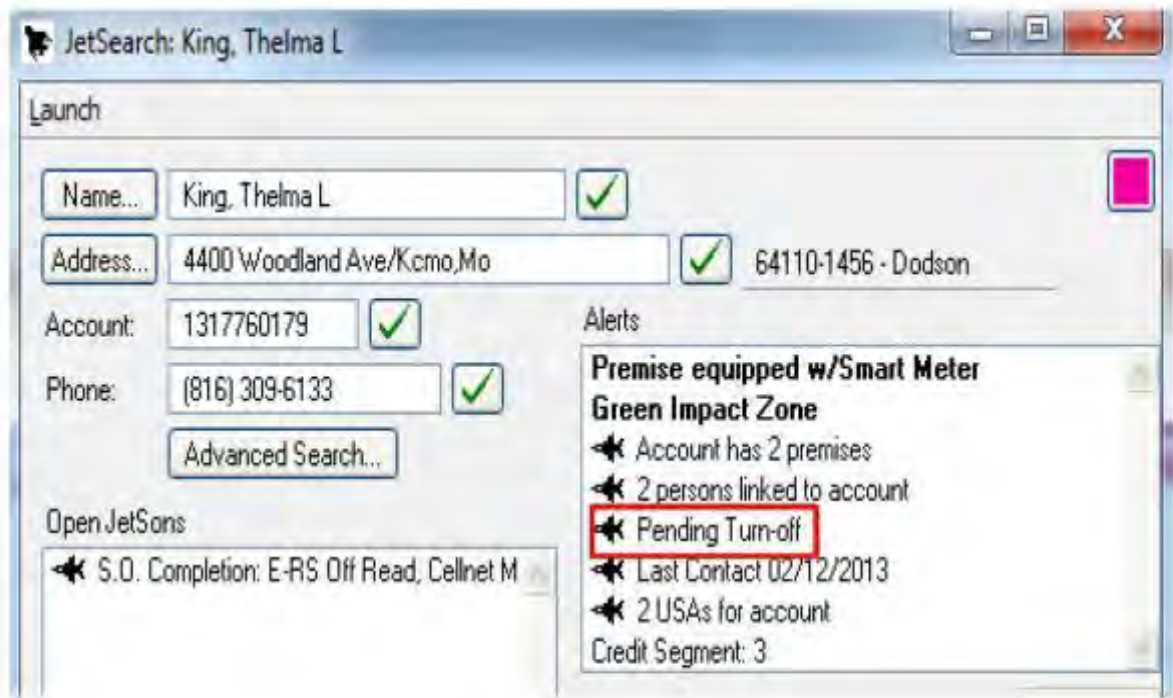
Electric

Miscellaneous

Go to Jet Search Window: Updated Information



Select "Pending Turn-Off"



Status of Service Order "Pending"

S.O. Completion: E-RS Off Read, Cellnet Mtr Left On

Action

Service Order: 195157901 Initiated On 02/11/2013 By Ah-Mu, Anne

Order Type: Turn Off Off Read, Cellnet Mtr Left On

Status: Pending Fid Order: (1) 5028203007 Pending

Service Point: 6779916584 Conn On E-RS, 1RS1A, 10439383G, DW, PH1

Acct/Premise: 1317760179 King, Thelma L / 4400 Woodland Ave/Kcmo,Mo RSSM/AR

Order Date: 02/14/2013 SP Location: DW - Outside West

Effective Date/Time: 02/14/2013 8:39 am Service Person:

Work Done: 02/14/2013 Mileage: 0

Comments:

Meter: 10439383 Jnk: 94104522 1/2648

MC ID	Reading	MC Details	Last Read Date/Type	Last Reading
16173430		KWP, 5.2 digits, 1.0000	02/14/13 RN	0.30000
36808915		KWH +, 5.0 digits, 1.0000	02/14/13 RN	17770.00000

Reading:

Lock Device Type: Lock Device Action:

Lock Action Date: 09/06/2011

Seal Number: Seal Color: G - Gray

Status "Acknowledged" After Process is Started

S.O. Maintenance: E-RS Off Read, Cellnet Mtr Left On

Action

Service Order... 195157901 Initiated on 02/11/2013 by Ah-Mu, Anne

Status: Pending **Fid Order: (1) 5028203007 Acknowledged**

Service Point: 6779916584 Conn On E-RS, 1RS1A, 10439383G, DW, PH1 RSSM/AIL...

Acct/Premise: 1317760179 King, Thelma L / 4400 Woodland Ave/Kcmo,Mo

Order Type: Turn Off Order Date: 02/14/2013

Order Subtype: Off Read, Cellnet Mtr Left On

Origin: T - Telephone

Ordered by: Thelma Service Person:

Urgency: C - Companys Convenience

Block User... Blocked Date:

Instructions: 01302 045 5690

Comments:

Turn Off Info:

Mailing Address: 4207 Mongall Ave/Kansas City, Mo 64130-1318 Change Address...

Initiation Confirmation Window Attributes...

After Disconnect, Status of Service Order “Completed”

S.O. Completion: E-RS Off Read, Cellnet Mtr Left On

Action

Service Order: 195157901 Initiated On 02/11/2013 By Ah-Mu, Anne

Order Type: Turn Off Off Read, Cellnet Mtr Left On

Status: Complete on 02/14/2013 09:18 by Mdm, System **Fld Order: (1) 5028203007 Completed**

Service Point: 6779916584 Conn Offs E-RS, 1RS1A, 10439383G, OW, PH1

Acct/Premise: 1317760179 King, Thelma L / 4400 Woodland Ave/Kcmo,Mo R5SM/Akt.

Order Date: 02/14/2013 SP Location: OW - Outside West

Effective Date/Time: 02/14/2013 9:18 am Service Person:

Work Done: 02/14/2013 Mileage: 0

Comments:

Meter

Meter: 10439383 Int: 94104522 1/2848

MC ID	Reading	MC Details	Last Read Date/Type	Last Reading
16173430	8.30000	KWH P, 5.2 digits, 1.0000		
36808915	17791.00000	KWH +, 5.0 digits, 1.0000		

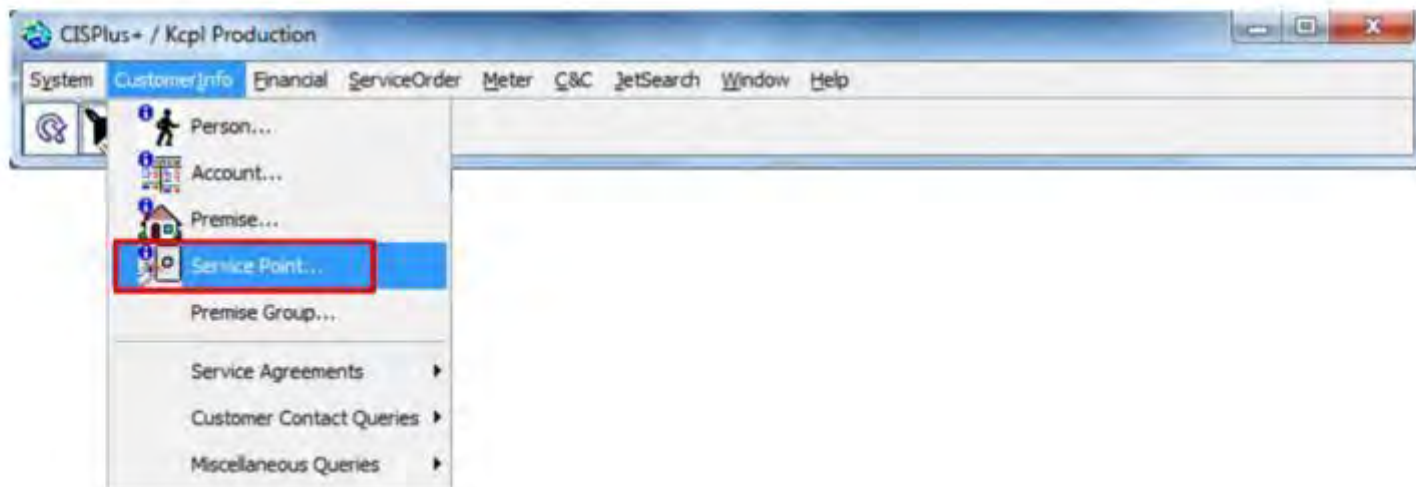
Reading: 8.30000 Record Reading

Lock Device Type: Lock Device Action:

Lock Action Date: 09/06/2011

Seal Number: Seal Color: G - Gray

Go to "Service Point"



Service Point Displays “Meter On”

Service Point: E-RS @ 4400 Woodland Ave/Kcmo,Mo

Action Launch

Service Point... 6779916584 4400 Woodland Ave/Kcmo,Mo

Meter: 10439383T (Int: 94104522), Active: 1/2848, MC's = 2 Utility Type: Electricity

Status: I - In Service

Utility Type: E - Electricity Temporary Service

Premise... 4400 Woodland Ave/Kcmo,Mo 5089821464

Source Status: C - Connected

Meter@SP Status: S - Mtr Off Switched

Metered SP Under Construction

Read Cycle

MR Cycle/Route... 05 050d Seq: 1140

ERT Message:

Use Code: Print Use Code

Suggested Rate Class: RS - Residential Service

Lock Device Type:

Locking Device Action:

Last Action Date: 09/06/2011

Main

- Meter / Equipment
- MR / Location
- MRU
- Electric
- Miscellaneous

Demand Response – AMI Thermostat

- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program



Launch DERM WebUI

The screenshot shows the OATI WebDistribute interface. At the top, there is a navigation menu with items: Overview, Base Data, Customers, Operations, Grid Management, Post Operations, Interface Management, User Administration, Debug, and Window. The browser title is 'Dashboard' and the date is 'Thu 12/19 9:14 AM CPT'. The main content area is divided into several sections:

- DR MANAGEMENT TABULAR:** A table with the following data:

MTD Peak (MW)	.0
Current Billing Demand (MW)	
Current Date/Time	12/19 09:10
Current Temp (F)	
MTD System Peak Demand (MW)	
Current System Peak Demand (MW)	
Current Industrial Load (MW)	.0
- TEMPERATURE FORECAST:** A panel labeled 'UnitSched2'.
- DR AVAILABILITY:** A panel labeled 'UnitSched'.
- SYSTEM:** A table with the following data:

Number of Programs	6
Number of Customers	4382
Number of Asset	759
Users Currently Logged in	1
Number of Resources	26
Committed Schedules	0
Active Schedules	0
Completed Schedules	0
- PERFORMANCE:** A panel labeled 'UnitSched1'.
- QUICK KEY LINKS:** A list of function keys with corresponding actions:

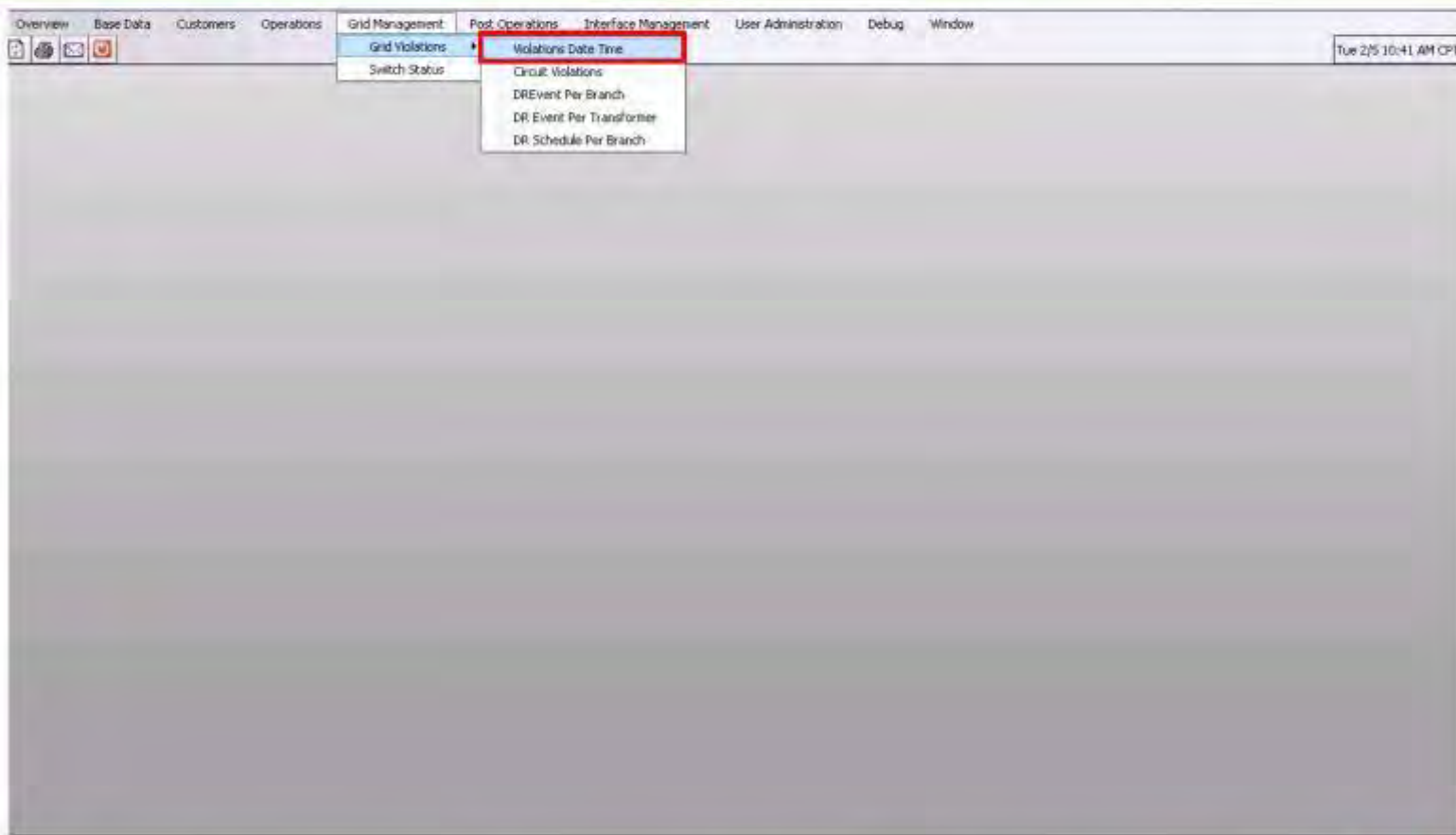
F2	Define Quick Key
F6	Define Quick Key
F7	Define Quick Key
F8	Define Quick Key
F9	Define Quick Key
F10	Define Quick Key
F12	Define Quick Key

2

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Go to "Violations Date Time"



3

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



List of Violations

Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window

Dashboard Violations Date Time Push Web Service Log Web Service Inbound Log

Fri 6/28 12:19 PM CPT

0477 Violations Date Time Study Date: ALL

Case Name	TimeStamp	No Of Violations	Consider for DR Study
RT	06/28/2013 12:19	1	<input type="checkbox"/>

06/28/2013 12:19:30 CPT Page 1 of 1 Record 1 of 1

Get Study Cases Get DPF Limit Violation Get Discrete Measurements

Trace Circuit Violations Switch Status

4 This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Select "Circuit Violations"

The screenshot shows a web application interface with a menu bar at the top containing: Overview, Base Data, Customers, Operations, Grid Management, Post Operations, Interface Management, Settlements, User Administration, Debug, Window. Below the menu bar are several tabs: Dashboard, Violations Date Time, Push Web Service Log, and Web Service Inbound Log. The current date and time are displayed as Fri 6/28 12:19 PM CPT. The main content area is titled "Violations Date Time" with a sub-header "Study Date: ALL". It features a table with the following data:

Case Name	TimeStamp	No Of Violations	Consider for DR Study
RT	06/28/2013 12:19	1	↑

Below the table, there is a status bar indicating "Page 1 of 1" and "Record 1 of 1". A set of buttons is located below the status bar, including "Get Study Cases", "Get DPF Limit Violation", "Get Discrete Measurements", "Trace", "Circuit Violations" (highlighted with a red box), and "Switch Status".

5

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



List of Circuit Violations

Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window

Dashboard Violations Date Time Push Web Service Log Web Service Inbound Log Circuit Violations

Circuit Violations Case Name: RT

Equipment Name	Violation [%]	Limit ABC [A]	Current ABC [A]	Limit Per Phase [A]	Phase A [A]	Phase B [A]	Phase C [A]	Date Time	Description	Chosen for DR
1061021	1730.00	.10	1.83	.10	.00	.00	1.83	06/28/2013 16:19 CPT	Overload	<input checked="" type="checkbox"/>

06/28/2013 12:20:02 CPT Record 1 of 1

Grid Aggregation Required/Available DR

6

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Select "Grid Aggregation"

The screenshot shows a software application window titled "Circuit Violations" with a case name of "RT". The window has a menu bar with options: Overview, Base Data, Customers, Operations, Grid Management, Post Operations, Interface Management, Settlements, User Administration, Debug, and Window. Below the menu bar are several tabs: Dashboard, Violations Date Time, Push Web Service Log, Web Service Inbound Log, and Circuit Violations. The main content area contains a table with the following data:

Equipment Name	Violation [%]	Limit ABC [A]	Current ABC [A]	Limit Per Phase [A]	Phase A [A]	Phase B [A]	Phase C [A]	Date Time	Description	Chosen for DR
1061021	1730.00	.10	1.83	.10	.00	.00	1.83	06/28/2013 16:19 CPT	Overload	<input checked="" type="checkbox"/>

Below the table, there is a status bar showing "06/28/2013 12:20:02 CPT" and "Record 1 of 1". A red box highlights a "Grid Aggregation" button, and next to it is a text field containing "Required/Available DR".

7

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



List of Available DR

Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window

Dashboard Violations Date Time Push Web Service Log Web Service Inbound Log Circuit Violations Required/Available DR Fri 6/28 12:21 PM CPT

Required/ Available DR Case Name: RT

Equipment Name	Required DR per Phase				Available DR per Phase				Requested DR per Phase						
	ABC [kW]	A [kW]	B [kW]	C [kW]	A [A]	B [A]	C [A]	ABC [kW]	A [kW]	B [kW]	C [kW]	ABC [kW]	A [kW]	B [kW]	C [kW]
1081024	12.18	.00	.00	12.18	.00	.00	1.73	26.50	.00	.00	26.40	26.40	.00	.00	26.40

12:21:01 CPT Record 1 of 1

Update DR Event Per Branch

8

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Select "DR Event per Branch"

Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window

Dashboard Violations Date Time Push Web Service Log Web Service Inbound Log Circuit Violations Required/Available DR Fri 6/28 12:21 PM CPT

Required/ Available DR Case Name: RT

Equipment Name	Required DR per Phase				Available DR per Phase				Requested DR per Phase						
	ABC [kW]	A [kW]	B [kW]	C [kW]	A [A]	B [A]	C [A]	ABC [kW]	A [kW]	B [kW]	C [kW]	ABC [kW]	A [kW]	B [kW]	C [kW]
1081024	12.18	.00	.00	12.18	.00	.00	1.73	26.50	.00	.00	26.40	26.40	.00	.00	26.40

12:21:01 CPT Record 1 of 1

Update DR Event Per Branch

9

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



List of DR Events per Branch

Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window

Dashboard Violations Date Time Push Web Service Log Web Service Inbound ... Circuit Violations Required/Available DR DREvent Per Branch Fri 6/28 12:21 PM CPT


DREvent Per Branch Case Name: RT

Equipment Name	Scheduled DR				Requested DR			
	A TkWh	B TkWh	C TkWh	ABC TkWh	A TkWh	B TkWh	C TkWh	ABC TkWh
1061021	.00	.00	26.40	26.40	.00	.00	26.40	26.40

Page 1 of 1 Record 1 of 1

DR Event per Transformer

10 This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Select "DR Event per Transformer"

Equipment Name	Scheduled DR				Requested DR			
	A [kW]	B [kW]	C [kW]	ABC [kW]	A [kW]	B [kW]	C [kW]	ABC [kW]
1061021	.00	.00	26.40	26.40	.00	.00	26.40	26.40

Page 1 of 1 Record 1 of 1

DR Event per Transformer

11

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



List of DR Event per Transformer

Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window

Dashboard X Violations Date Time X Push Web Service ... X Web Service Info... X Circuit Violations X Required/Availabl... X DREvent Per Branch X DR Event Per Tran... X Fri 6/28 12:21 PM CDT

DR Event Per Transformer Case Name: RT

Transformer	Scheduled			Total kW
	DR_A [kW]	DR_B [kW]	DR_C [kW]	
1079335	.00	.00	10.20	10.20
1079330	.00	.00	10.20	10.20
1327575	.00	.00	6.00	6.00
Total	.00	.00	26.40	26.40

9/28/2011 12:21:22 CDT Records: 1-3 of 3

Schedule DR Controls Delete DR Controls Get DRF Solution

Save For Validation Validate DR Event

Select "Schedule DR Controls"

The screenshot displays a software application window titled "DR Event Per Transformer" with a case name of "RT". The window contains a table with the following data:

Transformer	Scheduled			Total KW
	DR_A [kW]	DR_B [kW]	DR_C [kW]	
1079325	.00	.00	10.20	10.20
1079330	.00	.00	10.20	10.20
1327675	.00	.00	6.00	6.00
Total	.00	.00	26.40	26.40

Below the table, the date and time "09/28/2013 12:21:22 CPT" and "Records 1-3 of 3" are displayed. A red box highlights the "Schedule DR Controls" button, which is located next to "Delete DR Controls" and "Get DPF Solution" buttons. Below these are "Save For Validation" and "Validate DR Event" buttons.

13

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Enter Schedule Information

The screenshot displays a software application window titled "DR Event Per Transformer" with "Case Name: RT". The main content area features a table with the following data:

Transformer	Scheduled			
	DR_A [kW]	DR_B [kW]	DR_C [kW]	Total kW
1029325	.00	.00	10.20	10.20
1029330	.00	.00	10.20	10.20
1327575	.00	.00	5.00	5.00
Total	.00	.00	25.40	25.40

Overlaid on the table is a modal dialog box titled "Enter Schedule Information". The dialog contains the following fields and values:

- Schedule Name: GridViolation_RT_DCE Test 1 (05/28/2013)
- Schedule Date: 05/28/2013
- Start Time: 12 : 26
- End Time: 13 : 00

Buttons for "Create" and "Cancel" are visible at the bottom of the dialog.



List of Committed DR Events

Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window

Dashboard Violations Date ... Push Web Serv... Web Service In... Circuit Violations Required/Avail... DREvent Per Br... DR Event Per T... Schedule Event... Fri 6/28 12:23 PM CPT

Schedule Event Summary Date: **Today (06/28/2013)** Interval: **1 Hour Interval**


View Graph	Schedule Event	Program	Date	Status	Strategy	Firm	Notification Date	Start		End		Ramping		Relax	
								Hour	Min	Hour	Min	Begin	End	Time	Ramping / No
<input type="checkbox"/>	GridViolation_RT_06/28/2013_M_67	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 08:03	8	5	8	48	0	0	Yes	Yes
<input type="checkbox"/>	GridViolation_RT_test1(06/28/2013)_68	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 08:57	8	59	8	59	0	0	Yes	Yes
<input type="checkbox"/>	GridViolation_RT_test1(06/28/2013)_69	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 08:57	8	59	8	59	0	0	Yes	Yes
<input type="checkbox"/>	GridViolation_RT_TEST1(06/28/2013)_70	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 09:13	9	15	9	17	0	0	Yes	Yes
<input type="checkbox"/>	GridViolation_RT_TEST1(06/28/2013)_71	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 09:13	9	15	9	17	0	0	Yes	Yes
<input type="checkbox"/>	GridViolation_RT_Test_1(06/28/2013)_72	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 10:43	10	45	10	51	0	0	Yes	Yes
<input type="checkbox"/>	GridViolation_RT_Test_1(06/28/2013)_73	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 10:43	10	45	10	51	0	0	Yes	Yes
<input type="checkbox"/>	801 LCS resource - notification test (06/28/2013)	801 load control devices	06/28/2013	Cancelled	LCS	Yes	06/28/2013 10:55	11	0	23	59			No	No
<input type="checkbox"/>	801 tstat resource - cooling test (06/28/2013)	801 thermostats	06/28/2013	Cancelled	PCT	Yes	06/28/2013 11:07	11	12	23	59			No	No
<input type="checkbox"/>	801 tstat resource - temp change(06/28/2013)	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 11:15	11	20	11	34			No	No
<input type="checkbox"/>	GridViolation_RT_DOE Test 1 (06/28/2013)_74	801 thermostats	06/28/2013	Notified	PCT	Yes	06/28/2013 12:21	12	26	13	0	0	0	Yes	Yes
<input type="checkbox"/>	GridViolation_RT_DOE Test 1 (06/28/2013)_75	801 load control devices	06/28/2013	Notified	LCS	Yes	06/28/2013 12:21	12	26	13	0	0	0	Yes	Yes

12:23:04 Records 1-18 of 18

Modify Reset Update Availability

Select Schedule Event to see the Graph

15 This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Status Changes to Active After Event Starts

Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window

Dashboard Violations Date ... Push Web Serv... Web Service In... Circuit Violations Required/Avail... DR Event Per Br... DR Event Per T... Schedule Event... Fri 6/28 12:23 PM CPT

Schedule Event Summary Date: Today (06/28/2013) Interval: 1 Hour Interval

View Graph	Schedule Event	Program	Date	Status	Strategy	Firm	Notification Date	Start		End		Ramping		Rel	
								Hour	Min	Hour	Min	Begin	End		Time
	GridViolation_RT_06/28/2013_M_67	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 08:03	8	5	8	48	0	0	Yes	Yes
	GridViolation_RT_test1(06/28/2013)_68	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 08:57	8	59	8	59	0	0	Yes	Yes
	GridViolation_RT_test1(06/28/2013)_69	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 08:57	8	59	8	59	0	0	Yes	Yes
	GridViolation_RT_TEST1(06/28/2013)_70	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 09:13	9	15	9	17	0	0	Yes	Yes
	GridViolation_RT_TEST1(06/28/2013)_71	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 09:13	9	15	9	17	0	0	Yes	Yes
	GridViolation_RT_Test_1(06/28/2013)_72	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 10:43	10	45	10	51	0	0	Yes	Yes
	GridViolation_RT_Test_1(06/28/2013)_73	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 10:43	10	45	10	51	0	0	Yes	Yes
	801 LCS resource - notification test (06/28/2013)	801 load control devices	06/28/2013	Cancelled	LCS	Yes	06/28/2013 10:55	11	0	23	59			No	No
	801_tstat resource - cooling test (06/28/2013)	801 thermostats	06/28/2013	Cancelled	PCT	Yes	06/28/2013 11:07	11	12	23	59			No	No
	801_tstat resource - temp change(06/28/2013)	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 11:15	11	20	11	34			No	No
	GridViolation_RT_DCE Test 1 (06/28/2013)_74	801 thermostats	06/28/2013	Active	PCT	Yes	06/28/2013 12:21	12	26	13	0	0	0	Yes	Yes
	GridViolation_RT_DCE Test 1 (06/28/2013)_75	801 load control devices	06/28/2013	Active	LCS	Yes	06/28/2013 12:21	12	26	13	0	0	0	Yes	Yes

06/28/2013 12:26:13 CPT

Records 1-18 of 18

Modify Reset Update Availability

Select Schedule Event to see the Graph

Launch AHE Command Center



17

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Enter Meter Number

Command Center Kansas City Power & Light Test Environment

Setup Network Operations Reporting Help

Search Q+

Executive Dashboard

Executive Dashboard Message Center

smart grid solutions

advanced metering personal energy management distribution automation

manage energy better

Thank you!

Thank you for upgrading to Command Center 5.7.0.

Note: Please take a moment to review our upcoming Classroom and WebEx Training opportunities. Register for a class that's right for you.

2/21/2013 10:04 AM

Welcome back. © 2003-2013 Itron Technologies, LLC a/k/a Landis+Gyr

Event Started in AHE

Gridstream RF Endpoint Information

Meter #1284810711063 Endpoint S/N 4028145577(F0189FA9)

Status: Normal [\[View History\]](#)

Last Reading: 334.0002 - 5/10/2013 2:53 AM

Model: RF Integrated Focus AX

Configuration Group: [RF Residential Configuration HAN DR](#)

Latitude: 39.103626 Longitude: -94.573129

Collector: [801 GAP Collector](#) - Layer: 1

WAN Address: FE.F0.18.9F.A9.80

801 CHARLOTTE ST, KCMO, MO 64106

Current Neighbor: S/N [4045789723\(F125DA1B\)](#) (Normal)

ApTitle: n/a

General Manage Readings Interval Data **History** HAN Security

Please note that at most the 100 most recent events and errors in the last 7 days are being displayed.

Event	Description	Received	Collector
Load control event started	HAN Device Short ID = 50345 Load Control Event ID = 243001 Load Control Event Status Code = 2	6/28/2013 12:26 PM	801 GAP Collector
HAN Load Control Scheduled	SendSmartEnergyPacketText=Success	6/28/2013 12:23 PM	801 GAP Collector
Load control event received	HAN Device Short ID = 50345 Load Control Event ID = 243001 Load Control Event Status Code = 1	6/28/2013 12:23 PM	801 GAP Collector
HAN Load Control All Cancelled	SendSmartEnergyPacketText=Success	6/28/2013 11:35 AM	801 GAP Collector
Endpoint Power Restore	Power restore on serial number 4028145577.	6/28/2013 11:33 AM	801 GAP Collector
			801 GAP



Event Completed in AHE

Gridstream RF Endpoint Information

Meter #1284810711063 Endpoint S/N 4028145577(F0189FA9)

Status: Normal [View History](#)

Last Reading: 334.0002 - 5/10/2013 2:53 AM

Model: RF Integrated Focus AX

Latitude: 39.103626 Longitude: -94.573129

Configuration Group: [RF Residential Configuration HAN DR](#)

WAN Address: FE.F0.18.9F.A9.80

Collector: [801 GAP Collector](#) - Layer: 2

Current Neighbor: S/N [4045789723\(F12SOA1B\)](#) (Normal)

801 CHARLOTTE ST, KCMO, MO 64106

ApTitle: n/a

General Manage Readings Interval Data History HAN Security

Please note that at most the 100 most recent events and errors in the last 7 days are being displayed.

Events

Event	Description	Received	Collector
Load control event completed	HAN Device Short ID = 50345 Load Control Event ID = 243001 Load Control Event Status Code = 3	6/28/2013 1:00 PM	801 GAP Collector
Load control event started	HAN Device Short ID = 50345 Load Control Event ID = 243001 Load Control Event Status Code = 2	6/28/2013 12:26 PM	801 GAP Collector
HAN Load Control Scheduled	SendSmartEnergyPacketText=Success	6/28/2013 12:23 PM	801 GAP Collector
Load control event received	HAN Device Short ID = 50345 Load Control Event ID = 243001 Load Control Event Status Code = 1	6/28/2013 12:23 PM	801 GAP Collector
HAN Load Control All Cancelled	SendSmartEnergyPacketText=Success	6/28/2013 11:35 AM	801 GAP Collector

Demand Response – HAN Devices

- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program



Launch DERM WebUI

The screenshot shows the OATI WebDistribute interface. At the top, there is a navigation menu with items: Overview, Base Data, Customers, Operations, Grid Management, Post Operations, Interface Management, User Administration, Debug, and Window. The browser title is 'Dashboard' and the time is 'Thu 12/19 9:14 AM CPT'. The main content area is divided into several sections:

- DR MANAGEMENT TABULAR:** A table with the following data:

MTD Peak (MW)	.0
Current Billing Demand (MW)	
Current Date/Time	12/19 09:10
Current Temp (F)	
MTD System Peak Demand (MW)	
Current System Peak Demand (MW)	
Current Industrial Load (MW)	.0
- TEMPERATURE FORECAST:** A panel labeled 'UnitSched2'.
- DR AVAILABILITY:** A panel labeled 'UnitSched'.
- SYSTEM:** A table with the following data:

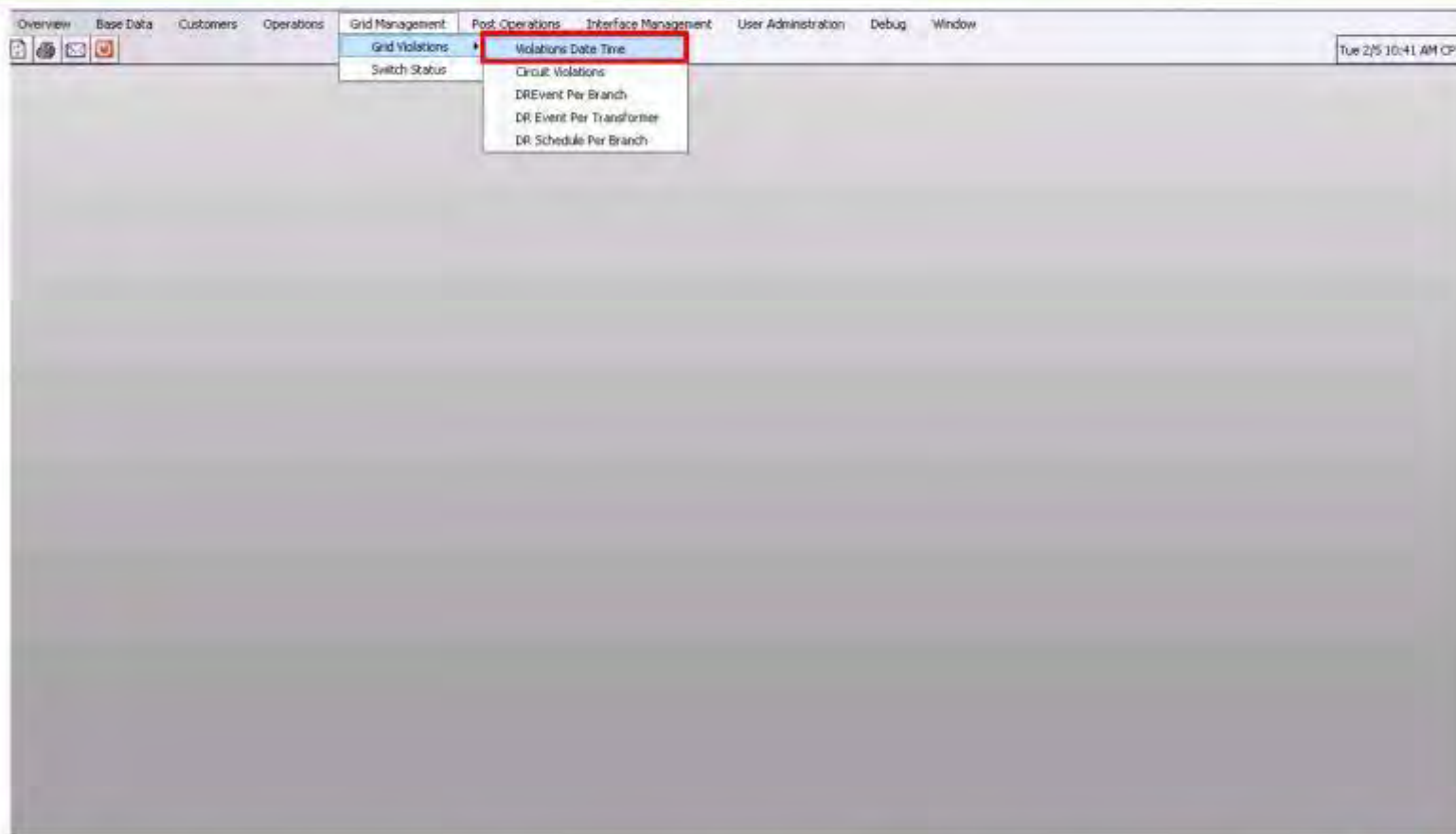
Number of Programs	6
Number of Customers	4382
Number of Asset	759
Users Currently Logged in	1
Number of Resources	26
Committed Schedules	0
Active Schedules	0
Completed Schedules	0
- PERFORMANCE:** A panel labeled 'UnitSched1'.
- QUICK KEY LINKS:** A list of function keys with links to 'Define Quick Key':
 - F2: Define Quick Key
 - F6: Define Quick Key
 - F7: Define Quick Key
 - F8: Define Quick Key
 - F9: Define Quick Key
 - F10: Define Quick Key
 - F12: Define Quick Key

2

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Go to "Violations Date Time"



3

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



List of Violations

The screenshot shows a web application interface with a menu bar at the top containing: Overview, Base Data, Customers, Operations, Grid Management, Post Operations, Interface Management, Settlements, User Administration, Debug, Window. Below the menu is a breadcrumb trail: Dashboard > Violations Date Time > Push Web Service Log > Web Service Inbound Log. The current page title is 'Violations Date Time' and the 'Study Date' is set to 'ALL'. The main content area features a table with the following data:

Case Name	TimeStamp	No Of Violations	Consider for DR Study
RT	06/28/2013 12:19	1	<input type="checkbox"/>

Below the table, there is a status bar indicating 'Page 1 of 1' and 'Record 1 of 1'. A set of buttons is visible, including 'Get Study Cases', 'Get DPF Limit Violation', 'Get Discrete Measurements', 'Trace', 'Circuit Violations', and 'Switch Status'.

4

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Select "Circuit Violations"

The screenshot shows a web application interface with a menu bar at the top containing: Overview, Base Data, Customers, Operations, Grid Management, Post Operations, Interface Management, Settlements, User Administration, Debug, and Window. Below the menu bar are several tabs: Dashboard, Violations Date Time, Push Web Service Log, and Web Service Inbound Log. The current date and time are displayed as Fri 6/28 12:19 PM CPT. The main content area is titled "Violations Date Time" and "Study Date: ALL". It features a table with the following data:

Case Name	TimeStamp	No Of Violations	Consider for DR Study
RT	06/28/2013 12:19	1	↑

Below the table, there is a status bar indicating "Page 1 of 1" and "Record 1 of 1". A set of buttons is located below the status bar, including "Get Study Cases", "Get DPF Limit Violation", "Get Discrete Measurements", "Trace", "Circuit Violations" (highlighted with a red box), and "Switch Status".

5

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



List of Circuit Violations

Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window

Dashboard Violations Date Time Push Web Service Log Web Service Inbound Log Circuit Violations

Circuit Violations Case Name: RT

Equipment Name	Violation [%]	Limit ABC [A]	Current ABC [A]	Limit Per Phase [A]	Phase A [A]	Phase B [A]	Phase C [A]	Date Time	Description	Chosen for DR
1061021	1730.00	.10	1.83	.10	.00	.00	1.83	06/28/2013 16:19 CPT	Overload	<input checked="" type="checkbox"/>

06/28/2013 12:20:02 CPT Record 1 of 1

Grid Aggregation Required/Available DR

6

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Select "Grid Aggregation"

Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window

Dashboard Violations Date Time Push Web Service Log Web Service Inbound Log Circuit Violations

Circuit Violations Case Name: RT

Equipment Name	Violation [%]	Limit ABC [A]	Current ABC [A]	Limit Per Phase [A]	Phase A [A]	Phase B [A]	Phase C [A]	Date Time	Description	Chosen for DR
1061021	1730.00	.10	1.83	.10	.00	.00	1.83	06/28/2013 16:19 CPT	Overload	<input checked="" type="checkbox"/>
06/28/2013 12:20:02 CPT										Record 1 of 1

Grid Aggregation Required/Available DR.

7

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



List of Available DR

Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window

Dashboard Violations Date Time Push Web Service Log Web Service Inbound Log Circuit Violations Required/Available DR Fri 6/28 12:21 PM CPT

Required/ Available DR Case Name: RT

Equipment Name	Required DR per Phase				Available DR per Phase				Requested DR per Phase						
	ABC [kW]	A [kW]	B [kW]	C [kW]	A [A]	B [A]	C [A]	ABC [kW]	A [kW]	B [kW]	C [kW]	ABC [kW]	A [kW]	B [kW]	C [kW]
1081024	12.18	.00	.00	12.18	.00	.00	1.73	26.40	.00	.00	26.40	26.40	.00	.00	26.40

12:21:01 CPT Record 1 of 1

Update DR Event Per Branch

8

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Select "DR Event per Branch"

Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window

Dashboard Violations Date Time Push Web Service Log Web Service Inbound Log Circuit Violations Required/Available DR Fri 6/28 12:21 PM CPT

Required/ Available DR Case Name: RT

Equipment Name	Required DR per Phase				Available DR per Phase				Requested DR per Phase						
	ABC [kW]	A [kW]	B [kW]	C [kW]	A [A]	B [A]	C [A]	ABC [kW]	A [kW]	B [kW]	C [kW]	ABC [kW]	A [kW]	B [kW]	C [kW]
1081024	12.18	.00	.00	12.18	.00	.00	1.73	26.50	.00	.00	26.40	26.40	.00	.00	26.40

12:21:01 CPT Record 1 of 1

Update DR Event Per Branch

9

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



List of DR Events per Branch

Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window

Dashboard Violations Date Time Push Web Service Log Web Service Inbound ... Circuit Violations Required/Available DR DREvent Per Branch Fri 6/28 12:21 PM CPT


DREvent Per Branch Case Name: RT

Equipment Name	Scheduled DR				Requested DR			
	A TkWh	B TkWh	C TkWh	ABC TkWh	A TkWh	B TkWh	C TkWh	ABC TkWh
1061021	.00	.00	26.40	26.40	.00	.00	26.40	26.40

Page 1 of 1 Record 1 of 1

DR Event per Transformer

10 This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Select "DR Event per Transformer"

Equipment Name	Scheduled DR				Requested DR			
	A [kW]	B [kW]	C [kW]	ABC [kW]	A [kW]	B [kW]	C [kW]	ABC [kW]
1061021	.00	.00	26.40	26.40	.00	.00	26.40	26.40

Page 1 of 1 Record 1 of 1

DR Event per Transformer

List of DR Event per Transformer

Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window

Dashboard X Violations Date Time X Push Web Service ... X Web Service Info... X Circuit Violations X Required/Availabl... X DREvent Per Branch X DR Event Per Tran... X Fri 6/28 12:21 PM CDT

DR Event Per Transformer Case Name: RT

Transformer	Scheduled			Total kW
	DR_A [kW]	DR_B [kW]	DR_C [kW]	
1079335	.00	.00	10.20	10.20
1079330	.00	.00	10.20	10.20
1327575	.00	.00	6.00	6.00
Total	.00	.00	26.40	26.40

6/28/2011 12:21:22 CDT Records: 1-3 of 3

Schedule DR Controls Delete DR Controls Get DRF Solution

Save For Validation Validate DR Event

Select "Schedule DR Controls"

The screenshot shows a software application window titled "DR Event Per Transformer" with a case name of "RT". The window contains a table with the following data:

Transformer	Scheduled			Total KW
	DR_A [kW]	DR_B [kW]	DR_C [kW]	
1079325	.00	.00	10.20	10.20
1079330	.00	.00	10.20	10.20
1327675	.00	.00	6.00	6.00
Total	.00	.00	26.40	26.40

Below the table, the date and time are shown as "09/28/2013 12:21:22 CPT" and "Records 1-3 of 3". A red box highlights the "Schedule DR Controls" button, which is located next to "Delete DR Controls" and "Get DPF Solution" buttons. Below these are "Save For Validation" and "Validate DR Event" buttons.

13

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Enter Schedule Information

The screenshot displays a software application window titled "DR Event Per Transformer" with "Case Name: RT". The main content area features a table with the following data:

Transformer	Scheduled			Total kW
	DR_A [kW]	DR_B [kW]	DR_C [kW]	
1029325	.00	.00	10.20	10.20
1029330	.00	.00	10.20	10.20
1327575	.00	.00	5.00	5.00
Total	.00	.00	25.40	25.40

An "Enter Schedule Information" dialog box is overlaid on the table. It contains the following fields:

- Schedule Name: GridViolation_RT_DCE Test 1 (05/28/2013)
- Schedule Date: 05/28/2013
- Start Time: 12 : 26
- End Time: 13 : 00

Buttons for "Create" and "Cancel" are visible at the bottom of the dialog box.

List of Committed DR Events

Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window

Dashboard Violations Date ... Push Web Serv... Web Service In... Circuit Violations Required/Avail... DREvent Per Br... DR Event Per T... Schedule Event... Fri 6/28 12:23 PM CPT

Schedule Event Summary Date: **Today (06/28/2013)** Interval: **1 Hour Interval**


View Graph	Schedule Event	Program	Date	Status	Strategy	Firm	Notification Date	Start		End		Ramping		Relax	
								Hour	Min	Hour	Min	Begin	End	Time	Ramping / No
<input type="checkbox"/>	GridViolation_RT_06/28/2013_M_67	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 08:03	8	5	8	48	0	0	Yes	Yes
<input type="checkbox"/>	GridViolation_RT_test1(06/28/2013)_68	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 08:57	8	59	8	59	0	0	Yes	Yes
<input type="checkbox"/>	GridViolation_RT_test1(06/28/2013)_69	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 08:57	8	59	8	59	0	0	Yes	Yes
<input type="checkbox"/>	GridViolation_RT_TEST1(06/28/2013)_70	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 09:13	9	15	9	17	0	0	Yes	Yes
<input type="checkbox"/>	GridViolation_RT_TEST1(06/28/2013)_71	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 09:13	9	15	9	17	0	0	Yes	Yes
<input type="checkbox"/>	GridViolation_RT_Test_1(06/28/2013)_72	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 10:43	10	45	10	51	0	0	Yes	Yes
<input type="checkbox"/>	GridViolation_RT_Test_1(06/28/2013)_73	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 10:43	10	45	10	51	0	0	Yes	Yes
<input type="checkbox"/>	801 LCS resource - notification test (06/28/2013)	801 load control devices	06/28/2013	Cancelled	LCS	Yes	06/28/2013 10:55	11	0	23	59			No	No
<input type="checkbox"/>	801 tstat resource - cooling test (06/28/2013)	801 thermostats	06/28/2013	Cancelled	PCT	Yes	06/28/2013 11:07	11	12	23	59			No	No
<input type="checkbox"/>	801 tstat resource - temp change(06/28/2013)	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 11:15	11	20	11	34			No	No
<input type="checkbox"/>	GridViolation_RT_DOE Test 1 (06/28/2013)_74	801 thermostats	06/28/2013	Notified	PCT	Yes	06/28/2013 12:21	12	26	13	0	0	0	Yes	Yes
<input type="checkbox"/>	GridViolation_RT_DOE Test 1 (06/28/2013)_75	801 load control devices	06/28/2013	Notified	LCS	Yes	06/28/2013 12:21	12	26	13	0	0	0	Yes	Yes

12:23:04 Records 1-18 of 18

Modify Reset Update Availability

Select Schedule Event to see the Graph

15 This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Status Changes to Active After Event Starts

Overview Base Data Customers Operations Grid Management Post Operations Interface Management Settlements User Administration Debug Window

Dashboard X Violations Date ... X Push Web Serv... X Web Service In... X Circuit Violations X Required/Avail... X DR Event Per Br... X DR Event Per T... X Schedule Event... X

Schedule Event Summary Date: Today (06/28/2013) Interval: 1 Hour Interval

View Graph	Schedule Event	Program	Date	Status	Strategy	Firm	Notification Date	Start		End		Ramping		Rel.	
								Hour	Min	Hour	Min	Begin	End		Time
	GridViolation_RT_06/28/2013_67	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 08:03	8	5	8	48	0	0	Yes	Yes
	GridViolation_RT_test1(06/28/2013)_68	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 08:57	8	59	8	59	0	0	Yes	Yes
	GridViolation_RT_test1(06/28/2013)_69	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 08:57	8	59	8	59	0	0	Yes	Yes
	GridViolation_RT_TEST1(06/28/2013)_70	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 09:13	9	15	9	17	0	0	Yes	Yes
	GridViolation_RT_TEST1(06/28/2013)_71	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 09:13	9	15	9	17	0	0	Yes	Yes
	GridViolation_RT_Test_1(06/28/2013)_72	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 10:43	10	45	10	51	0	0	Yes	Yes
	GridViolation_RT_Test_1(06/28/2013)_73	801 load control devices	06/28/2013	Aborted	LCS	Yes	06/28/2013 10:43	10	45	10	51	0	0	Yes	Yes
	801 LCS resource - notification test (06/28/2013)	801 load control devices	06/28/2013	Cancelled	LCS	Yes	06/28/2013 10:55	11	0	23	59			No	No
	801_tstat resource - cooling test (06/28/2013)	801 thermostats	06/28/2013	Cancelled	PCT	Yes	06/28/2013 11:07	11	12	23	59			No	No
	801_tstat resource - temp change(06/28/2013)	801 thermostats	06/28/2013	Aborted	PCT	Yes	06/28/2013 11:15	11	20	11	34			No	No
	GridViolation_RT_DCE Test 1 (06/28/2013)_74	801 thermostats	06/28/2013	Active	PCT	Yes	06/28/2013 12:21	12	26	13	0	0	0	Yes	Yes
	GridViolation_RT_DCE Test 1 (06/28/2013)_75	801 load control devices	06/28/2013	Active	LCS	Yes	06/28/2013 12:21	12	26	13	0	0	0	Yes	Yes

06/28/2013 12:26:13 CPT

Records 1-18 of 18

Modify Reset Update Availability

Select Schedule Event to see the Graph

Thermostat Before the DR Event (Pre-Event)



Launch KCP&L Portal – HAN Devices (During-Event)

Lab_1284810711065 - Help - Sign Out RIDING ALONG

TEMP 73° OUTLETS 1 2 3

GET OUTLETS

- Desk Light ON OFF
- LCS ON OFF
- Outlet ON OFF

Edit Settings

Your Account Summary Account Settings Device Settings Device Schedule & R

Events

Action/Response	Event Type	Start	End	Duration	Status
Opt In	Load Control	12:26 PM, Jun 28	01:00 PM, Jun 28	34min	In Progress
Opt In	Load Control	12:26 PM, Jun 28	01:00 PM, Jun 28	34min	In Progress
Opt In	Load Control	11:20 AM, Jun 28	12:00 PM, Jun 28	40min	Canceled
Opt In	Load Control	11:12 AM, Jun 28	11:59 PM, Jun 28	12hr 47min	Canceled
Opt In	Load Control	11:00 AM, Jun 28	11:59 PM, Jun 28	12hr 59min	Canceled



KCP&L Portal – Temperature (During-Event)

Lab_1284810711065 Help Sign Out RIDING ALONG

KCP&L
energizing life

TEMP 73° OUTLETS 1 2 3

Thermostat 1

ACTUAL TEMP 73°

77°

Edit Settings

Your Account Summary Account Settings Device Settings Events

Events

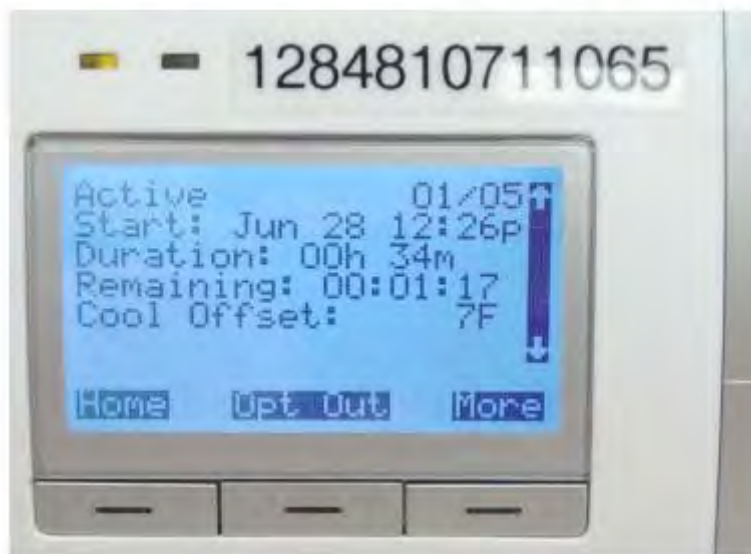
Action/Response	Event Type	Start	End	Duration	Status
Opt In	Load Control	12:26 PM, Jun 28	01:00 PM, Jun 28	34min	In Progress
Opt In	Load Control	12:26 PM, Jun 28	01:00 PM, Jun 28	34min	In Progress
Opt In	Load Control	11:20 AM, Jun 28	12:00 PM, Jun 28	40min	Canceled
Opt In	Load Control	11:12 AM, Jun 28	11:59 PM, Jun 28	12hr 47min	Canceled
Opt In	Load Control	11:00 AM, Jun 28	11:59 PM, Jun 28	12hr 59min	Canceled

19

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Thermostat During the DR Event (During-Event)



Launch KCP&L Portal – HAN Devices (After-Event)

The screenshot shows the KCP&L portal interface. At the top right, the user is logged in as 'Lab_1284810711065' with options for 'Help' and 'Sign Out'. The temperature is displayed as 73° and there are three outlets listed. A 'SET OUTLETS' dropdown menu is open, showing 'Desk Light', 'LCS', and 'Outlet', each with 'ON' and 'OFF' buttons. The 'ON' buttons for 'Desk Light' and 'Outlet' are highlighted with a red box. Below the navigation tabs, the 'Your Account' section is visible with sub-links for 'Summary', 'Account Settings', 'Device Settings', and 'Device Schedule & R'. The 'Events' section contains a table with the following data:

Action/Response	Event Type	Start	End	Duration	Status
Opt In	Load Control	12:26 PM, Jun 28	01:00 PM, Jun 28	34min	Completed
Opt In	Load Control	12:26 PM, Jun 28	01:00 PM, Jun 28	34min	Completed
Opt In	Load Control	11:20 AM, Jun 28	12:00 PM, Jun 28	40min	Canceled
Opt In	Load Control	11:12 AM, Jun 28	11:59 PM, Jun 28	12hr 47min	Canceled
Opt In	Load Control	11:00 AM, Jun 28	11:59 PM, Jun 28	12hr 59min	Canceled

21

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



KCP&L Portal – Temperature (After-Event)

Lab_1284810711065 - Help - Sign Out RIDING ALONG

TEMP 73° OUTLETS 1 2 3

Thermostat 1

ACTUAL TEMP 73°

70°

Edit Settings

Your Account Summary Account Settings Device Settings Device Events

Events

Action/Response	Event Type	Start	End	Duration	Status
Opt In	Load Control	12:26 PM, Jun 28	01:00 PM, Jun 28	34min	Completed
Opt In	Load Control	12:26 PM, Jun 28	01:00 PM, Jun 28	34min	Completed
Opt In	Load Control	11:20 AM, Jun 28	12:00 PM, Jun 28	40min	Canceled
Opt In	Load Control	11:12 AM, Jun 28	11:59 PM, Jun 28	12hr 47min	Canceled
Opt In	Load Control	11:00 AM, Jun 28	11:59 PM, Jun 28	12hr 59min	Canceled

22

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Thermostat After the DR Event (After-Event)

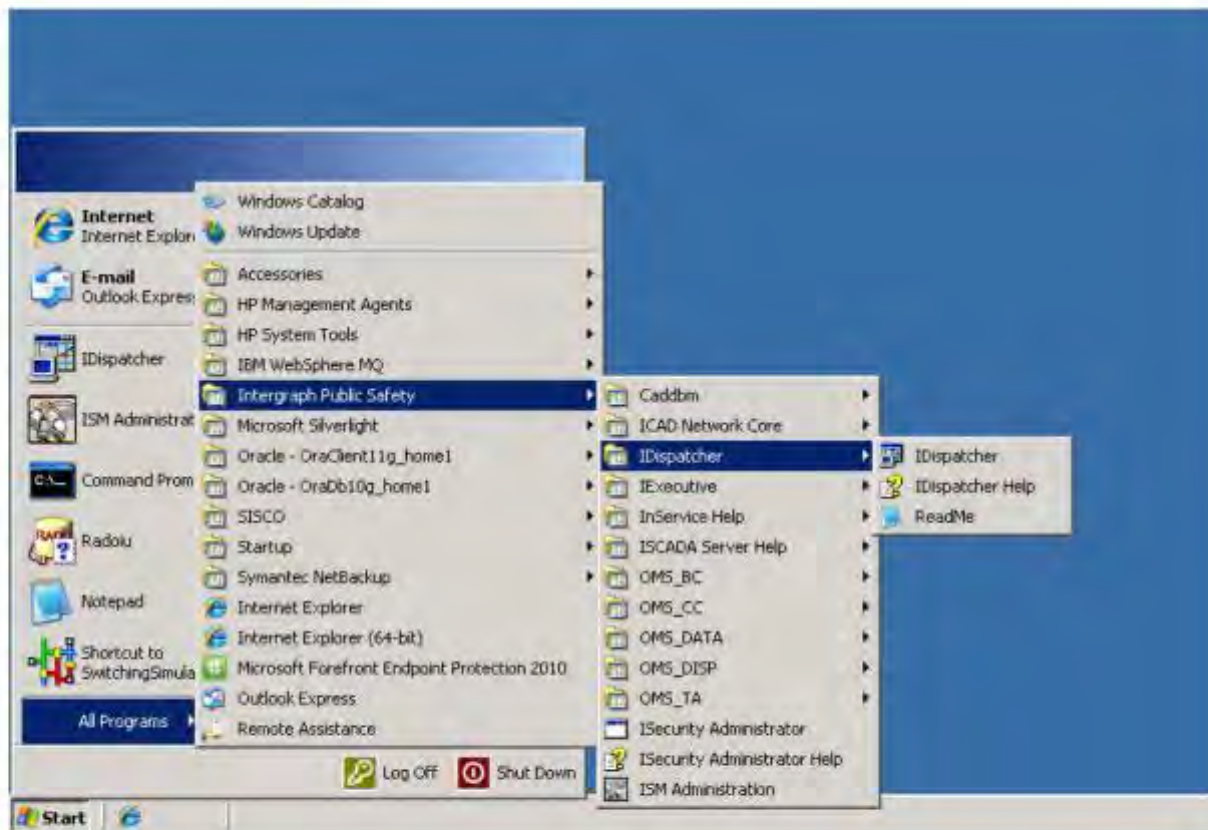


Demand Response – Battery

- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program



Launch InService I/Dispatcher



2

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



InService I/Dispatcher Main Screen

Job Number	Job Type	Location
0002593	TRF	JA 2092
0002595	FDR	7532
0002596	RCL	1860007
0002597	FDR	7532
0002598	FDR	7532
0002599	FDR	7532
0002581	FDR	7532
0002582	FDR	7532
0002583	FDR	7532
0002584	FDR	7532
0002585	FDR	7532
0002586	FDR	7532
0002587	FDR	7532
0002488	FDR	7532

Unit	A	Type	St	Time	Event Number	Event	Loc
36		FS	AQ	21587 34			
36		FS	AV	0850 11			7532
55		FS	AV	22080 42			JA
74		FS	ER	08230 95	00025943	SWC	143
75		FS	AQ	21587 34			
75		FS	AM	11762 95			F97
75		FS	AQ	21587 34			
75		FS	AQ	21587 34			
75		FS	AQ	21587 34			
75		FS	AQ	21587 34			
75		FS	AQ	21587 34			
75		FS	AQ	21587 34			
75		FS	AQ	21587 34			
75		FS	AQ	21587 34			

Agency	R	P	Loc Unit	Area	Group	Event Number	ET
FLDSDW							
RESTORE							

3

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Feature Information: Battery

Workstation Crew Job Info View Inquiry Tools Database InService Report/Info Admin/Config View/Display Help

Feature Information
Device: 1888105 Refresh

Name	Value
Active State	Normal
Active Status	OFF
Alarm - Inhibit	OK
Alarm - Isolate	OK
Alarm - Trip Offline	OK
Alarm - Warning	Alarm
BESS Status	Enabled
Charge Mode	OFF
Energy Available (%)	69
Local - Remote	Local
Power Mode	OFF
Reactive Mode	Fixed KVAR
Recalculation Time (sec)	0
SCADA Device Comm Failure	OK
Schedule Override Status	Disabled
KVAR - Discharge Duration (min)	5
KVAR - Discharge Start Time (0-23)	13
KVAR - Fixed PF (%)	0
KVAR - Max Discharge Rate	125
KW - Charge Duration (min)	0
KW - Charge Following	0
KW - Charge Start Time (0-23)	0
KW - Discharge Duration (min)	5
KW - Discharge Start Time (0-23)	0
KW - Load Following	0
KW - Max Charge Rate	0
KW - Max Discharge Rate	100

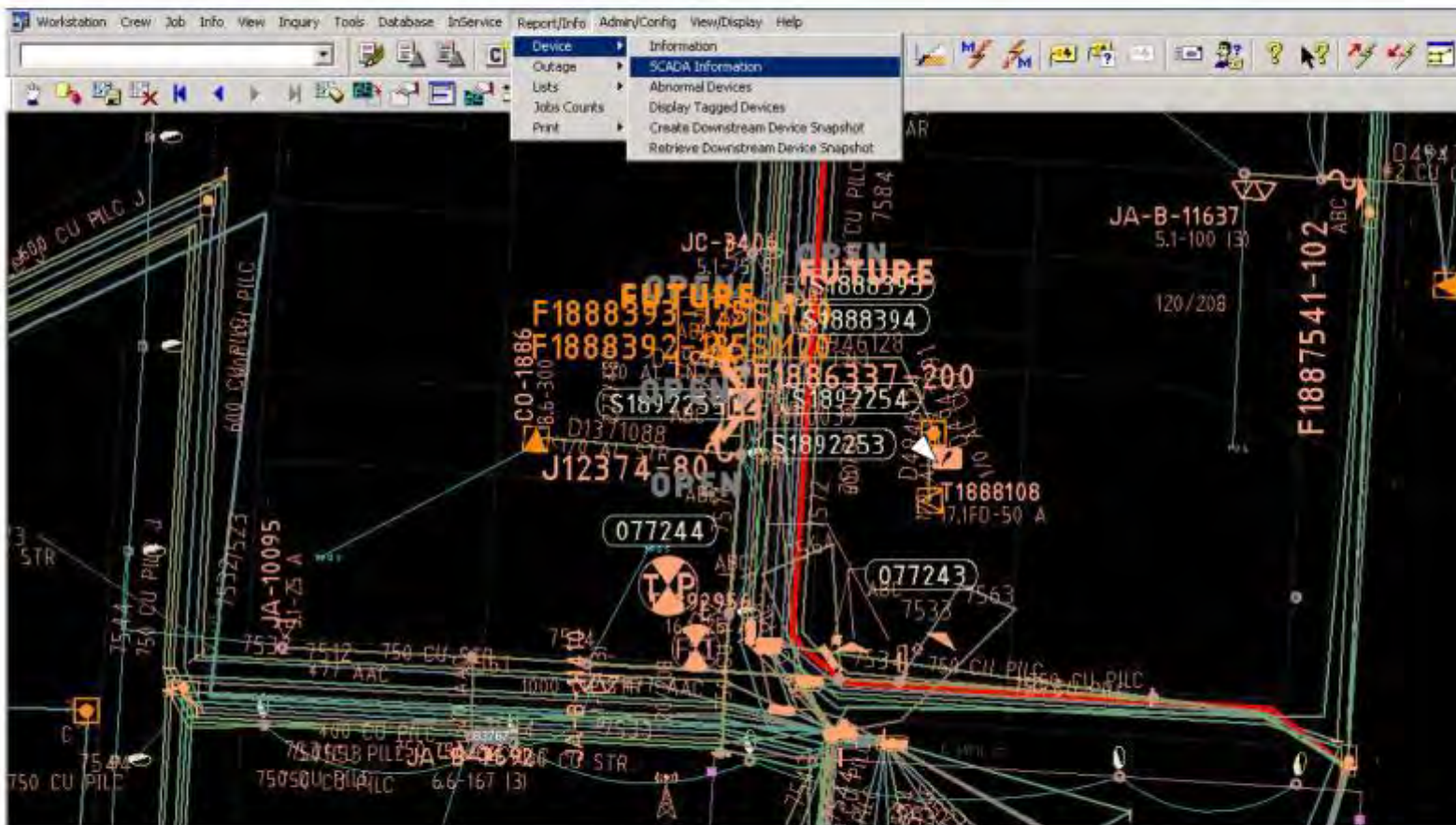
Right Click to Control SCADA points

4

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Launch “SCADA Device Information”

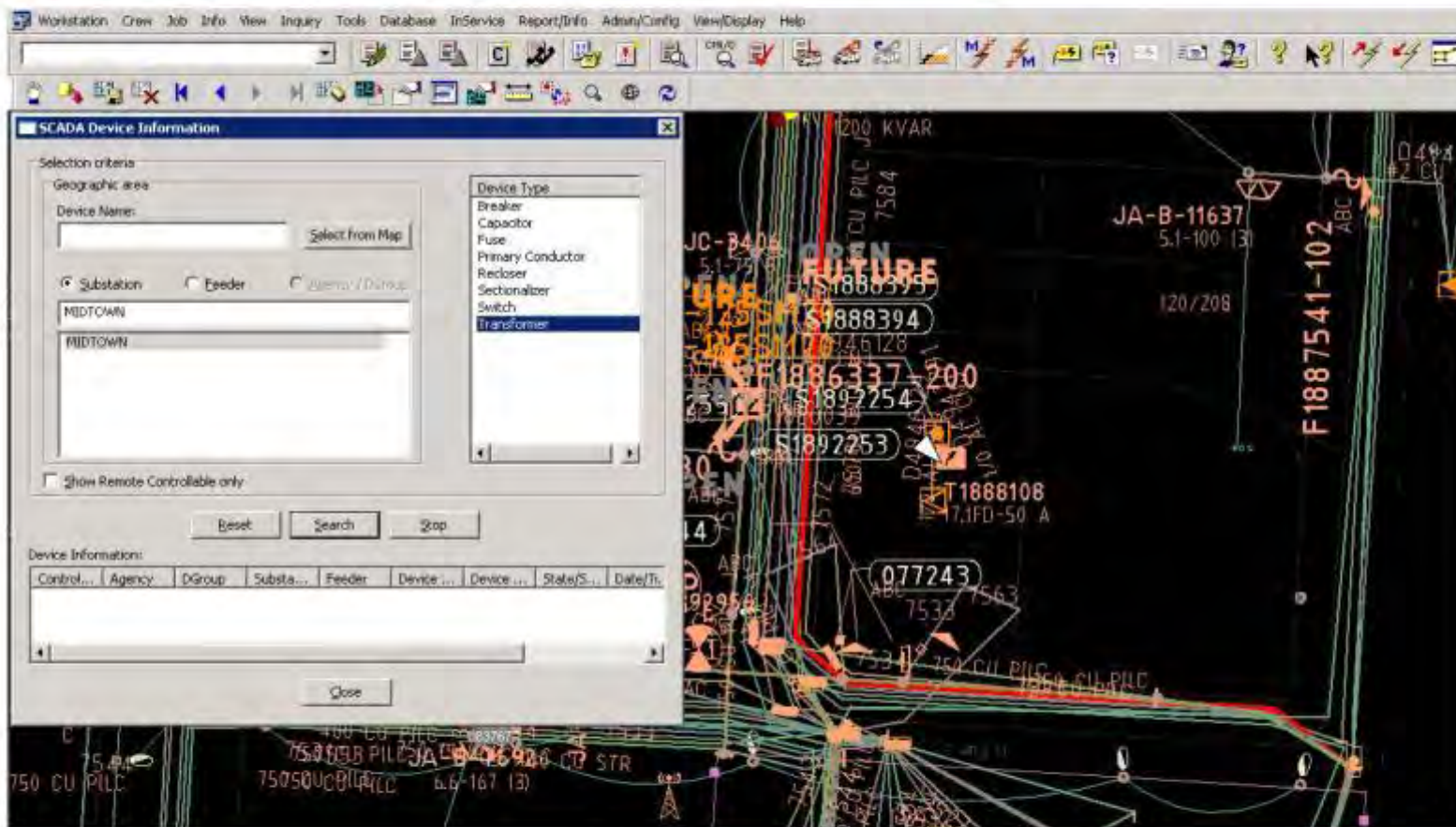


5

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



SCADA Device Information Window



6

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Battery in Device Information

The screenshot displays the SCADA Device Information interface. On the left, a search window titled "SCADA Device Information" is open. It includes a "Selection criteria" section with a "Device Name" field containing "1888105" and a "Select from Map" button. Below this are radio buttons for "Substation", "Feeder", and "Battery (0/0/0)". A list box shows "MIDTOWN" selected. A "Device Type" list on the right includes Breaker, Capacitor, Fuse, Primary Conductor, Reducer, Sectionalizer, Switch, and Transformer. At the bottom of the search window is a table with the following data:

Control...	Agency	DGroup	Substa...	Feeder	Device Type	Device ...	State/S...	Date
Y	FLDSRV	FLDSV	MIDTOWN	7564	Transformer	1888105		

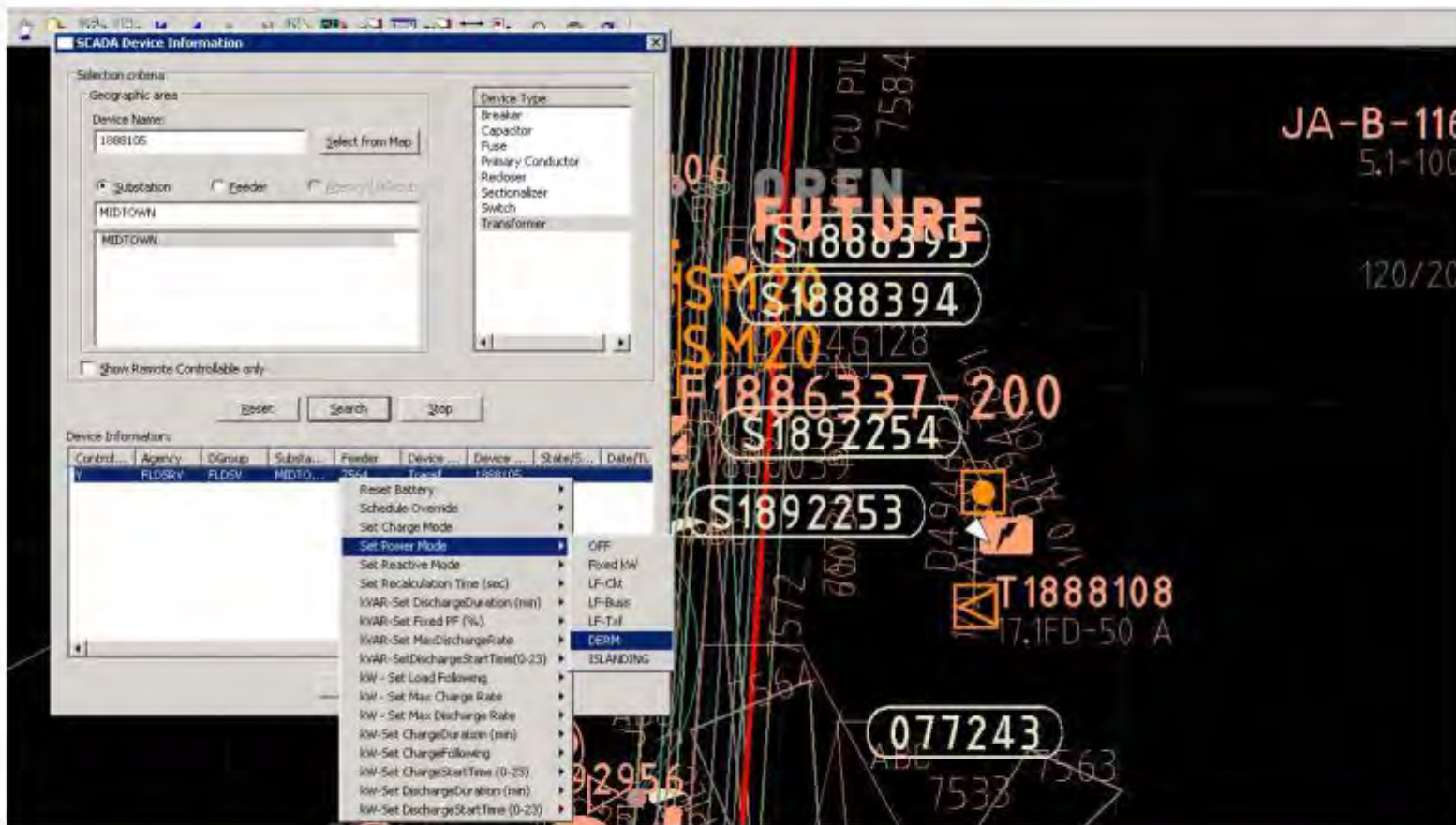
Buttons for "Reset", "Search", "Stop", and "Close" are also visible. The background shows a network diagram with various components labeled, including "200 KVAR", "JA-B-11637 5.1-100 13", "F1887541-102 ABC", "T1888108 7,IFD-50 A", and "S1888394".

■ 7

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Set Battery to DERM Mode



8

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Battery set to DERM Power Mode

The screenshot displays a SCADA software interface. On the left, a 'Feature Information' window is open for device '1888105'. The 'Power Mode' is highlighted in red and set to 'DERM'. The main window shows a detailed power grid diagram with various components and labels.

Name	Value
Active State	Ready
Active Status	Event(s) Pending
Alarm - Inhibit	OK
Alarm - Isolate	OK
Alarm - Trip Offline	OK
Alarm - Warning	OK
BESS Status	Enabled
Charge Mode	OFF
Energy Available (%)	99
Local - Remote	Remote
Power Mode	DERM
Reactive Mode	OFF
Recalculation Time (sec)	0
SCAM Device Comm Failure	OK
Schedule Override Status	Disabled
KVAR - Discharge Duration (min)	0
KVAR - Discharge Start Time (0-23)	0
KVAR - Fixed PF (%)	0
KVAR - Max Discharge Rate	0
KW - Charge Duration (min)	0
KW - Charge Following	0
KW - Charge Start Time (0-23)	0
KW - Discharge Duration (min)	0
KW - Discharge Start Time (0-23)	0
KW - Load Following	0
KW - Max Charge Rate	0
KW - Max Discharge Rate	0

9

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Launch DERM WebUI

DR MANAGEMENT TABULAR

MTD Peak (MW)	.0
Current Billing Demand (MW)	
Current Date/Time	12/19 09:10
Current Temp (F)	
MTD System Peak Demand (MW)	
Current System Peak Demand (MW)	
Current Industrial Load (MW)	.0

SYSTEM

Number of Programs	6
Number of Customers	4382
Number of Asset	759
Users Currently Logged in	1
Number of Resources	26
Committed Schedules	0
Active Schedules	0
Completed Schedules	0

QUICK KEY LINKS

F2	Define Quick Key
F6	Define Quick Key
F7	Define Quick Key
F8	Define Quick Key
F9	Define Quick Key
F10	Define Quick Key
F12	Define Quick Key

10

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Go to "Resource Summary"

The screenshot shows the OATI WebDistribute software interface. At the top, there is a navigation menu with tabs: Overview, Base Data, Customers, Operations, Grid Management, Post Operations, Interface Management, User Administration, Debug, and Window. The 'Operations' tab is active, and a dropdown menu is open, showing options: Weather Forecast, Resources (highlighted with a red box), Availability Assessment, Scheduling, Voltage Reduction DR, DR Analysis, Dispatch, and Workflow. The 'Resources' dropdown also has sub-options: Create Resource, Resource Summary (highlighted with a red box), and Program Resource Group Summary. The main dashboard area is divided into several sections: DR MANAGEMENT TABULAR (with metrics like MTD Peak, Current Billing Demand, etc.), TEMPERATURE FORECAST (UnitSched2), DR AVAILABILITY (UnitSched), SYSTEM (with metrics like Number of Programs, Customers, Assets, etc.), PERFORMANCE (UnitSched1), and QUICK KEY LINKS (F2-F12). The OATI logo and 'OATI WebDistribute' text are visible in the top left and right respectively. The date and time 'Thu 12/19 9:14 AM CPT' are shown in the top right corner.

11

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



List of Available Resources

Select	Resource	Resource Type	Program	Product	Response Time	Location Detail	Asset Detail	Customer Detail	Resource Capacity	Assets	Start Date	End Date
<input type="checkbox"/>	GridViolation_RT_-_test1(06/28/2013)_69	Violation	801 load control devices	Capacity	1 Min	View	View	View	16.0	2	06/26/2013	06/20/2014
<input type="checkbox"/>	GridViolation_RT_TEST1(06/28/2013)_70	Violation	801 thermostats	Capacity	1 Min	View	View	View	10.4	4	06/26/2013	06/26/2014
<input type="checkbox"/>	GridViolation_RT_TEST1(06/28/2013)_71	Violation	801 load control devices	Capacity	1 Min	View	View	View	16.0	2	06/26/2013	06/20/2014
<input type="checkbox"/>	GridViolation_RT_Test_1_(06/28/2013)_72	Violation	801 thermostats	Capacity	1 Min	View	View	View	10.4	4	06/26/2013	06/26/2014
<input type="checkbox"/>	GridViolation_RT_Test_1_(06/28/2013)_73	Violation	801 load control devices	Capacity	1 Min	View	View	View	16.0	2	06/26/2013	06/20/2014
<input type="checkbox"/>	801 thermostat resource	Dynamic	801 thermostats	Energy	1 Min	View	View	View	10.4	4	06/26/2013	06/26/2014
<input type="checkbox"/>	GridViolation_RT_DOE_Test_1_(06/28/2013)_74	Violation	801 thermostats	Capacity	1 Min	View	View	View	10.4	4	06/26/2013	06/26/2014
<input type="checkbox"/>	GridViolation_RT_DOE_Test_1_(06/28/2013)_75	Violation	801 load control devices	Capacity	1 Min	View	View	View	16.0	3	06/28/2013	06/28/2013
<input type="checkbox"/>	GridViolation_RT_(07/11/2013)_76	Violation	801 thermostats	Capacity	1 Min	View	View	View	10.4	3	06/26/2013	06/26/2014
<input type="checkbox"/>	GridViolation_RT_(07/11/2013)_77	Violation	801 load control devices	Capacity	1 Min	View	View	View	20.0	2	07/11/2013	07/11/2013
<input type="checkbox"/>	GridViolation_RT_(07/18/2013)_78	Violation	801 thermostats	Capacity	1 Min	View	View	View	10.4	4	06/26/2013	06/26/2014
<input type="checkbox"/>	GridViolation_RT_(07/18/2013)_79	Violation	801 load control devices	Capacity	1 Min	View	View	View	26.0	5	07/18/2013	07/18/2013
<input type="checkbox"/>	GridViolation_RT_(07/18/2013)_80	Violation	801 thermostats	Capacity	1 Min	View	View	View	10.4	4	06/26/2013	06/26/2014
<input type="checkbox"/>	GridViolation_RT_(07/18/2013)_81	Violation	801 load control devices	Capacity	1 Min	View	View	View	26.0	5	07/18/2013	07/18/2013
<input type="checkbox"/>	GridViolation_RT_(07/18/2013)_82	Violation	801 thermostats	Capacity	1 Min	View	View	View	10.4	4	06/26/2013	06/26/2014
<input type="checkbox"/>	GridViolation_RT_(07/18/2013)_83	Violation	801 load control devices	Capacity	1 Min	View	View	View	26.0	5	07/18/2013	07/18/2013
<input type="checkbox"/>	GridViolation_RT_(07/29/2013)_84	Violation	801 thermostats	Capacity	1 Min	View	View	View	10.4	4	06/26/2013	06/26/2014
<input type="checkbox"/>	GridViolation_RT_(07/29/2013)_85	Violation	801 load control devices	Capacity	1 Min	View	View	View	26.0	5	07/29/2013	07/29/2013
<input type="checkbox"/>	GridViolation_RT_(07/29/2013)_86	Violation	801 thermostats	Capacity	1 Min	View	View	View	10.4	4	06/26/2013	06/26/2014
<input type="checkbox"/>	GridViolation_RT_(07/29/2013)_87	Violation	801 load control devices	Capacity	1 Min	View	View	View	26.0	5	07/29/2013	07/29/2013
<input checked="" type="checkbox"/>	Battery	Dynamic	Battery	Energy	Daily	View	View	View	1000.0	1	08/12/2013	06/20/2014
<input type="checkbox"/>	ChargePoint_Resource	Program Dynamic	ChargePoint	Capacity	Daily	View	View	View	10.0	1	10/01/2013	06/20/2014

12

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



“Schedule Resource” to Schedule DR Event

Select	Resource	Resource Type	Program	Product	Response Time	Location Detail	Asset Detail	Customer Detail	Resource Capacity	Assets	Start Date	End Date
<input type="checkbox"/>	GridViolation_RT -- test1(06/28/2013)_69	Violation	801 load control devices	Capacity	1 Min	View	View	View	16.0	2	06/26/2013	06/20/2014
<input type="checkbox"/>	GridViolation_RT_TEST1(06/28/2013)_70	Violation	801 thermostats	Capacity	1 Min	View	View	View	10.4	4	06/26/2013	06/26/2014
<input type="checkbox"/>	GridViolation_RT_TEST1(06/28/2013)_71	Violation	801 load control devices	Capacity	1 Min	View	View	View	16.0	2	06/26/2013	06/20/2014
<input type="checkbox"/>	GridViolation_RT_Test_1 (06/28/2013)_72	Violation	801 thermostats	Capacity	1 Min	View	View	View	10.4	4	06/26/2013	06/26/2014
<input type="checkbox"/>	GridViolation_RT_Test_1 (06/28/2013)_73	Violation	801 load control devices	Capacity	1 Min	View	View	View	16.0	2	06/26/2013	06/20/2014
<input type="checkbox"/>	801 thermostat resource	Dynamic	801 thermostats	Energy	1 Min	View	View	View	10.4	4	06/26/2013	06/26/2014
<input type="checkbox"/>	GridViolation_RT_DOE_Test_1 (06/28/2013)_74	Violation	801 thermostats	Capacity	1 Min	View	View	View	10.4	4	06/26/2013	06/26/2014
<input type="checkbox"/>	GridViolation_RT_DOE_Test_1 (06/28/2013)_75	Violation	801 load control devices	Capacity	1 Min	View	View	View	16.0	3	06/28/2013	06/28/2013
<input type="checkbox"/>	GridViolation_RT (07/11/2013)_76	Violation	801 thermostats	Capacity	1 Min	View	View	View	10.4	3	06/26/2013	06/26/2014
<input type="checkbox"/>	GridViolation_RT (07/11/2013)_77	Violation	801 load control devices	Capacity	1 Min	View	View	View	20.0	2	07/11/2013	07/11/2013
<input type="checkbox"/>	GridViolation_RT (Ilya_0718)_78	Violation	801 thermostats	Capacity	1 Min	View	View	View	10.4	4	06/26/2013	06/26/2014
<input type="checkbox"/>	GridViolation_RT (Ilya_0718)_79	Violation	801 load control devices	Capacity	1 Min	View	View	View	26.0	5	07/18/2013	07/18/2013
<input type="checkbox"/>	GridViolation_RT (Ilya0718)_80	Violation	801 thermostats	Capacity	1 Min	View	View	View	10.4	4	06/26/2013	06/26/2014
<input type="checkbox"/>	GridViolation_RT (Ilya0718)_81	Violation	801 load control devices	Capacity	1 Min	View	View	View	26.0	5	07/18/2013	07/18/2013
<input type="checkbox"/>	GridViolation_RT (07/18/Ilya)_82	Violation	801 thermostats	Capacity	1 Min	View	View	View	10.4	4	06/26/2013	06/26/2014
<input type="checkbox"/>	GridViolation_RT (07/18/Ilya)_83	Violation	801 load control devices	Capacity	1 Min	View	View	View	26.0	5	07/18/2013	07/18/2013
<input type="checkbox"/>	GridViolation_RT (07/29/2013)_84	Violation	801 thermostats	Capacity	1 Min	View	View	View	10.4	4	06/26/2013	06/26/2014
<input type="checkbox"/>	GridViolation_RT (07/29/2013)_85	Violation	801 load control devices	Capacity	1 Min	View	View	View	26.0	5	07/29/2013	07/29/2013
<input type="checkbox"/>	GridViolation_RT (07/29/Ilya)_86	Violation	801 thermostats	Capacity	1 Min	View	View	View	10.4	4	06/26/2013	06/26/2014
<input type="checkbox"/>	GridViolation_RT (07/29/Ilya)_87	Violation	801 load control devices	Capacity	1 Min	View	View	View	26.0	5	07/29/2013	07/29/2013
<input checked="" type="checkbox"/>	Battery	Dynamic	Battery	Energy	Daily	View	View	View	1000.0	1	08/12/2013	06/20/2014
<input type="checkbox"/>	ChargePoint_Resource	Program Dynamic	ChargePoint	Capacity	Daily	View	View	View	10.0	1	10/01/2013	06/20/2014

09:14:31
Page 2 of 2
Records 31 - 56 of 56

13

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Enter Schedule Information

The screenshot displays a web application interface with a menu bar at the top (Overview, Base Data, Customers, Operations, Grid Management, Post Operations, Interface Management, User Administration, Debug, Window) and a breadcrumb trail (Dashboard > Resource Summary). The main content area features a table of resources with columns: Select, Resource, Resource Type, Program, Product, Response Time, Location Detail, Asset Detail, Customer Detail, Resource Capacity, Assets, Start Date, and End Date. A modal window titled "Enter Schedule Information" is overlaid on the table, containing the following fields:

- Schedule Name: Battery - test1 (12/19/2013)
- Schedule Date: 12/19/2013
- Start Time: 10 : 00 Notification: 12/19/2013 09:20
- End Time: 10 : 10 Notification: 12/19/2013 10:10
- Relax Notifications:
- Relax Program Time Constraints:
- Create button

At the bottom of the interface, there is a status bar showing "Page 2 of 2" and "Records 50-56 of 56".

14

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Event Schedule Created

The screenshot displays a web application interface for resource management. At the top, there is a navigation menu with options like Overview, Base Data, Customers, Operations, Grid Management, Post Operations, Interface Management, User Administration, Debug, and Window. Below the menu is a breadcrumb trail: Dashboard > Resource Summary. The main content area features a table with columns: Select, Resource, Resource Type, Program, Product, Response Time, Location Detail, Asset Detail, Customer Detail, Resource Capacity, Assets, Start Date, and End Date. The table lists various resources such as 'GridViolation_RT - test1(06/28/2013)_69', 'GridViolation_RT_TEST1(06/28/2013)_70', and 'Battery'. A modal dialog box titled 'Enter Schedule Information' is open, showing fields for Schedule Name (Battery), Schedule Date (12/19/), Start Time (10), and End Time (10). Below these fields are checkboxes for 'Relax Notifications' and 'Relax Program Time Constraints', and a 'Create' button. A 'Message from webpage' dialog box is also open, displaying a yellow warning icon and the text 'Schedule(s) created successfully', with an 'OK' button highlighted by a red box. At the bottom of the interface, there is a status bar showing 'Page: 2 of 2' and 'Records: 31-56 of 96'. Buttons for 'Schedule Resource', 'New Resource', and 'Delete Resource' are visible at the bottom center.

15

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Go to "Schedule Event Summary"

Select	Resource	Type	Response Time	Location Detail	Asset Detail	Customer Detail	Resource Capacity	Assets	Start Date	End Date
<input type="checkbox"/>	GridViolation_RT_03/26/2013_42	Violation	1 Min	View	View	View	338.0	167	03/26/2013	03/26/2013
<input type="checkbox"/>	GridViolation_RT_03/26/2013_43	Violation	1 Min	View	View	View	338.0	167	03/26/2013	03/26/2013
<input type="checkbox"/>	GridViolation_RT_03/27/2013_44	Violation	1 Min	View	View	View	8.0	4	03/27/2013	03/27/2013
<input type="checkbox"/>	GridViolation_RT_04/01/2013_45	Violation	1 Min	View	View	View	8.0	4	04/01/2013	04/01/2013
<input type="checkbox"/>	GridViolation_RT_04/01/2013_46	Violation	1 Min	View	View	View	8.0	4	04/01/2013	04/01/2013
<input type="checkbox"/>	GridViolation_RT_04/02/2013_47	Violation	1 Min	View	View	View	8.0	4	04/02/2013	04/02/2013
<input type="checkbox"/>	GridViolation_RT_04/03/2013_48	Violation	1 Min	View	View	View	8.0	4	04/03/2013	04/03/2013
<input type="checkbox"/>	GridViolation_RT_04/03/2013_49	Violation	1 Min	View	View	View	6.0	2	04/03/2013	04/03/2013
<input type="checkbox"/>	GridViolation_RT_04/03/2013_50	Violation	1 Min	View	View	View	8.0	4	04/03/2013	04/03/2013
<input type="checkbox"/>	GridViolation_RT_04/03/2013_51	Violation	1 Min	View	View	View	2.0	1	04/03/2013	04/03/2013
<input type="checkbox"/>	GridViolation_RT_04/03/2013_52	Violation	1 Min	View	View	View	6.0	2	04/03/2013	04/03/2013
<input type="checkbox"/>	GridViolation_RT_04/04/2013_53	Violation	1 Min	View	View	View	8.0	4	04/04/2013	04/04/2013
<input type="checkbox"/>	GridViolation_RT_04/08/2013_54	Violation	1 Min	View	View	View	8.0	4	04/08/2013	04/08/2013
<input type="checkbox"/>	GridViolation_RT_04/11/2013_55	Violation	1 Min	View	View	View	8.0	4	04/11/2013	04/11/2013
<input type="checkbox"/>	GridViolation_STUDY_250_04/11/2013_56	Violation	1 Min	View	View	View	8.0	4	04/11/2013	04/11/2013
<input type="checkbox"/>	GridViolation_STUDY_250_04/11/2013_57	Violation	1 Min	View	View	View	8.0	4	04/11/2013	04/11/2013
<input type="checkbox"/>	GridViolation_STUDY_251_05/08/2013_58	Violation	1 Min	View	View	View	8.0	4	05/08/2013	05/08/2013
<input type="checkbox"/>	GridViolation_RT_05/09/2013_59	Violation	1 Min	View	View	View	8.0	4	05/09/2013	05/09/2013
<input type="checkbox"/>	GridViolation_RT_05/09/2013_60	Violation	1 Min	View	View	View	8.0	4	05/09/2013	05/09/2013
<input type="checkbox"/>	GridViolation_RT_3/05/09/2013_61	Violation	1 Min	View	View	View	8.0	4	05/09/2013	05/09/2013
<input type="checkbox"/>	GridViolation_RT_ItvaEvent_60	Violation	1 Min	View	View	View	8.0	4	05/15/2013	05/15/2013
<input type="checkbox"/>	801 LCS resource	Dynamic	1 Min	View	View	View	26.0	5	06/26/2013	06/20/2014

16

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



List of Scheduled Event Summaries

Overview Base Data Customers Operations Grid Management Post Operations Interface Management User Administration Debug Window

Dashboard Resource Summary Schedule Event Summary Thu 12/19 9:16 AM CPT

647 Schedule Event Summary Date: ALL Interval: 1 Hour Interval

Schedule Event	Program	Date	Status	Strategy	Firm	Notification Date	Start		End		Ramping		Relax	
							Hour	Min	Hour	Min	Begin	End	Time	Ramping
Battery - test8(11/06/2013)	Battery	11/06/2013	Aborted	LCS	Yes	11/06/2013 14:57	15	00	15	12			No	No
Battery - test10(11/07/2013)	Battery	11/07/2013	Cancelled	LCS	Yes	11/06/2013 15:18	04	00	04	30			No	No
Battery - test11(11/06/2013)	Battery	11/06/2013	Cancelled	LCS	Yes	11/06/2013 16:05	17	00	17	12			No	No
Battery - test13(11/06/2013)	Battery	11/06/2013	Completed	LCS	Yes	11/06/2013 16:11	17	00	17	08			No	No
ChargePoint_Resource - test1(11/13/2013)	ChargePoint	11/13/2013	Completed	CYCLING	Yes	11/13/2013 08:58	09	00	09	15			No	No
801 total resource - test1(11/21/2013)	801 thermostats	11/21/2013	Cancelled	PCT	Yes	11/21/2013 17:17	17	27	17	35			No	No
801 total resource - test2(11/21/2013)	801 thermostats	11/21/2013	Completed	PCT	Yes	11/21/2013 17:19	17	29	17	35			No	No
801 LCS resource - test1(11/25/2013)	801 load control devices	11/25/2013	Completed	LCS	Yes	11/25/2013 11:15	11	20	11	25			No	No
801 total resource - test2(11/25/2013)	801 thermostats	11/25/2013	Completed	PCT	Yes	11/25/2013 11:46	11	56	12	00			No	No
ChargePoint_Resource(12/02/2013)	ChargePoint	12/02/2013	Completed	CYCLING	Yes	12/02/2013 10:03	10	05	10	10			No	No
ChargePoint_Resource - test2(12/02/2013)	ChargePoint	12/02/2013	Completed	CYCLING	Yes	12/02/2013 10:28	10	30	10	40			No	No
ChargePoint_Resource(12/04/2013)	ChargePoint	12/04/2013	Cancelled	CYCLING	Yes	12/04/2013 04:08	04	10	04	12			No	No
ChargePoint_Resource(12/03/2013)	ChargePoint	12/03/2013	Aborted	CYCLING	Yes	12/03/2013 16:11	16	13	16	17			No	No
ChargePoint_Resource(12/03/2013)_2	ChargePoint	12/03/2013	Completed	CYCLING	Yes	12/03/2013 17:53	17	55	17	59			No	No
ChargePoint_Resource(12/04/2013)_1	ChargePoint	12/04/2013	Completed	CYCLING	Yes	12/04/2013 12:19	12	21	12	22			No	No
ChargePoint_Resource(12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 08:03	08	05	08	10			No	No
ChargePoint_Resource - test2(12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 08:25	08	27	08	33			No	No
ChargePoint_Resource - test5(12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 04:13	04	15	04	25			No	No
ChargePoint_Resource - test7(12/06/2013)	ChargePoint	12/06/2013	Aborted	CYCLING	Yes	12/06/2013 16:15	16	17	16	24			No	No
801 LCS resource - test1(12/06/2013)	801 load control devices	12/06/2013	Completed	LCS	Yes	12/06/2013 16:16	16	21	16	25			No	No
ChargePoint_Resource - test10(12/06/2013)	ChargePoint	12/06/2013	Aborted	CYCLING	Yes	12/06/2013 16:26	16	26	16	28			No	No
801 LCS resource - test2(12/06/2013)	801 load control devices	12/06/2013	Cancelled	LCS	Yes	12/06/2013 16:32	16	37	16	42			No	No
ChargePoint_Resource - test13(12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 17:38	17	40	17	55			No	No
Battery(12/11/2013)	Battery	12/11/2013	Cancelled	LCS	Yes	12/11/2013 09:55	10	00	10	59			No	No
ChargePoint_Resource(12/09/2013)	ChargePoint	12/09/2013	Completed	CYCLING	Yes	12/09/2013 15:15	15	17	15	20			No	No
Battery(12/10/2013)	Battery	12/10/2013	Aborted	LCS	Yes	12/10/2013 11:05	11	10	11	20			No	No
Battery(12/19/2013)	Battery	12/19/2013	Cancelled	LCS	Yes	12/19/2013 09:10	10	00	10	10			No	No
Battery - test1(12/19/2013)	Battery	12/19/2013	Committed	LCS	Yes	12/19/2013 09:20	10	00	10	10			No	No

12/19/2013 09:16:02 CPT Records 1-211 of 211

Modify Reset Update Availability

Status Change to "Notified" after Event Sent from DERM

Overview Base Data Customers Operations Grid Management Post Operations Interface Management User Administration Debug Window

Dashboard Resource Summary Schedule Event Summary Thu 12/19 9:20 AM CPT

Schedule Event Summary Date: ALL Interval: 1 Hour Interval

Schedule Event	Program	Date	Status	Strategy	Firm	Notification Date	Start		End		Ramping		Relax		
							Hour	Min	Hour	Min	Begin	End	Time	Ramping	Notified
Battery - test9(11/06/2013)	Battery	11/06/2013	Aborted	LCS	Yes	11/06/2013 14:57	15	00	15	12			No	No	No
Battery - test10(11/07/2013)	Battery	11/07/2013	Cancelled	LCS	Yes	11/06/2013 15:18	04	00	04	30			No	No	No
Battery - test11(11/06/2013)	Battery	11/06/2013	Cancelled	LCS	Yes	11/06/2013 16:05	17	00	17	12			No	No	No
Battery - test13(11/06/2013)	Battery	11/06/2013	Completed	LCS	Yes	11/06/2013 16:11	17	00	17	08			No	No	No
ChargePoint_Resource - test1(11/13/2013)	ChargePoint	11/13/2013	Completed	CYCLING	Yes	11/13/2013 08:58	09	00	09	15			No	No	No
801 test resource - test 1(11/21/2013)	801 thermostats	11/21/2013	Cancelled	PCT	Yes	11/21/2013 17:17	17	27	17	35			No	No	No
801 test resource - test2(11/21/2013)	801 thermostats	11/21/2013	Completed	PCT	Yes	11/21/2013 17:19	17	29	17	35			No	No	No
801 LCS resource - test 1(11/25/2013)	801 load control devices	11/25/2013	Completed	LCS	Yes	11/25/2013 11:15	11	20	11	25			No	No	No
801 test resource - test2(11/25/2013)	801 thermostats	11/25/2013	Completed	PCT	Yes	11/25/2013 11:46	11	56	12	00			No	No	No
ChargePoint_Resource (12/02/2013)	ChargePoint	12/02/2013	Completed	CYCLING	Yes	12/02/2013 10:03	10	05	10	10			No	No	No
ChargePoint_Resource - test2(12/02/2013)	ChargePoint	12/02/2013	Completed	CYCLING	Yes	12/02/2013 10:28	10	30	10	40			No	No	No
ChargePoint_Resource (12/04/2013)	ChargePoint	12/04/2013	Cancelled	CYCLING	Yes	12/04/2013 04:08	04	10	04	12			No	No	No
ChargePoint_Resource (12/03/2013)	ChargePoint	12/03/2013	Aborted	CYCLING	Yes	12/03/2013 16:11	16	13	16	17			No	No	No
ChargePoint_Resource (12/03/2013)_2	ChargePoint	12/03/2013	Completed	CYCLING	Yes	12/03/2013 17:53	17	55	17	59			No	No	No
ChargePoint_Resource (12/04/2013)_1	ChargePoint	12/04/2013	Completed	CYCLING	Yes	12/04/2013 12:19	12	21	12	22			No	No	No
ChargePoint_Resource (12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 08:03	08	05	08	10			No	No	No
ChargePoint_Resource - test3(12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 08:25	08	27	08	33			No	No	No
ChargePoint_Resource - test5(12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 04:13	04	15	04	25			No	No	No
ChargePoint_Resource - test 7(12/06/2013)	ChargePoint	12/06/2013	Aborted	CYCLING	Yes	12/06/2013 16:15	16	17	16	24			No	No	No
801 LCS resource - test 1(12/06/2013)	801 load control devices	12/06/2013	Completed	LCS	Yes	12/06/2013 16:16	16	21	16	25			No	No	No
ChargePoint_Resource - test 10(12/06/2013)	ChargePoint	12/06/2013	Aborted	CYCLING	Yes	12/06/2013 16:26	16	28	16	28			No	No	No
801 LCS resource - test2(12/06/2013)	801 load control devices	12/06/2013	Cancelled	LCS	Yes	12/06/2013 16:32	16	37	16	42			No	No	No
ChargePoint_Resource-test13(12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 17:38	17	40	17	55			No	No	No
Battery (12/11/2013)	Battery	12/11/2013	Cancelled	LCS	Yes	12/11/2013 09:55	10	00	10	59			No	No	No
ChargePoint_Resource (12/09/2013)	ChargePoint	12/09/2013	Completed	CYCLING	Yes	12/09/2013 15:15	15	17	15	20			No	No	No
Battery (12/10/2013)	Battery	12/10/2013	Aborted	LCS	Yes	12/10/2013 11:05	11	10	11	20			No	No	No
Battery (12/19/2013)	Battery	12/19/2013	Cancelled	LCS	Yes	12/19/2013 09:10	10	00	10	10			No	No	No
Battery - test1 (12/19/2013)	Battery	12/19/2013	Notified	LCS	Yes	12/19/2013 09:20	10	00	10	10			No	No	No

12/19/2013 09:20:52 27 Records 1-211 of 211

Modify Reset Update Availability

18

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Go to Web Service Inbound Log

Item	Message ID	Request Time	Response Time	Web Service Name	Outcome	Status	Outbound XML	Inbound XML	Message Content
5738	83060	12/19/2013 07:30:01	12/19/2013 07:30:02	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5739	83061	12/19/2013 07:35:00	12/19/2013 07:35:01	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5740	83062	12/19/2013 07:40:01	12/19/2013 07:40:02	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5741	83063	12/19/2013 07:45:02	12/19/2013 07:45:03	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5742	83064	12/19/2013 07:50:01	12/19/2013 07:50:01	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5743	83065	12/19/2013 07:55:01	12/19/2013 07:55:02	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5744	83066	12/19/2013 08:00:01	12/19/2013 08:00:02	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5745	83067	12/19/2013 08:05:01	12/19/2013 08:05:02	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5746	83068	12/19/2013 08:10:05	12/19/2013 08:10:06	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5747	83069	12/19/2013 08:15:01	12/19/2013 08:15:03	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5748	83090	12/19/2013 08:20:02	12/19/2013 08:20:03	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5749	83091	12/19/2013 08:25:01	12/19/2013 08:25:02	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5750	83092	12/19/2013 08:30:01	12/19/2013 08:30:02	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5751	83093	12/19/2013 08:35:01	12/19/2013 08:35:02	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5752	83094	12/19/2013 08:40:02	12/19/2013 08:40:03	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5753	83095	12/19/2013 08:45:01	12/19/2013 08:45:02	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5754	83096	12/19/2013 08:50:00	12/19/2013 08:50:01	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5755	83097	12/19/2013 08:55:01	12/19/2013 08:55:02	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5756	83098	12/19/2013 09:00:01	12/19/2013 09:00:03	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5757	83099	12/19/2013 09:05:01	12/19/2013 09:05:03	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5758	83100	12/19/2013 09:10:01	12/19/2013 09:10:02	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5759	83101	12/19/2013 09:10:02	12/19/2013 09:10:03	DMSDERMPutGetMessageServices	Success	Undefined	View	View	View
5760	83102	12/19/2013 09:15:01	12/19/2013 09:15:03	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5761	83103	12/19/2013 09:20:01	12/19/2013 09:20:02	DMSDERMPutGetMessageServices	Success	Success	View	View	View
5762	83104	12/19/2013 09:20:02	12/19/2013 09:20:03	DMSDERMPutGetMessageServices	Success	Undefined	View	View	View



Web Service Inbound Logs

Overview Base Data Customers Operations Grid Management Post Operations Interface Management User Administration Debug Window

Dashboard Resource Summary Schedule Event Summary Push Web Service Log Web Service Inbound Log Thu 12/19/13 7:23 AM PPT

Web Service Inbound Log Duration: Today (12/19/2013)

Transaction ID	Request Time	Respond Time	Operation	Message Type	Sender	Outcome	Client Certificate Issuer	Client Certificate Identifier	Outbound XML	Inbound XML	Message Content
105351	12/19/2013 09:10	12/19/2013 09:10	DMSDERMPutMessageService	Deleted Distribution PowerLine Limit Violation	10.238.1.168	Success	view	view	view	view	view
105352	12/19/2013 09:20	12/19/2013 09:20	DMSDERMPutMessageService	LoadCreatedEvent	10.238.1.168	Success	view	view	view	view	view

Records 91-92 of 92

Page 4 of 4

OMS: Battery Information Updated

Workstation: Crew Job Info View Inquiry Tools Database InService Report/Info Admin/Config View/Display Help

Feature Information
Device: 1890105 Refresh

Attributes	Counts	SCADA	DNA
Name	Value		
Active State	Ready		
Active Status	Event(s) Pending		
Alarm - Inhibit	OK		
Alarm - Isolate	OK		
Alarm - Trip Offline	OK		
Alarm - Warning	OK		
BESS Status	Enabled		
Charge Mode	OFF		
Energy Available (%)	90		
Local - Remote	Remote		
Power Mode	DERM		
Reactive Mode	OFF		
Recalculation Time (sec)	0		
SICAM Device Comm Failure	OK		
Schedule Override Status	Disabled		
IWAR - Discharge Duration (min)	0		
IWAR - Discharge Start Time (0-23)	0		
IWAR - Fixed PF (%)	0		
IWAR - Max Discharge Rate	0		
kW - Charge Duration (min)	0		
kW - Charge Following	0		
kW - Charge Start Time (0-23)	0		
kW - Discharge Duration (min)	10		
kW - Discharge Start Time (0-23)	10		
kW - Load Following	0		
kW - Max Charge Rate	0		
kW - Max Discharge Rate	800		

Right Click to Control SCADA points

21

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



DERM: Status Updated to Active after Event Started

Overview Base Data Customers Operations Grid Management Post Operations Interface Management User Administration Debug Window

Dashboard Resource Summary Schedule Event Summary Push Web Service Log Web Service Inbound Log Thu 12/19 10:03 AM CPT

Schedule Event Summary Date: ALL Interval: 1 Hour Interval

Schedule Event	Program	Date	Status	Strategy	Firm	Notification Date	Start		End		Ramping		Relax	
							Hour	Min	Hour	Min	Begin	End	Time	Ramping
Battery - test6(11/06/2013)	Battery	11/06/2013	Aborted	LCS	Yes	11/06/2013 14:57	15	00	15	12			No	No
Battery - test10(11/07/2013)	Battery	11/07/2013	Cancelled	LCS	Yes	11/06/2013 15:18	04	00	04	30			No	No
Battery - test11(11/06/2013)	Battery	11/06/2013	Cancelled	LCS	Yes	11/06/2013 16:05	17	00	17	12			No	No
Battery - test13(11/06/2013)	Battery	11/06/2013	Completed	LCS	Yes	11/06/2013 16:11	17	00	17	08			No	No
ChargePoint_Resource - test1(11/13/2013)	ChargePoint	11/13/2013	Completed	CYCLING	Yes	11/13/2013 08:58	09	00	09	15			No	No
801_tstat_resource - test1(11/21/2013)	801 thermostats	11/21/2013	Cancelled	PCT	Yes	11/21/2013 17:17	17	27	17	35			No	No
801_tstat_resource - test2(11/21/2013)	801 thermostats	11/21/2013	Completed	PCT	Yes	11/21/2013 17:19	17	29	17	35			No	No
801_LCS_resource - test1(11/25/2013)	801 load control devices	11/25/2013	Completed	LCS	Yes	11/25/2013 11:15	11	20	11	25			No	No
801_tstat_resource - test2(11/25/2013)	801 thermostats	11/25/2013	Completed	PCT	Yes	11/25/2013 11:46	11	56	12	00			No	No
ChargePoint_Resource(12/02/2013)	ChargePoint	12/02/2013	Completed	CYCLING	Yes	12/02/2013 10:03	10	05	10	10			No	No
ChargePoint_Resource - test2(12/02/2013)	ChargePoint	12/02/2013	Completed	CYCLING	Yes	12/02/2013 10:29	10	30	10	40			No	No
ChargePoint_Resource(12/04/2013)	ChargePoint	12/04/2013	Cancelled	CYCLING	Yes	12/04/2013 04:08	04	10	04	12			No	No
ChargePoint_Resource(12/03/2013)	ChargePoint	12/03/2013	Aborted	CYCLING	Yes	12/03/2013 16:11	16	13	16	17			No	No
ChargePoint_Resource(12/03/2013)_2	ChargePoint	12/03/2013	Completed	CYCLING	Yes	12/03/2013 17:53	17	55	17	59			No	No
ChargePoint_Resource(12/04/2013)_1	ChargePoint	12/04/2013	Completed	CYCLING	Yes	12/04/2013 12:19	12	21	12	22			No	No
ChargePoint_Resource(12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 08:03	08	05	08	10			No	No
ChargePoint_Resource - test2(12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 08:25	08	27	08	33			No	No
ChargePoint_Resource - test5(12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 04:13	04	15	04	25			No	No
ChargePoint_Resource - test7(12/06/2013)	ChargePoint	12/06/2013	Aborted	CYCLING	Yes	12/06/2013 16:15	16	17	16	24			No	No
801_LCS_resource - test1(12/06/2013)	801 load control devices	12/06/2013	Completed	LCS	Yes	12/06/2013 16:16	16	21	16	25			No	No
ChargePoint_Resource - test10(12/06/2013)	ChargePoint	12/06/2013	Aborted	CYCLING	Yes	12/06/2013 16:26	16	28	16	28			No	No
801_LCS_resource - test2(12/06/2013)	801 load control devices	12/06/2013	Cancelled	LCS	Yes	12/06/2013 16:32	16	37	16	42			No	No
ChargePoint_Resource - test13(12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 17:38	17	40	17	55			No	No
Battery(12/11/2013)	Battery	12/11/2013	Cancelled	LCS	Yes	12/11/2013 09:55	10	00	10	59			No	No
ChargePoint_Resource(12/09/2013)	ChargePoint	12/09/2013	Completed	CYCLING	Yes	12/09/2013 15:15	15	17	15	20			No	No
Battery(12/10/2013)	Battery	12/10/2013	Aborted	LCS	Yes	12/10/2013 11:05	11	10	11	20			No	No
Battery(12/19/2013)	Battery	12/19/2013	Cancelled	LCS	Yes	12/19/2013 09:10	10	00	10	10			No	No
Battery - test1(12/19/2013)	Battery	12/19/2013	Active	LCS	Yes	12/19/2013 09:20	10	00	10	10			No	No

12/19/2013 10:03:41 CPT Records 1-211 of 211

Modify Reset Update Availability

22

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Launch SMS System Menu

The screenshot displays a Linux desktop environment. On the left side, there are several desktop icons: a folder named 'sandc', a 'Browser Based HMI' icon, and a 'Firefox Web Browser' icon which is highlighted with a red rectangular box. In the top right corner, a terminal window is open, displaying the following system information:

```
sandc@falom-u1004
Ubuntu 10.04 LTS
kernel: 2.6.35-25-generic

Image Name: 20111130_BASE-CCP
Site Name: SMS_Evergenix KCPL
Eth1: 192.168.13.100
Eth2: Not Defined

Uptime: 2362.20

For Technical Assistance
Reference: PUREWAVE
Business Hours: 0800-1700 CST M-F
Business Phone: 414-623-8778
After Hours Emergency #: 773-338-1000
```

At the bottom of the desktop, the taskbar shows the system tray with the date and time: 'Thu Mar 14, 10:38 AM'. The system status icons include network, volume, and power.

■23 This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

SMS System Menu: Go to SMS PCS Online

SMS SYSTEM MENU - Mozilla Firefox
http://localhost/menu

SMS System Overview **SMS PCS Online** SMS Master Status Screen SMS PCS Status Screen Snapshot Screen Trend Data Screen

SMS

OutputBus Currents

M	27	A
B	37	A
C	35	A

OutputBus Voltages

Vn	7830	V
Vb	7860	V
Vc	7877	V

1.25 MVA
480V / 13.2 kV

PCS #1
One-Line
Status

SMS Status

Real Power	0	kWatts
Reactive	54	kVAr
System Enabled / Disabled	ENABLED	
Master / System Status	READY	

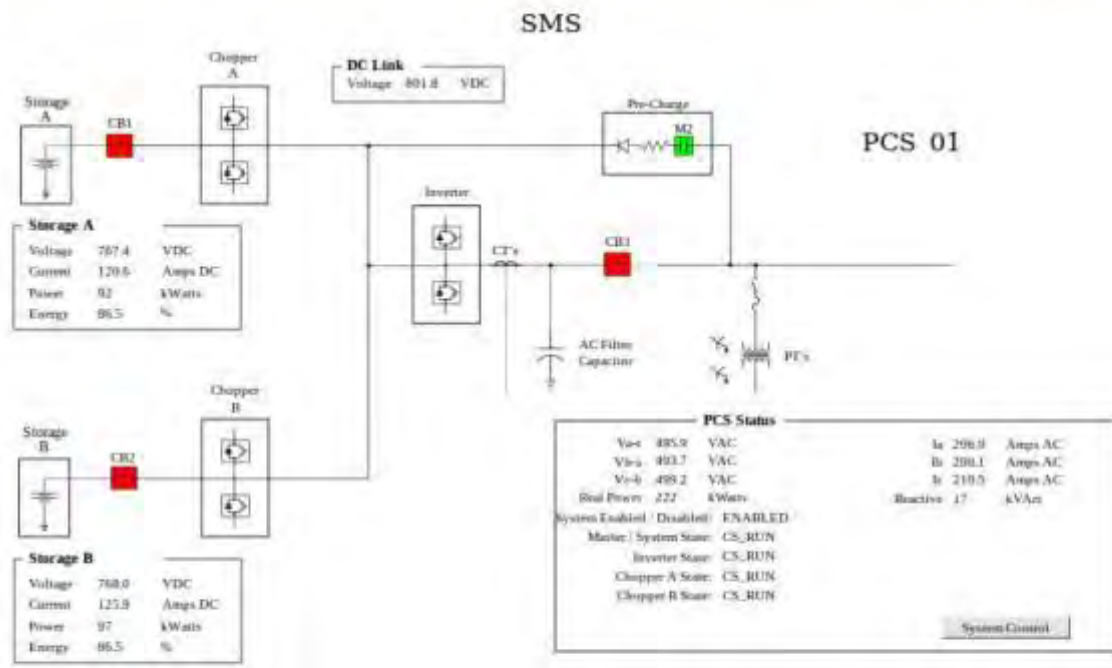
System Control

Dist Region: In 1, Time Stamp: 3/14/2013 4:47 PM

24 This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

SMS PCS Oneline: Battery is Discharging

SMS System Oneline | **SMS PCS Oneline** | SMS Master Status Screen | SMS PCS Status Screen | Snapshot Screen
 Trend Data Screen



25

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



DERM: Event Complete

Overview Base Data Customers Operations Grid Management Post Operations Interface Management User Administration Debug Window

Dashboard Resource Summary Schedule Event Summary Push Web Service Log Web Service Inbound Log Thu 12/19 10:13 AM CPT

Schedule Event Summary Date: ALL Interval: 1 Hour Interval

Schedule Event	Program	Date	Status	Strategy	Firm	Notification Date	Start		End		Ramping		Relax		
							Hour	Min	Hour	Min	Begin	End	Time	Ramping	Notificat
Battery - test8(11/06/2013)	Battery	11/06/2013	Aborted	LCS	Yes	11/06/2013 14:57	15	00	15	12			No	No	No
Battery - test10(11/07/2013)	Battery	11/07/2013	Cancelled	LCS	Yes	11/06/2013 15:18	04	00	04	30			No	No	No
Battery - test11(11/06/2013)	Battery	11/06/2013	Cancelled	LCS	Yes	11/06/2013 16:05	17	00	17	12			No	No	No
Battery - test13(11/06/2013)	Battery	11/06/2013	Completed	LCS	Yes	11/06/2013 16:11	17	00	17	08			No	No	No
ChargePoint_Resource - test1(11/13/2013)	ChargePoint	11/13/2013	Completed	CYCLING	Yes	11/13/2013 08:58	09	00	09	15			No	No	No
801_tstat_resource - test_1(11/21/2013)	801 thermostats	11/21/2013	Cancelled	PCT	Yes	11/21/2013 17:17	17	27	17	35			No	No	No
801_tstat_resource - test2(11/21/2013)	801 thermostats	11/21/2013	Completed	PCT	Yes	11/21/2013 17:19	17	29	17	35			No	No	No
801_LCS_resource - test_1(11/25/2013)	801 load control devices	11/25/2013	Completed	LCS	Yes	11/25/2013 11:15	11	20	11	25			No	No	No
801_tstat_resource - test2(11/25/2013)	801 thermostats	11/25/2013	Completed	PCT	Yes	11/25/2013 11:46	11	56	12	00			No	No	No
ChargePoint_Resource (12/02/2013)	ChargePoint	12/02/2013	Completed	CYCLING	Yes	12/02/2013 10:08	10	05	10	10			No	No	No
ChargePoint_Resource - test2(12/02/2013)	ChargePoint	12/02/2013	Completed	CYCLING	Yes	12/02/2013 10:28	10	30	10	40			No	No	No
ChargePoint_Resource (12/04/2013)	ChargePoint	12/04/2013	Cancelled	CYCLING	Yes	12/04/2013 04:38	04	10	04	12			No	No	No
ChargePoint_Resource (12/03/2013)	ChargePoint	12/03/2013	Aborted	CYCLING	Yes	12/03/2013 16:11	16	13	16	17			No	No	No
ChargePoint_Resource (12/03/2013)_2	ChargePoint	12/03/2013	Completed	CYCLING	Yes	12/03/2013 17:53	17	55	17	59			No	No	No
ChargePoint_Resource (12/04/2013)_1	ChargePoint	12/04/2013	Completed	CYCLING	Yes	12/04/2013 12:19	12	21	12	22			No	No	No
ChargePoint_Resource (12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 08:03	08	05	08	10			No	No	No
ChargePoint_Resource - test2(12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 08:25	08	27	08	33			No	No	No
ChargePoint_Resource - test5(12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 04:13	04	15	04	25			No	No	No
ChargePoint_Resource - test_7(12/06/2013)	ChargePoint	12/06/2013	Aborted	CYCLING	Yes	12/06/2013 16:15	16	17	16	24			No	No	No
801_LCS_resource - test_1(12/06/2013)	801 load control devices	12/06/2013	Completed	LCS	Yes	12/06/2013 16:16	16	21	16	25			No	No	No
ChargePoint_Resource - test_10(12/06/2013)	ChargePoint	12/06/2013	Aborted	CYCLING	Yes	12/06/2013 16:26	16	28	16	28			No	No	No
801_LCS_resource - test2(12/06/2013)	801 load control devices	12/06/2013	Cancelled	LCS	Yes	12/06/2013 16:32	16	37	16	42			No	No	No
ChargePoint_Resource-test13(12/06/2013)	ChargePoint	12/06/2013	Completed	CYCLING	Yes	12/06/2013 17:38	17	40	17	55			No	No	No
Battery (12/11/2013)	Battery	12/11/2013	Cancelled	LCS	Yes	12/11/2013 09:55	10	00	10	59			No	No	No
ChargePoint_Resource (12/09/2013)	ChargePoint	12/09/2013	Completed	CYCLING	Yes	12/09/2013 15:15	15	17	15	20			No	No	No
Battery (12/10/2013)	Battery	12/10/2013	Aborted	LCS	Yes	12/10/2013 11:05	11	10	11	20			No	No	No
Battery (12/19/2013)	Battery	12/19/2013	Cancelled	LCS	Yes	12/19/2013 09:10	10	00	10	10			No	No	No
Battery - test1 (12/19/2013)	Battery	12/19/2013	Completed	LCS	Yes	12/19/2013 09:20	10	00	10	10			No	No	No

12/19/2013 10:12:58 Records 1-211 of 211

Modify Reset Update Availability

26

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



OMS: Battery Finished Discharging

The screenshot displays a software interface for an OMS (Operational Monitoring System). A 'Feature Information' window is open on the left, showing a list of attributes and their values for device 1888105. The 'Event(s) Complete' attribute is highlighted with a red box. The background features a complex visualization of a power grid with various nodes, lines, and data points. Labels such as 'JC-B-406', 'OPEN', 'FUTURE', 'S1888394', 'S1888394', 'S1886337-200', 'S1892254', 'S1892253', 'T1888108', '077244', and '077243' are overlaid on the grid. The interface includes a menu bar at the top with options like 'Workstation', 'Crew', 'Job', 'Info', 'View', 'Inquiry', 'Tools', 'Database', 'InService', 'Report/Info', 'Admin/Config', 'View/Display', and 'Help'. A toolbar with various icons is located below the menu bar.

Name	Value
Active State	Ready
Active Status	Event(s) Complete
Alarm - Inhibit	OK
Alarm - Isolate	OK
Alarm - Trip Offline	OK
Alarm - Warning	OK
BESS Status	Enabled
Charge Mode	OFF
Energy Available (%)	92
Local - Remote	Remote
Power Mode	DERM
Reactive Mode	OFF
Recalculation Time (sec)	0
SCAM Device Comm Failure	OK
Schedule Override Status	Disabled
KVAR - Discharge Duration (min)	0
KVAR - Discharge Start Time (0-23)	0
KVAR - Fixed PF (%)	0
KVAR - Max Discharge Rate	0
KW - Charge Duration (min)	0
KW - Charge Following	0
KW - Charge Start Time (0-23)	0
KW - Discharge Duration (min)	10
KW - Discharge Start Time (0-23)	10
KW - Load Following	0
KW - Max Charge Rate	0
KW - Max Discharge Rate	800

27

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

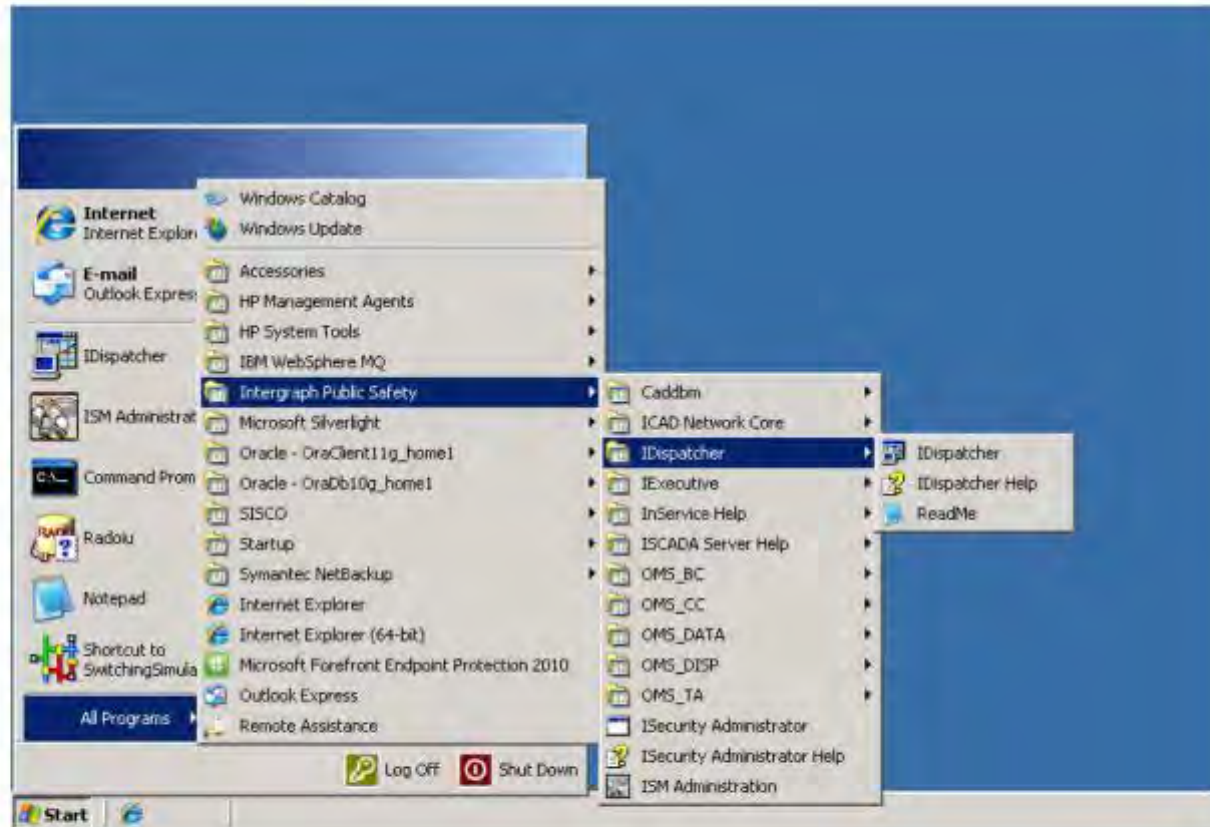


1st Responder Volt Var Control

- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program



Launch InService I/Dispatcher

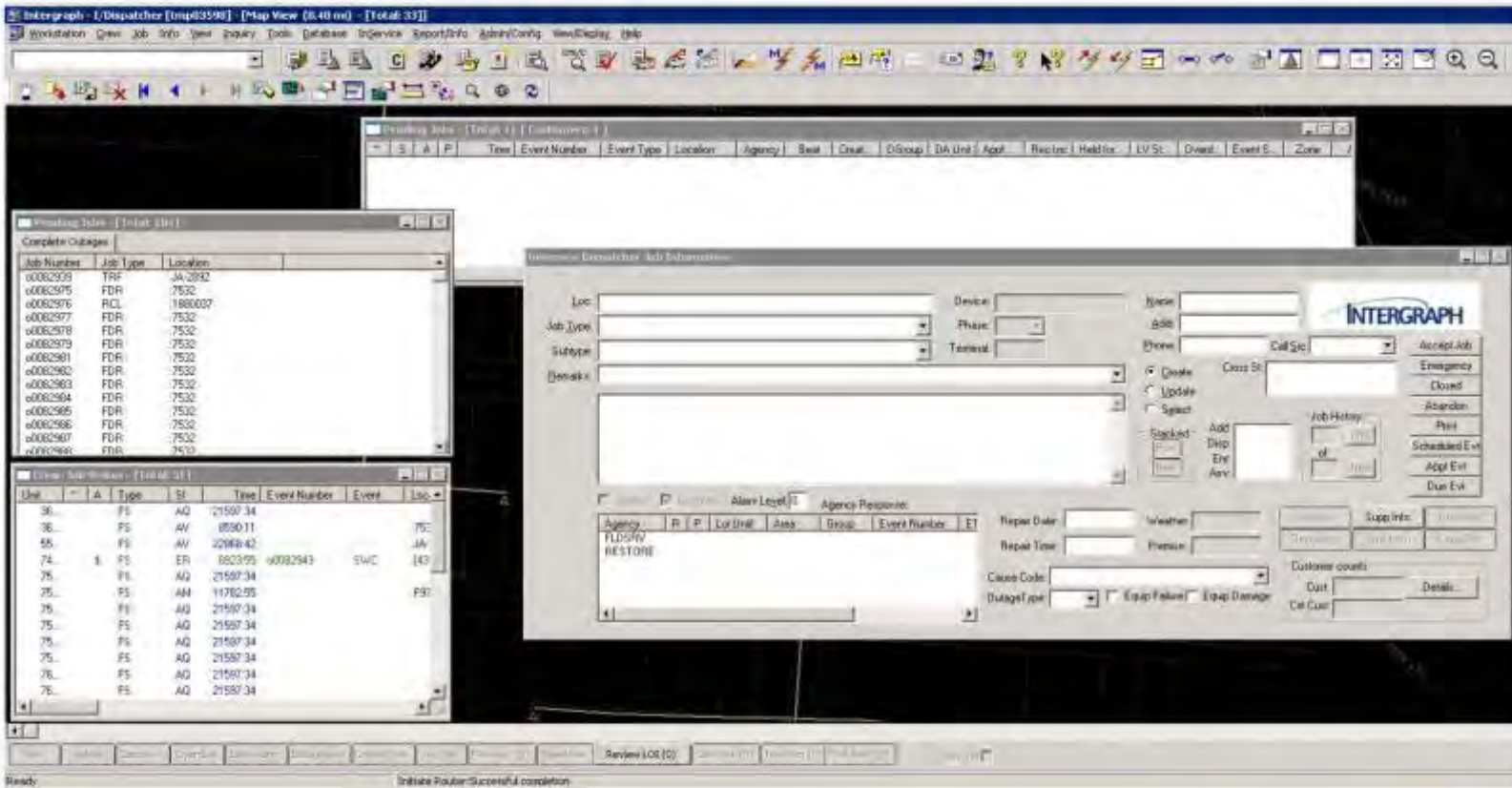


2

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



InService I/Dispatcher Main Screen

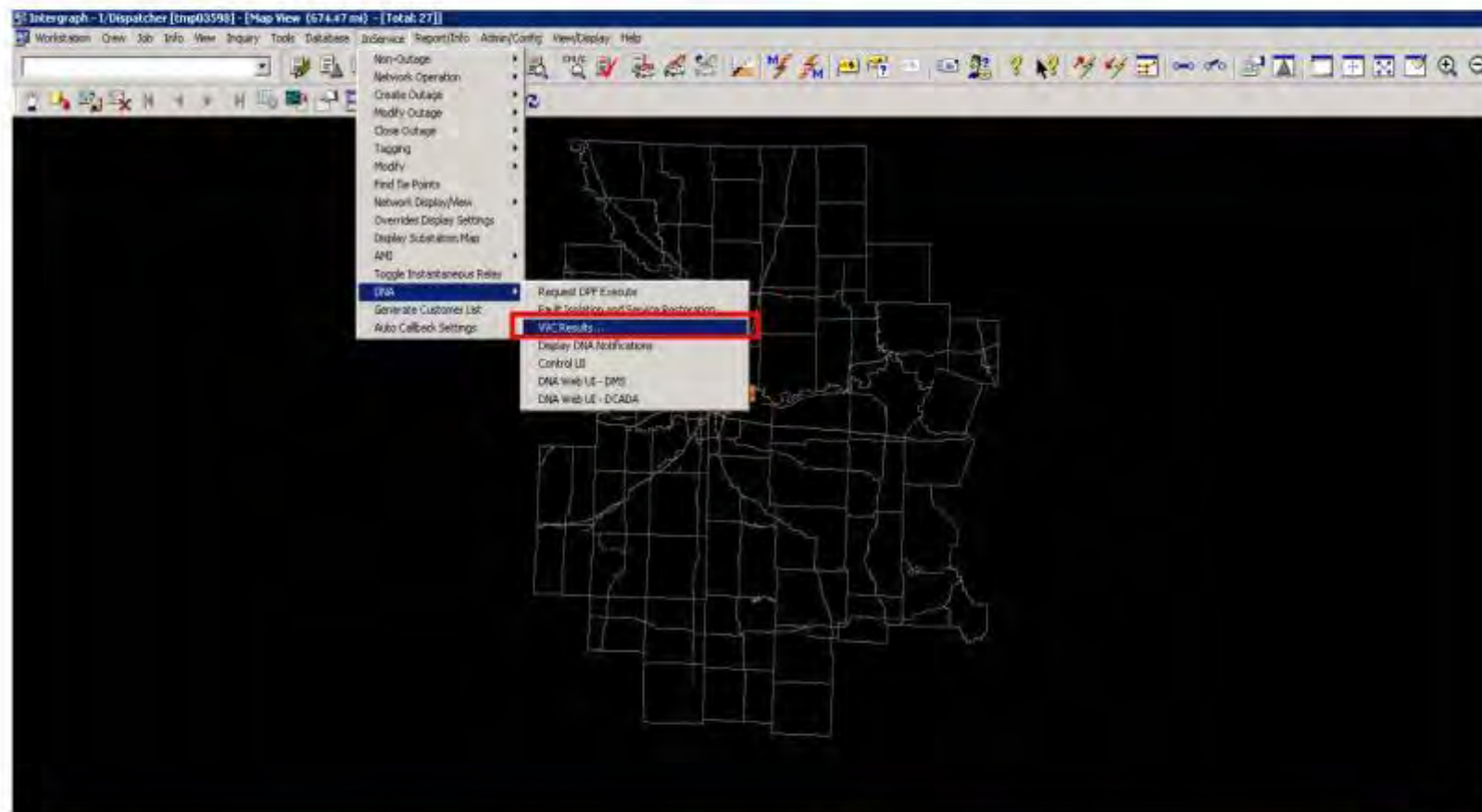


3

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Open the VVC Results Window

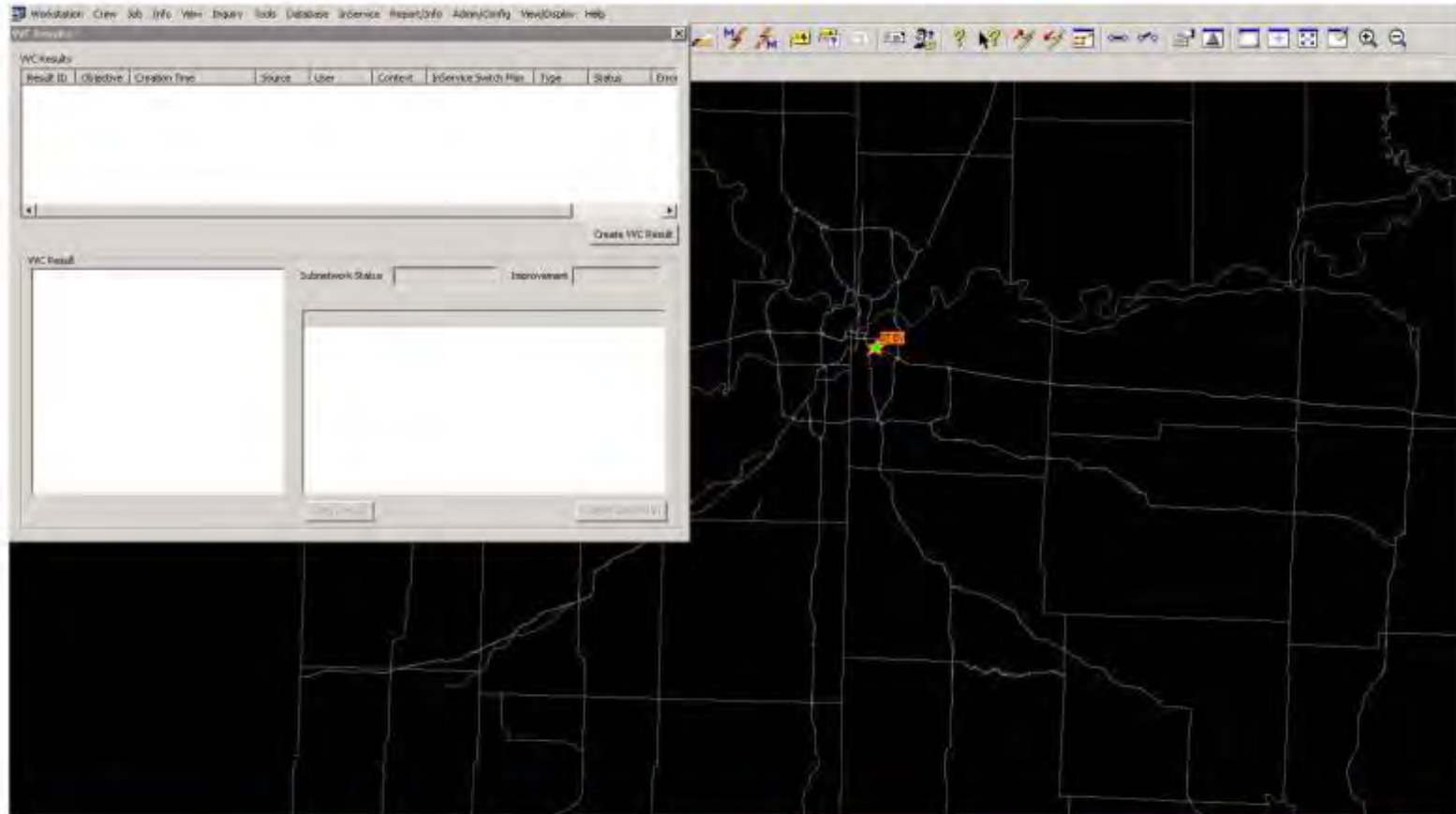


4

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



VVC Results Window

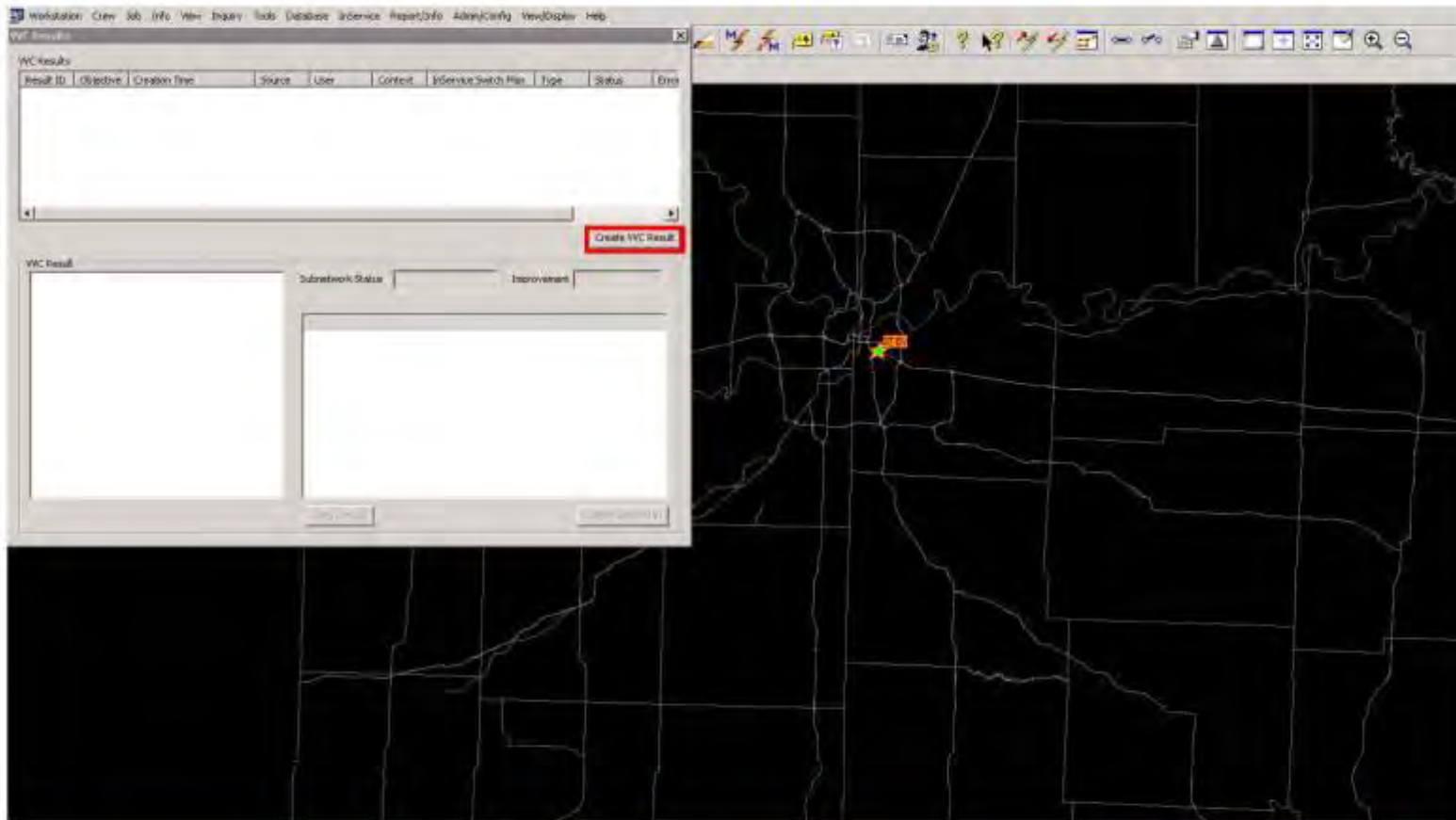


5

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



“Create VVC Results” to run VVC

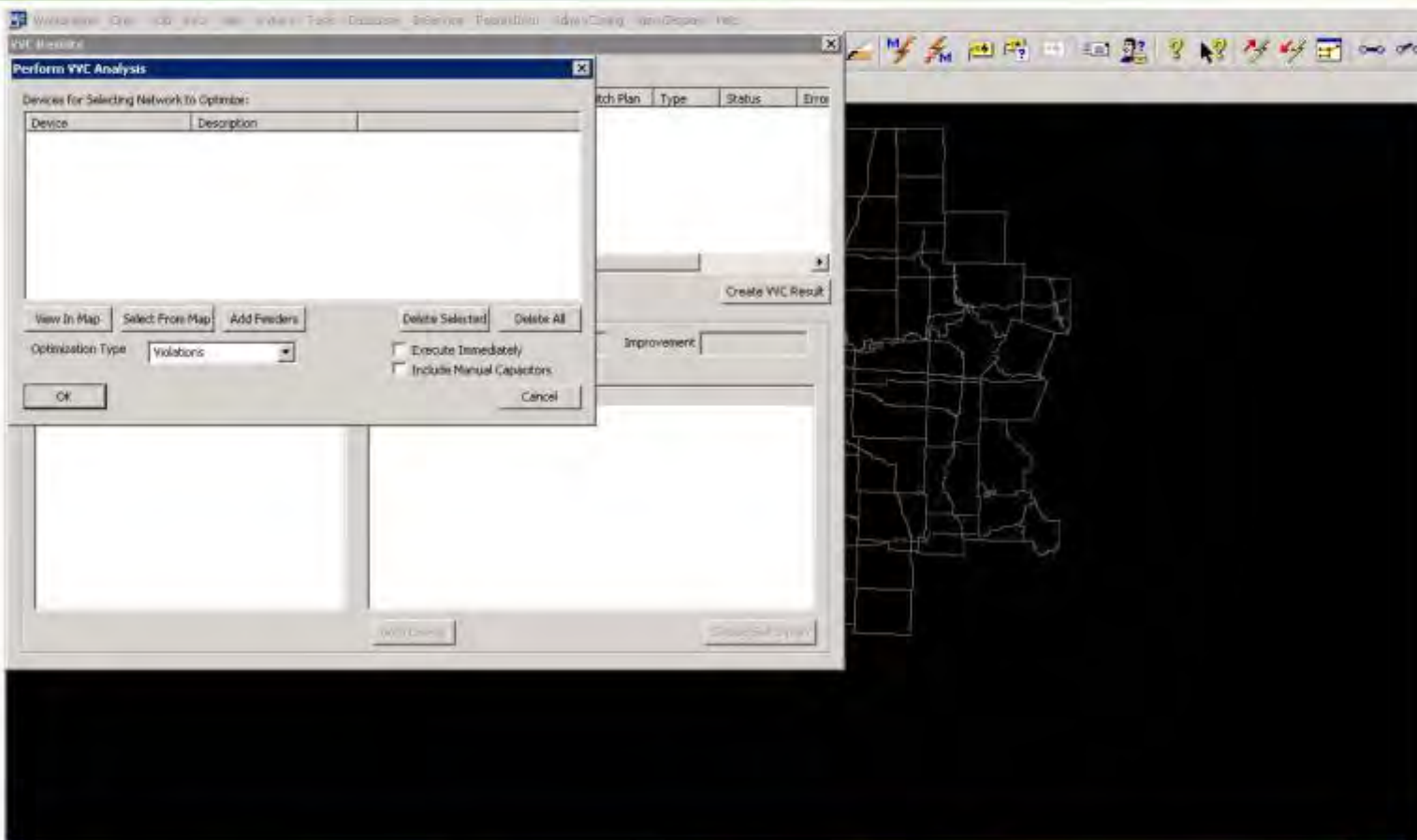


6

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



New Window Opened to Select Device

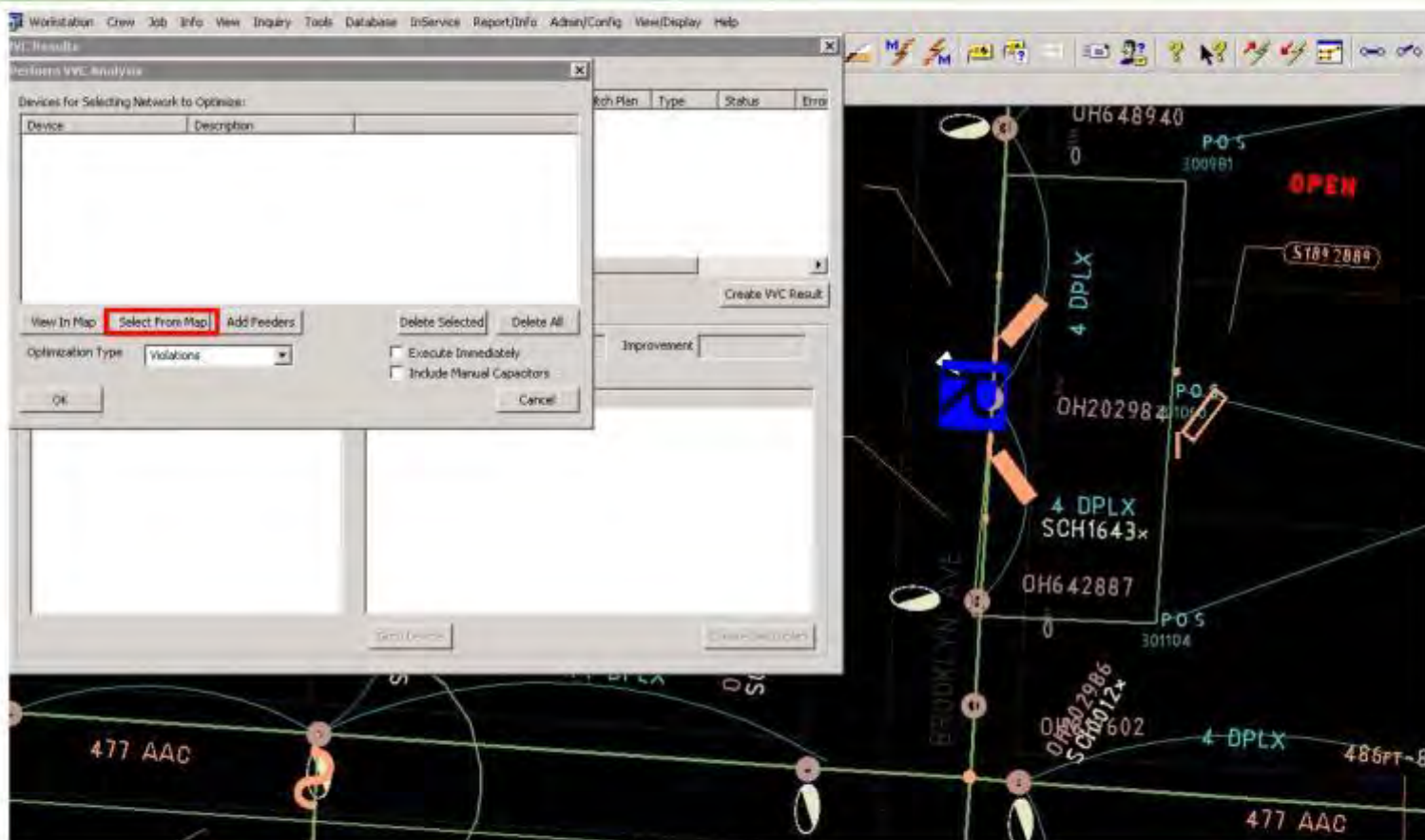


7

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



“Select from Map” to Select the Device from Map



8

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Device is Updated

The screenshot displays a software application window titled 'Workstation - Cree Job Info View Inquiry Tools Database InService Report/Info Admin/Config View/Display Help'. A 'Perform VVC Analysis' dialog box is open, showing a table of devices for selection:

Device	Description
1880047	Redcser

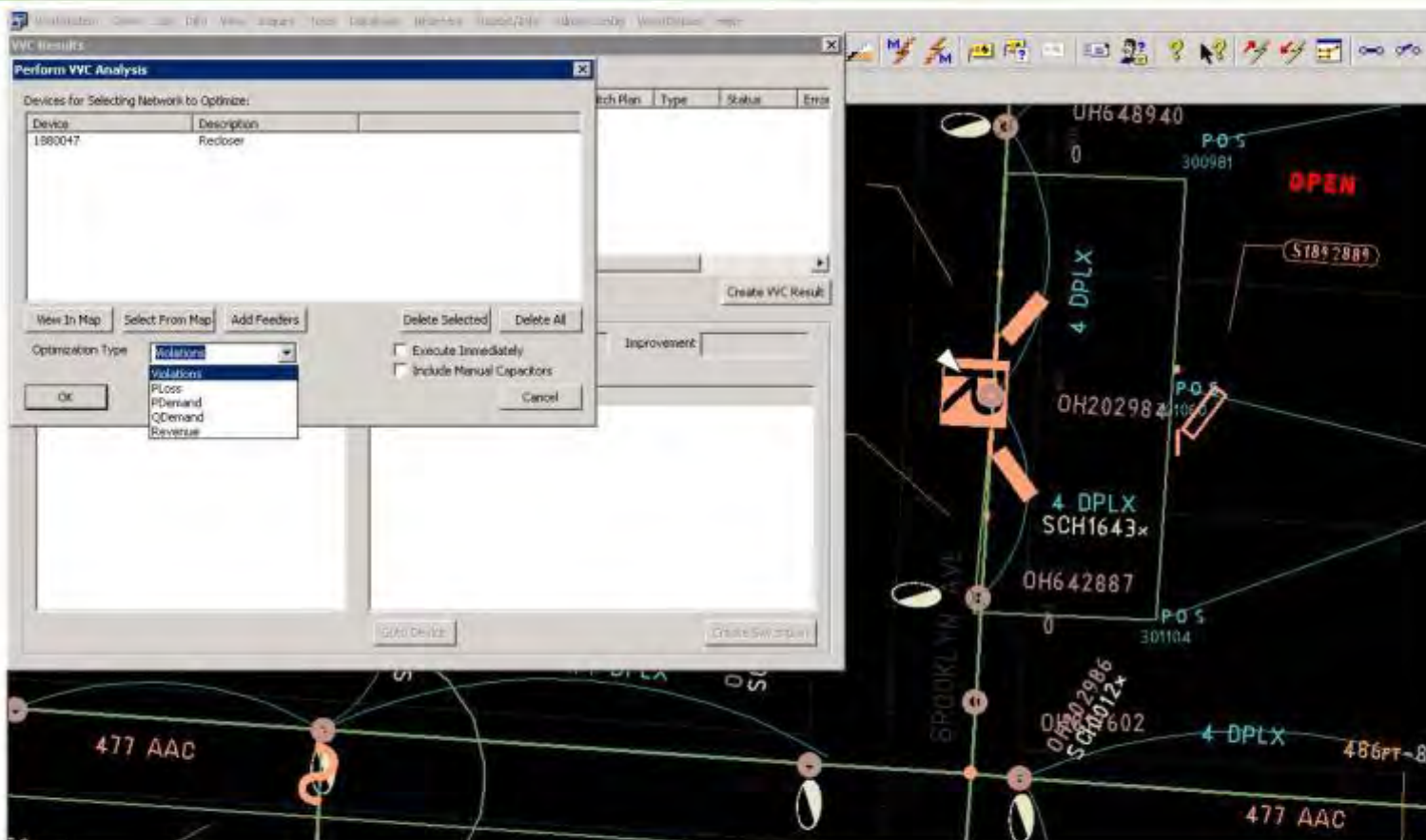
Below the table are buttons for 'View in Map', 'Select From Map', 'Add Feeders', 'Delete Selected', and 'Delete All'. The 'Optimization Type' is set to 'Voltage'. There are checkboxes for 'Execute Immediately' and 'Include Manual Capacitors'. The background map shows a network diagram with nodes and lines, including labels like '477 AAC', '4 DPLX', 'OH648940', 'OH20298', 'OH642887', 'OH602986', 'SCH0912x', 'SCH1643x', 'P-O-5', '300981', '301104', '486FT-8', and 'OPEN'.

9

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Select the Optimization Type to Run VVC

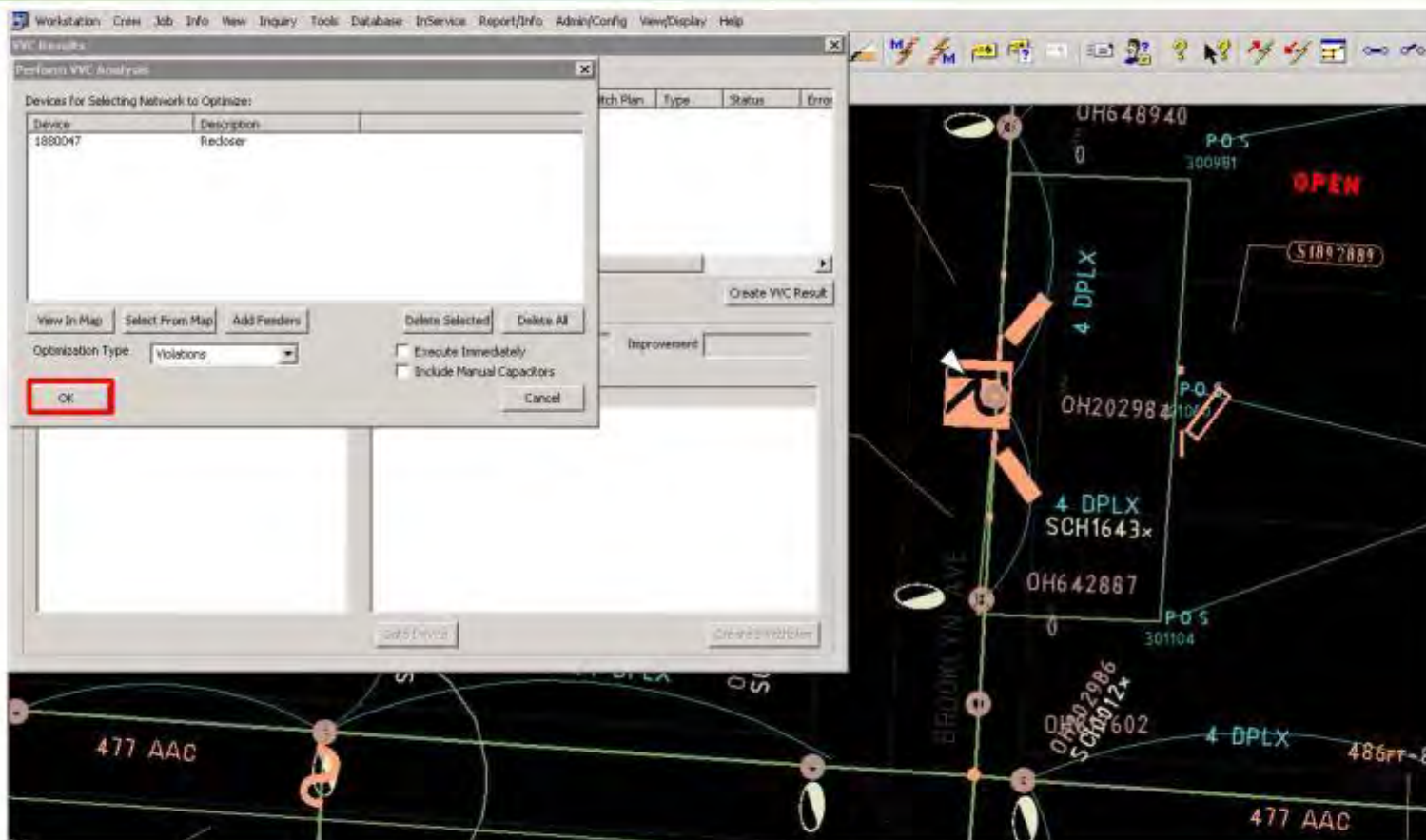


10

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Select "Ok" to execute VVC



11

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Executing VVC

Context	InService Switch Plan	Type	Status	Error
RT	Manual		Calculating	

12

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



VVC Results

The screenshot displays a software application window titled 'VVC Results'. It features a menu bar at the top with options like 'Workstation', 'Crew', 'Job', 'Info', 'View', 'Inquiry', 'Tools', 'Database', 'InService', 'Report/Info', 'Admin/Config', 'View/Display', and 'Help'. Below the menu is a toolbar with various icons.

The main content area is divided into several sections:

- VVC Results Table:** A table with columns: Result ID, Objective, Creation Time, Source, User, Contact, InService Switch Plan, Type, Status, and Error. The first row shows: 8043, Violations, 12/26/2013 10:46:14 AM, Depatc..., MATHEM..., RT, Manual, Calculated.
- VVC Result Summary:** A section with 'Subnetwork Status' (Closed, Subnetwork Power), 'Improvement' (+3), and a 'Steps' table.
- Steps Table:** A table with columns: #, Device, Description, State, and Phase. The first row is highlighted with a red border: 1, 989200, Capacitor, Close, ABC.
- Network Diagram:** A dark background diagram showing a network of nodes and lines. Nodes are labeled with IDs like 'UH648940', 'DH20298', 'DH642887', 'DH642986', and 'SCH0012'. Lines are labeled with '4 DPLX' and '477 AAC'. A red 'OPEN' label is visible on the right side.

13

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

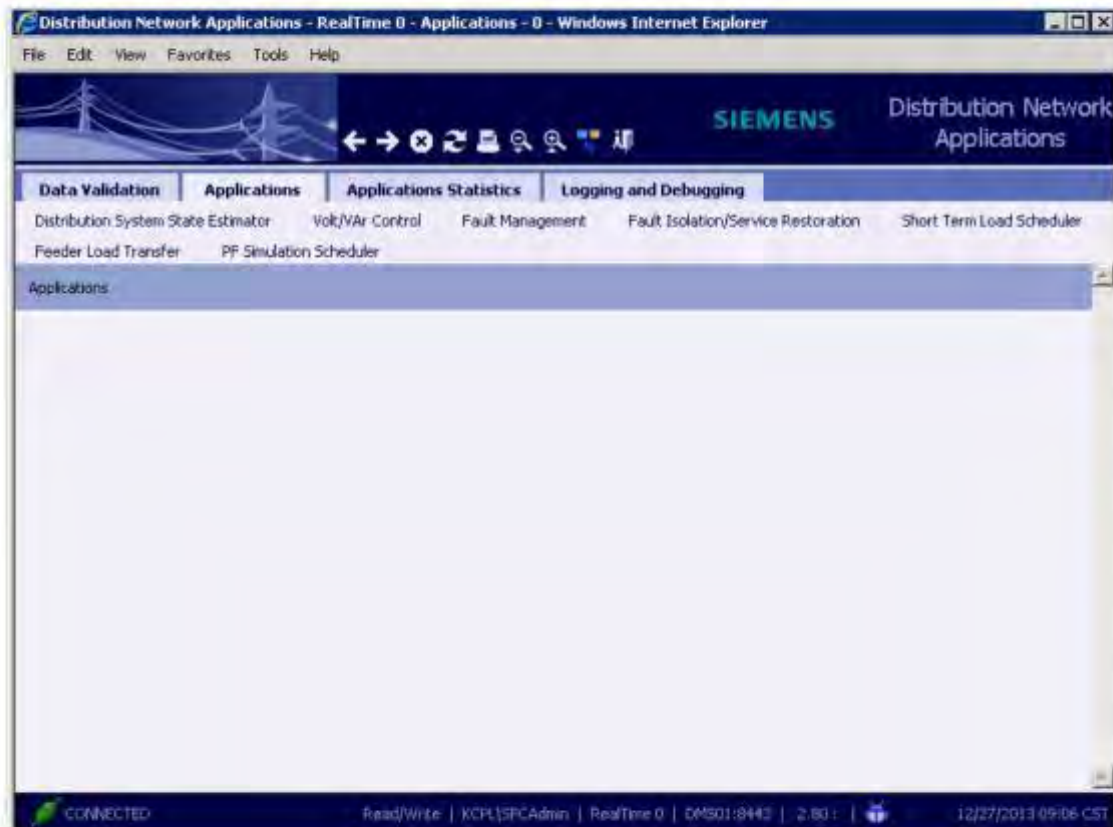


1st Responder Feeder Load Transfer

- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program



Launch DNA WebUI

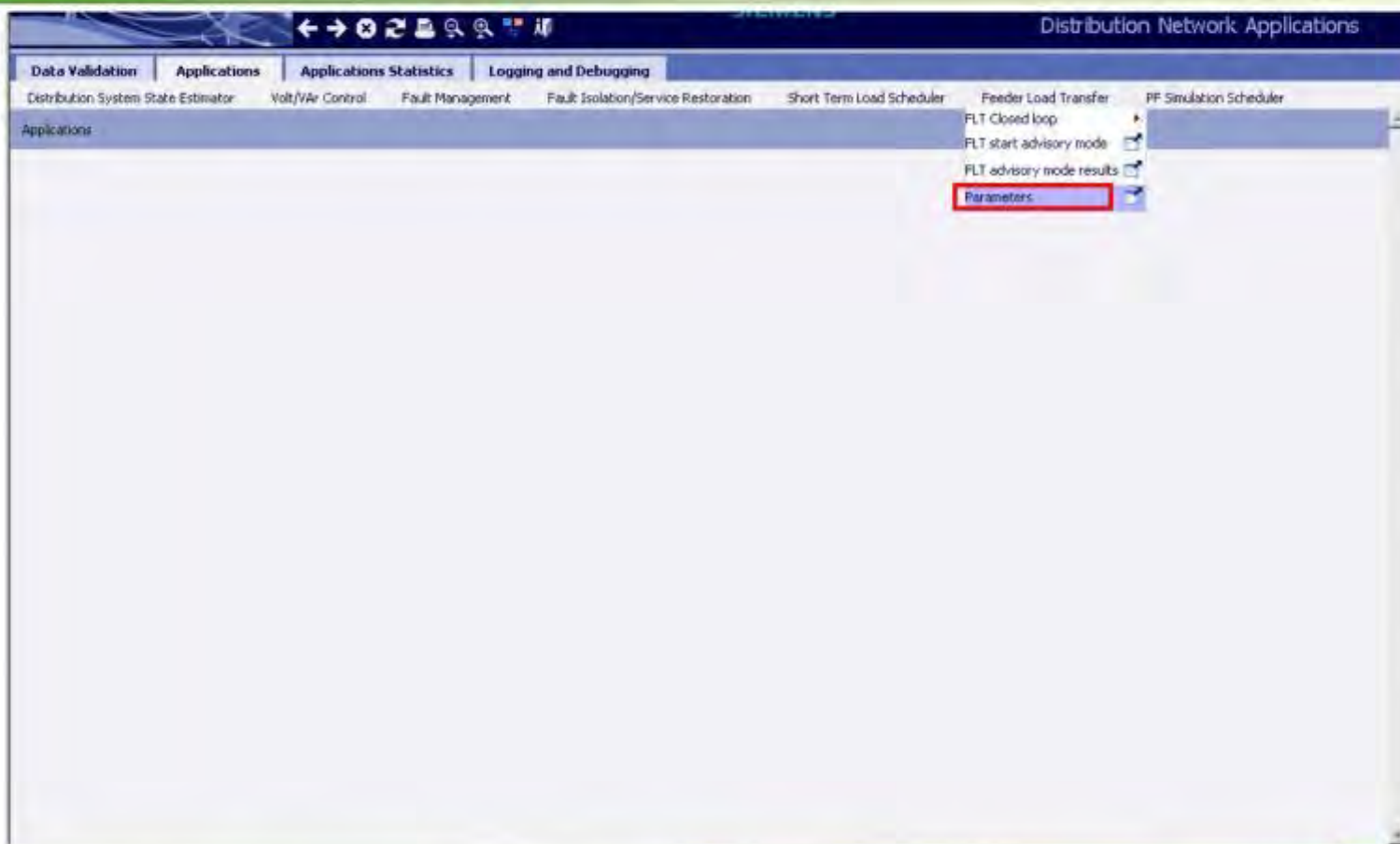


▪2

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Go to Parameters of Feeder Load Transfer



3

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



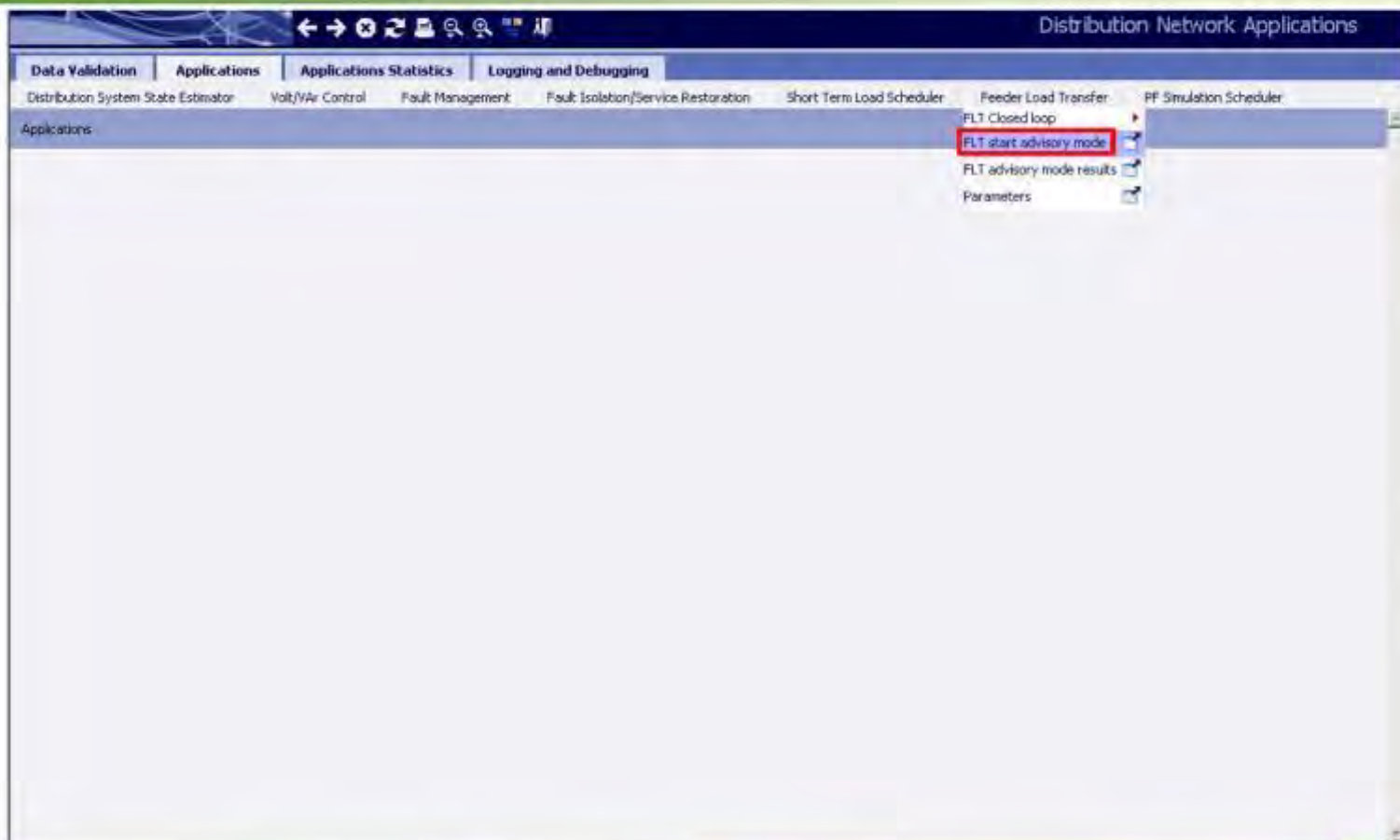
Update Feeder Load Transfer Parameters

■4

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



“FLT Start Advisory Mode”



5

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Select Subsystem/equipment

Distribution Network Applications

Data Validation Applications Applications Statistics Logging and Debugging

Distribution System State Estimator Volt/VAr Control Fault Management Fault Isolation/Service Restoration Short Term Load Scheduler Feeder Load Transfer PF Simulation Scheduler

Applications ▶ Feeder Load Transfer ▶ FLT start advisory mode

Select subsystem/equipment

No equipment selected

Used switches: All

Scope of execution: Selected subsystem only

Look ahead mode

Start time: []

End time: []

Security factor: 1

[] [Start] [Cancel]

6

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Select the system

Distribution Network: Applications - RealTime 0 - DMS Equipment Selection - Windows Internet Explorer

Path1 Path2 Path3 Path4 Path5 Path6 Path7 Path8

General
RDF Orphans
Accounting Areas
Control Area

Busbars Transformers Switches Lines Shunts Loads Generators Battery

Search Equipments Find Reset

Search Results

Instance Type	
---------------	--

Add Current View Add All

Selected Equipments

Remove All OK Cancel

7

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



System Selected

Path1 Control Area
Generation
ICCP
Net-E
PL

Path2 KCP, Conforming Load F
KCP, Line Spans
KCP, Regulation Sched.
TNE, Definitions
Net, Companies

Path3 KCP

Path4 KCP, ConnectivityNodes
MIDTOWN

Path5 13.2_KV
161_KV
1847431
1847432
1847437

Path6

Path7

Path8

Busbars Transformers Switches Lines Shunts Loads Generators Battery

Search Equipments: *161 Find Reset

Search Results

	Instance Type
/Net-E/Net Companies/KCP/MIDTOWN/161_KV/75-7-8-IND	BusbarSection
/Net-E/Net Companies/KCP/MIDTOWN/161_KV/75-5-6-IND	BusbarSection
/Net-E/Net Companies/KCP/MIDTOWN/161_KV/75-1-2-IND	BusbarSection
/Net-E/Net Companies/KCP/MIDTOWN/161_KV/75-3-4-IND	BusbarSection

↓ ↑ Add Current View Add All

Selected Equipments

- /Net-E/Net Companies/KCP/MIDTOWN/161_KV/75-7-8-IND
- /Net-E/Net Companies/KCP/MIDTOWN/161_KV/75-5-6-IND
- /Net-E/Net Companies/KCP/MIDTOWN/161_KV/75-1-2-IND
- /Net-E/Net Companies/KCP/MIDTOWN/161_KV/75-3-4-IND

Remove All OK Cancel

8

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Ready to Execute FLT

Distribution Network Applications

Data Validation | Applications | Applications Statistics | Logging and Debugging

Distribution System State Estimator | Volt/VAr Control | Fault Management | Fault Isolation/Service Restoration | Short Term Load Scheduler | **Feeder Load Transfer** | PF Simulation Scheduler

Applications #Feeder Load Transfer #FLT start advisory mode

Select subsystem/equipment

- /Net-E/Net_Companies/KCPL/MIDTOWN/1
- /Net-E/Net_Companies/KCPL/MIDTOWN/1
- /Net-E/Net_Companies/KCPL/MIDTOWN/1
- /Net-E/Net_Companies/KCPL/MIDTOWN/1

Used switches: All

Scope of execution: Selected subsystem only

Look ahead mode

Start time: []

End time: []

Security factor: 1

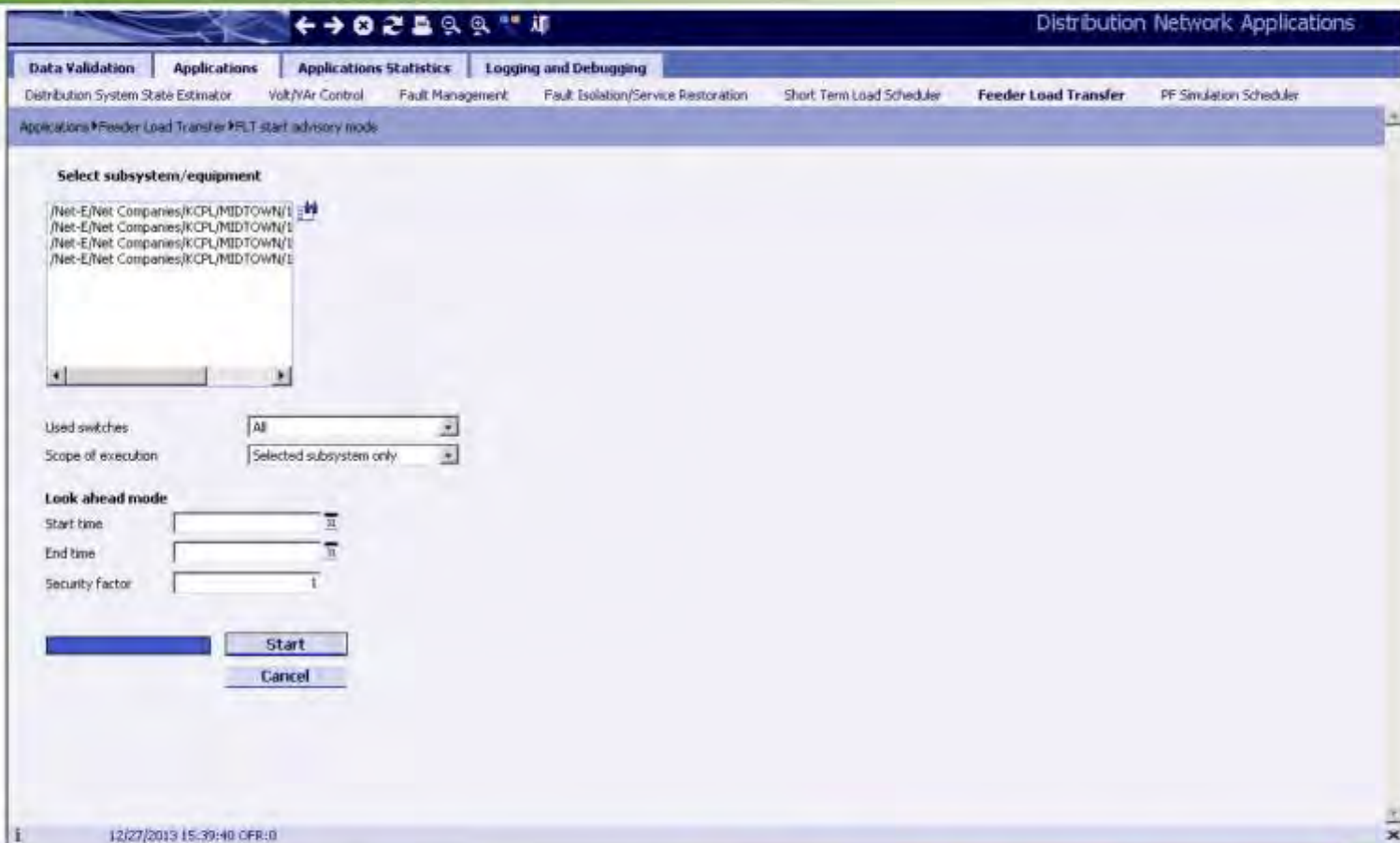
[] **Start** Cancel

9

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



FLT is Executing



10

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



FLT Results

Distribution System State Estimator Volt/VAr Control Fault Management Fault Isolation/Service Restoration Short Term Load Scheduler **Feeder Load Transfer** PF Simulation Scheduler

Applications: Feeder Load Transfer *FLT advisory mode results

Started by: [ALL] Session: [ALL] [Apply](#) [Reset](#)

Session summary

Session Number	Date/time	Subsystem	Used switches	Scope of execution	Look ahead mode		Status	Trigger	Started by	Improvement [%]	Switching order	Trust factor [%]
					Loading time							
1	12/20/2013 14:17:27	Net-E/Net Companies(KCP&L/MIDTOWN/161_XV/75-7-8-IND) All		Selected subsystem only			No Solution found	Manual	KCP\SPCAdmin	0.00	0	93.75

Output **Violations** Initially opened switches Affected injection sources Parameters Information

Objective summary

	Initial	Final
Total objective	100.00	100.00
Overload [A]	51.74	51.74

Switching proposal

Order	Step	Switch name	Action	Type	Phase	Overload [A]	Effect [%]	Temporary
No Data found								

[Create Switching Order](#)

[Call Display](#) [Highlight](#) [Highlighting Off](#)

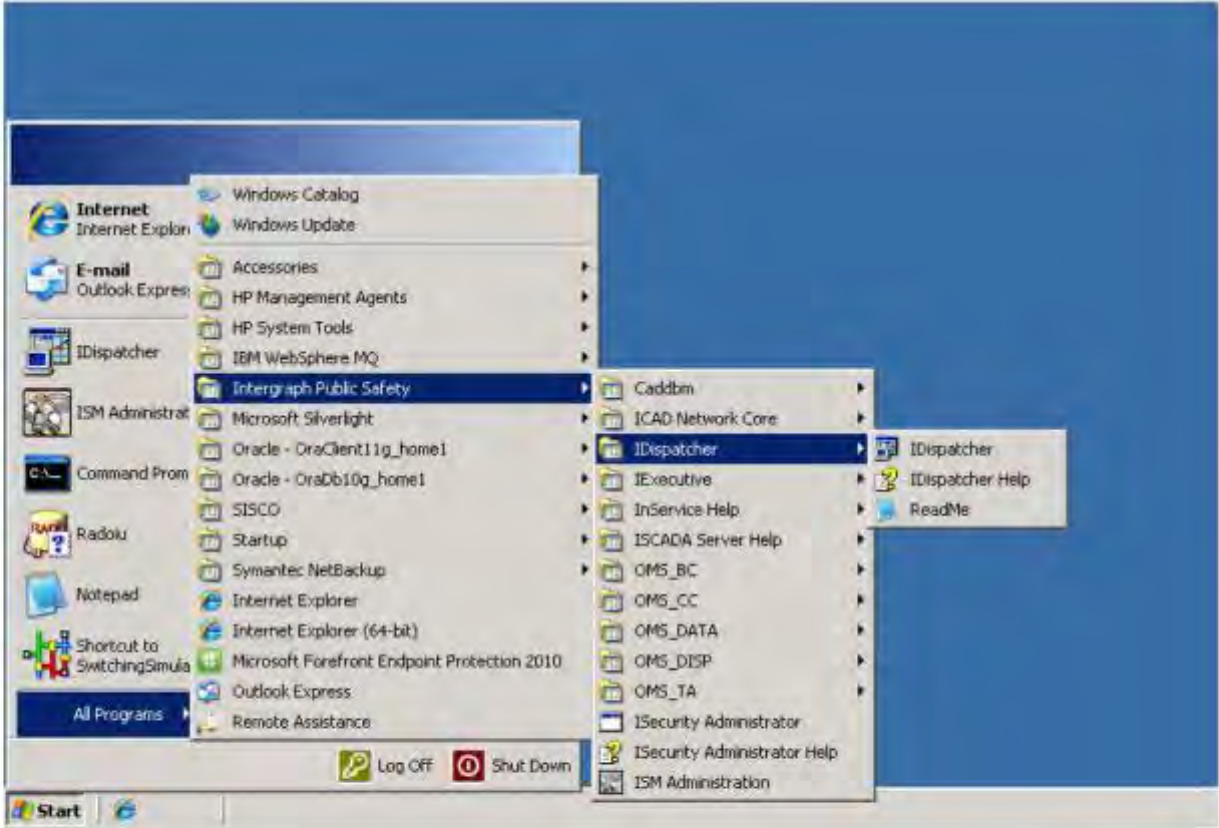
■ 11
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

1st Responder Fault Isolation and Service Restoration

- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program



Launch InService I/Dispatcher

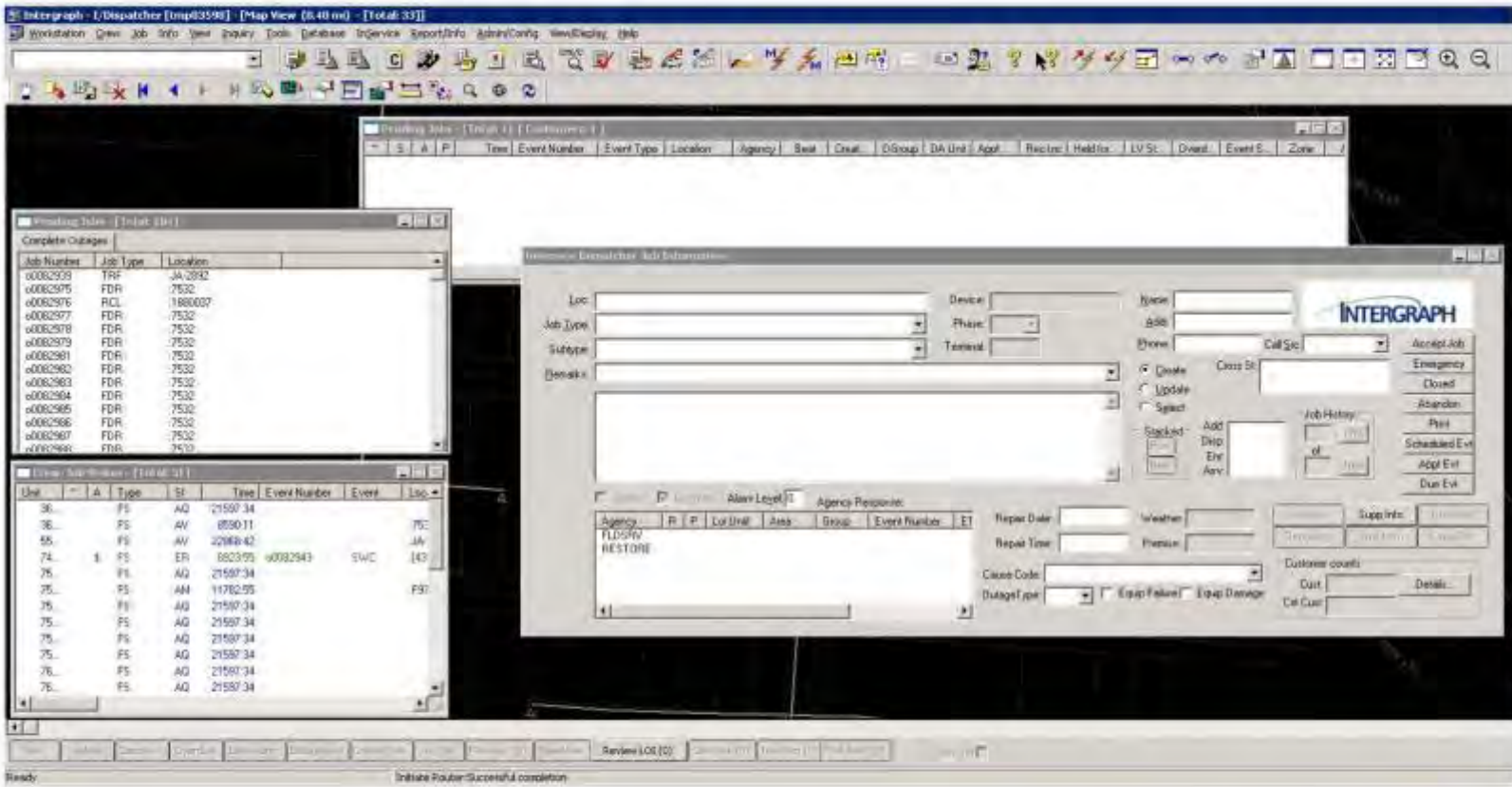


2

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



InService I/Dispatcher Main Screen

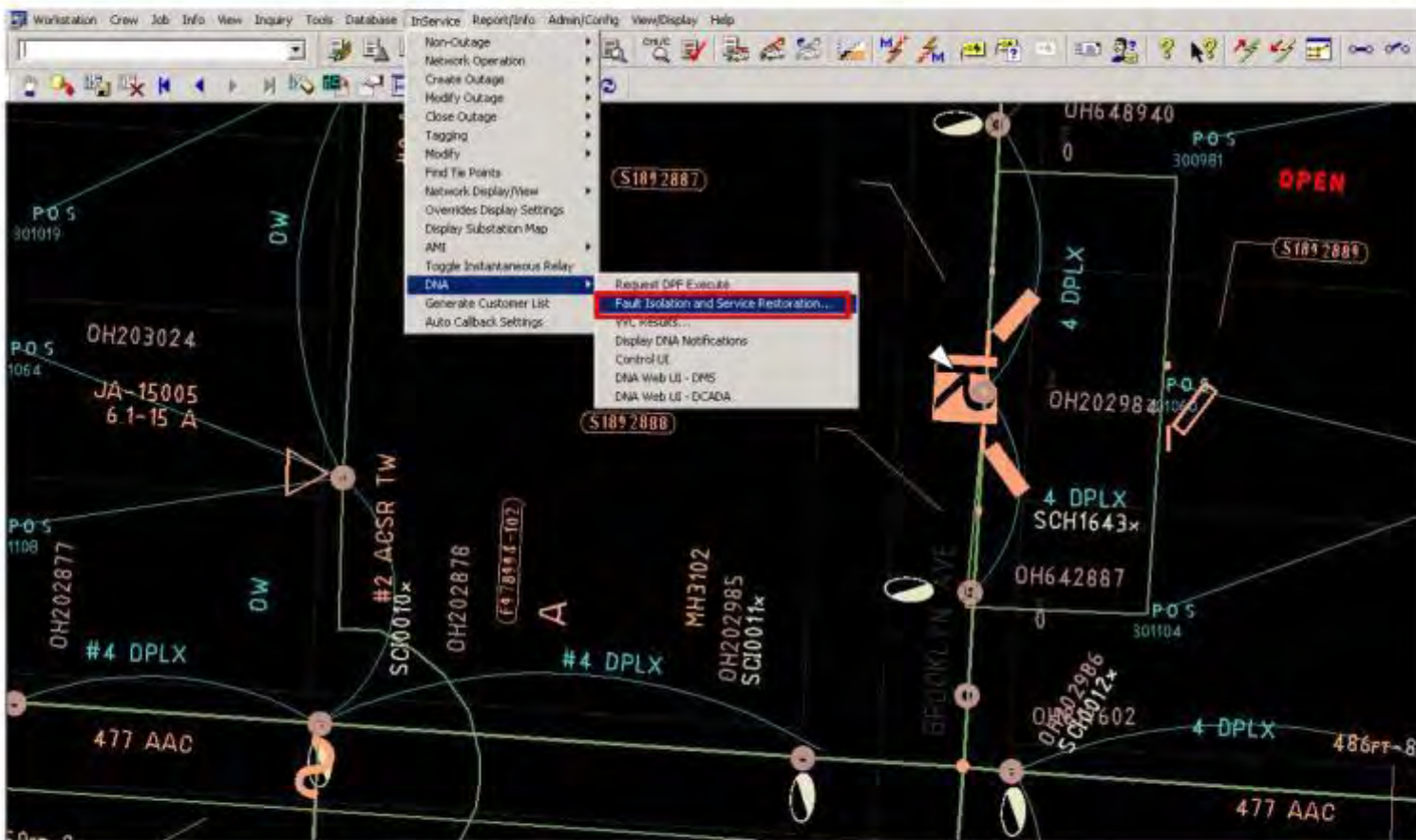


3

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Open the Fault Isolation and Service Restoration Window



4

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



FISR Window: Fault Isolation

Fault Isolation Requests:

Request ID	Outage Event	Request Sent	Reply Received	In-Service Switch Plan	Status	Error Message
1		8/30/2013 3:08:01 PM	8/30/2013 3:08:02 PM		Completed	
2		8/30/2013 3:24:50 PM	8/30/2013 3:24:50 PM		Completed	
4		8/30/2013 7:46:40 AM	8/30/2013 7:46:41 AM		Completed	
6		8/30/2013 7:53:41 AM	8/30/2013 7:53:42 AM		Completed	
7		8/30/2013 7:57:09 AM	8/30/2013 7:57:10 AM		Completed	
13		8/29/2013 12:04:18 PM	8/29/2013 12:04:19 PM		Completed	
14		8/30/2013 8:22:37 AM	8/30/2013 8:22:38 AM		Completed	
15		8/30/2013 8:31:45 AM	8/30/2013 8:31:46 AM		Completed	
16		8/30/2013 8:36:15 AM	8/30/2013 8:36:17 AM		Completed	
17		8/30/2013 8:43:44 AM	8/30/2013 8:43:45 AM		Completed	

Equipment To Isolate:

Device	Description	Phases To Isolate
1890019	Switch	ABC

Response Details:

Load Restores: 0 Meter Restores: 0 Customer Restores: 0 Power Loss: 0 Voltage Violations: 0
 Load Not Restores: 0 Meter Not Restores: 0 Customer Not Restores: 0 Line Overloads: 0 Meter Overloads: 0

Fault Isolation Switch Plan Steps:

#	Device	Description	State	Step Type	Phase
0	7251	Breaker	Open	SWITCH	ABC
1	1890017	Switch	Open	SWITCH	ABC
2	1890249	Monitoring Point	Open	SWITCH	ABC
3	1890247	Monitoring Point	Open	SWITCH	ABC
4	1890248	Monitoring Point	Open	SWITCH	ABC
5	1890018	Switch	Open	SWITCH	ABC
6	7451	Breaker	Open	SWITCH	ABC

■5

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



“Create Request” for Fault Isolation

Fault Isolation and Service Restoration

Fault Isolation (FI) | Service Restoration (SR) | Fault Isolation and Immediate Restoration (FIIR) | Restore to Normal (RN)

Fault Isolation Requests:

Request ID	Outage Event	Request Sent	Reply Received	In Service Switch Plan	Status	Error Message
1		8/30/2013 3:09:01 PM	8/30/2013 3:26:02 PM		Completed	
2		8/30/2013 3:24:50 PM	8/30/2013 3:24:50 PM		Completed	
4		8/30/2013 7:46:40 AM	8/30/2013 7:46:41 AM		Completed	
6		8/30/2013 7:53:41 AM	8/30/2013 7:53:42 AM		Completed	
7		8/30/2013 7:57:09 AM	8/30/2013 7:57:10 AM		Completed	
13		8/29/2013 12:04:18 PM	8/29/2013 12:04:19 PM		Completed	
14		8/30/2013 8:22:37 AM	8/30/2013 8:22:38 AM		Completed	
15		8/30/2013 8:31:45 AM	8/30/2013 8:31:46 AM		Completed	
16		8/30/2013 8:36:15 AM	8/30/2013 8:36:17 AM		Completed	
17		8/30/2013 8:47:54 AM	8/30/2013 8:47:55 AM		Completed	

Request Details:

Outage Event: View In Map

Equipment To Isolate:

Device	Description	Phases To Isolate
1890019	Switch	ABC

Response Details:

Load Restores: 0 | Other Restores: 0 | Customer Restores: 0 | Power Loss: 0 | Voltage Violations: 0
 Load Not Restores: 0 | Wire Not Restores: 0 | Customer Not Restores: 0 | Line Overloads: 0 | Other Overloads: 0
 Difficulty: 0

Fault Isolation Switch Plan Steps:

#	Device	Description	State	Step Type	Phase
0	7251	Breaker	Open	SWITCH	ABC
1	1890017	Switch	Open	SWITCH	ABC
2	1890249	Monitoring Point	Open	SWITCH	ABC
3	1890247	Monitoring Point	Open	SWITCH	ABC
4	1890248	Monitoring Point	Open	SWITCH	ABC
5	1890018	Switch	Open	SWITCH	ABC

Switch Plan ID:

6

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Request Created

Fault Isolation and Service Restoration

Fault Isolation (FI)
 Service Restoration (SR)
 Fault Isolation and Service Restoration (FISR)
 Restore to Normal (RM)

Fault Isolation Requests: Filter List...

Request ID	Outage Event	Request Sent	Reply Received	Service Switch Plan	Status	Error Message
7155		12/11/2013 10:18:23 AM	12/11/2013 10:24:29 AM		Completed	
7949		12/11/2013 6:35:03 PM	12/11/2013 6:20:04 PM		No Solution	No suggested switching ...
7950		12/11/2013 6:36:25 PM	12/11/2013 6:36:26 PM		Completed	
7951		12/11/2013 6:37:00 PM	12/11/2013 6:37:00 PM		No Solution	No suggested switching ...
7952		12/11/2013 6:38:24 PM	12/11/2013 6:38:25 PM		No Solution	No suggested switching ...
7962		12/11/2013 7:14:05 PM				
8000		12/11/2013 9:56:23 AM	12/11/2013 9:56:24 AM		Completed	
8007	00002705					
8007						

Request Details:

Outage Event:

Switch Type: All Remote Control Only

Equipment to Isolate:

Device	Description	Phases To Isolate

Response Details:

Load Restored: Wire Restored: Customer Restored: Power Loss: Voltage Violation:
 Load Not Restored: Wire Not Restored: Customer Not Restored: Line Overload: Wire Overload:

Fault Isolation Switch Plan Steps:

#	Device	Description	Status	Step Type	Phase	Priority

Switch Plan ID:

7

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



“Select from Map” to select Device to Isolate

Fault Isolation and Service Restoration

Fault Isolation Requests: 7888 List...

Request ID	Outage Event	Request Sent	Reply Received	InService Switch Plan	Status	Error Message
7155		12/11/2013 10:18:23 AM	12/11/2013 10:18:23 AM		Completed	
7949		12/11/2013 6:35:03 PM	12/11/2013 6:25:04 PM		No Solution	No suggested switching ...
7950		12/11/2013 6:36:25 PM	12/11/2013 6:36:25 PM		Completed	
7951		12/11/2013 6:37:00 PM	12/11/2013 6:37:00 PM		No Solution	No suggested switching ...
7952		12/11/2013 6:38:24 PM	12/11/2013 6:38:25 PM		No Solution	No suggested switching ...
7962		12/11/2013 7:14:05 PM				
8000		12/11/2013 9:56:23 AM	12/11/2013 9:56:24 AM		Completed	
8007	00002705					
8007						

Request Details:

Outage Event:

Switch Type: All Remote Control Only

Equipment To Isolate:

Device	Description	Phases To Isolate

Response Details:

Load Restored: Wire Restored: Customer Restored: Power Loss: Voltage Violation:
 Load Not Restored: Wire Not Restored: Customer Not Restored: Line Overloads: Wire Overloads:

Fault Isolation Switch Plan Steps:

#	Device	Description	Status	Step Type	Phase	Priority

Switch Plan ID:

8

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Select the Device from Map

Fault Isolation and Service Restoration

Fault Isolation (FI) |
 Service Restoration (SR) |
 Fault Isolation and Immediate Restoration (FIR) |
 Restore to Normal (RN)

Fault Isolation Requests:

Request ID	Outage Event	Request Sent	Reply Received	Service Switch Plan	Status	Error Message
7155		12/11/2013 10:18:28 AM	12/11/2013 10:18:29 AM		Completed	
7949		12/11/2013 6:35:03 PM	12/11/2013 6:35:04 PM		No Solution	No suggested switching ...
7950		12/11/2013 6:36:25 PM	12/11/2013 6:36:26 PM		Completed	
7951		12/11/2013 6:37:00 PM	12/11/2013 6:37:01 PM		No Solution	No suggested switching ...
7952		12/11/2013 6:38:24 PM	12/11/2013 6:38:25 PM		No Solution	No suggested switching ...
7962		12/11/2013 7:14:25 PM				
8008		12/11/2013 9:56:33 AM	12/11/2013 9:56:34 AM		Completed	
8009	00003705					
8007						

Request Details:

Outage Event:

Switch Type: All Remote Control Only

Equipment To Isolate:

Device	Description	Phase To Isolate

Response Details:

Load Restores: Other Restores: Customer Restores: Power Out: Voltage Violations:
 Load Not Restores: Other Not Restores: Customer Not Restores: Line Overloads: Other Overloads:
 Fault Isolation Switch Plan Steps: Difficulty:

Fault Isolation Switch Plan Steps:

#	Device	Description	Status	Step Type	Phase

Switch Plan ID:

9

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Device is Updated

Fault Isolation and Service Restoration

Traffic Station (TTL) | Service Restorator (SR) | Fault Isolation and Immediate Restoration (FIR) | Restore to Normal (RN)

Fault Isolation Requests:

Request ID	Outage Event	Request Sent	Reply Received	Service Switch Plan	Status	Error Message
7155		10/11/2013 10:18:28 AM	10/11/2013 10:18:29 AM		Completed	
7949		12/11/2013 6:28:03 PM	12/11/2013 6:28:04 PM		No Solution	No suggested switching ...
7950		12/11/2013 6:36:25 PM	12/11/2013 6:36:26 PM		Completed	
7951		12/11/2013 6:37:00 PM	12/11/2013 6:37:01 PM		No Solution	No suggested switching ...
7952		12/11/2013 6:38:24 PM	12/11/2013 6:38:25 PM		No Solution	No suggested switching ...
7962		12/11/2013 7:14:25 PM				
8008					Completed	
8009	00001702	12/13/2013 9:56:33 AM	12/13/2013 9:56:34 AM		Completed	
8037						

Request Details:

Outage Event: View In Map Select From Map Clear Event

Switch Type: All Remote Control Only

Equipment To Isolate:

Device	Description	Phase To Isolate
16763073	Primary Conductor - LU Conductor	ABC

Response Details:

Load Restores: Other Restores: Customer Restores: Power Out: Voltage Violations:

Load Not Restores: Other Not Restores: Customer Not Restores: Line Overloads: Other Overloads:

Fault Isolation Switch Plan Steps:

#	Device	Description	Status	Step Type	Phase

10

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



“Send Request” to Isolate Fault

Fault Isolation and Service Restoration

Request ID | Outage Event | Request Sent | Reply Received | In/Service Switch Plan | Status | Error Message

7195		10/21/2013 10:18:28 ...	10/21/2013 10:18:29 ...		Completed	
7949		12/11/2013 6:35:03 PM	12/11/2013 6:35:04 PM		No Solution	No suggested switching ...
7990		12/11/2013 6:36:25 PM	12/11/2013 6:36:26 PM		Completed	
7991		12/11/2013 6:37:00 PM	12/11/2013 6:37:01 PM		No Solution	No suggested switching ...
7992		12/11/2013 6:38:24 PM	12/11/2013 6:38:25 PM		No Solution	No suggested switching ...
7962		12/11/2013 7:14:05 PM				
8000		12/12/2013 9:56:23 AM	12/12/2013 9:56:34 AM		Completed	
8009	00081705					
8037						

Request Details:

Outage Event: View In Map Select From Map Clear Event

Equipment To Isolate:

Device	Description	Phases To Isolate
045903	Primary Conductor - US Conductor	ABC

Response Details:

Load Restores: Other Restores: Customer Restores: Power Loss: Voltage Violations:

Load Not Restores: Other Not Restores: Customer Not Restores: Line Overloads: Other Overloads:

Fault Isolation Switch Plan Steps:

#	Device	Description	Status	Step Type	Phase	Priority

Map View: 045903, ABC

11

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Fault Isolation Results

Fault Isolation and Service Restoration

Fault Isolation (FI) | Service Restoration (SR) | Fault Isolation and Immediate Restoration (FIR) | Restore to Normal (RN)

Filter List...

Request ID	Outage Event	Request Sent	Reply Received	Service Switch Plan	Status	Error Message
7155		12/11/2013 10:18:29 AM	12/11/2013 10:18:29 AM		Completed	
7949		12/11/2013 6:35:03 PM	12/11/2013 6:35:03 PM		No Solution	No suggested switching ...
7950		12/11/2013 6:36:25 PM	12/11/2013 6:36:25 PM		Completed	
7951		12/11/2013 6:37:00 PM	12/11/2013 6:37:00 PM		No Solution	No suggested switching ...
7952		12/11/2013 6:38:24 PM	12/11/2013 6:38:24 PM		No Solution	No suggested switching ...
7952		12/11/2013 7:14:05 PM				
8008		12/11/2013 9:56:33 AM	12/11/2013 9:56:33 AM		Completed	
8009	00083765					
8007		12/09/2013 1:20:12 PM	12/09/2013 1:20:14 PM		Completed	

Create Request | Copy Request

Request Details:

Outage Event: View In Map

Switch Type:

Equipment To Isolate:

Device	Description	Phase To Isolate
4763073	Primary Conductor - LG Conductor	ABC

View In Map

Requester Details:

Load Restores: 0 Wfs Restores: 0 Customer Restores: 0 Power Loss: 0 Voltage Restores: 0

Load Not Restores: 0 Wfs Not Restores: 0 Customer Not Restores: 0 Line Overloads: 0 Wfs Overloads: 0

Difficulty: 0

Fault Isolation Switch Plan Steps:

#	Device	Description	Status	Step Type	Phase
1	1492603	Equipment Cont.	Open	Test/Chk	ABC

View In Map

Switch Plan ID:

Open "Service Restoration" to Restore Faulted Device

Service Restoration Requests:

Request ID	Outage Event	Request Sent	Reply Received	In-Service Switch Plan	Status	Error Message
3		8/29/2013 10:50:30 AM	8/29/2013 10:50:33 AM		No Solution	No suggested switching ...
5		8/30/2013 7:56:21 AM	8/30/2013 7:56:22 AM		No Solution	No suggested switching ...
6		8/30/2013 7:51:36 AM	8/30/2013 7:51:37 AM		No Solution	No suggested switching ...
17		8/30/2013 8:21:17 AM	8/30/2013 8:21:18 AM		No Solution	No suggested switching ...
18		8/30/2013 8:21:46 AM	8/30/2013 8:21:46 AM		No Solution	No suggested switching ...
57		8/30/2013 8:23:26 AM	8/30/2013 8:23:28 AM		No Solution	No suggested switching ...
227		8/30/2013 8:24:03 AM	8/30/2013 8:24:04 AM		No Solution	No suggested switching ...
1897		8/28/2013 7:35:49 AM	8/28/2013 7:36:08 AM		No Solution	No proper input equipm...
1898		8/28/2013 7:40:42 AM	8/28/2013 7:46:16 AM		No Solution	No proper input equipm...
1911		8/28/2013 7:54:10 AM			No Solution	No proper input equipm...

Request Details:

Outage Event: View In Map

Switch Type:

Equipment To Restore:

Device	Description
1042046	Primary Conductor ...

Equipment Not To Restore:

Device	Description
1036031	Primary Conductor ...

Response Details:

Load Restores: Other Restores: Customer Restores: Power Loss: Voltage Violations:
 Load Not Restores: Other Not Restores: Customer Not Restores: Line Overloads: Other Overloads:
 Difficulty:

FSR Service Restoration Switch Plan Steps:

#	Device	Description	Start	Stop Type	Phase
1					

13

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



“Create Request” for Service Restoration

Service Restoration Requests:

Request ID	Outage Event	Request Sent	Reply Received	Service Switch Plan	Status	Error Message
3		8/29/2013 10:50:30 AM	8/29/2013 10:50:33 AM		No Solution	No suggested switching ...
5		8/30/2013 7:56:21 AM	8/30/2013 7:56:22 AM		No Solution	No suggested switching ...
6		8/30/2013 7:51:36 AM	8/30/2013 7:51:37 AM		No Solution	No suggested switching ...
17		8/30/2013 8:21:17 AM	8/30/2013 8:21:18 AM		No Solution	No suggested switching ...
18		8/30/2013 8:21:46 AM	8/30/2013 8:21:46 AM		No Solution	No suggested switching ...
57		8/30/2013 8:23:26 AM	8/30/2013 8:23:28 AM		No Solution	No suggested switching ...
227		8/30/2013 8:24:03 AM	8/30/2013 8:24:04 AM		No Solution	No suggested switching ...
1897		8/28/2013 7:35:49 AM	8/28/2013 7:36:08 AM		No Solution	No proper input equipm...
1898		8/28/2013 7:40:42 AM	8/28/2013 7:41:16 AM		No Solution	No proper input equipm...
1911		8/28/2013 7:44:10 AM			No Solution	No proper input equipm...

Request Details:

Outage Event: View In Map

Switch Type:

Equipment To Restore:

Service	Description
1042046	Primary Conductor ...

Equipment Not To Restore:

Device	Description
1036031	Primary Conductor ...

Response Details:

Load Restores: 0 Other Restores: 0 Customer Restores: 0 Power Loss: 0 Voltage Violations: 0

Load Not Restores: 0 Other Not Restores: 0 Customer Not Restores: 0 Line Overloads: 0 Other Overloads: 0

DFSR Service Restoration Switch Plan Steps:

#	Device	Description	Start	Stop Type	Phase
1					

Map View: Shows a power line network with a node labeled '045903' and 'ABC'.

14

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Request Created

Service Restoration Requests

Request ID	Outage Event	Request Sent	Reply Received	In/Service Switch Plan	Status	Error Message
7102		10/31/2013 3:52:30 PM	10/31/2013 3:52:40 PM		Completed	
7196		11/1/2013 11:51:55 AM	11/1/2013 11:51:58 AM		No Solution	No suggested switching...
7199		11/1/2013 11:52:49 AM	11/1/2013 11:52:46 AM		Completed	
7964		12/11/2013 7:17:02 PM	12/11/2013 7:17:04 PM		Completed	
8010		12/13/2013 10:00:03 ...	12/13/2013 10:00:05 ...		Completed	
8015		12/13/2013 10:48:22 ...	12/13/2013 10:48:24 ...		Completed	
8016		12/13/2013 11:47:31 ...	12/13/2013 11:47:32 ...		Completed	
8017		12/13/2013 11:49:13 ...	12/13/2013 11:49:15 ...		Completed	
8020						

Request Details:
 Outage Event: [] View In Map Select From Map Clear Event
 Switch Type: All Remote Control Only

Equipment To Restore:

Device	Description	Device	Description	Device	Description

Response Details:
 Load Restores: [] Other Restores: [] Customer Restores: [] Power Loss: [] Voltage Violations: []
 Load Not Restores: [] Other Not Restores: [] Customer Not Restores: [] Line Overloads: [] Other Overloads: []
 (Difficulty)

FSR Service Restoration Switch Plan Steps:

#	Device	Description	Step	Step Type	Phase

15

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



“Select from Map” to Select a Device

Service Restoration Requests:

Request ID	Outage Event	Request Sent	Reply Received	In Service Switch Plan	Status	Error Message
7102		10/21/2013 3:52:30 PM	10/21/2013 3:52:40 PM		Completed	
7196		11/1/2013 11:51:55 AM	11/1/2013 11:51:56 AM		No Solution	No suggested switching...
7199		11/1/2013 11:52:44 AM	11/1/2013 11:52:46 AM		Completed	
7964		12/11/2013 7:17:02 PM	12/11/2013 7:17:04 PM		Completed	
8010		12/13/2013 10:00:03 ...	12/13/2013 10:00:05 ...		Completed	
8015		12/13/2013 10:48:22 ...	12/13/2013 10:48:24 ...		Completed	
8016		12/13/2013 11:47:31 ...	12/13/2013 11:47:32 ...		Completed	
8017		12/13/2013 11:49:13 ...	12/13/2013 11:49:15 ...		Completed	
8020						

Request Details:
 Outage Event: View In Map Select From Map Clear Event
 Switch Type: All Remote Control Only

Equipment To Exclude:
 Device: Description:

Equipment As Restoration Source:
 Device: Description:

Equipment Not To Restore:
 Device: Description:

View In Map **Select From Map** Delete Selected Delete All

Use Look Ahead Start Date: Year: End Date: View: Security Factor:

Response Details:
 Load Restores: Other Restores: Customer Restores: Power Loss: Voltage Violations:
 Load Not Restores: Other Not Restores: Customer Not Restores: Line Overloads: Other Overloads:

FSR Service Restoration Switch Plan Steps:

#	Device	Description	Start	Stop Type	Phase
1					

Switch Plan ID:

•16

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Device Updated

Service Restoration Requests:

Request ID	Outage Event	Request Sent	Reply Received	Service Switch Plan	Status	Error Message
7182		10/31/2013 3:52:39 PM	10/31/2013 3:52:40 PM		Completed	
7198		11/1/2013 11:51:58 AM	11/1/2013 11:51:56 AM		No Solution	No suggested switching ...
7199		11/1/2013 11:52:44 AM	11/1/2013 11:52:46 AM		Completed	
7964		12/11/2013 7:17:52 PM	12/11/2013 7:17:54 PM		Completed	
8010		12/13/2013 10:00:03 ...	12/13/2013 10:00:05 ...		Completed	
8015		12/13/2013 10:48:22 ...	12/13/2013 10:48:24 ...		Completed	
8016		12/13/2013 11:47:31 ...	12/13/2013 11:47:32 ...		Completed	
8017		12/13/2013 11:49:13 ...	12/13/2013 11:49:15 ...		Completed	

Request Details:

Outage Event: View In Map Select From Map Clear Event

Switch Type: 48 Remote Control Only

Equipment To Restore:

Device	Description
4163872	Primary Conductor ...

Equipment Not To Restore:

Device	Description
--------	-------------

Response Details:

Load Restored: Wires Restored: Customer Restored: Power Loss: Voltage Violations:
 Load Not Restored: Wires Not Restored: Customer Not Restored: Line Overloads: Wires Overloads:
 Difficulty:

PISR Service Restoration Switch Plan Steps:

#	Device	Description	Status	Step Type	Phase
---	--------	-------------	--------	-----------	-------

17

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



“Send Request” for Service Restoration

Service Restoration Requests:

Request ID	Outage Event	Request Sent	Reply Received	In-Service Switch Plan	Status	Error Message
7152		10/31/2013 3:52:38 PM	10/31/2013 3:52:40 PM		Completed	
7196		11/1/2013 11:51:25 AM	11/1/2013 11:51:56 AM		No Solution	No suggested switching ...
7199		11/1/2013 11:52:44 AM	11/1/2013 11:52:46 AM		Completed	
7664		12/11/2013 7:17:02 PM	12/11/2013 7:17:04 PM		Completed	
8050		12/13/2013 10:00:03 ...	12/13/2013 10:00:05 ...		Completed	
8025		12/13/2013 10:48:22 ...	12/13/2013 10:48:24 ...		Completed	
9005		12/13/2013 11:47:31 ...	12/13/2013 11:47:32 ...		Completed	
9017		12/13/2013 11:49:13 ...	12/13/2013 11:49:15 ...		Completed	
9038						

Request Details:

Outage Event: View In Map Select From Map Clear Events

Switch Type: All Remote Control Only

Equipment To Restore:

Device	Description	Device	Description	Device	Description
452923	Primary Conductor				

Response Details:

Load Restores: Other Restores: Customer Restores: Power Loss: Voltage Violations:
 Load Not Restores: Other Not Restores: Customer Not Restores: Line Overloads: Other Overloads:
 FSR Service Restoration Switch Plan Steps: Difficulty:

Send Request

18

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



“Service Restoration” Results

Service Restoration Requests:

Request ID	Outage Event	Request Sent	Reply Received	In-Service Switch Plan	Status	Error Message
7152		10/31/2013 3:52:38 PM	10/31/2013 3:52:40 PM		Completed	
7196		11/1/2013 11:51:25 AM	11/1/2013 11:52:16 AM		No Solution	No suggested switching ...
7199		11/1/2013 11:52:44 AM	11/1/2013 11:52:46 AM		Completed	
7864		12/11/2013 7:17:02 PM	12/11/2013 7:17:04 PM		Completed	
8050		12/13/2013 10:00:03 ...	12/13/2013 10:00:05 ...		Completed	
8055		12/13/2013 10:48:22 ...	12/13/2013 10:48:24 ...		Completed	
8055		12/13/2013 11:47:31 ...	12/13/2013 11:47:32 ...		Completed	
8057		12/13/2013 11:49:13 ...	12/13/2013 11:49:15 ...		Completed	
8058		12/20/2013 1:44:09 PM	12/20/2013 1:44:10 PM		Completed	

Request Details:

Outage Event: View In Map Switch Type:

Equipment To Restore:

Device	Description	Device	Description	Device	Description
4703873	Primary Conductor ...				

Response Details:

Load Restored: 88 Other Restored: 0 Customer Restored: 297 Power Loss: 47 Voltage Violations: 2
 Load Not Restored: 0 Other Not Restored: 0 Customer Not Restored: 0 Line Overloads: 0 Other Overloads: 1
 Difficulty: 0

FSR Service Restoration Switch Plan Steps:

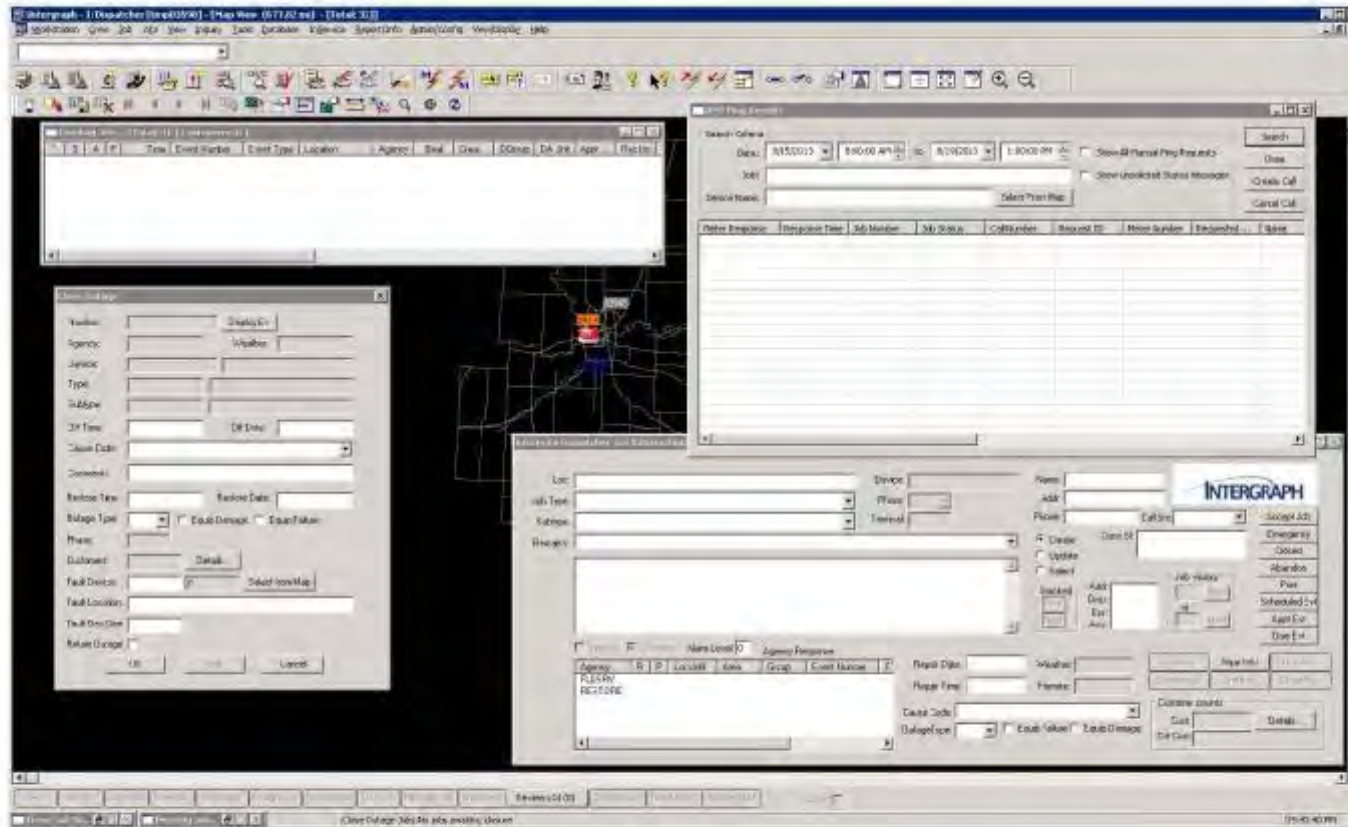
#	Device	Description	Status	Step Type	Phase
0	1490681	Switch	Close	SWITCH	ABC
1	972994	Switch	Close	SWITCH	ABC

Outage and Restoration Events

- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program



Windows Used for Outage and Restoration

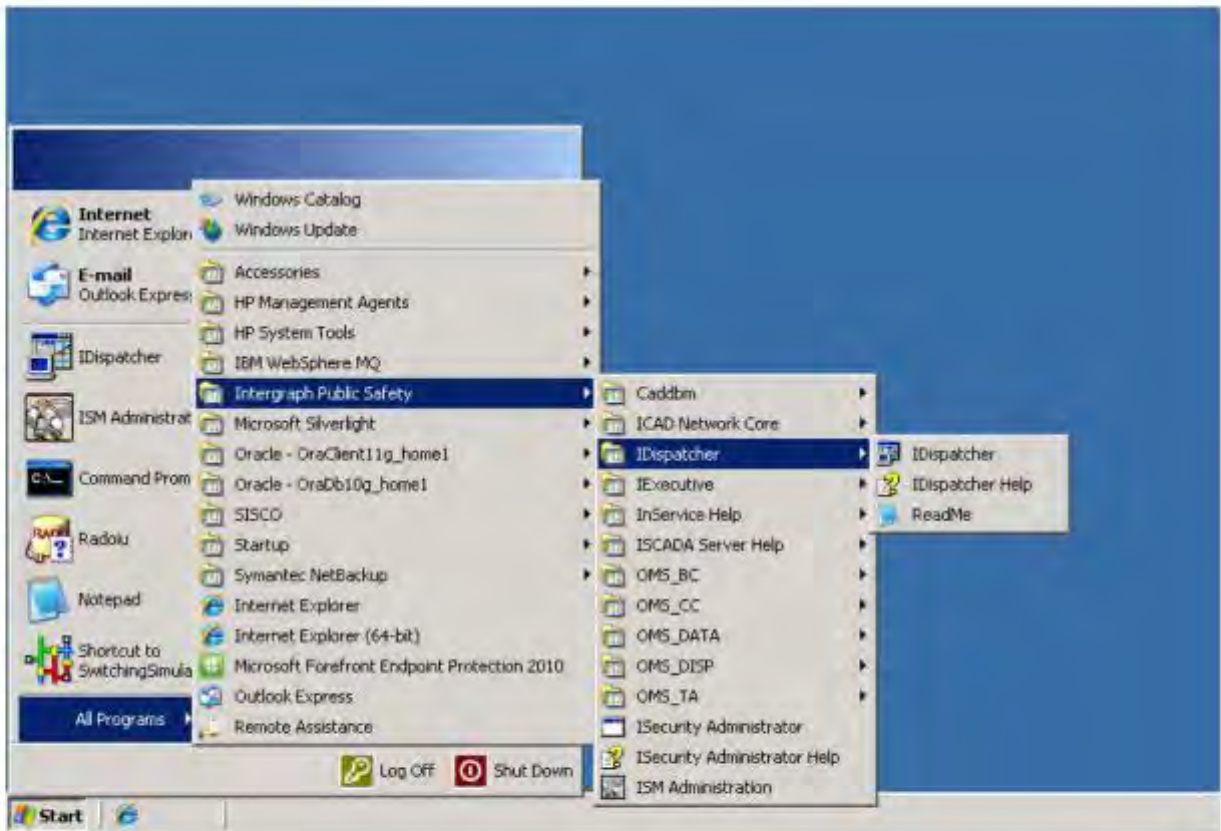


2

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Launch InService I/Dispatcher

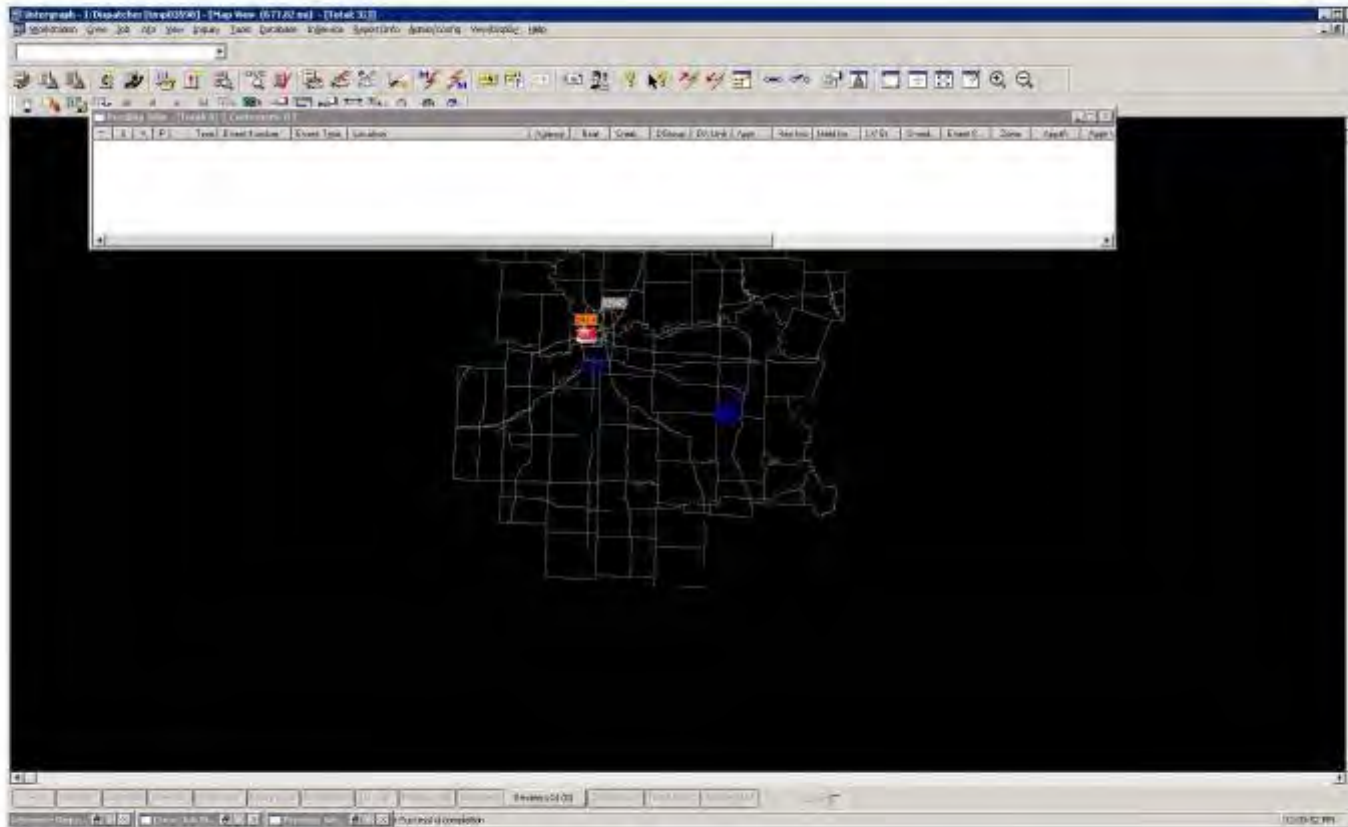


3

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



“Pending Jobs” Window

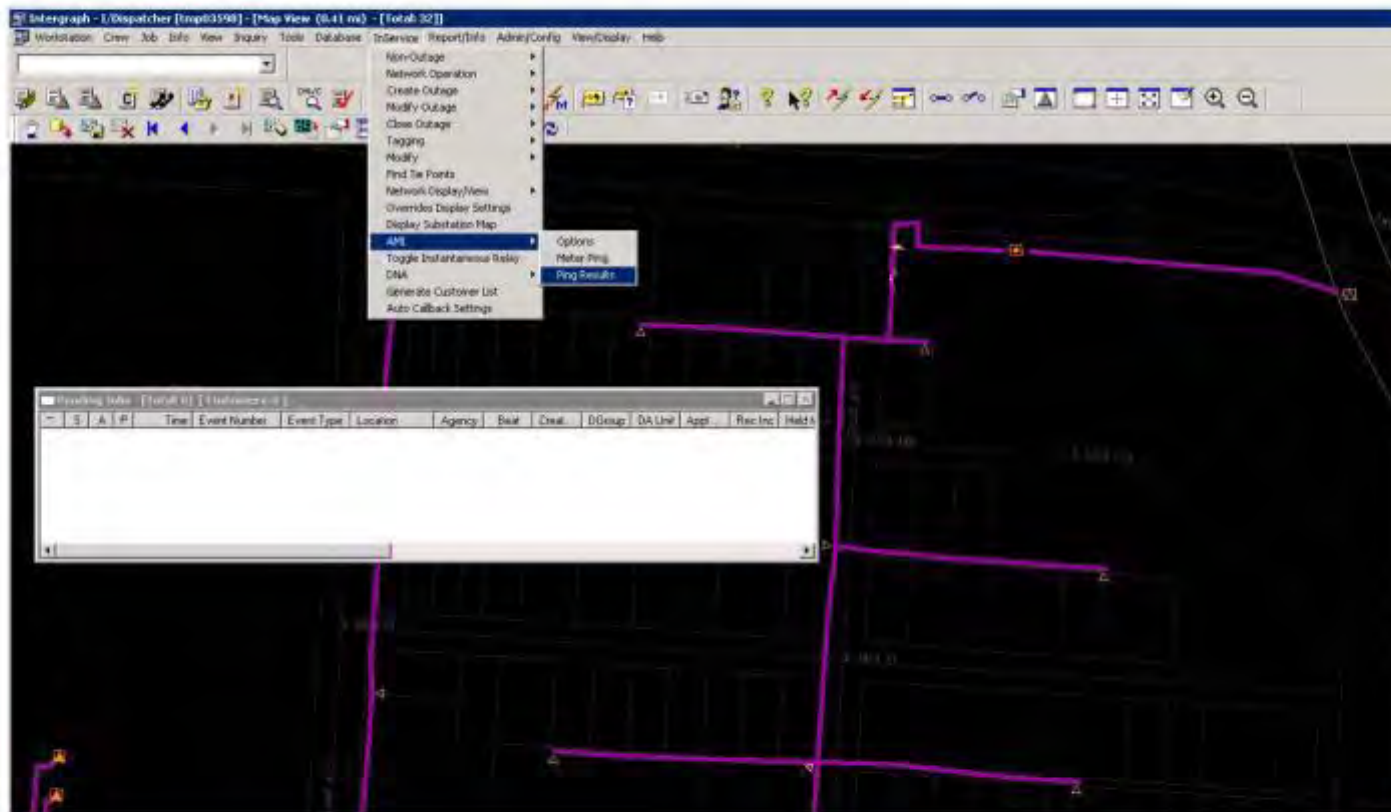


5

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Open the “AMI Ping Results” Window



6

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Service-Level Outage in “Pending Jobs” Window

The screenshot displays a software application window titled "Pending Jobs - [Total: 1] | Customers: 1". The window contains a table with the following columns: S, A, P, Type, Event Number, **Event Type**, Location, Agency, Base, Date, Group, DA Unit, App, Re: No, Held by, LV St, Over, Event Subtype, Zone, AppA, App/Wrt, Date W. The "Event Type" column header is highlighted with a red box.

Below the "Pending Jobs" window is another window titled "AMI Ping Results". It features search criteria fields for Date (8/15/2013) and Time (6:24:39 AM to 8:24:39 AM), along with checkboxes for "Show All Manual Ping Requests" and "Show Unlinked Status Messages". There are buttons for "Search", "Close", "Create Call", and "Cancel Call". Below these fields is a table with columns: Meter Response, Response Time, Job Number, Job Status, Call Number, Request ID, Meter Number, Requested, Name, Location, Phone, Transformer, Unlabeled, Employee ID, Event.

8

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Search in “AMI Ping Results” for Outage Information

The screenshot displays the Intergraph software interface for searching AMI Ping Results. The search criteria are set to Date: 8/15/2013 and Time: 8:00:00 AM to 10:00:00 AM. The search button is highlighted with a red box. Below the search criteria, there is a table with the following data:

Meter Request	Request Time	Job Number	Job Status	Call Number	Request ID	Meter Number	Requested Device	Meter Location	Phone	Transformer	Unsubscribed	Employee ID	Event Type	Event Subtype	Request Time	Job Device	Meter Status
X	08/15/2013 08:00:00			00004	8	109610711004		4415	4415	1079-00	101						

9

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Transformer-Level Outage in "Pending Jobs" Window

The screenshot shows a software application window titled "Intergraph - 1/Dispatcher [Emp02590] - [Map View (677.82 mi)] - [Total: 33]". Below the title bar is a menu bar with options: "Workstation", "Crew", "Job", "Info", "View", "Display", "Tools", "Database", "In-Service", "Report/Print", "Admin/Config", "View/Display", "Help". A toolbar with various icons is located below the menu bar.

The main window displays a "Pending Jobs" window with a table. The table has the following columns: "Time", "Event Number", "Event Type", "Location", "Agency", "Eoat", "Dist", "DGroup", "Gd Unit", "App", "Rec Inc", "Hold Inc", "L/S St", "Ovrd", "Event Subtype", "Zone", "AppA", "Appt Wkr", "Dist W...". The "Event Type" column is highlighted with a red box.

Below the table is a search criteria section with fields for "Date" (8/15/2013), "Time" (8:00:00 AM to 10:00:00 AM), and "Device Name". There are checkboxes for "Show All Manual Ping Requests" and "Show Unpublished Status Messages". Buttons for "Search", "Close", "Create Call", and "Cancel Call" are also present.

The table below the search criteria has the following columns: "Meter Response", "Response Time", "Job Number", "Job Status", "Call Number", "Request ID", "Meter Number", "Requested Device", "Name", "Location", "Phone", "Transformer", "Unpublished", "Employee ID", "Event Type", "Event Subtype", "Request Time", "Job Device", "Meter Status".

10

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Search in "AMI Ping Results" for Outage Information

The screenshot shows a software application window titled "AMI Ping Results". At the top, there is a search criteria section with the following fields and options:

- Date: 8/15/2013
- Time: 6:00:00 AM
- To Date: 8/15/2013
- To Time: 10:00:00 AM
- Buttons: Search (highlighted in red), Close, Create Call, Cancel Call
- Checkboxes: Show All Manual Ping Requests, Show Unpublished Status Messages
- Field: Job: [Empty]
- Field: Device Name: [Empty] with a "Select From Map" button.

Below the search criteria is a data table with the following columns:

Meter Response	Response Time	Job Number	Job Status	Call Number	Request ID	Meter Number	Requested Device	Name	Location	Phone	Transformer	Unpublished	Employee ID	Event Type	Event Subtype	Request Title	Job Device	Meter Status
	8/15/2013 6:07:51			01599	0	129490711500		JA	512 E...	284	1079130	104						
	8/15/2013 6:08:19			01504	0	129490711502		AA	4418 ...	251	1079130	105						

Fuse-Level Outage in "Pending Jobs" Window

The screenshot displays the Intergraph Dispatcher software interface. At the top, the title bar reads "Intergraph - 1/Dispatcher [Imp02598] - [Map View (672.82 mi) - [Total: 32]]". Below the title bar is a menu bar with options: "Workstation", "View", "Job", "Info", "View", "History", "Tools", "Database", "InService", "Report/Info", "Admin/Config", "View/Display", "Help". A toolbar with various icons is located below the menu bar.

The main window is titled "Pending Jobs - [Total: 1] [Click to expand]". It contains a table with the following columns: "Time", "Event Number", "Event Type", "Location", "Agency", "Root", "Class", "Device", "DA User", "App", "Req No", "Held For", "LVSL", "Overst", "Event Subtype", "Zone", "Appn", "App Wks", "Date Wk". The table contains one row of data:

Time	Event Number	Event Type	Location	Agency	Root	Class	Device	DA User	App	Req No	Held For	LVSL	Overst	Event Subtype	Zone	Appn	App Wks	Date Wk	
8/15/2013 6:00:00 AM	00000220	FUSE	1310357	RESTORE	LOGON	INTG	PC00							01	PHILUCK				

Below the table is a search criteria panel titled "AMI-Pending Requests". It includes fields for "Date" (8/15/2013), "Time" (6:00:00 AM), "End Date" (8/15/2013), and "End Time" (10:00:00 AM). There are checkboxes for "Show All Manual Pending Requests" and "Show Unchecked Status Messages". Buttons for "Search", "Clear", "Create Call", and "Cancel Call" are also present.

Below the search panel is a table with the following columns: "Meter Requests", "Response Time", "Job Number", "Job Status", "Call Number", "Request ID", "Meter Number", "Requested Device", "Phase", "Location", "Phone", "Transformer", "Unchecked", "Employee ID", "Event Type", "Event Subtype", "Request Time", "Job Device", "Meter Status". The table contains two rows of data:

Meter Requests	Response Time	Job Number	Job Status	Call Number	Request ID	Meter Number	Requested Device	Phase	Location	Phone	Transformer	Unchecked	Employee ID	Event Type	Event Subtype	Request Time	Job Device	Meter Status
00000220	8/15/2013 6:00:00 AM	00000220	0	00000	0	1224500711000	RESTORE	A	1310357	284	1076930	104		FUSE	01	8/15/2013 6:00:00 AM	PC00	
00000220	8/15/2013 6:00:00 AM	00000220	0	00000	0	1224500711000	RESTORE	A	1310357	284	1076930	104		FUSE	01	8/15/2013 6:00:00 AM	PC00	

12

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Search in "AMI Ping Results" for Outage Information

The screenshot displays the 'AMI Ping Results' search window. The search criteria are: Date: 8/15/2013, Time: 6:00:00 AM to 10:00:00 AM. The search button is highlighted with a red box. Below the search criteria is a table of results with the following columns: Meter Response, Response Time, Job Number, Job Status, Call Number, Request ID, Meter Number, Requested Device, Name, Location, Phone, Transformer, Unlocked, Employee ID, Event Type, Event Subtype, Request Time, Job Device, and Meter Status.

Meter Response	Response Time	Job Number	Job Status	Call Number	Request ID	Meter Number	Requested Device	Name	Location	Phone	Transformer	Unlocked	Employee ID	Event Type	Event Subtype	Request Time	Job Device	Meter Status
X	8/15/13 06:38:29	00000	0	00000	0	10941230503	DL	440	200	327100	101							
X	8/15/13 06:52:01	00000	0	00000	0	109452711060	DL	440	200	305930	101							
X	8/15/13 06:55:13	00000	0	00000	0	109452711060	DL	440	200	305930	101							

13

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Confirm the Outage

The screenshot displays the Intergraph software interface. At the top, a title bar reads "Intergraph - I.Dispatcher [Emp02598] - [Map View (677.62 mi) - [Total: 22]]". Below the title bar is a menu bar with options: "Workstation", "Draw", "Job", "Info", "View", "Query", "Tools", "Database", "Dispatcher", "Reports/Info", "Admin/Config", "View/Display", "Help". A toolbar with various icons is located below the menu bar. A data table is visible, with the "Event Subtype" column highlighted in red. The table contains the following data:

Tree	Event Number	Event Type	Location	Agency	Beat	Dist	DGroup	GA Unit	Appl	Pac Inct	Heater	LV Str	Dvend	Event Subtype	Zone	PostA	Appl Ver	Date W
14	60003220	FUSE	1010907	RESTORE	00000	mg	R000					V	00	FUSE(CT)				

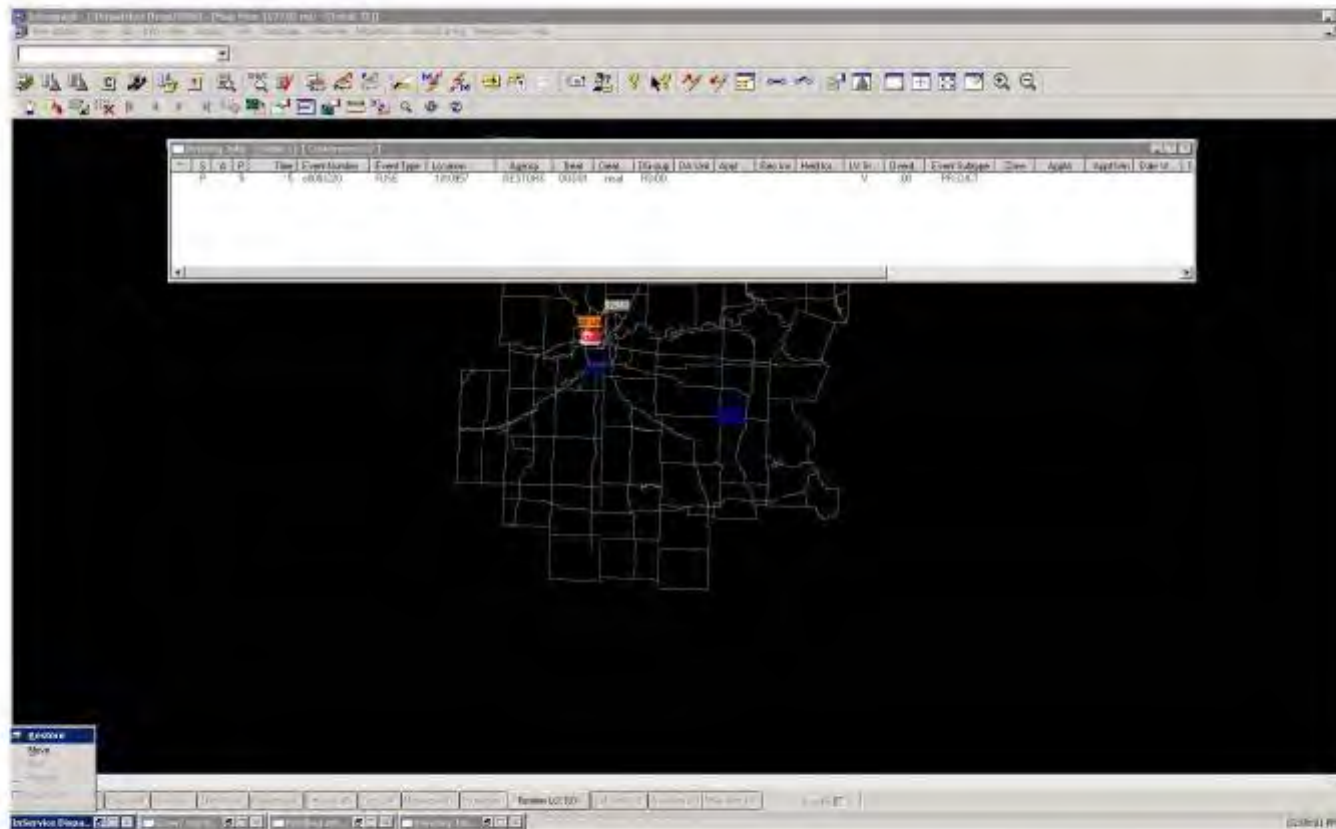
Below the table is a map showing a network of lines and nodes. A red circle highlights a specific node on the map, corresponding to the event data in the table above.

14

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Restore “InService Dispatcher Job Information” Window

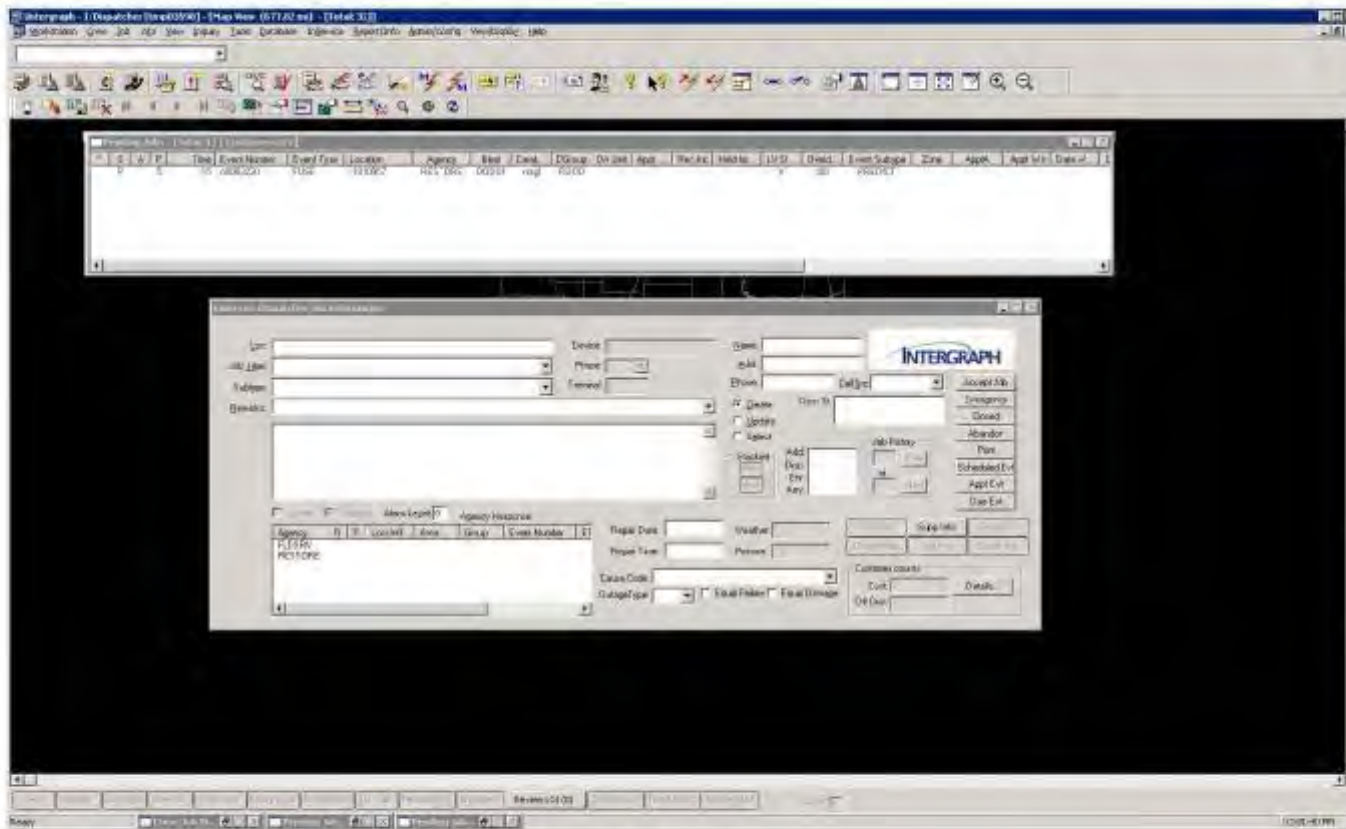


15

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Select the Job in “Pending Jobs” Window

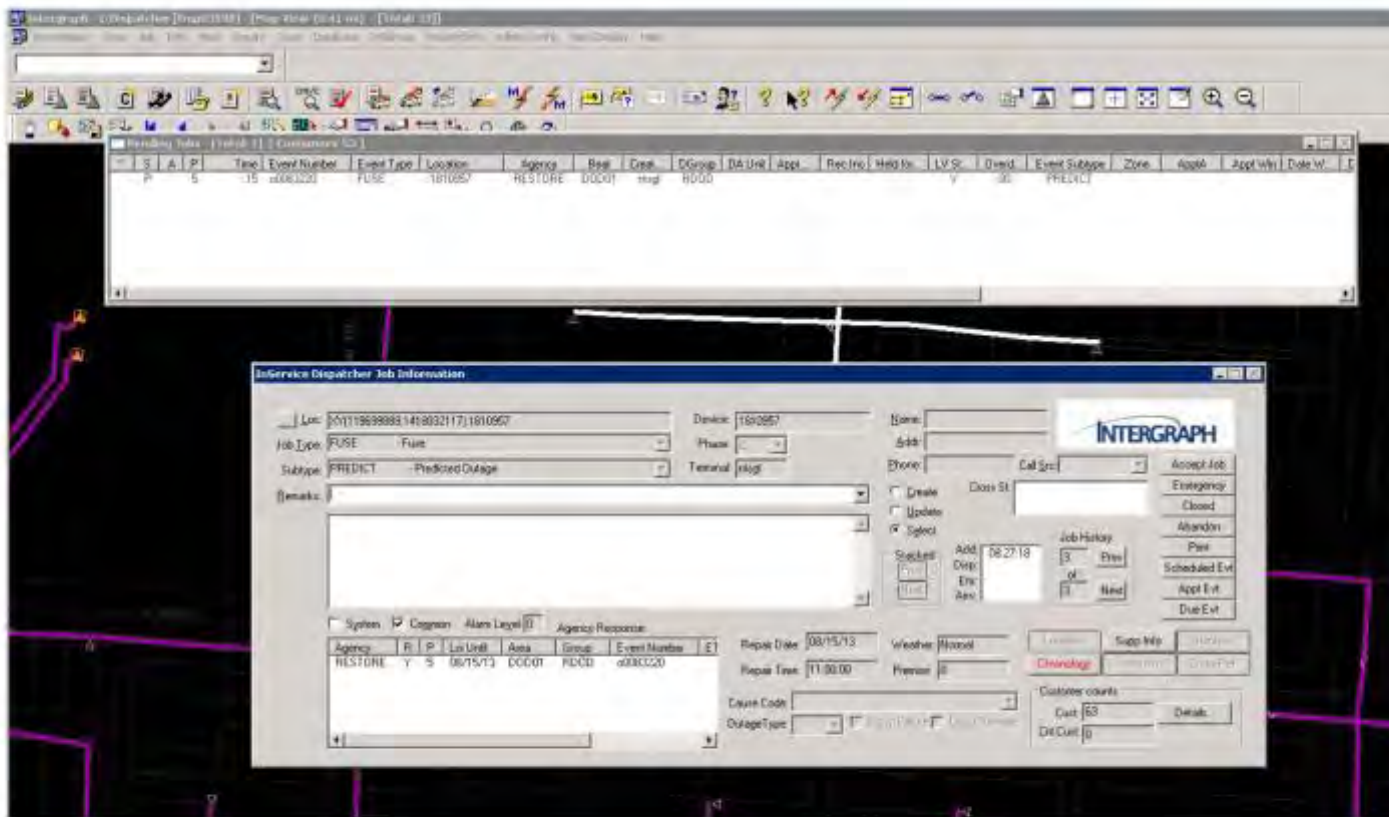


16

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Fields in “InService Dispatcher Job Information” Window

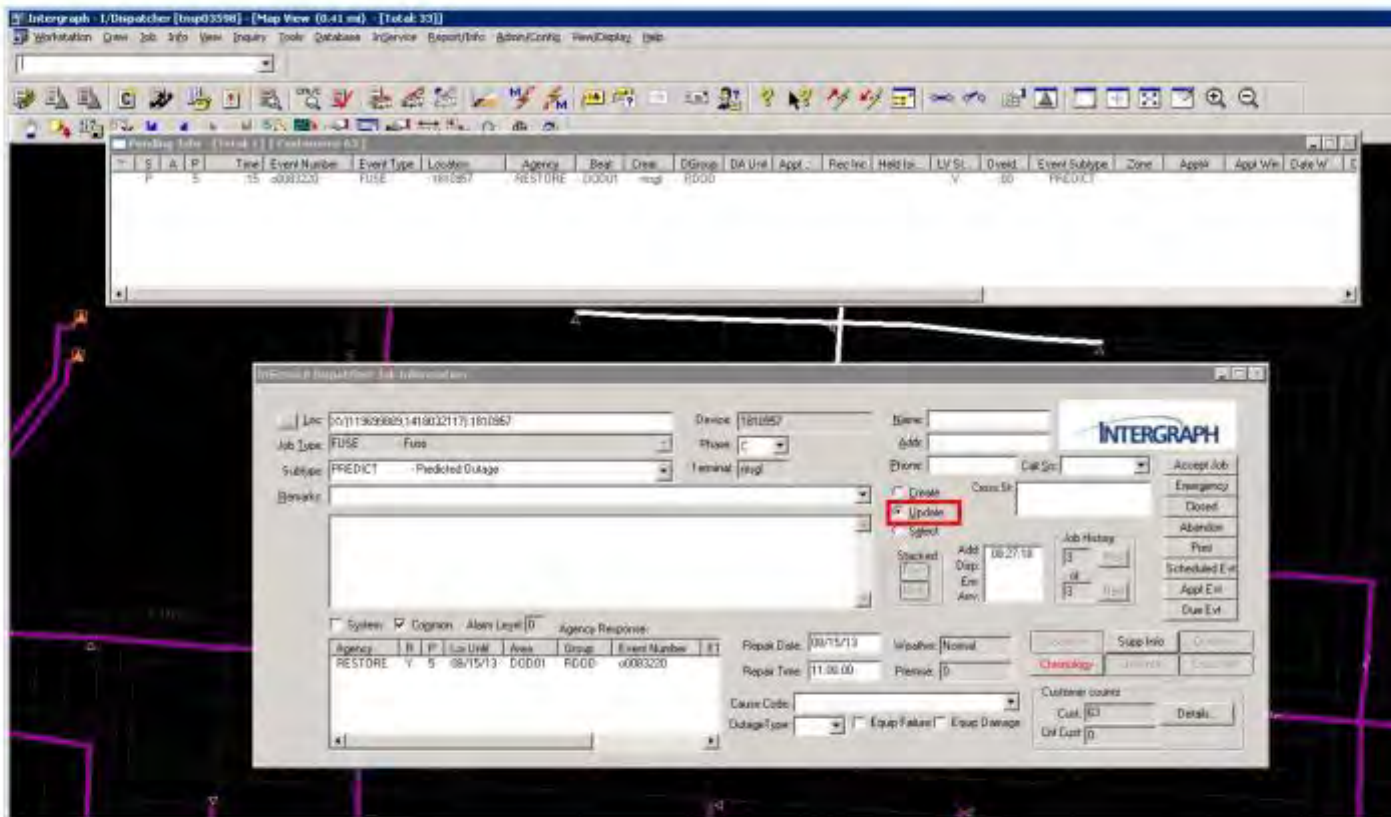


17

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Select "Update" to Confirm the Outage



18

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Update Outage from "PREDICT" to "CONFIRM"

The screenshot displays the Intergraph software interface. At the top, a table lists outage events. The highlighted row is as follows:

Time	Event Number	Event Type	Location	Agency	Reg	Comp	CGroup	DA Unit	Appr	Rec Ino	Held In	LV St	Overst	Event Subtype	Zone	Appld	Appl Wky	Date Wk
5	15	00003200	FUSE	1810957	RESTORE	00001	reg	R000				Y		30	PREDICT			

Below the table, the 'Dispatcher Job Information' window is open. It shows the following details:

- Job Type: FUSE
- Subtype: PREDICT - Rowlock Outage
- Default: PREDICT - Predicted Outage
- Agency: RESTORE
- Repair Date: 08/15/13
- Weather: Normal
- Customer Count: 93

Confirm the Outage

The screenshot displays the Intergraph software interface. At the top, a table lists event data:

Time	Event Number	Event Type	Location	Agency	Rest	Cost	DRGID	DA Unit	Appr	Rec Inv	Held On	LV St	Overst	Event Subtype	Zone	AppA	App Info	Dist W
16	0008229	FUSE	1810957	RESTORE	00001	000								PREDICT				

The main dialog box, titled 'Confirm the Outage', contains the following information:

- Location:** 0V117969008 14180321711810957
- Device:** 1810957
- Job Type:** FUSE - Fuse
- Subtype:** CONFIRM - Confirmed Outage
- Terminal:** ysg2
- Agency Restores Table:**

Agency	R	P	Last Mod	Area	Susp	Event Number	ET
RESTORE	Y	S	08/15/13	D0001	R000	0008229	
- Repair Date:** 08/15/13
- Repair Time:** 11:00:00
- Weather:** Normal
- Pressure:** 0
- Buttons:** Accept Job, Emergency, Closed, Abandon, Print, Scheduled Ev, Appl Ev, Out Ev, Supp Info, Customer counts, Details.

Enter Remarks

The screenshot displays two windows from the Intergraph software interface. The top window shows a data table with the following columns: S, A, P, Time, Event Number, Event Type, Location, Agency, Bear, Crest, DGroup, DA Unit, Appl, Pac In, Held In, LV St, Direct, Event Subtype, Zone, Appl, Appr Win, Date W. A single row of data is visible: P, 5, 15, 0033220, FUSE, 1810957, RESTORE, DUCO, HJG, HJG, DA Unit, Appl, Pac In, Held In, LV St, Direct, Event Subtype, Zone, Appl, Appr Win, Date W.

The bottom window is titled "Service Dispatcher Job Information" and contains the following fields and sections:

- Job Details:**
 - Link: 0-111-9593893.14190321175.1810957
 - Device: 1810957
 - Job Type: FUSE - Fuse
 - Subtype: CIND/FHM - Confined Outage
 - Remarks: meter outage
- INTERGRAPH Logo**
- Buttons:** Accept Job, Emergency, Closed, Abandon, Print, Scheduled Ev, Appl Ev, Due Ev
- Agency Response Table:**

Agency	R	P	LV Unit	Appr	Group	Event Number	ET
RESTORE	Y	5	00/15/13	DUCO	HJG	0033220	
- Other Fields:**
 - Repair Date: 08/15/13
 - Repair Time: 11:00:00
 - Weather: Normal
 - Pressure: 0
 - Cause Code: [Dropdown]
 - Outage Type: [Dropdown]
 - Equip Failure: [Checkbox]
 - Equip Damage: [Checkbox]
 - Customer count: [Dropdown]
 - Est: 63
 - Est Cost: 0

21

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Outage Confirmed

The screenshot displays a software interface with a table of events and a detailed 'Dispatcher Job Information' window. The table lists event details, and the job information window provides specific data for a confirmed outage.

Time	Event Number	Event Type	Location	Agency	Real	Dist	DGroup	LA Unit	App	Fac In	Hold In	LV Br	Direct	Event Subtype	Zone	Appl	Appl Win	Date W
P	5	15	00083220	FUSE	1810957	RESTORE	D0001	Intgr	R000			V	IE	PREDICT				

Dispatcher Job Information

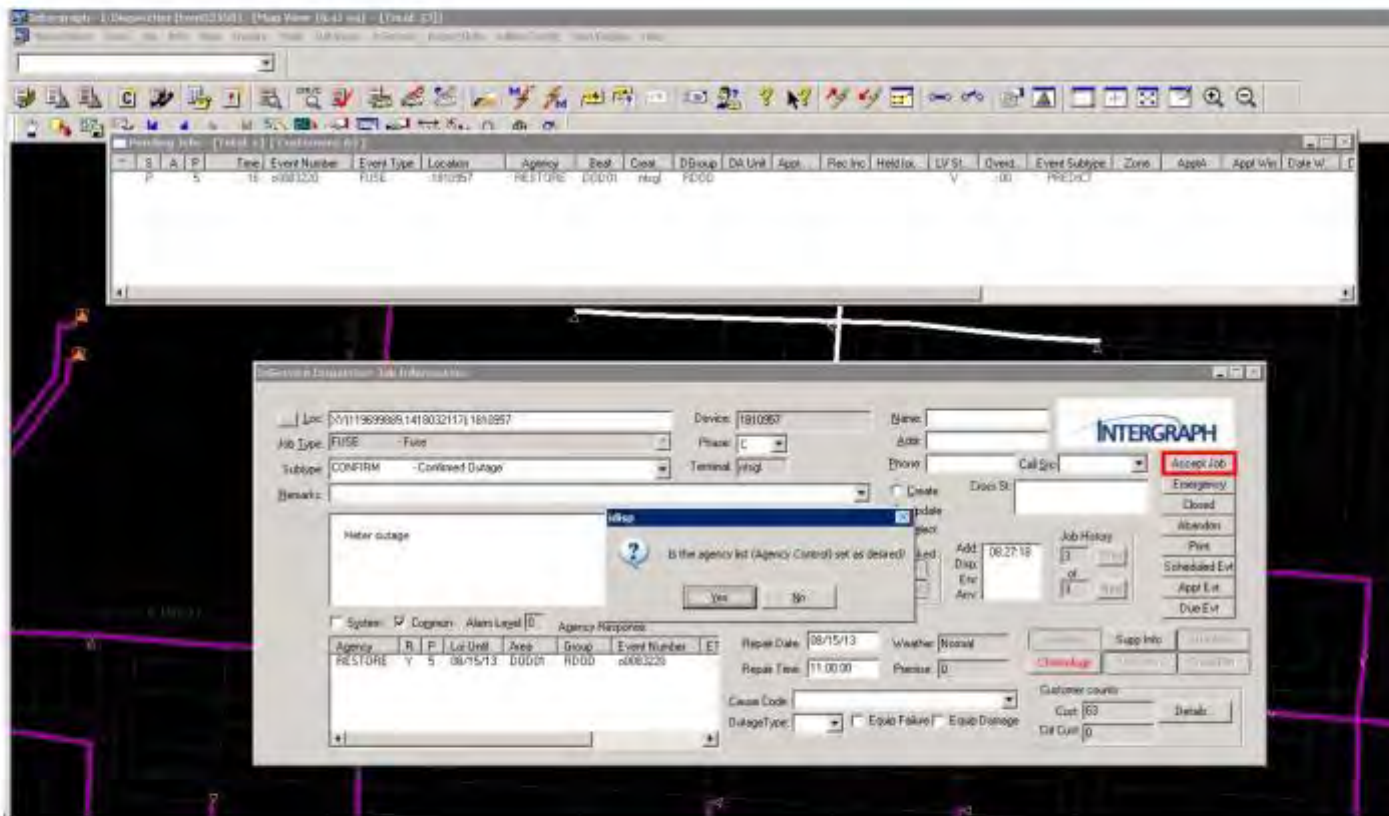
Job Type: FUSE - Fuse
 Subtype: CONFIRM - Confirmed Outage
 Device: 1810957
 Phase: C
 Terminal: Intgr
 Cause Code: Water outage
 Repair Date: 08/15/13
 Repair Time: 11:00:00
 Weather: Normal
 Pressure: 0
 Cause Code: OutageType
 Equip Failure: Equip Damage

22

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Click "Accept Job"



23

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Job is Accepted and Outage is Confirmed

The screenshot displays the Intergraph software interface. At the top, a 'Pending Jobs' table is visible with the following data:

Time	Event Number	Event Type	Location	Agency	Reg	Dist	DGroup	DA Unit	App	Fac Inv	Held For	LV St	Dist	Event Subtype	Zone	Appl	App Wk	Date W
9	00082220	FUSE	1810957	RESTORE	DUCO	REG	R000					Y	00	CONFIRM				

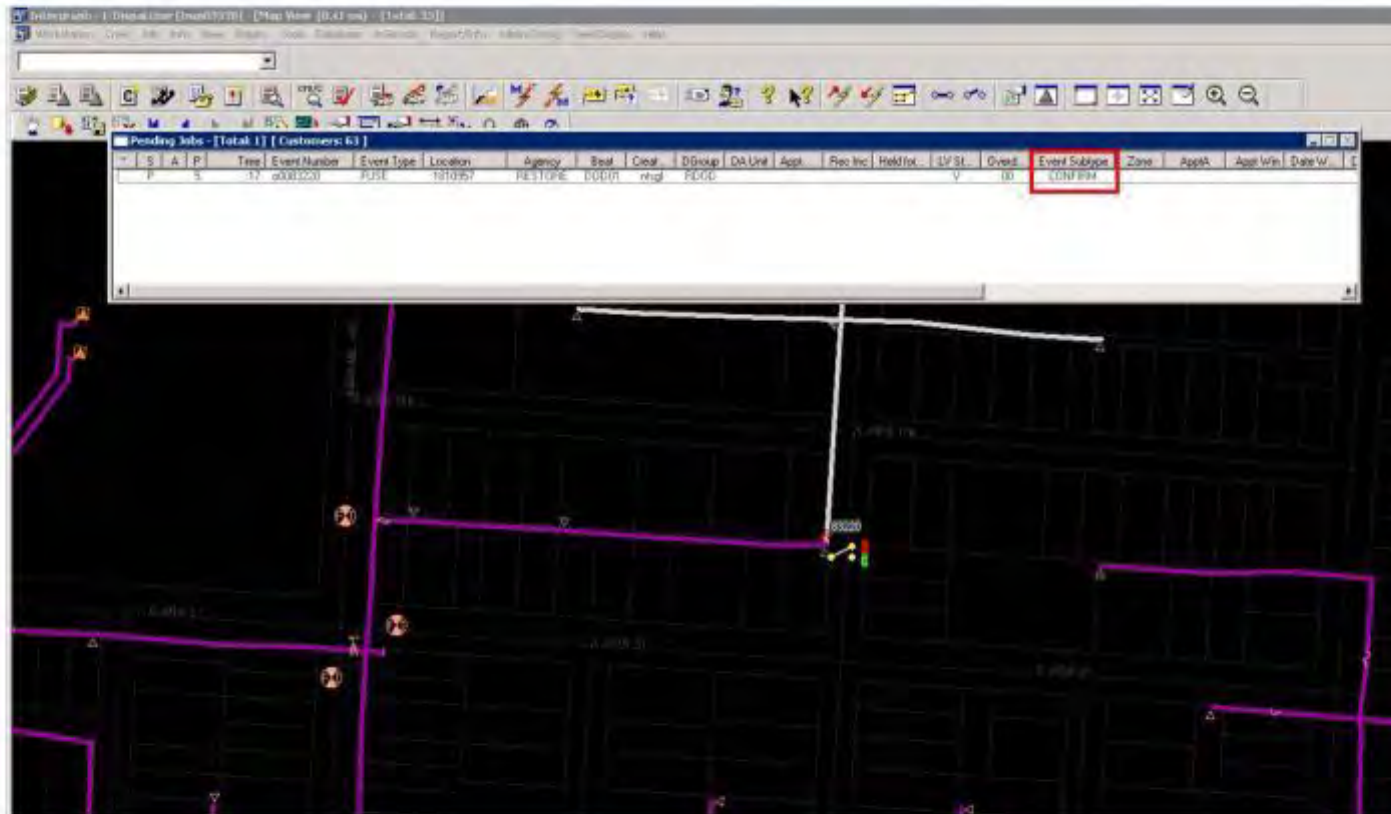
Below the table, a 'Dispatcher Job Information' dialog box is open. The 'Job Type' is 'FUSE' and the 'Subtype' is 'CONFIRM - Confirmed Outage', which is highlighted with a red box. The dialog also shows a description: 'Water outage. Outage update request for event 00082220 sent to Trouble Analysis.' Other fields include 'Loc: 041115699893.141803211711810957', 'Device: 1810957', 'Phase: F', and 'Terminal: REG'. The 'INTERGRAPH' logo is visible in the top right of the dialog.

24

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Event Subtype updated to "CONFIRM"



25

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Fields in “AMI Ping Results” after Outage is Confirmed

The screenshot displays a software window titled "AMI Ping Results" with a search criteria section and a data table. The search criteria include Date (8/15/2013), Time (6:00:00 AM to 10:00:00 AM), and checkboxes for "Show All Manual Ping Requests" and "Show Unchecked Status Messages".

Meter Response	Resource Time	Job Number	Job Status	Call Number	Request ID	Meter Number	Requested Device	Name	Location	Phone	Transformer	Unchecked	Employee ID	Event Type	Event Subtype	Request Time	Job Device	Meter Status
X	8/15/13 06:26:18	0000220	P	01504	0	109461071862	SA	4610	287	1079030	100			PING	CONFIRM	8/15/13 06:26:18	1810957	
X	8/15/13 06:26:29	0000220	P	01506	0	110441226272	SA	4602	824	1079030	100			PING	CONFIRM	8/15/13 06:26:29	1810957	
X	8/15/13 06:26:41	0000220	P	01509	0	102461071862	SA	4602	286	1079030	100			PING	CONFIRM	8/15/13 06:26:41	1810957	

26

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Search in "AMI Ping Results" for Restoration Information

The screenshot shows the Intergraph software interface with a search dialog box open. The search criteria are set to State: NJ, Start Time: 8/15/2013 6:00:00 AM, and End Time: 8/15/2013 10:00:00 AM. The search results table is displayed below the dialog box.

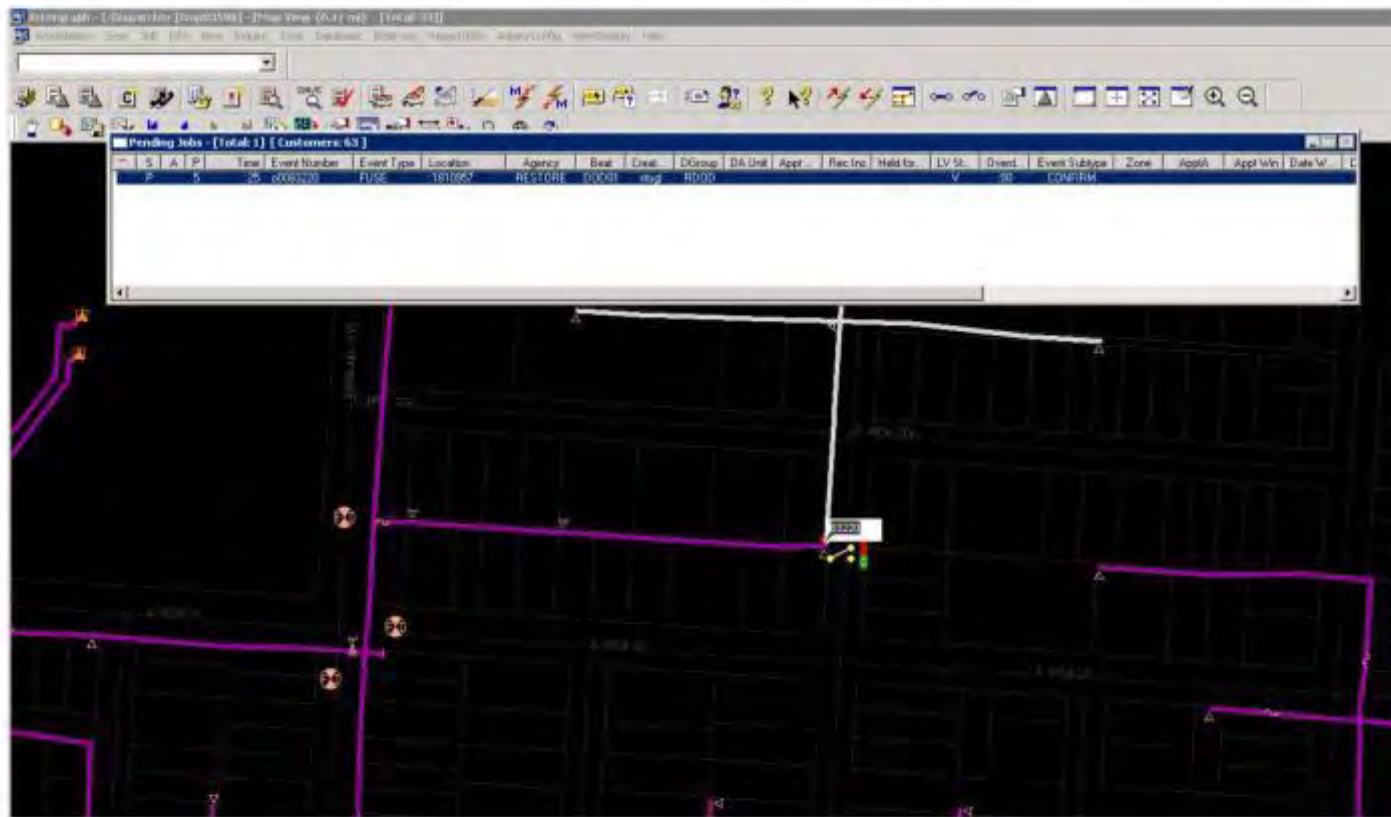
Meter Response	Response Time	Job Number	Job Status	Call Number	Request ID	Meter Number	Requested Device	Name	Location	Phone	Transformer	Unlocked	Employee ID	Event Type	Event Subtype	Request Time	Job Device	Meter Status
V	08/15/13 08:50:14	0008223	P	04596	0	1104412952973	PA...	4925	324	1224016	108			PLSE	CONFIRM		1810957	
V	08/15/13 08:20:13	0008231	P	04594	0	1104410711062	34...	4418	355	1075030	107			PLSE	CONFIRM		1810957	
V	08/15/13 08:49:42	0008233	P	04592	0	1104410711068	36...	532	386	1075030	106			PLSE	CONFIRM		1810957	
V	08/15/13 08:28:29	0008235	P	04598	0	1104412952973	04...	4925	324	1224016	108			PLSE	CONFIRM		1810957	
V	08/15/13 08:33:51	0008238	P	04595	0	1104410711063	35...	532	390	1075030	104			PLSE	CONFIRM		1810957	
X	08/15/13 08:25:18	0008223	P	04594	0	1104410711062	48...	4414	355	1075030	109			PLSE	CONFIRM		1810957	

27

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Select the Job in "Pending Jobs" to View Location on Map

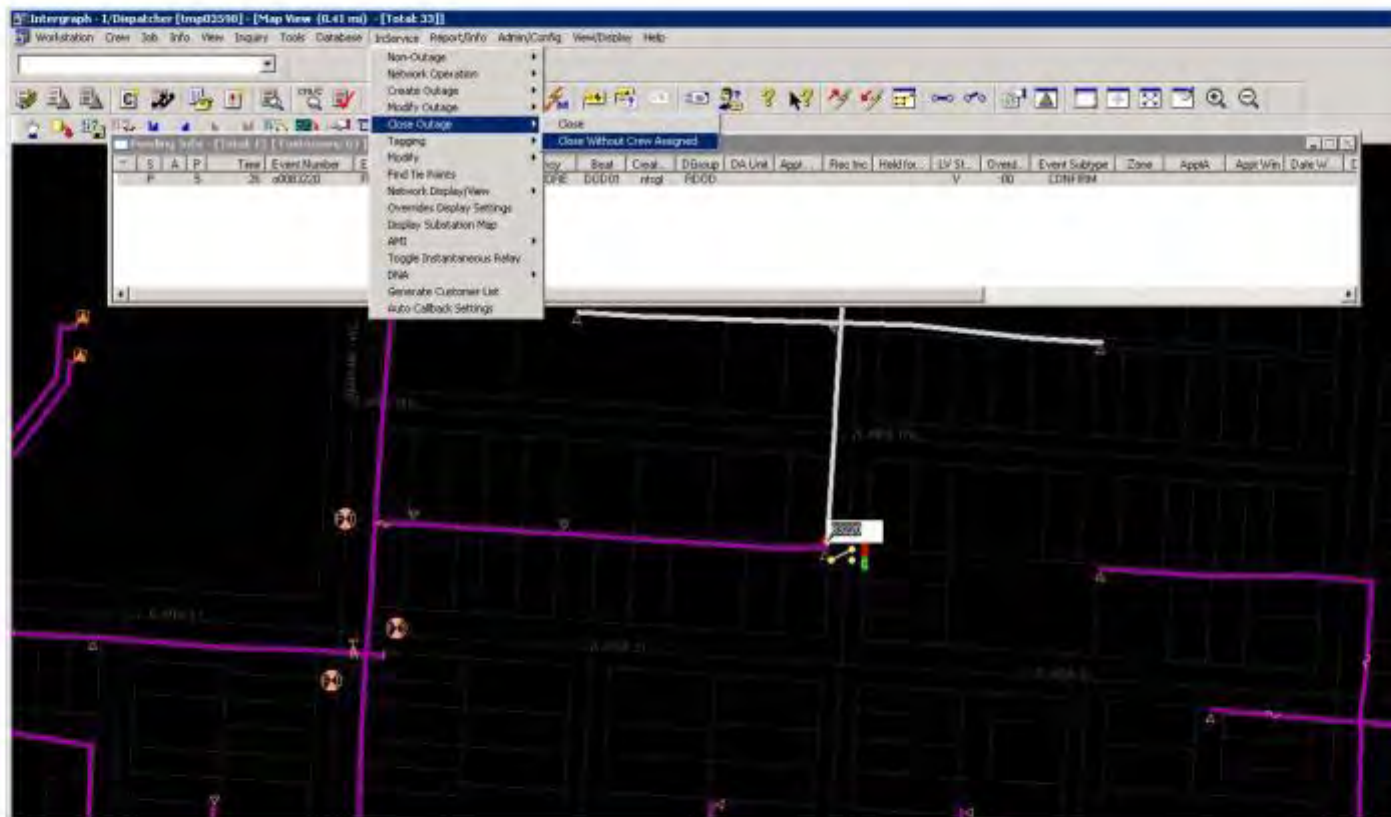


28

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Open the "Close Outage" Window

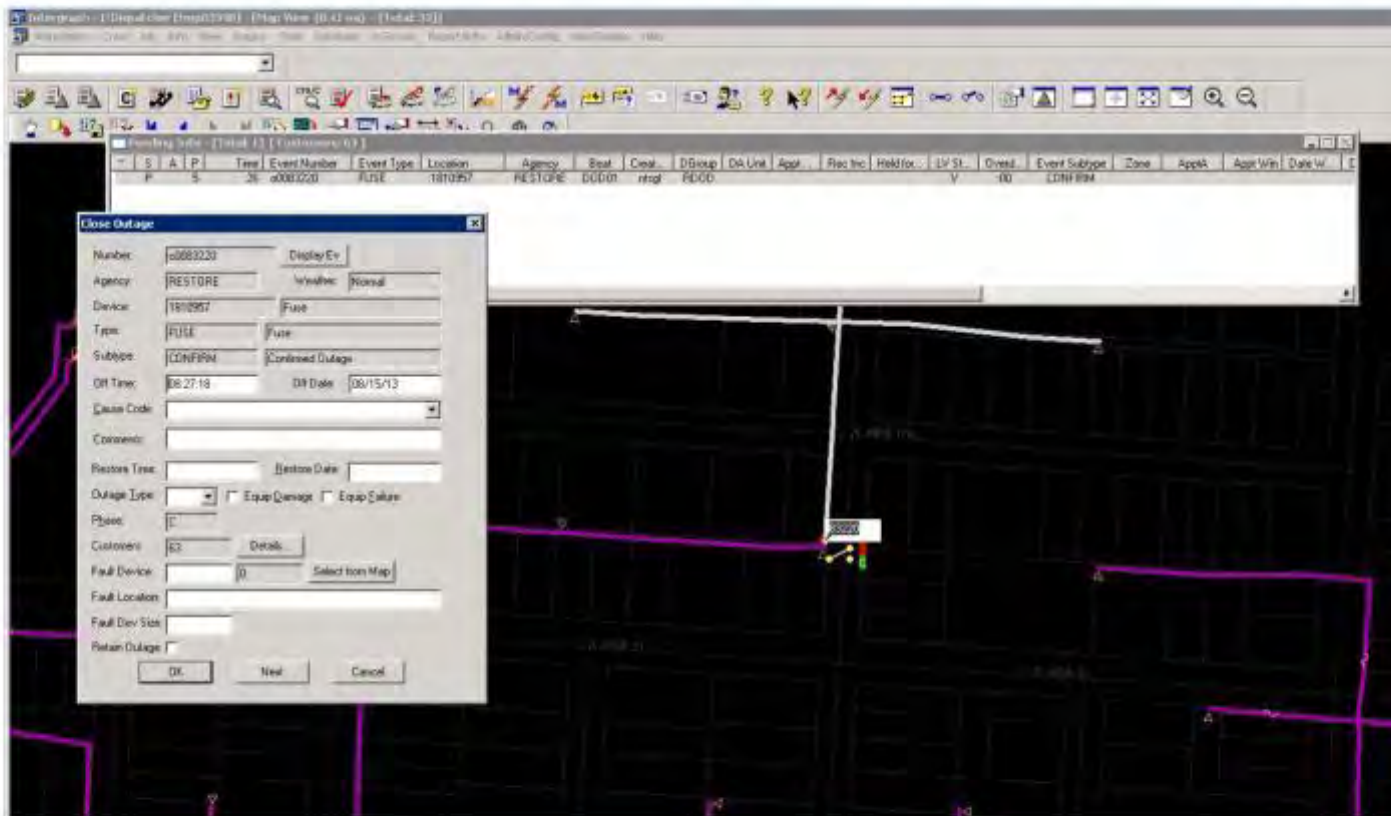


29

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Fields in "Close Outage" Window

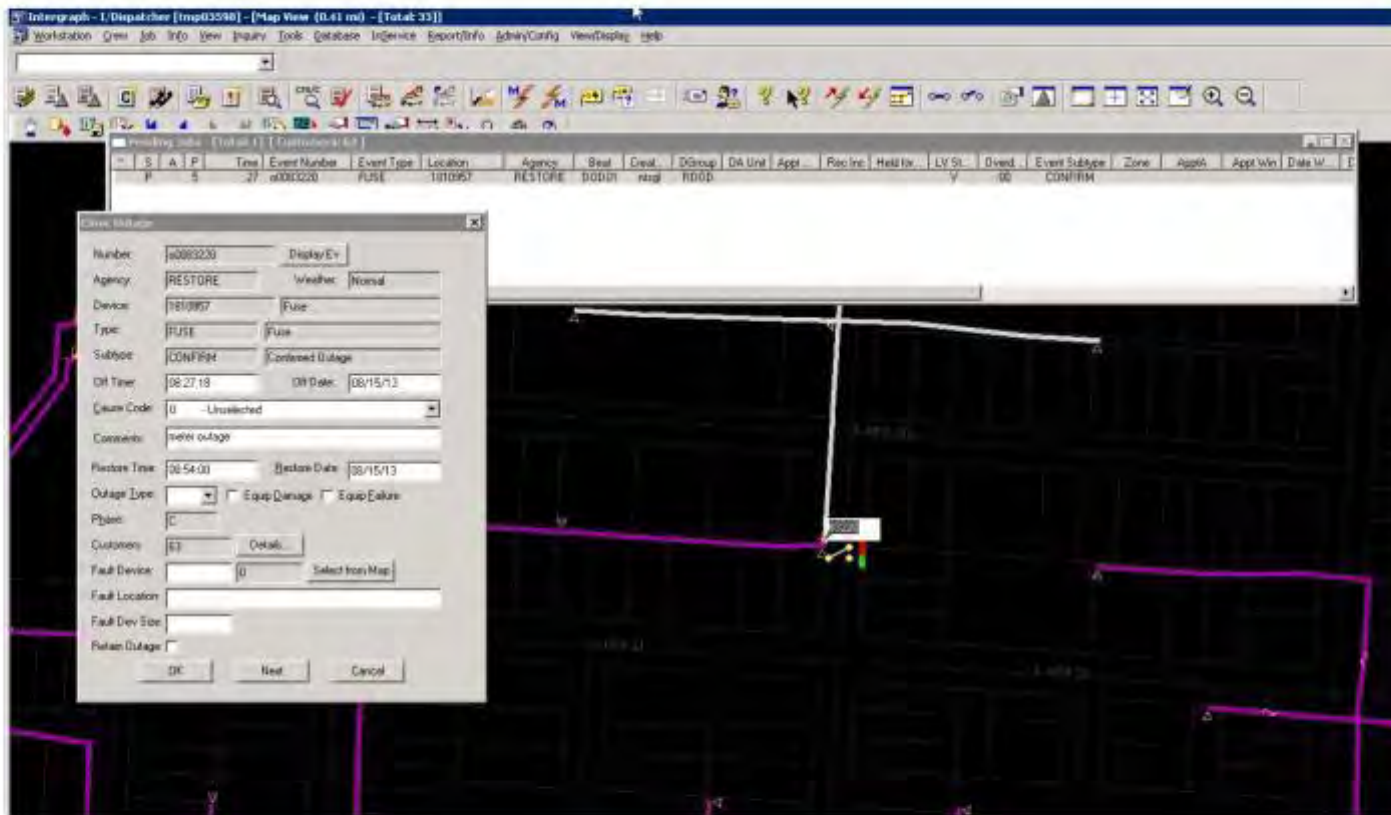


30

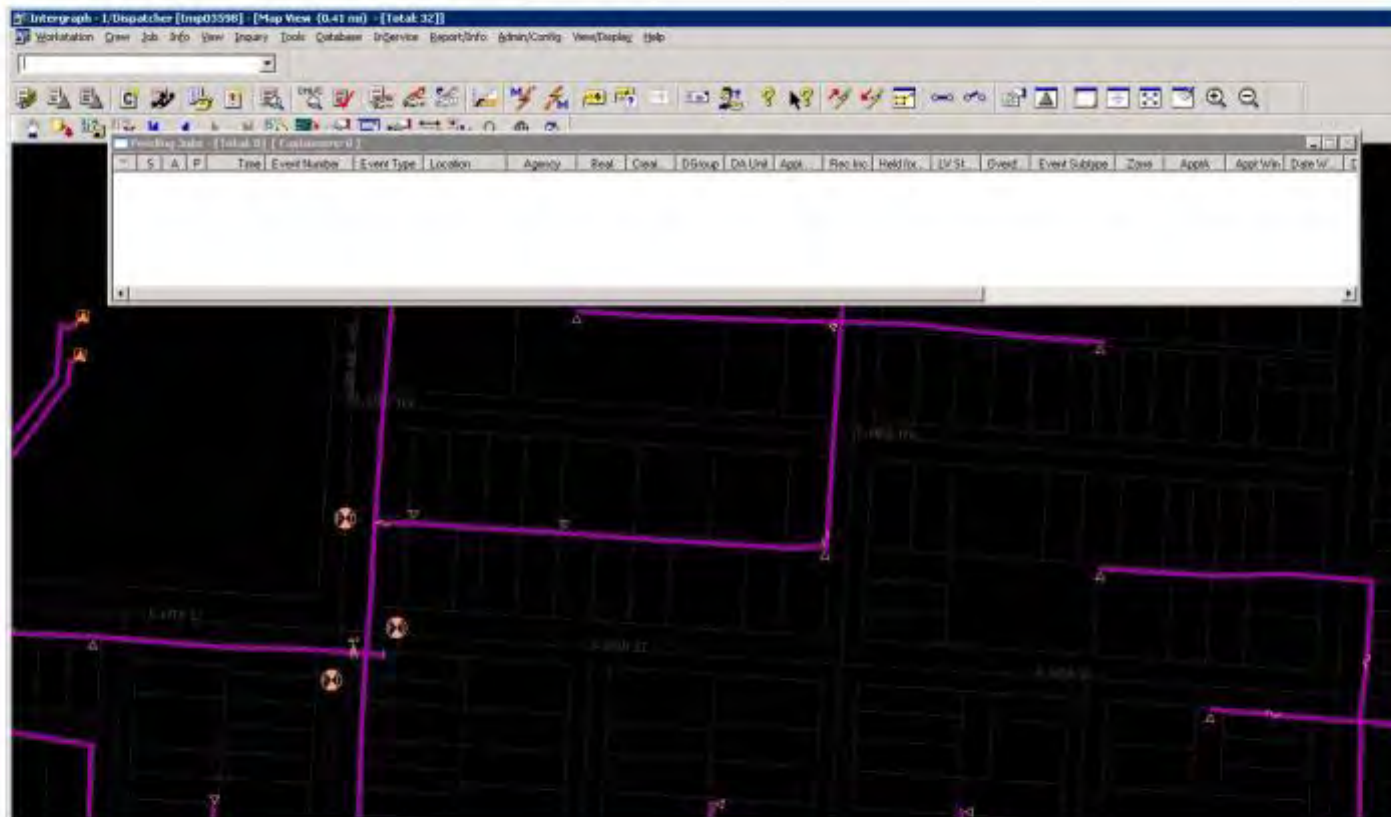
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Enter Information in "Close Outage" Window



Outage Job is Closed



■32

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

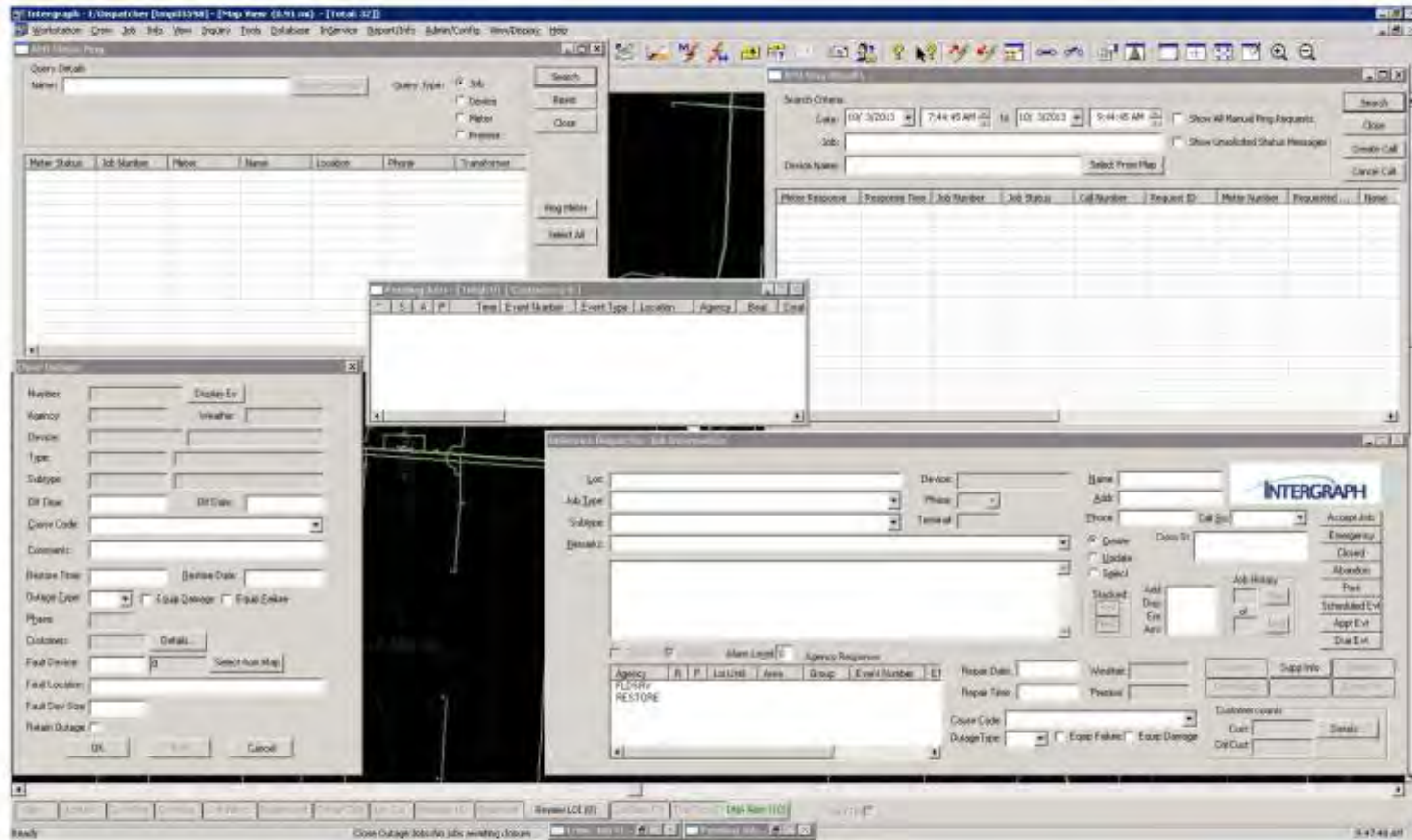


Power Status Verification

- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program



Windows Used for Power Status Verification

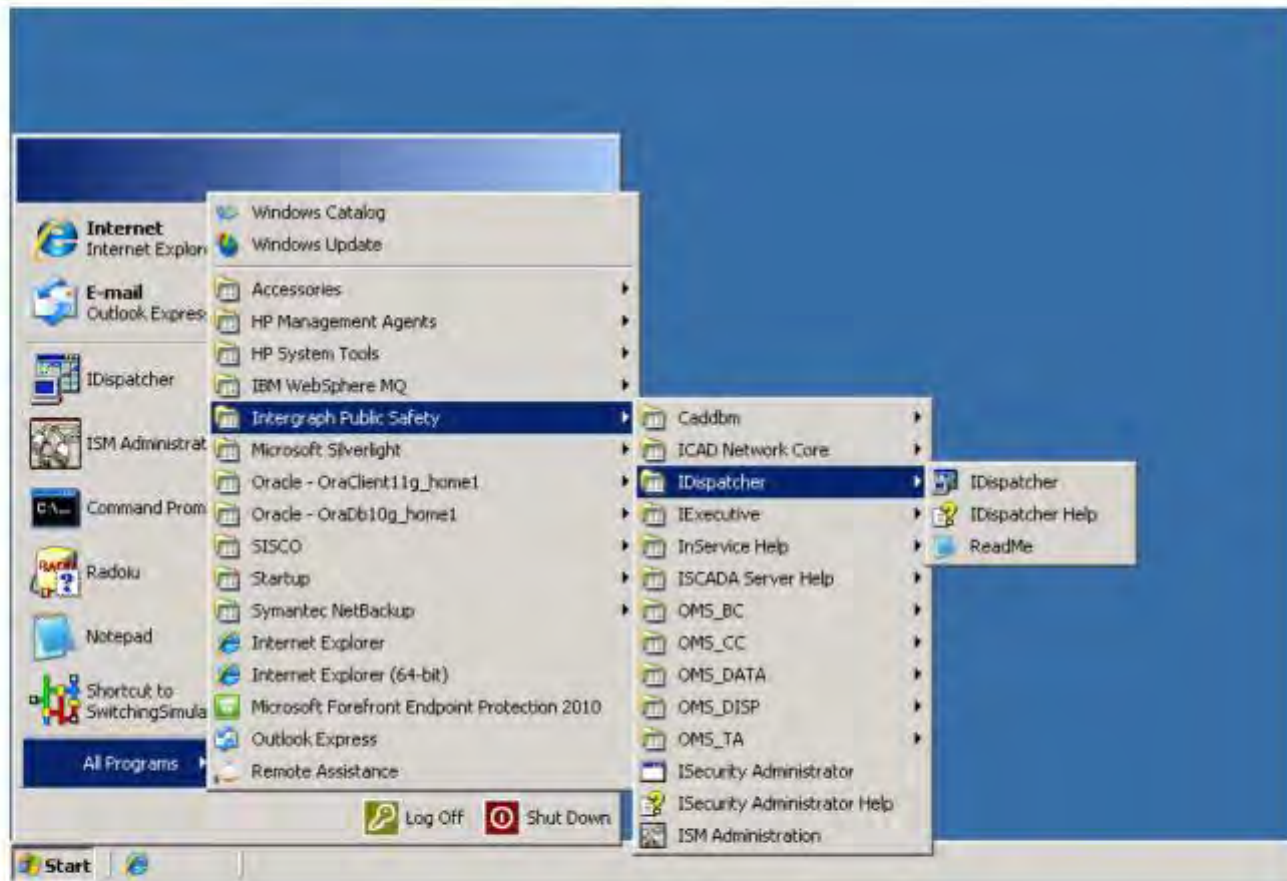


2

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Launch InService I/Dispatcher

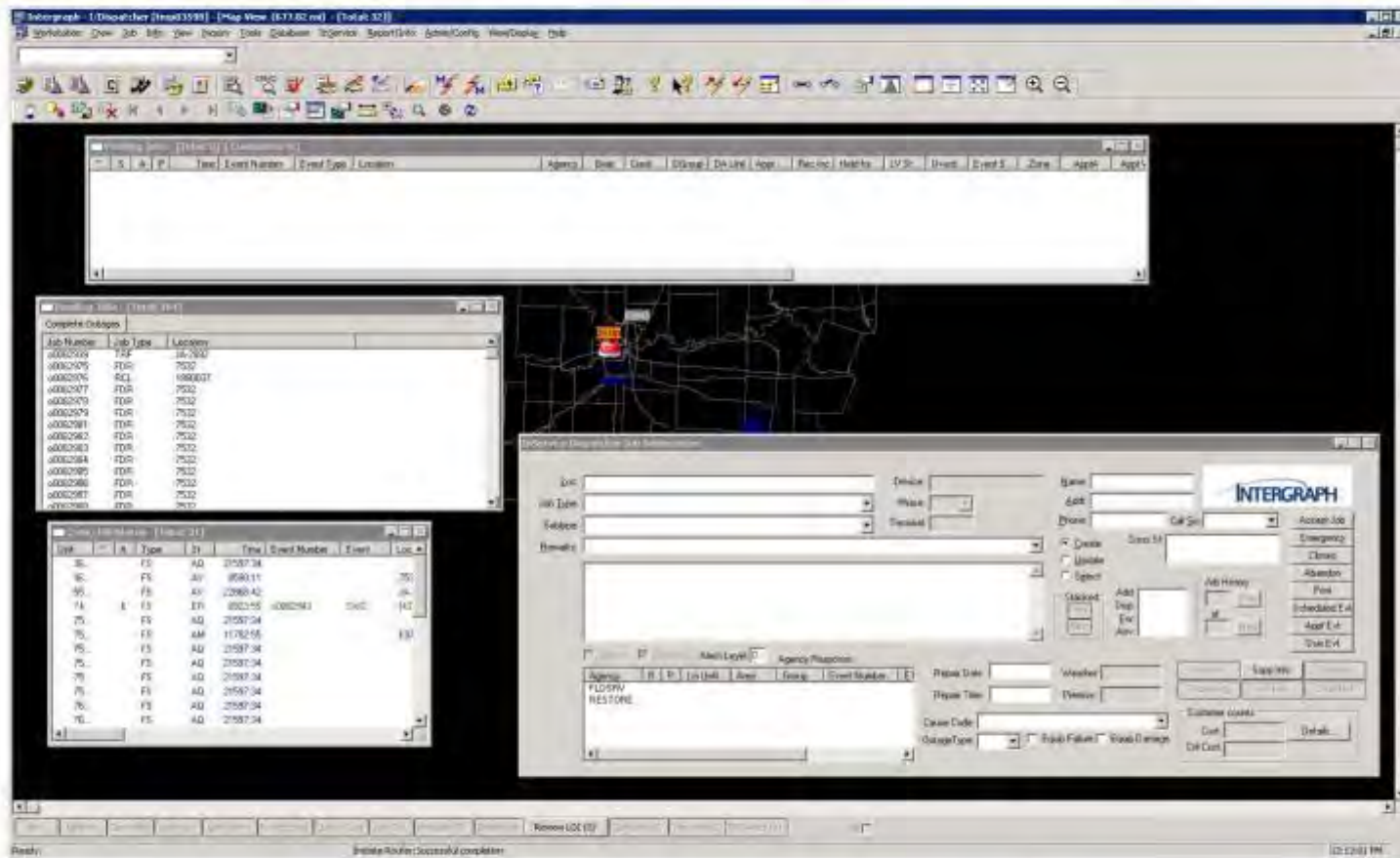


3

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



InService I/Dispatcher Main Screen

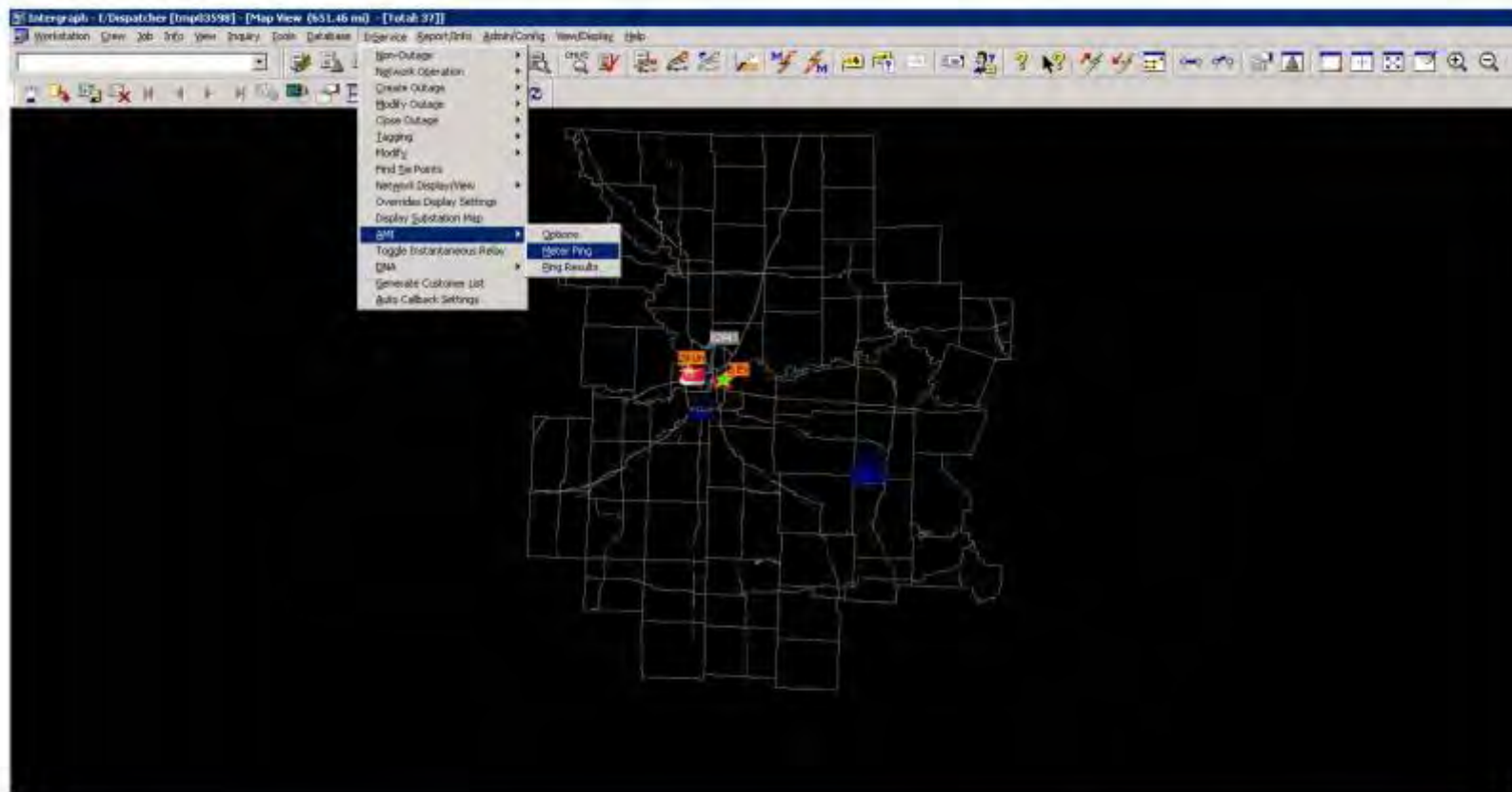


4

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Open “AMI Meter Ping” to send Power Status Verification

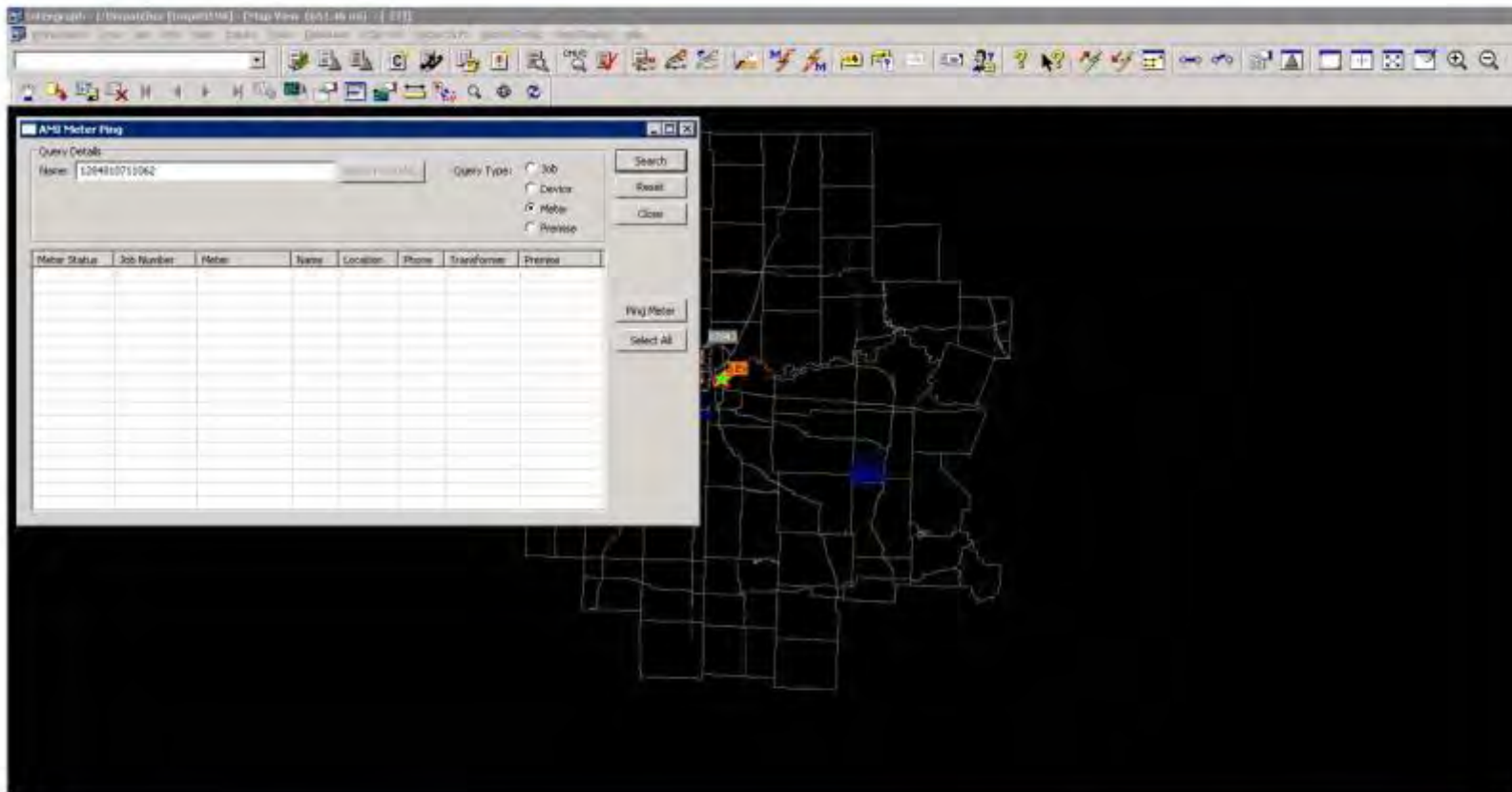


■5

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Scenario #1: Meter is "Powered On"



6

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Send Meter Ping Request

Query Details

Name: 1294810711062

Query Type: Job Device Meter Process

Meter Status	ID Number	Meter	Name	Location	Phone	Transformer	Inverse
	1294810711062	AR211...	4416	202	1079030	909463990	

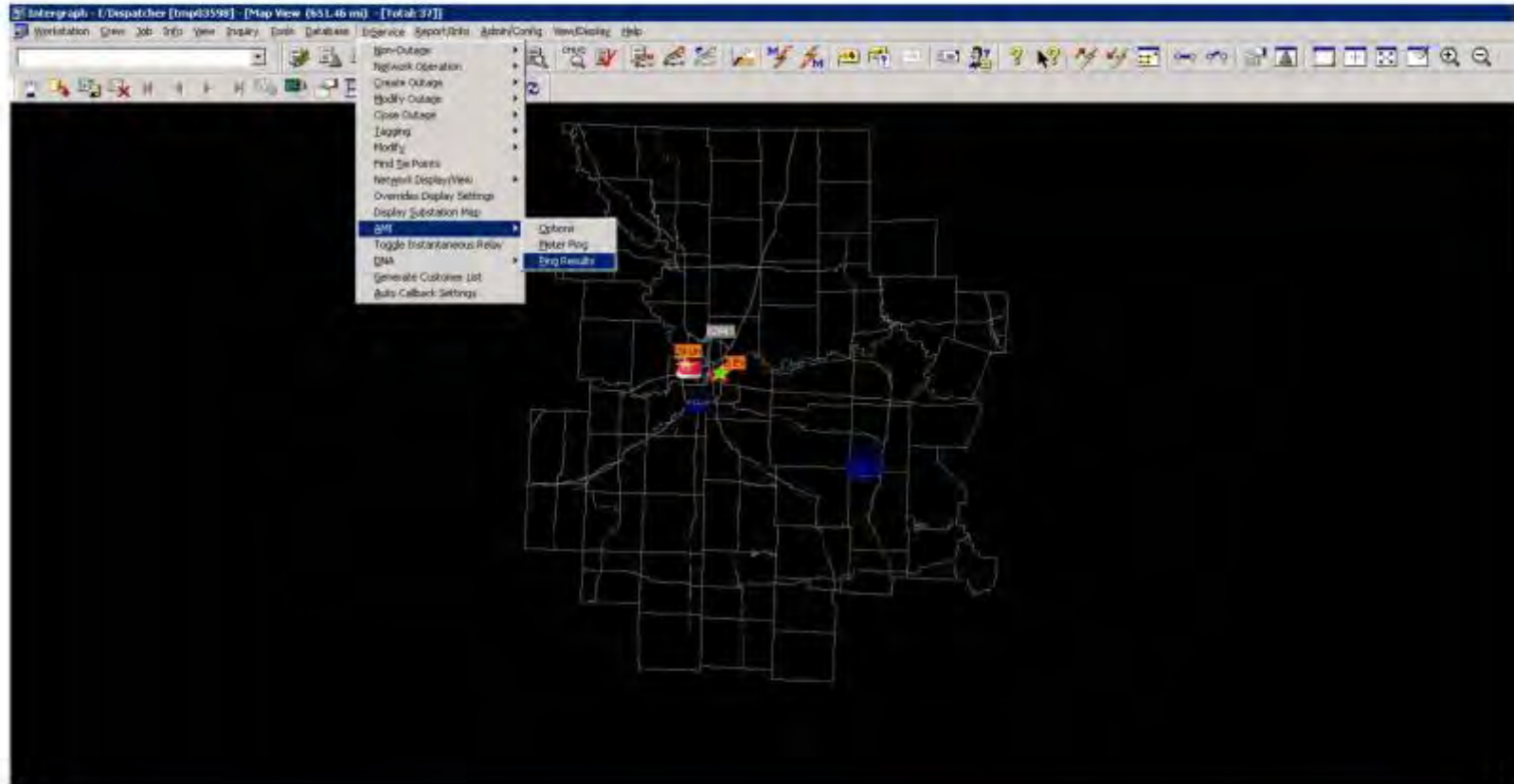
Buttons: Search, Reset, Close, Ping Meter, Select All

7

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Open AMI Ping Results



■8

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Meter Ping Request in "AMI Ping Results"

The screenshot shows a web browser window displaying the 'AMI Ping Results' interface. At the top, there is a search criteria section with the following fields and options:

- Date: 10/9/2013 to 10/9/2013
- Time: 3:15:00 PM to 5:00:00 PM
- Buttons: Search, Close, Create Call, Cancel Call
- Checkboxes: Show All Manual Ping Requests, Show Unacknowledged Status Messages
- Device Name: [Text Field] Select From Map

Below the search criteria is a table with the following columns:

Meter Response	Response Time	Job Number	Job Status	Call Number	Request ID	Meter Number	Requested Device	Type	Location	Phone	Transformer	Unacknowledged	Employee ID	Event Type	Event Subtype	Request Time	Job Device	Meter Status
SI					602	1204610711062		AM...	4116...	255...	1079330	0	3536			10/09/13 15:16:25		

9

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Received Meter Ping Response

The screenshot displays a software application window titled "AMI Ping Results". At the top, there is a search criteria section with fields for "Date" (10/9/2013 to 10/9/2013), "Time" (5:15:00 PM to 5:00:00 PM), and checkboxes for "Show All Manual Ping Requests" and "Show Unlinked Status Messages". Below the search criteria is a table with the following columns: Meter Response, Response Time, Job Number, Job Status, Call Number, Request ID, Meter Number, Requested Device, Name, Location, Phone, Transformer, Unlinked, Employee ID, Event Type, Event Subtype, Request Time, Job Device, and Meter Status. The first row of the table contains the following data: "Y" (highlighted with a red box), "10/09/13 15:16:24", "", "", "602", "1294610711062", "AB...", "4418...", "205...", "1079120", "0", "3598", "", "", "10/09/13 15:16:25", "", and "". Below the table, there is a faint map of a geographic area.

10

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Scenario #2: Meter is "Powered Off"

The screenshot shows a GIS application window titled "AMR Meter Ping". The window is divided into a left-hand data table and a right-hand map. The data table has the following columns: Meter Status, Job Number, Meter, Name, Location, Phase, Transformer, and Prebid. The table is currently empty. The map on the right shows a grid of utility lines with several colored markers (red, orange, yellow, green, blue) indicating different meter statuses or locations. The application interface includes a toolbar at the top with various GIS tools and a search box on the right side of the data table.

Send Meter Ping Request

The screenshot shows a GIS application window titled 'Send Meter Ping Request'. The main interface features a map with a grid overlay and several colored markers. A dialog box is open in the foreground, containing a search form and a table of meter data.

Query Details:
Name: 1284810711064
Query Type: Job Device Meter Process

Meter Status	Job Number	Meter	Name	Location	Phone	Transformer	Precede
		1284810711064	ROW...	1507...	901...	1079030	622329240

Buttons: Search, Reset, Close, Ping Meter, Select All

Meter Ping Request in “AMI Ping Results”

The screenshot shows a web browser window displaying a map and a data table titled "AMI Ping Results". The search criteria are set to Date: 09/ 9/2013, 3:25:00 PM to 10/ 9/2013, 5:00:00 PM. The table contains one row of data with a red box highlighting the "Meter Response" column.

Meter Response	Response Time	Job Number	Job Status	Call Number	Request ID	Meter Number	Requested Device	Name	Location	Phone	Transformer	Unolicited	Employee ID	Event Type	Event Subtype	Request Time	Job Device	Meter Status
OK				604		1204610711064		RO...	1507 ...	921 ...	1039230	0	3599			10/09/13 15:26:06		

13

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Received Meter Ping Response

The screenshot shows a software application window titled "AMI Ping Results". At the top, there is a search criteria section with fields for Date (10/9/2013), Time (3:25:00 PM), and Job ID (10/9/2013). Below this is a table with the following columns: Meter Response, Response Time, Job Number, Job Status, Call Number, Request ID, Meter Number, Requested Device, Name, Location, Phone, Transformer, Unpollled, Employee ID, Event Type, Event Subtype, Request Time, Job Device, and Meter Status. The first row of data shows a question mark in the "Meter Response" column, which is highlighted with a red box. The rest of the table is empty.

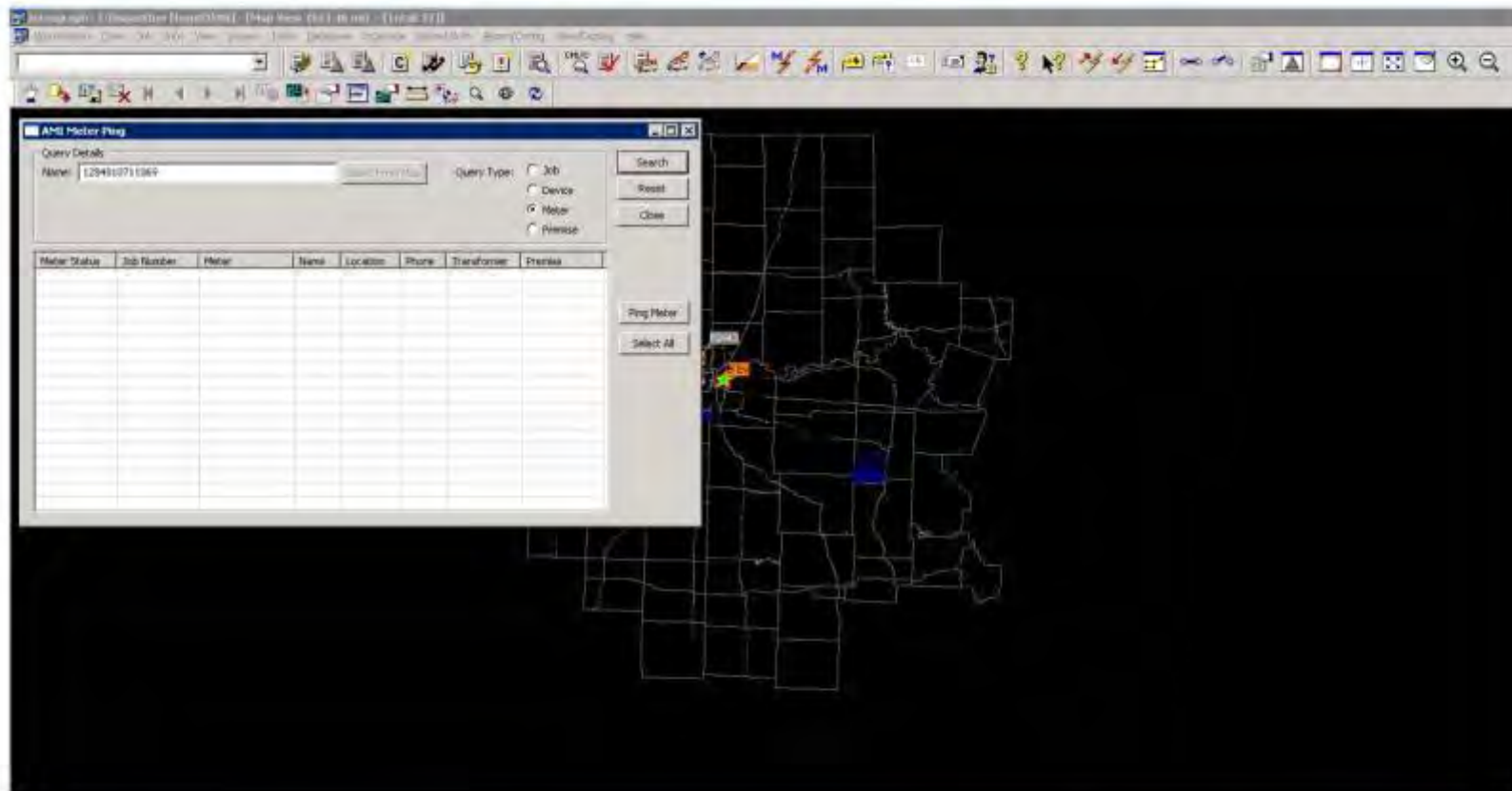
Meter Response	Response Time	Job Number	Job Status	Call Number	Request ID	Meter Number	Requested Device	Name	Location	Phone	Transformer	Unpollled	Employee ID	Event Type	Event Subtype	Request Time	Job Device	Meter Status
?	10/09/13 15:27:26				504	1294810711064		RO...	1507 ...	931 ...	1079330	0	3009			10/09/13 15:26:00		

14

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Scenario #3: Meter is “De-energized” in CIS



15

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Send Meter Ping Request

The screenshot shows a web browser window with a toolbar and a main content area. The main content area is divided into two parts: a left-hand panel and a right-hand map.

The left-hand panel, titled "AMI Meter Ping", contains a "Query Details" section with a "Name" field containing "1209410711008" and a "Query Type" section with radio buttons for "Job", "Device", "Meter" (which is selected), and "Previous". Below this is a table with the following data:

Meter Status	Job Number	Meter	Name	Location	Phone	Transformer	Preload
		1209410711008	3049 M...	5318...	1079024	200665423	

Below the table are buttons for "Ping Meter" and "Select All".

The right-hand side of the interface shows a map with a grid overlay, representing a geographic area with various colored markers.

Meter Ping Request/Response in “AMI Ping Results”

The screenshot displays a web application window titled "AMI Ping Results". At the top, there is a search criteria section with the following fields and options:

- Date: 10/ 9/2013, 3:40:00 PM to 10/ 9/2013, 5:00:00 PM
- Job: [Empty field]
- Device Name: [Empty field]
- Buttons: Search, Close, Create Call, Cancel Call
- Checkboxes: Show All Manual Ping Requests, Show Unsolicited Status Messages
- Search From Map button

Below the search criteria is a data table with the following columns:

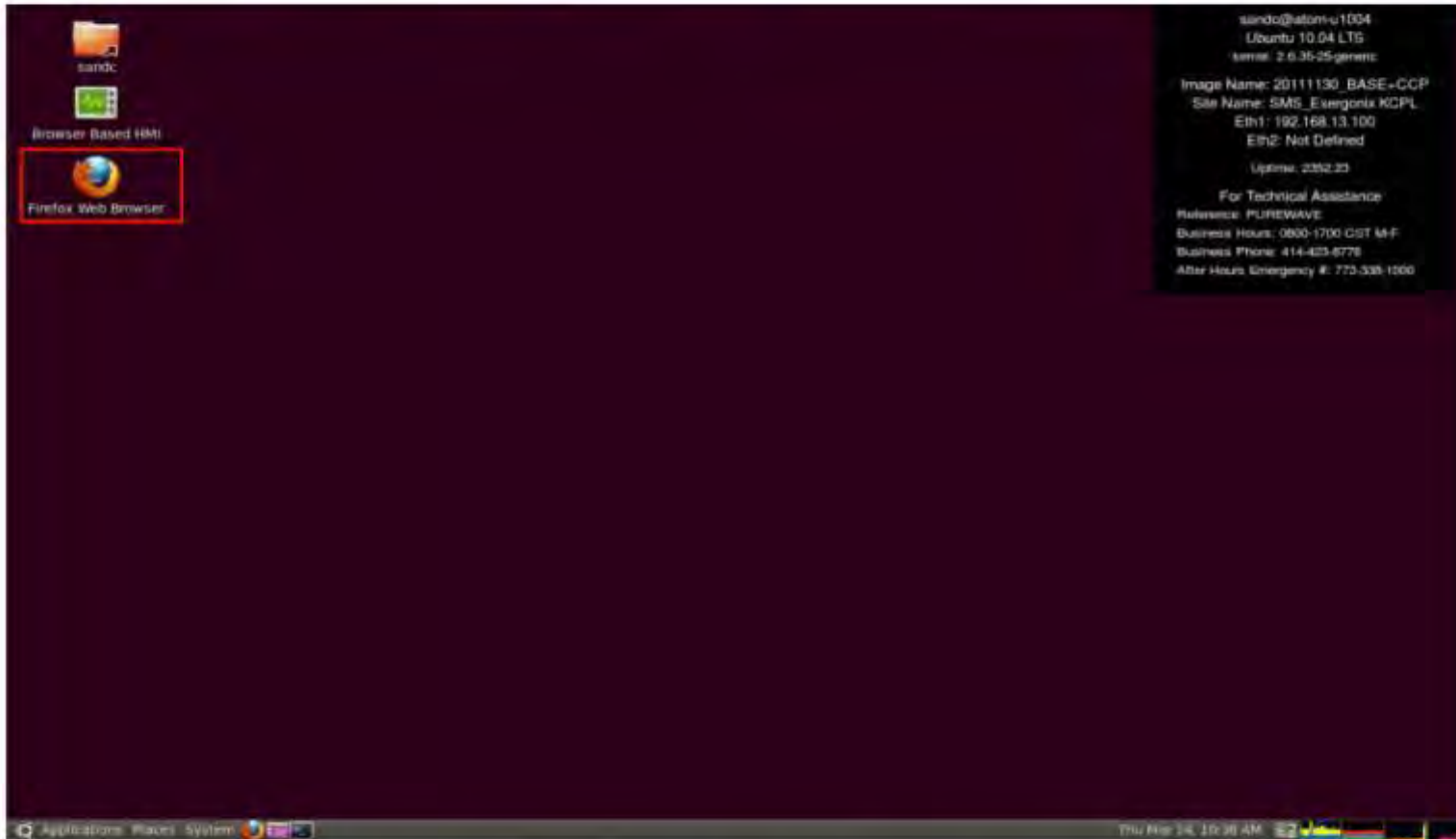
Meter Response	Response Time	Job Number	Job Status	Call Number	Request ID	Meter Number	Requested Device	Name	Location	Phone	Transformer	Unolicited	Employee ID	Event Type	Event Subtype	Request Time	Job Device	Meter Status
X	10/09/13 15:40:26			606	1204810711069				3849...	531...	1079326	0	2599			10/09/13 15:40:26		

Battery Operation: Local Control

- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program



Launch Firefox Web Browser



▪2

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



SMS System Menu Main Screen

SMS

OutputBus Currents

Ia	2.7	A
Ib	2.7	A
Ic	1.5	A

OutputBus Voltages

Vab	7920	V
Vbc	7980	V
Vca	7977	V

SMS Status

Real Power: -5 KWatt
 Reactive: 54 KVar
 System Enabled / Disabled: ENABLED
 Master / System State: READY

Data Request in 1 s, Time Stamp: 1/14/2013 1:40:07 PM

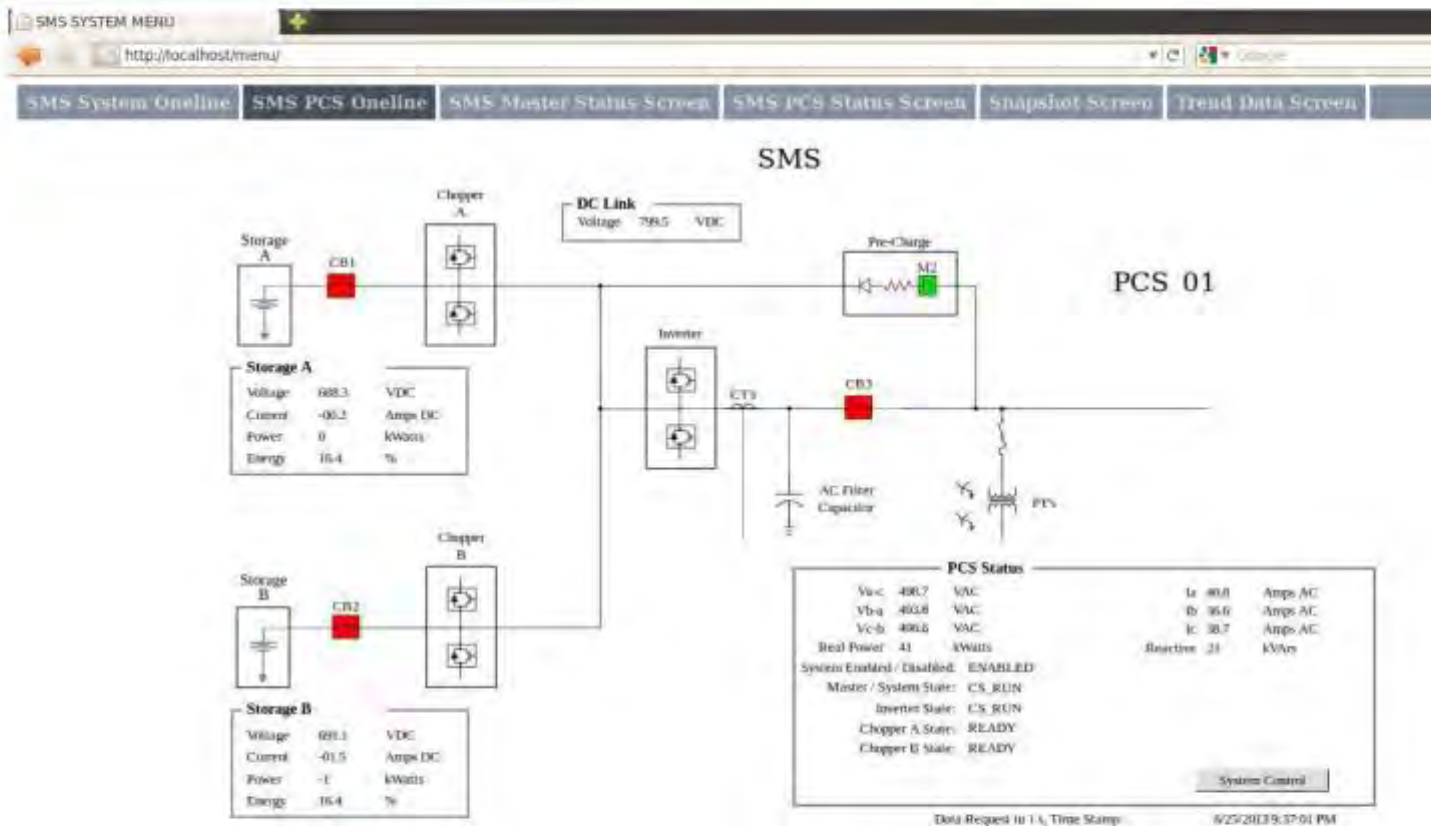
Thu Mar 14, 10:40 AM

KCP&L
energizing life

3

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

Open SMS PCS Online



4

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Launch Browser Based HMI



5

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



SMS KCPL Window is Opened



6

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Expand "System"



7

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Expand "SCADA"



Expand “NonVolatileVariables”

- SMS KCPL
- File Help
- System
 - SCADA
 - EOS-MCU
 - FirmwareVersion
 - Parameters
 - Variables
 - NonVolatileVariables**
 - ActiveSetpoints
 - HMIRequests
 - SCADARequests
 - Diagnostics
 - ScheduledPowerProfile
 - ScheduleDay
 - SchedulingErrors
 - BatteryBmsRaw
 - Controller
 - Inverter001
 - Chopper101

Expand "HMIRequests"



10

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Expand “PulsedControlBits”

The screenshot shows the SMS KCPL software interface. On the left is a tree view with the following structure:

- System
 - SCADA
 - EOS-MCU
 - FirmwareVersion
 - Parameters
 - Variables
 - NonVolatileVariables
 - ActiveSetpoints
 - HMIRequests
 - Setpoints
 - PulsedControlBits** (highlighted with a red box)
 - LatchedControlBits
 - SCADARequests
 - Diagnostics
 - ScheduledPowerProfile
 - ScheduleDay
 - SchedulingErrors
 - BatteryBmsRaw
 - Controller
 - Inverter001

On the right is a table with the following header:

Name	Value	Units	Min	Max	Scale	Offset
------	-------	-------	-----	-----	-------	--------

11

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Click on "bit"

The screenshot shows the SMS KCPL software interface. On the left is a tree view of the system structure. On the right is a table of system variables.

Name	Value	Units	Min	Max	Scale	Offset
all	00000000000000000000000000000000					
ResetRequest	0		0	1	1	0
EnableRequest	0		0	1	1	8
DisableRequest	0		0	1	1	9
IncrementVoltageRequest	0		0	1	1	10
DecrementVoltageRequest	0		0	1	1	11
RealPowerFromSetpoint	0		0	1	1	16
RealPowerFromSchedule	0		0	1	1	17
RemoveSystemInhibit	0		0	1	1	22
InhibitSystem	0		0	1	1	23
StartVSMModeRequest	0		0	1	1	24
StopVSMModeRequest	0		0	1	1	25
ReactivePowerFromSetpointRequest	0		0	1	1	26
ReactivePowerFromVoltageRegRequest	0		0	1	1	27
SyncToSource1Request	0		0	1	1	29



Set RealPowerFromSetpoint Value to 1

The screenshot shows a SCADA software window titled 'SMS KCPL' with a menu bar (File, Help) and a toolbar. On the left is a tree view of the system hierarchy, including SCADA, EOS-MCU, Parameters, Variables, and ActiveSetpoints. The 'ActiveSetpoints' folder is expanded, showing a list of variables. The main pane displays a table with the following data:

Name	Value	Units	Min	Max	Scale	Offset
all	00000000000000000000000000000000					
ResetRequest	0		0	1	1	0
EnableRequest	0		0	1	1	8
DisableRequest	0		0	1	1	9
IncrementVoltageRequest	0		0	1	1	10
DecrementVoltageRequest	0		0	1	1	11
RealPowerFromSetpoint	1		0	1	1	16
RealPowerFromSchedule	0		0	1	1	17
RemoveSystemInhibit	0		0	1	1	22
InhibitSystem	0		0	1	1	23
StartVSMODERequest	0		0	1	1	24
StopVSMODERequest	0		0	1	1	25
ReactivePowerFromSetpointRequest	0		0	1	1	26
ReactivePowerFromVoltageRegRequest	0		0	1	1	27
SyncToSource1Request	0		0	1	1	29

13

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Confirm the Changes

The screenshot shows a software window titled 'SMS SYSTEM MENU - M...' with a menu bar containing 'File' and 'Help'. On the left is a tree view of system components, including SCADA, EOS-MCU, Parameters, Variables, and various requests. The main area displays a table of parameters:

Name	Value	Units	Min	Max	Scale	Offset
all	00000000000000000000000000000000					
ResetRequest	0		0	1	1	0
EnableRequest	0		0	1	1	8
DisableRequest	0		0	1	1	9
IncrementVoltageRequest	0		0	1	1	10
DecrementVoltageRequest	0		0	1	1	11
RealPowerFromSetpoint	1		0	1	1	16
RealPowerFromSchedule	0		0	1	1	17
RemoveSystemInhibit			0	1	1	22
InhibitSystem			0	1	1	23
StartVSMODERequest			0	1	1	24
StopVSMODERequest			0	1	1	25
ReactivePowerFromSetp			0	1	1	26
ReactivePowerFromVoltageRequest	0		0	1	1	27
SyncToSource1Request	0		0	1	1	29

A 'Confirm Edit' dialog box is centered over the table, with 'Ok' and 'Cancel' buttons.

Expand “LatchedControlBits”

The screenshot shows a software interface for 'SMS KCPL'. On the left is a tree view with the following structure:

- System
 - SCADA
 - EOS-MCU
 - FirmwareVersion
 - Parameters
 - Variables
 - NonVolatileVariables
 - ActiveSetpoints
 - HMIRequests
 - Setpoints
 - PulsedControlBits
 - bit
 - LatchedControlBits** (highlighted with a red box)
 - bit
 - SCADARequests
 - Diagnostics
 - ScheduledPowerProfile
 - ScheduleDay
 - SchedulingErrors
 - BatteryBmsRaw
 - Controller
 - Inverter001
 - Chopper101

On the right is a table with the following headers: Name, Value, Units, Min, Max, Scale, Offset. The table is currently empty.

Go to HMIRequests > Setpoints

The screenshot shows the HMI interface for SMS KCP&L. The left sidebar contains a tree view with 'HMIRequests' and 'Setpoints' highlighted. The main window displays a table of system variables.

Name	Value	Units	Min	Max	Scale	Offset
RealPower	0.000	1.0 p.u. = SMS-Rated-RealPower (+Discharge, -Charge)	-3.403E+38	3.403E+38	1.000	0.000
ScheduledPower	0.000	1.0 p.u. = SMS-Rated-RealPower (+Discharge, -Charge)	-3.403E+38	3.403E+38	1.000	0.000
ReactivePower	0.000	1.0 p.u. = SMS-Rated-ReactivePower (+Cap, -Ind)	-3.403E+38	3.403E+38	1.000	0.000
Voltage	1.000	1.0 p.u. = Nominal	-3.403E+38	3.403E+38	1.000	0.000
VoltageDelta	0.001	1.0 p.u. = Nominal	-3.403E+38	3.403E+38	1.000	0.000
MaxSoc	100.0	%	-3.403E+38	3.403E+38	1.000	0.000
MinSocCs	20.0	%	-3.403E+38	3.403E+38	1.000	0.000
MinSocVs	1.0	%	-3.403E+38	3.403E+38	1.000	0.000

Set the Discharge Value in RealPower Value

The screenshot shows the 'SMS SYSTEM MENU' application window. On the left is a tree view of system components, with 'Setpoints' expanded. The main window displays a table of system variables. The 'RealPower' variable is highlighted with a red box, showing a value of 5. The table columns are Name, Value, Units, Min, Max, Scale, and Offset.

Name	Value	Units	Min	Max	Scale	Offset
RealPower	5	1.0 p.u. = SMS-Rated-RealPower (+Discharge, -Charge)	-3.403E+38	3.403E+38	1.000	0.000
ScheduledPower	0.000	1.0 p.u. = SMS-Rated-RealPower (+Discharge, -Charge)	-3.403E+38	3.403E+38	1.000	0.000
ReactivePower	0.000	1.0 p.u. = SMS-Rated-ReactivePower (+Cap., -Ind.)	-3.403E+38	3.403E+38	1.000	0.000
Voltage	1.000	1.0 p.u. = Nominal	-3.403E+38	3.403E+38	1.000	0.000
VoltageDelta	0.001	1.0 p.u. = Nominal	-3.403E+38	3.403E+38	1.000	0.000
MaxSoC	100.0	%	-3.403E+38	3.403E+38	1.000	0.000
MinSoC/s	20.0	%	-3.403E+38	3.403E+38	1.000	0.000
MinSoC/v	1.0	%	-3.403E+38	3.403E+38	1.000	0.000

18

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



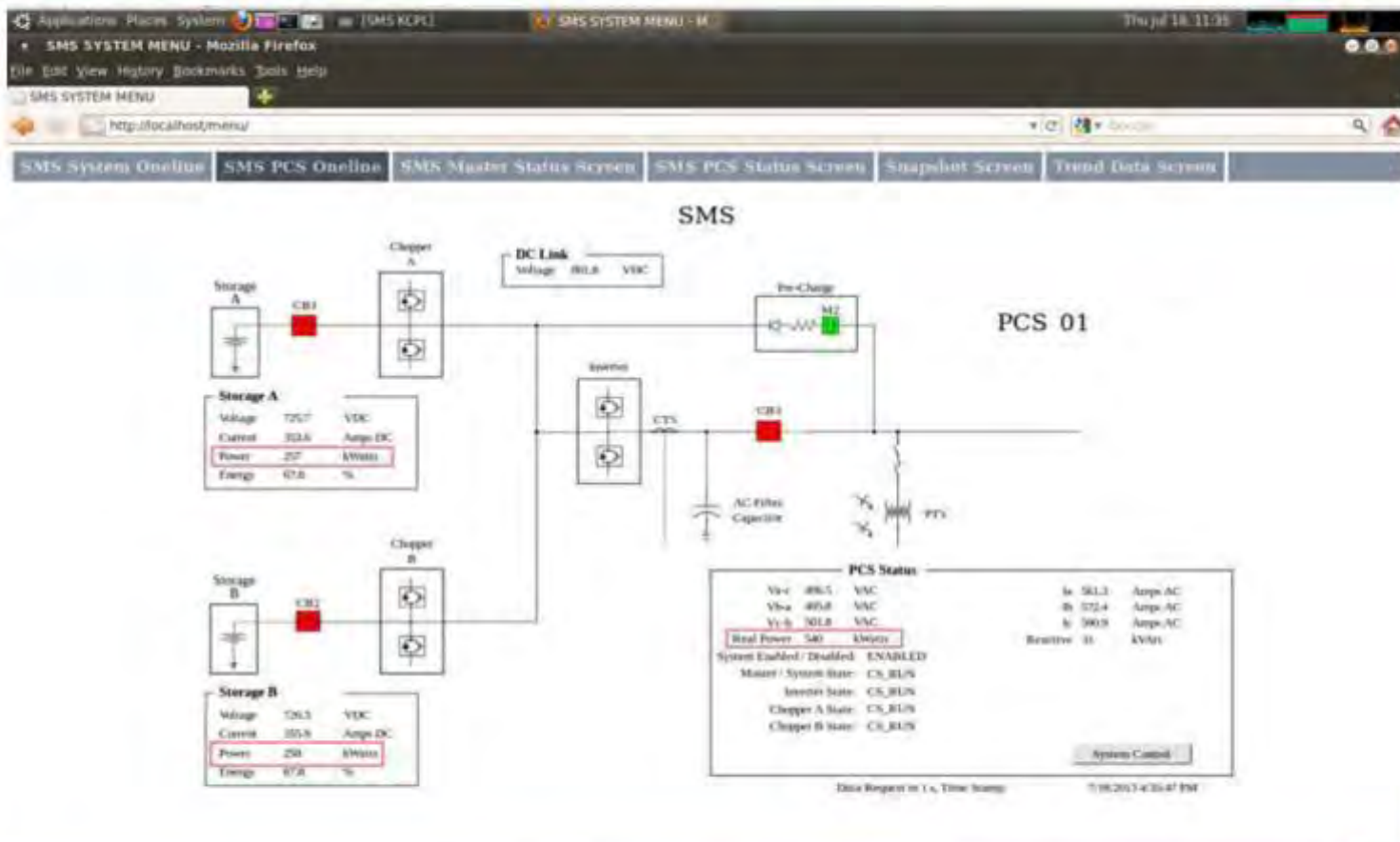
Confirm the Changes

The screenshot shows the 'SMS SYSTEM MENU' application window. On the left is a tree view of the system hierarchy, including SCADA, EOS MCU, Parameters, Variables, NonvolatileVariables, ActiveSetpoints, HMRequests, Setpoints, PulsedControlBits, LatchedControlBits, SCADARequests, Diagnostics, ScheduledPowerProfile, ScheduledDay, SchedulingErrors, BatteryBmsKw, Controller, Inverter001, and Chopper101. The main area displays a table of parameters:

Name	Value	Units	Min	Max	Scale	Offset
RealPower	5	1.0 p.u. = SMS-Rated-RealPower (+Discharge, -Charge)	-3.403E+38	3.403E+38	1.000	0.000
ScheduledRealPower	0.000	1.0 p.u. = SMS-Rated-RealPower (+Discharge, -Charge)	-3.403E+38	3.403E+38	1.000	0.000
ReactivePower	0.000	1.0 p.u. = SMS-Rated-ReactivePower (+Cap., -Ind.)	-3.403E+38	3.403E+38	1.000	0.000
Voltage	1.000	1.0 p.u. = Nominal	-3.403E+38	3.403E+38	1.000	0.000
VoltageDelta	0.001	1.0 p.u. = Nominal	-3.403E+38	3.403E+38	1.000	0.000
MaxSoC	100.0	%	-3.403E+38	3.403E+38	1.000	0.000
MinSoC/s	20.0	%	-3.403E+38	3.403E+38	1.000	0.000
MinSoC/v	1.0	%	-3.403E+38	3.403E+38	1.000	0.000

A 'Confirm Edit' dialog box is overlaid on the table, with 'Ok' and 'Cancel' buttons.

Navigate to SMS PCS Online to view Battery Discharging



20

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

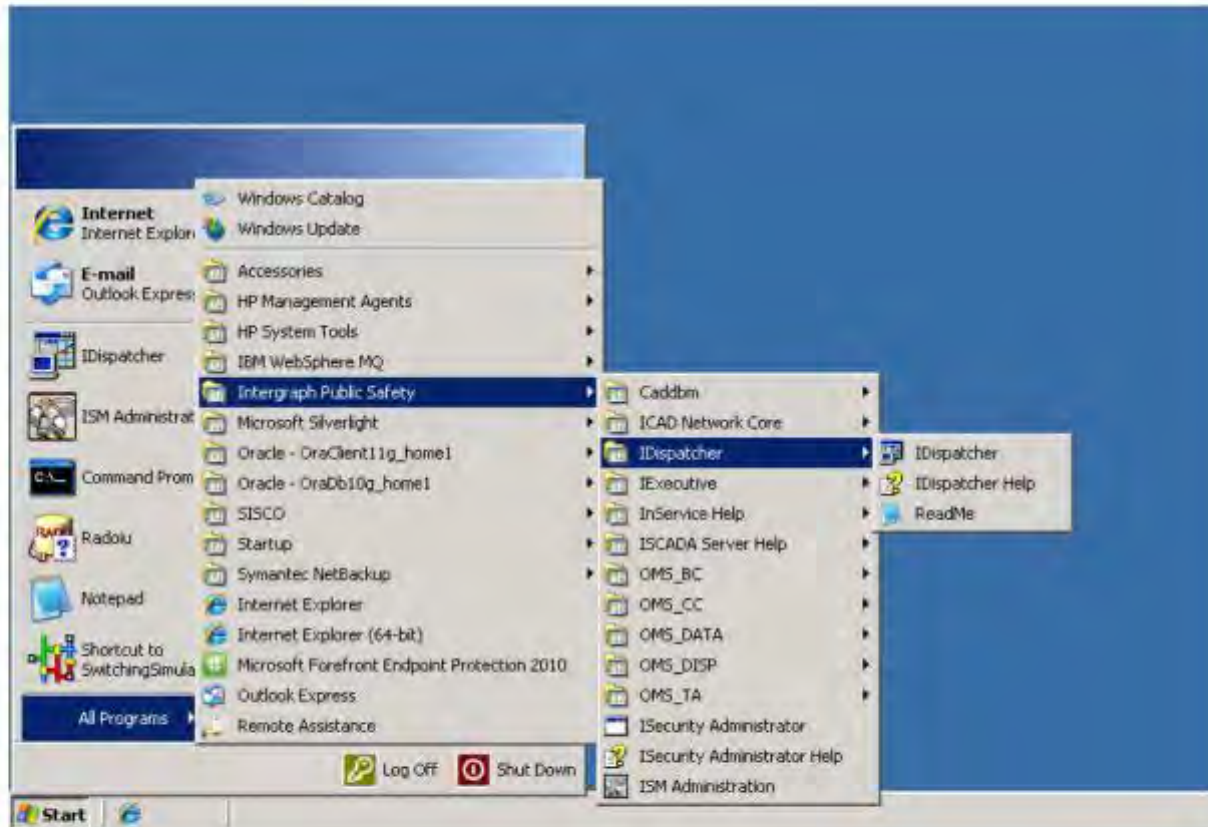


Battery Operation: Fixed kW Discharge

- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program



Launch InService I/Dispatcher



2

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Feature Information: Battery

Workstation Crew Job Info View Inquiry Tools Database InService Report/Info Admin/Config View/Display Help

Feature Information
Device: 1888105 Refresh

Name	Value
Active State	Normal
Active Status	OFF
Alarm - Inhibit	OK
Alarm - Isolate	OK
Alarm - Trip Offline	OK
Alarm - Warning	Alarm
BESS Status	Enabled
Charge Mode	OFF
Energy Available (%)	69
Local - Remote	Local
Power Mode	OFF
Reactive Mode	Fixed KVAR
Recalculation Time (sec)	0
SCADA Device Comm Failure	OK
Schedule Override Status	Disabled
KVAR - Discharge Duration (min)	5
KVAR - Discharge Start Time (0-23)	13
KVAR - Fixed PF (%)	0
KVAR - Max Discharge Rate	125
KW - Charge Duration (min)	0
KW - Charge Following	0
KW - Charge Start Time (0-23)	0
KW - Discharge Duration (min)	5
KW - Discharge Start Time (0-23)	0
KW - Load Following	0
KW - Max Charge Rate	0
KW - Max Discharge Rate	100

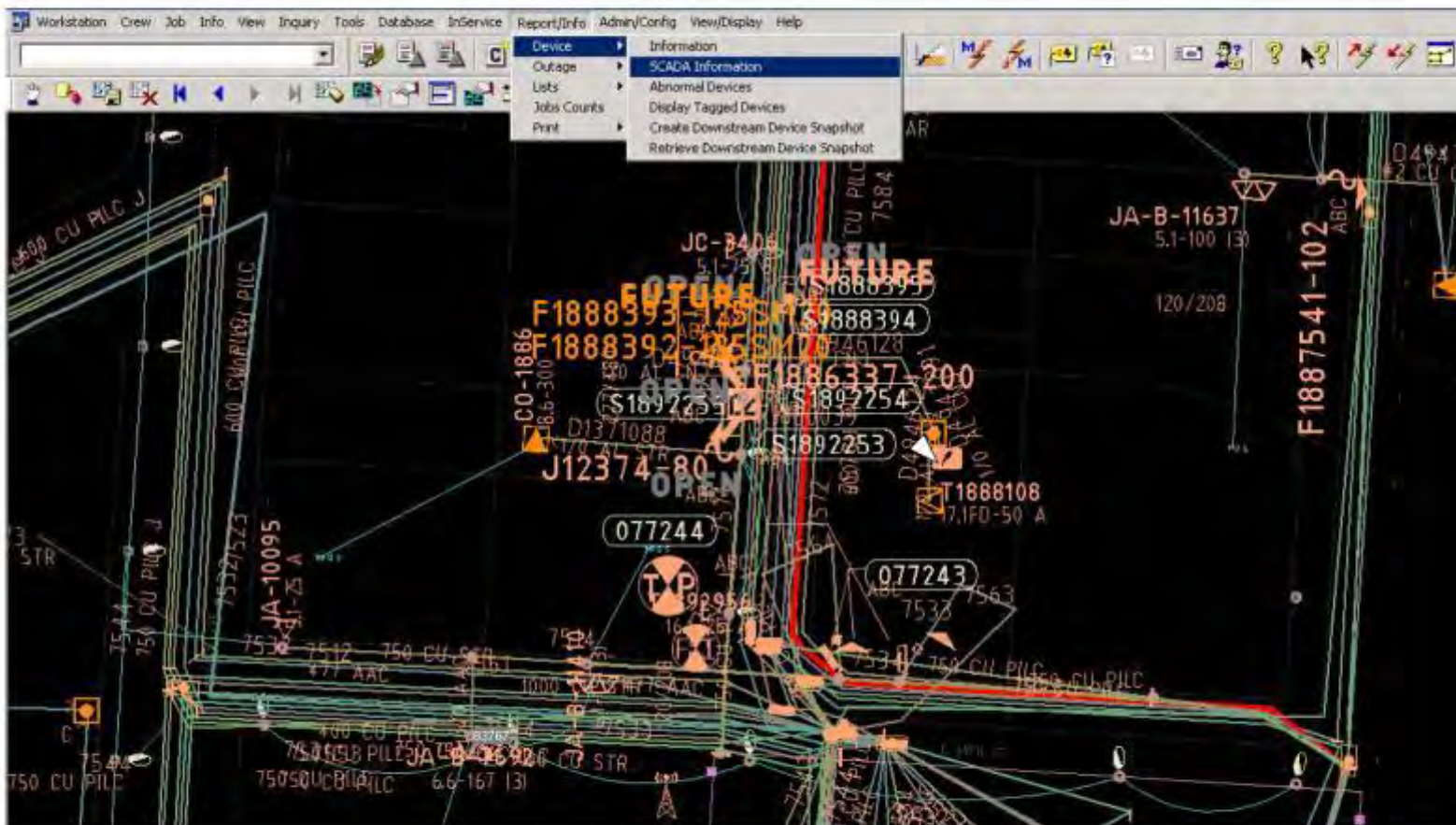
Right Click to Control SCADA points

4

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Launch "SCADA Device Information"

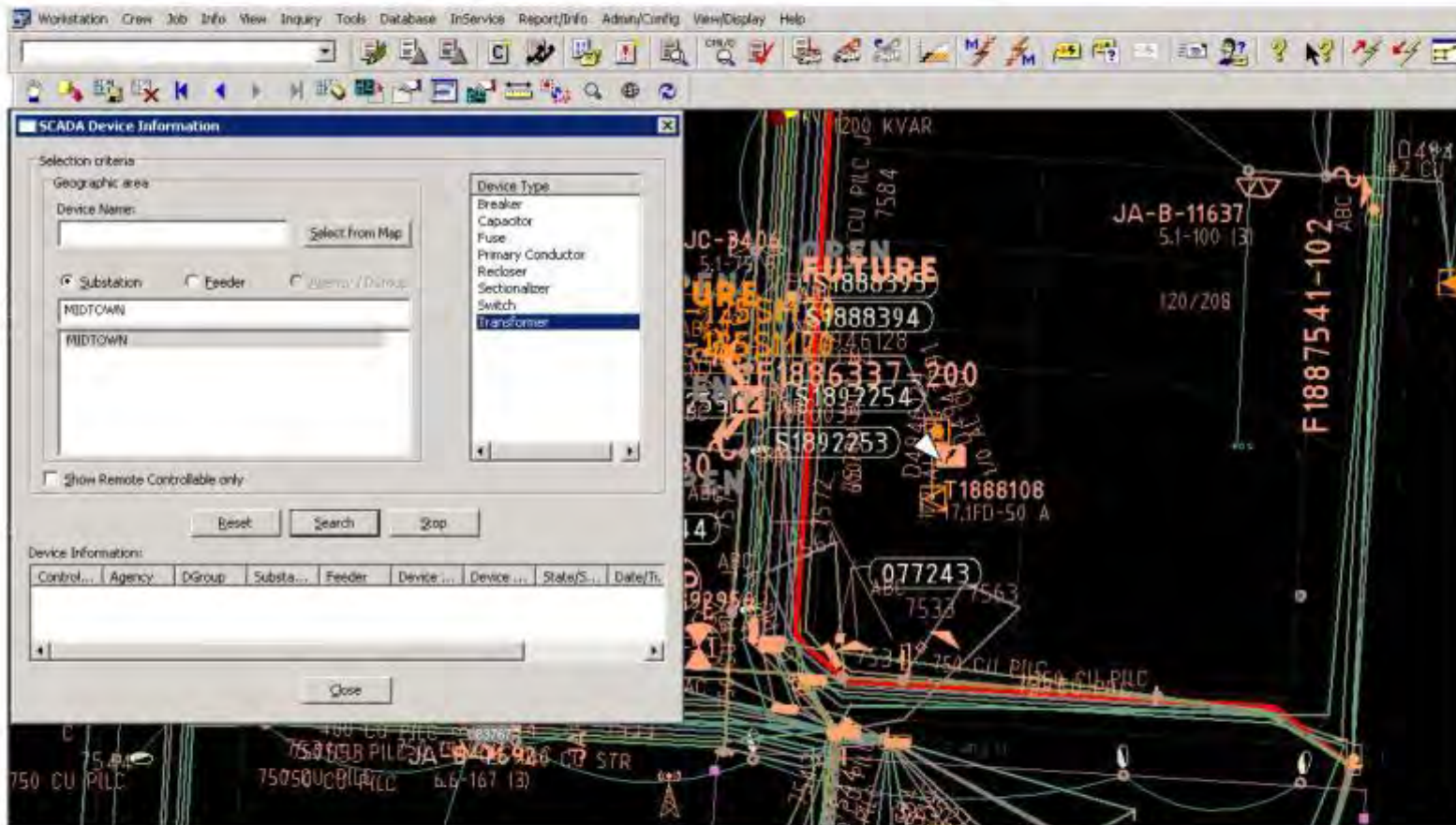


5

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



SCADA Device Information Window



6

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Battery in Device Information

The screenshot displays the SCADA Device Information interface. On the left, a search window titled "SCADA Device Information" is open. It includes a "Selection criteria" section with a "Device Name" field containing "1888105" and a "Select from Map" button. Below this are radio buttons for "Substation", "Feeder", and "Battery (0/0/0/0)". A list box shows "MIDTOWN" selected. A "Device Type" list on the right includes Breaker, Capacitor, Fuse, Primary Conductor, Reducer, Sectionalizer, Switch, and Transformer. At the bottom of the search window is a "Device Information" table with one row of data.

Control...	Agency	DGroup	Substa...	Feeder	Device Type	Device ...	State/S...	Date
Y	FLDSRV	FLDSV	MIDTOWN	7564	Transformer	1888105		

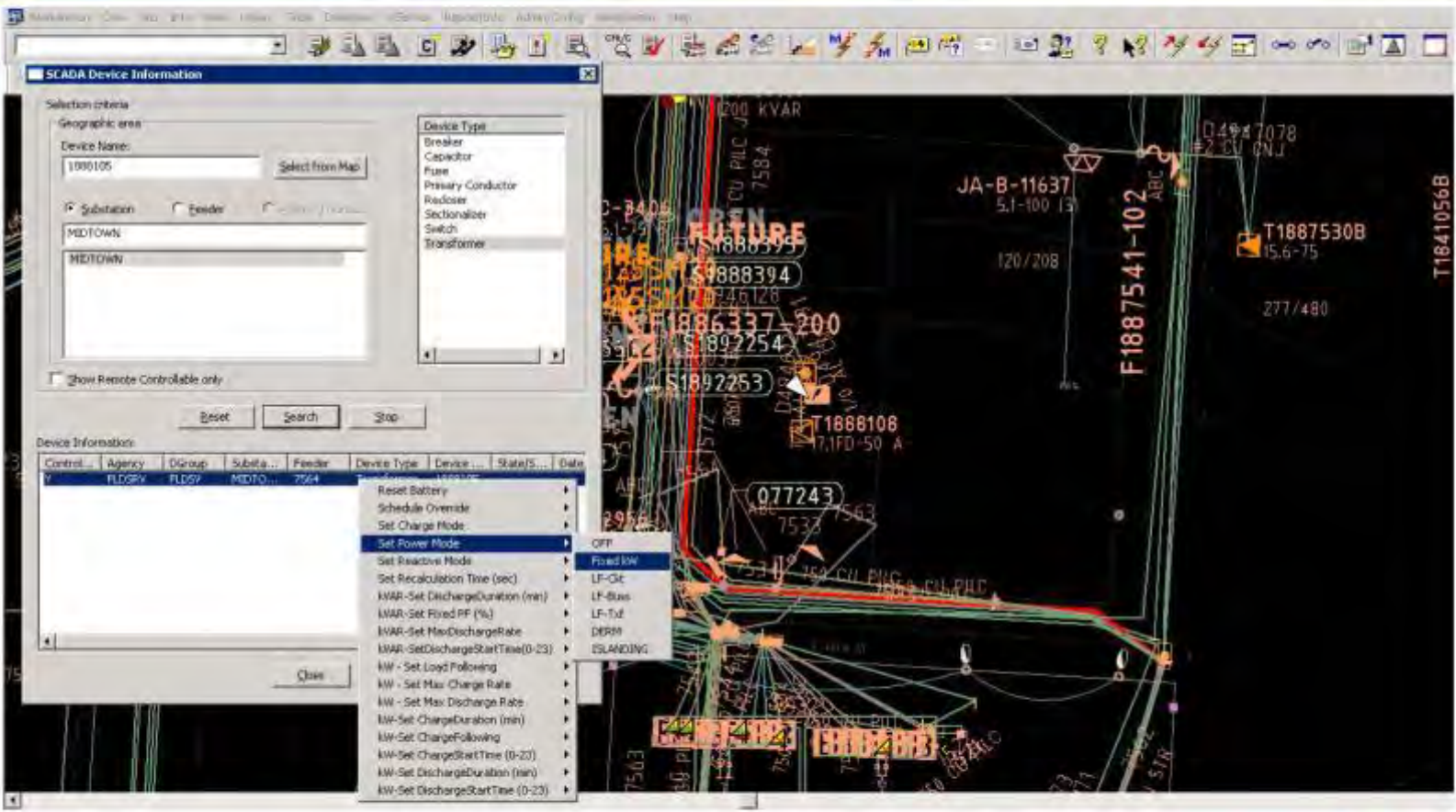
The background of the software shows a network diagram with various components labeled, including "200 KVAR", "JA-B-11637 5.1-100 13", "F1887541-102 ABC", "T1888108 7,IFD-50 A", and "077243 ABC 7533 7563".

7

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Set Battery to Fixed kW Mode



8

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Battery set to Fixed kW Power Mode

The screenshot displays a SCADA software interface. On the left, a 'Feature Information' window is open for device '1888108'. The window has tabs for 'Attributes', 'Counts', 'SCADA', and 'DNA'. The 'Attributes' tab is active, showing a list of parameters and their values. The 'Power Mode' is set to 'Fixed kW'. The main area of the interface shows a complex network diagram with various nodes, lines, and labels such as 'F1888393', 'S1892254', and 'T1888108'. The diagram is overlaid with semi-transparent text including 'FUTURE', 'OPEN', and 'TIP'.

Name	Value
Active State	Ready
Active Status	Unknown
Alarm - Inhibit	OK
Alarm - Isolate	OK
Alarm - Trip Offline	OK
Alarm - Warning	OK
BESS Status	Enabled
Charge Mode	OFF
Energy Available (%)	98
Local - Remote	Remote
Power Mode	FIXED kW
Reactive Mode	OFF
Recalculation Time (sec)	0
SICAM Device Comm Failure	OK
Schedule Override Status	Disabled
KVAR - Discharge Duration (min)	0
KVAR - Discharge Start Time (0-23)	0
KVAR - Fixed PF (%)	0
KVAR - Max Discharge Rate	0
kW - Charge Duration (min)	0
kW - Charge Following	0
kW - Charge Start Time (0-23)	0
kW - Discharge Duration (min)	0
kW - Discharge Start Time (0-23)	0
kW - Load Following	0
kW - Max Charge Rate	0
kW - Max Discharge Rate	0

9

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Set kW Discharge Start Time

The screenshot shows a SCADA interface with a 'SCADA Device Information' dialog box. The dialog has a 'Selection criteria' section with fields for 'Device Name' (1888105), 'Substation' (MIDTOWN), and 'Feeder' (MIDTOWN). A 'Device Type' list on the right includes Breaker, Capacitor, Fuse, Primary Conductor, Reducer, Sectionalizer, Switch, and Transformer. Below this is a 'Device Information' table with columns for Control, Agency, DGroup, Substa..., Feeder, Device Type, Device..., State..., and Date. A context menu is open over the table, listing various device settings. The selected item is 'kW-Set DischargeStartTime (0-23)', with '<Enter Value>' at the bottom. The background shows a network diagram with various components like '700 KVAR', 'JA-B-11637', 'F1887541-102', and 'T18875308'.

10

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Enter Time for Battery to Start Discharging

Selection criteria:

Geographic area:

Device Name: 1888105 [select from Map]

Substation Feeder Export / Import

MIDTOWN

MIDTOWN

Device Type:

- Breaker
- Capacitor
- Fuse
- Primary Conductor
- Redozer
- Sectionalizer
- Switch
- Transformer

Enter Value

Value: []

Show Remote Controllable only

Device Information:

Control...	Agency	Dgroup	Substa...	Feeder	Device Type	Device ...	State/S...	Date
Y	FLDSRV	FLOSV	MIDTO...	7564	Transformer	1888105		

11

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Set kW Discharge Duration

The screenshot displays the SCADA Device Information window for a device named '1008105'. The window is divided into several sections:

- Selection criteria:** Includes fields for 'Device Name' (1008105), 'Substation' (MDTOWN), and 'Feeder' (MDTOWN).
- Device Type:** A list of device types including Breaker, Capacitor, Fuse, Primary Conductor, Rectifier, Sectionalizer, Switch, and Transformer.
- Device Information Table:** A table with columns for Control, Agency, DGroup, Substa..., Feeder, Device Type, Device..., State/S..., and Date.
- Parameter List:** A list of parameters for the selected device. The parameter 'kW-Set DischargeDuration (min)' is highlighted, and a context menu is open with 'Enter Value' selected.

The background shows a network diagram with various devices and connections, including labels like 'F1887541-102', 'T1887530B', and 'T1888108'.

12

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Enter Duration of Battery Discharging

The screenshot displays a software application window titled "KCP&L Green Impact Zone SmartGrid Demonstration". The main interface is a network diagram with various components labeled, including transformers (T1888108, T1887530B, T1841056B), feeders (F1886337-200, F1887541-102), and other equipment (JA-B-11637, S1888394, S1888395, S1887754, S1892253, 077243, 7532, 7533, 7534, 7535, 7536, 7537, 7538, 7539, 7540, 7541, 7542, 7543, 7544, 7545, 7546, 7547, 7548, 7549, 7550, 7551, 7552, 7553, 7554, 7555, 7556, 7557, 7558, 7559, 7560, 7561, 7562, 7563, 7564, 7565, 7566, 7567, 7568, 7569, 7570, 7571, 7572, 7573, 7574, 7575, 7576, 7577, 7578, 7579, 7580, 7581, 7582, 7583, 7584, 7585, 7586, 7587, 7588, 7589, 7590, 7591, 7592, 7593, 7594, 7595, 7596, 7597, 7598, 7599, 7600). A dialog box titled "Selection criteria" is open, showing "Device Name: 1888105", "Substation: MIDTOWN", and "Device Type: Transformer". An "Enter Value" dialog box is also open, with a "Value:" field. The background network diagram shows a complex web of connections between these components.

13

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Set kW Maximum Discharge Rate

The screenshot shows a SCADA interface with a 'SCADA Device Information' window open. The window has a 'Selection criteria' section with fields for 'Geographic area', 'Device Name', 'Substation', and 'Feeder'. Below this is a 'Device Type' list including Breaker, Capacitor, Fuse, Primary Conductor, Reducer, Sectionalizer, Switch, and Transformer. A 'Device Information' table is visible at the bottom of the window. A context menu is open over the table, listing various control actions. The 'kW - Set Max Discharge Rate' option is highlighted, and a small input box with the text '<Enter Value>' is visible next to it.

Control...	Agency	DGroup	Substa...	Feeder	Device Type	Device...	State/S...	Date
7	FLSRY	FLSRY	MIDTOW...	7064	Reset Battery			

14

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Enter Battery Discharge Rate

The screenshot shows a software application window titled "KCP&L Green Impact Zone SmartGrid Demonstration". The main window displays a network diagram with various components labeled, including "F1886337-200", "T1888108", "F1887541-102", and "T1887530B". A dialog box titled "Selection criteria" is open, showing "Device Name: 1888105", "Substation: MIDTOWN", and "Device Type: Transformer". An "Enter Value" dialog box is also open, with a "Value:" field. Below the dialog boxes is a table with the following data:

Control...	Agency	Dgroup	Substa...	Feeder	Device Type	Device ...	State/S...	Date
Y	FLDSRV	FLOSV	MIDTO...	7564	Transformer	1888105		

15

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Battery Ready to Discharge

The screenshot displays a SCADA software interface. On the left, a 'Feature Information' window is open for device 'L888176'. The 'Attributes' tab is selected, showing a list of parameters and their values. Three values are highlighted with red boxes: 'Active State' (Ready), 'Power Mode' (FIXED KW), and 'KW - Discharge Duration (min)' (5). The main area shows a complex network diagram with various nodes and connections, including labels like 'F1888393', 'S1892253', and 'T1888108'. The interface includes a menu bar at the top with options like 'Workstation', 'Crew', 'Job', 'Info', 'View', 'Inquiry', 'Tools', 'Database', 'In/Service', 'Report/Info', 'Admin/Config', 'View/Display', and 'Help'. A toolbar with various icons is located below the menu bar.

Name	Value
Active State	Ready
Active Status	Unknown
Alarm - Inhibit	OK
Alarm - Isolate	OK
Alarm - Trip Offline	OK
Alarm - Warning	OK
BESS Status	Enabled
Charge Mode	OFF
Energy Available (%)	95
Local - Remote	0
Power Mode	FIXED KW
Reactive Mode	0
Recalculation Time (sec)	0
SICAM Device Comm Failure	OK
Schedule Override Status	Disabled
KVAR - Discharge Duration (min)	0
KVAR - Discharge Start Time (0-23)	0
KVAR - Fixed PF (%)	0
KVAR - Max Discharge Rate	0
KW - Charge Duration (min)	0
KW - Charge Following	0
KW - Charge Start Time (0-23)	0
KW - Discharge Duration (min)	5
KW - Discharge Start Time (0-23)	16
KW - Load Following	0
KW - Max Charge Rate	0
KW - Max Discharge Rate	800

16

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Battery Started to Discharge

The screenshot displays a SCADA software interface. A 'Feature Information' window is open, showing details for device '1888108'. The 'Event(s) Pending' field is highlighted with a red box. The background shows a complex network diagram with various nodes and connections.

Name	Value
Active State	Event(s) Pending
Active Status	OK
Alarms - Inhibit	OK
Alarms - Isolate	OK
Alarms - Trip Offline	OK
Alarms - Warning	OK
BESS Status	Enabled
Charge Mode	OFF
Energy Available (%)	95
Local - Remote	Remote
Power Mode	FIXED kW
Reactive Mode	OFF
Recalculation Time (sec)	0
SCADA Device Comms Failure	OK
Schedule Override Status	Disabled
KVAR - Discharge Duration (min)	0
KVAR - Discharge Start Time (0-23)	0
KVAR - Fixed PF (%)	0
KVAR - Max Discharge Rate	0
kW - Charge Duration (min)	0
kW - Charge Following	0
kW - Charge Start Time (0-23)	0
kW - Discharge Duration (min)	5
kW - Discharge Start Time (0-23)	16
kW - Load Following	0
kW - Max Charge Rate	0
kW - Max Discharge Rate	800

17

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Launch Browser Based HMI

▪18 This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

SMS System Menu Main Screen

SMS

A:	2.7	A
B:	2.7	A
C:	1.5	A

V _{A-B} :	7920	V
V _{B-C} :	7980	V
V _{C-A} :	7977	V

SMS Status

Real Power: -5 KWatt
 Reactive: 54 KVAR
 System Enabled / Disabled: ENABLED
 Master / System State: READY

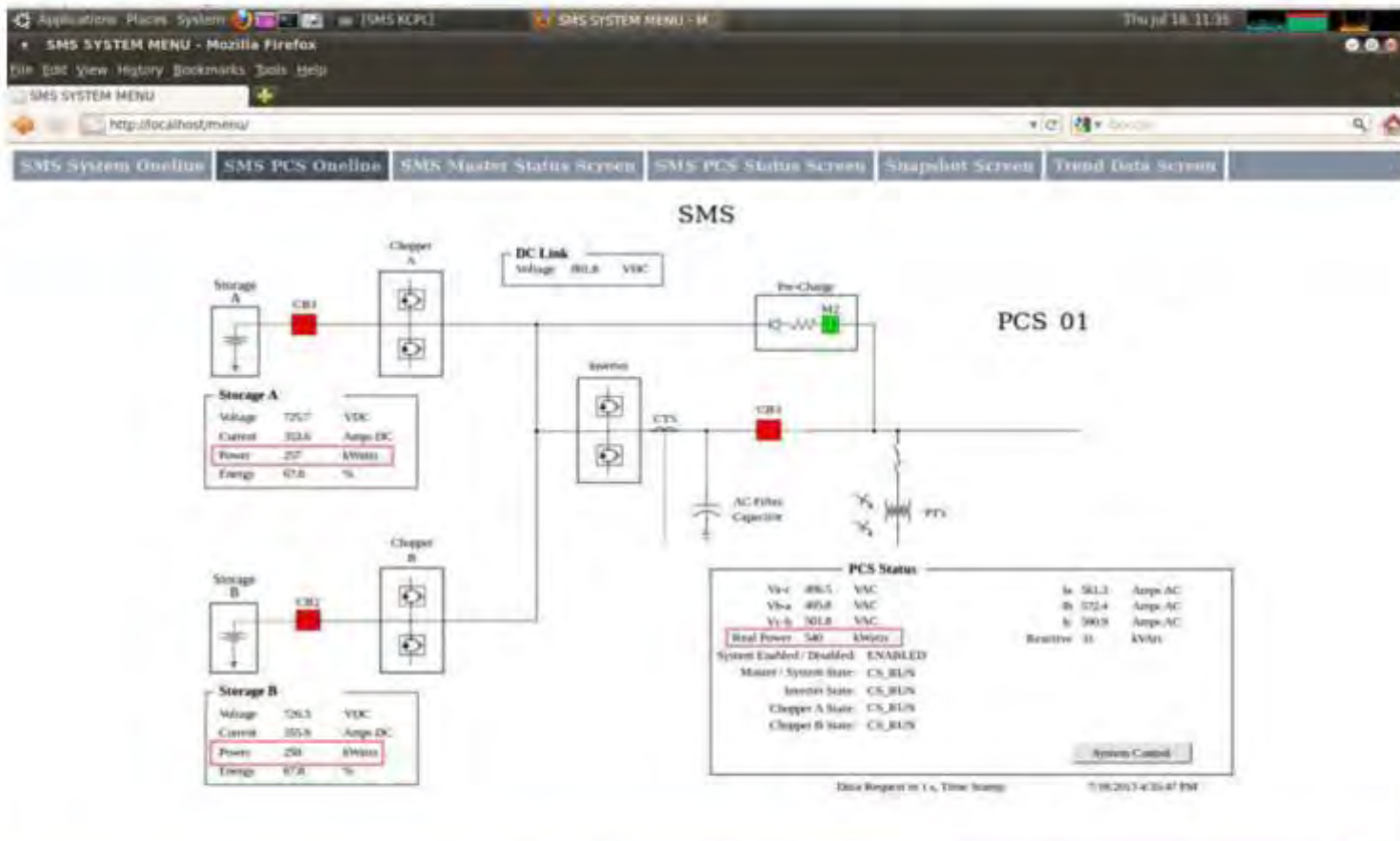
System Control

Date Requested In: Time Stamp: 5/14/2013 10:40:07 PM

Thu May 16, 10:40 AM

19
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

SMS PCS Online: Battery is Discharging



20

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Battery Finished Discharging

The screenshot displays a SCADA software interface. A 'Feature Information' window is open, showing details for device 1888105. The 'Event(s) Complete' field is highlighted in red. The background shows a complex network diagram with various nodes and labels.

Name	Value
Active State	Ready
Active Status	Event(s) Complete
Alarms - Inhibit	OK
Alarms - Isolate	OK
Alarms - Trip Offline	OK
Alarms - Warning	OK
BESS Status	Enabled
Charge Mode	OFF
Energy Available (%)	91
Local - Remote	Remote
Power Mode	FIXED kW
Reactive Mode	OFF
Recalculation Time (sec)	0
SICAM Device Comm Failure	OK
Schedule Override Status	Disabled
KVAR - Discharge Duration (min)	0
KVAR - Discharge Start Time (0-23)	0
KVAR - Fixed PF (%)	0
KVAR - Max Discharge Rate	0
kW - Charge Duration (min)	0
kW - Charge Following	0
kW - Charge Start Time (0-23)	0
kW - Discharge Duration (min)	5
kW - Discharge Start Time (0-23)	16
kW - Load Following	0
kW - Max Charge Rate	0
kW - Max Discharge Rate	800

21

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

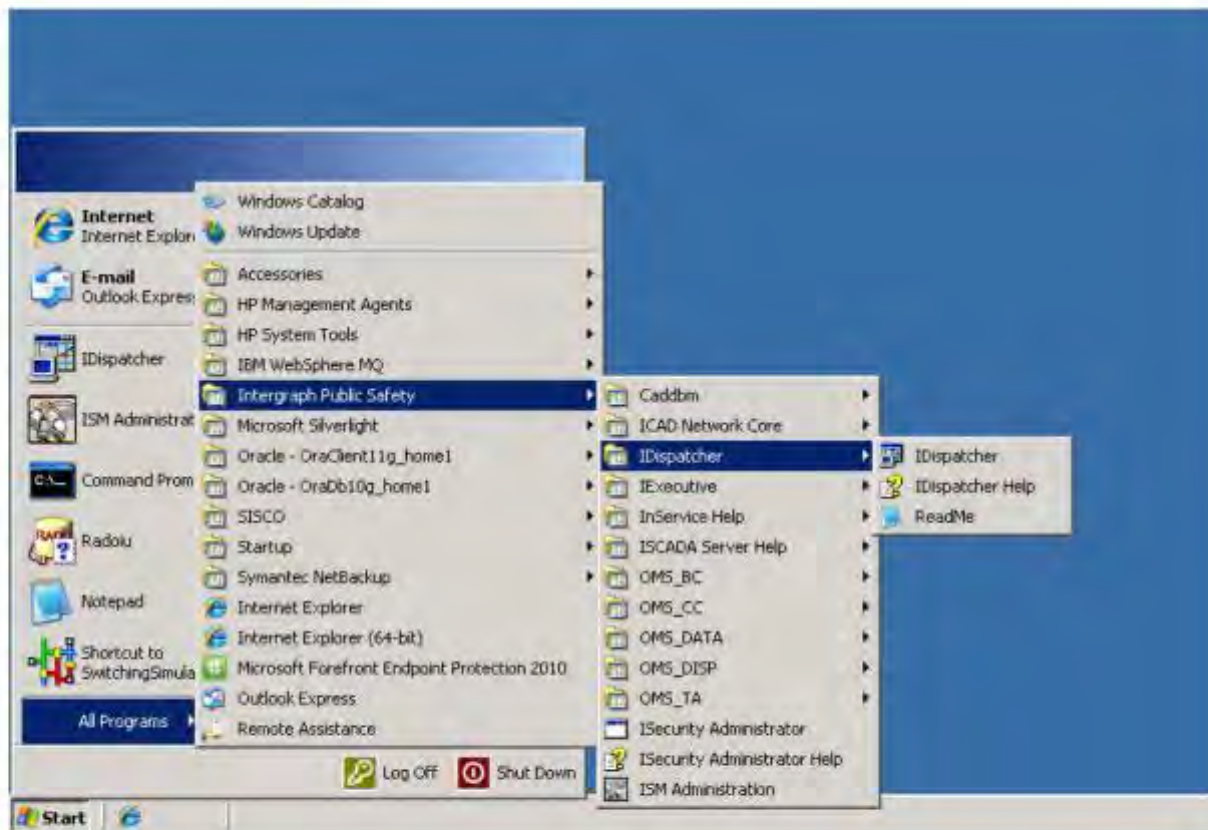


Battery Operation: Load Following Discharge

- KC Green Impact Zone Initiative
- DOE Regional SmartGrid Demonstration Program
- EPRI SmartGrid Demonstration Program



Launch InService I/Dispatcher



2

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



InService I/Dispatcher Main Screen

The screenshot displays the Intergraph I/Dispatcher software interface. At the top, there is a menu bar with options like 'Workstation', 'Draw', 'Job', 'Info', 'View', 'Query', 'Tools', 'Database', 'InService', 'Support/Info', 'Admin/Config', and 'View/Display'. Below the menu is a toolbar with various icons for navigation and actions.

Several windows are open:

- Pending Jobs - [Total: 33]**: A table showing pending jobs with columns for Time, Event Number, Event Type, Location, Agency, Rest, Crat, DGroup, DA Unit, Appl, Recirc, Held for, LV St, Overl, Event S, and Zone.
- Complete Outages - [Total: 20]**: A table listing completed outages with columns for Job Number, Job Type, and Location.

Job Number	Job Type	Location
0002539	TRF	JA 2092
0002575	FDR	7532
0002576	RCL	1860007
0002577	FDR	7532
0002578	FDR	7532
0002579	FDR	7532
0002581	FDR	7532
0002582	FDR	7532
0002583	FDR	7532
0002584	FDR	7532
0002585	FDR	7532
0002586	FDR	7532
0002587	FDR	7532
0002488	FDR	7532
- Draw - [Total: 33]**: A table showing draw information with columns for Unit, A, Type, St, Time, Event Number, Event, and Loc.

Unit	A	Type	St	Time	Event Number	Event	Loc
36		FS	AQ	21587 34			
36		FS	AV	0850 11			75
55		FS	AV	22088 42			JA
74		FS	ER	082375	0002543	SWC	143
75		FS	AQ	21587 34			
75		FS	AM	11762 95			F97
75		FS	AQ	21587 34			
75		FS	AQ	21587 34			
75		FS	AQ	21587 34			
75		FS	AQ	21587 34			
75		FS	AQ	21587 34			
75		FS	AQ	21587 34			
75		FS	AQ	21587 34			
75		FS	AQ	21587 34			
75		FS	AQ	21587 34			
75		FS	AQ	21587 34			
- Interim Dispatcher Job Information**: A detailed form for job information. It includes fields for Job Number, Job Type, Subtype, Device, Device, Phone, Technician, Agency, and various status buttons like 'Accept Job', 'Emergency', 'Closed', 'Abandon', 'Print', 'Schedule Ev', 'Apply Ent', and 'Due Ev'. It also has sections for 'Agency Response' and 'Customer counts'.

At the bottom of the screen, there is a status bar showing 'Ready' and a message: 'Initiate Router: Successful completion'.

3

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Feature Information: Battery

Workstation Crew Job Info View Inquiry Tools Database InService Report/Info Admin/Config View/Display Help

Feature Information
Device: 1888105 Refresh

Name	Value
Active State	Normal
Active Status	OFF
Alarm - Inhibit	OK
Alarm - Isolate	OK
Alarm - Trip Offline	OK
Alarm - Warning	Alarm
BESS Status	Enabled
Charge Mode	OFF
Energy Available (%)	69
Local - Remote	Local
Power Mode	OFF
Reactive Mode	Fixed KVAR
Recalculation Time (sec)	0
SCADA Device Comm Failure	OK
Schedule Override Status	Disabled
KVAR - Discharge Duration (min)	5
KVAR - Discharge Start Time (0-23)	13
KVAR - Fixed PF (%)	0
KVAR - Max Discharge Rate	125
KW - Charge Duration (min)	0
KW - Charge Following	0
KW - Charge Start Time (0-23)	0
KW - Discharge Duration (min)	5
KW - Discharge Start Time (0-23)	0
KW - Load Following	0
KW - Max Charge Rate	0
KW - Max Discharge Rate	100

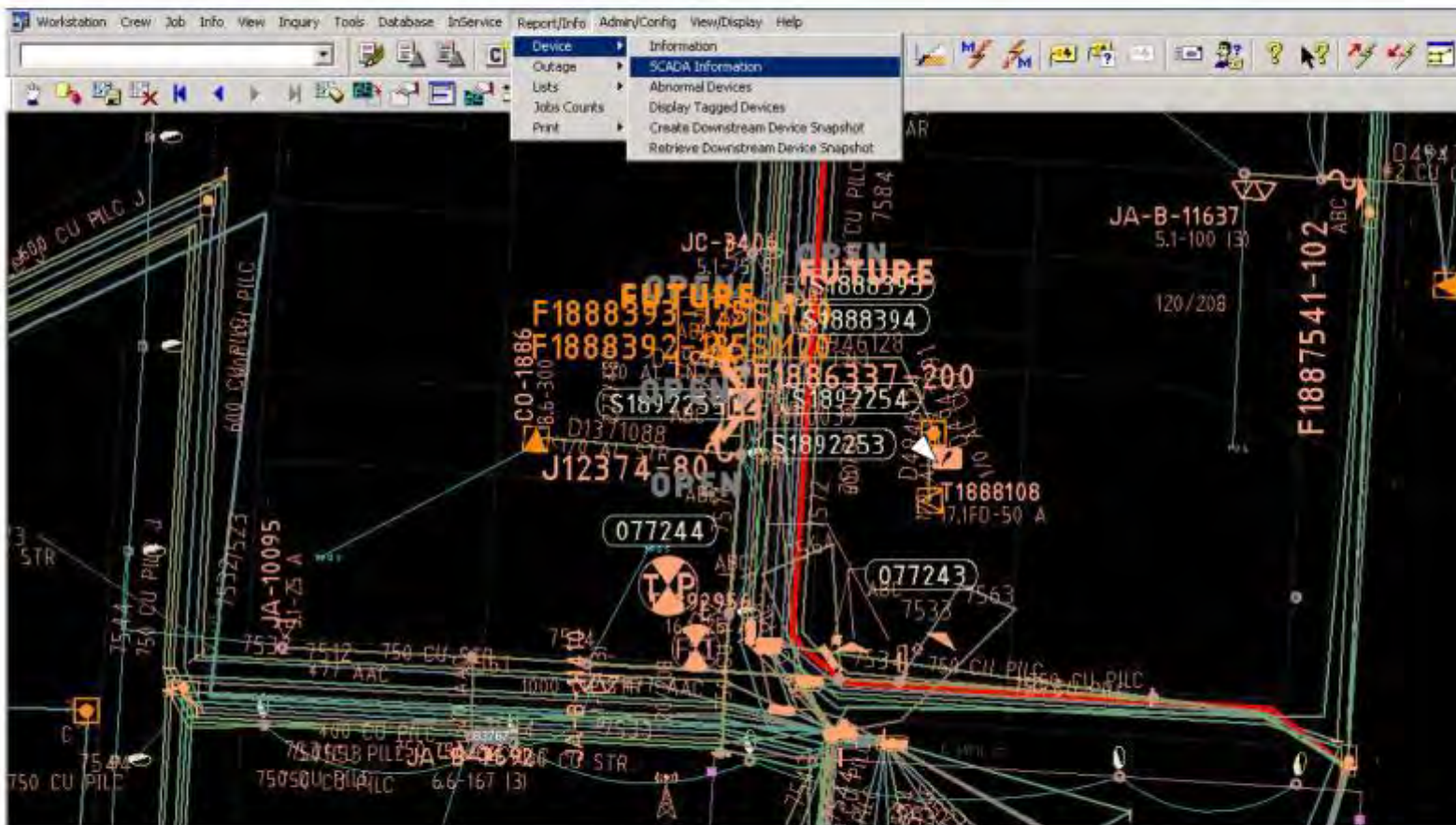
Right Click to Control SCADA points

4

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Launch “SCADA Device Information”

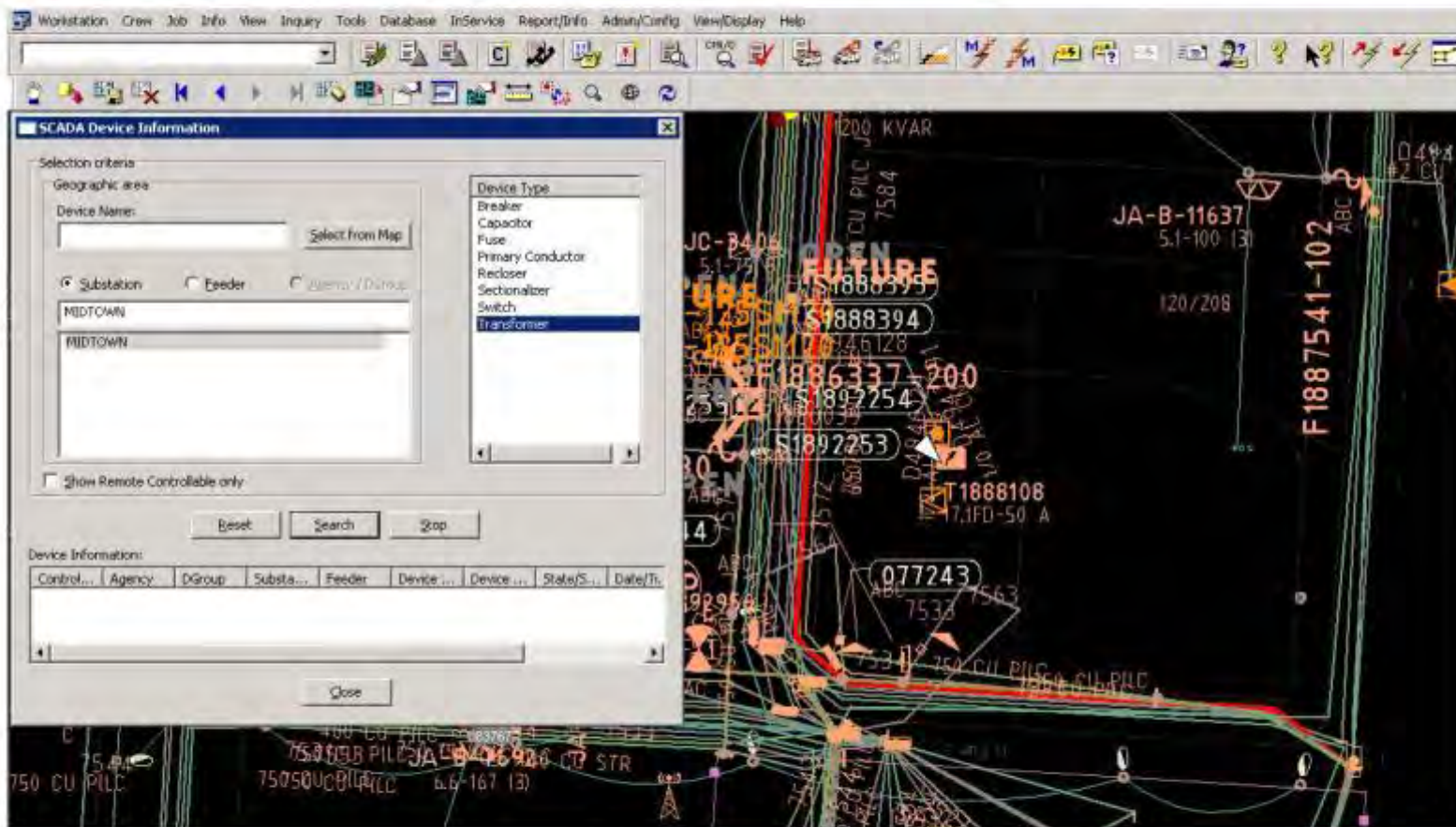


5

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



SCADA Device Information Window



6

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Battery in Device Information

The screenshot displays a software interface for SCADA Device Information. On the left, a search window titled "SCADA Device Information" is open. It includes a "Selection criteria" section with a "Device Name" field containing "1888105" and a "Select from Map" button. Below this are radio buttons for "Substation", "Feeder", and "Battery (0/0/0/0)". A list box shows "MIDTOWN" selected. A "Device Type" list on the right includes Breaker, Capacitor, Fuse, Primary Conductor, Reducer, Sectionalizer, Switch, and Transformer. At the bottom of the search window is a table with the following data:

Control...	Agency	DGroup	Substa...	Feeder	Device Type	Device ...	State/S...	Date
Y	FLDSRV	FLDSV	MIDTOWN	7564	Transformer	1888105		

Buttons for "Reset", "Search", "Stop", and "Close" are also visible. The background of the software shows a network diagram with various components labeled, including "200 KVAR", "JA-B-11637 5.1-100 13", "F1887541-102 ABC", "T1888108 7,IFD-50 A", and "077243 ABC 7533 7563".

7

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Set Battery to Load Following - Circuit Mode

The screenshot displays a SCADA interface with a circuit diagram on the right and a configuration window on the left. The circuit diagram shows various components like transformers (T1888108, T1887530B), breakers (F1887541-102), and feeders (JA-B-11637). The configuration window, titled 'SCADA Device Information', has 'Device Name' set to '1008105' and 'Substation' set to 'MIDTOWN'. A context menu is open over the device, with 'Set Power Mode' selected, and a sub-menu showing 'Load Following' as the chosen option.

Control	Agency	DGroup	Substa...	Feeder	Device Type	Device...	State(S...	Date
Y	FLDSV	FLDSV	MIDT...	7564				

8

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Battery set to LF-Ckt Power Mode

The screenshot displays a SCADA software interface. On the left, a 'Feature Information' window is open for device '1888105'. The 'Attributes' tab is selected, showing a list of parameters and their values. The 'Power Mode' attribute is highlighted with a red box and set to 'LF-Ckt'. The main area shows a complex power grid diagram with various components labeled, including '200 KVAR', 'JA-B-11637', 'F1888393', 'F1888392', 'F1886337', 'S1892254', 'S1892253', 'T1888108', '077244', and '077243'. The interface includes a menu bar at the top with options like 'Workstation', 'Crew', 'Job', 'Info', 'View', 'Inquiry', 'Tools', 'Database', 'InService', 'Report/Info', 'Admin/Config', 'View/Display', and 'Help'. A toolbar with various icons is located below the menu bar.

Name	Value
Active State	Ready
Active Status	Unknown
Alarm - Inhibit	OK
Alarm - Isolate	OK
Alarm - Trip Offline	OK
Alarm - Warning	OK
BESS Status	Enabled
Charge Mode	OFF
Energy Available (%)	98
Local - Remote	
Power Mode	LF-Ckt
Reactive Mode	OFF
Recalculation Time (sec)	0
SICAM Device Comm Failure	OK
Schedule Override Status	Disabled
IWAR - Discharge Duration (min)	0
IWAR - Discharge Start Time (0-23)	0
IWAR - Fixed PF (%)	0
IWAR - Max Discharge Rate	0
IW - Charge Duration (min)	0
IW - Charge Following	0
IW - Charge Start Time (0-23)	0
IW - Discharge Duration (min)	0
IW - Discharge Start Time (0-23)	0
IW - Load Following	0
IW - Max Charge Rate	0
IW - Max Discharge Rate	0

9

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Set kW Discharge Start Time

The screenshot shows a SCADA interface with a 'SCADA Device Information' dialog box. The dialog has a 'Selection criteria' section with fields for 'Device Name' (1888105), 'Substation' (MIDTOWN), and 'Feeder' (MIDTOWN). A 'Device Type' list on the right includes Breaker, Capacitor, Fuse, Primary Conductor, Reducer, Sectionalizer, Switch, and Transformer. Below the dialog is a table of device information with columns for Control, Agency, DGroup, Substa..., Feeder, Device Type, Device..., State..., and Date. A context menu is open over the table, listing various control options. The option 'kW-Set DischargeStartTime (0-23)' is selected, and a '<Enter Value>' button is visible at the bottom of the menu. The background shows a network diagram with various components labeled, such as '700 KVAR', 'JA-B-11637', 'F1887541-102', and 'T18875308'.

10

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Enter Time for Battery to Start Discharging

The screenshot shows a software application window with a menu bar and a toolbar. The main area displays a complex network diagram with various components labeled, including 'F1886337-200', 'T1888108', 'F1887541-102', and 'T1887530B'. A dialog box titled 'Enter Value' is open, allowing the user to input a value for a selected device. Below the dialog is a table of device information.

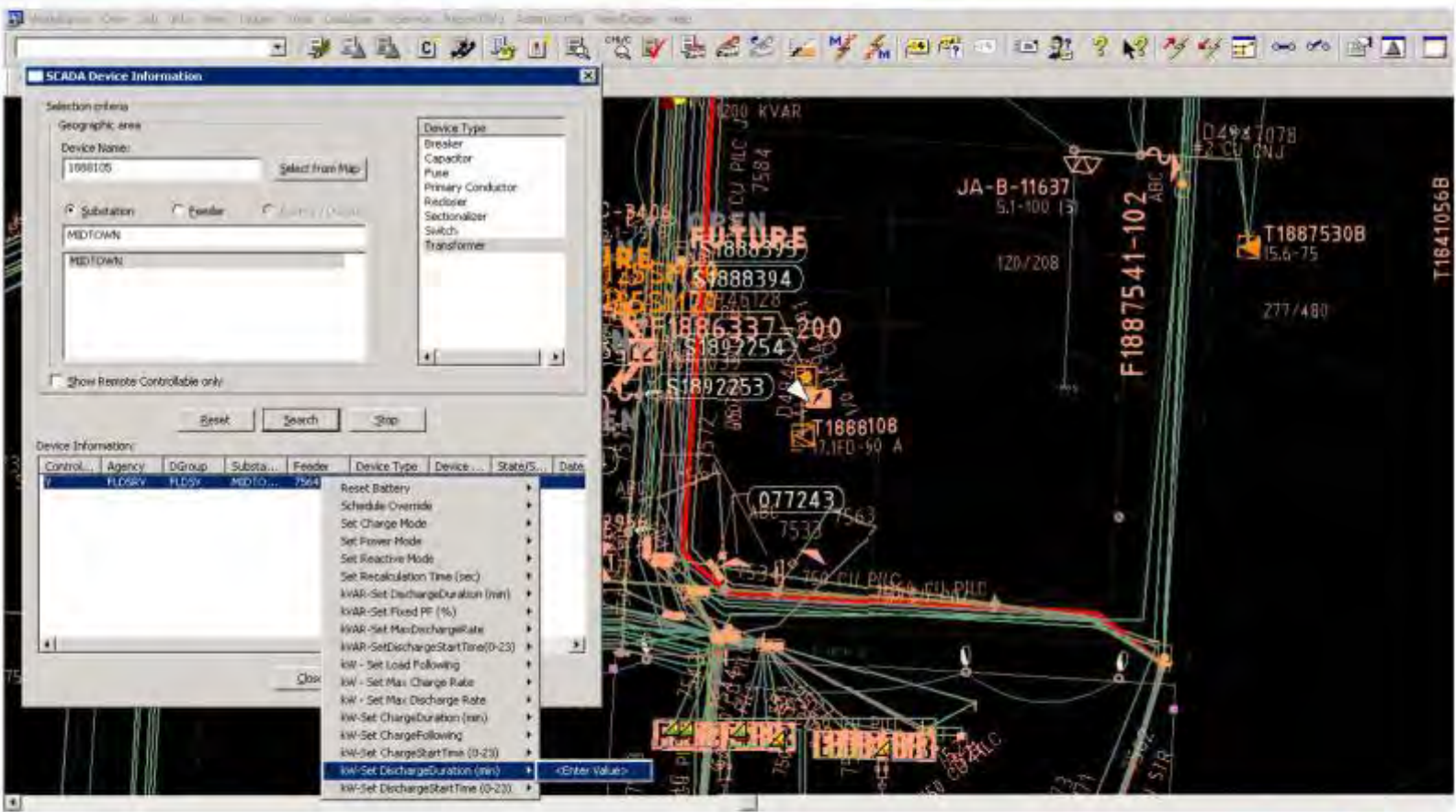
Control...	Agency	Dgroup	Substa...	Feeder	Device Type	Device ...	State/S...	Date
Y	FLDSRV	FLOSV	MIDTO...	7564	Transformer	1888105		

11

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Set kW Discharge Duration



12

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Enter Duration of Battery Discharging

The screenshot shows a software application window titled "KCP&L Green Impact Zone - Information" with a menu bar and toolbar. A "Selection criteria" dialog box is open, showing "Geographic area" with "MIDTOWN" selected, and "Device Type" with "Transformer" selected. An "Enter Value" dialog box is also open, with a "Value:" field. Below the dialog boxes is a "Device Information:" table.

Control...	Agency	Dgroup	Substa...	Feeder	Device Type	Device ...	Status	Date
Y	FLDSRV	FLOSV	MIDTO...	7564	Transformer	1888105		

13

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Set Load Following Discharge Rate

The screenshot displays the SCADA Device Information window. On the left, the 'Selection criteria' section includes 'Geographic area' (Device Name: 1888105, Substation: MEDTOWN) and 'Device Type' (Transformer). A context menu is open over the map, with 'KW - Set Load Following' selected. The map shows a complex network of power lines and devices with various labels like 'F1888337-200', 'T1888108', and 'F1887541-102'.

Control	Agency	DGroup	Substa...	Feeder	Device Type	Device ...	State(S...	Date
V	FLDSV	FLDSV	MEDTO...	7564	Transformer			

14

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Enter Battery Discharge Rate

The screenshot displays a software application window titled "KCP&L Green Impact Zone SmartGrid Demonstration". The main interface is a network diagram with various components labeled, including transformers (T1888108, T1887530B, T1841056B), feeders (F1886337-200, F1887541-102), and other equipment (JA-B-11637, S1888394, S1887754, S1892253, 077243, 04947078). A dialog box titled "Selection criteria" is open, showing "Device Name: 1888105", "Substation: MIDTOWN", and "Device Type: Transformer". An "Enter Value" dialog box is also open, with a "Value:" field. Below the dialog boxes is a table of device information:

Control...	Agency	Dgroup	Substa...	Feeder	Device Type	Device ...	State/S...	Date
Y	FLDSRV	FLOSV	MIDTO...	7564	Transformer	1888105		



Battery Started to Discharge

Workstation Crew Job Info View Inquiry Tools Database InService Report/Info Admin/Config View/Display Help

Feature Information

Device: 1888105 Refresh

Attributes	Counts	SCADA	DNA
Name			
Active State		Ready	
Active Status		Event(s) Pending	
Alarm - Inhibit		OK	
Alarm - Isolate		OK	
Alarm - Trip Offline		OK	
Alarm - Warning		OK	
BESS Status		Enabled	
Charge Mode		OFF	
Energy Available (%)		90	
Local - Remote		Ready	
Power Mode		LF-OK	
Reactive Mode		ON	
Recalculation Time (sec)		0	
SICAM Device Comm Failure		OK	
Schedule Override Status		Disabled	
IVAR - Discharge Duration (min)		0	
IVAR - Discharge Start Time (0-23)		0	
IVAR - Fixed PF (%)		0	
IVAR - Max. Discharge Rate		0	
kW - Charge Duration (min)		0	
kW - Charge Following		0	
kW - Charge Start Time (0-23)		0	
kW - Discharge Duration (min)		5	
kW - Discharge Start Time (0-23)		10	
kW - Load Following		200	
kW - Max. Charge Rate		0	
kW - Max. Discharge Rate		0	

Right Click to Control SCADA points

16

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Launch Browser Based HMI

▪17 This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221

SMS System Menu Main Screen

SMS

OutputBus Currents

Ia:	2.7	A
Ib:	2.7	A
Ic:	1.5	A

OutputBus Voltages

Vab:	7920	V
Vbc:	7980	V
Vca:	7977	V

SMS Status

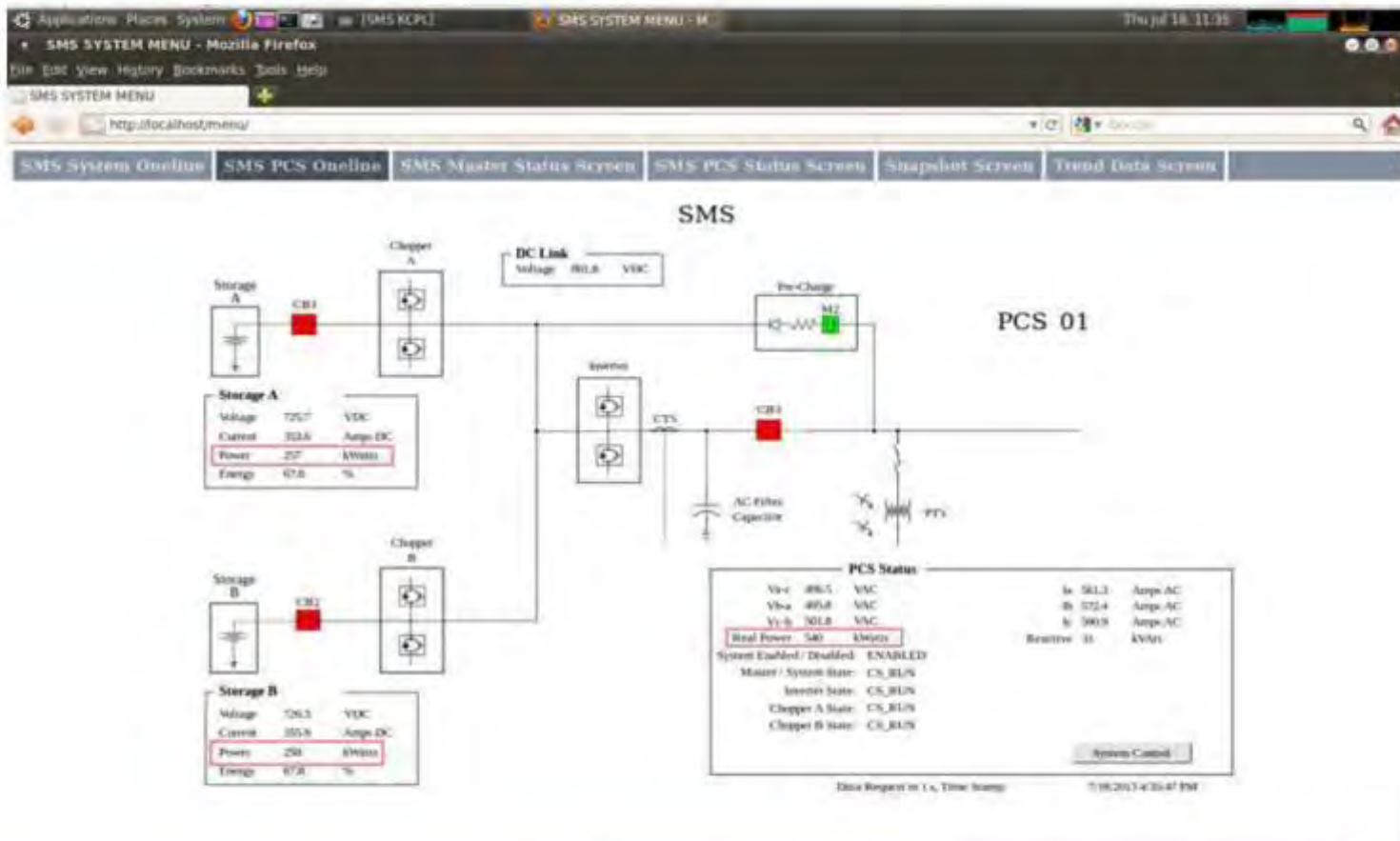
Real Power: -5 KWatt
 Reactive: 24 KVar
 System Enabled/Disabled: ENABLED
 Master/ System State: READY

Data Request in 1 s, Time Stamp: 1/14/2013 10:40:07 PM

Thu Mar 14, 10:40 AM



SMS PCS Online: Battery is Discharging



19

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



Battery Finished Discharging

The screenshot displays a SCADA software interface. A 'Feature Information' window is open, showing details for device 1888105. The 'Event(s) Complete' field is highlighted with a red box. The background shows a complex network diagram with various nodes and labels.

Name	Value
Active State	Ready
Active Status	Event(s) Complete
Alarm - Inhibit	OK
Alarm - Isolate	OK
Alarm - Trip Offline	OK
Alarm - Warning	OK
BESS Status	Enabled
Charge Mode	OFF
Energy Available (%)	92
Local - Remote	Remote
Power Mode	LF-Clt
Reactive Mode	OFF
Recalculation Time (sec)	0
SCADA Device Comm Failure	OK
Schedule Override Status	Disabled
KVAR - Discharge Duration (min)	0
KVAR - Discharge Start Time (0-23)	0
KVAR - Fixed PF (%)	0
KVAR - Max Discharge Rate	0
KW - Charge Duration (min)	0
KW - Charge Following	0
KW - Charge Start Time (0-23)	0
KW - Discharge Duration (min)	5
KW - Discharge Start Time (0-23)	10
KW - Load Following	200
KW - Max Charge Rate	0
KW - Max Discharge Rate	0

20

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000221



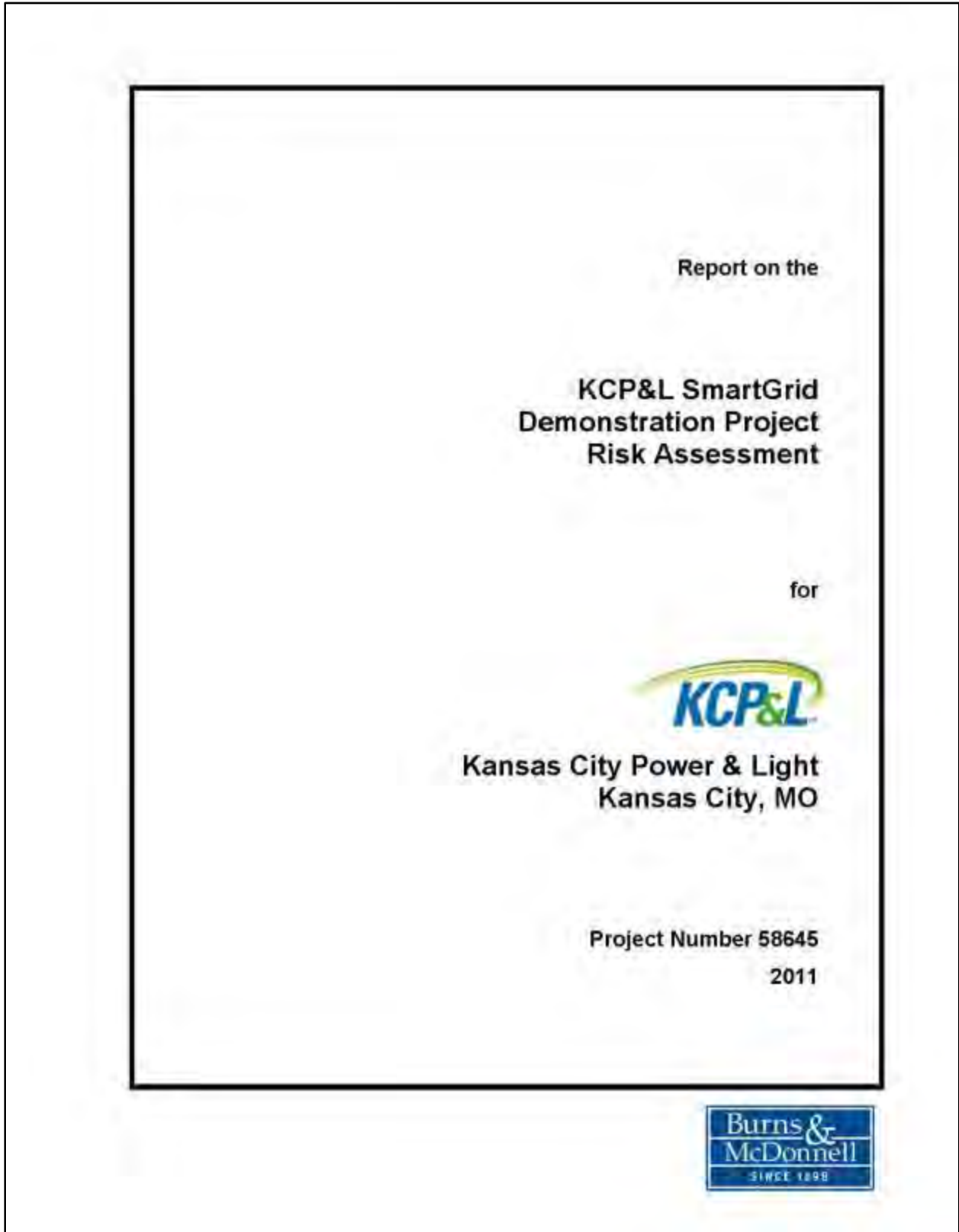
This page intentionally blank.

Appendix L SmartGrid Interoperability Implemented

To be completed in future releases of this report.

This page intentionally blank.

Appendix M KCP&L SmartGrid Risk Assessment Master Report



**KCP&L SmartGrid
Demonstration Project
Risk Assessment Report**

prepared for

**Kansas City Power & Light
Kansas City, Missouri**

November 18, 2011

Project No. 58645

prepared by

**Burns & McDonnell Engineering Company, Inc.
Kansas City, Missouri**

COPYRIGHT © 2011 BURNS & McDONNELL ENGINEERING COMPANY, INC.



November 18, 2011

Edward T. Hedges, P.E.
Mgr, SmartGrid Technology Planning
Kansas City Power & Light
P.O. Box 418679
Kansas City, MO 64141-9679

KCP&L SmartGrid Demonstration Project - Risk Assessment Report - B&McD Project No. 58645

Dear Mr. Hedges:

We are pleased to submit the final version of the Risk Assessment Report for the KCP&L SmartGrid Demonstration Project.

We based the risk assessment on the guidelines provided by the National Institute of Standards and Technology (NIST) in their Special Publication 800-30: Risk Management Guide for Information Technology Systems. We measured all SmartGrid systems on a common risk model, which covered the following risk components: Threats, Vulnerabilities, Likelihoods, Impacts, and Mitigations. We developed methodologies for each risk component and applied them to each SmartGrid system to assess its risk. The methodologies and their outcomes are detailed in different sections of the report. The report includes the analysis of the applicability (to the KCP&L SmartGrid systems) of the security controls recommended by NIST in their Interagency Report 7628. The report also provides a list of security controls to mitigate risks from these systems.

Our recommendations outline actionable technical and procedural steps towards securing the SmartGrid systems. While developing the recommendations, the risk assessment team was careful to include U.S. Department of Energy and industry suggested best practices. This report is intended to be a guide for the Information Security, WAN Services, Physical Security, IT Strategy & Management, and SmartGrid Project Management Office departments to design a secure KCP&L SmartGrid program.

Sincerely,

Rahul Chhabra
Cyber Security Compliance Consultant

9400 Ward Parkway • Kansas City, MO 64114-3319
Tel: 816 333-9400 • Fax: 816 333-3690 • www.burnsmcd.com

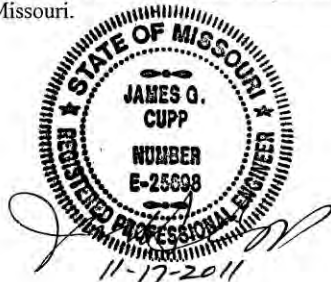
INDEX AND CERTIFICATION

KCP&L SmartGrid Demonstration Project Risk Assessment Report Project 58645 Report Index

<u>Section Number</u>	<u>Chapter Title</u>	<u>Number of Pages</u>
ES	Executive Summary	11
INT	Introduction	3
1.0	System Characterization	4
2.0	Threat Identification	10
3.0	Vulnerability Assessment	10
4.0	Likelihood Determination	27
5.0	Impact Analysis	12
6.0	Existing Mitigation	5
7.0	Risk Determination	6
8.0	Risk Mitigation	11
9.0	Project Recommendations	7
Appendix A	The NISTIR-7628 Logical Interface Categories	1
Appendix B	KCP&L to NISTIR-7628 Logical Interface Mapping	2
Appendix C	KCP&L SmartGrid System Descriptions	3
Appendix D	Definition Location of NISTIR-7628 Recommended Security Requirements	6
Appendix E	Control Analysis Results	7
Appendix F	Security Requirements for Control Sets	7
Appendix G	Sample Questionnaire for Hosting Vendors	7
Appendix H	Unconfirmed Security Requirements from UCAIug AMI and DM Security Profiles	3
Appendix I	Additional References	1

Certification

I hereby certify, as a Professional Engineer in the state of Missouri, that the information in the document was assembled under my direct personal charge. This report is not intended or represented to be suitable for reuse by Kansas City Power & Light or others without specific verification or adaptation by the Engineer. This certification is made in accordance with the provisions of the laws and rules of the State of Missouri.





James G. Cupp, PE Missouri License # 25698
Date: 11-17-11
(Reproductions are not valid unless signed, dated, and embossed with Engineer's seal)

TABLE OF CONTENTS

	<u>Page No.</u>
EXECUTIVE SUMMARY	ES-1
INTRODUCTION.....	IN-1
1.0 SYSTEM CHARACTERIZATION	1-1
1.1 System-Related Information	1-1
2.0 THREAT IDENTIFICATION	2-1
2.1 Threat Source Identification	2-1
2.2 Motivation and Threat Actions	2-9
3.0 VULNERABILITY ASSESSMENT	3-1
3.1 Vulnerability Sources.....	3-1
3.2 Vulnerability Ratings.....	3-3
3.3 Vulnerability Assessment.....	3-4
3.4 Vulnerability Assessment Results.....	3-9
4.0 LIKELIHOOD DETERMINATION.....	4-1
4.1 Analysis of Threat Likelihood.....	4-2
4.2 Likelihood Determination Results.....	4-27
5.0 IMPACT ANALYSIS.....	5-1
5.1 Impact Assessment Approach.....	5-2
5.2 Impact Assessment.....	5-4
5.3 Impact Assessment Results.....	5-10
6.0 EXISTING MITIGATION.....	6-1
6.1 Mitigation Analysis Assumptions.....	6-1
6.2 Mitigation Analysis Technique.....	6-1
6.3 Mitigation Analysis Results.....	6-1
6.4 Mitigation Evaluation.....	6-3
7.0 RISK DETERMINATION	7-1
7.1 Risk-Rating Matrix	7-1
7.2 Risk Determination	7-2
8.0 RISK MITIGATION	8-1
8.1 Creation of Security Zones and Implementation of Tailored Control Sets.....	8-1
8.2 Industry-Suggested Controls.....	8-8
9.0 PROJECT RECOMMENDATIONS	9-1
9.1 Select and Implement Controls.....	9-1



KCP&L SmartGrid
 Demonstration Project
 Risk Assessment Report

Table of Contents

9.2	Create Security Zones	9-1
9.3	Create a Security Implementation Plan	9-2
9.4	Update the Cyber Security Plan for the DOE	9-2
9.5	Create Security Requirements for all Systems in the Project	9-2
9.6	Recommendations for Externally Hosted Systems	9-2
9.7	Policy Updates on Recommended Procedural Controls	9-5
9.8	Create & Execute Test Cases	9-5
9.9	Perform Periodic Security Assessment	9-6
9.10	Participate in Working Groups	9-6
9.11	Conclusion	9-7

APPENDIX A THE NISTIR-7628 LOGICAL INTERFACE CATEGORIES

APPENDIX B KCP&L TO NISTIR-7628 LOGICAL INTERFACE MAPPING

APPENDIX C KCP&L SMARTGRID SYSTEM DESCRIPTIONS

APPENDIX D DEFINITION LOCATION OF NISTIR-7628 RECOMMENDED SECURITY REQUIREMENTS

APPENDIX E CONTROL ANALYSIS RESULTS

APPENDIX F SECURITY REQUIREMENTS FOR CONTROL SETS

APPENDIX G SAMPLE QUESTIONNAIRE FOR HOSTING VENDORS

APPENDIX H UNCONFIRMED SECURITY REQUIREMENTS FROM UCAIUG AMI AND DM SECURITY PROFILES

APPENDIX I ADDITIONAL REFERENCES



TOC-2



LIST OF TABLES

Page No.

Table ES 1	SmartGrid Systems Included in the Risk Assessment	ES-2
Table ES 2	SmartGrid Systems Excluded from the Risk Assessment.....	ES-2
Table ES 3	Threat Ratings for the SmartGrid Systems	ES-4
Table ES 4	Vulnerability Ratings for the SmartGrid Systems.....	ES-5
Table ES 5	Likelihood Ratings for the SmartGrid Systems	ES-6
Table ES 6	Impact Ratings for the SmartGrid Systems.....	ES-7
Table ES 7	Combined Mitigation Ratings for the SmartGrid Systems	ES-8
Table ES 8	Overall Risk Ratings for the SmartGrid Systems.....	ES-9
Table 1-1	System Classifications in the Extended Smart Grid Domains	1-3
Table 1-2	Applicable NISTIR-7628 Volume-I Logical Interface Categories	1-4
Table 2-1	Threat Determination Calculation Results	2-8
Table 2-2	Threat Source Motivations and Threat Actions	2-10
Table 3-1	Relative Vulnerability Ratings of SmartGrid Systems	3-9
Table 4-1	Likelihood Evaluation Criteria	4-1
Table 4-2	Likelihood Ratings.....	4-27
Table 5-1	Example Criticality Assignment Guideline.....	5-2
Table 5-2	Confidentiality Impact Level Definitions	5-3
Table 5-3	Integrity Impact Level Definitions	5-3
Table 5-4	Availability Impact Level Definitions	5-4
Table 5-5	Impact Assessment Results	5-11
Table 6-1	Fulfilled NISTIR-7628 Security Requirements by Family	6-2
Table 6-2	Determination of Mitigation Equation Coefficients.....	6-4
Table 6-3	Mitigation Rating for Systems	6-5
Table 7-1	Risk Rating Matrix.....	7-2
Table 7-2	Mitigation Effort Criteria	7-3
Table 7-3	Estimated Mitigation Effort for SmartGrid Systems.....	7-3
Table 8-1	Security Zone Recommendations for SmartGrid Systems	8-4
Table 8-2	NISTIR-7628 Security Requirements Applicability by System	8-10
Table 9-1	Industry Working Groups.....	9-6

LIST OF FIGURES

	<u>Page No.</u>
Figure ES-1 Risk Rating Categories	ES-10
Figure 3-1 Graphical Representation of Relative Vulnerability Ratings	3-10
Figure 5-1 Graphical Representation of Relative Criticality Results	5-12
Figure 7-1 Risk Rating Categories	7-5
Figure 7-2 Risk Management Cycle	7-6
Figure 8-1 Representation of SmartGrid Systems in Respective Security Zones	8-5
Figure 8-2 Representation of Control Sets for Inter-Security Zone Communication	8-8



LIST OF ACRONYMS

ACL	Access Control List
AES	Advanced Encryption Standard
AHE	Advanced Metering Infrastructure Head-End
ALNK	AccountLink
AMI	Advanced Metering Infrastructure
ASIS	American Society for Industrial Security
BMS	Building Management System
CIA	Confidentiality, Integrity, and Availability
CIS	Customer Information System
DAC	Distribution Automation Controller
DAD	Distribution Automation Device
DCADA	Distributed Control and Data Acquisition
DDC	Distribution Data Concentrator
DDoS	Distributed Denial of Service
DER	Distributed Energy Resources
DERM	Distributed Energy Resources Management System
DHS	Department of Homeland Security
DMAT	Data Mining & Analysis Tool
DMS	Distribution Management System
DOE	Department of Energy
DR	Demand Response or Disaster Recovery
EAVF	Ease of Access Vulnerability Factor
EMS	Energy Management System
EVSE	Electric Vehicle Supply Equipment
GIS	Geographic Information System
GUI	Graphical User Interface
HAN	Home Area Network
HAND	Home Area Network Device
HANG	Home Area Network Gateway
HEMP	Home Energy Management Portal
HVAC	Heating, Ventilation, and Air Conditioning
HTTP	Hypertext Transfer Protocol
ICSJWG	Industrial Control Systems Joint Working Group
IEC	International Electrotechnical Commission
IHD	In-Home Display
IP	Internet Protocol
ISA	International Society of Automation
KPI	Key Performance Indicator
L+G	Landis+Gyr
MAC	Media Access Control
MDM	Meter Data Management System
MTR	SmartMeter
MWFM	Mobile Workforce Management System
NERC	North American Electric Reliability Organization
NESCO	National Electric Sector Cybersecurity Organization
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NIST SP	National Institute of Standards and Technology Special Publication

KCP&L SmartGrid
 Demonstration Project
 Risk Assessment Report

Table of Contents

NVD	National Vulnerability Database
OATI	Open Access Technology International
OMS	Outage Management System
OWASP	Open Web Application Security Project
PEV	Plug-in Electric Vehicle
PII	Personally Identifiable Information
RF	Radio Frequency
RSA	Rivest, Shamir, and Adleman (an algorithm for public key cryptography)
RTO	Regional Transmission Organization
RVR	Relative Vulnerability Rating
SDLC	Software Development Life Cycle
SDT	Standard Drafting Team
SGIP	Smart Grid Interoperability Panel
SGMM	Smart Grid Maturity Model
SIA	Security Industry Association
SME	Subject Matter Expert
SSL	Secure Sockets Layer
SSN	Social Security Number
TEVF	Tech Ease Vulnerability Factor
UCA	Utility Communications Architecture
UCAug	UCA International Users Group
UTC	Utilities Telecom Council
VEMS	Vehicle Energy Management System
VPN	Virtual Private Network



TOC-6



Executive Summary

Kansas City Power & Light Company (KCP&L) chose to conduct a comprehensive risk assessment of all the systems within their SmartGrid Demonstration Project (hereafter called the "project"). KCP&L made this decision to meet the requirement set forth in both their SmartGrid Cyber Security Plan¹ and the U.S. Department of Energy (DOE) Smart Grid Demonstration funding announcement² that states implementing sound cyber security controls for all SmartGrid systems.

According to the KCP&L SmartGrid Cyber Security Plan, the risk assessment performed for the project was primarily based on the guidelines provided in the National Institute of Standards and Technology (NIST) in their Special Publication 800-30 – Risk Management Guide for Information Technology Systems (NIST SP 800-30). The NIST Interagency Report 7628 Volumes I-III (NISTIR-7628) along with the UCAI International Users Group's Advanced Metering Infrastructure and Distribution Management (UCAIug AMI and UCAIug DM) security profiles were also used to conduct the analysis and provide cyber security suggestions for the KCP&L project. Several additional resources were used where applicable. Any references not included in the footnotes throughout the report are provided in Appendix I.

The risk assessment team used a mathematical model to assess the risk of each system. Using a model ensures that an identical method is used to evaluate risk for each system. The model is expressed using the following equation:

$$\text{Risk} = \text{Threat} + \text{Vulnerability} + \text{Likelihood} + \text{Impact} - \text{Mitigation}$$

Separate methodologies were developed to calculate the values of the variables: Threat, Vulnerability, Likelihood, Impact and Mitigation. Each methodology was applied uniformly to all systems to determine values of the risk rating model variables.

¹ KCP&L Green Impact Zone SmartGrid Demonstration, *SmartGrid Cyber Security Plan*, Version v1.0 - November 18, 2010

² U.S. Department of Energy, National Energy Technology Laboratory, Funding Opportunity Number: DE-FOA-0000036, CFDA Number: 81.122 Electricity Delivery and Energy Reliability Research, Development and Analysis, *Financial Assistance Funding Opportunity Announcement*, June 25, 2009

³ NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems. <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

⁴ National Institute of Standards and Technology Interagency Report 7628. http://csrc.nist.gov/publications/nistir/7628/nistir-7628_vol1.pdf

⁵ UCA International Users Group <http://www.ncainz.org/default.aspx>

⁶ UCA International Users Group (UCAIug) <http://www.ucaiug.org/default.aspx>



As a prerequisite to the risk assessment, all systems within the KCP&L SmartGrid portfolio were identified along with their respective interfaces. This step formed the boundaries of the scope and created a foundation for the assessment. The resultant scope of the risk assessment was identified to include the following SmartGrid systems:

SmartGrid Systems included in the Risk Assessment	Commonly Referred as
Advanced Metering Infrastructure Head-End	AHE
AccountLink	ALNK
Building Management System	BMS
Customer Information System	CIS
Distributed Control and Data Acquisition	DCADA
Distributed Energy Resources – Commercial & Industrial	DER – C&I
Distributed Energy Resources – Grid-Connected	DER – Grid-Connected
Distributed Energy Resources Management System	DERM
Distributed Energy Resources – Residential	DER – Residential
Data Mining and Analysis Tool	DMAT
Distribution Management System	DMS
Energy Management System	EMS
Field Distribution Automation Devices	Field DADs
Geographic Information System	GIS
Home Area Network Device	HANDs
Home Area Network Gateway	HANG
Home Energy Management Portal	HEMP
Meter Data Management System	MDM
SmartMeter	MTR
Mobile Workforce Management System	MWFM
Substation Distribution Automation Devices	Substation DADs

Table ES 1 SmartGrid Systems Included in the Risk Assessment

The systems that were in the early stages of definition and planning were not included in this assessment. Also excluded were the systems whose integration with the SmartGrid program at the time of assessment was planned but not completely defined. The assessment relied heavily upon analyzing the functionalities of each system and creating a rating for each of the risk components. The exclusions were required so as not to lessen the overall integrity of the results.

Following is the list of systems identified as part of the project that were excluded from the risk assessment:

SmartGrid Systems excluded from the Risk Assessment	Commonly Referred as
Electric Vehicle Supply Equipment	EVSE
Outage Management System	OMS
Plug-in Electric Vehicle	PEV
Integration with Regional Transmission Organization	RTO
Vehicle Energy Management System	VEMS

Table ES 2 SmartGrid Systems Excluded from the Risk Assessment

For the systems that were included in the scope, several methods were used to develop a deeper understanding of KCP&L's implementation of SmartGrid technologies. These methods included the review of system documents such as use cases, interface diagrams, and vendor software specifications. The interactive methods included focus group interviews with the Subject Matter Experts (SMEs) using a set of targeted questions. The result was a grouping of SmartGrid systems in several business function domains that were later used as one of the criteria to recommend creation of security zones. The collaborative work with the SMEs also resulted in classification of all system interfaces in one of the NIST specified logical interface categories. This classification was later used to determine the security controls that will be required to secure the systems.

In order to assess the value of the Threat variable in the risk model, several internal and external threat sources were identified. The general perception is that a threat source is a malicious computer user with an intention to harm the organization. However this is not completely true. Threat can be defined as the intent and method targeted at the exploitation of a vulnerability, or a situation and method that may accidentally trigger a vulnerability⁵. This assessment also included threats resulting from unintentional acts and natural occurrences. Once the threat sources were identified, a listing of motivations and possible threat actions taken by each threat source was produced. In order to determine threat rating to be used in the risk rating model, each threat source was evaluated to determine if it could impact a given system. A threat rating was thus assigned to each system equating to the count of the number of threat sources identified to pose a risk to that system. The results of the threat determination calculation are shown in the following table on a scale of 0-10.

⁵ U.S. Department of Commerce, Computer Security Division, National Institute of Standards and Technology, *Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems*, March 2006



KCP&L SmartGrid
Demonstration Project
Risk Assessment Report

Executive Summary

System	Total Number of Potential Threat Sources
AHE	8
ALNE	8
BMS	7
CIS	7
DADs (Field and Substation)	6
DCADA	8
DER - C&I	6
DER - Grid-Connected	6
DERM	6
DER - Residential	6
DMLAT	5
DMS	8
EMS	8
GIS	7
HAND/HANG	6
REMP	7
MDM	8
MTB	8
MWFM	7

Table ES 3 Threat Ratings for the SmartGrid Systems

Vulnerability is defined as the susceptibility of a system to attacks. Numerous vulnerabilities are discovered every week. To evaluate a large program like KCP&L for every potential vulnerability at a single point-in-time is a large undertaking. Furthermore, the validity of vulnerabilities four to six months after the assessment is done is difficult to determine. To overcome these issues, systems were evaluated for the broader categories of vulnerabilities: System and Operational. The system vulnerabilities included were the ones that directly affect one of the three cyber security goals of Confidentiality, Integrity and Availability. The operational vulnerabilities were categorized into People, Policy and Procedural vulnerabilities. To provide a numerical value to the vulnerability of a system, an approach was used to quantify two of the fundamental reasons that make a system vulnerable. The resulting two variables were the relative technical ease of coordinating an attack and the relative ease of access to parts of the system. Table ES 4 lists each system along with the calculated vulnerability rating on a scale of 0-10.



ES-4



System	Technical Ease	Ease of Access	Vulnerability Rating
AHE	3	3	6
ALNK	4	4	8
BMS	2	3	5
CIS	3	3	6
DCADA	2	3	5
DER - CAI	2	3	5
DER - Grid-Connected	2	3	5
DERM	3	4	7
DER - Residential	3	4	7
DMAT	2	3	5
DMS	2	2	4
EMS	2	2	4
FieldDADs	2	3	5
GIS	3	2	5
HAND	4	4	8
HANG	4	4	8
HEMP	4	4	8
MDM	2	3	5
MTR	3	5	8
MWFM	2	2	4
Substation DADs	2	3	5

Table ES 4 Vulnerability Ratings for the SmartGrid Systems

Several measuring criteria were used to assess the *Likelihood* of an attack. These criteria included the evaluation of a potential threat source's motivation and capabilities, as well as the nature and frequency of existing vulnerabilities. The assessment was done to determine the likelihood of an attack, not represent the likelihood of a successful attack. Similar to other risk model components, a rating methodology was developed to assign a likelihood number to all systems. Each threat sources was applied to each system and its likelihood of an attack was given a rating. The highest assigned likelihood rating of a threat source for a system was then used as that system's overall likelihood rating on a scale of 0-10. The results of the likelihood assessment are shown in the following table, Table ES 5.

System	Likelihood Rating
AHE	8
ALNK	10
BMS	4
CIS	8
DADs	6
DCADA	6
DER - C&I	6
DER - Grid-Connected	6
DERM	6
DER - Residential	6
DMAT	6
DMS	8
EMS	10
GIS	6
HAND/HANG	8
HEMP	10
MDM	6
MTR	10
MWFM	6

Table ES 5 Likelihood Ratings for the SmartGrid Systems

Impact can be defined as the effect or influence a successful attack may have on a system and/or the organization. Some of the big impacts include: significant monetary damage, compromised consumer privacy, loss of important business operations for long periods, national-level damage to company reputation and/or years of litigation. For the risk rating model, a quantifying approach was developed to estimate the effects a cyber compromise of confidentiality, integrity, and/or availability will have on the system and the organization. The confidentiality impact was judged based on the qualitative assessment of sensitivity of the data and the effects of a data leak event. The integrity impacts were assessed in terms of cost impacts of fixing an integrity issue. Lastly, the losses due to unavailability of each system were estimated taking into account the loss in productivity. The assessment results in the form of each system's impact rating (on a scale 0-10) are listed in the following table, Table ES 6.



KCP&L SmartGrid
Demonstration Project
Risk Assessment Report

Executive Summary

System	Confidentiality Impact Level	Integrity Impact Level	Availability Impact Level	Overall Impact Level
AHE	8	8	6	7.33
ALNE	8	6	2	7.33
BMS	4	6	4	4.67
CIS	10	4	10	6.00
DADs (Field & Substation)	4	4	6	4.67
DCADA	4	6	2	6.00
DER – C&I	4	4	4	4.00
DER – Grid-Connected	4	6	4	4.67
DER – Residential	4	6	2	4.00
DERM	4	10	2	7.33
DMAT	6	4	4	4.67
DMS	4	10	10	6.00
EMS	6	10	10	6.67
GIS	4	6	6	5.33
HAND/HANG	6	4	6	5.33
HEMP	8	6	2	7.33
MDM	8	6	6	6.67
MTR	8	6	6	6.67
MWPM	4	6	4	4.67

Table ES 6 Impact Ratings for the SmartGrid Systems

Mitigations are defined as the risk reducing efforts or controls commissioned to moderate the vulnerability, impact, or likelihood of an attack on a system. To assess the mitigations, first the cyber controls suggested by NISTIR-7628 and the UCAIug AMI & DM profiles were studied for their applicability to the KCP&L SmartGrid systems. Once the applicable sets of controls were identified, they were matched with the security controls mandated in the KCP&L policies, standards and processes. A methodology was created to quantify the existing mitigation so that it can be used in the risk rating model. The methodology was based on the assumption that all requirements stated in the KCP&L policies, standards and processes are enforced on all existing and new systems at KCP&L. The results of existing mitigation (with maximum possible rating of 30) are provided in the following table, Table ES 7.

KCP&L SmartGrid
 Demonstration Project
 Risk Assessment Report

Executive Summary

System	Combined Mitigation Rating
AHE	13.00
ALNK	15.36
BMS	8.19
CIS	13.41
DADs (Field & Substation)	9.49
DCADA	10.33
DER - C&I	9.07
DER - Grid-Connected	9.49
DER - Residential	10.14
DERM	12.23
DMAT	9.49
DMS	12.35
EMS	14.51
GIS	9.91
HAND/HANG	12.81
HEMP	15.36
MDM	10.75
MTE	14.94
MWFM	8.96

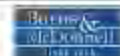
Table ES 7 Combined Mitigation Ratings for the SmartGrid Systems

The primary purpose for this risk assessment, as stated earlier, was to identify the risk of each SmartGrid system so that KCP&L can strategize its efforts towards securing the project as a whole. The prioritization task becomes less complex with a risk rating available for each system. The final risk rating for each system was calculated using the model:

$$R = T + V + L + I - M$$



ES-8



KCP&L SmartGrid
Demonstration Project
Risk Assessment Report

Executive Summary

System ID	System	Threat Rating (T)	Relative Vulnerability Rating (V) ↓	Highest Likelihood Rating (L) ↓	System Impact Rating (I) ↓	Combined Mitigation Rating (M) ↑	Overall Risk Rating (R)
1	AHE	8	6	8	7.33	13.00	16.34
2	ALNK	8	8	10	7.33	15.36	17.97
3	BMS	7	5	4	4.67	8.19	12.48
4	CTS	7	6	8	6.00	13.41	15.59
5	DADs (Field & Substation)	6	5	6	4.67	9.49	12.18
6	DCADA	8	5	6	6.00	10.33	14.67
7	DER - C&I	6	5	6	4.00	9.07	11.93
8	DER - Grid-Connected	6	5	6	4.67	9.49	12.18
9	DER - Residential	6	7	6	4.00	10.14	12.86
10	DERM	6	7	6	7.33	12.23	14.10
11	DMAT	5	5	6	4.67	9.49	11.18
12	DMS	8	4	8	6.00	12.35	15.65
13	EMS	8	4	10	8.67	14.31	16.15
14	GIS	7	5	6	5.33	9.91	13.42
15	HAND/HANG	6	8	8	5.33	12.81	14.53
16	HEMP	7	8	10	7.33	15.36	16.97
17	MDM	8	5	6	6.67	10.75	14.92
18	MTR	8	8	10	6.67	14.94	17.72
19	MWFM	7	4	6	4.67	8.96	12.71

Table ES 8 Overall Risk Ratings for the SmartGrid Systems

↓ - Denotes that lowering the component rating will lower the Overall Risk Rating.
↑ - Denotes that raising the component rating will lower the Overall Risk Rating.

Based on the risk ratings calculated above, the systems were plotted against an estimate of the effort required to further mitigate the threats, likelihoods and impacts. The following figure, Figure ES 1, shows the system IDs plotted against calculated overall risk rating and estimated effort to mitigate.



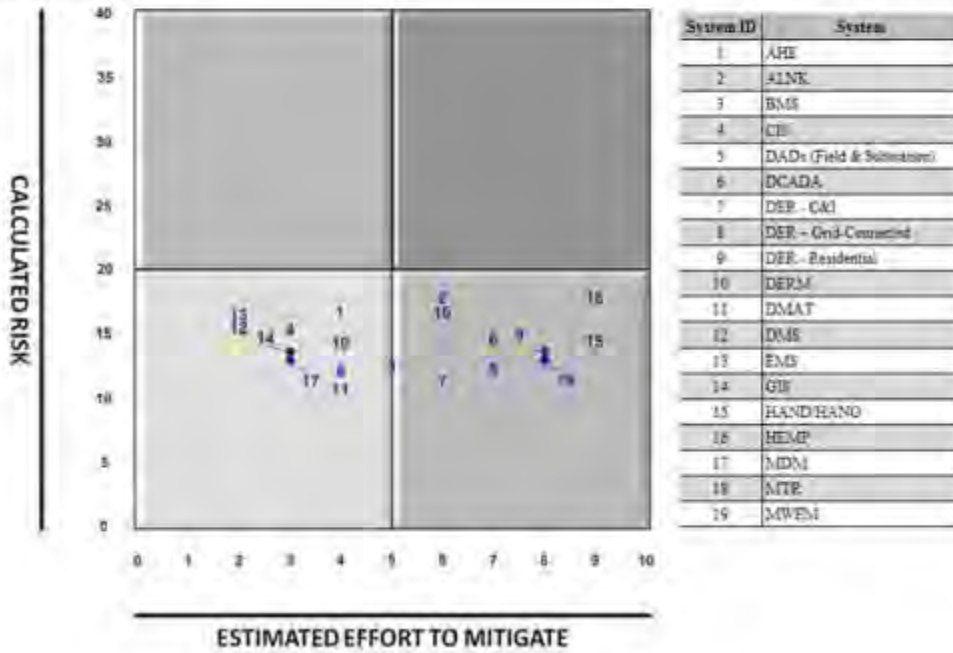


Figure ES 1 Risk Rating Categories

There is not, nor should there be, an “ideal” level of risk, or a static “target” level of risk at which to aim. These calculated risk ratings should be used to prioritize efforts to reduce overall system risk. Risk may be reduced by mitigations and controls applied at the policy, network, or system level.

There are ten major recommendations given in this report. Some are technical in nature, such as assessing and implementing recommended security controls, or designing and implementing recommended network security zones. Others are more policy- and process-based, such as updating policies and documenting mitigation activities. The following list is an overview of the ten major recommendations:

- Implement the provided sets of security controls in a phased approach.
- Implement the recommended conceptual security zones using network design techniques.
- Create an implementation plan that covers the recommended security controls and security zones.
- Update the KCP&L SmartGrid Cyber Security Plan to maintain focus on security and to meet DOE expectations.



- Create security requirements for all systems to convert the security controls from concept to implementation.
- Develop minimum security requirements for any SmartGrid system externally hosted by a third-party.
- Update KCP&L policies, standards, and/or processes to include protection of SmartGrid systems based upon the provided set of procedural controls.
- Create and execute test cases to verify the placement and functionality of the security controls.
- Perform periodic security assessments to identify and mitigate new risks.
- Participate in working groups to learn and create best practices and standards for securing the grid.

These recommendations cover the entire project, but specifically target the systems evaluated as being the most at risk, or the most impactful, and should be evaluated and considered for inclusion in the project moving forward.

Introduction

The successful demonstration of SmartGrid capabilities at KCP&L includes achieving the three cyber security goals: Confidentiality, Integrity, and Availability (CIA) of the data being processed, stored, and transmitted by the SmartGrid systems. These goals can be attained with a strategic and carefully crafted risk management program. As one of the first steps of a successful risk management program, a good risk assessment provides a realistic risk rating utilizing a uniform, repeatable process and measurable criteria.

To obtain useful risk ratings, the same measurement criteria must be applied consistently for every system without partiality or influence added to any one aspect. In this way, decision makers may be confident that an assessed risk rating is an accurate measure relative to all systems within scope of the risk assessment, and can be used to evaluate and prioritize mitigation actions.

In order to present somewhat subjective criteria in a quantifiable and measurable manner, this assessment utilized a uniform series of evaluation criteria. These criteria were used to evaluate five variables of a risk rating model: Threat Sources, Vulnerabilities, Likelihood, Impact, and Existing Mitigations. The output of each preliminary evaluation was passed through the risk rating model shown below and calculated to produce the final risk rating.

$$\text{Risk} = \text{Threat} + \text{Vulnerability} + \text{Likelihood} + \text{Impact} - \text{Mitigation}$$

$$R = T + V + L + I - M$$

Sections 2.0, 3.0, 4.0, 5.0, and 6.0 of this report describe in detail how the risk assessment team arrived at the values used in the risk rating model. Each of those sections provides evaluation criteria for each SmartGrid system to be input into the risk rating model. Although the assessment used a formula to calculate relative overall risk to each SmartGrid system, it is important to understand that the risk rating model is not necessarily a mathematical problem to be solved. It is merely a template for consistently applying the chosen criteria in order to provide measurable and reliable risk ratings.

In strict mathematical terms, it is evident from the model that increasing mitigations or decreasing threats, vulnerabilities, likelihood, or impact will decrease the level of risk. In other words, a higher mitigation rating lowers a system's risk. Similarly, lowering the threat, vulnerability, likelihood, or impact ratings lowers a system's risk. However in practical terms, mitigations are applied to systems to guard vulnerabilities, decrease the likelihood of an attack, or minimize the overall impact of an attack. The

model also conveys that applying more mitigations will always lead to less risk, but a balance is required to ensure that adding more mitigations does not result in diminishing returns.

In order to properly understand the contents and output of sections 2.0 through 6.0, the criteria and rating systems used to arrive at the variable values for each SmartGrid system must first be understood.

Threat Source (T): The value for T was measured on a scale of 0-10, with 0 being no relevant threats and 10 being all identified threats.

Vulnerabilities (V): The value for V was calculated as an aggregate total of Technical Ease and Ease of Access. Those sub criteria were evaluated and given values between 0-10.

Likelihood (L): The value for L was measured on a scale of 0-10, with 0 being negligible likelihood of a threat source exercising any vulnerability on a system, and 10 being a very high likelihood.

Impact (I): The value for I was measured on a scale of 0-10, with 2 being very low impact to the system if a vulnerability were to be successfully exploited, and 10 being very high impact.

Existing Mitigations (M): The value for M was calculated (with maximum possible rating of 30) based on percentage of proposed security controls believed to be already met by the KCP&L Policies, Standards, and/or Processes, in one of risk model components: V, L, or I.

The risk assessment performed for the KCP&L SmartGrid Demonstration Project is primarily based on the National Institute of Standards and Technology (NIST) specified guidelines in NIST SP 800-30⁷. The evaluations of security controls were performed based on the guidelines presented in the NIST Interagency Report, NISTIR-7628, Volume-1.⁸ Assessors used several other federal government and public sources throughout the process and such sources are appropriately cited in the report.

⁷ NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems.
<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

⁸ National Institute of Standards and Technology Interagency Report 7628.
http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf



A risk assessment provides limited value without a comprehensive plan to address the risks identified. In standard Governance, Risk, and Compliance management, there are four common ways to deal with identified risk: Avoidance, Transference, Mitigation, and Acceptance.

Risk Avoidance: Avoiding risk involves removing vulnerabilities or ceasing the vulnerable or otherwise risky behavior.

Risk Transference: Transference, in this instance, refers to shifting the burden of loss to another party, as in the purchase of an insurance policy.

Risk Mitigation: Mitigating risk is the process of systematically reducing the likelihood or impact of vulnerabilities.

Risk Acceptance: Accepting risk is an informed and conscious decision to accept the consequences and likelihood of a particular vulnerability or risk.

Of the four, Mitigation is by far the most common reaction to identified risks. The term "mitigation" can cover a broad range of actions, including: the creation of policies and procedures, identifying and applying system patches and updates, performing regular backups of critical data, developing robust configuration and change management processes, and any number of similar actions.

The assessment produced a number of additional recommended security controls and other recommendations for consideration. The final sections outline high level plans for prioritizing and implementing those recommendations.

The risk management lifecycle is a continuous loop of evaluating risk, implementing appropriate policies and controls, educating users and promoting risk awareness, and monitoring and evaluating the effectiveness of implemented controls. This risk assessment is the just the first step in the risk management lifecycle for the SmartGrid systems.



1.0 SYSTEM CHARACTERIZATION

The first step for a comprehensive risk assessment is to ensure that all the information system components are clearly identified and the system boundaries are carefully delineated. As evident, the KCP&L SmartGrid Demonstration Project (hereafter called the "project") is a collection of several smart systems that belong to different "Smart Grid Domains", thereby making the project a "system of systems". Thus the activity of accurately identifying the systems and their interfaces is crucial in defining the real boundaries of the project.

1.1 SYSTEM-RELATED INFORMATION

The widely accepted NIST Special Publication 800-30 was used as the guiding document for collecting information and performing the risk assessment for the project. A complete review of the project documentation was performed, which was followed by targeted questionnaires sent to the Subject Matter Experts (SMEs) to lay the foundation of the risk assessment effort. The SMEs' responses were studied and then discussed in focus group interviews. In parallel, the use cases of all the systems were studied and business functions were discussed with the SMEs. The results of the process led to classification of each application into one of the several "Smart Grid Domains". These domains can be best viewed as logical groupings of systems based on either the similarity of business functions they perform or their implementation. These logical groupings are primarily based on the guidelines provided in the NIST Interagency Report 7628 (commonly referred as the NISTIR-7628). The "Smart Grid Domains" suggested in the NISTIR-7628 are Transmission, Distribution, Operations, Bulk Generation, Markets, Customer, and Service Provider. However, as every implementation of the SmartGrid suite is unique, it is important to take NIST guidelines and tailor them to best fit KCP&L's implementation.

After studying the KCP&L SmartGrid systems, it was determined that the NISTIR-7628 domains would need to be extended to accomplish this. As such the Operations domain was divided to represent two classes of SmartGrid operations: Energy Management and Consumer Management. In addition, it was determined that the Transmission, Bulk Generation, and Markets domains were not applicable to any systems in the project.

* Smart Grid Domains are elaborately defined in the National Institute of Standards and Technology Interagency Report 7628. http://csrc.nist.gov/publications/nistir/n7628/nistir-7628_vol1.pdf

The following list provides a brief description of the extended SmartGrid domains unique to KCP&L's implementation.

Customer Facing Operations: All systems that aide or perform the business functions of managing energy consumption. These systems can be accessed* either by the consumer or the utility.

Examples: AccountLink (ALNK) and Home Energy Management Portal (HEMP)

*Access - Can be either through a Graphical User Interface (GUI) or a Data Interface.

Utility Operations: All systems contributing towards the supply, control, and management of energy from the utility to the consumer. Access to these systems is limited only to the utility.

Examples: Distribution Management System (DMS) and Customer Information System (CIS)

Field Distribution: The collection of systems that typically reside in the field and provide measurements or asset locations. Access to these systems is limited only to the utility.

Examples: SmartMeter (MTR) and Distributed Control and Data Acquisition (DCADA)

Customer: The collection of systems and devices that reside at the customer location and aide in usage management. These systems can be accessed either by the consumer or the utility.

Examples: Building Management System (BMS), Home Area Network Gateway (HANG), and Home Area Network Devices (HANDs)

Service Provider: The collection of systems that provide aggregation services or third-party analysis to the consumer(s) or the utility. These systems can be accessed either by the consumer, an authorized third-party, or the utility.

Example: Data Mining and Analysis Tool (DMAT)

Table 1-1 lists the classifications of all KCP&L SmartGrid systems according to the extended SmartGrid domains. A brief description of each system is provided in Appendix C.

System	Utility Operations	Customer Facing Operations	Field Distribution	Customer	Service Provider
AHE			X		
ALNK		X			
BMS				X	
CIS	X				
DCADA			X		
DER - C&I				X	
DER - Grid-Connected			X		
DERM	X				
DER - Residential				X	
DMAT					X
DMS	X				
EMS	X				
Field DADs			X		
GIS	X				
HANDs				X	
ILANG				X	
HEMP		X			
MDM	X				
MTR			X		
MWFM	X				
Substation DADs			X		

Table 1-1. System Classifications in the Extended Smart Grid Domains

Before threats, vulnerabilities, impacts, likelihood, and risks of each system could be assessed, the next logical step was to classify the communication paths (interfaces) between the SmartGrid systems. The classification of interfaces is necessary, as the security profile and requirements of the grouped interfaces are likely to have a common set of controls. The guidelines provided in NISTIR-7628 Volume-I for "Logical Interface Categories"¹¹ are extremely helpful in this respect. With aid from KCP&L SMEs, all the known project interfaces were mapped to these Logical Interface Categories. This mapping is shown in Appendix B. The mapping includes the following for each project interface:

- KCP&L interface number
- Systems involved
- Applicable NISTIR-7628 Logical Interface
- Applicable NISTIR-7628 Logical Interface Category and Description

Of the twenty-two NISTIR-7628 Volume-I Logical Interface Categories, thirteen were found to be applicable to the project. This can be seen in the following table, Table 1-2.

¹¹ National Institute of Standards and Technology Interagency Report 7628
http://csrc.nist.gov/publications/nistir/tr7628/nistir-7628_vol1.pdf

NISTIR-7628 Logical Interface Category	NISTIR-7628 Logical Interface Category Description
1	Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints
2	Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints
3	Interface between control systems and equipment with high availability, without compute nor bandwidth constraints
5	Interface between control systems within the same organization
7	Interface between back office systems under common management authority
8	Interface between back office systems not under common management authority
9	Interface with B2B connections between systems usually involving financial or market transactions
10	Interface between control systems and non-control/corporate systems
11	Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements
13	Interface between systems that use the AMI network
14	Interface between systems that use the AMI network with high availability
15	Interface between systems that use customer (residential, commercial, and industrial) site networks
16	Interface between external systems and the customer site

Table 1-2 Applicable NISTIR-7628 Volume-I Logical Interface Categories



2.0 THREAT IDENTIFICATION

The purpose of this section is to identify the various threats which may pose a risk to the KCP&L SmartGrid Demonstration Project systems, data, or network and communication infrastructure. NIST SP 800-30 defines a threat as:

“...the potential for a particular threat source to successfully exercise a particular vulnerability.”¹¹

Because a Likelihood value was added to the Risk Rating Model for this assessment, the definition of a threat was modified. For this risk assessment, a threat, by itself, was not presumed to indicate the presence of risk to a system or network. Looking again at the risk calculation model, a threat requires the presence of a system or network vulnerability in order to present any level of risk. As such, only the threat sources that were determined to have the capability to exploit one or more system vulnerabilities were considered in this assessment. A threat can be internal or external, but generally cannot be influenced by KCP&L actions. The security controls discussed later in this report are intended to mitigate the risk posed by specific threat sources, vulnerabilities, or impacts—not to directly influence threats.

2.1 THREAT SOURCE IDENTIFICATION

A threat source, sometimes referred to as a threat vector, can be defined as

“... a path or a tool that a Threat Actor uses to attack the target.”¹²

An attack on a target is not necessarily an intentional action, nor is the Threat Actor always a human. An attack, in this instance, is any event which has the potential to impact the confidentiality, integrity, or availability of a system, or the data generated, stored, or transmitted by that system. A Threat Actor is the source of any event, be it a human, an object, or the force of nature. Often, threats are viewed as strictly malicious or intentional. This report uses a broad definition of a threat, to include unintentional acts and natural occurrences.

Threats are commonly grouped into three categories: natural, human, and environmental. Each category contains possible threat sources which must be identified and evaluated to determine if there is opportunity and likelihood for that threat source to exercise an existing or potential vulnerability. In

¹¹ U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, *Special Publication 800-30: Risk Management Guide for Information Technology Systems*, July 2002

¹² Phil Withers, “Information Security Threat Vectors”, <http://isaca-va.org/Threat%20Vectors.pdf>

practical terms, it is not possible to determine every possible threat or vulnerability. KCP&L should perform further periodic risk analyses as new threats or vulnerabilities are discovered. This section will describe the current threat sources identified during the risk assessment. To prevent the implication that one threat source is more likely or serious than another, the following threat sources are listed in alphabetical order.

2.1.1 Acts of Nature

An Act of Nature can threaten facilities, systems, personnel, vital utility infrastructure, and physical operations of SmartGrid systems. The assessment determined that the project is susceptible to a variety of natural disturbances. The likelihood of any individual occurrence impacting the SmartGrid systems is detailed in Section 4.0 of this report, but the most common sources pertaining to an Act of Nature for the area in and around Kansas City include:

Wind Damage: This threat includes damaging winds and flying debris. An occurrence of this threat may also include additional threat sources such as Dependency Failures (personnel or system), Physical Intrusion and/or Theft (looting), or System and Environmental Failures (power failure).

Floods: This threat primarily concerns large scale flooding from nearby streams and rivers. On a smaller scale, this threat may also include localized flash flooding from non-tornadic severe thunderstorms.

Lightning: The largest threat posed by lightning are cloud-to-ground flashes, however, intra-cloud and inter-cloud lightning may also cause brief interference on radio frequency (RF) communications.

Ice: The ice threat refers to both large-scale ice producing storms which may cause damage to infrastructure, as well as localized ice formation which may injure personnel.

2.1.2 Autonomous Systems and Malicious Code

This threat source is most commonly identified with viruses or self-replicating malware such as the recent Stuxnet worm. However, any cyber asset connected to a network may be subjected to a wide range of threats in this category, including such things as:¹¹

Viruses: A program or programming code that replicates by being copied or initiating its copying to another program, computer boot sector, or document.

¹¹ All definitions courtesy of <http://searchsecurity.techtarget.com/>.

Worms: A self-replicating virus that does not alter files but resides in active memory and duplicates itself.

Trojan Horses: A program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do some intended form of damage.

Spyware: Programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties.

2.1.3 Dependency Failures

An often overlooked threat source is the failure of another system or service outside the direct control of the system owner, which harms or interferes with its ability to function. Events included in dependency failures also include personnel dependencies. The assessment determined the systems within the project may be susceptible to the following dependency failure threats:

Power Failures: This threat may be localized or wide-spread and affect multiple areas of the project.

Downstream Processing Failures: Downstream threats may interfere with data processing, communications, or reporting and may have a negative impact on a system.

System Administrator or SME Job Termination or Reassignment: Loss of key personnel may reduce efficiency of operations and potentially impact system performance.

Failure of a Service or Control Owned by Another Entity Within KCP&L: Loss of processing, data storage, or communications required for optimal operation of a system.

2.1.4 Errors and Omissions

A common internal threat source is an authorized individual performing an inadvertently disruptive or even destructive action. These actions are sometimes difficult to prevent, even with robust change management and quality control programs. Errors can and do happen, even in the most robust environments. Some threats of this source which may impact the project are:

Network Configuration Errors: Mis-configured Network Infrastructure which produces an unintentional vulnerability.

Security Configuration Errors: Poorly written or implemented firewall or other security boundary rules.

Improper Change Management: Performing maintenance on the wrong system (primary instead of secondary, for example).

Improper Configuration Management: Poorly written administration scripts or batch files which create an adverse condition.

Incomplete System Identification: Mislabeling systems or neglecting to update system documentation resulting in confusion or a potential outage situation.

2.1.5 External Attack

This is the threat source most often referenced in the media and identified with cyber security. Threats in this category bring to mind the classic hacker image and are nearly universally applicable for any system connected to an external network, either directly or through intermediate systems. An external network most often refers to the Internet, however, any network outside an existing security boundary, especially those not managed by KCP&L, qualifies as an untrusted external network. The most common examples of external attack which may affect the project are:

System Compromise: This is the classic hacking attack which provides an intruder with elevated privileges, unauthorized access to processes and data, or complete control of a system.

Data and Account Harvesting: This threat is usually an attempt to crack passwords in order to gain unauthorized access, but can also lead to an intruder impersonating a legitimate user in an effort to gain access to more sensitive data or systems.

Website Defacement: Public websites are the online face of KCP&L. Malicious or prank alterations of those public websites may cause damage to the reputation or public image of KCP&L.

Computer Crime: The primary goal of a computer criminal is usually monetary gain. This is one threat in which identity theft may be categorized.

Password Guessing: This threat is related to Data and Account Harvesting, although much less sophisticated and often easier to detect.

Denial of Service: This attack attempts to deny access to a cyber asset or assets. It can often be used as a form of blackmail, but can also be a sign of an attempted spoofing attack on another system.

Social Engineering: This threat can be defined as "...the act of manipulating a person to accomplish goals that may or may not be in the "target's" best interest. This may include obtaining information, gaining access, or getting the target to take certain action."¹⁴

2.1.6 Insider Abuse and Unauthorized Acts

Although not intentionally malicious in nature, abusing company resources to perform unauthorized, illegal, or inappropriate actions may have unintended consequences which may cause disruption or harm. This threat source can be difficult to detect without active monitoring of employee activities. Threats in this source which may adversely impact the project include:

Sharing or Distribution of Copyrighted Material: Downloading unauthorized copies of music, movies, or other copyrighted material for personal gain, or utilizing file sharing applications on corporate IT systems.

Invasion of Privacy: Unauthorized attempts to access personally identifiable information, defined as "...any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual."¹⁵

Unauthorized Exploration of Computer Systems: Reconnaissance or mapping of networks without express written consent of the network or system owner(s).

Use of Computing Resources to Harass Others: Threatening or demeaning electronic communication which creates "...an unpleasant or hostile situation for especially by uninvited and unwelcome verbal or physical conduct."¹⁶

Disregard for or Actively Circumventing Security Controls: Refusing to implement or comply with required security controls, disabling active security controls, or performing actions intended to work around required security controls.

¹⁴Chris Hadnagy, <http://www.social-engineer.org/>

¹⁵ Executive Office of the President, Office of Management and Budget, M-06-19 Memorandum for Chief Information Officers, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006

¹⁶ Merriam-Webster Online Dictionary, 2011. <http://www.merriam-webster.com>

Use of Computing Resources to Perform Illegal Acts: Accessing or attempting to access information or locations which violate local ordinances, state, or Federal law, such as online gambling, child pornography, seditious or anarchist websites, or sites espousing or financing threats against the government.

2.1.7 Insider Attack

Although sometimes overlooked, the insider attack threat source is the most common and most difficult to defend against. Similar in nature to the external attack threat source, an inside attacker has many advantages, possibly including authorized access, with which to perform and hide the attack. The KCP&L SmartGrid Demonstration Project systems, as with any systems, provide many opportunities for insider attack, including:

System Compromise: This is the classic hacking attack which provides an intruder with elevated privileges, unauthorized access to processes and data, or complete control of a system.

Escalation of Privileges: Attempts to gain access to information, systems, technical capabilities, or physical locations to which the individual is not authorized.

Electronic Eavesdropping: Unauthorized access or installation of surveillance devices or software for the purpose of obtaining information which would otherwise be unavailable.

Password Guessing: This threat is usually an attempt to ascertain another user's login credentials in order to gain unauthorized access, but can also lead to an intruder impersonating a legitimate user in an effort to gain access to more sensitive data or systems.

Denial of Service: This attack attempts to deny access to a cyber asset or assets. It can often be used as a form of blackmail, but can also be a sign of an attempted spoofing attack on another system.

Social Engineering: This threat can be defined as "...the act of manipulating a person to accomplish goals that may or may not be in the "target's" best interest. This may include obtaining information, gaining access, or getting the target to take certain action."¹⁷

¹⁷Chris Hadnagy, <http://www.social-engineer.org/>

2.1.8 Legal and Administrative Actions

This threat source is usually the result of failure to comply with regulatory requirements, or unauthorized or illegal actions performed on systems, including the activation of malicious software. Law enforcement or administrative measures in response to those actions may result in an adverse effect on the KCP&L SmartGrid Demonstration Project systems. Threats from legal or administrative actions may include:

Regulatory Findings and Penalties: Internal or external audit findings which result in significant changes to a system which may temporarily impact performance or availability.

Law Enforcement Proceedings Resulting in System Seizure: Investigative measures resulting in the complete loss of a system for forensic analysis or evidential material.

2.1.9 Physical Intrusion and/or Theft

The compromise of a facility or theft of physical resources can pose a significant threat to both the operational capability of the KCP&L SmartGrid systems and the reputation of the company. In this instance, a physical resource refers to more than systems. Theft may also affect items such as proprietary or confidential hard-copy printouts, employee access badges or tokens, and copper or other metals.

Theft can also include non-physical resources such as company data, personal customer information, or passwords.

2.1.10 System and Environmental Failures

This threat source is one of the most commonly recognized and mitigated, and is only occasionally the result of human actions. There are many threats associated with this source, but they can be condensed into generic types. Some of the most common types of threats in this source which may affect the project are:

System Hardware Failures: Malfunction or interruption of hardware devices essential to the function of the system.

Environmental Control Failures: Disruption of systems or devices managing the local environment which houses the system, such as HVAC, humidity, or electronic emissions control.

Software or Data Corruption: Inadvertent altering of system applications, local or offsite system information, or system firmware.

2.1.11 Violent Acts of Man

The violence indicated by this threat source includes not only violence directed against KCP&L personnel or systems, but also violence on a regional or local level that results in indirect harm or dependency failure. Examples of violent threats which may affect the project include:

Riots: Violent public disorder or widespread disturbance of the peace.

Gang-Related Violence: Planned or spontaneous incidents involving members of criminal gangs, which result in damage or disruption to systems.

Domestic Incidents: Violent disturbances within or around a household which damage or disrupt a system.

Random Acts of Violence: Unplanned and unaccountable violence perpetrated with no apparent or logical pattern or motivation.

In order to determine a consistent threat rating for the risk calculation model, each threat source was evaluated to determine if it had a chance to impact a given system. The value for this variable is a total number of potential threat sources which may affect the system. The exception is the Acts of Nature threat source, which is assumed to affect every system, and is therefore omitted from the risk calculations. The results of the threat determination calculation are shown in Table 2-1.

System	Identified Threat Sources	Total Number of Potential Threat Sources
AHE	2, 3, 4, 5, 6, 7, 8, 10	8
ALNF	2, 3, 4, 5, 6, 7, 8, 10	8
BMS	2, 3, 4, 5, 6, 8, 10	7
CIS	3, 4, 5, 6, 7, 8, 10	7
DADs (Field and Substation)	3, 4, 5, 7, 9, 11	6
DCADA	3, 4, 5, 6, 7, 8, 10, 11	8
DER - C&I	3, 4, 5, 9, 10, 11	6
DER - Grid-Connected	3, 4, 5, 9, 10, 11	6
DERM	2, 4, 5, 7, 8, 10	6
DER - Residential	3, 4, 5, 9, 10, 11	6
DMAT	3, 4, 6, 7, 10	5
DMS	2, 3, 4, 5, 6, 7, 8, 10	8
EMS	2, 3, 4, 5, 6, 7, 8, 10	8
GIS	2, 3, 4, 6, 7, 8, 10	7
HAND/HANG	3, 5, 8, 9, 10, 11	6
HEMP	2, 3, 4, 5, 7, 8, 10	7
MDM	2, 3, 4, 5, 6, 7, 8, 10	8
MTR	3, 4, 5, 6, 8, 9, 10, 11	8
MWFM	3, 4, 5, 7, 8, 9, 11	7

Table 2-1 Threat Determination Calculation Results



Likelihood and impact levels are discussed later in this report, so it is important to note that this threat rating is only indicating the presence of a threat source with the potential to exercise system vulnerabilities, not the presence of any vulnerability, or the likelihood or impact of such an event.

2.2 MOTIVATION AND THREAT ACTIONS

To assist in determining if a threat source may pose a risk to a specific system, it is important to determine what motivation, if any, a threat source may have to exploit one or more vulnerabilities on that system.

Determining threat motivations is restricted to intentional human threats, since natural, environmental, and inadvertent threats are not premeditated and have no motivation to assess. The motivation for a human threat will vary depending upon the type of threat source. For example, a hacker will have a different motivation to attempt to penetrate the KCP&L SmartGrid Demonstration network than a computer criminal (challenge or ego vs. profit).

Table 2-2 lists the intentional human threat sources described above and assigns potential motivations for each. This table is not intended to imply that these are the only possible motivations, only to give examples of common possible motivations in order to provide guidance in determining if a threat source may pose a risk to a selected system.

As can be seen in Table 2-2, many of the motivations are similar for various threat sources, however, different sources will use varying threat actions to achieve a goal, even if their motivations are the same.

KCP&L SmartGrid
 Demonstration Project
 Risk Assessment Report

Threat Identification

Threat Source	Potential Motivations	Possible Threat Actions
Autonomous Systems and Malicious Code	<ul style="list-style-type: none"> • Ego/Notoriety • Destruction or Unauthorized Disclosure of Data • Unauthorized Data Alteration • Profit • Blackmail • Revenge 	<ul style="list-style-type: none"> • Broad-Reaching, Self-Replicating Malware (i.e. Code Red) • Targeted Malware (i.e. Stuxnet) • Spyware & Adware Proliferation • System Control Malware (i.e. Win32/Winwebsec)
External Attack	<ul style="list-style-type: none"> • Challenge • Ego/Notoriety • Destruction or Unauthorized Disclosure of Data • Unauthorized Data Alteration • Industrial Espionage • Blackmail • Revenge 	<ul style="list-style-type: none"> • Hacking • Social Engineering • Unauthorized Privilege Escalation • Spoofing • System Attack (DDoS) • Terrorism
Insider Abuse and Unauthorized Acts	<ul style="list-style-type: none"> • None (Poorly Trained Personnel) • Ego • Harassment/Stalking • Curiosity 	<ul style="list-style-type: none"> • Computer Abuse • Bypassing Security Controls • Browning Proprietary or Confidential Data • Pirating Software
Inside Attack	<ul style="list-style-type: none"> • Challenge • Ego/Notoriety • Curiosity • Profit • Destruction or Unauthorized Disclosure of Data • Unauthorized Data Alteration • Blackmail • Revenge 	<ul style="list-style-type: none"> • Hacking • Social Engineering • Spoofing • Assault • Malicious Code • Unauthorized Privilege Escalation
Legal and Administrative Actions	<ul style="list-style-type: none"> • Law Enforcement Investigation • Audit Findings • Litigation 	<ul style="list-style-type: none"> • System Seizure • Overly Stringent Security Controls • Legal Hold
Physical Intrusion and/or Theft	<ul style="list-style-type: none"> • Challenge • Ego/Notoriety • Curiosity • Profit • Destruction of Systems • Blackmail • Revenge 	<ul style="list-style-type: none"> • Jumping or Cutting Fences • Picking or Destroying Physical Locks • Assault • Terrorism
Violent Acts of Man	<ul style="list-style-type: none"> • Ego • Protest • Territory Infighting 	<ul style="list-style-type: none"> • Assault • Looting • Random Gunfire

Table 2-2 Threat Source Motivations and Threat Actions



3.0 VULNERABILITY ASSESSMENT

For a large program like the KCP&L SmartGrid Demonstration Project, measuring each system's relative weakness for sets of vulnerabilities was the taken approach for the risk assessment. The goal of this assessment was to identify the relative risk level of all SmartGrid systems. As the established model suggests, the vulnerabilities of each system play a large role in the relative risk level determination. For this report, the risk assessment team analyzed the vulnerabilities for each system using a high level approach. Each application was evaluated for broad sets of vulnerabilities that range from system to operational. This approach worked well and produced credible results, especially for several systems that needed to be evaluated whose implementation was still in the early stages at the time this risk assessment was performed.

3.1 VULNERABILITY SOURCES

Vulnerability sources primarily lie in two categories: systems or operations. Within the systems category, it is beneficial to look at generic vulnerabilities that threaten one of the three cyber security goals: Confidentiality, Integrity, and Availability. Operational vulnerabilities, on the other hand, are internal to the organization, and as such, are better assessed in the categories of People, Policy, and Procedures.

The system set of vulnerabilities are either inherited from the original equipment manufacturer (operating systems, firewalls, firmware, third-party software, etc.) or from security oversight during the in-house Software Development Life Cycle (SDLC) process. Unfortunately, the eventual user (in this case, KCP&L) has little or no control in eliminating the threats, but many actions can be taken to guard the vulnerable points. System vulnerabilities can be guarded by placing a combination of security controls like hardening the operating system, utilizing Access Control Lists (ACLs) or firewalls, and implementing secure networks such as Virtual Private Networks (VPNs).

Operational vulnerabilities can be controlled by existing policies enhancement, managerial enforcement, and close monitoring. A list of all known system and operational vulnerabilities that could adversely affect the organization can be found through many credible agencies like the National Labs, Department of Homeland Security (DHS), National Domestic Preparedness Coalition, and vulnerability databases like the National Vulnerability Database (NVD) and Open Web Application Security Project (OWASP)¹⁶. Their applicability to the KCP&L project, however, should be looked at on a case-by-case basis. The

¹⁶ NISTIR-7628 Volume-III http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf

intent of this section is to provide a high-level understanding of the types of vulnerabilities that exists in each category.

3.1.1 Confidentiality Vulnerabilities

This set of vulnerabilities directly threatens the confidentiality of the data stored or processed in the systems. Insufficient authentication and authorization mechanisms give an attacker easy access to classified data. Inadequate data encryption during data transmission provides attackers the means to “sniff” through sensitive material. Insufficient logging and auditing procedures allow an attacker to learn about the system settings and clear its traces once the “intrusion” is over. Holes in the password protection processes provide an attacker access to otherwise restricted areas.

3.1.2 Integrity Vulnerabilities

Vulnerabilities that directly threaten the integrity of a system or its data usually arise from negligence in the SDLC process. Attackers often use this set of vulnerabilities when their motive is not to steal but to create disruption to normal business operations. For such attackers, poorly coded systems or unprotected code repositories are gold mines to be exploited. Inadequate input data ranges and counters are often seen as attack vectors, which can lead to the systems being unreliable. Protocols and communication mediums that do not provide enough protection during data transfer give attackers mechanisms to compromise data integrity. Network devices that do not verify the integrity of data packets against the implemented protocol provide weaker openings that are more susceptible to attacks.

3.1.3 Availability Vulnerabilities

Vulnerabilities exploited in this set result in unavailability of the information system or its data for several hours or in extreme cases, several days. Networks not designed with the philosophy of creating protection zones allow an attacker to inundate applications with rouge requests, resulting in system unavailability and crashes. A type of unavailability attack common to Internet-facing applications is referred to as a Denial-of-Service (DoS) attack. Applications deployed without adequate system redundancy result in complete unavailability during times of forced (attacks) or planned (maintenance) outage events.

3.1.4 Policy Vulnerabilities

The security policy of an organization provides the foundation for protecting information systems against potential threats. Up until the introduction of Advanced Metering Infrastructure (AMI), utilities’ IT departments’ touchpoints never entered consumer homes. A failure to adjust the security policy to provide protection related to the extended touchpoints may open doors for attackers to penetrate KCP&L.



environments. In addition, new systems such as the AMLHead-End (AHE) will collect more granular data that could be used to draw inferences about the consumers' usage patterns. This data is considered private by many consumers. As such, a security policy that does not cover restricted access allows a malicious user to freely review private data.

3.1.5 People Vulnerabilities

New business offerings bring new cyber challenges, masking the implementation of good security controls paramount to the success of the project. Further, any sound security implementation requires an equally sound training program. The annual training program for KCP&L employees covers the existing business processes and technologies. However, the introduction of several SmartGrid technologies at KCP&L requires enhancement to the training programs to cover consumer privacy, new standards, and industry best practices. The KCP&L SmartGrid system users and implementers should not be expected to keep systems secure without adequate cyber security training in the SmartGrid domain. An oversight in training may lead to accidental cyber compromise or suboptimal security infrastructure.

3.1.6 Procedural Vulnerabilities

The multi-vendor profile of the project creates opportunities for inconsistencies in configurations, code changes, and patches for system maintenance. Each vendor's development, testing, and implementation timelines for patches and functionality upgrades usually follow different paths, thus opening up windows of exploitations. One of the big challenges in a multi-vendor program such as the KCP&L demonstration project is the coordination of changes to the production environments. Mismatches and frequent releases in the production environment, if not controlled carefully, may result in either system and/or data unavailability or compromised integrity. SmartGrid systems also require additional attention during regression testing, as the patches and upgrades to one system may trigger functional issues in other system(s). An oversight in configuration documentation and disaster recovery processes may also leave systems vulnerable.

3.2 VULNERABILITY RATINGS

The intent of this section is first to introduce a vulnerability rating method and then to evaluate a rating for each of the KCP&L SmartGrid systems. The method was designed to evaluate a Relative Vulnerability Rating (RVR) of each system by looking at the project as a whole. As such, these RVRs should not be used in situations where the requirement is to find a system's stand-alone vulnerability level and not a relative vulnerability level with respect to the other KCP&L SmartGrid systems. To assign a RVR, the first question to answer for each system was, "Relative to other systems, how technically easy

is it to exploit a vulnerability?" For example, EMS and DMS require high technical skills to be exploited and hence their Tech Ease Vulnerability Factor (TEVF) is relatively low. The second question to be answered was, "Relative to other systems, how easy is it to gain access to parts of the assessed system?" Since HEMP is an Internet-facing application, its Ease of Access Vulnerability Factor (EAVF) is relatively high. These two questions were first answered on a qualitative scale ranging from Negligible to Very High and then converted to a numerical representation using a scale of 0 to 10 (0 = Negligible, 2 = Very Low, 4 = Low, 6 = Medium, 8 = High, 10 = Very High).

The overall relative vulnerability rating for each system was then calculated using the formula:

$$RVR = TEVF + EAVF$$

Where:

RVR = Relative Vulnerability Rating

TEVF = Technical Ease Vulnerability Factor

EAVF = Ease of Access Vulnerability Factor

Thus, the values for RVR for the SmartGrid systems ranged from 0 to 10.

3.3 VULNERABILITY ASSESSMENT

The following subsections list the assessment of each planned system in the KCP&L SmartGrid Demonstration Project.

3.3.1 AMI Head-End (AHE)

At the time that this report was developed, the AHE was planned to be hosted external to KCP&L's environment. To perform a thorough assessment, a full review of the vendor's security policy was conducted. The vendor has appropriate focus in securing systems it supports, but the implementation needs to be tested and verified. The TEVF was determined to be Medium (3) because the RF mesh network being utilized and its vulnerabilities are well understood and do not require a very skilled person to coordinate an attack. The EAVF was also found to be Medium (3) because the RF mesh network is physically accessible to the public.

3.3.2 AccountLink (ALNK)

Since ALNK has an Internet-facing customer interface and is implemented with very well-known Internet technologies, its TEVF was determined to be High (4). The EAVF was also determined to be High (4) for two primary reasons. First, gaining access to customer account login information is relatively easy through the use of social engineering techniques. Second, the access point is available to anyone who has access to the World Wide Web.

3.3.3 Building Management System (BMS)

The BMS is envisioned to be third-party software installed at commercial and industrial customer sites to manage their Distributed Energy Resources (DER). A thorough vulnerability assessment was deferred because the technology, control mechanism, and protocols were not completely defined when this risk assessment was performed. However, from the little that was known, the TEVF was believed to be Low (2) due to the fact that the BMS (much like the EMS) requires highly technical skills to cause damage. The EAVF was believed to be Medium (3) because the control signals will likely be sent using VPN connections via the Internet.

3.3.4 Customer Information System (CIS)

Due to the many installations of CIS in the utility industry, the technology and the inner workings of the application are very well-known. As a result, the TEVF was determined to be Medium (3). The EAVF was also determined to be Medium (3) because the CIS is well-protected inside the KCP&L network.

3.3.5 Distributed Control and Data Acquisition (DCADA)

The DCADA system is comprised of highly technical information subsystems with complex engineering algorithms. An attacker would have to be very well-versed in engineering applications to cause any damage to these subsystems. As a result, the TEVF for DCADA was estimated to be Low (2). Since access to this application is both electronically and physically designed to be restricted, the only vulnerable points are the connection points between it and the Field and Substation Distribution Automation Devices (DADs). The resultant EAVF was therefore estimated to be Medium (3).

3.3.6 Distributed Energy Resources – Commercial & Industrial (DER – C&I)

The DER - C&I will be managed directly by commercial and industrial customers through their BMS. These resources and their technologies were not completely known at the time of writing this report. Therefore, a thorough risk assessment on DER - C&I could not be done. From the little that was known, the TEVF was estimated to be Low (2) as the technologies are less understood in the attacker community.



The EAVF was estimated to be Medium (3) since the number of implementations is expected to grow, creating new avenues to penetrate. Also, each implementation may not have stringent security measures in place.

3.3.7 Distributed Energy Resources – Grid-Connected (DER – Grid-Connected)

The DER – Grid-Connected will be owned and managed by KCP&L. The first installation will include a battery with a generation management system. The TEVF was determined to be Low (2) because it will require an attacker to understand not only the control logic of battery operations, but also the generation management system. The EAVF, however, was estimated to be Medium (3) because there is more than one communication interface planned for the battery: one from DCADA to send DR signals and the other from a remote location (battery vendor) to manage configurations.

3.3.8 Distributed Energy Resource Management System (DERM)

The DERM will be used to manage DR calculations and requests. This system is planned to be hosted at a vendor site. Any vulnerability at the vendor site could be exploited to affect KCP&L operations. A review of the vendor's security principles was conducted and the results were found to be focused in addressing security needs. However, testing and verification is needed to confirm the implementation. The TEVF was determined to be Medium (3) due to the known vulnerabilities in the communication channels. In addition, since the communication channels between the DERM and KCP&L is planned to be over external networks, the EAVF was determined to be High (4).

3.3.9 Distributed Energy Resources – Residential (DER – Residential)

The DER – Residential will be comprised of customer-managed demand response units and load curtailment units that will be directly managed by KCP&L. The TEVF was determined to be Medium (3) because the control signals will traverse through various systems and devices with a mix of TEVF ratings. The EAVF, on the other hand, was estimated to be High (4) since the attacker will have multiple avenues (several exposed communication channels, systems, and devices) to modify DR signals.

3.3.10 Data Mining and Analysis Tool (DMAT)

The DMAT application is a third-party data mining tool hosted at a vendor site. The answers provided by the vendor in the security questionnaire were found to adequately address the existing security issues. The TEVF was found to be Low (2) because the vendor controls were determined to be satisfactory. However, the EAVF was determined to be Medium (3) due to the existence of several data interfaces between KCP&L and DMAT.

3.3.11 Distribution Management System (DMS)

This suite of applications is the coordinator of energy distribution and is built using complex engineering algorithms. Superior technical skills are required to create and manage this type of application. Thus, an attacker breaking into this application is not a trivial task, which made the TEVF Low (2). The ease of access was estimated to be limited since the DMS will not have many external access points, which also made the EAVF Low (2).

3.3.12 Energy Management System (EMS)

The EMS application (like the DMS) is built upon highly technical principles requiring a highly skilled attacker to exploit system vulnerabilities. The TEVF was therefore estimated to be Low (2). The EAVF was also estimated to be Low (2) because this system resides deep inside KCP&L protection zones.

3.3.13 Field and Substation Distribution Automation Devices (Field-DADs and Substation DADs)

The Distribution Automation Devices have control modules that are used to remotely manage the device functions. It requires a high knowledge of embedded systems to break into such devices, and in many cases, it requires physical access to make changes to the control modules. Due to the relatively high technical knowledge required to break into a DAD, the TEVF was estimated to be Low (2). Since many of these devices will be deployed in the field with less physical security around them, the EAVF was estimated to be Medium (3).

3.3.14 Geographic Information System (GIS)

The GIS application has been in use in many industries for some time, and the inner workings of these applications are not relatively complex. If there are routes available, breaking into these kinds of applications is relatively easy. Therefore, the appropriate TEVF was estimated to be Medium (3). The EAVF was determined to be Low (2) because this system resides inside the KCP&L corporate network (external entities do not have direct connections to it).

3.3.15 Home Area Network Devices and Gateway (HAND and HANG)

The HAN Device(s) and Gateway technologies are still at their nascent stages. Although progress has been made in securing home area networks and the devices connected to them, much work still needs to be done. At the time this report, many cyber security questions remained unanswered for the proposed primary protocol (ZigBee 1.0). Within the protocol stack, different network layers are not cryptographically separated, so access policies are needed and correct design is assumed. ZigBee uses

128-bit keys to implement its security mechanisms, which means different services must use different one-way variations of the link key in order to avoid leaks and security risks. As a result, the TEVF assigned to HANs and HANG was High (4). The EAVF was also determined to be High (4) because the HAN would exist in every participant's home and any one of those networks could become the target of an attack.

3.3.16 Home Energy Management Portal (HEMP)

The HEMP is the primary interface that KCP&L SmartGrid residential consumers will utilize to manage their HAN, participate in DR events, and view their energy usage. It is planned to be hosted at a vendor site. The TEVF was determined to be High (4) because HEMP is an Internet application. The primary determinant of the rating was the attacker community's awareness of this application being very impactful to KCP&L's reputation. The fact that this application is hosted at a vendor site (making KCP&L's security mandate indirect) also supports the High TEVF rating. The EAVF was also determined to be High (4) for two reasons. First, social engineering attempts with consumers can result in easy access, and second, the Internet interface, along with several connections to other systems, opens up multiple avenues for an attack.

3.3.17 Meter Data Management System (MDM)

The MDM acts as the repository of meter inventory and individual consumer usage. This system is hosted at a well-secured vendor site. The TEVF was found to be Low (2) because the encryption and security measures will require a skilled person to coordinate an attack. The EAVF was found to be Medium (3) because the MDM will have interfaces with multiple KCP&L systems, each one requiring data transmission external to KCP&L's corporate network.

3.3.18 SmartMeter (MTR)

MTR refers to the physical SmartMeter that resides on the consumer's premise. The MTR will have capabilities to perform several smart functions like capturing and storing consumer usage and accepting and executing remote connect or disconnect signals. This device has drawn a lot of attention lately from energy theft enablers and hackers. Even though the MTR has embedded systems which require high skill levels to break into, the motivation and desire in the attacker community is large enough that the TEVF was determined to be Medium (3). The EAVF was determined to be Very High (5) because the MTR will be at every consumer location and will have its own broadcasting network (communicates with the consumer's HANG using ZigBee 1.0 protocol).

3.3.19 Mobile Work Force Management System (MWFM)

MWFM is the system used by the field service dispatchers to solve customer issues that require a technician to visit the site. None of the SmartGrid systems will directly interface with the MWFM. The TEVF was determined to be Low (2) because the technical difficulty will be high for an attacker to break into multiple applications to gain access to MWFM. The EAVF was also determined to be Low (2) since no direct access points were planned (at the time of this assessment) between MWFM and any of the SmartGrid systems. An assessment of other vulnerable routes was out of scope because this assessment only covered relative vulnerability ratings within the SmartGrid portfolio.

3.4 VULNERABILITY ASSESSMENT RESULTS

Table 3-1 is based on the assessment performed in the previous section. It provides a quick view of the relative vulnerabilities of the systems by comparing their RVR numbers.

System	TEVF	EAVF	RVR
AHE	3	3	6
ALNK	4	4	8
BMS	2	3	5
CIS	3	3	6
DCADA	2	3	5
DER - C&I	2	3	5
DER - Grid-Connected	2	3	5
DERM	3	4	7
DER - Residential	3	4	7
DMAT	2	3	5
DMS	2	2	4
EMS	2	2	4
Field DADs	2	3	5
GIS	3	2	5
HAND	4	4	8
HANG	4	4	8
HEMP	4	4	8
IDM	2	3	5
MTR	3	5	8
MWFM	2	2	4
Substation DADs	2	3	5

Table 3-1 Relative Vulnerability Ratings of SmartGrid Systems

A summary of the relative vulnerability rating results is graphically represented in Figure 3-1 where each system is placed in either the Low, Medium or High region.

KCP&L SmartGrid
 Demonstration Project
 Risk Assessment Report

Vulnerability Assessment

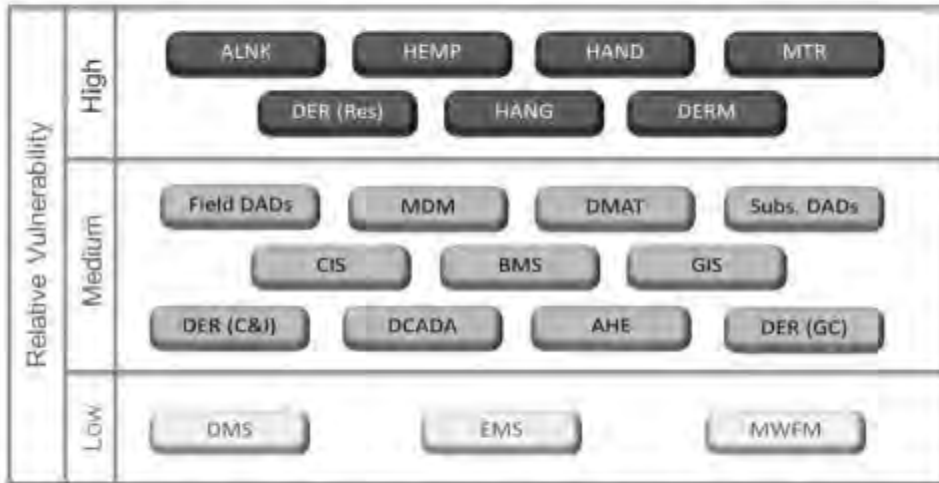


Figure 3-1 Graphical Representation of Relative Vulnerability Ratings



4.0 LIKELIHOOD DETERMINATION

The likelihood of a threat source attempting to impact a system is determined by evaluating a potential threat source's motivation, the nature and frequency of existing vulnerabilities, and perhaps performing a level of statistical analysis for occurrences of common vulnerabilities and exploits.

For example, a disgruntled former employee may have a very high motivation, but the frequency of that sort of threat materializing against a vulnerability is very low. Alternatively, an act of nature has no motivation factor, but different geographic areas present a higher frequency of certain natural occurrences; e.g. severe thunderstorms and tornadoes in the Midwest, hurricanes along the Gulf Coast, and earthquakes in California.

Referencing the Risk Calculation Model, the likelihood of attack is one element of the risk calculation. When evaluating the likelihood of an attempted vulnerability exploit, it is important to realize that this determination does not indicate the likelihood of success, merely the likelihood that an attempt will be made by a threat source to exercise a vulnerability on a system. The following evaluation criteria will be used to assign a value to the likelihood that a potential vulnerability could be exercised by a given threat source.

Likelihood Level	Likelihood Definition	Assigned Value
Very High	The threat-source is highly motivated, capable and presents a targeted attack against KCP&L resources	10
High	The threat-source is highly motivated and sufficiently capable ¹⁰	8
Medium	The threat-source is motivated or capable ¹¹	6
Low	The threat-source lacks motivation or capability ¹²	4
Very Low	The threat-source lacks motivation and capability	2
Negligible	The threat-source poses no probability of exercising a vulnerability against KCP&L	0

Table 4-1 Likelihood Evaluation Criteria

The following sections list each system within the scope of this risk assessment of the KCP&L SmartGrid Demonstration. Each of these systems was deemed essential to the reliable operation and management of the project. Each system was evaluated to determine the event likelihood for each threat source. The overall likelihood rating for each system is the highest value determined for any threat source that may target that system.

¹⁰ U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, *Special Publication 800-30: Risk Management Guide for Information Technology Systems*, July 2002
¹¹ Phil Withers, "Information Security Threat Vectors", <http://isaca-va.org/Threat%20Vectors.pdf>



4.1 ANALYSIS OF THREAT LIKELIHOOD

4.1.1 Common Likelihood Ratings

Some threat sources are common across all the systems within the scope of the SmartGrid risk assessment. To avoid repetition within the report, these common threat sources are listed here. These common values will be used in the event that a common threat source represents the highest likelihood of a vulnerability being exercised on a given system.

4.1.1.1 Acts of Nature

HIGHEST LIKELIHOOD RATING: 6

There is, of course, no motivating factor to consider for this threat source, and with the randomness of Acts of Nature, it is difficult to assign a likelihood value without extensive statistical analysis beyond the scope of this assessment. The following are the most likely Acts of Nature to affect the Kansas City area.

Wind Damage: Damage from straight line winds or tornados is a slight risk for the Kansas City metro area. The potential of a strong tornado (F2 or greater) striking the Kansas City area is less than .025%²¹. Although this ranks as the 35th highest likelihood in the nation, it still represents a very low possibility of this event affecting any of the systems within scope of this assessment.

Likelihood Rating: 4

Floods: Kansas City frequently experiences flooding along rivers and lakes, however, significant flooding which may affect the SmartGrid systems are much less common. In order to require closing levees along the Missouri River in Kansas City, river levels must be forecast to reach 39 feet²². Since 1900, there have been 9 instances of flooding significant enough to reach this level.²³ This presents a very low probability of this event affecting any of the systems within scope of this assessment. Although localized or flash flooding is more common, it is not deemed a significant threat to the data centers housing the SmartGrid systems, the communications network, or the Midtown Substation itself.

Likelihood Rating: 2

²¹ Climatological Threat Potential, National Oceanic and Atmospheric Administration (NOAA), <http://www.spc.noaa.gov/climo/online/rda/EAX.html>

²² NOAA, National Weather Service, Advanced Hydrologic Prediction Service, *Missouri River at Kansas City, Flood Impacts*.

<http://water.weather.gov/ahps2/hydrograph.php?wfo=eax&gage=kcdm7&view=1,1,1,1,1&toples=10,7,8,2,9,15,6>

²³ NOAA, National Weather Service, Advanced Hydrologic Prediction Service, *Historical Crests for Missouri River at Kansas City*. <http://water.weather.gov/ahps2/crests.php?wfo=eax&gage=kcdm7>

Ice: The primary danger posed from this threat source is loss of power, or inability of support personnel to physically access the SmartGrid systems. Statistics for ice storms are difficult to come by, but a review of local weather patterns indicates this is a real, but relatively low likelihood event.

Likelihood Rating: 4

Lightning: Cloud-to-Ground Lightning flashes average over 995,000 occurrences per year in Missouri and over 899,000 per year in Kansas. Those numbers equate to 14.3 strikes per square mile in Missouri and 11 strikes per square mile in Kansas.²⁴ These numbers rank in the top thirty percent of lightning strikes per square mile in the United States, indicating the frequency and severity of thundersorms in Kansas City and throughout the region, making this threat the most likely Act of Nature to impact the systems of the SmartGrid Demonstration.

Likelihood Rating: 6

4.1.1.2 Autonomous Systems and Malicious Code

The likelihood of a malware vulnerability being exploited is more dependent upon the platform being attacked than the specific application or system function. While instances of malware targeting applications are becoming more prevalent, vulnerabilities to those applications are still primarily dependent upon the operating system on which they are deployed.

For this reason, the Autonomous Systems and Malicious Logic threat source is split into two possible likelihood ratings, based upon the system platform and operating system. Threats to mobile computing devices are not considered in this risk assessment. If mobile computing is deployed within the KCP&L SmartGrid environment in the future, another risk assessment should be performed which includes an evaluation of those threats.

4.1.1.2.1 Microsoft Windows-Based Cyber Assets

The Windows-Based likelihood rating assumes some common applications and utilities are not present or active on the Windows cyber asset. These common applications include: Java and JavaScript, Adobe Acrobat, and any application from the Microsoft Office Suite. Although Internet Explorer is integral to

²⁴ NOAA, National Weather Service, Weather Forecast Office, Central Region Headquarters, *Rank of Cloud-to-Ground Flash Densities by State from 1996 to 2008*, http://www.crh.noaa.gov/image/txt/wcm/96-08Cloud_to_Ground.pdf

any installation of Microsoft Windows, an additional assumption is that HTTP connections are not permitted to untrusted networks from the cyber assets in the KCP&L SmartGrid demonstration.

Vulnerabilities and exploits targeting Windows-based applications, although generally declining, still represent a far larger percentage of the overall reported vulnerabilities in 2010, as opposed to operating system or browser vulnerabilities.¹⁶ For that reason, if any of the assumptions stated above prove incorrect, the likelihood rating would potentially be much higher.

Although Windows operating system vulnerabilities and exploits are smaller in number relative to those for Windows-based applications, there are still a large number of reported exploits against the Windows operating system, perhaps due to its large installation base around the world. Exploits detected by Microsoft numbered just under 200,000 in each of the first two quarters of 2010.¹⁷

An additional consideration for this likelihood rating is the version of Microsoft Windows installed on each cyber asset. Newer versions such as Windows Server 2003 or the Windows 7 Desktop obtain better and more up to date support, and were developed with more security built in than older versions of the Windows operating system. Due to the range of operating systems and versions in the KCP&L SmartGrid demonstration, this report maintains a "highest likelihood rating" approach.

Likelihood Rating: 8

4.1.1.2.2 Unix-Based and Linux-Based Cyber Assets

The likelihood rating for Unix and Linux-based systems is predicated on existing data indicating fewer identified vulnerabilities for those operating systems.¹⁸ As with the Windows-based likelihood rating, prior to assigning a likelihood rating for this threat source, the assumption was made that certain applications were not present or active on the system. These common applications include: Java and Javascript, Adobe Acrobat, and web browsers such as Mozilla.

Likelihood Rating: 6

¹⁶ Microsoft Corporation, *Microsoft Security Intelligence Report, Volume 10*, July 11, 2011

¹⁸ GFI Software, *Top Most Vulnerable Applications and Operating Systems in 2010*, February 17, 2011.
<http://www.gfi.com/blog/top-vulnerable-applications-operating-systems-2010/>

4.1.1.3 Errors and Omissions:

The likelihood of this threat source being exercised is nearly random. The execution of errors and omissions is almost exclusively inadvertent human interaction, so it may be influenced to a degree if there is more human interaction with a cyber asset. However, it is impossible to assign a realistic figure to the likelihood rating for Errors and Omissions without a thorough statistical analysis of related events at KCP&L. Such an in depth analysis is outside the scope of this risk assessment.

For the purposes of this assessment, beginning with a global average likelihood rating of 3 will provide a baseline for the evaluation of risk for this threat source.

Likelihood Rating: 6

4.1.1.4 Insider Abuse and Unauthorized Acts:

This likelihood rating is similar to Errors and Omissions, in that it is a nearly random occurrence with little evidence to support a quantitative likelihood rating, outside of an exhaustive statistical analysis.

For that reason, and also similar to Errors and Omissions, Insider Abuse and Unauthorized Acts is given a global average likelihood rating of 3 to provide a baseline for risk evaluation.

Likelihood Rating: 6

4.1.1.5 Legal and Administrative Actions:

Any system may be affected by audit findings or become involved in a criminal investigation. Although it may seem that systems with fewer security controls would be more apt to incur attacks and negative audit results, this is not always the case. Due to the unpredictable nature of this threat source, a global average likelihood rating of 3 is provided as a baseline for risk evaluation.

Likelihood Rating: 6

4.1.2 System-Specific Likelihood Ratings

4.1.2.1 AMI Head End (AHE)

HIGHEST LIKELIHOOD RATING: 8

Dependency Failures: The AHE system collects data from meters and interfaces with the MDM, CIS, DERM, and HEMP systems. The loss of a small number of meters is more likely than losing connectivity with any of the primary systems which interface with AHE.

Likelihood Rating: 4

External Attack: The AHE System is hosted outside the physical control of KCP&L, in a secure Landis+Gyr datacenter. Although this fact is not common knowledge outside the SmartGrid demonstration project, neither is it classified as Restricted information. As a known collection point for the most visible elements of the SmartGrid network, namely the meters, the AHE system presents a higher profile target than many systems of the SmartGrid. Therefore, the likelihood of an external threat source targeting this system is elevated.

Likelihood Rating: 6

Insider Attack: Access to the AHE becomes much easier and knowledge of the importance of the AHE system more common from inside the KCP&L or Landis+Gyr environments. This makes an insider a more likely threat to the AHE system.

Likelihood Rating: 5

Physical Intrusion and/or Theft: The physical location of the Landis+Gyr datacenter is unknown, so an analysis of crime statistics for the area is unavailable. No national statistics are available for data center thefts but based on a cursory search of Internet information, it can be ascertained that datacenter theft, although rare, is not unprecedented.

Likelihood Rating: 4

System and Environmental Failures: The AHE system is hosted in an environmentally controlled Landis+Gyr data center outside the physical control of KCP&L. The environmental controls and equipment are managed and monitored continuously and regularly maintained, lessening the likelihood of a malfunction or other operational failure. However, even the best maintained equipment is occasionally

offline, whether planned or unplanned, making it possible albeit unlikely for this threat source to impact the AHE system.

Likelihood Rating: 4

Violent Acts of Man: Similar to the Physical Intrusion and/or Theft threat source, it is difficult to perform an analysis of crime statistics near the Landis+Gyr datacenter because the exact physical location is unknown. However, instances of random violence serious enough to threaten the AHE system do not seem likely.

Likelihood Rating: 2

4.1.2.2 AccountLink (ALNK)

HIGHEST LIKELIHOOD RATING: 10

Dependency Failures: The ALNK system accepts connections from the Internet and interfaces with the HEMP system to provide customers a portal into their energy usage and billing. The ALNK system does not rely upon external data for operations and while it is possible that all the network circuits may fail, the likelihood of that occurring is fairly low.

Likelihood Rating: 4

External Attack: As the Internet-facing customer portal for KCP&L, the ALNK system may be the highest profile system and therefore the most likely target in the SmartGrid environment. Realizing also that, according to some statistics, four of the top 10 external vulnerabilities target web services, the likelihood of this threat source being exercised is very high.

Likelihood Rating: 10

Insider Attack: The primary motivations for an insider attack would be monetary gain, blackmail, or revenge using the personal information stored on the system. These types of intrusions are fairly rare, lessening the likelihood of such an event occurring on the ALNK system. However, the presence of large amounts of personal customer information may provide additional motivation to exploit a vulnerability on this system.

Likelihood Rating: 5



Physical Intrusion and/or Theft: Other than the value of the hardware, there is little to gain from the theft of the ALNK system. Obtaining the system's data would be more likely accomplished through cyber means. A cursory examination of crime statistics in the area of the KCP&L data center did not indicate a large concentration of break-ins or business-related crime.²³

Likelihood Rating: 4

System and Environmental Failures: The ALNK system is hosted in an environmentally controlled data center, which is managed and monitored continuously and regularly maintained, lessening the likelihood of a malfunction or other operational failure. However, even the best maintained equipment is occasionally offline, whether planned or unplanned, making it possible albeit unlikely for this threat source to impact the ALNK system.

Likelihood Rating: 4

Violent Acts of Man: The most accurate method to determine this likelihood rating is a thorough investigation into the statistical probability of violence in the area around the datacenter, which is outside the scope of this risk assessment. However, a quick search of random violence in the North Kansas City area indicated that instances of random violence serious enough to threaten the ALNK system within a secured datacenter do not appear likely.

Likelihood Rating: 2

4.1.2.3 Building Management System (BMS)

HIGHEST LIKELIHOOD RATING: 4

Dependency Failures: The BMS system manages DER systems in commercial and industrial locations, and interfaces with the DERM system. The likelihood of these connections failing is low.

Likelihood Rating: 4

External Attack: The presence of the BMS system interface at customer locations increases the likelihood of curious or malicious individuals will attempt to penetrate the system from that location. However, the relatively low current profile of DER resources reduces that likelihood greatly.

Likelihood Rating: 4

²³ <https://www.crimereports.com/>

Insider Attack: The likelihood of an internal attacker exercising a vulnerability on the BMS is relatively low due to the presence of higher profile targets with greater opportunity to gain valuable data or disrupt operations.

Likelihood Rating: 4

Physical Intrusion and/or Theft: Other than the value of the hardware, there is little to gain from the theft of the BMS system. Obtaining the system's data would be more likely accomplished through cyber means. The likelihood of theft may increase in neighborhoods more prone to criminal activity, but such a determination cannot be made for the current KCP&L SmartGrid demonstration.

Likelihood Rating: 4

System and Environmental Failures: Unlike many of the systems in the KCP&L SmartGrid environment, the BMS system is not located in a controlled environment. The potential for weather-related interruptions increases the likelihood of a temporary failure of individual communication channels, or sections of wireless communication.

Likelihood Rating: 4

Violent Acts of Man: The most accurate method to determine this likelihood rating is a thorough investigation into the statistical probability of violence in the area around the datacenter, which is outside the scope of this risk assessment. As such, a more accurate determination cannot be made for the current KCP&L SmartGrid demonstration.

Likelihood Rating: 2

4.1.2.4 Customer Information System (CIS)

HIGHEST LIKELIHOOD RATING: 8

Dependency Failures: The CIS system interfaces with many other systems to send and receive data. The likelihood of failure for the most important interfaces to the AHE, MDM, or HEMP is greater due to the distance between the locally maintained CIS and those remotely hosted systems.

Likelihood Rating: 6

External Attack: The CIS is not a customer-facing system, nor does it directly interface with public networks. However, there are three interfaces to externally hosted systems. Moreover, the presence of

large amounts of personal customer information may provide additional motivation to exploit a vulnerability on this system.

Likelihood Rating: 8

Insider Attack: The primary motivations for an insider attack would be monetary gain, blackmail, or revenge using the personal information stored on the system. These types of intrusions are fairly rare, lessening the likelihood of such an event occurring on the CIS system. However, the presence of large amounts of personal customer information may provide additional motivation to exploit a vulnerability on this system.

Likelihood Rating: 8

Physical Intrusion and/or Theft: Other than the value of the hardware, there is little to gain from the theft of the CIS system. Obtaining the system's data would be more likely accomplished through cyber means. A cursory examination of crime statistics in the area of the KCP&L data center did not indicate a large concentration of break-ins or business-related crime.*

Likelihood Rating: 4

System and Environmental Failures: The CIS system is hosted in an environmentally controlled data center, which is managed and monitored continuously and regularly maintained, lessening the likelihood of a malfunction or other operational failure. However, even the best maintained equipment is occasionally offline, whether planned or unplanned, making it possible albeit unlikely for this threat source to impact the CIS system.

Likelihood Rating: 4

Violent Acts of Man: The most accurate method to determine this likelihood rating is a thorough investigation into the statistical probability of violence in the area around the datacenter, which is outside the scope of this risk assessment. However, a quick search of random violence in the North Kansas City area indicated that instances of random violence serious enough to threaten the CIS system within a secured datacenter are not likely.

Likelihood Rating: 2

* <https://www.crimereports.com/>

4.1.2.5 Distribution Automation Devices (DADs)

HIGHEST LIKELIHOOD RATING- 6

Dependency Failures: The DADs transmit system parameter data to the DMS and DCADA for processing. These systems are located in controlled and monitored environments and are considered critical to the operation of the distribution network, increasing the frequency of maintenance and reducing the potential for failure.

Likelihood Rating: 4

External Attack: The DADs use a wireless network to communicate, presenting an attractive attack vector for a potential intruder, and the large number of DADs presents a target-rich environment.

Likelihood Rating: 6

Insider Attack: Although an inside attacker would have access to the systems upstream from the DADs and potentially the ability to affect their operation, the only real motivation for an insider would be revenge or data leak from a disgruntled employee, reducing the likelihood of an internal intrusion.

Likelihood Rating: 4

Physical Intrusion and/or Theft: The distributed locations of the DADs presents a greater profile for theft, however, there is a limited market for resale. Since profit would be the most common motivation for theft of these devices, their limited appeal also limited their attractiveness to thieves. An attacker bent on destructive or disruptive motives would most likely target systems farther upstream in order to impact a larger area.

Likelihood Rating: 4

System and Environmental Failures: Unlike many of the systems in the KCP&L SmartGrid environment, the DADs are not located in a controlled environment. The potential for weather-related interruptions increases the likelihood of a temporary failure of individual DADs or sections of the wireless communication. In addition, due to the large number of DADs, a communication failure to any one of them becomes more likely.

Likelihood Rating: 6



Violent Acts of Man: The location of the DADs much closer to the general public makes them more susceptible to damage if there is an outbreak of violence in the area. Although the DADs are unlikely to be a direct target, their proximity alone increases the likelihood of public violence making an impact. However, a review of crime statistics in the area provides no indication of such widespread violence, reducing the likelihood of impact.²⁹

Likelihood Rating: 4

4.1.2.6 Distribution Control and Data Acquisition (DCADA)

HIGHEST LIKELIHOOD RATING: 6

Dependency Failures: The DCADA accepts input from the DADs, and provided data to the DMS. The loss of individual DADs would not impact the ability of the DAC or DDC subsystems to function, but would impact the accuracy of their output to DMS, increasing the likelihood of a loss due to the large number of systems DCADA depends upon for information.

Likelihood Rating: 4

External Attack: Remote access to the DCADA system is primarily controlled via the DMS, but their connection to an IP network provides additional avenues of attack. The most likely motivation for this threat source would be revenge or espionage, meaning an attacker would need to have at least cursory knowledge of distribution automation, reducing the likelihood that either the DAC or DDC would be primary targets.

Likelihood Rating: 4

Insider Attack: The primary motivation for an insider to target the DCADA system would most likely be revenge, meaning unless the attacker had detailed knowledge of the DAC or DDC systems specifically, a higher profile target would be more appealing. However, any insider with access to the system would be able to cause extensive disruption, which may provide incentive to an insider bent upon causing damage to KCP&L's equipment or reputation.

Likelihood Rating: 6

²⁹ <http://www.crimereports.com/>

Physical Intrusion and/or Theft: The location of the DCADA systems within the perimeter of a substation reduces their availability for theft and the likelihood they would be targeted. Even if an intruder gained access to the substation, they would need to be directly targeting the DCADA system, further reducing the likelihood of this threat source impacting them.

Likelihood Rating: 4

System and Environmental Failures: Unlike many of the systems in the KCP&L SmartGrid environment, the DADs are not located in a controlled environment. The potential for weather-related interruptions increases the likelihood of a temporary failure of individual DADs and/or their communication network.

Likelihood Rating: 6

Violent Acts of Man: The location of the DCADA systems much closer to the general public makes them more susceptible to damage if there is an outbreak of violence in the area. Although DCADA is unlikely to be a direct target, its proximity alone increases the likelihood of public violence making an impact. However, a review of crime statistics in the area provides no indication of such widespread violence, reducing the likelihood of impact.²⁹

Likelihood Rating: 4

4.1.2.7 Distributed Energy Management System (DERM)

HIGHEST LIKELIHOOD RATING: 6

Dependency Failures: The DERM system interfaces with many other systems both to provide and receive data. The likelihood of failure for the most important interfaces to the DMS, MDM, or HEMP systems is greater due to the distance and complexity of communication between remotely hosted systems.

Likelihood Rating: 6

External Attack: The use of a proprietary operating system means an external attacker would need direct knowledge of this specific product in order to successfully mount an attack other than denial of service. This fact limits the potential motivations to revenge or unauthorized data disclosure. Since the HEMP

²⁹ <https://www.crimereports.com/>

system contains customer load information and processes demand response schedules, it presents a more likely target for an external attacker wishing to cause damage to the local distribution network or KCP&L's reputation.

Likelihood Rating: 6

Insider Attack: The demand response functions of the DERM system could present an attractive target to an insider with knowledge of the environment and the motivation of causing disruption to the local distribution network.

Likelihood Rating: 6

Physical Intrusion and/or Theft: The physical location of the OATI datacenter is unknown, so an analysis of crime statistics for the area is unavailable. No national statistics are available for datacenter thefts but a cursory search of internet information shows that datacenter theft, although rare, is not unprecedented.

Likelihood Rating: 4

System and Environmental Failures: The DERM system is hosted in an environmentally controlled OATI data center, which places it outside the physical control of KCP&L. The environmental controls and equipment are managed and monitored continuously and regularly maintained, lessening the likelihood of a malfunction or other operational failure. However, even the best maintained equipment is occasionally offline, whether planned or unplanned, making it possible albeit unlikely for this threat source to impact the DERM system.

Likelihood Rating: 4

Violent Acts of Man: Similar to the Physical Intrusion and/or Theft threat source, it is difficult to perform an analysis of crime statistics near the OATI datacenter because the exact physical location is unknown. However, instances of random violence serious enough to threaten the DERM system do not seem likely.

Likelihood Rating: 2



4.1.2.8 Distributed Energy Resources (DER - C&I, DER - Residential, Grid-Connected DER))

HIGHEST LIKELIHOOD RATING: 6

Dependency Failures: Various implementations of DER would have different interfaces within the SmartGrid environment. The common theme for dependencies is response for DR purposes. Most of these systems will be outside the immediate physical control of KCP&L, increasing the likelihood of this type of threat impacting them.

Likelihood Rating: 4

External Attack: Due to its limited capacity, the current plans for DER in the SmartGrid demonstration environment make it an unlikely target for an external attack. However, if an attacker were motivated by curiosity, the likelihood of this threat would increase.

Likelihood Rating: 6

Insider Attack: The limited capacity and impact of the various DER systems make it an unlikely target for an inside attacker. Widespread deployment or an increased impact on DR operations or decisions may increase the likelihood of an insider attack.

Likelihood Rating: 4

Physical Intrusion and/or Theft: The DER system is too large to steal, but could be used as blackmail if an event were leaked to the local media.

Likelihood Rating: 4

System and Environmental Failures: Implementation of the DER system is proposed for inside the substation of the SmartGrid demonstration. This limits the potential for an environmental or system failure.

Likelihood Rating: 4



Violent Acts of Man: The planned locations of the various DER systems in homes, businesses, and substations bring them closer to potential violence. However, instances of random violence serious enough to threaten the DER systems do not seem likely.

Likelihood Rating: 4

4.1.2.9 Data Mining and Analysis Tool (DMAT)

HIGHEST LIKELIHOOD RATING: 6

Dependency Failures: DMAT receives input and provides data to the MDM system. The likelihood of a dependency failure for any one communications circuit is relatively small.

Likelihood Rating: 4

External Attack: DMAT contains customer energy usage data, which may make it an attractive target for an attacker motivated by revenge, curiosity, or third party marketing.

Likelihood Rating: 6

Insider Attack: The information processed by DMAT is available for less effort from other systems accessible by an insider, making it unlikely an insider would use this avenue of compromise.

Likelihood Rating: 4

Physical Intrusion and/or Theft: The physical location of the DataRaker datacenter is unknown, so an analysis of crime statistics for the area is unavailable. No national statistics are available for datacenter thefts but a cursory search of Internet information shows that datacenter theft, although rare, is not unprecedented.

Likelihood Rating: 4

System and Environmental Failures: The DMAT system is hosted in an environmentally controlled DataRaker data center, which places it outside the physical control of KCP&L. The environmental controls and equipment are managed and monitored continuously and regularly maintained, lessening the likelihood of a malfunction or other operational failure. However, even the best maintained equipment is occasionally offline, whether planned or unplanned, making it possible albeit unlikely for this threat source to impact the DMAT system.

Likelihood Rating: 4



Violent Acts of Man: Similar to the Physical Intrusion and/or Theft threat source, it is difficult to perform an analysis of crime statistics near the DMAT datacenter because the exact physical location is unknown. However, instances of random violence serious enough to threaten the DMAT system do not seem likely.

Likelihood Rating: 2

4.1.2.10 Distribution Management System (DMS)

HIGHEST LIKELIHOOD RATING: 8

Dependency Failures: The DMS interfaces with at least six other systems, making the loss of any one communication path possible but unlikely.

Likelihood Rating: 4

External Attack: The DMS is the backbone of the SmartGrid distribution network, increasing the public profile and presenting a more attractive target for an attacker.

Likelihood Rating: 6

Insider Attack: If an insider wanted to do the most possible damage to the KCP&L SmartGrid demonstration, the DMS may be the system most likely to be attacked due to its high profile.

Likelihood Rating: 8

Physical Intrusion and/or Theft: Other than the value of the hardware, there is little to gain from the theft of the DMS system. Obtaining the system's data would be more likely accomplished through cyber means. A cursory examination of crime statistics in the area of the KCP&L data center did not indicate a large concentration of break-ins or business-related crime.³⁹

Likelihood Rating: 4

³⁹ <https://www.crimereports.com/>

System and Environmental Failures: The DMS system is hosted in an environmentally controlled data center, which is managed and monitored continuously and regularly maintained, lessening the likelihood of a malfunction or other operational failure. However, even the best maintained equipment is occasionally offline, whether planned or unplanned, making it possible albeit unlikely for this threat source to impact the DMS system.

Likelihood Rating: 4

Violent Acts of Man: The most accurate method to determine this likelihood rating is a thorough investigation into the statistical probability of violence in the area around the datacenter, which is outside the scope of this risk assessment. However, a quick search of random violence in the North Kansas City area indicated that instances of random violence serious enough to threaten the DMS system within a secured datacenter are not likely.

Likelihood Rating: 4

4.1.2.11 Energy Management System (EMS)

HIGHEST LIKELIHOOD RATING: 10

Dependency Failures: Within the scope of the SmartGrid environment, the EMS interfaces with the DADs at the Substation. This line of communication is unlikely to be broken during normal operation.

Likelihood Rating: 4

External Attack: The EMS is a very visible part of KCP&L's transmission and distribution network. As such, it presents a larger attack profile than a lesser known system. An attacker could be motivated by a range of factors, including destruction or unauthorized disclosure of data, industrial espionage, blackmail, or revenge.

Likelihood Rating: 8

Insider Attack: A malicious insider could have multiple motives for attacking the EMS, and would understand its importance to the KCP&L mission, including the SmartGrid environment. This makes the EMS a very likely target.

Likelihood Rating: 10



Physical Intrusion and/or Theft: Other than the value of the hardware, there is little to gain from the theft of the EMS system other than disruption of KCP&L's transmission network. Obtaining the system's data would be more likely accomplished through cyber means. A cursory examination of crime statistics in the area of the KCP&L control center did not indicate a large concentration of break-ins or business-related crime.¹²

Likelihood Rating: 4

System and Environmental Failures: The EMS system is hosted in an environmentally-controlled control center, which is managed and monitored continuously and regularly maintained, lessening the likelihood of a malfunction or other operational failure. However, even the best maintained equipment is occasionally offline, whether planned or unplanned, making it possible albeit unlikely for this threat source to impact the EMS system.

Likelihood Rating: 4

Violent Acts of Man: The most accurate method to determine this likelihood rating is a thorough investigation into the statistical probability of violence in the area around the datacenter, which is outside the scope of this risk assessment. However, a quick search of random violence in the North Kansas City area indicated that instances of random violence serious enough to threaten the EMS system within a secured control center are not likely.

Likelihood Rating: 4

4.1.2.12 Geographical Information System (GIS)

HIGHEST LIKELIHOOD RATING: 6

Dependency Failures: The GIS system has two interfaces into the KCP&L SmartGrid environment, to the CIS and the DMS. The likelihood of these connections failing is fairly low.

Likelihood Rating: 4

¹² <https://www.crimereports.com/>

External Attack: The geographical data provided by GIS provides detailed hard copy maps of the distribution system that are kept in field vehicles. This information may focus an attacker's energy on discovering what other information is contained in GIS, or falsifying data to disrupt operations.

Likelihood Rating: 6

Insider Attack: A knowledgeable insider could attempt to alter GIS data to disrupt maintenance or repair efforts, among other things.

Likelihood Rating: 6

Physical Intrusion and/or Theft: Other than the value of the hardware, there is little to gain from the theft of the GIS system. Obtaining the system's data would be more likely accomplished through cyber means. A cursory examination of crime statistics in the area of the KCP&L data center did not indicate a large concentration of break-ins or business-related crime.⁶⁹

Likelihood Rating: 4

System and Environmental Failures: The GIS system is hosted in an environmentally controlled data center, which is managed and monitored continuously and regularly maintained, lessening the likelihood of a malfunction or other operational failure. However, even the best maintained equipment is occasionally offline, whether planned or unplanned, making it possible albeit unlikely for this threat source to impact the GIS system.

Likelihood Rating: 4

Violent Acts of Man: The most accurate method to determine this likelihood rating is a thorough investigation into the statistical probability of violence in the area around the datacenter, which is outside the scope of this risk assessment. However, a quick search of random violence in the North Kansas City area indicated that instances of random violence serious enough to threaten the GIS system within a secured datacenter are not likely.

Likelihood Rating: 4

⁶⁹ <http://www.crimereports.com/>

4.1.2.13 Home Area Network Devices/Gateway (HAND/HANG)

HIGHEST LIKELIHOOD RATING: 8

Dependency Failures: The Home Area Network devices receive data from multiple sources to provide accurate information to the customer. Many of these interfaces may rely upon power line or wireless communications, increasing the likelihood of a disruption.

Likelihood Rating: 6

External Attack: As the devices closest to the customer, the HAN devices and gateway are a high profile target for attackers interested in how they work, or attempting to alter power usage data. The presence of these devices within customer's homes increases the likelihood of malicious or curious tampering with them.

Likelihood Rating: 6

Insider Attack: An insider would understand the importance of the HAN to individuals involved with the KCP&L SmartGrid environment, but would also understand the benefit of attacking further downstream in the data processing.

Likelihood Rating: 4

Physical Intrusion and/or Theft: The location of HAN devices and gateways within private residences creates an opportunity for customers to physically break into them for curiosity's sake, to attempt to alter their energy bill, or to sell them in an effort to make a profit.

Likelihood Rating: 8

System and Environmental Failures: Power failures in residential areas are common enough to be an issue for HAN devices. The physical environment is also outside the control of KCP&L, which may lead to overheating, water damage, fire damage, etc.

Likelihood Rating: 8



Violent Acts of Man: Domestic violence is a more likely scenario for causing damage or malfunction on Home Area Network devices. KCP&L has no impact or local authority to prevent or deter such violence from damaging or destroying HAN devices.

Likelihood Rating: 6

4.1.2.14 Home Energy Management Portal (HEMP)

HIGHEST LIKELIHOOD RATING: 10

Dependency Failures: The HEMP system interfaces with many other systems to provide and receive data for processing and/or display to customers. The system also accepts inputs from customers for their account. This amount of interaction provides many opportunities for failure.

Likelihood Rating: 6

External Attack: The HEMP is a web-based front-end into a customer's energy usage and efficiency. It is accessed via a link from another web-based portal (ALNK). The combination of a high-profile application and high-profile platform vulnerabilities leads to a very high likelihood of this threat source attempting to impact HEMP.

Likelihood Rating: 10

Insider Attack: The motivations an insider may have to affect the data or function of HEMP range from revenge to curiosity. In such cases, the HEMP provides a high-profile target for attempted penetration.

Likelihood Rating: 6

Physical Intrusion and/or Theft: The physical location of the Tendril datacenter is unknown, so an analysis of crime statistics for the area is unavailable. No national statistics are available for datacenter thefts but a cursory search of Internet information shows that datacenter theft, although rare, is not unprecedented.

Likelihood Rating: 4

System and Environmental Failures: The HEMP system is hosted in an environmentally controlled Tendril data center, which places it outside the physical control of KCP&L. The environmental controls and equipment is managed and monitored continuously and regularly maintained, lessening the likelihood of a malfunction or other operational failure. However, even the best maintained equipment is

occasionally offline, whether planned or unplanned, making it possible albeit unlikely for this threat source to impact the HEMP system.

Likelihood Rating: 4

Violent Acts of Man: Similar to the Physical Intrusion and/or Theft threat source, it is difficult to perform an analysis of crime statistics near the Tendril datacenter because the exact physical location is unknown. However, instances of random violence serious enough to threaten the HEMP system do not seem likely.

Likelihood Rating: 2

4.1.2.15 Meter Data Management System (MDM)

HIGHEST LIKELIHOOD RATING: 6

Dependency Failures: The MDM system interfaces with many other systems to process energy usage and information for customer billing. The number of inputs presents more opportunities for dependency failure.

Likelihood Rating: 6

External Attack: The MDM may present an attractive target for an attacker attempting to view or alter customer usage or billing information.

Likelihood Rating: 6

Insider Attack: The most likely scenario for an insider to attack the MDM is for revenge or curiosity. There is minimal personal information on the system, so an attack to find that data would focus on other systems.

Likelihood Rating: 4

Physical Intrusion and/or Theft: The physical location of the Siemens datacenter is unknown, so an analysis of crime statistics for the area is unavailable. No national statistics are available for datacenter thefts but a cursory search of Internet information shows that datacenter theft, although rare, is not unprecedented.

Likelihood Rating: 4

System and Environmental Failures: The MDM system is hosted in an environmentally controlled Siemens data center, which places it outside the physical control of KCP&L. The environmental controls and equipment are managed and monitored continuously and regularly maintained, lessening the likelihood of a malfunction or other operational failure. However, even the best maintained equipment is occasionally offline, whether planned or unplanned, making it possible albeit unlikely for this threat source to impact the MDM system.

Likelihood Rating: 4

Violent Acts of Man: Similar to the Physical Intrusion and/or Theft threat source, it is difficult to perform an analysis of crime statistics near the Siemens datacenter because the exact physical location is unknown. However, instances of random violence serious enough to threaten the MDM system do not seem likely.

Likelihood Rating: 2

4.1.2.16 SmartMeter (MTR)

HIGHEST LIKELIHOOD RATING: 10

Dependency Failures: Meters provide data upstream for processing and billing purposes and in some cases pass signals on to the HAN devices. These connections can be either wired or wireless, which increases the likelihood of interference or interruption.

Likelihood Rating: 6

External Attack: Smart meters have become the symbol of the SmartGrid for many consumers, and often in a negative light. Hackers have already demonstrated exploits against smart meters in public forums and will continue to do so, making the meters perhaps the highest likelihood point of attack in the environment.

Likelihood Rating: 10

Insider Attack: The lack of customer identifiable information reduces the likelihood of meters being a target for internal attack or compromise. No matter the motivation, an insider is more likely to target a system farther downstream.

Likelihood Rating: 4



Physical Intrusion and/or Theft: Meters are already subject to customer and criminal break-ins. Occasionally, the motivation is self-repair in order to avoid a visit fee from the utility, but most often the motive is criminal in nature, such as attempting to artificially lower reported energy usage.

Likelihood Rating: 6

System and Environmental Failures: Meters are designed to withstand power outages and data disruptions. However, the addition of wireless radio and smart functionality increases the likelihood of component failure.

Likelihood Rating: 4

Violent Acts of Man: The presence of meters on every building increases the likelihood of damage any time violence breaks out, no matter the cause or location.

Likelihood Rating: 6

4.1.2.17 Mobile Workforce Management System (MWFM)

HIGHEST LIKELIHOOD RATING: 6

Dependency Failures: The MWFM system receives input from and sends data to the CIS. Each mobile device communicates independently via wireless communication from the field. Individual loss of connectivity is more likely than widespread failure or disruption.

Likelihood Rating: 4

External Attack: The mobile laptops are located in each truck and communicate wirelessly, increasing their network footprint and attack profile.

Likelihood Rating: 6

Insider Attack: The lack of useful data or login credentials make MWFM an unattractive target for malicious insiders.

Likelihood Rating: 4

Physical Intrusion and/or Theft: The mobile laptops are located in each truck and visible from outside the vehicle, making them a tempting target for attackers.

Likelihood Rating: 6

System and Environmental Failures: The mobile laptops contain battery backup and are able to function without power for some time. On the other hand, the rigors of field use may reduce the life expectancy of the mobile laptops.

Likelihood Rating: 4

Violent Acts of Man: It is unlikely for a mobile laptop to become engaged in local or regional violence. Accidental damage during use is more likely.

Likelihood Rating: 6



4.2 LIKELIHOOD DETERMINATION RESULTS

The highest likelihood ratings for all the systems are summarized in Table 4-2.

System	Highest Likelihood (L) Rating
AHE	8
ALNK	10
BMS	4
CIS	8
DADs	6
DCADA	8
DER - C&I	6
DER - Grid-Connected	6
DERM	6
DER - Residential	6
DMAT	6
DMS	8
EMS	10
GIS	6
HAND/HANG	8
HEMP	10
MDM	6
MTF	10
MWFM	6

Table 4-2 Likelihood Ratings

5.0 IMPACT ANALYSIS

The next major step in the risk assessment is to carefully and methodically evaluate the impact of a threat exercising one or more vulnerabilities. An impact could go deep enough to damage public image, open up windows of potential litigations, cause significant operational disruptions or monetary damages, or any combination of the above. Mitigating or minimizing the impacts thus becomes a high priority. This can be achieved by careful selection and placement of control elements based on the criticality of a system. The criticality of a system is directly proportional to the impact a security compromise can cause:

Criticality \propto Impact

The magnitude of an impact depends on the depth of the security breach compromising one or more of the three security goals: Confidentiality, Integrity, and Availability. Clearly, a sound approach for impact determination takes all three security goals into account. Interviewing business users and system owners as well as studying system requirement documentation and use cases are some key methods used to assess impacts. As an example, if the business users' tolerance towards a system outage is very low and the loss of availability directly affects the organization's primary business functions, then the system undoubtedly becomes a high-impact, highly critical system. In most utilities, the Energy Management System (EMS) and Distribution Management System (DMS) are considered highly critical systems. Similarly, if a business function requires very high quality data and an integrity compromise is unacceptable, then the system belongs to the highly critical category. On the other hand, if a system's unavailability or a moderate loss of its data integrity does not adversely affect business operations, then the system can be placed in the medium or low criticality level. System criticality may also fluctuate based on the impact of an information leak to business operations. As such, the higher the confidentiality of a system's data, the higher the system criticality or impact level is.

Table 5-1 provides a guideline that could be used for criticality assignment. However, a more quantitative criticality assessment approach was used for this risk assessment effort and is covered in the following section.

Criticality Level	Result of Security Breach
Very High	Significant monetary damage, Compromised consumer privacy, Loss of important business operation for a long period, National level damage to the company reputation, Years of litigation
High	Consumers opting out of SmartGrid programs, Loss of large sums of money, Stained public image, Penalties by regulating authorities, Temporary loss of important business operation, Regional level damage to company reputation
Medium	Few hours loss of operations, Some loss of public trust, Inquiry from monitoring authorities, Localized level damage to company reputation
Low	Loss of business operations, Some damage to company reputation, Monitoring authorities attention, Strained consumer relationship
Very Low	Consumer complaints, Minor loss in productivity due to unavailability or data corruption

Table 5-1 Example Criticality Assignment Guideline

5.1 IMPACT ASSESSMENT APPROACH

The key to a successful impact assessment is development of a good approach to quantify the impact magnitude. The approach should result in a relative impact rating for each system, which can be used later to assess the relative risk level of the system. It is prudent to understand that the quantifying process requires the evaluators to make a sound qualitative judgment at some point in the analysis.

The security goal of confidentiality is the first such qualitative judgment, which can be converted into a numerical assignment as shown in the following table, Table 5-2. A straightforward way to judge the confidentiality of the data is to look at its sensitivity and the impact a leak will have on KCP&L's image and operations. Any system that processes information such as KCP&L's trade secrets, operational security, and consumer privacy should be considered highly sensitive. A system could be considered moderately sensitive if the data it owns could not be used by a threatening entity to compromise KCP&L's image and operations. A system that stores or processes data that is usually available in the public domain can be placed in relatively low sensitivity category.

KCP&L SmartGrid
Demonstration Project
Risk Assessment Report

Impact Analysis

Confidential / Sensitive Data Examples	Impact Level	Impact Numerical Assignment
KCP&L Trade Secrets (Delta Production Cost), Consumer Private Data (Social Security Numbers)	Very High	10
Financial Data (billing), Consumer Data (Credit Card Numbers, Bank Account Numbers)	High	8
Customer Usage Data, Control Signals	Medium	6
Equipment Location, Telemetry Data	Low	4
KCP&L Internet Site (Generic Outage Data)	Very Low	2

Table 5-2 Confidentiality Impact Level Definitions

The impact of an *integrity* compromise can be best assessed by looking at the cost of a security breach. A formula to assess the cost of an integrity compromise can be expressed as:

$$\text{Cost}(i) = (\text{Number of work hours spent on a fix}) \times (\text{Hourly rate})$$

In a simple scenario, an integrity compromise event results in ten operations and IT engineers spending a ten-hour day to fix the issue. If they are all paid at a rate of \$100 per hour, the total cost would be \$10,000. This cost could increase exponentially if the solutions are hosted at vendor sites and may require expensive specialized resources to resolve.

Table 5-3 can be used to quantify a system's integrity impact based upon the cost per day to resolve an integrity compromise.

Cost (i) per day	Impact Level	Impact Numerical Assignment
$i \geq \$100,000$	Very High	10
$\$50,000 < i < \$100,000$	High	8
$\$10,000 < i < \$50,000$	Medium	6
$\$1,000 < i < \$10,000$	Low	4
$i < \$1,000$	Very Low	2

Table 5-3 Integrity Impact Level Definitions

The impact of a security event affecting the availability (third security goal) of a system can be best assessed by calculating the overall cost caused by system unavailability. The cost calculation can be expressed as:

$$\text{Cost}(a) = \text{Lost Productivity Cost} + \text{Lost Opportunity Cost} + \text{Cost of Lost Business Image} + \text{Increased Business Cost}$$



In a scenario where the system unavailability results in twenty engineers losing productivity for a day, parts of power distribution being managed through manual processes, power being supplied through expensive routes (examples include turning on higher cost units or overusing power lines resulting in congestions), and customers losing power for an undefined amount of time, the total cost could easily reach hundreds of thousands of dollars. Since the intent of this report is to identify the relative IT risk level of each system, a complete economic impact assessment is out of scope. However, using the established Disaster Recovery (DR) priority list at KCP&L as an aide, an assessment can be made regarding the relative importance of systems based upon operational area similarities.

Table 5-4 provides the method to quantify each system's availability impact level with respect to the acceptable length of system unavailability.

Acceptable unavailability duration (Time)	Impact Level	Impact Numerical Assignment
1 to 60 minutes	Very High	10
1 Hour to 4 Hours	High	8
4 Hours to 12 Hours	Medium	6
12 Hours to 48 hours	Low	4
Greater than 48 Hours	Very Low	2

Table 5-4 Availability Impact Level Definitions

Once the numerical assignment for each security goal is completed for each system, the criticality level is calculated by averaging the assigned impact numbers:

$$\text{Criticality Level} = \frac{\text{Confidentiality Impact} + \text{Integrity Impact} + \text{Availability Impact}}{3}$$

5.2 IMPACT ASSESSMENT

The following subsections include the relative impact assessment of each planned system in the KCP&L SmartGrid Demonstration Project.

5.2.1 AMI Head-End (AHE)

AHE will be processing control signals such as meter reads, connect/disconnect commands, and demand response (DR) signals. It will also be the hub for the collection of customer usage data, which affects billing. The impact of a confidentiality breach of such data was found to be High (8). A breach resulting in the release of several hundred consumers' usage data collectively will have a high negative impact on KCP&L's reputation. Since AHE is planned to be hosted and managed externally to KCP&L, the impact

of an integrity issue was found to be High (8). The primary contributing factor for this rating was the fact that any integrity fix will require a combination of internal (IT, Operations) and external (vendor) resources. Since the MTRs can store several days of usage data and the other communication between the AHE and the MTRs is not critical to overall operations, an unavailability of AHE for 4 to 12 hours (Medium - 6) was found to be acceptable.

5.2.2 AccountLink (ALNK)

Since ALNK is the repository of consumer financial data, any confidentiality breach could be very damaging to KCP&L's reputation. The confidentiality compromise in this application was thus assigned a High (8) value. Since the code and services are managed in-house, the integrity fix cost was determined to be Medium (6). The SMEs verified that any unavailability exceeding one hour may affect thousands of monetary transactions. Thus, ALNK was given a High (8) availability impact level.

5.2.3 Building Management System (BMS)

Since the BMS control signals only convey the DR signals, the confidentiality of this data was determined to be Low (4). The integrity factor, however, belonged to the Medium (6) category as any malicious modification to the control signals could discourage DR participation by larger consumers. The unavailability of a single instance of BMS would not affect KCP&L operations; thus, the impact was determined to be Low (4).

5.2.4 Customer Information System (CIS)

The CIS manages all aspects of KCP&L's relationship with its customers including the storage of sensitive information such as customer Social Security Number (SSN), bank account numbers, and credit card numbers. Any leak of such information will likely greatly decrease KCP&L's credibility and its consumers' trust level. The confidentiality impact was thus determined to be Very High (10). The cost of fixing an integrity issue in CIS was estimated to be Low (4) as the technology is well known and does not require highly technical resources. The availability of CIS is the highest priority according to the KCP&L IT disaster recovery plan. As such, the unavailability factor assigned to CIS for this assessment was Very High (10).

5.2.5 Distributed Control and Data Acquisition (DCADA)

Since the DCADA system primarily manages information that relates to energy distribution point-in-time, a leak of this information does not affect the confidentiality of the system. The resultant confidentiality factor was determined to be Low (4). The DCADA applications are designed to manage single instance

integrity issues. An integrity compromise, however, may require the time of skilled resources only if the issue is persistent over several cycles. As a result, the integrity impact factor for DCADA was determined to be Medium (6). The DCADA application will be the primary application to manage Midtown Substation. Its unavailability will cause operations to shift from automated to either manual or a less controlled mode. The resultant unavailability impact factor was estimated to be High (8).

5.2.6 Distributed Energy Resources – Commercial & Industrial (DER – C&I)

The DER - C&I are customer installations; a leak of information about these DERs will not have any effect on the confidentiality according to KCP&L. The confidentiality factor was therefore estimated to be Low (4). Similarly, an integrity issue at the customer end does not affect KCP&L. Thus, the integrity impact factor was also determined to be Low (4). The unavailability of a single customer's DER has minimal impact on KCP&L operations. However, if multiple customers' DER are out of commission, then the DR program can get paralyzed. Still, the overall impact was determined to be Low (4).

5.2.7 Distributed Energy Resources (DER – Grid-Connected)

The battery and other similar grid-connected DER do not contain confidential data other than configuration data, which would cause a relatively low impact should there be a data leak. The confidentiality impact factor was thus given a rating of Low (4). However, any integrity compromise will require expensive vendor resources to fix or rectify. Thus, the integrity impact factor was determined to be Medium (6). Unavailability of the battery would remove a large, inexpensive DER from the grid, but the impact will still be small relative to other systems, making the unavailability factor Low (4).

5.2.8 Distributed Energy Resource Management System (DERM)

The DERM is one of the key systems in the KCP&L SmartGrid project, as the overall success of the project is quite dependent on its secure deployment. The data and control signals generated by DERM were determined not to be sensitive in nature. Thus, the confidentiality rating was determined to be Low (4). However, an integrity issue could get costly as the fix would involve multiple resources from the various vendors (OATL, Tendril, Landis+Gyr, KCP&L, and in some cases, the customers). The resultant integrity factor was estimated to be Very High (10). The unavailability of the DERM could cost KCP&L a loss of DR participation during the time of greatest need (summer peaks). The impact of unavailability during these times could be very high. Unavailability during normal, off-peak business operations will have only a moderate impact. Based on that reasoning, the appropriate rating for unavailability was determined to be High (8).

5.2.9 Distributed Energy Resources – Residential (DER – Residential)

The DER - Residential will be a collection of load curtailment and small storage devices. These devices will not have any sensitive data, which resulted in a confidentiality impact rating of Low (4). A data integrity problem will be an easier fix, but identification could get expensive. Nevertheless, an incorrect or unnecessary load curtailment signal can impact customers in an adverse way. Therefore, an integrity impact rating of Medium (6) was justified. The impact of unavailability of residential DER will be minimal to KCP&L operations. Thus, a rating of Very Low (2) was suitable.

5.2.10 Data Mining and Analysis Tool (DMAT)

The DMAT system analyzes metering data, creates usage patterns, estimates missing metering data, and provides visualization of the analysis. The usage data was estimated to be moderately sensitive (Medium - 6) as the leak of this information may not adversely affect KCP&L or its customers. The system's integrity is also not a big concern as the data integrity issues are corrected by vendor processes. Therefore, a resultant rating of Low (4) was justified. DMAT's unavailability also does not affect KCP&L operations, as this system is not considered mission-critical, thereby resulting in a rating of Low (4).

5.2.11 Distribution Management System (DMS)

The DMS is the main computing resource behind the distribution operations. It does not manage confidential data (thus, the confidentiality impact rating was determined to be Low (4)) but an integrity loss has the potential to be detrimental to KCP&L operations. The remedy will likely get expensive depending on the number of hours required and the resulting loss in productivity. Therefore, the impact rating of integrity compromise was determined to be Very High (10). The unavailability of this system will interrupt the automated operations for the length of time associated with a sustained outage. As a result, the suitable rating for unavailability of this system was determined to be Very High (10).

5.2.12 Energy Management System (EMS)

The EMS manages the generation and transmission of bulk energy. As such, the EMS does not contain or manage highly confidential data, but with some effort a knowledgeable attacker could deduce energy cost related data by understanding generation levels and transmission networks. On a confidentiality scale this information was estimated to be Medium (6). The integrity cost however can be Very High (10) depending on the depth of the issues. EMS resources are typically the most expensive, and the amount of time to fix issues can also be on the higher side. The unavailability impact (like the DMS) was also

determined to be Very High (10) as KCP&L operations are largely dependent on applications like the EMS.

5.2.13 Field and Substation Distribution Automation Devices (Field-DADs and Substation DADs)

The Distribution Automation Devices are used to remotely manage the distribution of energy and as such do not contain any sensitive data. For this reason, the confidentiality rating was considered to be Low (4). Since the automation devices operate on point-in-time control signals, an integrity compromise (unless repeated over several cycles) will not cause damage to KCP&L operations. The resultant rating was thus estimated to be Low (4). Individual or localized unavailability of the DADs will likely not affect operations. However, large-scale unavailability could hamper KCP&L distribution operations. For the purposes of the demonstration project, the unavailability impact rating of Medium (6) was more appropriate.

5.2.14 Geographic Information System (GIS)

The data contained in GIS helps designers and planners perform geographical analysis. The data managed inside the GIS system is not considered sensitive from an operational perspective. However, the locations of critical customers like hospitals, fire departments, and police departments are marked on the spatial files. The confidentiality rating was still determined to be Low (4) as most of this information is available in the public domain. An integrity compromise was estimated to be Medium (6) as the fixes are not expensive but the productivity lost due to incorrect field work locations may get high. The SMEs verified that the IT disaster recovery plan allows for six hours of unavailability. This system was thus assigned the unavailability impact rating of Medium (6).

5.2.15 Home Area Network Devices and Gateway (HAND and HANG)

The HAN Devices and Gateway will contain information such as device MAC addresses, installation code, device type, installation date, pair ID, etc. This information, by itself, is not considered sensitive, but if leaked could be manipulated to adversely affect the consumer. The resultant confidentiality impact rating was determined to be Medium (6). The integrity compromise cost, by itself, for these devices was determined to be Low (4), however a data integrity issue propagating into other systems could have a medium to high impact. Lastly, the unavailability impact of these devices for a single consumers or a small number of consumers is going to be low for KCP&L. However, impact could be high for the consumer if the appliances that these devices control become unavailable or malfunction. As a result, the unavailability rating was determined to be Medium (6).

5.2.16 Home Energy Management Portal (HEMP)

The HEMP is the primary interface that the KCP&L SmartGrid consumers will utilize to manage their HAN, participate in DR events, and view their usage. Information like usage data and billing levels has been determined by many consumer groups to be private. A leak of this information will be damaging for KCP&L's reputation and its SmartGrid program. The impact rating of a confidentiality compromise was thus determined to be High (8). The cost of a data integrity fix could be anywhere from low to medium depending on the number of consumers affected by the issue. The impact rating of Medium (6) was thus justified to cover for events that affect large numbers of consumers. Unavailability of HEMP for a few consumers is going to be insignificant. However, mass unavailability will affect many consumers and could result in a large number of complaints and trust issues with KCP&L's SmartGrid program. For this reason, the unavailability impact rating was determined to be High (8).

5.2.17 Meter Data Management System (MDM)

The MDM acts as the repository of meter inventory and individual consumer usage. Because of the sensitivity of the usage information contained in MDM, the most suitable category for this system was High (8). An integrity fix for this application may not get costly unless a large amount of consumer data gets affected, and the duration of the integrity issue is long. The resultant rating for this application was therefore evaluated to be Medium (6). After discussion with the SMEs, it was determined that the unavailability of MDM for up to six hours is not believed to cause major operational impacts. However, an unavailability lasting any longer could result in billing issues. As a result, the appropriate rating determined for MDM was Medium (6).

5.2.18 SmartMeter (MTR)

A breach resulting in an unauthorized entity getting access to the usage data stored in a MTR will be very damaging to the consumer and to KCP&L. Since this type of data is considered private by many consumer groups, it was reason enough to place MTR at High (8) on the sensitivity scale. A data integrity event for one MTR installation will not be costly for KCP&L, however any compromise to the control signals (a false disconnect command being sent for example) could have far-reaching effects. As a result, an integrity impact rating of medium (6) was suitable for this device. One instance of MTR unavailability will have minimal impact on KCP&L, but a large number of MTR outages could easily have a large impact on the KCP&L bottom line. Thus, the unavailability impact rating for MTR was determined to be Medium (6).

5.2.19 Mobile Work Force Management System (MWFM)

MWFM is the system used by the field service dispatchers to solve customer issues that require a technician visit to the site. This type of data was determined to be low in sensitivity and thus, a Low (4) confidentiality impact rating was given. Due to the high number of mobile client installations, the coordination of an integrity fix rollout, coupled with time spent on creating and testing the fix may require a large number of man-hours. Thus, an integrity fix cost for this system was determined to be Medium (6). The unavailability impact rating was determined to be Low (4) as an outage of this system is not considered critical to overall operations. To cover for lengthy outages, KCP&L has backup functionalities that involve manual business processes.

5.3 IMPACT ASSESSMENT RESULTS

Based on the assessment in the previous section, Table 5-5 was created to summarize the results in a tabular format. The table provides a quick view of the relative criticalities of the SmartGrid systems with respect to each other.

KCP&L SmartGrid
Demonstration Project
Risk Assessment Report

Impact Analysis

System	Confidentiality Impact Level	Integrity Impact Level	Availability Impact Level	Overall Impact Level
AHE	8	8	6	7.33
ALNK	8	6	8	7.33
BMS	4	6	4	4.67
CTS	10	4	10	8.00
DADs (Field & Substation)	4	4	6	4.67
DC/ADA	4	6	8	6.00
DER – C&I	4	4	4	4.00
DER – Grid-Connected	4	6	4	4.67
DER – Residential	4	6	2	4.00
DERM	4	10	6	7.33
DMAT	6	4	4	4.67
DMS	4	10	10	8.00
EMS	6	10	10	8.67
GIS	4	6	6	5.33
HAND/HANG	6	4	6	5.33
HEMP	8	6	8	7.33
MDM	8	6	6	6.67
MTR	8	6	6	6.67
MWFM	4	6	4	4.67

Table 5-5 Impact Assessment Results

A summary of the relative criticality results is graphically represented in Figure 5-1, where each system is placed in the Low, Medium or High region.

KCP&L SmartGrid
 Demonstration Project
 Risk Assessment Report

Impact Analysis



Figure 5-1 Graphical Representation of Relative Criticality Results



6.0 EXISTING MITIGATION

As described in the risk assessment model, the identification of existing controls (mitigation) plays an important role in evaluating the overall risk rating of the systems. To identify the existing controls several mechanisms are used, these include: interviewing the security implementation team, reviewing system documentation, and studying organization policies and procedures. The identification and analysis can then be used to create a method to quantify the mitigation and which can be used in the risk rating model.

6.1 MITIGATION ANALYSIS ASSUMPTIONS

This mitigation analysis relies heavily on the existing KCP&L policies, processes and the standards. Two assumptions are made while this assessment was conducted. First, all security requirements mandated in the said documents are enforced and are fully implemented in all existing and new systems at KCP&L. Second, all requirements mentioned in these documents are also mandated to the vendors for implementing (at the minimum) similar controls to KCP&L systems hosted by them.

6.2 MITIGATION ANALYSIS TECHNIQUE

The mitigation analysis technique consisted of a series of methodical steps. First, all data transfer interfaces between SmartGrid systems were identified. The interface scope included all interfaces that were planned or existed (at the time this risk assessment was performed) however limited to and/or from the SmartGrid systems. Second, all identified interfaces were mapped to one of the twenty-two NISTIR-7628 Volume-I defined logical interface categories. This task was performed in collaboration with the KCP&L SMEs (the results of the mapping are provided in Appendix B). In the next step, controls recommended in the NISTIR-7628 Volume-I, UCAIug AML, and the UCAIug DM Security Profiles were identified for each applicable interface category. As the final step, the identified controls were compared to the requirements that are mandated by KCP&L policies, standards, and processes for all new and existing systems. A control was considered "fulfilled" if there was a close match between the NISTIR control and the KCP&L requirement. The matching process resulted in a set of security controls that are applicable to SmartGrid systems and their implementation mechanisms already exist at KCP&L.

6.3 MITIGATION ANALYSIS RESULTS

It was determined that only thirteen of the twenty-two interface categories were applicable to KCP&L SmartGrid implementation. And based on the applicable categories, one hundred eighty-one out of one hundred ninety-seven (total recommended security controls in the NISTIR-7628) were found to be applicable to the project. Appendix D lists the applicable security requirements, along with the page

KCP&L SmartGrid
Demonstration Project
Risk Assessment Report

Existing Mitigation

number(s) that each is defined on in the NISTIR-7628 Volume-I. The comparison of the applicable controls with the requirements in the KCP&L's policies, standards, and/or processes, confirmed that ninety-three of the one hundred eighty-one were mandated.

Table 6-1 lists the total number controls recommended by NISTIR-7628 Volume-I and of that total, the number of controls currently mandated by KCP&L. These controls are grouped together by the NISTIR defined control families.

NISTIR 7628 SmartGrid Control Family	Total Number of Controls in each NISTIR-7628 Control Family	Number of Controls Mandated by the KCP&L Policies, Standards, and/or Processes
Access Control (SG.AC)	21	16
Awareness and Training (SG.AT)	7	5
Audit and Accountability (SG.AU)	16	4
Security Assessment and Authorization (SG.SA)	6	2
Configuration Management (SG.CM)	11	10
Continuity of Operations (SG.CO)	11	9
Identification and Authentication (SG.IA)	6	5
Information and Document Management (SG.ID)	5	4
Incident Response (SG.IR)	11	10
Smart Grid Information System Development and Maintenance (SG.SD)	7	5
Media Protection (SG.MP)	6	6
Physical and Environmental Security (SG.PE)	12	0*
Planning (SG.PL)	5	3
Security Program Management (SG.SM)	8	5
Personnel Security (SG.PS)	9	6
Risk Management and Assessment (SG.RA)	6	5
Smart Grid Information System and Services Acquisition (SG.SA)	11	10
Smart Grid Information System and Communication Protection (SG.SC)	30	7
Smart Grid Information System and Information Integrity (SG.SI)	9	5

Table 6-1 Fulfilled NISTIR-7628 Security Requirements by Family

* - The physical security requirements in the NISTIR-7628 are not currently mandated in KCP&L policies, standards, and processes for any of the systems *except* for the EMS. In the case of EMS, it is believed that all 12 physical security requirements are currently mandated by KCP&L. For more information regarding how the mitigation ratings were calculated for both EMS and all other systems, see section 6.4, Table 6-2, and Table 6-3.



6.4 MITIGATION EVALUATION

The method developed to quantify the Mitigation takes into account the NISTIR-7628 listed security controls believed to be implemented for all systems at KCP&L, as well as the Impact, Likelihood and Vulnerability ratings calculated for each system.

The Mitigation calculation for each system can be expressed as:

$$M = (a \times I) + (b \times L) + (c \times V)$$

Where:

a is the Impact Coefficient

I is the Impact Rating

b is the Likelihood Coefficient

L is the Likelihood Rating

c is the Vulnerability Coefficient

V is the Vulnerability Rating

The coefficients are a numerical representation of the number of controls that are specifically put in place by KCP&L to minimize impacts, decrease likelihoods, or guard vulnerabilities. The Impact Coefficient ("a") was determined to be 0.627, which represents the 62.7% of the impact minimizing requirements that are believed to be implemented for all systems at KCP&L. The Likelihood Coefficient ("b") was calculated to be 0.650, which represents the 65.0% of the likelihood decreasing requirements covered by KCP&L policies, procedures, and standards. Similarly, the Vulnerability Coefficient ("c") was calculated to be 0.533, representing the 53.3% of the requirements that specifically address the protection of system vulnerabilities. Thus, the mitigation equation becomes:

$$M = 0.627I + 0.650L + 0.533V$$

To determine the percentages and eventually the coefficients, each of the NISTIR-7628 control families were first assigned a primary purpose: Minimize Impact, Decrease Likelihood, or Guard Vulnerability. The requirements (within each family) that are mandated by KCP&L, were then counted, and a percentage was calculated using the total number of requirements in each NISTIR-7628 control family as a basis.



KCP&L SmartGrid
 Demonstration Project
 Risk Assessment Report

Existing Mitigation

Table 6-2 shows the total requirements for each control family, the number of requirements in each currently mandated by KCP&L, and the calculated percentages for the three coefficients.

NISTIR-7628 Smart Grid Requirement Family	Total Number of Controls in each NISTIR 7628 Control Family	Number of Controls Fulfilled by KCP&L Policies, Standards, and/or Processes	Affect Assignment	Affect Coefficient
Audit and Accountability (SG.AU)	16	4	Impact	0.627
Continuity of Operations (SG.CO)	11	9	Impact	
Information and Document Management (SG.ID)	5	4	Impact	
Incident Response (SG.IR)	11	10	Impact	
Smart Grid Information System Development and Maintenance (SG.MA)	7	5	Impact	
Smart Grid Information System and Information Integrity (SG.SI)	9	5	Impact	
Awareness and Training (SG.AT)	7	5	Likelihood	
Planning (SG.PL)	5	3	Likelihood	
Security Program Management (SG.PM)	8	5	Likelihood	
Access Control (SG.AC)	21	16	Vulnerability	0.533*
Security Assessment and Authorization (SG.CA)	6	2	Vulnerability	
Configuration Management (SG.CM)	11	10	Vulnerability	
Identification and Authentication (SG.IA)	6	5	Vulnerability	
Media Protection (SG.MP)	6	6	Vulnerability	
Physical and Environmental Security (SG.PE)	12	0*	Vulnerability	
Personnel Security (SG.PS)	9	6	Vulnerability	
Risk Management and Assessment (SG.RA)	6	5	Vulnerability	
Smart Grid Information System and Communication Protection (SG.SC)	30	7	Vulnerability	
Smart Grid Information System and Services Acquisition (SG.SA)	11	10	N/A	

Table 6-2 Determination of Mitigation Equation Coefficients

* - A vulnerability coefficient of 0.645 was used to calculate the mitigation rating for EMS. The value of 0.645 was calculated based upon the belief that all 12 physical security requirements from the NISTIR-7628 are currently mandated by KCP&L for the EMS. Currently, KCP&L policies, standards, and processes do not mandate the same level of physical security for the other assessed systems. As implementation of SmartGrid technologies progresses from demonstration to enterprise-wide deployment, the physical security controls mandated by KCP&L policies, standards, and processes will need to be extended to include the other assessed systems to achieve a balanced security profile.



Table 6-3 provides the mitigation values determined for each of the KCP&L SmartGrid System.

System	Relative Vulnerability (V) Rating	Highest Likelihood (L) Rating	System Impact (I) Rating	Combined Mitigation (M) Rating ^a
AHE	6	8	7.33	13.00
ALNK	8	10	7.33	15.36
BMS	5	4	4.67	8.19
CIS	6	8	8.00	13.41
DAD ^b	5	6	4.67	9.49
DCADA	5	6	6.00	10.33
DER - C&I	5	6	4.00	9.07
DER - Grid-Connected	5	6	4.67	9.99
DER - Residential	7	6	4.00	10.14
DERM	7	6	7.33	12.23
DMAT	5	6	4.67	9.49
DMS	4	8	8.00	12.35
EMS	4	10	8.67	14.07 + 0.44**
GIS	5	6	5.33	9.91
HAND/HANG	8	8	5.33	12.81
HEMP	8	10	7.33	15.36
MDM	5	6	6.67	10.75
MTR	8	10	6.67	14.94
MWFM	4	6	4.67	8.96

Table 6-3 Mitigation Rating for Systems

^a - The maximum possible value of 30 for Combined Mitigation Rating is obtained if all security requirements are implemented to guard vulnerabilities, decrease likelihoods, and minimize impacts.

^{**} - The Combined Mitigation Rating for EMS was calculated to be 14.51 (the sum of 14.07 and 0.44) using a vulnerability coefficient of 0.645. The value of 14.07 corresponds to the Combined Mitigation Rating for the EMS if none of the physical security requirements from the NISTIR-7628 were being mandated by KCP&L (i.e. using a vulnerability coefficient of 0.533). See note below Table 6-2 for additional information.

7.0 RISK DETERMINATION

The purpose of this step is to assess the level of risk to the IT system. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of:

- The likelihood of a given threat-source's attempting to exercise a given vulnerability.
- The magnitude of the impact should a threat-source successfully exercise the vulnerability.
- The adequacy of planned or existing security controls for reducing or eliminating risk.⁸

The ultimate goal of a risk assessment is to determine the relative risk of all systems within the scope of the assessment. The risk rating model used in this assessment evaluates all the SmartGrid systems in the environment using common criteria in order to provide a scaled risk value for each. Since each system was evaluated using the same criteria, the resulting risk ratings may be used to prioritize mitigation actions.

There are many kinds of risk which may require different kinds of response or mitigation. For example, reliability risk to a substation would be given a different priority than reputational risk to the corporate website. Some examples of different types of risk are:

- Operational Risk: Risk that directly concerns the functions or operational state of systems
- Reliability Risk: Risk that directly impacts the local or regional reliability of power systems
- Financial Risk: Risk of lost revenue or reduced profit
- Reputational Risk: Risk of damage to corporate reputation or public goodwill
- Compliance Risk: Risk of failing to meet regulatory requirements

7.1 RISK-RATING MATRIX

The model used in this report to evaluate system risk is described in the Introduction section and referenced throughout the report. Values for the criteria used in the risk rating model have been evaluated and described earlier in this report. For each system, existing mitigating controls reduce the calculated risk rating in order to arrive at the Overall Risk Rating value. The output of those evaluations and calculations has been entered into Table 7-1 which shows the Overall Risk Rating for each system.

⁸ U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, *Special Publication 800-30: Risk Management Guide for Information Technology Systems*, July 2002.

KCP&L SmartGrid
Demonstration Project
Risk Assessment Report

Risk Determination

System	Threat Rating (T) ↓	Relative Vulnerability Rating (V) ↓	Highest Likelihood Rating (L) ↓	System Impact Rating (I) ↓	Combined Mitigation Rating (M) ↑	Overall Risk Rating (R)
AHE	8	6	8	7.33	13.00	16.34
ALNK	8	8	10	7.33	15.36	17.97
BMS	7	5	4	4.67	8.19	12.48
CTS	7	6	8	8.00	13.41	15.59
DADs (Field & Substation)	6	5	6	4.67	9.49	12.18
DCADA	8	5	6	5.00	10.33	14.67
DER - C&I	6	3	6	4.00	9.07	11.93
DER - Grid-Connected	6	3	6	4.67	9.49	12.18
DER - Residential	6	7	6	4.00	10.14	12.86
DERM	6	7	6	7.33	12.23	14.10
DMAT	5	5	6	4.67	9.49	11.18
DMS	8	4	8	8.00	12.35	15.65
EMS	8	4	10	8.67	14.51	16.15
GIS	7	5	6	5.33	9.91	13.42
HAND/HANG	6	8	8	5.33	12.81	14.53
HEMP	7	8	10	7.33	15.36	16.97
MDM	8	5	6	6.67	10.75	14.92
MTR	8	8	10	6.67	14.94	17.72
MWFM	7	4	6	4.67	8.96	12.71

Table 7-1 Risk Rating Matrix

↓ - Denotes that lowering the component rating will lower the Overall Risk Rating.

↑ - Denotes that raising the component rating will lower the Overall Risk Rating.

7.2 RISK DETERMINATION

The calculated values for the Overall Risk Rating can be used to assist with prioritizing mitigation actions. An established level of acceptable risk must be determined for each individual system based on operational and business-level factors. These risk ratings will change over time and should be re-evaluated regularly in order to recalculate each system's overall risk.

To further prioritize mitigation actions, it was necessary to calculate a high-level estimate of effort necessary to mitigate each system. This estimate was based solely upon environmental considerations for each system: physical location, operating system, availability of updates, etc. The rating uses the criteria listed in Table 7-2 to calculate the estimate of effort required to apply mitigations to each system. The maximum value for the estimated mitigation effort is 10. With some SmartGrid systems still in the planning phases, and considering the complexity of the environment, certain aspects of the mitigation effort criteria have been estimated based on information gained during personal interviews. For example, the "No Remote Administration" criterion was only applied if that information was specifically identified for a particular system. Similarly, for systems hosted remotely, criteria were assigned based on

KCP&L SmartGrid
Demonstration Project
Risk Assessment Report

Risk Determination

conversations and questionnaire responses. The criteria were carefully evaluated, however, it is possible that some criteria were missed, or have been incorrectly assigned.

Criteria #	Criteria	Effort Rating Modifier
1	System Hosted Locally	+1
2	System Hosted Remotely	+2
3	System Located at Customer or Field Locations	+3
4	Windows Operating System or applications	+1
5	Unix-based Operating System or applications	+1
6	Proprietary Operating System or Applications	+2
7	No Remote Administration	+2
8	No Regularly Scheduled Updates	+1
9	Public Access to System	+2
10	Greater than 20 Devices in System	+1
11	Virtual Server	+1
12	Unsupported Operating System	+2
13	System Contains PII	+1

Table 7-2 Mitigation Effort Criteria

Table 7-3 assigns estimated mitigation effort values to each KCP&L SmartGrid system within the scope of this assessment.

System	System ID	Assigned Mitigation Effort Criteria	Estimated Mitigation Effort
AHE	1	2, 4, 11	4
ALNK	2	1, 4, 9, 11, 13	6
BMS	3	3, 9	5
CIS	4	1, 5, 13	3
DADs (Field & Substation)	5	3, 6, 8, 10	7
DCADA	6	1, 6, 7, 8, 10	7
DER - C&I	7	3, 6, 8	6
DER - Grid-Connected	8	1, 6, 8	4
DER - Residential	9	3, 6, 8, 9	8
DERM	10	2, 6	4
DMAT	11	2, 6	4
DMS	12	1, 4	2
EMS	13	1, 4	2
GIS	14	1, 5, 8	3
HAND/BANG	15	3, 6, 8, 9, 10	9
HEMP	16	2, 5, 9, 13	6
MDM	17	2, 4	3
MTR	18	3, 6, 7, 8, 10	9
MWFM	19	3, 6, 8, 10, 13	8

Table 7-3 Estimated Mitigation Effort for SmartGrid Systems

As stated in the Introduction, the most common action which can be taken in response to an evaluated threat is mitigation. The goal of applying mitigating security controls to systems is to reduce the level of



risk by eliminating vulnerabilities, or lessening the likelihood or impact of a threat exploiting vulnerabilities.

Figure 7-1 illustrates the distribution of KCP&L's SmartGrid systems within the risk rating and mitigation effort values. Each system was assigned a numeric identification number in Table 7-3, which is used to represent that system in Figure 7-1.

The first step in planning risk mitigation is to prioritize which systems and controls will be implemented first. When planning mitigations, reducing the risk of all systems should be a goal, but using Figure 7-1 as a guide, mitigations for each system can be prioritized to focus on those systems most at risk first, while still working to reduce the overall risk to all systems. Section 8.0 provides more risk mitigation recommendations and details.

Although the Risk Rating values can be used to prioritize mitigation actions, there is no ideal or static target Risk Rating. Since environments are always changing, new threats are always emerging, and new vulnerabilities are discovered every day, system risk is not a static point. Therefore, mitigation actions must not be static either. Risk must be regularly re-evaluated to ensure newly implemented mitigations and controls are functioning as expected, and new threats or vulnerabilities have not increased system risk.



KCP&L SmartGrid
 Demonstration Project
 Risk Assessment Report

Risk Determination

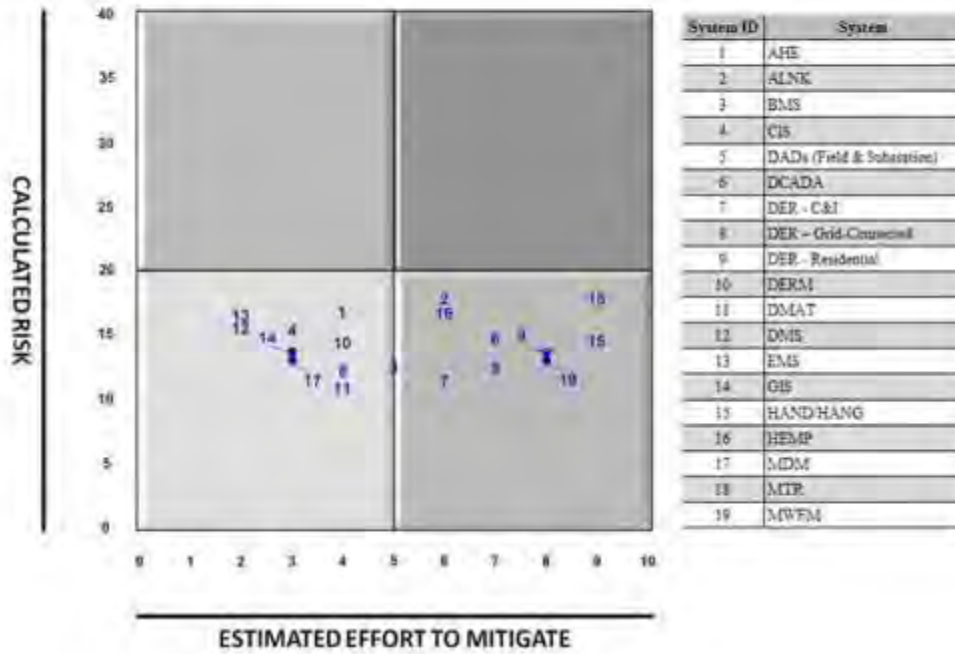


Figure 7-1 Risk Rating Categories

As shown in Figure 7-2, Risk Management is not a one-time process but rather a cycle of continuous improvement.





Figure 7-2 Risk Management Cycle

This report is the conclusion of the Assessment Phase of the cycle. In the Mitigation Phase, policy procedure, and technical controls are implemented to reduce the factors of vulnerability, impact, or likelihood. In the Educate Phase, management, administrators, users, and customers are trained in or informed of the new controls, how they operate, and why they are in place. In the Evaluate Phase, the new controls are reviewed and monitored to assure they both function as expected and do not introduce any unexpected vulnerability.

8.0 RISK MITIGATION

The completion of a risk assessment should result in a set of actionable mitigation steps that can be taken by the organization to make its systems secure. The mitigation recommendations provided in this section are specific to the SmartGrid project at KCP&L and are primarily driven by the results from the end-to-end risk assessment. The KCP&L SmartGrid Trust Model³ was also used as an important reference while creating these mitigation recommendations. The KCP&L Trust Model domains (*Secured, Restricted, Controlled, and Uncontrolled*) were used to develop recommended security zones for KCP&L SmartGrid systems and to determine the security controls for data stored and/or generated by the systems. The Trust Model transport classes (*Trusted, Managed, and Public*) were used to determine the security controls for data transmitted between systems.

The mitigation recommendations resulting from the risk assessment fall into one of the following two types of security control implementations:

Creation of Security Zones and Implementation of Tailored Control Sets: A security zone is defined as a group of SmartGrid systems that have the same criticality level and perform similar business functions. A tailored control set is a collection of security requirements that are applicable to all systems in a security zone or to all interfaces between two security zones.

Implementation of Industry-Suggested Control Sets: An industry-suggested control set is a subset of the NISTIR-7628 Volume-1 security requirements that are applicable to a SmartGrid system based upon its interfaces.

Detailed descriptions of both security control implementations are covered in the following subsections.

8.1 CREATION OF SECURITY ZONES AND IMPLEMENTATION OF TAILORED CONTROL SETS

This type of security control implementation includes a collection of security controls specifically tailored for the SmartGrid project based upon security zones and interfaces between security zones. As mentioned above, each security zone includes SmartGrid systems that have the same criticality level and perform similar business functions. The goal of this implementation is to recommend controls that will bring high risk systems down to medium risk and adequately protect the systems based on their impact levels. As

³ KCP&L Green Impact Zone SmartGrid Demonstration, *SmartGrid Cyber Security Plan*, Version v1.0 - November 18, 2010

such, the selection of controls in this type of implementation is also based on the risk and impact ratings calculated for each system as part of the end-to-end risk assessment.

8.1.1 Security Zones

First, the SmartGrid systems are placed into cyber security zones. This placement should be based upon the criticality of the system and the business function it performs. The eight security zones that are recommended are as follows:

8.1.1.1 Energy Operations - High

The primary purpose of this group of systems is energy management. All systems belonging to this zone are highly critical. These systems also belong to the *Secured* KCP&L Trust Model domain. In addition, all interfaces receiving or sending data to or from this security zone belong to the *Trusted* transport class within KCP&L's Trust Model.

8.1.1.2 Distribution Operations - High

All highly critical systems that contribute towards the function of distribution management reside in this security zone. The *Secured* KCP&L Trust Model domain will be applicable to this zone, while the interfaces will be in the *Trusted* transport class.

8.1.1.3 Customer Operations - High

Systems included in this zone are also highly critical, but their primary function is customer management. These systems fall under the *Secured* domain in the KCP&L Trust Model, while its interfaces belong to the *Trusted* transport class.

8.1.1.4 Distribution Operations - Medium

Systems in this security zone have the primary function of distribution management; however, their criticality level is medium. The KCP&L Trust Model domain applicable to this zone is the *Restricted* domain. The zone interfaces belong to either the *Trusted* or *Managed* transport classes.

8.1.1.5 Delivery Operations – Medium

This group of systems performs the function of energy delivery, yet all its systems are all moderately critical to overall operations. These systems are within the *Restricted* KCP&L Trust Model domain, while their data interfaces fall under the *Trusted* or the *Managed* transport classes.

8.1.1.6 Customer Operations – Medium

All systems whose criticality to the organization is moderate and whose primary functionality is customer-facing business operations fall within this security zone. The applicable KCP&L Trust Model domain for this security zone is the *Restricted* domain. As with the other moderately critical security zones, the interfaces in this zone belong to either the *Trusted* or *Managed* transport classes.

8.1.1.7 Distribution Operations – Low

This security zone should house systems that are part of the distribution network but only the ones whose criticality is determined to be low. These systems belong to the *Controlled* domain in the KCP&L Trust Model. The interfaces for the systems in this security zone belong to the *Managed* transport class.

8.1.1.8 Deliver Operations – Low

Systems in this security zone have low criticality and solve the business function of servicing or supporting field issues. Systems from this security zone reside in the *Controlled* domain, while their interfaces belong to the *Managed* transport class within the KCP&L Trust Model.

8.1.1.9 Customer Operations – Low

All systems that are owned and managed by KCP&L customers belong to this security zone. Since KCP&L has little to no control over these systems, the Trust Model domain assigned to this zone is *Uncontrolled*. The interfaces for these systems are mainly located at customer premises, and as such, the transport class most suitable is the *Public* class.

Table 8-1 lists the recommended security zone for each SmartGrid system.



KCP&L SmartGrid
 Demonstration Project
 Risk Assessment Report

Risk Mitigation

System	Security Zone
AHE	Delivery Operations - Medium
ALNK	Customer Operations - Medium
BMS	Customer Operations - Low
CIS	Customer Operations - High
DCADA	Distribution Operations - Medium
DER - C&I	Customer Operations - Low
DER - Grid-Connected	Distribution Operations - Low
DERM	Distribution Operations - Medium
DER - Residential	Customer Operations - Low
DMAT	Delivery Operations - Low
DMS	Distribution Operations - High
EMS	Energy Operations - High
Field DADs	Distribution Operations - Low
GIS	Delivery Operations - Low
HAND	Customer Operations - Low
HANG	Customer Operations - Low
HEMP	Customer Operations - Medium
MDM	Delivery Operations - Medium
MTR	Delivery Operations - Medium
MWFM	Delivery Operations - Low
Substation DADs	Distribution Operations - Low

Table 8-1 Security Zone Recommendations for SmartGrid Systems

Figure 8-1 provides a graphical view of the recommended security zones.



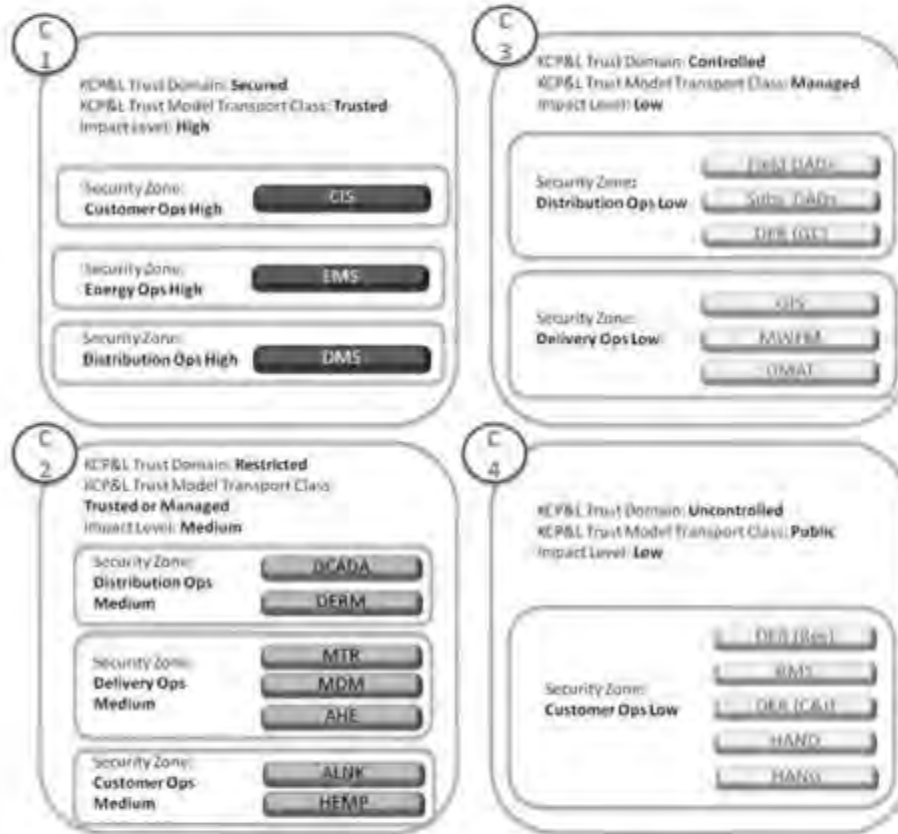


Figure 8-1 Representation of SmartGrid Systems in Respective Security Zones

8.1.2 Tailored Control Sets

Second, security control sets are created that tailor to the security zones and interfaces between them. Each control set is a collection of security requirements from the NISTIR-7628 Volume-I as well as many of the ones included in the UCA International Users Group (UCAIUG)³⁸ AMI and DM Security Profiles. The security requirements in each set are also determined based upon the risk and impact ratings calculated for the SmartGrid systems as part of the risk assessment. Following is the definition of each control set and its applicability in the SmartGrid project.

* UCA International Users Group <http://www.ucaiug.org/default.aspx>



8.1.2.1 Control Set – C0

The control set C0 represents security requirements that are common to all security zones (except *Customer Operations – Low*) and the interfaces between any two security zones.

8.1.2.2 Control Set – C1

This set represents common requirements for systems that belong to one of the high impact security zones. This control set is also applicable to all data transfers within the high impact security zones. That is, any system that is part of *Customer Operations – High*, *Distribution Operations – High*, or *Energy Operations – High* should be implemented with C0 and C1.

8.1.2.3 Control Set – C2

This control set is specifically chosen for systems that belong to one of the medium impact security zones. As such, any system that has been placed in *Delivery Operations – Medium*, *Customer Operations – Medium*, or *Distribution Operations – Medium* should be implemented with control sets C0 and C2. This control set is also applicable to all data transfers within the medium impact security zones.

8.1.2.4 Control Set – C3

This set represents security requirements for low impact systems that are managed by the KCP&L staff. This set, therefore, is only applicable to the systems that are either in the *Distribution Operations – Low* or *Delivery Operations – Low* security zones. This control set is also applicable to all data transfers within the low impact security zones managed by KCP&L. The control sets C0 and C3 should be implemented in conjunction for these zones.

8.1.2.5 Control Set – C4

This set of security requirements is created for KCP&L end customers. The set represents control mechanisms to be suggested to the customers as they manage the *Customer Operations – Low* security zones. This set may not be mandated by KCP&L; however, it is recommended that KCP&L suggest this set to all customers participating in the SmartGrid program. To restate, all systems within the *Customer Operations – Low* security zone need only implement the controls within set C4.

8.1.2.6 Control Set - C5

This set represents the security requirements that are recommended for all interfaces between high impact security zone(s) and medium impact security zone(s). This set should be implemented along with the control set C0.



8.1.2.7 Control Set – C6

All interfaces between high impact security zone(s) and low impact security zone(s) should be implemented with these requirements. The control sets C0 and C6 should be implemented together for all such interfaces.

8.1.2.8 Control Set – C7

This set represents the security requirements that are recommended for all interfaces between medium impact security zone(s) and low impact security zone(s). This set should be implemented along with the control set C0.

8.1.2.9 Control Set – C8

All interfaces between medium impact security zone(s) and the *Customer Operations - Low* security zone should be implemented with these requirements. Note that some of these requirements may need to be fulfilled by the consumers. For the interfaces that involve data being sent to KCP&L from the *Customer Operations - Low* security zone, both control sets C0 and C8 should be implemented.

Figure 8-2 provides a visual representation of the control sets applicable to each security zone and their interfaces. For a list of the NISTIR-7628 security controls that are contained in each control set, see Appendix F.

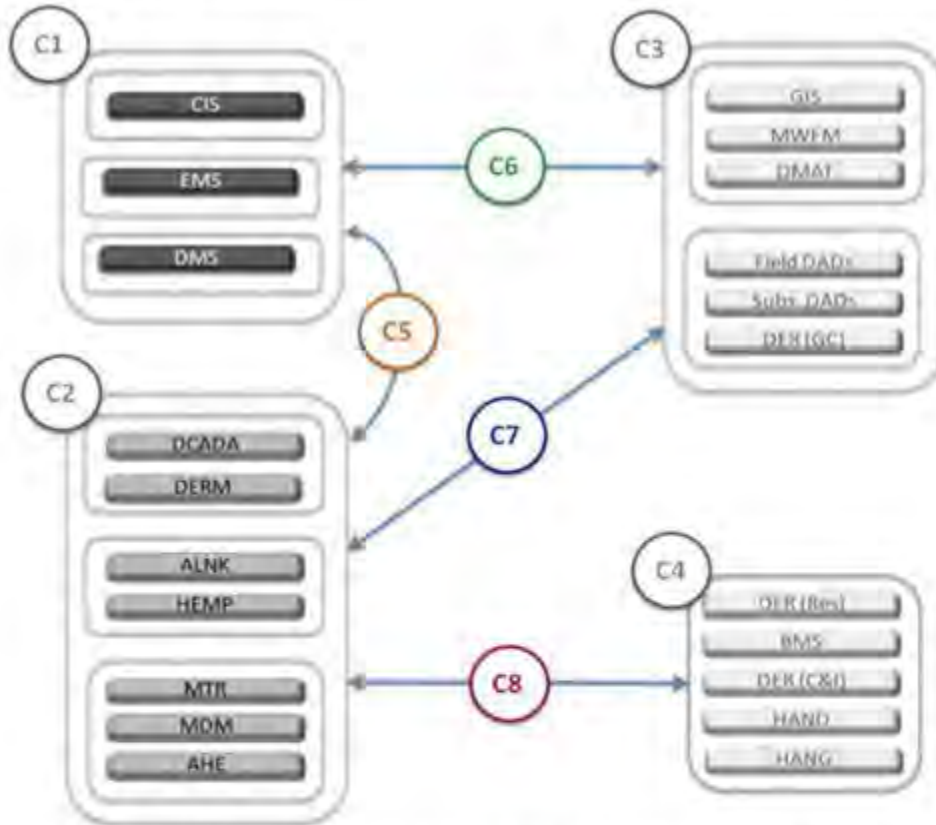


Figure 8-2 Representation of Control Sets for Inter-Security Zone Communication

8.2 INDUSTRY-SUGGESTED CONTROLS

The second type of security control implementation is a collection of controls based on industry best practices and guidelines. This type lists all the controls suggested in the NISTIR-7628 Volume-1²⁷ based strictly on the applicable Logical Interface Categories and their recommended controls. These security requirements, if implemented to their fullest, should adequately secure the SmartGrid systems. It is worth noting that the controls recommended in the implementation type discussed in section 8.1.2 are a subset of the controls recommended in this type.

²⁷ NIST Interagency Report 7628 Volume 1, http://csrc.nist.gov/publications/nistir/nistir-7628_vol1.pdf

Table 8-2 provides a summarized listing of the KCP&L SmartGrid systems along with their applicable NISTIR-7628 Logical Interface Categories. A brief definition of each NISTIR Logical Interface Category is available in Appendix A. The table indicates that a majority of the NISTIR-7628 security requirements were found to be applicable to all the SmartGrid systems. To improve readability and act as a quick reference, the table lists requirements in the format "All Except..." the requirements found not to be applicable."



KCP&L SmartGrid
 Demonstration Project
 Risk Assessment Report

Risk Mitigation

SmartGrid System	Applicable NISTIR-7628 Logical Interface Categories	Applicable NISTIR-7628 Security Controls ⁶
AHE	5, 13, 14	All Except: SG.AC-12, SG.IA-5, SG.SC-4, SG.SC-17
BMS	15	All Except: SG.AC-11, SG.AC-12, SG.AU-16, SG.IA-5, SG.SC-4, SG.SC-6, SG.SC-9, SG.SC-17, SG.SC-26, SG.SC-29
CIS	7, 8, 10	All Except: SG.SC-6, SG.SC-9, SG.SC-17
DCADA	1, 2, 3, 3	All Except: SG.AC-12, SG.AU-16, SG.SC-4, SG.SC-9, SG.SC-17, SG.SC-26
DER - C&I, DER - Grid- Connected, DER - Residential	11	All Except: SG.AC-11, SG.AC-12, SG.AC-14, SG.AU-16, SG.IA-4, SG.IA- 5, SG.IA-6, SG.SC-3, SG.SC-4, SG.SC-5, SG.SC-6, SG.SC-7, SG.SC-9, SG.SC-17, SG.SC-26, SG.SC-29, SG.SI-7
DERM	8, 9, 16	All Except: SG.SC-6, SG.SC-17, SG.SC-29
DMS	5, 10	All Except: SG.AC-12, SG.AU-16, SG.IA-5, SG.SC-3, SG.SC-9, SG.SC-26
FMS	1	All Except: SG.AC-12, SG.AU-16, SG.SC-4, SG.SC-6, SG.SC-9, SG.SC-26
Field DADs, Substation DADs	11	All Except: SG.AC-11, SG.AC-12, SG.AC-14, SG.AU-16, SG.IA-4, SG.IA- 5, SG.IA-6, SG.SC-3, SG.SC-4, SG.SC-5, SG.SC-6, SG.SC-7, SG.SC-9, SG.SC-26, SG.SC-29, SG.SI-7
GIS	10	All Except: SG.AC-12, SG.AU-16, SG.IA-5, SG.SC-3, SG.SC-6, SG.SC-9, SG.SC-26
HAND, HANG	15	All Except: SG.AC-11, SG.AC-12, SG.AU-16, SG.IA-5, SG.SC-6, SG.SC-4, SG.SC-9, SG.SC-26, SG.SC-29
HEMP	8, 16	All Except: SG.SC-5, SG.SC-6, SG.SC-29
MDM	7, 8, 10	All Except: SG.SC-6, SG.SC-9
MTR	15	All Except: SG.AC-11, SG.AC-12, SG.AU-16, SG.IA-5, SG.SC-4, SG.SC-6, SG.SC-9, SG.SC-26, SG.SC-29

Table 8-2 NISTIR-7628 Security Requirements Applicability by System

⁶ - ALHE, DMAT, and MWEM are not specifically listed in this table because their interfaces are covered under the interfaces of HEMP, MFD, and CIS, respectively.



The detailed results of determining which security controls are currently mandated by KCP&L are included in Appendix E. For each of recommended security control from the NISTIR-7628, this appendix lists the following information:

- The applicable Logical Interface Category from Table 1-2
- The corresponding recommended security control from the UCAIug Security Profile for AMI
- The corresponding recommended security control from the UCAIug Security Profile for DM
- Indication of requirement being mandated by KCP&L policies, standards, and/or processes
- Reference to KCP&L policy, standard, and/or process, if applicable

For a few requirements, the readers will find that the fulfillment of a control is stated as *No*. This is to indicate that the requirement is believed to not be currently fulfilled based upon analysis of KCP&L's policies, standards, and processes and discussion with the KCP&L Security Team.

See Appendix H for a list of the security requirements from the UCAIug Security Profiles for AMI and DM that were not confirmed to be covered in the NISTIR-7628. A further discussion will be needed with the KCP&L security team to confirm whether these security requirements are already fulfilled and if not, whether they should be implemented as part of the project.

9.0 PROJECT RECOMMENDATIONS

The success of the SmartGrid program is heavily dependent on the commitment from Senior Management and the implementers to deploy secure systems. This risk assessment for the KCP&L SmartGrid program was an important step towards ensuring cyber security. The United States Department of Energy (DOE) has also made cyber security a key focus area in all government-funded SmartGrid programs. On several occasions, the DOE has indicated that the success of individual programs will be dependent on the strength of deployed cyber security. The recommendations provided in this section are aimed towards maintaining KCP&L's focus on and commitment to implementing a secured SmartGrid program.

9.1 SELECT AND IMPLEMENT CONTROLS

Section 8.0 provided a recommended a list of procedural, operational, and technical controls to be implemented for securing the SmartGrid systems. The KCP&L cyber security team should assess each of these controls and select the ones that will be implemented. For the systems that are hosted externally by a third-party, the selected list of security controls should be made mandatory implementations enforced through contracts. For the systems that are hosted internally, the selection process should start with verification of all controls that are unconfirmed (Appendix E) to be currently met by KCP&L policies, procedures, and standards.

A three-phase implementation strategy should be considered. Phase I should include controls that need be implemented immediately to increase the security of systems already in place and the systems whose implementation is planned to be in next 1-3 months time. Phase II should include all controls not included in Phase I but are suggested in the tailored control sets (Section 8.0). The implementation of Phase II controls should be coordinated with the master system implementation schedule. Phase III implementation should include all controls that are covered in Section 8.0 but not included in Phases I and II.

9.2 CREATE SECURITY ZONES

Network segregation based on systems' business functions, criticality level, and physical location is one of the key factors for a successful cyber security implementation. It is recommended that the eight security zones suggested in Section 8.0 are implemented using a combination of firewalls, switch and router access control lists, authentication boundaries, and physical security measures. This action should be performed in collaborative design sessions between network designers, system integrators, subject matter experts and the security team. The creation of security zones is an important step towards a secured architecture.



9.3 CREATE A SECURITY IMPLEMENTATION PLAN

A plan should be created to depict the commissioning of controls and the security zones. The plan should identify the controls, implementation schedule, roles, responsibilities and the budget. This plan should be approved, signed, and periodically reviewed by KCP&L Senior Management. A Key Performance Indicators (KPI) matrix should be created to keep track of the implementation and provide KCP&L management a quick view of the progress. Close attention by Senior Management on the cyber security implementation is verified to be one of the key periodic evaluation criteria for the DOE.

A very tight working relationship between the integration and security team is strongly encouraged for the success of the security program for the SmartGrid systems. The security implementation schedule should mirror the master implementation schedule with key milestones tied between the two plans. The security team should also be required to provide their official "sign-offs" to all system documentation.

9.4 UPDATE THE CYBER SECURITY PLAN FOR THE DOE

The findings of the risk assessment and the resultant controls selection should be conveyed to the DOE by updating the previously submitted cyber security plan. A periodic review and update to the cyber security plan is not only one of the requirements of DOE grant projects, but is also another criterion used by the DOE during their evaluation visits. It is recommended that the signed security implementation plan be submitted as a supplement to the cyber security plan as an evidence of Senior Management's commitment to the cyber security of the SmartGrid systems.

9.5 CREATE SECURITY REQUIREMENTS FOR ALL SYSTEMS IN THE PROJECT

The control sets provided in Section 8.0 are conceptual controls which need to be converted to actual controls. The actual controls should identify firewalls, port numbers, monitoring software, encryption techniques, authentication, authorization, and other specific parameters. The actual security requirements should be created for each system and data interface. Each vendor should be provided with their system's security requirements and, where applicable, the contracts should be modified to make implementation of security requirements as payment milestones.

9.6 RECOMMENDATIONS FOR EXTERNALLY HOSTED SYSTEMS

Several systems within the SmartGrid environment are hosted by contracted vendors outside the physical control of KCP&L support and management personnel. This produces some unique challenges for

ensuring the Confidentiality, Integrity, and Availability of the data produced, processed, stored, or transmitted to or from those systems.

Although each vendor is bound by service contracts with KCP&L, the nature of the information being exchanged dictates the need to actively monitor and assess the measures being taken to provide safeguards for both data at rest, and data in motion. During the course of this risk assessment, it became apparent that each vendor had implemented or planned specific controls to protect the data that will be transmitted to and stored on their systems. It was also apparent that each vendor implemented controls according to their own internal policies and processes.

Providing guidance to vendors and ensuring uniform and adequate security controls for KCP&L's data is just one aspect of a robust vendor risk management program that KCP&L should implement. In 2009, Gartner Research released a series of papers in a special report dedicated to assessing, managing, and reducing all aspects of vendor risks.³⁸ This Special Report also outlines many aspects of managing vendor risks outside of information and IT security.

Many other organizations and security professionals have also provided guidance for managing vendor risk. For example, Evantix lists the steps for establishing a vendor risk management program as: Corporate Governance, Vendor Contracts, Risk Assessments, Onsite Audit, Reporting, and Risk Monitoring.³⁹ Another risk management vendor, PivotPoint Security, points out that companies may outsource many things, including call centers, application development, or IT operations, but they cannot outsource responsibility or liability.⁴⁰

At the current stage of implementation and integration, KCP&L should begin by focusing on performing a thorough risk assessment of their chosen SmartGrid service providers, potentially including an onsite audit of information, transmission, and physical security. If the current service contracts do not have a provision for performing such an audit, KCP&L should ask each vendor to document their operational and security controls as thoroughly as possible. Appendix G provides a sample questionnaire that can be customized for each vendor to simplify the information gathering process.

³⁸ Gartner, Inc., *Special Report: Vendor Risk Management*, 2009.

<http://www.gartner.com/technology/research/reports/vendor-risk-management.jsp>

³⁹ Evantix, LLC, Rene Baraza, *6 Steps to Establishing A Vendor Risk Management Program*, 26 July, 2010.

<http://www.evantix.com/blog/39941/6-Steps-For-Building-a-Vendor-Risk-Management-Program>

⁴⁰ Pivot Point Security, Inc., *Vendor (& Partner) Information Security Risk Management*, 28 March, 2011

Security control recommendations are detailed earlier in this report, but for externally hosted systems, the following should be the minimum recommended high-level requirements for maintaining the Confidentiality, Integrity, and Availability of KCP&L's data. Note that these recommendations do not supersede those made in Section 8.0. This list is merely a benchmark to ensure that external vendors meet a set of minimum security requirements. Vendors should provide written documentation verifying compliance with these baseline security control requirements.

9.6.1 Authentication

All access to externally hosted systems, whether interactive human access, or automated system or application access, should provide some type of authentication. This authentication may take the form of interactive passwords, public key certificates, secret key cryptography, or similar mechanisms.

9.6.2 Authorization

Every account on externally hosted systems should limit the user or remote system to specific functions required to perform specific tasks.

9.6.3 Transmission Security (Public)

Data in motion across public transmission media such as the Internet, cellular networks, or wireless networks, should be encrypted with a strong, proven algorithm such as AES and RSA, or certificate encryption such as SSL. This recommendation applies to KCP&L data classified as "Restricted" or "Internal Use Only."

9.6.4 Transmission Security (Private)

Data in motion across private transmission media such as dedicated hardwired circuits should be accessed only by those individuals with a justified need (i.e. data owner or administrator).

9.6.5 Data Storage Security

Data at rest on backup or storage media should be afforded the same level of security controls as the externally hosted system from which the data originated. Backup media stored in a public facility should be afforded the same level of control listed above under "Transmission Security (Public)".

9.6.6 Physical Security

Physical access to externally hosted systems should be restricted to those individuals requiring access for specific functions, such as system administrators, data center staff, or select maintenance personnel.



9.6.7 Auditing and Accountability

All externally hosted systems should be configured to provide detailed audit logs of all unauthorized activity and all system-level or privilege use activity on the system. These audit logs should be kept for a period of time prescribed by KCP&L and should be made available to authorized KCP&L personnel upon request.

9.6.8 Incident Response and Disaster Recovery

Externally hosted systems should be covered by a robust incident response plan, produce verified backups on a regular basis, and be subject to periodic recovery tests to ensure system recoverability in the event of an incident. In addition, highly critical systems should be designed with network and system redundancy with rapid failover in the event of a major service disruption.

9.6.9 Risk Assessment

All externally hosted systems should be subject to scheduled security audits and risk assessments performed by KCP&L or a designated third-party vendor.

Ensuring these baseline security controls are implemented for all externally hosted systems will establish a minimum level of assured security for KCP&L data residing outside the control of KCP&L personnel.

9.7 POLICY UPDATES ON RECOMMENDED PROCEDURAL CONTROLS

Several procedural and operational controls were recommended in Section 8.0. It is recommended that existing KCP&L Policies, Standards and Processes documentation be modified with these controls. This could be accomplished by either creating addendums to the existing policies or creating supplements. It is also recommended that existing policy enforcement mechanisms be extended to the SmartGrid systems, serving as further evidence of commitment from Senior Management to a secured implementation of SmartGrid program at KCP&L.

9.8 CREATE & EXECUTE TEST CASES

It is very important that the security controls and architecture are tested to verify deployment as intended. A series of test cases should be created and executed to ensure systems are secured. The test cases should also cover any externally hosted system and field equipment. Considerations should be given to create a test environment to perform rigorous testing. Two types of tests should be conducted: Verification against the Design Specifications and Penetration Tests. The results should be reviewed with the Senior Management, system integrators, network designers, and security team. Changes to the system should be

made and tests re-executed when needed. The processes should be repeated until the results are accepted by the SmartGrid system stakeholders.

9.9 PERFORM PERIODIC SECURITY ASSESSMENT

A security assessment in each SDLC phase shall be conducted to assess cyber vulnerabilities and threats to the SmartGrid systems. The assessments should be conducted in accordance with principles and standards set forth by organizations like NIST and NERC. This step will ensure that the systems are protected up to the date and cyber security focus is maintained throughout the project duration. A strategy should be crafted to incorporate SmartGrid systems (once the project is over) into the existing production systems security assessments.

9.10 PARTICIPATE IN WORKING GROUPS

There are several ways to keep pace with ever-changing cyber security requirements. It is recommended that the security and operational teams at KCP&L participate and collaborate in cyber security working groups created specifically for the utility industry, several of which are mentioned in this report. Table 9-1 provides a good coverage of working groups dealing with various aspects of security and functionality of smart grid applications.

Area of Responsibility	Industry Interest Group	Website
Distribution	SGIP	http://collaborate.nsl.gov/wiki/smartgrid/bin/view/SmartGrid/SGIP
	Zigbee Alliance	http://www.zigbee.org/
	UCADag	http://www.ucadag.org/default.aspx
	SGMM	http://www.sei.cmu.edu/smartgrid/tecol/
Transmission	Transmission Forum	http://www.transmissionforum.net/forum/
	ICSFWG	http://www.us-cert.gov/control_systems/icsfwg/index.html
	IEC 61850 User Group	http://iec61850.ucadag.org/default.aspx
	NERC 706 SDT	http://www.nerc.com/files/standards/Cyber_Security_initiatives.html
Cyber Security	EEL Cyber Security	http://www.eel.org/ourissues/Electricity_Transmission/Pages/CyberSecurity.aspx
	NERC 706 SDT	http://www.nerc.com/files/standards/Cyber_Security_initiatives.html
	ISA	http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821
	NEESCO	http://www.energysoc.org/nesco
Physical Security	UTC	http://www.utc.org/
	ASIS International	http://www.asisonline.org/
	NERC 706 SDT	http://www.nerc.com/files/standards/Cyber_Security_initiatives.html
	SIA	http://www.siaonline.org/

Table 9-1 Industry Working Groups

9.11 CONCLUSION

Performing a risk assessment on the majority of systems in the KCP&L SmartGrid Demonstration Project produced a large amount of documentation and data. The analysis for some systems confirmed the risk level previously assumed prior to the risk assessment, while for others indicated the need for either additional security, or the need to reduce some of the focus. It soon became apparent that the protection of systems like the DMS, HEMP, AHE, and others was critical to the success of the project. In other cases, systems like the Field and Substations DADs, were found to be at lower risk than originally expected.

Another discovery was that the most critical and highest impact systems were not necessarily those with the highest level of assessed risk, due to existing security controls in place for those systems. Processing each cyber asset through the risk rating model provided an accurate and objective evaluation of each system's current risk, and allowed the assessment team to provide focused recommendations for system security zones, network segmentation, and mitigating controls.

To date, KCP&L SmartGrid program personnel have provided proper attention to the cyber security needs of the project in accordance with the DOE's expectations. This risk assessment and its reliance on industry standards and best practices was an important step towards a secure KCP&L SmartGrid infrastructure. Continued support from KCP&L management and focus from the project and security teams to implement these recommendations is needed to ensure the success of the project.



APPENDIX A THE NISTIR-7628 LOGICAL INTERFACE CATEGORIES

NISTIR-7628 Logical Interface Category	NISTIR-7628 Logical Interface Category Description
1	Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints
2	Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints
3	Interface between control systems and equipment with high availability, without compute nor bandwidth constraints
4	Interface between control systems and equipment without high availability, without compute nor bandwidth constraints
5	Interface between control systems within the same organization
6	Interface between control systems in different organizations
7	Interface between back office systems under common management authority
8	Interface between back office systems not under common management authority
9	Interface with B2B connections between systems usually involving financial or market transactions
10	Interface between control systems and non-control/corporate systems
11	Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements
12	Interface between sensor networks and control systems
13	Interface between systems that use the AMI network
14	Interface between systems that use the AMI network with high availability
15	Interface between systems that use customer (residential, commercial, and industrial) site networks
16	Interface between external systems and the customer site
17	Interface between systems and mobile field crew laptops/equipment
18	Interface between metering equipment
19	Interface between operations decision support systems
20	Interface between engineering/maintenance systems and control equipment
21	Interface between control systems and their vendors for standard maintenance and service
22	Interface between security/network/system management consoles and all networks and systems

APPENDIX B KCP&L TO NISTIR-7628 LOGICAL INTERFACE MAPPING

NISTIR-7628 Logical Interface Category Description	NISTIR-7628 Logical Interface Category	From	To	KCP&L Logical Interface	NISTIR-7628 Logical Interface
Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints	1	EMS	Substation DADs	3	U67
		DDC	DER	26	U65
Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints	2	DDC	Field DAD	11	U117
Interface between control systems and equipment with high availability, without compute nor bandwidth constraints	3	DDC	Substation DAD	21	U117
Interface between control systems within the same organization	5	AHE	Legacy OMS	2	U26
		D-SCADA	DNA	7	U9
		D-SCADA	DAC	12a	New
		D-SCADA	DDC	22	New
Interface between back office systems under common management authority	7	DAC	DDC	24	New
		MDM	DERM	4	New
		CIS	MDM	8	New
		CIS	Legacy MWFM	27	U131
Interface between back office systems not under common management authority	8	CIS	GIS	30	U110
		MDM	DMAT	33	New
		MDM	HEMP	9	New
		DERM	HEMP	15	U106
		DERM	VEMS	18	U106
		DERM	AHE	23	U22
		HEMP	AHE	25	U2
		HEMP	ALNK	29	New
CIS	HEMP	31	U119		
CIS	DERM	32	U33		
Interface with B2B connections between systems usually involving financial or market transactions	9	DERM	RTO	20	U93
Interface between control systems and non-control/corporate systems	10	CIS	AHE	1	U21
		MDM	AHE	6	U2
		DMS	MDM	10	U8
		GIS	MWFM	13	U102
		DNA	DERM	14a	U11
Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements	11	DADC	DAD-A/DAD-M	54	U112
		DERC	DER-A/DER-M	55	U112

Interface between systems that use customer (residential, commercial, and industrial) site networks	15	VEMS	EVSE	19	U62
		HANG	Residential DER	28	U130
		EVSE	PEV	34	New
		BMS	Commercial & Industrial DER	35	U45
		ESI	HAND	52a	U120
		HAND	ESI	52b	U120
		HAND	HAND	52c	N/A
		CHR	HAND	53a	N/A
		HAND	CHR	53b	N/A
Interface between external systems and the customer site	16	HAND	HAND	53c	N/A
		HEMP	IPI	16	U42
Interface between systems that use the AMI network (with high availability)	13 (14)	DERM	BMS	17	U106
		AHE	MFR	5	U24

APPENDIX C KCP&L SMARTGRID SYSTEM DESCRIPTIONS

System	Name	Description
AHE	AMI Head-End	The Advanced Metering Infrastructure Head-End (AHE) is a system that serves as the operational control application for the Advanced Metering Infrastructure (AMI) solution. Optionally, it manages required meter reading collection and enacts other meter- and communication-related commands. The AHE also manages the transfer of meter information to the Meter Data Management System (MDM).
ALNK	AccountLink	AccountLink (ALNK) is an interactive Web-site that is accessible via the Internet that enables the exchange and display of account information for the Customer.
BMS	Building Management System	A Building Management System (BMS) is a system/service that monitors and controls building energy and responds to signals while minimizing impact on building occupants.
CIS	Customer Information System	The Customer Information System (CIS) is an enterprise-wide software application that allows the Utility to manage aspects of their relationship with Customers. In addition to Customer revenue management and service order management, the CIS supports the Utility function that manages Customer relationships by providing a point-of-contact and resolution for Customer issues and problems.
DAC	Distribution Automation Controller	The Distribution Automation Controller is the processing portion of the Distributed Control and Data Acquisition System (DCADA) that implements the following functionalities: Supervisory Control and Data Acquisition (SCADA), Switching Procedure Management (SPM), Distribution Network Analysis (DNA), Distribution System State Estimator (DSSE), Short-Term Load Scheduler (STLS), Fault Detection and Immediate Restoration (FDIR), Volt/var Control (VVC), and Feeder Load Transfer (FLT).
DDC	Distribution Data Concentrator	The Distribution Data Concentrator (DDC) acts as a multi-protocol pipeline for data flow between the Substation, Field Automation, and Distribution Operations security zones. It is the other main portion of the Distributed Control and Data Acquisition System (DCADA).
DER - C&I	Commercial & Industrial Distributed Energy Resource	Commercial & Industrial Distributed Energy Resources (C&I DER) include small-scale generation or storage of any form that is located on a commercial or industrial customer's premises. These energy resources include, but are not limited to, energy storage devices, photovoltaic panels, backup generators, and plug-in electric vehicles.
DER - Grid-Connected	Grid-Connected Distributed Energy Resource	Grid-Connected Distributed Energy Resources (DER) include small-scale generation or storage of any form that is attached to the distribution grid. These energy resources include, but are not limited to, energy storage devices, photovoltaic panels, backup generators, biomass, and plug-in electric vehicles. In this project, this energy resource is a grid-connected battery located in the Midtown Substation.
DER - Residential	Residential Distributed Energy Resource	Residential Distributed Energy Resources (DER) include small-scale generation or storage of any form that is located on a residential customer's premises. These generation facilities include, but are not limited to, energy storage devices, photovoltaic panels, wind generators, biomass, and plug-in electric vehicles.

System	Name	Description
DERM	Distributed Energy Resource Management System	The Distributed Energy Resource Management System (DERM) is a system used to manage demand response events. The DERM schedules events based on requests from Regional Transmission Organization Wholesale Markets (RTOs) and the Distribution Management System (DMS) and issues the appropriate event signals with the Home Energy Management Portal (HEMP), aggregators, commercial customers, and distribution Grid-Connected Distributed Energy Resources (DER).
DMAT	Data Mining & Analysis Tool	The Data Mining & Analysis Tool (DMAT) is a system that receives data from the Meter Data Management System (MDM), mines the data upon request, and passes it along to requestors.
DMS	Distribution Management System	The Distribution Management System (DMS) is a suite of application software that monitors and controls the distribution system equipment based on computer-aided applications, market information, and operator control decisions. The DMS integrates the Distribution Operator GUI (DOG), Distribution Supervisory Control and Data Acquisition (D-SCADA), Distribution Network Analysis (DNA), Outage Management System (OMS), and Mobile Workforce Management System (MWFM).
EMS	Energy Management Systems	Energy Management Systems (EMS) are a collection of systems used to manage the bulk power delivery system. These systems include Transmission Supervisory Control and Data Acquisition (T-SCADA), Transmission Management Systems (TMS), and Generation Management Systems (GMS).
EVSE	Electric Vehicle Supply Equipment	Electric Vehicle Supply Equipment (EVSE) are the physical electrical cord and connectors that are specified by applicable Society of Automotive Engineers (SAE) standards to provide the transfer of electric energy from the charging point to the Plug-in Electric Vehicle (PEV).
Field DADs	Field Distribution Automation Devices	Field Distribution Automation Devices (DADs) are a variety of devices (switches, automatic reclosers, capacitors, regulators, etc.) located throughout SmartGrid Demonstration Zone that support distribution automation functionality.
GIS	Geographic Information System	Geographic Information System (GIS) is a spatial asset management system that provides the Utility with asset information and network connectivity for advanced applications.
HAND	Home Area Network Device	A Home Area Network Device (HAND) is a device owned by a Customer or a third party that is registered on the Home Area Network (HAN). A HAND communicates in a secure way with other HANDs (e.g., Programmable Communicating Thermostat (PCT), Load Control Switch (LCS), and Customer Household Appliance (CHA)).
HANG	Home Area Network Gateway	A Home Area Network Gateway (HANG) is a device that registers with the SmartMeter (MTR) to receive usage data and creates a secondary HAN to which HAN Devices (HANDs) are registered. The HANG also connects the HAN to the Home Energy Management Portal (HEMP) via a customer broadband connection. The HANG provides cyber security and coordinates functions that enable secure interactions between relevant HANDs, MTRs, and the Utility.
HEMP	Home Energy Management Portal	The Home Energy Management Portal (HEMP) is an Internet-based system that provides access to various data, including billing plans and electricity usage, to the customer. The customer uses the Home Energy Management Portal (HEMP) to manage their in-premise Home Area Network Devices (HANDs) and, in turn, control their energy consumption.

System	Name	Description
MDM	Meter Data Management System	The Meter Data Management System (MDM) is a system that stores SmartMeter (MTR) data (e.g., energy usage, energy generation, meter logs, meter test results) and makes data available to authorized systems. The MDM performs VEE (validation, estimation, and editing) and creates bill determinants for the Customer Information System (CIS) billing engine.
MTR	SmartMeter	A SmartMeter (MTR) is a device that measures the amount of electricity used at a particular site. MTRs are typically located at the Customer facility and owned by the distributor (e.g., Utility) or retail provider.
MWFM	Mobile Workforce Management System	The Mobile Workforce Management System (MWFM) is an enterprise-wide system that is used to manage trouble order and customer order dispatch to field crews.
OMS	Outage Management System	The Outage Management System (OMS) is an enterprise-wide system that is used by operators of electric distribution systems to assist in outage identification and power restoration.
PEV	Plug-in Electric Vehicle	A Plug-In Electric Vehicle (PEV) is a motorized car or truck which runs exclusively or partially on stored battery power, as opposed to being powered directly by carbon-based fuel. Additionally, a PEV plugs into premise Electric Vehicle Supply Equipment (EVSE) to charge the vehicle.
RTO	Regional Transmission Organization Wholesale Market	A Regional Transmission Organization Wholesale Market (RTO) is a organization in charge of bulk electricity markets, such as Southwest Power Pool (SPP).
Substation DADs	Substation Distribution Automation Devices	Substation Distribution Automation Devices (DADs) are a variety of devices (switches, automatic reclosers, capacitors, regulators, etc.) located in Midtown Substation that support distribution automation functionality.
VEMS	Vehicle Energy Management System	A Vehicle Energy Management System (VEMS) is a system that encourages/discourages charging Plug-in Electric Vehicles (PEVs) through relevant pricing or other (dis)incentives, processes and stores data about PEV programs, contracts, and relevant historic information, creates behavioral models, and collects, processes, and stores customer-specific data.

APPENDIX D · DEFINITION LOCATION OF NISTIR-7628 RECOMMENDED SECURITY REQUIREMENTS

NISTIR-7628 Smart Grid Requirement Number	NISTIR-7628 Smart Grid Requirement Name	NISTIR-7628 Volume 1 Page Number(s)
SG.AC-1	Access Control Policy and Procedures	91-92
SG.AC-2	Remote Access Policy and Procedures	92
SG.AC-3	Account Management	92-93
SG.AC-4	Access Enforcement	93
SG.AC-6	Separation of Duties	94-95
SG.AC-7	Least Privilege	95
SG.AC-8	Unsuccessful Login Attempts	95-96
SG.AC-9	Smart Grid Information System Use Notification	96-97
SG.AC-11	Concurrent Session Control	97
SG.AC-12	Session Lock	98
SG.AC-14	Permitted Actions without Identification or Authentication	98-99
SG.AC-16	Wireless Access Restrictions	100
SG.AC-17	Access Control for Portable and Mobile Devices	100-101
SG.AC-18	Use of External Information Control Systems	101-102
SG.AC-19	Control System Access Restrictions	102
SG.AC-20	Publicly Accessible Content	103
SG.AC-21	Passwords	103-104
SG.AT-1	Awareness and Training Policy and Procedures	104-105
SG.AT-2	Security Awareness	105
SG.AT-3	Security Training	105-106
SG.AT-4	Security Awareness and Training Records	106
SG.AT-6	Security Responsibility Testing	107
SG.AT-7	Planning Process Training	107-108
SG.AU-1	Audit and Accountability Policy and Procedures	108-109
SG.AU-2	Auditable Events	109
SG.AU-3	Content of Audit Records	109-110
SG.AU-4	Audit Storage Capacity	110
SG.AU-5	Response to Audit Processing Failures	110-111
SG.AU-6	Audit Monitoring, Analysis, and Reporting	111-112
SG.AU-7	Audit Reduction and Report Generation	112
SG.AU-8	Time Stamps	112
SG.AU-9	Protection of Audit Information	113
SG.AU-10	Audit Record Retention	113
SG.AU-11	Conduct and Frequency of Audits	113-114
SG.AU-12	Auditor Qualification	114
SG.AU-13	Audit Tools	114-115

NISTIR-7628 Smart Grid Requirement Number	NISTIR-7628 Smart Grid Requirement Name	NISTIR-7628 Volume 1 Page Number(s)
SG.AU-14	Security Policy Compliance	115
SG.AU-15	Audit Generation	116
SG.AU-16	Non-Repudiation	116-117
SG.CA-1	Security Assessment and Authorization Policy and Procedures	117-118
SG.CA-2	Security Assessments	118
SG.CA-4	Smart Grid Information System Connections	119
SG.CA-5	Security Authorization to Operate	120
SG.CA-6	Continuous Monitoring	120-121
SG.CM-1	Configuration Management Policy and Procedures	121-122
SG.CM-2	Baseline Configuration	122
SG.CM-3	Configuration Change Control	122-123
SG.CM-4	Monitoring Configuration Changes	123-124
SG.CM-5	Access Restrictions for Configuration Change	124
SG.CM-6	Configuration Settings	124-125
SG.CM-7	Configuration for Least Functionality	125-126
SG.CM-8	Component Inventory	126
SG.CM-9	Addition, Removal, and Disposal of Equipment	127
SG.CM-10	Factory Default Settings Management	127-128
SG.CM-11	Configuration Management Plan	128
SG.CP-1	Continuity of Operations Policy and Procedure	128-129
SG.CP-2	Continuity of Operations Plan	129-130
SG.CP-3	Continuity of Operations Roles and Responsibilities	130
SG.CP-4	Continuity of Operations Training	130-131
SG.CP-5	Continuity of Operations Plan Testing	131
SG.CP-6	Continuity of Operations Plan Update	131-132
SG.CP-7	Alternate Storage Sites	132
SG.CP-8	Alternate Telecommunication Services	133
SG.CP-9	Alternate Control Center	133-134
SG.CP-10	Smart Grid Information System Recovery and Reconstitution	134-135
SG.CP-11	Fail-Safe Response	135
SG.IA-1	Identification and Authentication Policy and Procedures	136
SG.IA-2	Identifier Management	136-137
SG.IA-3	Authenticator Management	137

NISTIR-7628 Smart Grid Requirement Number	NISTIR-7628 Smart Grid Requirement Name	NISTIR-7628 Volume 1 Page Number(s)
SG.IA-4	User Identification and Authentication	138
SG.IA-5	Device Identification and Authentication	138-139
SG.IA-6	Authenticator Feedback	139
SG.ID-1	Information and Document Management Policy and Procedures	139-140
SG.ID-2	Information and Document Retention	140-141
SG.ID-3	Information Handling	141
SG.ID-4	Information Exchange	141-142
SG.IR-1	Incident Response Policy and Procedures	143-144
SG.IR-2	Incident Response Roles and Responsibilities	144
SG.IR-3	Incident Response Training	144-145
SG.IR-4	Incident Response Testing and Exercises	145
SG.IR-5	Incident Handling	145-146
SG.IR-6	Incident Monitoring	146
SG.IR-7	Incident Reporting	146-147
SG.IR-8	Incident Response Investigation and Analysis	147
SG.IR-9	Corrective Action	147-148
SG.IR-10	Smart Grid Information System Backup	148
SG.IR-11	Coordination of Emergency Response	149
SG.MA-1	Smart Grid Information System Maintenance Policy and Procedures	149-150
SG.MA-2	Legacy Smart Grid Information System Upgrades	150
SG.MA-3	Smart Grid Information System Maintenance	150-151
SG.MA-4	Maintenance Tools	152
SG.MA-5	Maintenance Personnel	152-153
SG.MA-6	Remote Maintenance	153
SG.MA-7	Timely Maintenance	154
SG.MP-1	Media Protection Policy and Procedures	154-155
SG.MP-2	Media Sensitivity Level	155
SG.MP-3	Media Marking	155-156
SG.MP-4	Media Storage	156
SG.MP-5	Media Transport	156-157
SG.MP-6	Media Sanitization and Disposal	157
SG.PE-1	Physical and Environmental Security Policy and Procedures	157-158
SG.PE-2	Physical Access Authorizations	158-159
SG.PE-3	Physical Access	159-160

NISTIR-7628 Smart Grid Requirement Number	NISTIR-7268 Smart Grid Requirement Name	NISTIR-7628 Volume 1 Page Number(s)
SG.PE-4	Monitoring Physical Access	160
SG.PE-5	Visitor Control	160-161
SG.PE-6	Visitor Records	161
SG.PE-7	Physical Access Log Retention	161-162
SG.PE-8	Emergency Shutoff Protection	162
SG.PE-9	Emergency Power	162-163
SG.PE-10	Delivery and Removal	163
SG.PE-11	Alternate Work Site	163-164
SG.PE-12	Location of Smart Grid Information System Assets	164
SG.PL-1	Strategic Planning Policy and Procedures	164-165
SG.PL-2	Smart Grid Information System Security Plan	165-166
SG.PL-3	Rules of Behavior	166
SG.PL-4	Privacy Impact Assessment	167
SG.PL-5	Security-Related Activity Planning	167
SG.PM-1	Security Policy and Procedures	168
SG.PM-2	Security Program Plan	168-169
SG.PM-3	Senior Management Authority	169-170
SG.PM-4	Security Architecture	170
SG.PM-5	Risk Management Strategy	170-171
SG.PM-6	Security Authorization to Operate Process	171
SG.PM-7	Mission/Business Process Definition	171
SG.PM-8	Management Accountability	171-172
SG.PS-1	Personnel Security Policy and Procedures	172-173
SG.PS-2	Position Categorization	173
SG.PS-3	Personnel Screening	173-174
SG.PS-4	Personnel Termination	174-175
SG.PS-5	Personnel Transfer	175
SG.PS-6	Access Agreements	175-176
SG.PS-7	Contractor and Third-Party Personnel Security	176
SG.PS-8	Personnel Accountability	176-177
SG.PS-9	Personnel Roles	177
SG.RA-1	Risk Assessment Policy and Procedures	177-178
SG.RA-2	Risk Management Plan	178-179
SG.RA-3	Security Impact Level	179
SG.RA-4	Risk Assessment	179-180
SG.RA-5	Risk Assessment Update	180
SG.RA-6	Vulnerability Assessment and Awareness	180-181

NISTIR-7628 Smart Grid Requirement Number	NISTIR-7268 Smart Grid Requirement Name	NISTIR-7628 Volume 1 Page Number(s)
SG.SA-1	Smart Grid Information System and Services Acquisition Policy and Procedures	181-182
SG.SA-2	Security Policies for Contractors and Third Parties	182-183
SG.SA-3	Life-Cycle Support	183
SG.SA-4	Acquisitions	183-184
SG.SA-5	Smart Grid Information System Documentation	184
SG.SA-6	Software License Usage Restrictions	184-185
SG.SA-7	User-Installed Software	185
SG.SA-8	Security Engineering Principles	185-186
SG.SA-9	Developer Configuration Management	186-187
SG.SA-10	Developer Security Testing	187
SG.SA-11	Supply Chain Protection	187-188
SG.SC-1	Smart Grid Information System and Communication Protection Policy and Procedures	188-189
SG.SC-3	Security Function Isolation	190
SG.SC-4	Information Remnants	190
SG.SC-5	Denial-of-Service Protection	190-191
SG.SC-6	Resource Priority	191
SG.SC-7	Boundary Protection	191-193
SG.SC-8	Communication Integrity	193
SG.SC-9	Communication Confidentiality	193
SG.SC-11	Cryptographic Key Establishment and Management	194
SG.SC-12	Use of Validated Cryptography	194-195
SG.SC-13	Collaborative Computing	195
SG.SC-15	Public Key Infrastructure Certificates	196
SG.SC-16	Mobile Code	196-197
SG.SC-18	System Connections	197-198
SG.SC-19	Security Roles	198
SG.SC-20	Message Authenticity	198-199
SG.SC-21	Secure Name/Address Resolution Service	199
SG.SC-22	Fail in Known State	199-200
SG.SC-26	Confidentiality of Information at Rest	201
SG.SC-29	Application Partitioning	203
SG.SC-30	Smart Grid Information System Partitioning	203-204
SG.SI-1	Smart Grid Information System and Information Integrity Policy and Procedures	204-205

NISTIR-7628 Smart Grid Requirement Number	NISTIR-7268 Smart Grid Requirement Name	NISTIR-7628 Volume 1 Page Number(s)
SG.SI-2	Flaw Remediation	205
SG.SI-3	Malicious Code and Spam Protection	206
SG.SI-4	Smart Grid Information System Monitoring Tools and Techniques	206-207
SG.SI-5	Security Alerts and Advisories	207-208
SG.SI-6	Security Functionality Verification	208
SG.SI-7	Software and Information Integrity	208-209
SG.SI-8	Information Input Validation	209
SG.SI-9	Error Handling	209-210

APPENDIX E CONTROL ANALYSIS RESULTS

NISTIR 7268 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Applicable Interface Categories	UCAug Security Profile for AMI	UCAug Security Profile for DM	Requirement Fulfilled by KCP&L Policies, Standards, & Processes	KCP&L Policy Number(s)	KCP&L Standard(s)	KCP&L Process(es)
SGAC-1	Access Control Policy and Procedures	All	DHS-2.15.1	Policy 4	Yes	KCP&L-S200, KCP&L-S300	Access Control Standard	Access Management Process
SGAC-2	Remote Access Policy and Procedures	All	DHS-2.15.24	Policy 4	Yes	KCP&L-S300	Remote Access Standard	Remote Access Procedure
SGAC-3	Account Management	All	DHS-2.15.2	Protection 26, Protection 15, Detection 25, Protection 51	Yes	None	Access Control Standard	Access Management Process
SGAC-4	Access Enforcement	All	DHS-2.15.7	Protection 29	Yes	None	Access Control Standard	None
SGAC-5	Information Flow Enforcement	None	DHS-2.15.15	Protection 35	Yes	None	Confidentiality Protection Standard	None
SGAC-6	Separation of Duties	All	DHS-2.15.8	Policy 2	Yes	None	Change Control Standard	Change Management Process
SGAC-7	Least Privilege	All	DHS-2.15.9	Protection 16	Yes	KCP&L-S300	None	None
SGAC-8	Unsuccessful Login Attempts	All	DHS-2.15.20	Reaction 6	Yes	None	Access Control Standard, Remote Access Standard	None
SGAC-9	Smart Grid Information System Use Notification	All	DHS-2.15.17	Policy 4	Yes	None	Access Control Standard, Remote Access Standard	None
SGAC-10	Previous Logon Notification	None	DHS-2.15.19	Detection 28	No	None	None	None
SGAC-11	Consent Session Control	1,2,3,5,7,8,9,10,13,14,16	DHS-2.15.18	Protection 37	No	None	None	None
SGAC-12	System Lock	7,8	DHS-2.15.21	Protection 38	No	None	None	None
SGAC-13	Remote Session Termination	None	DHS-2.15.22	Protection 39	No	None	None	None
SGAC-14	Permitted Actions without Identification or Authentication	1,2,3,5,7,8,9,10,13,14,15,16	DHS-2.15.11	Reaction 5	Yes	None	Access Control Standard	None
SGAC-15	Remote Access	None	DHS-2.15.24	Detection 14	Yes	KCP&L-S300	Remote Access Standard	Remote Access Procedure
SGAC-16	Wireless Access Restrictions	All	DHS-2.15.26	Policy 3	Yes	KCP&L-S300	Wireless Networking Standard	None
SGAC-17	Access Control for PDA and Mobile Devices	All	DHS-2.15.25	Protection 40	Yes	KCP&L-A100	Access Control Standard, Account Management	None
SGAC-18	Use of External Information Control Systems	All	DHS-2.15.29	Policy 4	Yes	None	Remote Access Standard	Remote Access Procedure, Access Management Process
SGAC-19	Control System Access Restrictions	All	N/A	Network 3, 4	Yes	None	Access Control Standard	None
SGAC-20	Publicly Accessible Content	All	N/A	N/A	No	None	None	None
SGAC-21	Passwords	All	DHS-2.15.16	Protection 36	Yes	None	Access Control Standard, Remote Access Standard	Access Management Process, Remote Access Process
SGAT-1	Awareness and Training Policy and Procedures	All	N/A	Policy 2	Yes	KCP&L-S200, KCP&L-S300, KCP&L-S102	Information Security Awareness Standard	PC Life Cycle Process
SGAT-2	Security Awareness	All	N/A	Policy 2	Yes	KCP&L-S200, KCP&L-S300, KCP&L-S102	Information Security Awareness Standard	PC Life Cycle Process
SGAT-3	Security Training	All	N/A	Policy 2	Yes	KCP&L-S300	None	None
SGAT-4	Security Awareness and Training Records	All	N/A	N/A	Yes	None	Information Security Awareness Standard	None
SGAT-5	Contact with Security Groups and Associations	None	N/A	N/A	No	None	None	None
SGAT-6	Security Responsibility Testing	All	N/A	N/A	No	None	None	None
SGAT-7	Planning Process Training	All	N/A	N/A	Yes	None	None	None

NISTIR 7268 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Applicable Interface Categories	UCAug Security Profile for AMI	UCAug Security Profile for DM	Requirement Fulfilled by KCP&L Policies, Standards, & Processes	KCP&L Policy Number(s)	KCP&L Standard(s)	KCP&L Process(es)
SGAU-1	Audit and Accountability Policy and Procedures	All	N/A	Policy 9	No	None	None	None
SGAU-2	Available Events	All	DHS-2.16.2	Policy 9	No	None	None	None
SGAU-3	Content of Audit Records	All	DHS-2.16.3	N/A	No	None	None	None
SGAU-4	Audit Storage Capacity	All	DHS-2.16.4	N/A	No	None	None	None
SGAU-5	Response to Audit Processing Failures	All	DHS-2.16.5	N/A	No	None	None	None
SGAU-6	Audit Monitoring, Analysis, and Reporting	All	N/A	Policy 9	No	None	None	None
SGAU-7	Audit Reduction and Report Generation	All	DHS-2.16.7	N/A	No	None	None	None
SGAU-8	Time Stamps	All	DHS-2.16.8	N/A	No	None	None	None
SGAU-9	Protection of Audit Information	All	DHS-2.16.9	N/A	No	None	None	None
SGAU-10	Audit Record Retention	All	N/A	Policy 9	No	None	None	None
SGAU-11	Conduct and Frequency of Audits	All	N/A	N/A	Yes	None	None	None
SGAU-12	Auditor Qualification	All	DHS-2.16.12	N/A	Yes	None	None	None
SGAU-13	Audit Tools	All	AAMSP-2.16.1	Policy 9	Yes	None	None	None
SGAU-14	Security Policy Compliance	All	N/A	Policy 2	Yes	None	None	None
SGAU-15	Audit Generation	All	N/A	N/A	No	None	None	None
SGAU-16	Non-Repudiation	7,8,9,13,14,16	N/A	N/A	No	None	None	None
SGCA-1	Security Assessment and Authorization Policy and Procedures	All	N/A	Policy 5	No	None	None	None
SGCA-2	Security Assessments	All	N/A	Policy 5, Detection 12	No	None	None	None
SGCA-3	Continuous Improvement	None	N/A	Policy 10	No	None	None	None
SGCA-4	Smart Grid Information System Connections	All	N/A	Policy 3	Yes	None	Remote Access Standard	Remote Access Procedure
SGCA-5	Security Authorization to Operate	All	N/A	N/A	Yes	None	None	Change Control Procedure
SGCA-6	Continuous Monitoring	All	N/A	Policy 5	No	None	None	None
SGCM-1	Configuration Management Policy and Procedures	All	N/A	Policy 7	Yes	KCP&L-S300	Configuration Management Standard	Configuration Management Process
SGCM-2	Baseline Configuration	All	N/A	Detection 8	Yes	KCP&L-S300	None	None
SGCM-3	Configuration Change Control	All	N/A	Policy 7	Yes	None	None	Configuration Management Process
SGCM-4	Monitoring Configuration Changes	All	N/A	Policy 7	Yes	None	Configuration Management Standard	Configuration Management Process
SGCM-5	Access Restrictions for Configuration Change	All	N/A	N/A	Yes	None	None	Configuration Management Process
SGCM-6	Configuration Settings	All	N/A	Detection 10	Yes	None	Configuration Management Standard	Configuration Management Process
SGCM-7	Configuration for Least Functionality	All	N/A	Policy 7	Yes	None	Access Control Standard	None
SGCM-8	Component Inventory	All	N/A	Detection 7	Yes	None	Configuration Management Standard	Access Management Hardware Process, Computer Service Request Process, Information Technology Planning Process

NISTIR 7268 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Applicable Interface Categories	UCAug Security Profile for AMD	UCAug Security Profile for DM	Requirement Fulfilled by KCP&L Policies, Standards, & Processes	KCP&L Policy Number(s)	KCP&L Standard(s)	KCP&L Process(es)
SGCM-9	Addition, Removal, and Disposal of Equipment	All	N/A	Policy 3	Yes	None	Configuration Management Standard	Access Management Hardware Process, Configuration Management Process
SGCM-10	Factory Default Settings Management	All	N/A	Protection 9	No	None	None	None
SGCM-11	Configuration Management Plan	All	N/A	Policy 7	Yes	None	Configuration Management Standard	Configuration Management Process
SGCP-1	Continuity of Operations Policy and Procedure	All	N/A	N/A	No	None	None	None
SGCP-2	Continuity of Operations Plan	All	DHS-2.12.2	Recovery 3	Yes	None	Availability Protection Standard	Recovery
SGCP-3	Continuity of Operations Roles and Responsibilities	All	DHS-2.12.3	N/A	Yes	None	Incident Response Standard	None
SGCP-4	Continuity of Operations Training	All	AMISP-2.12.1	Policy 2	Yes	None	None	None
SGCP-5	Continuity of Operations Plan Testing	All	DHS-2.12.5	N/A	Yes	None	Availability Protection Standard	None
SGCP-6	Continuity of Operations Plan Update	All	AMISP-2.12.2	N/A	Yes	None	Availability Protection Standard	None
SGCP-7	Alternate Storage Sites	All	N/A	Policy 6	Yes	None	None	Backup and Recovery Process
SGCP-8	Alternate Telecommunication Services	All	N/A	Policy 6	No	None	None	None
SGCP-9	Alternate Control Center	All	N/A	Policy 6	Yes	KCP&L-S300	None	None
SGCP-10	Smart Grid Information System Recovery and Reconstitution	All	N/A	Policy 6	Yes	KCP&L-S300	None	None
SGCP-11	Fail-Safe Response	All	N/A	Protection 19, 20	Yes	KCP&L-S300	None	None
SGIA-1	Identification and Authentication Policy and Procedures	All	DHS-2.15.7	Protection 1, 10, 11, 27, 28, 29, 30, 31	Yes	None	Access Control Standard	None
SGIA-2	Identifier Management	All	DHS-2.15.4	Detection 26	Yes	None	Access Control Standard	None
SGIA-3	Authenticator Management	All	DHS-2.15.3	Protection 27	Yes	None	Access Control Standard	None
SGIA-4	User Identification and Authentication Device Identification and Authentication	All	1,2,3,5,7,8,9,10,13,14,15,16	DHS-2.15.10	Protection 31	Yes	None	Access Control Standard
SGIA-5	Device Identification and Authentication	All	1,2,3,7,8	DHS-2.15.12	Protection 32	Yes	KCP&L-S300	None
SGIA-6	Authenticator Feedback	All	1,2,3,5,7,8,9,10,13,14,15,16	DHS-2.15.13	Protection 33	No	None	None
SGID-1	Information and Document Management Policy and Procedures	All	DHS-2.9.0	Policy 8	Yes	None	None	Information Management Process
SGID-2	Information and Document Retention	All	DHS-2.9.2	Policy 8	Yes	None	None	Change Management Process, Framework Process
SGID-3	Information Handling	All	DHS-2.9.3	Policy 8	Yes	None	Confidentiality Protection Standard	None
SGID-4	Information Exchange	All	DHS-2.9.5	Policy 8	Yes	None	Remote Access Standard	Information Management Process
SGID-5	Automated Labeling	None	AMISP-2.9.1	Protection 31	No	None	None	None
SGIR-1	Incident Response Policy and Procedures	All	DHS-2.12.1	Policy 8	Yes	KCP&L-S300	Incident Response Standard	None
SGIR-2	Incident Response Roles and Responsibilities	All	N/A	Policy 2	Yes	None	Incident Response Standard	None
SGIR-3	Incident Response Training	All	AMISP-2.12.1	Policy 2	No	None	None	None
SGIR-4	Incident Response Testing and Exercises	All	N/A	N/A	Yes	None	Incident Response Standard	None
SGIR-5	Incident Handling	All	N/A	Policy 6	Yes	None	None	Remote Access Procedure

NISTIR 7268 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Applicable Interface Categories	UCAug Security Profile for AMD	UCAug Security Profile for DM	Requirement Fulfilled by KCP&L Policies, Standards, & Processes	KCP&L Policy Number(s)	KCP&L Standard(s)	KCP&L Process(es)
SGIR-6	Incident Monitoring	All	N/A	Policy 6	Yes	None	Incident Response Standard	None
SGIR-7	Incident Reporting	All	N/A	Policy 6	Yes	None	Incident Response Standard	None
SGIR-8	Incident Response Investigation and Analysis	All	N/A	Policy 6	Yes	None	Incident Response Standard	None
SGIR-9	Corrective Action	All	N/A	Policy 6	Yes	None	Incident Response Standard	None
SGIR-10	Smart Grid Information System Backup	All	DHS-2.10.4	Policy 6	Yes	None	None	Backup and Recovery Process
SGIR-11	Coordination of Emergency Response	All	N/A	N/A	Yes	None	Incident Response Standard	None
SGMA-1	Smart Grid Information System Maintenance Policy and Procedures	All	DHS-2.10.1	Policy 3	Yes	None	Configuration Management Standard	Infrastructure Process
SGMA-2	Legacy Smart Grid Information System Upgrades	All	DHS-2.10.2	Policy 3	Yes	None	None	Infrastructure Process
SGMA-3	Smart Grid Information System Maintenance	All	DHS-2.10.6	Policy 7	Yes	None	Configuration Management Standard	Infrastructure Process
SGMA-4	Maintenance Tools	All	AMISP-2.10.1	Policy 3	No	None	None	None
SGMA-5	Maintenance Personnel	All	DHS-2.10.8	Policy 7	Yes	None	Remote Access Standard	None
SGMA-6	Remote Maintenance	All	DHS-2.10.9	Policy 3	Yes	None	Remote Access Standard	None
SGMA-7	Timely Maintenance	All	N/A	N/A	No	None	None	None
SGMP-1	Media Protection Policy and Procedures	All	N/A	Policy 2	Yes	None	Confidentiality Protection Standard	None
SGMP-2	Media Sensitivity Level	All	N/A	N/A	Yes	None	Confidentiality Protection Standard	None
SGMP-3	Media Marking	All	N/A	Policy 8	Yes	None	Confidentiality Protection Standard	None
SGMP-4	Media Storage	All	N/A	Policy 8	Yes	None	Confidentiality Protection Standard	None
SGMP-5	Media Transport	All	N/A	Policy 8	Yes	None	Confidentiality Protection Standard	None
SGMP-6	Media Shredding and Disposal	All	N/A	Policy 8	Yes	None	Confidentiality Protection Standard	Access Management Hardware Process
SGPE-1	Physical and Environmental Security Policy and Procedures	All	N/A	Policy 2, Protection 2,3	No*	None	None	None
SGPE-2	Physical Access Authentication	All	N/A	Policy 4, Protection 2,3	No*	None	None	None
SGPE-3	Physical Access	All	N/A	Policy 4, Protection 2,3	No*	None	None	None
SGPE-4	Monitoring Physical Access	All	N/A	Detection 1, Protection 2,3	No*	None	None	None
SGPE-5	Visitor Control	All	N/A	Policy 4	No*	None	None	None
SGPE-6	Visitor Records	All	N/A	Policy 9	No*	None	None	None
SGPE-7	Physical Access Log Retention	All	N/A	Policy 9	No*	None	None	None
SGPE-8	Emergency Shutoff Protection	All	N/A	Protection 4	No*	None	None	None
SGPE-9	Emergency Power	All	N/A	Recovery 1, 2	No*	None	None	None
SGPE-10	Delivery and Removal	All	N/A	N/A	No*	None	None	None
SGPE-11	Alternate Work Site	All	N/A	Policy 6	No*	None	None	None

NISTIR 7268 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Applicable Interface Categories	UCAng Security Profile for AMD	UCAng Security Profile for DM	Requirement Fulfilled by KCP&L Policies, Standards, & Processes	KCP&L Policy Number(s)	KCP&L Standard(s)	KCP&L Process(es)
SGPE-1	Location of Smart Grid Information System Assets	All	N/A	N/A	No	None	None	None
SGPL-1	Strategic Planning Policy and Procedures	All	N/A	Policy 1	Yes	None	None	Information Technology Planning Process
SGPL-2	Smart Grid Information System Security Plan	All	N/A	Policy 1, Protection 42, 46	No	None	None	None
SGPL-3	Rules of Behavior	All	N/A	Policy 2, Network 2	Yes	KCP&L-S200	None	None
SGPL-4	Privacy Impact Assessment	All	N/A	N/A	No	None	None	None
SGPL-5	Security-Related Activity Planning	All	N/A	Policy 3	Yes	None	None	Information Technology Planning Process
SGPM-1	Security Policy and Posture	All	N/A	Policy 1	Yes	KCP&L-S200, KCP&L-S300	System Lifecycle Management Security Standard	None
SGPM-2	Security Program Plan	All	N/A	Policy 1	Yes	KCP&L-S200, KCP&L-S300	None	None
SGPM-3	Senior Management Authority	All	N/A	N/A	Yes	KCP&L-S300	None	None
SGPM-4	Security Architecture	All	N/A	N/A	No	None	None	None
SGPM-5	Risk Management Strategy	All	N/A	Policy 1	Yes	KCP&L-S300	Cyber Risk Management Standard	None
SGPM-6	Security Authorization to Operate Process	All	N/A	N/A	No	None	None	None
SGPM-7	Mission/Business Process Definition	All	N/A	Policy 5	No	None	None	None
SGPM-8	Management Accountability	All	N/A	Policy 2	Yes	None	System Lifecycle Management Security Standard	None
SGPS-1	Personal Security Policy and Procedures	All	N/A	Policy 4	Yes	KCP&L-S200, KCP&L-S300	System Lifecycle Management Security Standard	Access Management Process
SGPS-2	Position Categorization	All	N/A	N/A	No	None	None	None
SGPS-3	Personal Screening	All	N/A	Policy 4	No	None	None	None
SGPS-4	Personal Termination	All	N/A	Policy 4	Yes	None	None	Access Management Process
SGPS-5	Personal Transfer	All	N/A	Policy 4	Yes	None	None	Access Management Process
SGPS-6	Access Agreements	All	N/A	N/A	No	None	None	None
SGPS-7	Contracts and Third-Party Personnel Security	All	N/A	N/A	Yes	None	Remote Access Standard	Access Management Process, Information Management Process
SGPS-8	Personal Accountability	All	N/A	Policy 2	Yes	Policy and Procedure Overview, KCP&L-P200	None	None
SGPS-9	Personal Roles	All	N/A	N/A	Yes	Policy and Procedure Overview	None	None
SGRA-1	Risk Assessment Policy and Procedures	All	N/A	Policy 5	Yes	KCP&L-S300	Cyber Risk Management Standard, Vulnerability Assessment Standard	None
SGRA-2	Risk Management Plan	All	N/A	Policy 5	Yes	KCP&L-S300	Cyber Risk Management Standard, Vulnerability Assessment Standard	None
SGRA-3	Security Impact Level	All	N/A	N/A	No	None	None	None
SGRA-4	Risk Assessment	All	N/A	Policy 5	Yes	KCP&L-S300	Cyber Risk Management Standard	None
SGRA-5	Risk Assessment Update	All	N/A	Policy 5	Yes	None	Cyber Risk Management Standard	None

NISTIR 7268 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Applicable Interface Categories	UCAng Security Profile for AMD	UCAng Security Profile for DM	Requirement Fulfilled by KCP&L Policies, Standards, & Processes	KCP&L Policy Number(s)	KCP&L Standard(s)	KCP&L Process(es)
SGSA-6	Vulnerability Assessment and Remediation	All	N/A	Policy 5, Definition 13	Yes	KCP&L-S300	Vulnerability Assessment Standard, Vulnerability Management Standard	None
SGSA-1	Smart Grid Information System and Services Acquisition Policy and Procedures	All	N/A	N/A	Yes	KCP&L-S300	None	None
SGSA-2	Security Policies for Contractors and Third Parties	All	N/A	Policy 2	Yes	None	Remote Access Standard	Access Management Process, Information Management Process
SGSA-3	Life-Cycle Support	All	N/A	Policy 3	Yes	KCP&L-S300	System Lifecycle Management Security Standard	PC Life Cycle Process, System Development Life Cycle Process
SGSA-4	Acquisitions	All	N/A	Policy 3	Yes	KCP&L-S300	None	None
SGSA-5	Smart Grid Information System Decommission	All	N/A	Policy 3	Yes	None	System Lifecycle Management Security Standard	System Development Life Cycle Process
SGSA-6	Software License Usage Restrictions	All	N/A	N/A	Yes	None	Configuration Management Standard	Software Management Process, PC Life Cycle Process
SGSA-7	User-Installed Software	All	N/A	Policy 3	Yes	None	None	Software Management Process
SGSA-8	Security Engineering Principles	All	N/A	Protection 48	Yes	None	System Lifecycle Management Security Standard	System Development Life Cycle Process
SGSA-9	Developer Configuration Management	All	N/A	Policy 3, Protection 48	Yes	KCP&L-S300	Change Control Standard	Change Management Process, System Development Life Cycle Process
SGSA-10	Developer Security Training	All	N/A	Policy 3	Yes	None	System Lifecycle Management Security Standard	System Development Life Cycle Process
SGSA-11	Supply Chain Protection Smart Grid Information System and Communication Protection Policy and Procedures	All	N/A	N/A	No	None	None	None
SGSC-1	Communications Partitioning	None	DHS-2.8.2	Protection 10	No	None	None	None
SGSC-2	Security Function Isolation	1,2,3,7,8,13,14,15,16	DHS-2.8.3	Protection 11	No	None	None	None
SGSC-3	Information Remnants	7,8,10	DHS-2.8.4	Protection 10	No	None	None	None
SGSC-4	Denial-of-Service Protection	1,2,3,5,9,10,11,13,15	DHS-2.8.5	Protection 44	No	None	None	None
SGSC-5	Resource Priority	5,11	DHS-2.8.6	Protection 12	No	None	None	None
SGSC-6	Broadcast Protection	1,2,3,5,8,9,10,13,14,15,16	DHS-2.8.7	Policy 2	Yes	None	Confidentiality Protection Standard, Remote Access Standard	LAD System Process, Remote Access Process
SGSC-7	Communication Integrity	All	DHS-2.8.8	Protection 11	Yes	None	Configuration Management Standard	Information Management Process, Remote Access Process
SGSC-8	Communication Confidentiality	13,14,16	DHS-2.8.9	Protection 13	Yes	None	Confidentiality Protection Standard, Remote Access Standard	Remote Access Process
SGSC-9	Trusted Path	None	DHS-2.8.10	N/A	No	None	None	None
SGSC-10	Cryptographic Key Establishment and Management	All	DHS-2.8.11	Protection 15, 13	No	None	None	None
SGSC-11	Use of Validated Cryptography	All	DHS-2.8.12	Policy 3, Protection 13	No	None	None	None
SGSC-12	Collaborative Computing	All	DHS-2.8.13	N/A	No	None	None	None
SGSC-13	Transmission of Security Parameters	None	DHS-2.8.14	N/A	No	None	None	None

NISTIR 7628 Smart Grid Requirement Number	NISTIR 728 Smart Grid Requirement Name	Applicable Interface Categories	UCAmg Security Profile for AMI	UCAmg Security Profile for DM	Requirement Fulfilled by KCP&L Policies, Standards, & Processes	KCP&L Policy Number(s)	KCP&L Standard(s)	KCP&L Process(es)
SG-SC-15	Public Key Infrastructure Certificates	All	DHS-2.8.15	Policy 3	No	None	None	None
SG-SC-16	Mobile Code	All	DHS-2.8.16	Protection 22	No	None	None	None
SG-SC-17	VeriCode Internet Protocol	None	DHS-2.8.17	Policy 3	No	None	None	None
SG-SC-18	System Connections	All	DHS-2.8.18	Policy 3	Yes	None	Remote Access Standard	Remote Access Process
SG-SC-19	Security Roles	All	DHS-2.8.19	Policy 2	No	None	None	None
SG-SC-20	Message Authenticity (Sender Name/Address Resolution Service)	All	DHS-2.8.20	Protection 17	No	None	None	None
SG-SC-21	Fail to Known State	All	DHS-2.8.22	Policy 3	No	None	None	None
SG-SC-22	Fail to Known State	All	N/A	Protection 19	No	None	None	None
SG-SC-23	Time Sinks	None	N/A	N/A	No	None	None	None
SG-SC-24	Hotspots	None	N/A	Detection 10	No	None	None	None
SG-SC-25	Operating System-Independent Applications	None	N/A	N/A	No	None	None	None
SG-SC-26	Confidentiality of Information at Rest	7,8,13,14,16	N/A	Policy 3	Yes	None	Access Control Standard	None
SG-SC-27	Heterogeneity	None	N/A	N/A	No	None	None	None
SG-SC-28	Virtualization Techniques	None	N/A	N/A	No	None	None	None
SG-SC-29	Application Partitioning Smart Grid Information System Partitioning	1,2,3,5,10,13,14	N/A	N/A	Yes	None	Access Management Standard	Infrastructure Process, LAN Systems Process
SG-SC-30	Smart Grid Information System and Information Industry Policy and Procedures	All	N/A	N/A	Yes	None	Availability Protection Standard	None
SG-SI-1	Smart Grid Information System and Information Industry Policy and Procedures	All	DHS-2.14.1	Policy 2	Yes	KCP&L-6300	None	Information Management Process
SG-SI-2	Flaw Remediation	All	DHS-2.14.2	Detection 15	No	None	None	None
SG-SI-3	Malicious Code and Spam Protection	All	DHS-2.14.3	Detection 18	Yes	KCP&L-6200	Anti-Virus Standard	Malicious Software Prevention Process
SG-SI-4	Smart Grid Information System Monitoring Tools and Techniques	All	DHS-2.14.4	Detection 19	Yes	KCP&L-6200	Anti-Virus Standard, Threat Monitoring Standard	Malicious Software Prevention Process, LAN Systems Process
SG-SI-5	Security Alerts and Advisories	All	DHS-2.14.5	Policy 6	Yes	KCP&L-6300	None	Malicious Software Prevention Process, LAN Systems Process
SG-SI-6	Security Functionality Verification	All	AMSP-2.14.1	N/A	No	None	None	None
SG-SI-7	Software and Information Integrity	1,2,3,5,7,8,9,10,13,14,15,16	DHS-2.14.7	Detection 16, 20, 11	Yes	None	Configuration Management Standard	Change Management Process, Configuration Management Process
SG-SI-8	Information Input Validation	All	AMSP-2.14.2	Detection 21	No	None	None	None
SG-SI-9	Error Handling	All	DHS-2.14.11	Detection 31, Protection 25	No	None	None	None

* - The physical security requirements in the NISTIR-7628 (PE Control Family) are *not* currently mandated in KCP&L policies, standards, and processes for any of the systems except for the EMS. In the case of EMS, it is believed that all 12 physical security requirements are currently mandated by KCP&L.

APPENDIX F SECURITY REQUIREMENTS FOR CONTROL SETS

NISTIR 7268 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Control Sets								
		C0	C1	C2	C3	C4	C5	C6	C7	C8
SG.AC-1	Access Control Policy and Procedures		X	X	X					
SG.AC-2	Remote Access Policy and Procedures		X	X	X					
SG.AC-3	Account Management		X	X	X					
SG.AC-4	Access Enforcement		X	X	X					
SG.AC-5	Information Flow Enforcement		X	X	X		X	X	X	X
SG.AC-6	Separation of Duties		X	X						
SG.AC-7	Least Privilege		X	X						
SG.AC-8	Unsuccessful Login Attempts		X	X	X	X				
SG.AC-9	Smart Grid Information System Use Notification		X	X	X					
SG.AC-10	Previous Logon Notification									
SG.AC-11	Concurrent Session Control		X	X						
SG.AC-12	Session Lock		X	X	X					
SG.AC-13	Remote Session Termination		X	X	X					
SG.AC-14	Permitted Actions without Identification or Authentication		X	X						
SG.AC-15	Remote Access		X	X	X					
SG.AC-16	Wireless Access Restrictions		X	X	X	X				
SG.AC-17	Access Control for Portable and Mobile Devices		X	X	X	X				
SG.AC-18	Use of External Information Control Systems	X								
SG.AC-19	Control System Access Restrictions		X							
SG.AC-20	Publicly Accessible Content	X								
SG.AC-21	Passwords	X								
SG.AT-1	Awareness and Training Policy and Procedures		X	X						
SG.AT-2	Security Awareness		X	X	X					
SG.AT-3	Security Training		X	X						
SG.AT-4	Security Awareness and Training Records		X							
SG.AT-5	Contact with Security Groups and Associations									
SG.AT-6	Security Responsibility Testing		X	X						
SG.AT-7	Planning Process Training									
SG.AU-1	Audit and Accountability Policy and Procedures		X	X						
SG.AU-2	Auditable Events		X	X						
SG.AU-3	Content of Audit Records		X	X						
SG.AU-4	Audit Storage Capacity		X	X						

NISTIR 7268 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Control Sets								
		C0	C1	C2	C3	C4	C5	C6	C7	C8
SG.AU-5	Response to Audit Processing Failures		X	X						
SG.AU-6	Audit Monitoring, Analysis, and Reporting		X	X						
SG.AU-7	Audit Reduction and Report Generation		X	X						
SG.AU-8	Time Stamps		X	X						
SG.AU-9	Protection of Audit Information		X	X						
SG.AU-10	Audit Record Retention		X	X						
SG.AU-11	Conduct and Frequency of Audits		X	X						
SG.AU-12	Auditor Qualification		X	X						
SG.AU-13	Audit Tools		X	X						
SG.AU-14	Security Policy Compliance	X								
SG.AU-15	Audit Generation									
SG.AU-16	Non-Repudiation									
SG.CA-1	Security Assessment and Authorization Policy and Procedures	X								
SG.CA-2	Security Assessments	X								
SG.CA-3	Continuous Improvement	X								
SG.CA-4	Smart Grid Information System Connections		X	X	X	X	X	X	X	X
SG.CA-5	Security Authorization to Operate	X				X				
SG.CA-6	Continuous Monitoring	X								
SG.CM-1	Configuration Management Policy and Procedures	X								
SG.CM-2	Baseline Configuration	X				X				
SG.CM-3	Configuration Change Control	X								
SG.CM-4	Monitoring Configuration Changes	X								
SG.CM-5	Access Restrictions for Configuration Change	X								
SG.CM-6	Configuration Settings	X				X				
SG.CM-7	Configuration for Least Functionality	X				X				
SG.CM-8	Component Inventory	X				X				
SG.CM-9	Addition, Removal, and Disposal of Equipment	X				X				
SG.CM-10	Factory Default Settings Management	X				X				
SG.CM-11	Configuration Management Plan	X								
SG.CP-1	Continuity of Operations Policy and Procedure	X				X				
SG.CP-2	Continuity of Operations Plan	X				X				
SG.CP-3	Continuity of Operations Roles and Responsibilities	X				X				
SG.CP-4	Continuity of Operations Training	X								

NISTIR 7268 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Control Sets								
		C0	C1	C2	C3	C4	C5	C6	C7	C8
SG.CP-5	Continuity of Operations Plan Testing	X				X				
SG.CP-6	Continuity of Operations Plan Update	X				X				
SG.CP-7	Alternate Storage Sites		X	X						
SG.CP-8	Alternate Telecommunication Services						X	X	X	
SG.CP-9	Alternate Control Center		X	X						
SG.CP-10	Smart Grid Information System Recovery and Reconstitution		X	X	X					
SG.CP-11	Fail-Safe Response		X	X						
SG.IA-1	Identification and Authentication Policy and Procedures	X								
SG.IA-2	Identifier Management	X								
SG.IA-3	Authenticator Management	X								
SG.IA-4	User Identification and Authentication		X	X	X					
SG.IA-5	Device Identification and Authentication		X	X	X	X	X	X	X	X
SG.IA-6	Authenticator Feedback	X								
SG.ID-1	Information and Document Management Policy and Procedures	X								
SG.ID-2	Information and Document Retention	X								
SG.ID-3	Information Handling	X								
SG.ID-4	Information Exchange	X								
SG.ID-5	Automated Labeling									
SG.IR-1	Incident Response Policy and Procedures	X								
SG.IR-2	Incident Response Roles and Responsibilities	X								
SG.IR-3	Incident Response Training	X								
SG.IR-4	Incident Response Testing and Exercises	X								
SG.IR-5	Incident Handling	X								
SG.IR-6	Incident Monitoring		X	X	X		X	X	X	
SG.IR-7	Incident Reporting	X								
SG.IR-8	Incident Response Investigation and Analysis	X								
SG.IR-9	Corrective Action	X								
SG.IR-10	Smart Grid Information System Backup		X	X	X					
SG.IR-11	Coordination of Emergency Response	X				X				
SG.MA-1	Smart Grid Information System Maintenance Policy and Procedures	X								
SG.MA-2	Legacy Smart Grid Information System Upgrades	X								
SG.MA-3	Smart Grid Information System Maintenance	X								

NISTIR 7268 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Control Sets								
		C0	C1	C2	C3	C4	C5	C6	C7	C8
SG.MA-4	Maintenance Tools	X								
SG.MA-5	Maintenance Personnel		X	X						
SG.MA-6	Remote Maintenance		X	X	X					
SG.MA-7	Timely Maintenance		X	X	X					
SG.MP-1	Media Protection Policy and Procedures	X								
SG.MP-2	Media Sensitivity Level	X								
SG.MP-3	Media Marking	X								
SG.MP-4	Media Storage	X								
SG.MP-5	Media Transport	X								
SG.MP-6	Media Sanitization and Disposal	X								
SG.PE-1	Physical and Environmental Security Policy and Procedures	X								
SG.PE-2	Physical Access Authorizations		X	X	X		X	X	X	
SG.PE-3	Physical Access		X	X	X		X	X	X	
SG.PE-4	Monitoring Physical Access		X	X	X		X	X	X	
SG.PE-5	Visitor Control		X	X	X		X	X	X	
SG.PE-6	Visitor Records		X	X	X		X	X	X	
SG.PE-7	Physical Access Log Retention		X	X	X		X	X	X	
SG.PE-8	Emergency Shutoff Protection	X								
SG.PE-9	Emergency Power				X				X	
SG.PE-10	Delivery and Removal		X	X	X					
SG.PE-11	Alternate Work Site		X	X						
SG.PE-12	Location of Smart Grid Information System Assets		X	X						
SG.PL-1	Strategic Planning Policy and Procedures	X				X				
SG.PL-2	Smart Grid Information System Security Plan	X				X				
SG.PL-3	Rules of Behavior	X								
SG.PL-4	Privacy Impact Assessment	X				X				
SG.PL-5	Security-Related Activity Planning	X				X				
SG.PM-1	Security Policy and Procedures	X				X				
SG.PM-2	Security Program Plan	X				X				
SG.PM-3	Senior Management Authority	X								

NISTIR 7268 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Control Sets								
		C0	C1	C2	C3	C4	C5	C6	C7	C8
SG-PM-4	Security Architecture	X								
SG-PM-5	Risk Management Strategy	X				X				
SG-PM-6	Security Authorization to Operate Process									
SG-PM-7	Mission/Business Process Definition	X				X				
SG-PM-8	Management Accountability	X								
SG-PS-1	Personnel Security Policy and Procedures	X								
SG-PS-2	Position Categorization		X	X	X					
SG-PS-3	Personnel Screening		X	X	X					
SG-PS-4	Personnel Termination	X								
SG-PS-5	Personnel Transfer	X								
SG-PS-6	Access Agreements	X								
SG-PS-7	Contractor and Third-Party Personnel Security	X								
SG-PS-8	Personnel Accountability	X								
SG-PS-9	Personnel Roles	X								
SG-RA-1	Risk Assessment Policy and Procedures	X				X				
SG-RA-2	Risk Management Plan	X				X				
SG-RA-3	Security Impact Level	X				X				
SG-RA-4	Risk Assessment	X				X				
SG-RA-5	Risk Assessment Update	X				X				
SG-RA-6	Vulnerability Assessment and Awareness	X								
SG-SA-1	Smart Grid Information System and Services Acquisition Policy and Procedures		X	X	X					
SG-SA-2	Security Policies for Contractors and Third Parties	X								
SG-SA-3	Life-Cycle Support	X				X				
SG-SA-4	Acquisitions	X								
SG-SA-5	Smart Grid Information System Documentation	X								
SG-SA-6	Software License Usage Restrictions	X								
SG-SA-7	User-Installed Software	X								
SG-SA-8	Security Engineering Principles	X								
SG-SA-9	Developer Configuration Management	X								
SG-SA-10	Developer Security Testing	X								
SG-SA-11	Supply Chain Protection		X	X	X		X	X	X	X
SG-SC-1	Smart Grid Information System and Communication Protection Policy and Procedures	X								
SG-SC-2	Communications Partitioning	X								

NISTIR 7268 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Control Sets								
		C0	C1	C2	C3	C4	C5	C6	C7	C8
SG-SC-3	Security Function Isolation	X				X				
SG-SC-4	Information Remnants	X								
SG-SC-5	Denial-of-Service Protection		X	X	X	X				
SG-SC-6	Resource Priority									
SG-SC-7	Boundary Protection		X	X	X		X	X	X	X
SG-SC-8	Communication Integrity	X								
SG-SC-9	Communication Confidentiality		X	X	X		X	X	X	X
SG-SC-10	Trusted Path		X	X	X		X	X	X	X
SG-SC-11	Cryptographic Key Establishment and Management	X								
SG-SC-12	Use of Validated Cryptography	X								
SG-SC-13	Collaborative Computing									
SG-SC-14	Transmission of Security Parameters	X								
SG-SC-15	Public Key Infrastructure Certificates	X								
SG-SC-16	Mobile Code									
SG-SC-17	Voice-Over Internet Protocol									
SG-SC-18	System Connections	X								
SG-SC-19	Security Roles	X								
SG-SC-20	Message Authenticity	X								
SG-SC-21	Secure Name/Address Resolution Service									
SG-SC-22	Fall in Known State		X	X	X					
SG-SC-23	Thin Nodes									
SG-SC-24	Honeypots									
SG-SC-25	Operating System-Independent Applications									
SG-SC-26	Confidentiality of Information at Rest		X	X						
SG-SC-27	Heterogeneity	X								
SG-SC-28	Virtualization Techniques									
SG-SC-29	Application Partitioning		X	X	X					
SG-SC-30	Smart Grid Information System Partitioning	X								
SG-SI-1	Smart Grid Information System and Information Integrity Policy and Procedures	X								
SG-SI-2	Flaw Remediation									
SG-SI-3	Malicious Code and Spam Protection		X	X	X					
SG-SI-4	Smart Grid Information System Monitoring Tools and Techniques		X	X			X	X	X	X
SG-SI-5	Security Alerts and Advisories		X	X			X	X	X	X
SG-SI-6	Security Functionality Verification	X								

NISTIR 7268 Smart Grid Requirement Number	NISTIR 7268 Smart Grid Requirement Name	Control Sets								
		C0	C1	C2	C3	C4	C5	C6	C7	C8
SG-SI-7	Software and Information Integrity		X	X	X					
SG-SI-8	Information Input Validation	X								
SG-SI-9	Error Handling	X								

APPENDIX G SAMPLE QUESTIONNAIRE FOR HOSTING VENDORS

Service/Software/System Description			
Name of Service/System			
Short Description of Service/System			
Sponsoring Department		Name	
Lead Project Administrator			
Lead Technical Contact			
Additional KCP&L Contacts		Name	Department
<i>list any additional administrative contacts or those providing technical support from other departments</i>			
Hosting Service Provider			
Company Name			
Contacts	Name	Phone	Email Address
Administrative Representative			
Technical Contact			
Reference URL			
Additional Information Needed			
Data Classification Definitions			
<u>Restricted:</u> Information for which inadvertent access or disclosure would have legal, regulatory, reputation, or financial repercussions. Access is limited to specific individuals.			
<u>Internal Use Only:</u> Information that is generally available to employees and approved non-employees			
<u>Public:</u> Information officially released for widespread public disclosure or considered to have value but no risk of unauthorized disclosure			

Security Controls**1.0 HIGH LEVEL DESCRIPTION**

1.1	Please provide a brief description of the purpose of the system, including how the information will be used. If possible, include a simple diagram of the dataflow and where Restricted or Internal Use Only Data will be stored.
------------	---

2.0 AUTHENTICATION

		<u>YES</u>	<u>NO</u>
2.1	Will users of the hosted service be authenticated by KCP&L systems?		
2.2	Will users be authenticated by the hosting service provider?		
2.2.1	Will userids assigned by the service provider match KCP&L userids?		
2.2.2	Will each user have a unique userid?		
2.2.3	Can the service provider's system be configured to require strong passwords?		
2.2.4	Can KCP&L dictate password criteria as needed to ensure compliance with KCP&L security standards?		
2.2.5	Can the service provider's system be configured to expire user passwords periodically in accordance with KCP&L security standards?		
2.2.6	Does the service provider provide a function to enable users to change their own password securely?		
2.2.7	Can accounts be locked after a KCP&L defined number of unsuccessful login attempts?		
2.2.8	Can the service provider's system de-authenticate users after a KCP&L defined period of inactivity?		
2.2.9	Does the hosted service provide a logout on-demand option?		
2.2.10	Are passwords entered in a non-display field?		
2.2.11	Are passwords encrypted during network transit?		
2.2.12	Are passwords encrypted in storage?		
2.2.13	Are all attempted and successful logins logged, include date/time, userid, source network address, and are maintained for at least one year?		

3.0 AUTHORIZATION – Logical Access Control		<u>YES</u>	<u>NO</u>
3.1	Will users be authorized by a KCP&L based system?		
3.2	Will users be authorized by the hosting service provider's system?		
3.2.1	Does the service provider's system offer the ability to restrict access within the application based on roles assigned to authorized users?		
3.2.2	Will the service provider's system provide easy to read security reports that identify users and their access levels for periodic review?		
3.2.3	Can the authorization process be configured to automatically disable user accounts or access privileges after a KCP&L defined period of non-use?		
3.3	Can the service provider's security controls detect and report unauthorized access attempts?		

4.0 DATA SECURITY		<u>YES</u>	<u>NO</u>
4.1	Is all network transfer of KCP&L Restricted or Internal Use Only Data encrypted when traversing the service provider's network and the KCP&L network or non-KCP&L networks?		
4.2	Is all network transfer of KCP&L Restricted or Internal Use Only Data encrypted between multiple service providers' systems (e.g. web and database servers)?		
4.3	Is all physical transfer of KCP&L Restricted Data encrypted (e.g. backups to tape, disk, DVD)?		
4.4	Will any KCP&L Restricted or Internal Use Only Data be stored, temporarily or otherwise, on end-user workstations, portable devices, or removable media?		
4.4.1	If so, will the data be stored encrypted using a strong encryption methodology?		
4.5	If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving?		
4.6	Does the service provider's software provide appropriate controls to ensure data integrity (e.g. input validation, checksums of stored data, transaction redo logs)?		
4.7	Will the service provider's developers and systems administration staff who have access to KCP&L Restricted or Internal Use Only Data, have unique account IDs assigned to them?		

4.8	Are the duties of the service provider's technical staff separated to ensure least privilege and individual accountability?		
4.8.1	Are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties?		
4.9	Is the activity of service provider's technical staff logged when performing system maintenance?		
4.9.1	If so, are activity logs maintained for at least one year?		
4.10	Is user-level access to KCP&L Restricted or Internal Use Only Data logged, monitored, and possible security violations investigated?		
4.10.1	Can this log data be made available to KCP&L?		
4.10.2	Does this log data specify the data element or data record accessed and the action taken upon the data (e.g. View, Modify, Delete)?		
4.10.3	Can the log data support after-the-fact investigations detailing who, when, and how data or systems were accessed?		
4.10.4	Will the service provider's system provide easy to read access audit reports for periodic review?		
4.10.5	Will access to the audit reports be logged and strictly controlled?		
5.0 RECOVERABILITY		<u>YES</u>	<u>NO</u>
5.1	Is the service provider fully aware of KCP&L's recoverability objectives?		
5.2	Does the service provider have and follow a data and system backup plan commensurate with KCP&L's recoverability objective?		
5.3	Does the service provider have an adequate hardware maintenance contract or hot spare inventory to meet KCP&L's recoverability objective after a hardware failure?		
5.4	Does the service provider have the capability to execute a recovery from a security incident, complete system failure or destruction within the time-frame of KCP&L's recoverability objective?		
5.5	To what extent does the hosting service provider ensure system availability consistent with KCP&L's recoverability objectives? (e.g. backup power systems, redundant network paths, use of virtual machines, etc)		

6.0 OPERATIONAL CONTROLS		YES	NO
6.1	Does the service provider outsource hosting of their application and data storage servers to a third-party?		
6.2	Has the service provider taken measures to ensure the physical security of the data center(s) in which the application and data storage servers are housed, specifically addressing access controlled and audited entry ways, temperature monitoring and control, fire prevention and suppression, and use of a backup power source?		
6.3	If the service provider is currently providing hosting services for other clients, is multi-client access effectively controlled to ensure users are restricted to only the data they are authorized to access?		
6.4	Does the service provider maintain and apply host security standards on their servers and verify them whenever changes in configuration are introduced into the system?		
6.5	Does the service provider have and exercise a process to maintain current patch levels of software running on their systems?		
6.6	Does the service provider implement anti-malware controls on servers?		
6.7	Does the service provider practice effective electronic data destruction procedures when hardware is recycled for repair or removed for disposal?		
8.6.1	If the service provider outsources information destruction services, is the outsourced destruction service a NAID Certified Operation? see: http://www.naidonline.org/certified_members.html		
8.6.2	If the service provider outsources information destruction services, please specify the name and address of the outsourced vendor:		
6.8	What process will be provided to purge old records from service provider systems?		
6.9	Does the service provider have an information security audit or evaluation program for their operation?		
6.10	What methods are used to ensure the expertise of service provider employees who have access to KCP&L Restricted or Internal Use Only Data?		
6.11	What methods are used to ensure that service provider employees, who have access to KCP&L Restricted or Internal Use Only Data, have been properly vetted? (e.g. law enforcement background checks)		
6.12	Does the service provider have an effective procedure for timely termination of access of their staff and KCP&L users (upon notification) who no longer need access to the service provider's system?		

6.13	What methods are used by service provider staff for remote access to systems that store KCP&L Restricted or Internal Use Only Data?		
6.14	What administrative access will KCP&L IT workers have to hosted service on vendor systems?		
6.15	To what extent does the service provider test its software for security vulnerabilities, including conducting software penetration tests?		
6.16	Are tests and examinations of key controls routinely made, i.e., network scans, analyses of router and switch settings, penetration testing?		
7.0 INCIDENT RESPONSE		<u>YES</u>	<u>NO</u>
7.1	Does the service provider have a documented process for reporting security incidents involving systems used to store/access/modify hosted KCP&L data to the KCP&L Department contact or, if appropriate, law enforcement?		
7.2	Are security incidents monitored and tracked until resolved?		
7.3	Is incident information and common vulnerabilities or threats shared with owners of interconnected systems or data hosting customers?		
7.4	Will a third party ever have access to the service provider's hardware or systems that store KCP&L Restricted or Internal Use Only Data?		
7.5	Are the service provider's database and web server access and error logs regularly reviewed for anomalies that could indicate a compromise?		
7.6	What process does the service provider have in place to identify security breaches on vendor managed systems (e.g. file integrity checks)?		
7.7	In the case of a security breach or unexpected exposure of KCP&L Restricted or Internal Use Only Data, what are the hosting service provider's incident response procedures?		
7.8	What is the service provider's process for disclosing to KCP&L any data requests, such as subpoenas or warrants, from a third party?		

8.0 APPLICATION SECURITY		<u>YES</u>	<u>NO</u>
8.1	Does the software development life-cycle model used by the hosting service provider in the development of their software, incorporate features from any standards based framework models (e.g. TSP-Secure, SAMM, Microsoft SDL, OWASP, NIST SP800-64 rev 2,)? If so, please specify.		
8.1.1	Are security components identified and represented during each phase of the software development life-cycle?		
8.2	Does the service provider have change management policies in place?		
8.2.1	Is a pre-determined maintenance window used to apply changes?		
8.2.2	How much lead-time will the service provider give KCP&L of upcoming changes?		
8.2.3	How are customers notified of changes?		
8.2.4	Does the service provider have a process to test their software for anomalies when new operating system patches are applied?		
8.2.5	Has a technical and/or security evaluation been completed or conducted when a significant change occurred?		
8.3	Are source code audits performed regularly?		
8.3.1	Are source code audits performed by someone other than the person or team that wrote the code?		
8.4	Is access to the service provider's application restricted to encrypted channels (e.g. https)?		
8.5	Describe the session management processes used by the hosted service's applications.		
9.0 TESTING AND VALIDATION		<u>YES</u>	<u>NO</u>
9.1	Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change?		
9.2	Can the hosting service provider make available a test evaluation instance of their service or application that can be used by KCP&L IT security staff to validate the information security assertions made by the vendor?		
9.2.1	Can the test evaluation instance include access at both the user-level interface and management-level interface?		



**APPENDIX H UNCONFIRMED SECURITY REQUIREMENTS FROM UCAIUG AMI AND DM
SECURITY PROFILES**

UCAIug AMI Security Profile Requirement	Requirement Title
DHS-2.8.21	Architecture and Provisioning for Name/Address Resolution Service
DHS-2.8.23	Secure Name/Address Resolution Service (Recursive or Caching Resolver)
AMISP-2.8.1	Secure Name/Address Resolution Service (Address Resolution Tampering)
DHS-2.9.4	Information Classification
DHS-2.9.6	Information and Document Classification
DHS-2.9.7	Information and Document Retrieval
DHS-2.9.8	Information and Document Destruction
DHS-2.9.9	Information and Document Management Review
DHS-2.10.3	System Monitoring and Evaluation
DHS-2.10.5	Unplanned System Maintenance
DHS-2.14.8	Unauthorized Communications Protection
DHS-2.14.9	Information Input Restrictions
DHS-2.14.12	Information Output Handling and Retention
AMISP-2.15.1	Supervision and Review
DHS-2.15.14	Cryptographic Module Authentication
DHS-2.15.27	Untrusted IT Equipment
DHS-2.15.28	External Access Protections
AMISP-2.15.2	Unauthorized Access Reporting
AMISP-2.17.1	Delay of Remote Connect/Disconnect

Source: The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG)
 - Security Profile for Advanced Metering Infrastructure V2.0

UCAIug DM Security Profile Requirement	Requirement Title
Network.1	DM Networks are Private
Network.5	Redundancy
Network.6	Emergency Network Segmentation
Detection.3	Electronic Log Format
Detection.4	Power Source Monitoring/Logging
Detection.5	Location of Mobile Components
Detection.6	Fire Detection
Detection.9	Self Identification
Detection.17	Firmware/Configuration Authenticity
Detection.22	Message Delay Detection
Detection.23	Device Self Test
Detection.24	Heartbeat
Detection.27	Inappropriate User Activity
Detection.29	IDS Architecture
Detection.30	Physical Access Indications
Detection.32	Message Validation
Protection.5	Power Sources and Cables
Protection.6	Component Location
Protection.7	Control Center Location
Protection.8	EMI/Surge Protection
Protection.14	Remote Interactive Sessions
Protection.18	Addressing
Protection.23	Disabling Unnecessary Communication Services
Protection.24	No Internet Access
Protection.34	Cryptographic Module Authentication
Protection.41	Wireless Encryption
Protection.43	WAN Communication Outage
Protection.45	Non-adjacent Network Restrictions
Protection.47	Centralized Authentication
Protection.49	Message Identities
Protection.50	Data Point State Indicators
Protection.52	Application Layer Security
Protection.53	Separate Keys for Separate Functions
Reaction.3	Physical Access Correlation
Reaction.4	Unscheduled or Unapproved Activity

UCAIug DM Security Profile Requirement	Requirement Title
Reaction.7	End Point Isolation
Recovery 4	Rebuild System

Source: The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) - Security Profile for Distribution Management V0.9

APPENDIX I | ADDITIONAL REFERENCES

- Standards for Security Categorization of Federal Information and Information Systems. FIPS PUB 199. <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>
- Creating a Patch and Vulnerability Management Program. National Institute of Standards and Technology (NIST) Special Publication 800-40 Version 2.0. <http://csrc.nist.gov/publications/nistpubs/800-40-Vcr2/SP800-40v2.pdf>
- Study of Security Attributes of Smart Grid Systems – Current Cyber Security Issues April 2009. Idaho National Lab (INL) Critical Infrastructure Protection/Resilience Center. U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability. http://www.inl.gov/scada/publications/d/securing_the_smart_grid_current_issues.pdf
- Recommended Security Controls for Federal Information Systems and Organizations. National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 3. <http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf>
- Guide to Industrial Control Systems (ICS) Security. Recommendations of the National Institute of Standards and Technology (NIST) Special Publication 800-82. <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>

Appendix N Cyber Security Controls Matrix

Legend (Non-Network Requirements)

For each control that was found to be applicable to a system ("Yes"), the cell is shaded a specific color to indicate the following:

Green indicates that the requirement is the responsibility of the vendor(s) to implement.

Yellow indicates that the requirement is the responsibility of both KCP&L and the vendor(s) to implement.

Blue indicates that the requirement is the responsibility of KCP&L to implement.

Cyber Security Controls Matrix										
Requirement Number	Requirement Name	Req. Type	NTWK	MDM	AMI	DERM	HEMP	DMS	DCADA DDC	BESS
SG.AC-1	Access Control Policy and Procedures	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-2	Remote Access Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-3	Account Management	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-4	Access Enforcement	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-5	Information Flow Enforcement	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-6	Separation of Duties	Tech	No	Yes	Yes	Yes	Yes	Yes	Yes	No
SG.AC-7	Least Privilege	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
SG.AC-8	Unsuccessful Login Attempts	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-9	Smart Grid Information System Use Notification	Tech	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-10	Previous Logon Notification	Tech	No	No	No	No	No	No	No	No
SG.AC-11	Concurrent Session Control	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-12	Session Lock	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-13	Remote Session Termination	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-14	Permitted Actions without Identification or Authentication	Tech	No	Yes	Yes	Yes	Yes	Yes	Yes	No
SG.AC-15	Remote Access	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AC-16	Wireless Access Restrictions	Tech	No	No	Yes	No	Yes	No	Yes	Yes
SG.AC-17	Access Control for Portable and Mobile Devices	Tech	No	No	No	No	Yes	No	No	No
SG.AC-18	Use of External Information Control Systems	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Cyber Security Controls Matrix										
Requirement Number	Requirement Name	Req. Type	NTWK	MDM	AMI	DERM	HEMP	DMS	DCADA DDC	BESS
SG.AC-19	Control System Access Restrictions	Admin	Yes	No	No	No	No	Yes	No	No
SG.AC-20	Publicly Accessible Content	Admin	No	No	No	No	No	No	No	No
SG.AC-21	Passwords	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AT-1	Awareness and Training Policy and Procedures	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AT-2	Security Awareness	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AT-3	Security Training	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	No
SG.AT-4	Security Awareness and Training Records	Admin	No	No	No	No	No	No	No	No
SG.AT-5	Contact with Security Groups and Associations	Admin	No	No	No	No	No	No	No	No
SG.AT-6	Security Responsibility Testing	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	No
SG.AT-7	Planning Process Training	Admin	No	No	No	No	No	No	No	No
SG.AU-1	Audit and Accountability Policy and Procedures	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-2	Auditable Events	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-3	Content of Audit Records	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-4	Audit Storage Capacity	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-5	Response to Audit Processing Failures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-6	Audit Monitoring, Analysis, and Reporting	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-7	Audit Reduction and Report Generation	Admin	No	No	No	No	No	No	No	No
SG.AU-8	Time Stamps	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-9	Protection of Audit Information	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-10	Audit Record Retention	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-11	Conduct and Frequency of Audits	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-12	Auditor Qualification	Admin	No	No	No	No	No	Yes	Yes	Yes
SG.AU-13	Audit Tools	Admin	No	No	No	No	No	No	No	No
SG.AU-14	Security Policy Compliance	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.AU-15	Audit Generation	Tech	No	No	No	No	No	No	No	No
SG.AU-16	Non-Repudiation	Tech	No	No	No	No	No	No	No	No
SG.CA-1	Security Assessment and Authorization Policy and Procedures	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Cyber Security Controls Matrix										
Requirement Number	Requirement Name	Req. Type	NTWK	MDM	AMI	DERM	HEMP	DMS	DCADA DDC	BESS
SG.CA-2	Security Assessments	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CA-3	Continuous Improvement	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CA-4	Smart Grid Information System Connections	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CA-5	Security Authorization to Operate	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CA-6	Continuous Monitoring	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CM-1	Configuration Management Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CM-2	Baseline Configuration	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CM-3	Configuration Change Control	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CM-4	Monitoring Configuration Changes	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CM-5	Access Restrictions for Configuration Change	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CM-6	Configuration Settings	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CM-7	Configuration for Least Functionality	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CM-8	Component Inventory	Tech	Yes	No	No	No	No	Yes	Yes	Yes
SG.CM-9	Addition, Removal, and Disposal of Equipment	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CM-10	Factory Default Settings Management	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.CM-11	Configuration Management Plan	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CP-1	Continuity of Operations Policy and Procedure	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CP-2	Continuity of Operations Plan	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CP-3	Continuity of Operations Roles and Responsibilities	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CP-4	Continuity of Operations Training	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.CP-5	Continuity of Operations Plan Testing	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CP-6	Continuity of Operations Plan Update	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CP-7	Alternate Storage Sites	Admin	No	No	No	No	No	Yes	Yes	No
SG.CP-8	Alternate Telecommunication Services	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CP-9	Alternate Control Center	Admin	Yes	No	No	No	No	No	No	No

Cyber Security Controls Matrix										
Requirement Number	Requirement Name	Req. Type	NTWK	MDM	AMI	DERM	HEMP	DMS	DCADA DDC	BESS
SG.CP-10	Smart Grid Information System Recovery and Reconstitution	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.CP-11	Fail-Safe Response	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IA-1	Identification and Authentication Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IA-2	Identifier Management	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IA-3	Authenticator Management	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IA-4	User Identification and Authentication	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IA-5	Device Identification and Authentication	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IA-6	Authenticator Feedback	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.ID-1	Information and Document Management Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.ID-2	Information and Document Retention	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.ID-3	Information Handling	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.ID-4	Information Exchange	Admin	No	Yes	Yes	Yes	Yes	No	No	No
SG.ID-5	Automated Labeling	Admin	No	No	No	No	No	No	No	No
SG.IR-1	Incident Response Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IR-2	Incident Response Roles and Responsibilities	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IR-3	Incident Response Training	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IR-4	Incident Response Testing and Exercises	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IR-5	Incident Handling	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IR-6	Incident Monitoring	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IR-7	Incident Reporting	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IR-8	Incident Response Investigation and Analysis	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IR-9	Corrective Action	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.IR-10	Smart Grid Information System Backup	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Cyber Security Controls Matrix										
Requirement Number	Requirement Name	Req. Type	NTWK	MDM	AMI	DERM	HEMP	DMS	DCADA DDC	BESS
SG.IR-11	Coordination of Emergency Response	Admin	No	No	No	No	No	Yes	Yes	Yes
SG.MA-1	Smart Grid Information System Maintenance Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.MA-2	Legacy Smart Grid Information System Upgrades	Admin	No	No	No	No	No	No	No	No
SG.MA-3	Smart Grid Information System Maintenance	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.MA-4	Maintenance Tools	Admin	Yes	No	No	No	No	No	No	No
SG.MA-5	Maintenance Personnel	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.MA-6	Remote Maintenance	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.MA-7	Timely Maintenance	Admin	Yes	No	No	No	No	No	No	No
SG.MP-1	Media Protection Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.MP-2	Media Sensitivity Level	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.MP-3	Media Marking	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.MP-4	Media Storage	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.MP-5	Media Transport	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.MP-6	Media Sanitization and Disposal	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PE-1	Physical and Environmental Security Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PE-2	Physical Access Authorizations	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PE-3	Physical Access	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PE-4	Monitoring Physical Access	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PE-5	Visitor Control	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PE-6	Visitor Records	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PE-7	Physical Access Log Retention	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PE-8	Emergency Shutoff Protection	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PE-9	Emergency Power	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PE-10	Delivery and Removal	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.PE-11	Alternate Work Site	Admin	No	No	No	No	No	No	No	No
SG.PE-12	Location of Smart Grid Information System Assets	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PL-1	Strategic Planning Policy and Procedures	Admin	Yes	No	No	No	No	Yes	Yes	Yes

Cyber Security Controls Matrix										
Requirement Number	Requirement Name	Req. Type	NTWK	MDM	AMI	DERM	HEMP	DMS	DCADA DDC	BESS
SG.PL-2	Smart Grid Information System Security Plan	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.PL-3	Rules of Behavior	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.PL-4	Privacy Impact Assessment	Admin	No	No	No	No	Yes	No	No	No
SG.PL-5	Security-Related Activity Planning	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.PM-1	Security Policy and Procedures	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.PM-2	Security Program Plan	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.PM-3	Senior Management Authority	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.PM-4	Security Architecture	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PM-5	Risk Management Strategy	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.PM-6	Security Authorization to Operate Process	Admin	No	No	No	No	No	No	No	No
SG.PM-7	Mission/Business Process Definition	Admin	Yes	No	No	No	No	No	No	No
SG.PM-8	Management Accountability	Admin	Yes	Yes	Yes	Yes	Yes	No	No	No
SG.PS-1	Personnel Security Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PS-2	Position Categorization	Admin	Yes	No	No	No	No	No	No	No
SG.PS-3	Personnel Screening	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PS-4	Personnel Termination	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PS-5	Personnel Transfer	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PS-6	Access Agreements	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PS-7	Contractor and Third-Party Personnel Security	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PS-8	Personnel Accountability	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.PS-9	Personnel Roles	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.RA-1	Risk Assessment Policy and Procedures	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.RA-2	Risk Management Plan	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.RA-3	Security Impact Level	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.RA-4	Risk Assessment	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.RA-5	Risk Assessment Update	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.RA-6	Vulnerability Assessment and Awareness	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Cyber Security Controls Matrix										
Requirement Number	Requirement Name	Req. Type	NTWK	MDM	AMI	DERM	HEMP	DMS	DCADA DDC	BESS
SG.SA-1	Smart Grid Information System and Services Acquisition Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SA-2	Security Policies for Contractors and Third Parties	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SA-3	Life-Cycle Support	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SA-4	Acquisitions	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SA-5	Smart Grid Information System Documentation	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SA-6	Software License Usage Restrictions	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SA-7	User-Installed Software	Admin	Yes	No	No	No	No	Yes	Yes	Yes
SG.SA-8	Security Engineering Principles	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SA-9	Developer Configuration Management	Admin	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SA-10	Developer Security Testing	Tech	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SA-11	Supply Chain Protection	Tech	Yes	No	No	No	No	No	No	No
SG.SC-1	Smart Grid Information System and Communication Protection Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-2	Communications Partitioning	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-3	Security Function Isolation	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-4	Information Remnants	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-5	Denial-of-Service Protection	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-6	Resource Priority	Tech	No	No	No	No	No	No	No	No
SG.SC-7	Boundary Protection	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-8	Communication Integrity	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-9	Communication Confidentiality	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-10	Trusted Path	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-11	Cryptographic Key Establishment and Management	Tech	No	No	No	No	No	Yes	Yes	Yes
SG.SC-12	Use of Validated Cryptography	Tech	No	No	No	No	No	Yes	Yes	Yes
SG.SC-13	Collaborative Computing	Admin	No	No	No	No	No	No	No	No
SG.SC-14	Transmission of Security Parameters	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Cyber Security Controls Matrix										
Requirement Number	Requirement Name	Req. Type	NTWK	MDM	AMI	DERM	HEMP	DMS	DCADA DDC	BESS
SG.SC-15	Public Key Infrastructure Certificates	Tech	No	No	No	No	No	Yes	Yes	Yes
SG.SC-16	Mobile Code	Tech	No	No	No	No	No	No	No	No
SG.SC-17	Voice-Over Internet Protocol	Tech	No	No	No	No	No	No	No	No
SG.SC-18	System Connections	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-19	Security Roles	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-20	Message Authenticity	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-21	Secure Name/Address Resolution Service	Tech	No	No	No	No	No	No	No	No
SG.SC-22	Fail in Known State	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-23	Thin Nodes	Tech	No	No	No	No	No	No	No	No
SG.SC-24	Honeypots	Tech	No	No	No	No	No	No	No	No
SG.SC-25	Operating System-Independent Applications	Tech	No	No	No	No	No	No	No	No
SG.SC-26	Confidentiality of Information at Rest	Tech	No	Yes	Yes	Yes	Yes	Yes	Yes	No
SG.SC-27	Heterogeneity	Tech	No	No	No	No	No	No	No	No
SG.SC-28	Virtualization Techniques	Tech	Yes	No	No	No	No	No	No	No
SG.SC-29	Application Partitioning	Tech	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SC-30	Smart Grid Information System Partitioning	Tech	Yes	Yes	Yes	Yes	Yes	No	No	No
SG.SI-1	Smart Grid Information System and Information Integrity Policy and Procedures	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SI-2	Flaw Remediation	Tech	Yes	No	No	No	No	Yes	Yes	Yes
SG.SI-3	Malicious Code and Spam Protection	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SI-4	Smart Grid Information System Monitoring Tools and Techniques	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SI-5	Security Alerts and Advisories	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SI-6	Security Functionality Verification	Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SI-7	Software and Information Integrity	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SI-8	Information Input Validation	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SG.SI-9	Error Handling	Tech	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Appendix O AMI Audit Results

To be completed in future releases of this report.

Appendix P Education & Outreach Collateral

To be completed in future releases of this report.

Appendix Q EPRI SmartEnd-Use Analysis Results

To be completed in future releases of this report.

Appendix R Navigant SmartEnd-Use Program Analysis Results

To be completed in future releases of this report.

Appendix S Customer Survey Results

To be completed in future releases of this report.

Appendix T Final Build Metrics

To be completed in future releases of this report.

Appendix U Final Impact Metrics

To be completed in future releases of this report.

This page intentionally blank.

This page intentionally blank.

DOE ACKNOWLEDGEMENT

This material is based upon work supported by the Department of Energy
under Award Number DE-OE0000221

FEDERAL DISCLAIMER

"This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof."