AMI Use Case:

B3 - Utility detects tampering or theft at customer site

03/16/06

Author: James McGrath

Document History

Revision History

Revision Number	Revision Date	Revision / Reviewed By	Summary of Changes	Changes marked
(#)	(yymmdd)	(Name)	(Describe change)	(N)
1.0	060201	Prafs Diwate	Initial document	N
1.1	060310	Ben Rankin	Updated document based on feedback from SAT	Y
1.2	060315	Ben Rankin	Final edits from session notes	N
1.3	060316	Ben Rankin	Corrected 4 requirement references to scenario steps	N

Approvals

This document requires following approvals.

Name	Title
James McGrath	*Mega-Team Lead*
Victor Pimentel	*Use Case Team Lead*
Kevin Wood	*System Architecture Team Chair*
Grant Watson	*Engineering Team Chair*

Contents

1. Use Case Description

1.1 Use Case Title

Utility detects tampering or theft at customer site

1.2 Use Case Summary

A serious threat to utilities is theft of services. There is also a large liability potential if tampering remains undetected.

This scenario describes the process by which the utility detects tamper/theft through communication with the meter. It includes the methods by which the communication equipment detects the tampering/theft. Tamper methods include, for example, comparison of the load profile data against historical records, or a spontaneous report of a tamper switch being triggered at the customer site.

This scenario excludes the actual reading of data required to support a determination of theft/tamper detection. This is covered by scenario B1. It also excludes the actual algorithms used to determine whether theft is occurring.

1.3 Use Case Detailed Narrative

Energy theft is a serious problem. Meter tampering and current diversion account for significant lost revenue. As energy prices increase, cases of energy theft are likely to rise also; resulting in consumer rate increases to offset the losses. Tampering and energy theft also pose serious public safety concerns. A tampered meter can cause burns, severe injury or even death to thieves, bystanders and utility personnel. Adding to this problem is the increased availability of information on energy theft techniques. Publications, and more often today the Internet, provide easily obtainable information on methods of stealing power.

Energy loss due to current diversion and meter tampering exists regardless of social or economic group. Theft can range from periodic meter interruptions to ongoing diversion. Even larger losses can be attributed to illegal taps into the power supply.

Energy theft, such as meter tampering, occurs daily and can go undetected for months, even years. Tampering can be as simple as inverting the meter to more sophisticated methods such as installing jumpers or other instruments to disrupt accuracy. Wiring in photocells or resistors to alter meter precision is a subtle and difficult to detect manner of meter tampering. Enterprising thieves have even gone as far as installing timers or switches to control meter validation.

The two main categories of energy theft are physically tampering with the meter (removing and reinstalling and/or breaching of the physical meter case) and bypassing the meter.

A more benign form of meter tampering is the temporary removal of a meter by a customer and/or contractor while electrical work is being performed at the customer’s premise. Once the work has been completed the meter is replaced and service fully restored. In most cases these temporary situations go unnoticed with the current state of residential metering, and for the most part little or no harm is done. However, in some cases when the meter is reinstalled it is not installed correctly or is damaged causing inaccurate measurements to be recorded.. This can result in inaccurate bills being issued as well as increased costs to the utility to replace/repair their meters once the fault has been isolated. An AMI meter with tamper detection capability would enable the utility to sense a change in consumption that could mean a damaged/malfunctioning meter. The ability to identify and resolve these situations in a timely manner would prevent an impact to bill quality from the damaged meter. A definite audit trail showing precisely when the tampering occurred and showing that the meter was operating correctly prior to the event and began malfunctioning after the meter was reinstalled would provide evidence sufficient to possibly compelled the customer and/or contractor to pay for the replacement/repair of the meter, which is after all the property of the utility.

1.4 Business Rules and Assumptions

- The use case applies to customers with a load smaller than 200 kW (non-RTEM)
- The meter may be compromised if access can be gained to its internal mechanism
- The meter has a seal/lock to prevent/detect removal or access to its internal mechanism
- Meter removal, bypass, and inversion is considered tampering

2. Actors

Describe the primary and secondary actors involved in the use case. This might include all the people (their job), systems, databases, organizations, and devices involved in or affected by the Function (e.g. operators, system administrators, customer, end users, service personnel, executives, meter, real-time database, ISO, power system). Actors listed for this use case should be copied from the global actors list to ensure consistency across all use cases.

Actor Name	***Actor Type (person, device, system etc.)***	***Actor Description***
Customer	Person	An individual or organization that is associated with the service delivery point. They may have physical custodianship, financial responsibility or both.
Meter	Device	The scenarios anticipate 3 types of tamper detection: meter removal, breaching of the meter case as well as detecting load side voltage when disconnect switch is open.
AMI Back Office system	System	This represents the components and function necessary to receive, store and/or process messages and events received from the AMI system and the messages/events that may be generated and sent through the AMI System to the meters/in-home display/other devices.
Unknown/Unauthorized person	Person	This individual may be the premise customer or an "agent" (i.e. contractor) of the premise customer or some other individual who intends to manipulate the meter and is not authorized by the utility to carry out these actions.

3. Step by Step analysis of each Scenario

Describe steps that implement the scenario. The first scenario should be classified as either a "Primary" Scenario or an "Alternate" Scenario by starting the title of the scenario with either the work "Primary" or "Alternate". A scenario that successfully completes without exception or relying heavily on steps from another scenario should be classified as Primary; all other scenarios should be classified as "Alternate". If there is more than one scenario (set of steps) that is relevant, make a copy of the following section (all of 3.1, including 3.1.1 and tables) and fill out the additional scenarios.

3.1 Primary Scenario: Meter removal

Triggering Event	***Primary Actor***	***Pre-Condition***	***Post-Condition***
(Identify the name of the event that start the scenario)	*(Identify the actor whose point-of-view is primarily used to describe the steps)*	*(Identify any pre-conditions or actor states necessary for the scenario to start)*	*(Identify the post-conditions or significant results required to consider the scenario complete)*
Removal of the meter	Meter	Meter must be installed and capable of communicating with the AMI system. The meter may or may not be energized.	AMI system successfully detects meter removal and sends event notice to back office system

3.1.1 Steps for this scenario

Describe the normal sequence of events that is required to complete the scenario.

Step #	***Actor***	***Description of the Step***	***Additional Notes***
#	*What actor, either primary or secondary is responsible for the activity in this step?*	*Describe the actions that take place in this step. The step should be described in active, present tense.*	*Elaborate on any additional description or value of the step to help support the descriptions. Short notes on architecture challenges, etc. may also be noted in this column..*

Step #	Actor	Description of the Step	Additional Notes
1	Unknown/Unauthorized person	Someone removes meter.	This could also be an authorized person. Whether the person is authorized or unauthorized is determined later in the scenario.
2	Meter	Meter detects removal	
3	Meter	Meter sends removal event to AMI back office system.	This alerts the utility that the meter has been removed. The utility can then check it's records to determine if the removal has been authorized. If unauthorized, one of the options may be to send a field representative to the customer's site to inspect the condition.
4	Meter	Meter records event (in case when meter cannot communicate) and attempts to send it to AMI back office system.	
5	Unknown/Unauthorized person	Meter is re-installed	
6	Meter	Meter sends re-installation event to AMI back office system.	This allows the utility to monitor the customer's usage pattern to determine if pattern changes have occurred, which may be an indication of tampering (e.g. jumpers inserted behind the meter.)

3.2 Alternate Scenario: Meter is removed and not reinstalled

Triggering Event	Primary Actor	Pre-Condition	Post-Condition
(Identify the name of the event that start the scenario)	*(Identify the actor whose point-of-view is primarily used to describe the steps)*	*(Identify any pre-conditions or actor states necessary for the scenario to start)*	*(Identify the post-conditions or significant results required to consider the scenario complete)*
Meter is removed	Ami Back Office System	Meter is removed per Scenario 3.1, steps 1 thru 4	Meter is not re-installed

3.2.1 Steps for this scenario

Describe the normal sequence of events that is required to complete the scenario.

Step #	Actor	Description of the Step	Additional Notes
#	*What actor, either primary or secondary is responsible for the activity in this step?*	*Describe the actions that take place in this step. The step should be described in active, present tense.*	*Elaborate on any additional description or value of the step to help support the descriptions. Short notes on architecture challenges, etc. may also be noted in this column..*
1	Unknown/Unauthorized person	Scenario 3.1, steps 1 thru 4 complete	It could be that an authorized person removed the meter. The scenario is the same for each.
2	Meter	Meter does not send re-installation event to AMI back office system after reasonable amount of time.	We would expect the meter to be reinstalled within a day or two.
3	AMI Back Office System	Back Office System attempts on demand read and meter does not respond	This step would occur at some predetermined time after the meter removal (e.g.one week later)
4	AMI Back Office System	Back Office System initiates Field Order to investigate condition	

Step #	Actor	Description of the Step	Additional Notes
5	Field Representative	Field Rep investigates condition at customer site.	

3.3 Alternate Scenario: Meter is Inverted

Triggering Event	Primary Actor	Pre-Condition	Post-Condition
(Identify the name of the event that start the scenario)	*(Identify the actor whose point-of-view is primarily used to describe the steps)*	*(Identify any pre-conditions or actor states necessary for the scenario to start)*	*(Identify the post-conditions or significant results required to consider the scenario complete)*
Meter is removed	Ami Back Office System	Meter is removed per Scenario 3.1, steps 1 thru 4	Meter is re-installed upside down

3.3.1 Steps for this scenario

Describe the normal sequence of events that is required to complete the scenario.

Step #	Actor	Description of the Step	Additional Notes
#	*What actor, either primary or secondary is responsible for the activity in this step?*	*Describe the actions that take place in this step. The step should be described in active, present tense.*	*Elaborate on any additional description or value of the step to help support the descriptions. Short notes on architecture challenges, etc. may also be noted in this column..*
1	Unknown/Unauthorized person	Scenario 3.1, steps 1 thru 4 complete	It could be that an authorized person removed the meter. The scenario is the same for each.

Step #	Actor	Description of the Step	Additional Notes
2	Meter	Meter is re-installed in an inverted fashion	We would expect the meter to be reinstalled within a day or two.
3	Meter	Meter sends re-installation event to AMI back office system.	This would allow the utility to immediately investigate the condition.
4	AMI Back Ofice System	Back Office System initiates Field Order to investigate condition	
5	Field Representative	Field Rep investigates condition at customer site.	

3.4 Primary Scenario: Meter bypass detection at meter

Triggering Event	Primary Actor	Pre-Condition	Post-Condition
(Identify the name of the event that start the scenario)	*(Identify the actor whose point-of-view is primarily used to describe the steps)*	*(Identify any pre-conditions or actor states necessary for the scenario to start)*	*(Identify the post-conditions or significant results required to consider the scenario complete)*
Customer bypasses meter	Meter	Customer is disconnected using remote disconnect switch.	Load-side voltage is detected and event successfully sent to AMI back office system

3.4.1 Steps for this scenario

Describe the normal sequence of events that is required to complete the scenario.

Step #	***Actor***	***Description of the Step***	***Additional Notes***
#	*What actor, either primary or secondary is responsible for the activity in this step?*	*Describe the actions that take place in this step. The step should be described in active, present tense.*	*Elaborate on any additional description or value of the step to help support the descriptions. Short notes on architecture challenges, etc. may also be noted in this column..*
1	Customer	Customer is disconnected using remote disconnect switch	
2	Customer	Customer bypasses meter.	This bypass could occur in a variety of ways, such as at the weatherhead or at the service panel.
3	Meter	Meter detects voltage at load side	
4	Meter	Meter generates event.	
5	Meter	Meter records event and sends it to AMI back office system.	
6	AMI Back Office System	Back Office System initiates Field Order to investigate condition	
7	Field Representative	Field Rep investigates condition at customer site.	

3.5 Primary Scenario: Physical tamper detection

Triggering Event	***Primary Actor***	***Pre-Condition***	***Post-Condition***

(Identify the name of the event that start the scenario)	*(Identify the actor whose point-of-view is primarily used to describe the steps)*	*(Identify any pre-conditions or actor states necessary for the scenario to start)*	*(Identify the post-conditions or significant results required to consider the scenario complete)*
Customer invades case	Meter	Customer attempts to tamper with meter by physically breaching the meter case	Meter detects breach and send breach event to utility

3.5.1 Steps for this scenario

Describe the normal sequence of events that is required to complete the scenario.

Step #	***Actor***	***Description of the Step***	***Additional Notes***
#	*What actor, either primary or secondary is responsible for the activity in this step?*	*Describe the actions that take place in this step. The step should be described in active, present tense.*	*Elaborate on any additional description or value of the step to help support the descriptions. Short notes on architecture challenges, etc. may also be noted in this column..*
1	Customer	Customer invades case. • Seal tampering • Case / cover removal	The alternatives in this step, of course, depends on the type of tamper detection present. Fo
2	Meter	Meter detects intrusion	
3	Meter	Meter generates event.	
4	Meter	Meter records event and attempts to send it to the AMI back office system.	
5	AMI Back Office System	Back Office System initiates Field Order to investigate condition	
6	Field Representative	Field Rep investigates condition at customer site.	

4. Requirements

Detail the Functional, Non-functional and Business Requirements generated from the workshop in the tables below. If applicable list the associated use case scenario and step.

4.1 Functional Requirements

Functional Requirements	*Associated Scenario # (if applicable)*	*Associated Step # (if applicable)*
The meter shall have a unique internal and external identity	1	2
The meter shall be able to detect removal from its socket	1	2
The meter shall differentiate between a meter removal event and a power outage event	1 2	0 0
Detection shall be possible after the meter is removed and before it stops communicating by use of communication infrastructure.	1	3
For each tamper event, the meter shall transmit and locally log the following information about the event • Timestamp • Tamper status (event type) • Meter ID	1	3
The meter shall be capable of sending a removal tamper event before communications is interrupted even if power line carrier is used.	1	3,4
The removal tamper event shall be generated and sent upon meter removal	1	3,4
Upon meter re-installation, any unsent tamper events shall be sent including the re-installation event	1	5
An event generated when the meter is reinstalled is different from the event generated if the meter is initially installed (provisioned) or re-energized (e.g. after an outage). This is to avoid transmission of useless information to the enterprise systems because of non tamper related	1	5

Functional Requirements	*Associated Scenario #* *(if applicable)*	*Associated Step #* *(if applicable)*
events		
All tamper related events shall be stored in the meter's event log	1 2	4 5
Tamper events shall be retained in the meter until sent to and received by the MDMS	1 2	4 5
The meter shall be able to detect voltage at the load side when the disconnect switch in the meter is open for the purpose of detecting meter bypass	2	3
Tamper event is always recorded in the meter even if the event has been reported to the AMI Back Office System.	1	4
Tamper event storage shall be long enough for the events to be transferred to the enterprise system in the case that communication with the meter is not possible for a period of time or to be read locally	1	4
Events related to tampering shall not roll off unless flagged for deletion. Tamper events will be flagged for deletion after being transferred to the AMI Back Office System and 45 days have passed.	1	4
Meter shall detect physical tampering, such as, seal tampering, meter removal, meter ring removal, case / cover removal etc and generate a tamper event	3	2
Meter shall detect physical inversion and generate a tamper event	3	2
Meter disconnect switch shall not close when there is voltage on the load side to prevent equipment damage or personal injury	4	3
There shall be a warning message on the meter (engraved, sticker, etc) indicating that the meter is capable of detecting tampering and will report tampering to the utility	1	0

4.2 Non-functional Requirements

Non-Functional Requirements	*Associated Scenario #* *(if applicable)*	*Associated Step #* *(if applicable)*
All tamper related events are created and recorded in the meter as soon as the event occurs	1	3,4
Tamper messages have higher priority than normal status messages	1	3,4
Analysis/comparison of energy theft between the distribution transformer and the customer meter by the enterprise system is done at least monthly	3	3
Tamper events shall be stored for at least 45 days (same as for usage data)	1	4
Interval data shall be stored for at least 45 days	1	0

4.3 Business Requirements

Business Requirement	*Associated Scenario #* *(if applicable)*	*Associated Step #* *(if applicable)*
Storage of tamper events is necessary to investigate, recover revenue, possible prosecution		

5. Use Case Models (optional)

This section is used by the architecture team to detail information exchange, actor interactions and sequence diagrams

5.1 Information Exchange

For each scenario detail the information exchanged in each step

Scenario #	***Step #, Step Name***	***Information Producer***	***Information Receiver***	***Name of information exchanged***
#	*Name of the step for this scenario.*	*What actors are primarily responsible for Producing the information?*	*What actors are primarily responsible for Receiving the information?*	*Describe the information being exchanged*
1	3, Meter sends removal event to AMI back office system.	Meter	AMI Back Office System	Tamper event
1	6, Meter sends re-installation event to AMI back office system.	Meter	AMI Back Office System	Meter re-install event
2	3, Back Office System attempts on demand read and meter does not respond	AMI Back Office System	Meter	On Demand read request
2	3, Back Office System attempts on demand read and meter does not respond	Meter	AMI Back Office System	On Demand read data
2	4, Back Office System initiates Field Order to investigate condition	AMI Back Office System	Field Order system	Field Order
3	3, Meter sends re-installation event to AMI back office system.	Meter	AMI Back Office System	Meter re-install event

Scenario #	Step #, Step Name	Information Producer	Information Receiver	Name of information exchanged
3	4, Back Office System initiates Field Order to investigate condition	AMI Back Office System	Field Order system	Field Order
4	4, Meter records event (voltage on disconnected meter) and sends it to AMI back office system.	Meter	AMI Back Office System	Voltage on disconnected meter event
4	5, Back Office System initiates Field Order to investigate condition	AMI Back Office System	Field Order system	Field Order
5	4, Meter records event and attempts to send it to the AMI back office system.	Meter	AMI Back Office System	Meter intrusion event
5	5, Back Office System initiates Field Order to investigate condition	AMI Back Office System	Field Order system	Field Order

5.2 Diagrams

The architecture team shall use this section to develop an interaction diagram that graphically describes the step-by-step actor-system interactions for all scenarios. The diagrams shall use standard UML notation. Additionally, sequence diagrams may be developed to help describe complex event flows.

6. Use Case Issues

Capture any issues with the use case. Specifically, these are issues that are not resolved and help the use case reader understand the constraints or unresolved factors that have an impact of the use case scenarios and their realization.

Issue
Describe the issue as well as any potential impacts to the use case.
~~Do we have to install lock rings if the meter is smart enough to detect tampering? This will help recover associated costs~~
~~Is there a need to add requirements for a scenario where the neutral is connected to the meter to support possible future changes in building codes, regulations etc?~~
~~Flag for deletion of tamper events in the log~~

7. Glossary

Insert the terms and definitions relevant to this use case. Please ensure that any glossary item added to this list should be included in the global glossary to ensure consistency between use cases.

Glossary	
Term	**Definition**

8. References

Reference any prior work (intellectual property of companies or individuals) used in the preparation of this use case.

9. Bibliography (optional)

Provide a list of related reading, standards, etc. that the use case reader may find helpful.