Attachment 5. Updated Baselining Study #3 for 2013 and First Half of 2014

Baselining Analysis Update 3

Six Months Data (February to July 2014)

Discovery Across Texas Project

Submitted to:
Center for Commercialization of Electric Technologies
Milton L. Holloway, Ph.D.
MHolloway@ElectricTechnologyCenter.com

Submitted By:

John Ballance
Romulo Barreno
Ajay Das
Song Xue

October 24, 2014

Contact Information:
Electric Power Group, LLC
(626) 685-2015
Lupe Garcia, Contracts and Administration
Garcia@electricpowergroup.com

External Report

Table of Contents

TABLES

APPENDICES (attached as separate documents)

A. Voltage Angles, Ref: North 7- Box Whiskers & Time Duration

B. Angles Differences Box Whiskers & Time Duration

C. Comparison of Median Values, 2012 to 2014

D. RTDMS DAILY REPORT Recommendations

1. INTRODUCTION

The Center for Commercialization of Electric Technologies (CCET) was awarded contract DE-OE0000194 by the Department of Energy to perform the Discovery Across Texas demonstration project. Electric Power Group, LLC (EPG) received a subaward from CCET to provide professional services to perform, among other things, a substation cluster analysis, comparison of phasor data versus state estimator data, and voltage and angle difference baselining. In October 2013, EPG completed a Baselining Study update (Update 1) using 2012 and January-June 2013 data that included the following: (1) substations having phasor measurement units (PMUs), which are geographically close to each other were grouped, and a voltage and angle difference analysis for each group (cluster analysis) was performed; (2) performed a comparison of voltage and angle differences obtained using phasor measurements versus similar results using state estimator data (phasor vs. state estimator comparison); and, (3) performed a baseline analysis for voltages and angle differences for selected pairs of substations. Alarm limits were established and documented based on the baseline analysis.

Twenty-eight new Competitive Renewable Energy Zone (CREZ) 345 kV lines were added to the Electric Reliability Council of Texas (ERCOT) system in 2013, which will change the results obtained with the 2012 data, and the first six-months of 2013 data, particularly in angle differences between locations. Nineteen of these lines were added in the second half of 2013. Since many CREZ lines were added in late 2013, the analysis results were still subject to change since the system configuration continued changing, and so did the voltage angles and angle differences.

In June 2014, Baselining Update 2 was completed using data for the full 12 months of 2013. The Update 2 report provided results that tracked the changes in voltage magnitudes and in voltage angle differences caused by the twenty-eight new 345 kV lines added to the ERCOT system throughout 2013.The Update 2 report shows how the angle differences were changing as CREZ lines were being added to the ERCOT system. In general, results shown in the Baselining Study Update 2 report indicated that the angle differences for 2013 were smaller (representing a tighter electrical grid) than those found with 2012 state estimator and phasor data. Alarm limits were developed and proposed in that report. However those alarm limits were expected to change because they were based on data obtained under continued changing system conditions, since new CREZ lines were being added month-by-month all the way to December 2013.

An additional seven CREZ lines were added during the first quarter of 2014. By the end of March 2014, all planned CREZ lines had been added to the ERCOT system and, by the end of July 2014, the ERCOT system has been operating with all these lines in service for 4 months. This Baselining Analysis Update 3, performed using data for the February to July, 2014 period, provides results that capture the effect of all the CREZ lines added to the ERCOT system. This Update was performed only for angle differences. Alarm limits for angle differences obtained in this Update 3 will reflect conditions that are not expected to change significantly in the foreseeable future since all the CREZ lines have been in service for several months and, therefore, can be used by operators in real-time monitoring of the ERCOT system. These alarm limits may need to be revised if major changes in transmission infrastructure, or major shifts in generation patterns, occur.

2. PROJECT SCOPE

A. Baseline Analysis for Voltage and Angle Differences

This study update analyzed the performance of the ERCOT grid using State Estimator data, plus phasor data, for the February to July 2014 period, to identify normal and abnormal voltage angle limits across the grid. In this analysis, EPG also compared the results obtained using 7 months of 2014 data with those obtained using 2013 and 2012 data, and summarized the differences, if any, due to addition of the 345 kV lines added in 2014. Activities performed as part of this Update 3:

1. Extracted key metric information (i.e., angles and angle differences).
2. Analyzed extracted data and developed baseline understanding of voltage phase angle, and angle difference patterns, for key pairs of substations similar to those used in Update 2.
3. Monitored angle differences (pairs), and developed patterns and statistics in the form of box-whisker plots and load duration curves. Substations selected for analysis of angle differences are listed in Table 3 below.
4. Prepared baselining analysis results for the selected pair of substations as Excel spreadsheet and charts, including:
   a. Voltage phase angle difference statistics (mean, maximum and minimum).
   b. Voltage and phase angle distribution functions.
5. Developed a comparison table to show the difference in results for voltages and angle differences using 2012, 2013, and the 6-months of 2014 data.
6. Prepared baselining analysis summary for discussion with ERCOT and the Synchrophasor Team.

B. Establishing Alarm Limits for Use in Operations

Based on this Baselining Analysis Update 3, EPG prepared a list of key angle pairs for monitoring in Real Time Dynamics Monitoring System[1] (RTDMS®), and voltage angle and angle difference alarm settings for use in RTDMS® to alert operators when grid critical variables are approaching limits.

As requested by ERCOT, EPG has conducted a Baselining Analysis Update 3 using data for the months of February to July 2014. No SE data was available for the month of January. Please note that a few CREZ 345 kV lines were added in January 2014, and a few more in late March 2014.

Final voltage and angle difference limits for use by operators should be reviewed with data collected for all 12 months of 2014. The ERCOT system will have no new CREZ lines added to it after March 2014, and the angle difference ranges should be more stable, resulting in a more current and accurate set of alarm limits.

[1] ® Electric Power Group. Built upon GRID-3P platform, US Patent 7,233,843, US Patent 8,060259, and US Patent 8,401,710.

3. DATA SOURCES

Two sources of data were utilized to perform the study update analysis of voltage and angle differences in the ERCOT network: phasor data and state estimator cases. A description of these sources of data is provided below. In-service dates for the new CREZ lines were also obtained from transmission owners and from ERCOT.

A. CREZ Lines Added to the ERCOT System

Table 1 below shows all the CREZ lines added to the ERCOT system during 2012, 2013, and 2014.

B. Phasor Data

ERCOT provided EPG with phasor data for the February to July 2014 period with a resolution of 30 samples per second (SPS). Through an automated process, EPG downloaded, cleaned, and filtered data dropout to make it suitable for analysis. Further manual cleaning was necessary to weed out remaining outliers.

After the data was extracted and pre-processed, another program, developed by EPG, was used to extract the information and compile it into a summary table, and two series of graphs. One graph (box-whisker) shows daily summaries of data, and the other, time duration curves, shows values versus percent time for each study variable. The time duration curves were used to obtain the metric values corresponding to 1% and 99% exceedance (the value which was less than 1% plus inflection or greater than 99% minus inflection).

Phasor Measurement Units (PMUs) Installed in the ERCOT System

As of May 27, 2014, there were 69 PMUs installed in 31 locations across the ERCOT service area. Table 2 below shows the 31 substations equipped with PMUs.

The Baselining Study Update 3 was completed using February to July, 2014, data which included state estimator data for locations for which PMUs are installed, or for which PMUs are planned.

Table 1 - CREZ 345 kV lines added to the ERCOT system as of April 14, 2014

Table 1: CREZ 345 Lines added to the ERCOT system as of April 14, 2014 (Subject to Confirmation by ERCOT)				
	FROM	TO	VOLTAGE	IN-SERVICE DATES
Year 2012				
1	West 2	West 23	345	February 10, 2012.
2	West 18	West 1	345	June 15, 2012.
3	West 23	West 1	345	June 16, 2012.
4	West 1	West 24	345	December 31, 2012.
5	West 24	North 7	345	December 31, 2012.
Year 2013				
1	South 9	South 16	345	February 27, 2013.
2	West 12	West 21	345	March 6, 2013.
3	North 9	North 8	345	March 21, 2013.
4	West 21	North 8	345	March 24, 2013.
5	West 19	West 9	345	April 15, 2013.
6	West 13	West 19	345	April 29, 2013.
7	West 18	West 8	345	May 23, 2013.
8	West 22	North 11	345	June 30, 2013.
9	West 14	North 10	345	June 30, 2013.
10	West 14	West 16	345	July 31, 2013.
11	West 15	West 14	345	August 13, 2013.
12	West 25	West 15	345	August 15, 2013.
13	West 15	West 16	345	August 15, 2013.
14	West 13	West 19	345	August 19, 2013.
15	West 26	West 13	345	August 21, 2013.
16	West 26	West 17	345	August 21, 2013.
17	West 17	West 27	345	August 21, 2013.
18	FarWest 10	West 8	345	August 31, 2013.
19	West 8	South 9	345	September 5, 2013.
20	West 13	West 15	345	September 18, 2013.
21	West 25	West 27	345	September 25, 2013.
22	West 12	FarWest 11	345	September 30, 2013.
23	West 3	West 9	345	November 6, 2013.
24	West 16	West 3	345	November 7, 2013.
25	West 27	West 13	345	November 15, 2013.
26	North 10	North 11	345	December 5, 2013.
27	West 3	West 21	345	December 18, 2013.
28	West 3	West 22	345	December 19, 2013.
Year 2014				
1	FarWest 12	FarWest 7	345	January 3. 2014.
2	FarWest 10	FarWest 12	345	January 3. 2014.
3	West 16	West 19	345	January 18. 2014.
4	FarWest 11	FarWest 13	345	March 22. 2014.
5	FarWest 13	FarWest 7	345	March 22. 2014.
6	FarWest 11	FarWest 14	345	March 22. 2014.
7	FarWest 14	West 28	345	March 22. 2014.

Table 2 - List of Substations with PMUs Currently Connected to the ERCOT Grid, as of May27, 2014

TABLE 2 - List of Substations with PMUs Currently Connected to the ERCOT Grid as of May 27, 2014

#	Company	PMU Name	PMU Name in D. Base	Name of the Station where PMU is located	Date–data stream connected to ERCOT	Enabled	Base kV
1	AEP	Line_1	Line_1@ West 14	West 14	7/25/2012	Yes	345
2	AEP	Line_3	Line_3@West_4	West 4	7/2/2012	Yes	138
3	AEP	Line_1	Line_1	Coast 3	4/30/2012	Yes	345
4	AEP	Line_1	Line_1	Coast 4	3/26/2012	Yes	345
5	AEP	Line_1	Line_1@Coast_1	Coast 1	1/23/2012	Yes	138
6	AEP	Line_1	Line_1@FarWest_9	FarWest 9	3/26/2012	Yes	138
7	AEP	Line_1	Line_1	West 10	8/1/2008.	Yes	69
8	AEP	Line_1	Line_1	West 15	9/16/2013	Yes	345
9	AEP	Line_1	Line_1	West 16	12/19/2013	Yes	345
10	AEP	Line_1*	Line_2@West_3	West 3	12/19/2013	Yes	345
11	AEP	Line_1	Line_1	Coast 2	?/2012	Yes	69
12	AEP	Line_1	Line_1@FarWest 2	FarWest 2	6/21/2013	Yes	69
13	AEP	Line_1	Line_1@South_3	South 3	6/21/2013	Yes	138
14	AEP	Line_1	Line_1@South_5	South 5	6/21/2013	Yes	69
15	AEP	Line_1	Line_1@West_7	West 7	6/21/2013	Yes	138
16	ONCOR	Line_1	Line_1	North 4	10/20/2010	Yes	138
17	ONCOR	Line_1	Line_1	North 5	10/20/2010	Yes	138
18	ONCOR	Line_1	Line_1	North 6	10/20/2010	Yes	138
19	ONCOR	Line_1	Line_1	North 7	10/20/2010	Yes	138
20	ONCOR	Line_1	Line_1	FarWest 4	10/20/2010	Yes	345
21	ONCOR	Line_1	Line_1	West 11	3/9/2012	Yes	345
22	ONCOR	Line_1	Line_1	FarWest 7	10/20/2010	Yes	345
23	ONCOR	Line_1	Line_1	FarWest 8	3/9/2012	Yes	138
24	ONCOR	Line_1	Line_1	West 6	10/20/2010	Yes	345
25	ONCOR	Line_1	Line_1	North 1	11/28/2012	Yes	345
26	ONCOR	Line_1	Line_1	West 9	6/21/2013	Yes	345
27	ONCOR	Line_1	Line_1	West 12	6/21/2013	Yes	345
28	ONCOR	Line_1	Line_1	West 5	6/21/2013	Yes	345
29	ONCOR	Line_1	Line_1	West 2	6/21/2013	Yes	345
30	ONCOR	Line_1	Line_1	West 1	6/21/2013	Yes	345
31	SHARYLAND	Line_3	Line_3@South 13	South 13	8/10/2012	Yes	138
	Note: *	Means new substations with PMU connected to ERCOT grid					

C. State Estimator (SE) Data

ERCOT provided EPG with SE data for the February to July months of 2014. EPG used the PowerWorld simulator, provided by ERCOT via PowerWorld, to extract approximately 25,419 SE cases. There was only one day, May 6, for which SE data was not available. This high-level of SE data availability in 2014 was a significant improvement over 2013.

D. Data Availability

Data availability for the phasor data sources varied from substation to substation; the summary table of phasor-based results shows the percent availability for each substation, or each pair, analyzed. As shown inTable A-1, availability ranges from less than 20%, for FarWest 2 and Coast 2, to greater than 90% for eighteen PMUs. The remaining ten PMUs have availability ranging

from 62.08% (Coast 4) to 89.06% (Coast 1). Box-whisker plots in Appendix A provide a view of data availability on a day-by-day basis.

Below is a summary of phasor data availability from Table A-1 for 2012, 2013, and 2014 (six months):

2014

<20%	**20% to 60%**	**61% to 90%**	**>90%**
Coast 2	None	Coast 1	West 10
FarWest 2		West 4	West 11
		West 14	South 3
		Coast 4	South 5
		Coast 3	West 1
		South 13	West 2
		FarWest 9	West 9
		West 16	West 12
		West 3	West 5
		West 15	West 6
			North 1
			North 4
			North 5
			North 6
			FarWest 4
			FarWest 7
			FarWest 8
			North 7

2013

<20%	**20% to 60%**	**61% to 80%**	**>80%**
West 16	West 1	West 14	West 10
West 3	West 2	West 4	West 11
West 15	West 9	Coast 4	West 6
	West 12	Coast 3	North 1
	West 5		North 4
	FarWest 2		North 5
	South 3		North 6
	South 5		North 7
			Coast 2
			Coast 1
			South 13
			FarWest 4
			FarWest 7
			FarWest 8
			FarWest 9

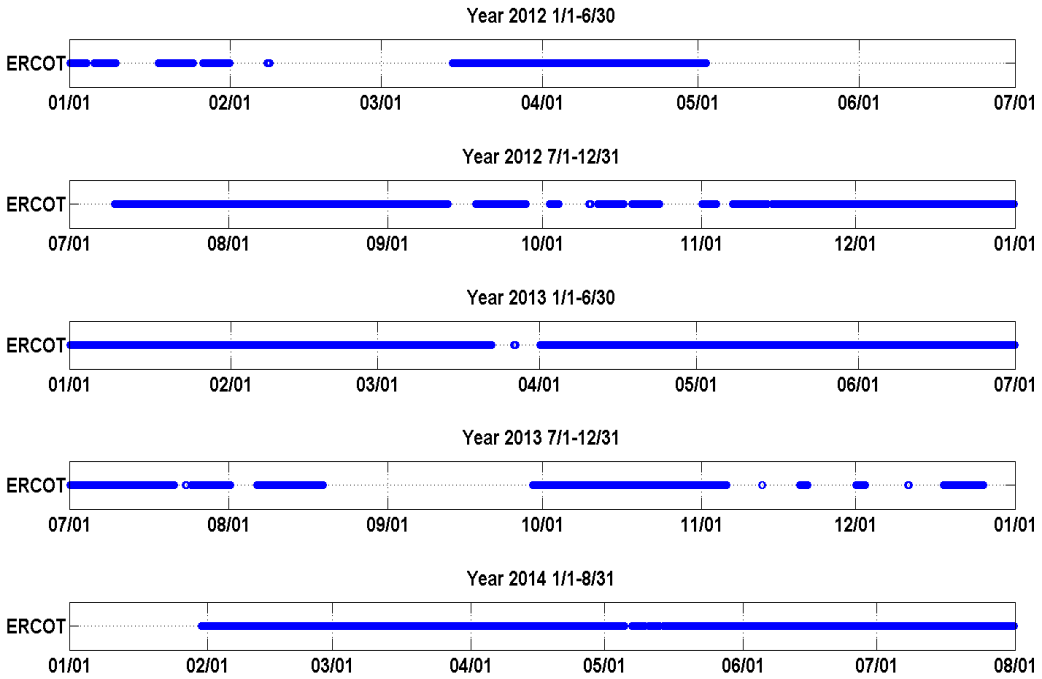
2012

<40%	**41% to 60%**	**61% to 80%**	**>80%**
	West 4	West 11	West 10
West 14			
North 1	Coast 4	Coast 1	North 7
Coast 2	Coast 3	FarWest 8	North 2
South 6	South 13		North 4
FarWest 7	FarWest 9		North 5
			West 6
			North 6
			FarWest 4

For SE data availability, ERCOT produces state estimator cases every 5 minutes for a total of 52,218 possible cases for the February to July months. ERCOT provided SE data at a rate of six cases per hour. The total possible number of cases at this rate for the February to July period is 26,064. EPG received 25,419 cases, which means the availability of SE data for these 6 months was approximately 97.5 %. State Estimator data availability has significantly improved during this six-month period.

The graph below shows ERCOT SE data availability since January 1, 2012 until July 31, 2014.

ERCOT SE Data Availability



4. METHODOLOGY FOR BASELINE ANALYSIS FOR VOLTAGE ANGLES

This baseline analysis update for voltage angle was performed using the phasor data and state estimator data obtained from ERCOT for six months of 2014 (February to July). This data was processed to extract voltage angles. Minimum and maximum values for these variables were documented in summary tables; box-whisker plots and time duration curves were developed for each variable, and for each type of data used. Below is an analysis of voltage angles.

For the substation pairs selected for study, the following work was performed:

1. Obtained and processed phasor data and state estimator data.
2. Identified the substations for which phasor data is available and for which PMUs are planned.
3. Selected angle pairs of interest to ERCOT and the synchrophasor team members by choosing substations that have, or soon will have, PMUs installed.
4. Extracted information to identify max, min, and average values from these data sources. Prepared summary tables for the selected pairs showing results of all data, including data saved during events.
5. Developed statistical charts, including time duration curve and box-whisker graphs, for voltage angle pairs.
6. Identified limits corresponding to normal operation, excluding events and outages. To exclude extreme values corresponding to outliers and to events, values corresponding to the metrics within the 1% to 99% percent of the time range were identified as normal operating limits.
7. Performed statistical analyses to identify angle differences limits for the selected pairs under all conditions. Summarized angle difference limits.
   - Established limits for normal operation based on the criteria described in the corresponding methodology. Summarized angle difference limits.
   - The limits for angle differences identified in this report shall be compared with ERCOT's criteria, if any, that apply to angle differences for the paths selected for this study.
8. Analyzed results, identified limits, and reported results for each pair selected.

5. BASELINE ANALYSIS FOR VOLTAGE ANGLES (REFERENCE: NORTH 7)

A. Substations Identified for Voltage Angle Analysis

The following substations were selected for voltage angle analysis, and the North 7 substation was selected as a common reference.

Table 3 - Substations for Voltage Angle Difference Monitoring

Table 3 - SUBSTATIONS FOR VOLTAGE ANGLE DIFFERENCE MONITORING (Reference: North 7)			
#	SUBSTATION	kV	REGION
1	West 10	69	Panhandle
2	West 14	345	Panhandle
3	West 1	345	Central
4	West 2	345	Central
5	West 9	345	Central
6	West 11	345	Central
7	West 12	345	Central
8	West 5	345	Central
9	West 6	345	Central
10	North 1	345	Dallas
11	North 4	138	Dallas
12	North 5	138	Dallas
13	North 6	138	East
14	FarWest 2	69	West Texas
15	West 4	138	SouthWest
16	Coast 2	69	Valley
17	Coast 1	138	Valley
18	South 3	138	Valley
19	South 5	138	Valley
20	Coast 4	345	Valley
21	Coast 3	345	Valley
22	South 13	138	Valley
23	FarWest 4	345	West Texas
24	FarWest 7	345	West Texas
25	FarWest 8	138	West Texas
26	FarWest 9	138	West Texas
27	West 16	345	Panhandle
28	West 3	345	Central
29	West 15	345	Panhandle
30	West 8*	345	Central
31	South 15	345	Central
32	South 2*	345	Central-East
33	South 4*	345	Central-East
34	South 7*	345	Central-East
35	South 9*	345	Central-East
36	South 11*	345	Central-East
37	South 10*	138	Valley
38	West 17*	345	Panhandle
39	West 13*	345	Panhandle
NOTE:	* Means substations without PMUs connected to ERCOT		

B. Summary of Results - All Data Included

The voltage angle results obtained from all solved SE cases, and all phasor data, are summarized in Table A-1 below.

These results were obtained using all data available, including event and outage conditions. Under these conditions, voltage angles would be expected to be larger than under normal conditions because, during event and outage conditions, the angle spreads tend to increase in absolute magnitude to reflect the changes in system conditions, or changes in system configuration. The maximum Max-Min spreads observed were 91.4 degrees for South 13 138 kV substation and 81.5 degrees for Coast 4 345 kV substation. The lowest spread of 19.5 degrees was seen at North 6. The angles for North 1 and North 6 were positive most of the time (93.5 and 78.8%, respectively), whereas North 4, North 5, West 4, and South 5 substations were positive less than 20% of the time; that is, the power flows from North 7 to these substations most of the time.

As expected, the Max-Min spreads from this update are smaller than those Max-Min spreads found in the 2013 baselining study, particularly for those substations in the western and Panhandle areas of Texas.

The phasor data for FarWest 2 appears to be unreliable given the inconsistent results (average of -130.2 degrees). The SE data for this substation seems reasonable.

Table A- 1 - Baselining Analysis – Voltage Angles – ALL Conditions

Table A-1: CCET DISCOVERY ACROSS TEXAS- BASELINING ANALYSIS - VOLTAGE ANGLES - ALL CONDITIONS
(Reference: North 7)

			Phasor Data - 2/1/2014 to 7/31/2014						State Estimator Data - 2/1/2014 to				
No	Angle Pair FROM - TO	Base kV	Min	Max	Average	Percent Positive	Max-Min Spread	% Data Availabl e	Min	Max	Average	Percent Positive	Max-Min Spread
1	West 10	69	-27.17	38.37	5.05	57.90	65.54	94.42	-26.56	37.13	4.63	56.53%	63.7
2	West 14	345	-18.62	19.39	3.32	72.36	38.01	75.78	-17.29	16.95	3.13	71.31%	34.2
3	West 1	345	-27.01	33.17	2.98	67.87	60.17	95.27	-10.60	16.71	2.88	67.11%	27.3
4	West 2	345	-15.54	22.72	3.70	64.06	38.25	96.31	-15.43	22.63	3.59	63.29%	38.1
5	West 9	345	-16.46	21.38	3.49	66.30	37.84	96.24	-16.34	21.45	3.49	65.66%	37.8
6	West 11	345	-18.16	26.39	3.59	60.44	44.55	92.55	-18.18	26.06	3.26	58.77%	44.2
7	West 12	345	-16.91	22.19	3.57	64.33	39.10	96.26	-16.83	22.41	3.56	63.63%	39.2
8	West 5	345	-16.73	23.95	3.97	64.32	40.67	96.16	-16.71	25.08	3.95	63.35%	41.8
9	West 6	345	-16.91	23.88	4.08	64.88	40.79	96.07	-17.02	23.82	3.86	63.41%	40.8
10	North 1	345	-11.21	16.64	5.56	93.32	27.85	96.14	-8.17	16.09	5.47	93.52%	24.3
11	North 4	138	-17.64	8.28	-3.88	11.70	25.92	96.21	-16.45	7.56	-3.50	13.06%	24.0
12	North 5	138	-21.82	10.06	-5.54	8.78	31.87	95.74	-20.90	8.89	-5.70	7.95%	29.8
13	North 6	138	-6.82	14.70	3.65	84.01	21.52	96.26	-6.15	13.30	2.82	78.81%	19.5
14	FarWest 2	69	-162.27	-90.41	-130.15	0.00	71.86	14.32	-21.25	9.01	-9.14	4.44%	30.3
15	West 4	138	-31.82	16.98	-6.27	17.11	48.80	88.34	-31.28	14.83	-6.70	14.97%	46.1
16	Coast 2	69	-24.78	20.95	-3.25	30.05	45.73	11.58	-31.62	24.32	-7.12	17.68%	55.9
17	Coast 1	138	-32.87	59.15	1.64	54.51	92.02	89.06	-31.69	45.22	1.08	52.67%	76.9
18	South 3	138	-44.24	44.77	0.58	51.79	89.01	90.82	-26.06	34.32	0.36	50.96%	60.4
19	South 5	138	-29.91	16.90	-7.46	10.45	46.80	92.41	-24.51	11.25	-7.31	12.83%	35.8
20	Coast 4	345	-33.74	51.82	5.15	63.02	85.55	62.08	-32.03	49.50	4.91	62.89%	81.5
21	Coast 3	345	-33.02	55.99	5.09	63.40	89.01	86.18	-32.03	49.03	4.58	62.21%	81.1
22	South 13	138	-42.85	48.42	-0.16	47.27	91.27	69.34	-44.63	47.00	-0.70	46.41%	91.6
23	FarWest 4	345	-19.45	29.63	3.87	59.46	49.08	96.06	-19.36	29.19	3.64	58.50%	48.6
24	FarWest 7	345	-24.48	28.17	1.05	51.98	52.65	95.91	-24.59	27.81	0.91	51.01%	52.4
25	FarWest 8	138	-35.13	20.96	-8.52	22.22	56.08	91.49	-34.23	21.16	-7.71	25.13%	55.4
26	FarWest 9	138	-25.35	31.81	1.19	51.54	57.16	75.44	-23.43	31.27	0.45	49.30%	54.7
27	West 16	345	-17.80	20.70	3.29	71.38	38.50	72.64	-17.01	17.50	3.36	70.95%	34.5
28	West 3	345	-14.90	16.41	3.45	73.71	31.31	83.88	-14.46	16.13	3.14	71.38%	30.6
29	West 15	345	-17.06	19.70	3.61	73.17	36.76	72.06	-16.92	18.22	3.55	71.36%	35.1
30	West 8*	345/138	No phasor data available for these substations for the study period (2/1 to 7/1/2014)						-13.59	25.61	2.05	57.60%	39.2
31	South 15	345/138							-7.71	15.46	1.43	62.28%	23.2
32	South 2*	345/138							-5.59	16.26	2.91	79.51%	21.9
33	South 4*	345/138							-8.57	16.91	1.54	61.77%	25.5
34	South 7*	345/138							-14.89	22.14	3.93	78.18%	37.0
35	South 9*	345/138							-10.29	11.74	1.06	63.08%	22.0
36	South 11*	345/138							-9.77	18.16	1.41	59.32%	27.9
37	South 10*	138							-34.29	24.01	-7.19	16.84%	58.3
38	West 17*	345/138							-16.73	19.66	4.04	71.99%	36.4
39	West 13*	345/138							-16.81	18.80	3.71	70.67%	35.6

NOTE: * Means substations without PMUs connected to ERCOTb July 31, 2014; no phasor data available

C. Summary of Results – Normal Conditions (Events and Outages Excluded)

The voltage angle results obtained from excluding extreme values based on analysis of the box-whisker plots and time duration curves are shown in Table A- 2 below.

Summaries of voltage angle pairs with their corresponding box-whisker and time duration curves based on state estimator data, and based on phasor data, are presented in Appendix A, Parts 1 and 2.

NOTE: Phasor data availability for FarWest 2 and Coast 2 was less than 15% for the study period; all other substations had data availability greater than 60%.

Table A- 2 - Baselining Analysis Update – Voltage Angles – Normal Conditions (Ref: 138 kV North 7)

Table A-2 - CCET DISCOVERY ACROSS TEXAS- BASELINING ANALYSIS - VOLTAGE ANGLES - NORMAL CONDITIONS (Reference: 138 kV North 7)

			Phasor Data			State Estimator Data - 2/1/14 to 7/31/14									SE Data-Normal		
No	Angle Pair FROM - TO	Base kV	Min Angle	Max Angle	Max-Min Spread	Percent Positive	Min Angle at POI or 100%	Percent (POI or 100%)	Min Angle at 99% or POI - 1%	Percent (99% or POI - 1%)	Max Angle at 1% or POI +1%	Percent (1% or POI +1%)	Max Angle at POI or 0%	Percent (POI or 0%)	Min Angle	Max Angle	Max-Min Spread
1	West 10	69/138	-26.42	35.08	61.50	56.53%	-26.33	99.98%	-22.65	98.98%	33.15	1.05%	35.22	0.05%	-26.33	35.22	61.6
2	West 14	345/138	-13.28	16.14	29.42	71.31%	-16.60	99.97%	-9.48	98.97%	13.90	1.02%	16.61	0.02%	-16.60	16.61	33.2
3	West 1	345/138	-10.38	16.58	26.96	67.11%	-9.26	99.94%	-7.01	98.94%	13.04	1.03%	15.89	0.03%	-9.26	15.89	25.1
4	West 2	345/138	-13.48	20.88	34.36	63.29%	-13.63	99.94%	-10.84	98.94%	18.60	1.06%	21.03	0.06%	-13.63	21.03	34.7
5	West 9	345/138	-13.47	19.41	32.88	65.66%	-13.06	99.81%	-10.71	98.81%	17.48	1.03%	20.77	0.03%	-13.06	20.77	33.8
6	West 11	345/138	-15.79	24.26	40.05	58.77%	-16.19	99.93%	-13.50	98.93%	21.03	1.03%	24.20	0.03%	-16.19	24.20	40.4
7	West 12	345/138	-14.21	20.33	34.54	63.63%	-14.63	99.93%	-11.36	98.93%	18.74	1.02%	21.86	0.02%	-14.63	21.86	36.5
8	West 5	345/138	-14.28	21.52	35.80	63.35%	-14.50	99.92%	-11.59	98.92%	21.26	1.02%	24.66	0.02%	-14.50	24.66	39.2
9	West 6	345/138	-14.34	21.84	36.18	63.41%	-14.92	99.94%	-11.68	98.94%	19.90	1.06%	22.51	0.06%	-14.92	22.51	37.4
10	North 1	345/138	-6.67	14.71	21.38	93.52%	-6.78	99.95%	-3.75	98.95%	12.45	1.02%	15.75	0.02%	-6.78	15.75	22.5
11	North 4	138	-15.94	6.11	22.05	13.06%	-16.15	99.98%	-12.88	98.98%	4.41	1.04%	6.79	0.04%	-16.15	6.79	22.9
12	North 5	138	-18.85	8.17	27.02	7.95%	-18.87	99.93%	-15.29	98.93%	4.33	1.04%	7.64	0.04%	-18.87	7.64	26.5
13	North 6	138	-4.95	12.50	17.45	78.81%	-5.91	99.99%	-3.81	98.99%	9.93	1.05%	12.56	0.05%	-5.91	12.56	18.5
14	FarWest 2	69/138	-151.20	-101.40	49.80	4.44%	-21.06	99.98%	-18.19	98.98%	3.80	1.05%	7.55	0.05%	-21.06	7.55	28.6
15	West 4	138	-31.12	13.81	44.93	14.97%	-29.59	99.91%	-23.63	98.91%	9.00	1.08%	12.89	0.08%	-29.59	12.89	42.5
16	Coast 2	69/138	-23.69	19.29	42.98	17.68%	-28.60	99.93%	-23.17	98.93%	14.15	1.05%	23.20	0.05%	-28.60	23.20	51.8
17	Coast 1	138	-28.38	40.80	69.18	52.67%	-29.94	99.98%	-24.09	98.98%	30.94	1.07%	41.21	0.07%	-29.94	41.21	71.2
18	South 3	138	-24.78	27.99	52.77	50.96%	-25.01	99.97%	-19.46	98.97%	22.40	1.08%	31.17	0.08%	-25.01	31.17	56.2
19	South 5	138	-24.90	13.04	37.94	12.83%	-21.72	99.78%	-19.16	98.78%	7.26	1.06%	10.82	0.06%	-21.72	10.82	32.5
20	Coast 4	345/138	-28.96	47.63	76.59	62.89%	-29.09	99.94%	-20.87	98.94%	34.65	1.04%	47.54	0.04%	-29.09	47.54	76.6
21	Coast 3	345/138	-26.38	46.84	73.22	62.21%	-29.06	99.94%	-20.89	98.94%	34.22	1.02%	47.73	0.02%	-29.06	47.73	76.8
22	South 13	138	-31.17	45.74	76.91	46.41%	-40.30	99.94%	-27.59	98.94%	30.63	1.02%	45.16	0.02%	-40.30	45.16	85.5
23	FarWest 4	345/138	-18.25	26.24	44.49	58.50%	-18.25	99.97%	-15.03	98.97%	23.91	1.02%	28.22	0.02%	-18.25	28.22	46.5
24	FarWest 7	345/138	-22.45	23.62	46.07	51.01%	-22.50	99.93%	-18.51	98.93%	20.71	1.05%	24.87	0.05%	-22.50	24.87	47.4
25	FarWest 8	138	-31.51	15.85	47.36	25.13%	-33.09	99.98%	-27.22	98.98%	13.62	1.02%	20.05	0.02%	-33.09	20.05	53.1
26	FarWest 9	138	-22.92	26.28	49.20	49.30%	-22.76	99.98%	-19.42	98.98%	23.22	1.04%	27.32	0.04%	-22.76	27.32	50.1
27	West 16	345	-13.41	16.31	29.72	70.95%	-15.72	99.95%	-9.17	98.95%	14.80	1.02%	17.22	0.02%	-15.72	17.22	32.9
28	West 3	345	-11.29	15.25	26.54	71.38%	-13.80	99.97%	-8.18	98.97%	13.36	1.02%	15.82	0.02%	-13.80	15.82	29.6
29	West 15	345	-13.38	17.43	30.81	71.36%	-13.37	99.88%	-9.12	98.88%	15.60	1.03%	17.87	0.03%	-13.37	17.87	31.2
30	West 8*	345	No phasor data available for these substations			57.60%	-12.53	99.88%	-8.30	98.88%	15.40	1.02%	24.59	0.02%	-12.53	24.59	37.1
31	South 15	345				62.28%	-6.84	99.95%	-5.03	98.95%	12.29	1.02%	15.18	0.02%	-6.84	15.18	22.0
32	South 2*	345				79.51%	-5.17	99.95%	-3.25	98.95%	12.95	1.04%	15.60	0.04%	-5.17	15.60	20.8
33	South 4*	345				61.77%	-6.73	99.84%	-5.45	98.84%	13.29	1.03%	16.40	0.03%	-6.73	16.40	23.1
34	South 7*	345				78.18%	-7.72	99.93%	-4.84	98.93%	17.58	1.06%	21.40	0.06%	-7.72	21.40	29.1
35	South 9*	345				63.08%	-8.06	99.92%	-6.00	98.92%	8.65	1.04%	11.25	0.04%	-8.06	11.25	19.3
36	South 11*	345				59.32%	-8.54	99.95%	-6.36	98.95%	14.18	1.02%	17.66	0.02%	-8.54	17.66	26.2
37	South 10*	138				16.84%	-33.46	99.98%	-24.81	98.98%	13.81	1.02%	23.43	0.02%	-33.46	23.43	56.9
38	West 17*	345				71.99%	-16.10	99.97%	-9.41	98.97%	16.84	1.09%	18.71	0.09%	-16.10	18.71	34.8
39	West 13*	345				70.67%	-14.68	99.92%	-9.42	98.92%	16.21	1.09%	18.09	0.09%	-14.68	18.09	32.8

Note: The substations market with * did not have PMUs installed by July 31, 2014: no phasor data available.

NOTE: the substations noted with a * have no phasor data available.

D. Observations – Normal Conditions

1. Angles and angle spreads from State Estimator data track well with those obtained with phasor data, except for FarWest 2 and Coast 2. Phasor data for these two substations was incomplete or unreliable.

2. Voltage angle fluctuations have been reduced and now they vary over a smaller range. There are only five substations with Max-Min angle spreads of more than 60 degrees. The largest angle variations occurred among the substations in the southern part of the state: South 13 with 85.5 degrees (-40.3 to 45.2 degrees), Coast 3 with 76.8 degrees (-29.1 to 47.7 degrees), Coast 4 with 76.6 degrees (-29.1 to 47.5 degrees), and Coast 1 with 71.2 degrees (-29.9 to 41.2 degrees).
3. Only two substations had a Max-Min angle spread of less than 20 degrees: North 6 (18.5 degrees) and South 9 (19.3 degrees). All other substations have Max-Min spreads in the 21 to 61 degree range.
4. With the addition of the CREZ lines, the voltage angles in the Central and Western part of the state (FarWest 7, West 11, West 6, FarWest 8, FarWest 9, FarWest 4, West 2, West 9, and West 5) varied within a range significantly smaller than in 2013.
5. The four largest normal condition angles in degrees observed were at Coast 3 (47.73), Coast 4 (47.74), South 13 (45.16), and Coast 1 (41.21).
6. The smallest normal condition angles in degrees occurred at South 13 (-40.30) and South 10 (-33.46).

6. COMPARISON OF VOLTAGE ANGLE PAIRS (Reference: North 7) – 2012 vs. 2013 vs. 2014

A. Goal:

EPG performed a comparison of voltage angle pairs for a number of pairs to determine the effect the new CREZ lines had on the performance of the ERCOT grid. The covered period includes the months of February to July for a fair comparison. Following are the results of that comparison.

B. Pairs Selected For Comparison

Sixteen pairs were selected to compare voltage angles between 2012, 2013 and 2014 conditions. They are listed in Table 4 below.

Table 4 - Angle Pairs for Voltage Angle Comparison (Monthly Median for 2012, 2013 and 2014)

TABLE 4: ANGLE PAIRS FOR VOLTAGE ANGLE COMPARISON (Monthly Median for 2012, 2013 and 2014)				
#	Substation A	Substation B	From Region	To Region
1	West 10	North 7	Panhandle	Central-East
2	West 14	North 7	Panhandle	Central-East
3	West 16	North 7	Panhandle	Central-East
4	West 19	North 7	Panhandle	Central-East
5	West 9	North 7	Panhandle	Central-East
6	West 5	North 7	Panhandle	Central-East
7	FarWest 7	North 7	West Texas	Central-East
8	FarWest 7	South 9	West Texas	Central-East
9	West 11	North 7	West Texas	Central-East
10	North 5	North 7	Dallas	Central-East
11	North 6	North 7	East	Central-East
12	Coast 1	North 7	Valley	Central-East
13	South 13	South 11	Valley	Valley
14	West 4	South 11	Valley	Valley
15	FarWest 9	South 11	West Texas	Valley

C. Procedure

This monthly median comparison was completed using median values to avoid, as much as possible, distortions in the comparison. State Estimator data was collected for the February to July months of 2012, 2013, and 2014, and analyzed to produce monthly median comparison values shown in Table 5 below.

Monthly median graphs for each of the 16 pairs are shown in Appendix C for the years 2012, 2013 and the six months of 2014. Box-whisker plots were also developed for each pair using median values, and are also shown in Appendix C.

D. Results

The results of the comparison are shown in Table 5 below.

Table 5 - Voltage Angle Comparison (Monthly Median), 2012, 2013 and 2014

Table 5 - BASELINING ANALYSIS UPDATE #3 - VOLTAGE ANGLE COMPARISON (February to July months) - 2012, 2013, and 2014

#	Angle Pair	2012 Median	2013 Median	2014 Median	2014-2013 Difference
1	West 10-North 7	13.12	9.42	3.29	-6.13
2	West 14-North 7	7.84	8.99	3.36	-5.63
3	West 16-North 7	N/A	N/A	3.51	N/A
4	West 19-North 7	N/A	10.38	3.31	-7.07
5	West 9-North 7	9.90	8.46	3.03	-5.43
6	West 5-North 7	9.45	8.34	3.04	-5.30
7	FarWest 7-North 7	7.61	6.84	0.27	-6.57
8	FarWest 7-South 9	4.18	7.98	-0.08	-8.06
9	West 11-North 7	9.68	8.20	2.33	-5.87
10	North 5-North 7	-1.38	-4.56	-5.96	-1.40
11	North 6-North 7	5.31	3.71	2.84	-0.87
12	Coast 1-North 7	11.21	-0.36	0.90	1.26
13	South 13-South 11	0.62	-3.08	-2.55	0.53
14	West 4-South 11	-9.84	-5.08	-7.95	-2.87
15	FarWest 9-South 11	3.53	5.00	-1.32	-6.32
16	South 11-North 7	3.83	-1.04	0.93	1.97

E. Review of Results in Table 5 Shows the Following:

i. All pairs in the list, except Coast 1 and North 5 to North 7, West 4 to South 11, and South 11 to North 7, had a decrease in monthly angle median.

ii. Nine pairs, all located in either west Texas or the Panhandle area, had a decrease in angle from 2013 to 2014, between 5.30 to 8.06 degrees. The largest difference of 8.06 degrees occurred on the FarWest 7 to South 9 pair. NOTE: 22 new CREZ lines were added to the ERCOT system between July 31, 2013 and January 18, 2014. All these lines were added in the Central, Western, and Panhandle areas of Texas.

iii. North 6 seems to be delivering less power to North 7, in 2014 than in 2013, since the median voltage angle went down 0.87 degrees.

iv. The North 5 and West 4 to North 7 pairs had their voltage angle go more negative; North 5 and West 4 appear to be drawing power from North 7 more often.

v. On the other hand, the voltage angle median for Coast 1 to North 7 increased by 1.26 degrees and, it seems, Coast 1 delivered power to North 7 in 2014 more days than it received.

vi. The South 13 to North 7 pair had their voltage angle go less negative; South 13 appears to be drawing less power from North 7.

F. Conclusions

i. The voltage angles for substations in west Texas and the Panhandle area have tightened (smaller angles referenced to North 7) significantly due to the addition, during the second half of 2013 and January of 2014, of 22 new CREZ lines between these substations and the central area of Texas.
ii. A re-distribution of power has occurred among the several transmission lines in the Valley area of Texas.
iii. These voltage angle monthly medians are likely to change less in the future, unless a significant amount of wind power is added in the western area and the Panhandle areas of Texas, displacing generation in other areas, such as the Valley area.
iv. The new CREZ lines, added in March 2014, are not expected to result in any major changes in voltage angle monthly medians.

7. BASELINE ANALYSIS FOR ANGLE DIFFERENCES

A. Pairs of Substations Identified for Angle Difference Analysis

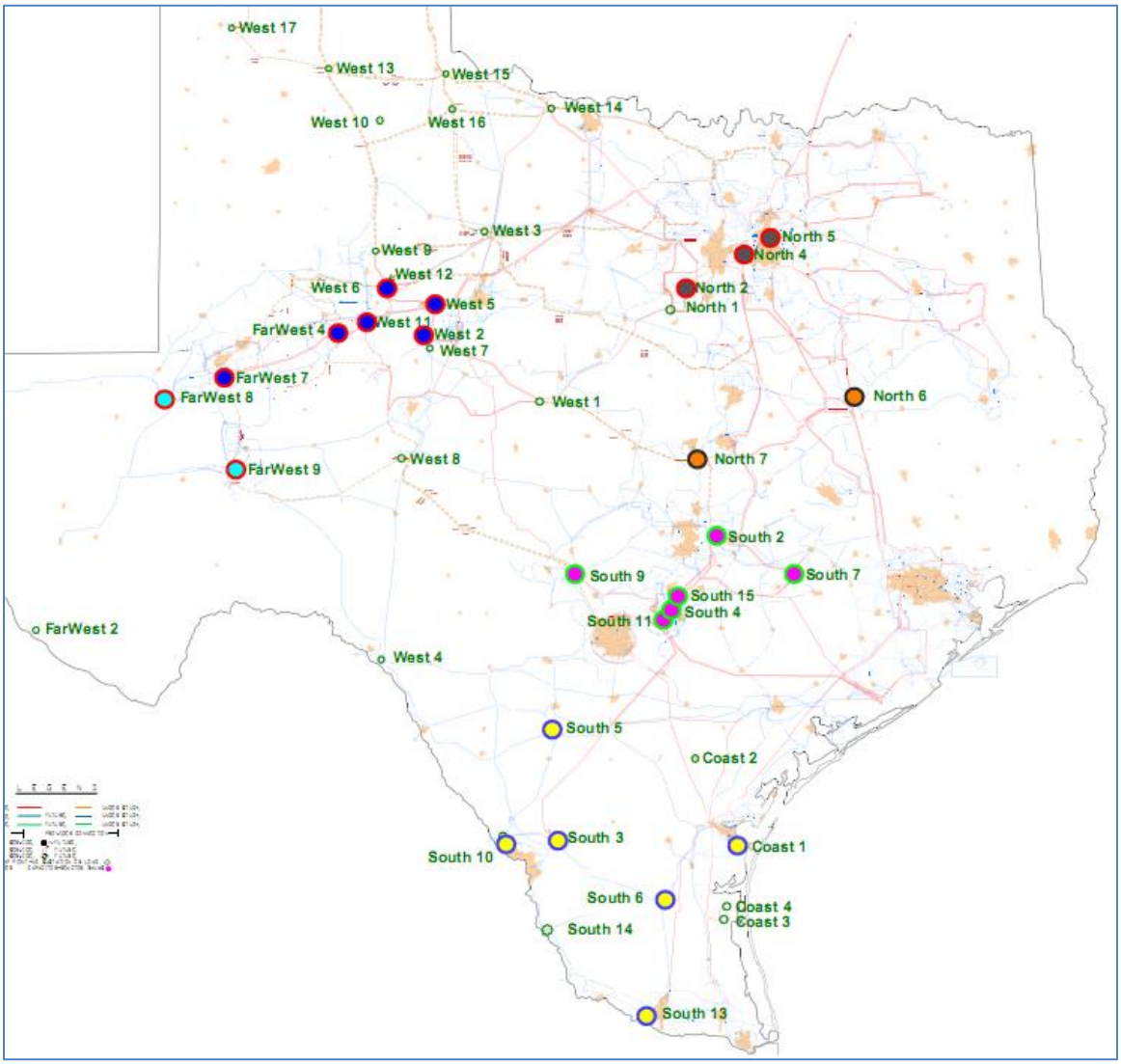
The following pairs of substations were selected to perform analysis of angle difference (also see map below):

Table 6 - Angle Pairs for Angle Differences Analysis Update 3

TABLE 6: ANGLE PAIRS FOR ANGLE DIFFERENCES ANALYSIS UPDATE #3				
PAIRS WITH PHASOR DATA AVAILABLE				
#	Substation A	Substation B	From Region	To Region
1	Coast 1	South 13	Valley	Valley
2	West 5	West 10	Central	Panhandle
3	West 5	FarWest 4	Central	West Texas
4	West 5	North 1	Central	Central
5	North 1	North 4	Dallas	Central
6	North 4	North 6	Central	East
7	FarWest 7	FarWest 4	West Texas	West Texas
8	FarWest 7	West 14	West Texas	Panhandle
9	FarWest 7	FarWest 8	West Texas	West Texas
10	FarWest 7	FarWest 9	West Texas	West Texas
11	West 12	FarWest 7	Central	West Texas
12	West 12	West 1	Central	Central-East
13	West 12	North 1	Central	Dallas
14	West 14	West 5	Panhandle	Central
15	West 14	North 1	Panhandle	Dallas
16	FarWest 9	West 4	West Texas	Southwest
17	West 16	West 3	Panhandle	Panhandle

18	West 16	West 14	Panhandle	Panhandle
19	West 15	West 14	Panhandle	Panhandle
	PAIRS WITHOUT PHASOR DATA AVAILABLE			
20	Coast 1	South 10*	Valley	Valley
21	South 3	South 11*	Valley	Central-East
22	South 11*	North 7	Valley	Central-East
23	North 7	South 7*	Central-East	Central-East
24	North 7	South 9*	Central-East	Central-East
25	West 11	West 8*	Central	Central
26	West 8	South 9*	Central	Central-East
27	FarWest 7	South 9*	West Texas	Central-East
28	FarWest 9	South 9*	West Texas	Central-East
29	West 19*	West 9	Panhandle	Panhandle

* Denotes substations without existing PMUs or w/o phasor data stream



B. Summary of Results – All Data Included

Table B-1 below contains angle difference results for all those angle pairs selected for study. Nineteen pairs with phasor data were included in the analysis (total of 29). Table B-1 shows min, max, and average values for angle differences obtained from all data received for the period of February to July, 2014 (all solved SE cases and all phasor data, normal and contingency conditions). Phasor data was not available for seven of the pairs selected for study; no phasor results are provided for those pairs.

NOTE: Phasor data availability for FarWest 2 and Coast 2 was less than 15% for the study period; all others had data availability greater than 60%. State Estimator data availability was very good for this period, with only one day of data missing.

Observation of Table B-1 results shows the following:

1. The highest Max-Min angle spread occurred at FarWest 9-South 9 (63.0 degrees).

2. Five pairs have spreads between 40 and 60 degrees: Coast 1-South 13, FarWest 9-West 4, Coast 1-South 10, West 8-South 9, and FarWest 7-South 9.
3. Max-Min angle spreads of less than 10 degrees occurred on four pairs: West 16-West 3, West 16-West 14, West 15-West 14, and West 19-West 9.
4. The remaining nineteen pairs have angle spreads between 11.2 and 39.9 degrees.
5. Angle spreads for the February-July, 2014 period are lower than those found for the same period in 2013, due to the addition of the CREZ lines to the ERCOT system.
6. The maximum voltage angle found in this update was 39.8 degrees on the Coast 1-South 10 pair.
7. Only two pairs have minimum voltage angles lower than -25 degrees: FarWest 7-South 9 (-28.73 degrees) and FarWest 9-South 9 (-29.98 degrees).

Table B- 1 - Baselining Analysis – Summary of Angle Differences – All Data

Table B-1 -CCET DISCOVERY ACROSS TEXAS- BASELINING ANALYSIS- SUMMARY OF ANGLE DIFFERENCES ALL DATA

			Phasor Data - 2/1/2014 to 7/31/2014					State Estimator Data - 2/1/2014 to				
	Angle Pair	Base kV	Min	Max	Max-Min	Percent Positive	% Data Available	Min	Max	Average	Percent Positive	Max-Min
1	Coast 1-South 13	138kV	-19.61	29.53	49.13	57.18	64.41	-18.05	25.38	1.95	58.7%	43.4
2	West 5-West 10	345/69kV	-18.11	17.25	35.36	49.13	94.22	-17.37	16.79	-0.69	50.2%	34.2
3	West 5-FarWest 4	345kV	-7.53	6.34	13.88	53.04	95.86	-7.19	6.01	0.32	57.5%	13.2
4	West 5-North 1	345kV	-15.49	16.48	31.97	39.25	95.94	-15.59	18.94	-1.53	39.0%	34.5
5	North 1-North 4	345/138kV	4.15	15.96	11.81	100.00	95.98	3.91	15.87	8.95	100.0%	12.0
6	North 4-North 6	138kV	-23.96	4.47	28.44	2.52	96.12	-22.28	4.89	-6.32	4.5%	27.2
7	FarWest 7-FarWest 4	345kV	-13.78	2.72	16.50	3.65	95.60	-8.55	2.60	-2.66	3.7%	11.2
8	FarWest 7-West 14	345kV	-18.00	15.72	33.72	39.11	75.41	-17.93	15.29	-2.22	36.4%	33.2
9	FarWest 7-FarWest 8	345/138kV	3.77	15.21	11.44	100.00	91.44	2.91	14.13	8.63	100.0%	11.2
10	FarWest 7-FarWest 9	345/138kV	-6.99	8.39	15.38	57.22	74.99	-7.61	7.98	0.46	56.7%	15.6
11	West 12-FarWest 7	345kV	-6.25	11.71	17.96	80.26	95.80	-5.73	11.15	2.63	81.7%	16.9
12	West 12-West 1	345kV	-19.99	23.53	43.52	55.78	95.18	-6.23	7.08	0.67	55.9%	13.3
13	West 12-North 1	345kV	-14.56	14.66	29.22	36.87	96.03	-14.38	14.51	-1.92	36.6%	28.9
14	West 14-West 5	345kV	-12.42	9.52	21.94	45.55	75.57	-14.74	9.36	-0.80	47.3%	24.1
15	West 14-North 1	345kV	-10.83	8.19	19.02	27.56	75.56	-10.51	8.08	-2.33	25.4%	18.6
16	FarWest 9-West 4	138kV	-25.83	35.38	61.21	76.95	73.49	-24.30	34.76	7.17	77.2%	59.1
17	West 16-West 3	345kV	-2.56	4.60	7.17	64.42	66.21	-3.40	4.34	0.20	65.2%	7.7
18	West 16-West 14	345kV	-1.46	1.60	3.06	61.37	58.57	-2.11	2.21	0.05	52.3%	4.3
19	West 15-West 14	345kV	-4.57	9.44	14.01	68.45	61.22	-2.41	2.95	0.27	65.2%	5.4
20	Coast 1-South 10*	138kV	Phasor data is not available for these pairs					-12.27	39.84	8.22	79.1%	52.1
21	South 3-South 11*	138kV						-20.61	19.30	-1.12	46.9%	39.9
22	South 11*-North 7	345/69kV						-9.77	18.16	1.41	59.3%	27.9
23	North 7-South 7*	138/345kV						-22.14	14.89	-3.92	21.9%	37.0
24	North 7-South 9*	138/345kV						-11.74	10.29	-1.04	37.1%	22.0
25	West 11-West 8*	345kV						-9.83	10.00	1.21	62.9%	19.8
26	West 8-South 9*	345kV						-20.58	22.57	0.98	56.6%	43.2
27	FarWest 7-South 9*	345kV						-28.73	30.91	-0.14	49.6%	59.6
28	FarWest 9-South 9*	138/345kV						-29.98	32.99	-0.60	46.8%	63.0
29	West 19*-West 9	345kV						-6.13	3.78	-0.07	50.4%	9.9

* Denotes substations without existing PMUs or w/o data stream; no phasor data available for the Feb-July, 2014 period.

C. Criteria to Identify Normal Operations Limits for Angle Differences

The data received, both phasor and state estimator, provide information for all conditions during the study period, including those conditions where the system experienced outages of lines or generators. This study is intended to provide angle difference limits that can be expected during normal operations; that is, when all facilities are in service. The following criteria were used to determine the angle difference limits expected during normal operations for the selected substation pairs.

i. If the angle difference time duration curves show only positive angles, then two limits will be identified: one corresponding to the angle difference that occurred at about one percent of the time, and the other corresponding to the maximum value observed.
ii. If the angle difference time duration curves show positive as well as negative angles, then four limits will be identified, two for one direction of flow, and two for the opposite direction of flow, based on the criteria below:
    - The first limit in either direction will be set using state estimator results by selecting the maximum (or minimum) angle difference observed on the corresponding time duration curves if the box-whisker and time duration plots show no extreme values (outliers or extreme values due to events in the system). If extreme values or outliers are present, a point of inflection will be determined, and the maximum or minimum angle will be set at the angle corresponding to the point of inflection.
    - The second maximum limit will be set at the angle difference which occurred 1% more time than the time corresponding to the selected first maximum limit, based on the time duration curve. The second minimum limit will be set at the angle difference corresponding to 1% less time than the time corresponding to the selected first minimum limit.
iii. In some cases, such as when there was an extended outage, EPG reproduced the time duration curve, excluding those days when the extended outage occurred, to determine the angle differences corresponding to normal conditions.
iv. The 1% values can be used to set alarms for the operators to be notified of impending maximum angle differences. The maximum and minimum values can be used to set alarms notifying the operator that expected maximum or minimum values have been reached.
v. The alarms should be monitored for a year against actual values observed during operation. If maximum values are exceeded, the observed values should be logged and documented for further analysis and updates.
vi. Maximum and minimum voltage angles and their differences obtained for the pair analyzed in this update are not expected to change significantly unless major changes occur in generation output, such as a large increase in wind power production, or additional major transmission lines are added to the ERCOT system in addition to those CREZ lines already in service.
vii. This analysis should be revised based on the entire 12 months of 2014 historical data obtained with all the new CREZ transmission lines in service.

D. Summary of Results – Normal Conditions

The angle difference results for normal conditions are summarized in Table B-2below, which was developed based on the criteria described above.

Box-whisker and time duration curves were developed for each of the pairs analyzed. Angle differences that may be the results of contingencies were excluded by reviewing points of inflection; that is, points that significantly deviated from the normal operation trend observed in the box-whisker plots. The value of angle difference at the point of inflection was considered to be the maximum angle during normal conditions. If no outlier points were identified, then the angle corresponding to the 0% or 100% time points represents the maximum and minimum angles reached during normal operations in either direction of flow. SE-based voltage angle pairs with their corresponding box-whisker and time duration curves, as well as phasor-based voltage angle pairs with their corresponding box-whisker and time duration curves, are presented in Appendix B.

Table B- 2 - Baselining Analysis – Summary of Angle Differences – Normal Data

Table B-2 -CCET DISCOVERY ACCROSS TEXAS- BASELINING ANALYSIS- SUMMARY OF ANGLE DIFFERENCES - NORMAL CONDITIONS

				DATA RESULTS (Study Period: February 1 to July 31, 2014)															
				Phasor Data				State Estimator Data									SE Data		
No	Angle Pair FROM - TO		Base kV	Min Angle	Max Angle	Max-Min Spread	Percent Positive	Min Angle at POI or 100%	Percent (POI or 100%)	Min Angle at 99% or POI - 1%	Percent (99% or POI - 1%)	Max Angle at 1% or POI +1%	Percent (1% or POI +1%)	Max Angle at POI or 0%	Percent (POI or 0%)	Min Angle	Max Angle	Max-Min Spread
1	Coast 1	South 13	138	-16.41	20.79	37.20	58.74%	-17.09	99.97%	-12.22	98.97%	17.08	1.03%	24.77	0.03%	-17.09	24.77	41.9
2	West 5	West 10	345/69	-16.88	17.05	33.93	50.21%	-16.81	99.98%	-15.09	98.98%	13.40	1.12%	16.31	0.12%	-16.81	16.31	33.1
3	West 5	FarWest 4	345	-5.99	6.08	12.07	57.47%	-5.93	99.94%	-4.44	98.94%	5.03	1.02%	5.85	0.02%	-5.93	5.85	11.8
4	West 5	North 1	345	-14.46	15.72	30.18	39.02%	-14.83	99.96%	-13.34	98.96%	15.15	1.04%	18.39	0.04%	-14.83	18.39	33.2
5	North 1	North 4	345/138	4.41	15.84	11.43	100.00%	3.98	99.98%	4.50	98.98%	13.64	1.03%	15.29	0.03%	3.98	15.29	11.3
6	North 4	North 6	138	-23.62	3.56	27.18	4.47%	-21.73	99.88%	-19.88	98.88%	2.27	1.02%	4.73	0.02%	-21.73	4.73	26.5
7	FarWest 7	FarWest 4	345	-9.66	1.48	11.14	3.67%	-8.00	99.93%	-5.98	98.93%	0.69	1.06%	2.13	0.06%	-8.00	2.13	10.1
8	FarWest 7	West 14	345	-16.58	14.59	31.17	36.42%	-16.19	99.90%	-14.80	98.90%	11.79	1.01%	15.02	0.01%	-16.19	15.02	31.2
9	FarWest 7	FarWest 8	345/138	6.08	14.66	8.58	100.00%	4.82	99.98%	5.80	98.98%	12.04	1.02%	13.79	0.02%	4.82	13.79	9.0
10	FarWest 7	FarWest 9	345/138	-6.88	6.73	13.61	56.69%	-7.10	99.97%	-5.83	98.97%	5.69	1.05%	7.20	0.05%	-7.10	7.20	14.3
11	West 12	FarWest 7	345	-5.36	11.47	16.83	81.73%	-5.40	99.97%	-3.53	98.97%	9.60	1.06%	10.95	0.06%	-5.40	10.95	16.4
12	West 12	West 1	345	-6.47	6.70	13.17	55.89%	-5.93	99.97%	-4.50	98.97%	5.85	1.01%	6.73	0.01%	-5.93	6.73	12.7
13	West 12	North 1	345	-13.86	14.03	27.89	36.62%	-14.14	99.96%	-12.59	98.96%	12.20	1.01%	14.39	0.01%	-14.14	14.39	28.5
14	West 14	West 5	345	-11.55	8.71	20.26	47.27%	-14.27	99.94%	-12.10	98.94%	7.31	1.04%	9.17	0.04%	-14.27	9.17	23.4
15	West 14	North 1	345	-10.53	7.86	18.39	25.43%	-10.32	99.98%	-8.84	98.98%	4.82	1.02%	8.01	0.02%	-10.32	8.01	18.3
16	FarWest 9	West 4	138	-24.16	33.55	57.71	77.17%	-23.42	99.95%	-14.49	98.95%	27.60	1.02%	34.29	0.02%	-23.42	34.29	57.7
17	West 16	West 3	345	-2.38	3.49	5.87	65.21%	-3.29	99.98%	-2.31	98.98%	3.58	1.04%	4.25	0.04%	-3.29	4.25	7.5
18	West 16	West 14	345	-1.32	1.51	2.83	52.35%	-2.04	99.95%	-1.38	98.95%	1.65	1.11%	2.15	0.11%	-2.04	2.15	4.2
19	West 15	West 14	345	-3.86	7.92	11.78	65.17%	-2.33	99.96%	-1.38	98.96%	2.13	1.02%	2.93	0.02%	-2.33	2.93	5.3
20	Coast 1	South 10*	138	NO PHASOR DATA AVAILABLE FOR THESE PAIRS			79.11%	-11.38	99.93%	-6.93	98.93%	25.86	1.02%	38.17	0.02%	-11.38	38.17	49.5
21	South 3	South 11*	138/345				46.89%	-20.36	99.99%	-16.23	98.99%	12.12	1.02%	18.02	0.02%	-20.36	18.02	38.4
22	South 11*	North 7	138/345				59.32%	-9.24	99.99%	-6.41	98.99%	14.21	1.01%	18.05	0.01%	-9.24	18.05	27.3
23	North 7	South 7*	138/345				21.92%	-21.56	99.95%	-17.62	98.95%	4.89	1.06%	13.70	0.06%	-21.56	13.70	35.3
24	North 7	South 9*	138/345				37.10%	-11.16	99.96%	-8.65	98.96%	6.06	1.02%	9.89	0.02%	-11.16	9.89	21.1
25	West 11	West 8*	345				62.92%	-9.19	99.96%	-6.74	98.96%	8.05	1.02%	9.88	0.02%	-9.19	9.88	19.1
26	West 8	South 9*	345				56.63%	-18.44	99.92%	-11.31	98.92%	12.69	1.05%	21.88	0.05%	-18.44	21.88	40.3
27	FarWest 7	South 9	345				49.58%	-27.44	99.94%	-21.70	98.94%	20.10	1.02%	29.95	0.02%	-27.44	29.95	57.4
28	FarWest 9	South 9*	138/345				46.80%	-29.16	99.97%	-22.63	98.97%	20.92	1.03%	31.73	0.03%	-29.16	31.73	60.9
29	West 19*	West 9	345				50.40%	-5.79	99.94%	-4.59	98.94%	2.81	1.01%	3.50	0.01%	-5.79	3.50	9.3

Note: The substations market with * did not have PMUs installed by July 31, 2014: no phasor data available.

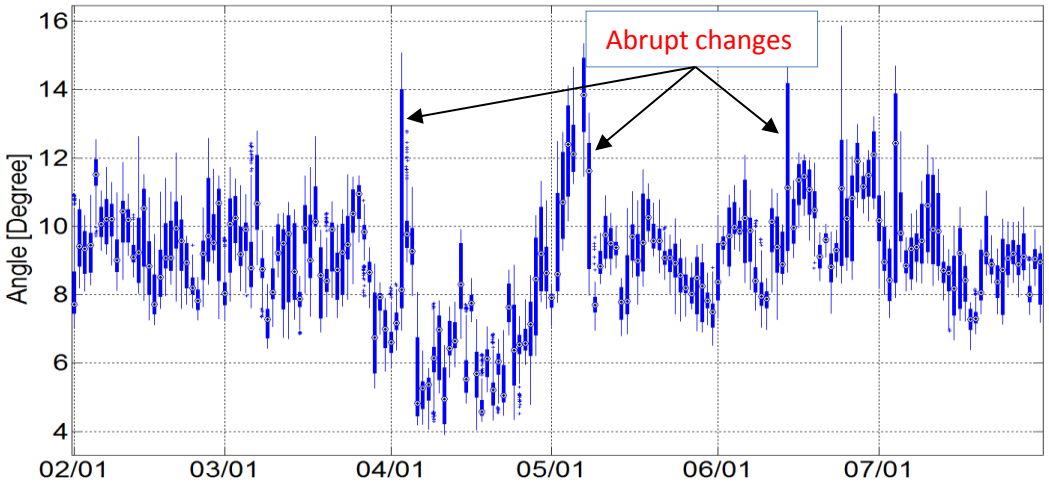
E. Observations from Table B-2:

I. The maximum Max-Min angle spreads under normal conditions occurred at FarWest 9-South 9 with 60.9 degrees.
II. Two pairs had Max-Min spreads between 57 and 60 degrees: FarWest 9-West 4 (57.7 degrees) and FarWest 7-South 9 (57.4 degrees).
III. Five pairs had minimum Max-Min voltage spreads of less than 10 degrees: West 16-West 14 (4.2), West 15-West 14 (5.3), West 16-West 3 (7.5), FarWest 7-FarWest 8 (9.0), and West 19-West 9 (9.3).
IV. The maximum voltage angles in degrees under normal conditions occurred at Coast 1-South 10 (38.2), FarWest 9-West 4 (34.3), and FarWest 9-South 9 (31.7).
V. Minimum angles occurred at FarWest 9-South 9 (-29.2) and FarWest 7-South 9 (-27.4).
VI. Four additional substations had minimum angles lower than -20 degrees.
VII. Four pairs had positive flows greater than 90% of the time: North 1-North 4 (100%), FarWest 7-FarWest 8 (100%), FarWest 4-FarWest 7 (96.3%), and North 6-North 4 (95.6%).

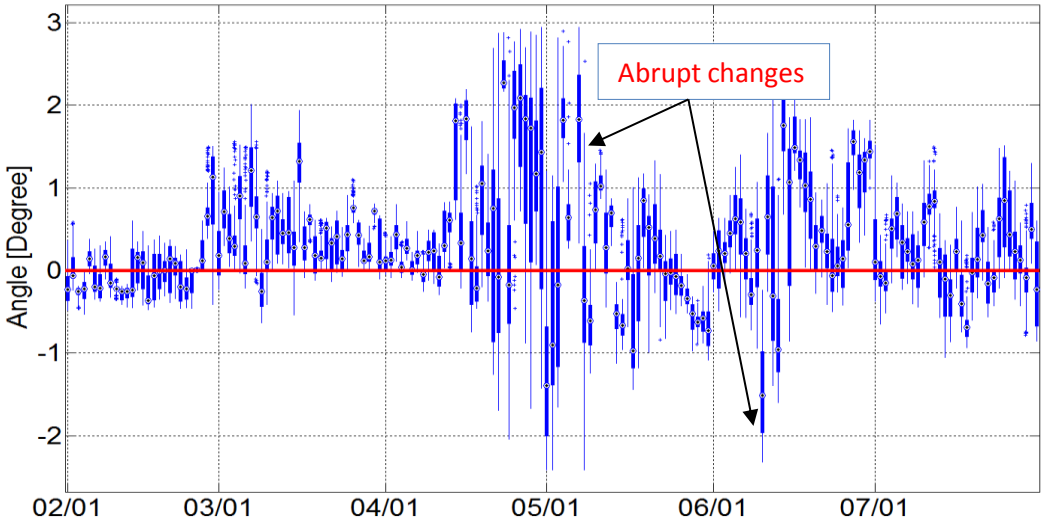
F. Observations from State Estimator Box-Whisker Plots (Appendix B - Part 1)

1. State Estimator data availability for this update was the best EPG has received so far. Only one day of data was missing (May 6). Aside from this missing day, two pairs show a gap in data: Coast 1 South 13 (second half of February) and West 19-West 9 (between April and May).
2. In general, the box-whisker plots show less variability than in 2013.
3. A few pairs show some variability: North 1-North 4, FarWest 7-West 14, West 12-FarWest 7, West 12-North 1, West 14-North 1, FarWest 9-West 4, Coast 1-South 10, South 3-South 11, South 11-North 7, and FarWest 9-South 9.
4. Box-whisker plots for four pairs show data that may be suspect: West 16-West 3, West 16-West 14, West 15-West 14, and West 19-West 9.
5. If there were extended outages, the angles corresponding to the outage times should be excluded from the data used to establish normal operation alarm limits. Outage data should be documented and taken into account for any future updates.
6. Examples of abrupt angle changes that may be due to outages are shown below:

North 1 – North 4



West 15 – West 14



8. PAIRS FOR REAL TIME MONITORING

A. Criteria for Selection of Angle Pairs for Real-time Monitoring

1. Choose a few transmission paths (pairs) from the wind areas to monitor wind power delivery.
2. Choose a load center such as North 1 and select transmission paths serving such loads.
3. Choose transmission paths delivering power from the Valley.
4. Choose transmission paths connecting the load centers, such as the Dallas, Austin, San Antonio and Houston areas (no PMUs in the Houston area at this time).

NOTE: Because there are not enough PMUs installed in the system, EPG chose pairs that meet this criteria as closely as possible.

B. Transmission Paths (Pairs) Selected for Real-Time Monitoring

The transmission paths selected for monitoring are shown in Table 7 below:

Table 7 - Angle Pairs Selected for Real-Time Monitoring (Based on PMU Availability)

TABLE 7: ANGLE PAIRS SELECTED FOR REAL-TIME MONITORING (Based on PMU Availability)				
	PAIRS WITH PHASOR DATA AVAILABLE			
#	Substation A	Substation B	From Region	To Region
1	Coast 1	South 13	Valley	Valley
2	Coast 1	North 7	Valley	Central-East
3	Coast 4	North 7	Valley	Central-East
4	South 3	South 11*	Valley	Valley
5	South 11*	North 7	Valley	Central-East
6	North 6	North 7	East	Central-East
7	North 4	North 7	Dallas	Central-East
8	West 14	North 1	Panhandle	Dallas
9	West 5	North 1	Central	Dallas
10	North 1	North 7	Dallas	Central-East
11	West 3	North 7	Central	Central-East
12	West 14	West 5	Panhandle	Central
13	West 5	North 7	Central	Central-East
14	West 12	West 1	Central	Central
15	West 12	FarWest 7	Central	West Texas
16	FarWest 7	North 7	West Texas	Central-East
17	FarWest 7	South 9*	West Texas	Valley
18	FarWest 7	FarWest 9	West Texas	West Texas
19	West 1	North 7	Central	Central-East
20	FarWest 9	West 4	West Texas	Southwest
21	West 4	North 7	Southwest	Central-East
22	West 15	West 14	Panhandle	Panhandle
23	West 16	West 14	Panhandle	Panhandle
24	West 16	West 3	Panhandle	Central
25	West 19*	West 9	Panhandle	Central
*	Means PMU planned for this substation but not available at this time.			

C. Proposed Alarm Limits

Table 8 below shows the proposed angle limits for the paths (pairs) selected for real-time monitoring. These proposed limits were selected from the results for normal conditions shown in Table A- 2 and Table B- 2 of this report. These results are based on the data for the February to July months of 2014 provided by ERCOT. Whereas in 2013 CREZ lines were being added almost on a monthly basis, causing an ongoing change in angle differences, during this most recent 6-month period all except for four CREZ lines have been in-service. As a result, the angle differences are now more stable. The four additional 345 kV CREZ lines, added to the ERCOT system in March 2014, are not expected to significantly change the angle differences under analysis. However, the alarm limits proposed in this section may change to some degree if generation is redistributed due to the addition of significant amounts of wind power, or significant decommissioning of old generation. EPG suggests that an alarm limits update be conducted in 2015 when the ERCOT system has had the opportunity to adjust to its new significantly expanded transmission infrastructure.

By monitoring these angle pairs, the ERCOT grid operators should have a good overview of power flow from generation centers to the load centers, and between load centers. It will provide them with a good idea of ongoing power flows among the different regions of the ERCOT grid.

EPG suggests that the ERCOT system operators document anytime these limits are exceeded, noting the possible reason, if known, for the deviations such as line or generation outages.

Note that all the pairs in Table 8 below have two negative alarm limit values and two positive alarm limit values. The negative values apply in the TO to FROM (inbound power flow) direction and the positive values apply in the FROM to TO (outbound power flow) direction.

Table 8 - Baselining Analysis – Recommended Alarm Limits for Real-Time Monitoring

Table 8 - BASELINING UPDATE 3 - RECOMMENDED ALARM LIMITS FOR REAL-TIME MONITORING										
				ALARM LIMITS UNDER NORMAL CONDITIONS (Based on February to July, 2014 Data)						
				SE Data-Normal			RECOMMENDED ALARM LIMITS			
No	Angle Pair FROM - TO		Base kV	Min Angle	Max Angle	Max-Min Spread	MINIMUM ALARM LIMIT	MINIMUM ALARM ALERT	MAXIMUM ALARM ALERT	MAXIMUM ALARM LIMIT
1	Coast 1	South 13	138	-17.09	24.77	41.86	-17.09	-12.22	17.08	24.77
2	Coast 1	North 7	138	-29.94	41.21	71.2	-29.94	-24.09	30.94	41.21
3	Coast 4	North 7	345	-29.09	47.54	76.6	-29.09	-20.87	34.65	47.54
4	South 3	South 11*	138/345	-20.36	18.02	38.4	-20.36	-16.23	12.12	18.02
5	South 11*	North 7	345	-8.54	17.66	41.9	-8.54	-6.36	14.18	17.66
6	North 6	North 7	138	-5.91	12.56	18.5	-5.91	-3.81	9.93	12.56
7	North 4	North 7	138/345	-16.15	6.79	22.9	-16.15	-12.88	4.41	6.79
8	West 14	North 1	345	-10.32	8.01	18.3	-10.32	-8.84	4.82	8.01
9	West 5	North 1	345	-14.83	18.39	33.2	-14.83	-13.34	15.15	18.39
10	North 1	North 7	345	-6.78	15.75	22.5	-6.78	-3.75	12.45	15.75
11	West 3	North 7	345	-13.80	15.82	29.6	-13.80	-8.18	13.36	15.82
12	West 14	West 5	345	-14.27	9.17	23.4	-14.27	-12.10	7.31	9.17
13	West 5	North 7	345	-14.50	24.66	39.2	-14.50	-11.59	21.26	24.66
14	West 12	West 1	345	-5.93	6.73	12.7	-5.93	-4.50	5.85	6.73
15	West 12	FarWest 7	345	-5.40	10.95	16.4	-5.40	-3.53	9.60	10.95
16	FarWest 7	North 7	345	-22.50	24.87	47.4	-22.50	-18.51	20.71	24.87
17	FarWest 7	South 9*	345	-27.44	29.95	57.4	-27.44	-21.70	20.10	29.95
18	FarWest 7	FarWest 9	345/138	-7.10	7.20	14.3	-7.10	-5.83	5.69	7.20
19	West 1	North 7	345	-9.26	15.89	25.1	-9.26	-7.01	13.04	15.89
20	FarWest 9	West 4	138	-23.42	34.29	57.7	-23.42	-14.49	27.60	34.29
21	West 4	North 7	138/345	-29.59	12.89	42.5	-29.59	-23.63	9.00	12.89
22	West 15	West 14	345	-2.33	2.93	5.3	-2.33	-1.38	2.13	2.93
23	West 16	West 14	345	-2.04	2.15	4.2	-2.04	-1.38	1.65	2.15
24	West 16	West 3	345	-3.29	4.25	7.5	-3.29	-2.31	3.58	4.25
25	West 19*	West 9	345	-5.79	3.50	9.3	-5.79	-4.59	2.81	3.50
	NOTE: These alarm limits were developed based on February to July, 2014 data.									

9. CONCLUSIONS

a. State Estimator (SE) Data Availability was Best in 2014

State estimator data, provided by ERCOT for the February to July, 2013 period, was the most complete EPG received in the baselining process. Of the six months of data provided by ERCOT, there was only one day of data missing (May 6, 2014). The state estimator collects data at a rate of 12 samples per hour. Overall SE availability was 48.7% of the total SE data collected, which was much better than the 29.6% availability for 2013, and the 13% availability for 2012. ERCOT provided SE data at a rate of six samples per hour. The SE data provided by ERCOT was 97.5% of all possible data at this rate.

b. Phasor Data Availability for 2014

All the PMUs providing data for this Baselining Update 3 were already in service by February 2014, which resulted in much improved phasor data availability compared to prior study periods. However, data availability was not uniformly high in all PMUs. Eighteen PMUs had availability greater than 90%, two PMUs had less than 20% availability (FarWest 2 and Coast 2), and the remaining ten PMUs had availability ranging from 62.08% (Coast 4) to 89.06% (Coast 1). Phasor data availability for all PMUs should be in the greater than 90% range for most accurate results.

c. Voltage Angle Variability (Reference: North 7)

Voltage angles with reference to North 7 have tightened considerably due to the completion of the CREZ project.

ALL DATA RESULTS:

i. The largest voltage angle variations occurred in the Valley. The maximum Max-Min spreads observed were 91.4 degrees for South 13 138 kV substation, 81.5 degrees for Coast 4 345 kV, and 81.1 degrees for Coast 3 substation.
ii. The lowest spread of 19.5 degrees was seen at North 6.
iii. The angles for North 1 and North 6 were positive most of the time (93.5 and 78.8%, respectively) whereas North 4, North 5, West 4, and South 5 substations are positive less than 20% of the time; that is, the power flows from North 7 to these substations most of the time.

NORMAL CONDITIONS: Due to the higher level of data availability for SE and Phasor data, the voltage angle spreads for normal conditions obtained from SE data were very similar to those voltage angle spreads obtained from phasor data.

i. Voltage angle fluctuations have been reduced and now vary over a smaller range. There are only five substations with Max-Min angle spreads of more than 60 degrees.
ii. The largest angle variations occurred among the substations in the southern part of the state: South 13, Coast 3, Coast 4, and Coast 1. South 13 with 85.5 degrees (-40.3 to 45.2

degrees), Coast 3 with 76.8 degrees (-29.1 to 47.7 degrees), Coast 4 with 76.6 degrees (-29.1 to 47.5 degrees), and Coast 1 with 71.2 degrees (-29.9 to 41.2 degrees).

iii. Only two substations had a Max-Min angle spread of less than twenty degrees: North 6 (18.5 degrees) and South 9 (19.3 degrees). All other substations have Max-Min spreads in the 21 to 61 degrees range.

iv. The smallest normal condition angles in degrees occurred at South 13 (-40.30) and South 10 (-33.46).

d. Maximum Voltage Angles Under Normal Conditions

The four largest normal condition angles in degrees observed were at Coast 3 (47.73), Coast 4 (47.74), South 13 (45.16), and Coast 1 (41.21).

e. Voltage Angle Variability (Angle Differences)

Voltage angle differences have also tightened (smaller angle differences) considerably due to the completion of the CREZ projects.

ALL DATA RESULTS:

i. The highest Max-Min angle spread occurred at FarWest 9-South 9 (63.0 degrees).

ii. Five pairs have spreads between 40 and 60 degrees: Coast 1-South 13, FarWest 9-West 4, Coast 1-South 10, West 8-South 9, and FarWest 7-South 9.

iii. Max-Min angle spread of less than 10 degrees occurred on four pairs: West 16-West 3, West 16-West 14, West 15-West 14, and West 19-West 9.

iv. The remaining nineteen pairs have angle spreads between 11.2 and 39.9 degrees.

v. Angle spreads for the February-July, 2014 period are smaller than those found for the same period in 2012, due to the addition of the CREZ lines to the ERCOT system.

vi. The maximum voltage angle found in this update was 39.8 degrees on the Coast 1-South 10 pair.

vii. Only two pairs have minimum voltage angles lower than -25 degrees: FarWest 7-South 9 (-28.73 degrees) and FarWest 9-South 9 (-29.98 degrees).

NORMAL CONDITIONS: Due to the higher level of data availability for SE and Phasor data, the voltage angle spreads for normal conditions obtained from SE data were very similar to those voltage angle spreads obtained from phasor data.

i. The maximum Max-Min angle spreads under normal conditions occurred at FarWest 9-South 9 with 60.9 degrees.

ii. Two pairs had Max-Min spreads between 57 and 60 degrees: FarWest 9-West 4 (57.7 degrees) and FarWest 7-South 9 (57.4 degrees).

iii. Five pairs had minimum Max-Min voltage spreads of less than 10 degrees: West 16-West 14 (4.2), West 15-West 14 (5.3), West 16-West 3 (7.5), FarWest 7-FarWest 8 (9.0), and West 19-West 9 (9.3).

iv. The maximum voltage angles in degrees under normal conditions occurred at Coast 1-South 10 (38.2), FarWest 9-West 4 (34.3), and FarWest 9-South 9 (31.7).
v. Minimum angles occurred at FarWest 9-South 9 (-29.2) and FarWest 7-South 9 (-27.4).
vi. Three additional substations had minimum angles lower than -20 degrees.
vii. Four pairs had percent positive flows greater than 90%: North 1-North 4 (100%), FarWest 7-FarWest 8 (100%), FarWest 4-FarWest 7 (96.3%), and North 6-North 4 (95.5).

f. Maximum Voltage Angles Under Normal Conditions

The three largest normal condition angles in degrees for angle differences were observed at Coast 1-South 10 (38.17), FarWest 9-West 4 (34.29), and FarWest 9-South 9 (31.73).

g. Voltage Spreads are Smaller in 2014

Voltage angle spreads for the substations in the western part of Texas, including the Panhandle, were much smaller in this update than in prior periods, because of the new CREZ transmission lines added between these regions and the rest of the ERCOT system. For example: 2014 voltage angle spreads for West 2, West 9, West 11, West 12, West 5, and West 6 referenced to North 7 experienced a reduction of more than 30-degrees from 2013.

h. Alarm Limits for Voltage Angles

All but four of the new CREZ lines were connected to the ERCOT system by January 2014. The remaining four lines were connected to the ERCOT system in March 2014. The ERCOT system has been operating with all the planned CREZ lines in-service since April 2014. The alarm limits obtained with the February to July 2014 data will be very stable unless major generation changes occur, such as major addition of wind power.

These alarm limits are not likely to change significantly in the near future unless a significant amount of wind power is added in the western area and the Panhandle areas of Texas, displacing generation in other areas, such as the Valley area. ERCOT operators can use the alarm limits established in this report to monitor real-time operations, keeping in mind that if major changes/shifts occur in generation production, these alarm limits should be revised, as appropriate.

Also, it is suggested that the ERCOT operators validate these limits by keeping track of the times when the limits are exceeded, indicating possible causes such as transmission or generation changes. A full year history of this validation tracking should be used to update alarm limits.

10. RECOMMENDATIONS

a. Data Monitoring and Data Integrity

State Estimator Data: The SE data provided by ERCOT for the February to July 2014 period was very good. However, data for January was not available. EPG recommends that SE data be fully preserved on a continuous basis for use in future alarm limits updates, and for calibrating phasor data.

Phasor Data: Of the 30 PMUs used in this update, eight PMUs show availability of less than 76%, of which two PMUs, FarWest 2 and Coast 2, show availability of less than 15%. EPG recommends that ERCOT and the PMU owners monitor phasor data for these eight PMUs to find and fix problems associated with missing data. PMUs signals, when available and producing accurate data, will allow system operators to accurately monitor the real-time conditions of the ERCOT system.

b. Alarm Limits for Real-Time Monitoring

EPG has produced alarm limits for 25 pairs for real-time monitoring; the recommended alarm limits for use by ERCOT system operators are shown in Section 8, Table 8 of this report. Each set of alarm limits includes two pairs, one pair of alarms to be used in the positive direction of flow (From-To) and the other pair of alarms to be used in the negative direction of flow (To-From). These recommended alarms can be implemented immediately.

c. Panhandle Wind Output Monitoring

There are four new CREZ lines connecting the Panhandle new 345 kV system with the Central ERCOT system: West 15-West 14, West 16-West 14, West 16-West 3, and West 19-West 9. The flows and angles on these four lines should provide a tool to monitor the wind output from that area. EPG recommends that ERCOT monitor this interface by including these four pairs in the RTDMS® daily report, or a separate report if necessary.

d. PMU at West 19

The Panhandle-North ERCOT interface, recommended above, has PMUs installed at all the substations, except for West 19. EPG recommends that, in order to monitor wind power flow from the Panhandle area to the Central area of the ERCOT system, PMUs be installed at this substation to be able to monitor voltage angle and power on all four lines comprising the interface.

e. RTDMS® Daily Report

The RTDMS® daily report should be simple, clear, meaningful, and easy to read quickly. EPG has produced some recommendations to accomplish these objectives. These recommendations are presented in Appendix D attached to this report.

f. Need for an Alarm Limits Update

The last four CREZ lines were placed in service in March 2014, completing the CREZ Project. The alarm limits proposed in this report are considered a good representation of present ERCOT conditions, since during most of the February to July 2014 period base of this update, all CREZ lines were already in-service.

With the new transmission infrastructure now in place, it is expected that, in future months and years, wind output will increase considerably, causing a re-distribution of power among the different generating areas of the ERCOT system. As a result, some angle differences may change, necessitating a periodic update of alarm limits. EPG recommends an annual update of alarm limits to reflect these changes. If major or sudden changes in these patterns occur, updates to the alarm limits should be performed.

Appendix A – Part 1
CCET Discovery Across Texas project

Baseline Analysis Update - Voltage Angles (Reference: North 7)

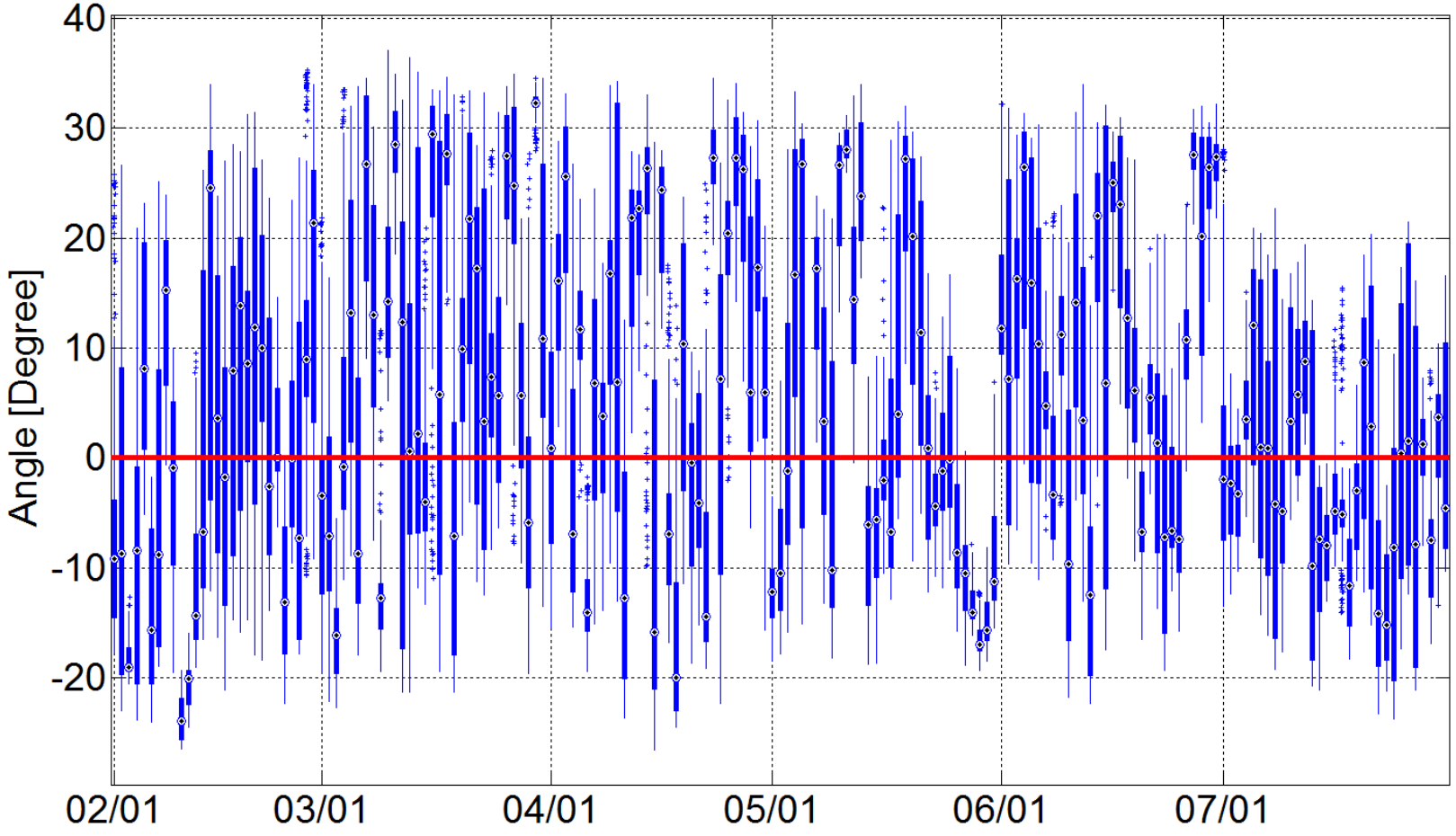
State Estimator Data: February to July 2014
Box-Whisker Plots and Time Duration Curves

Electric Power Group

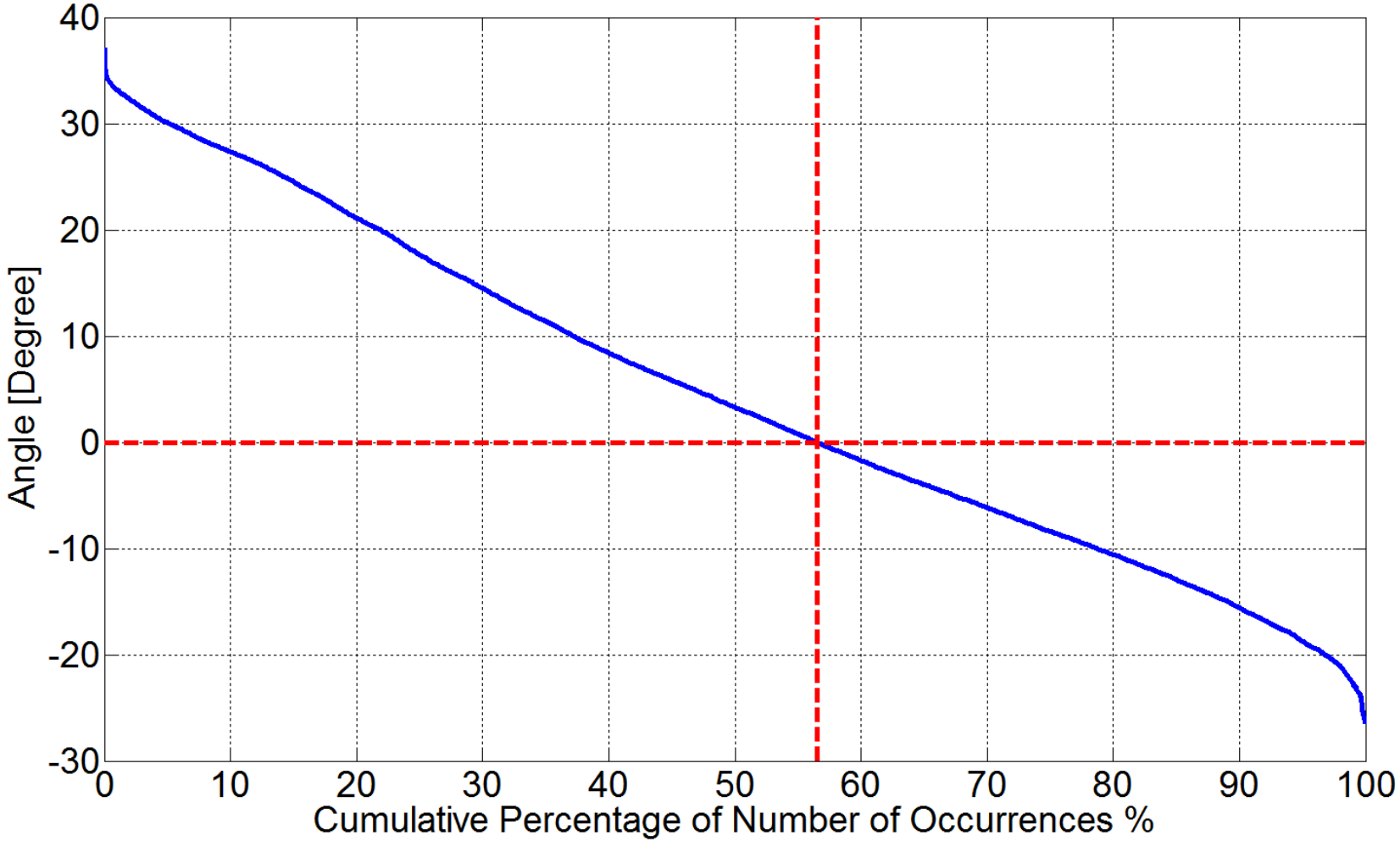
CCET

ERCOT

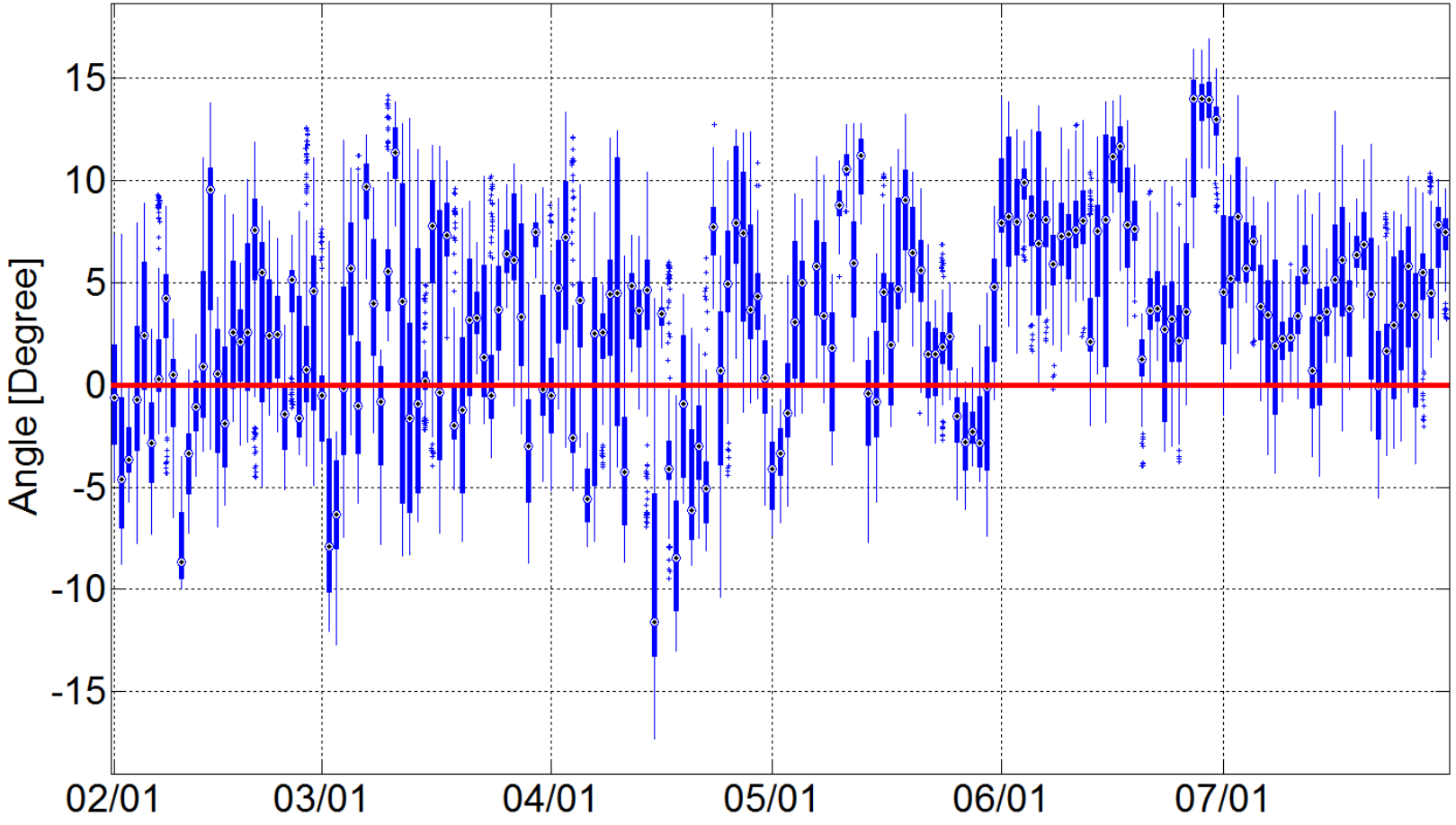
West 10-North 7



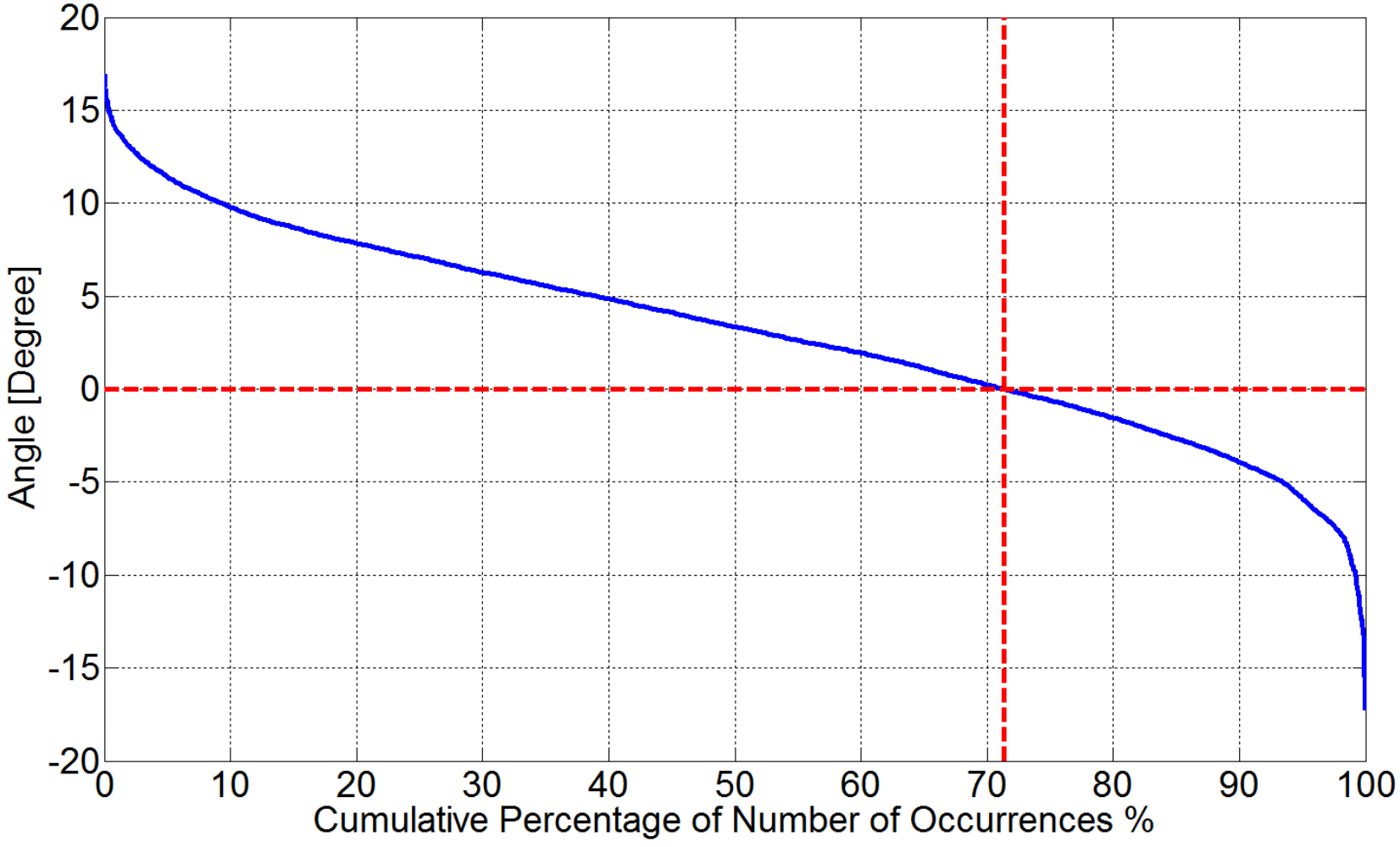
West 10-North 7



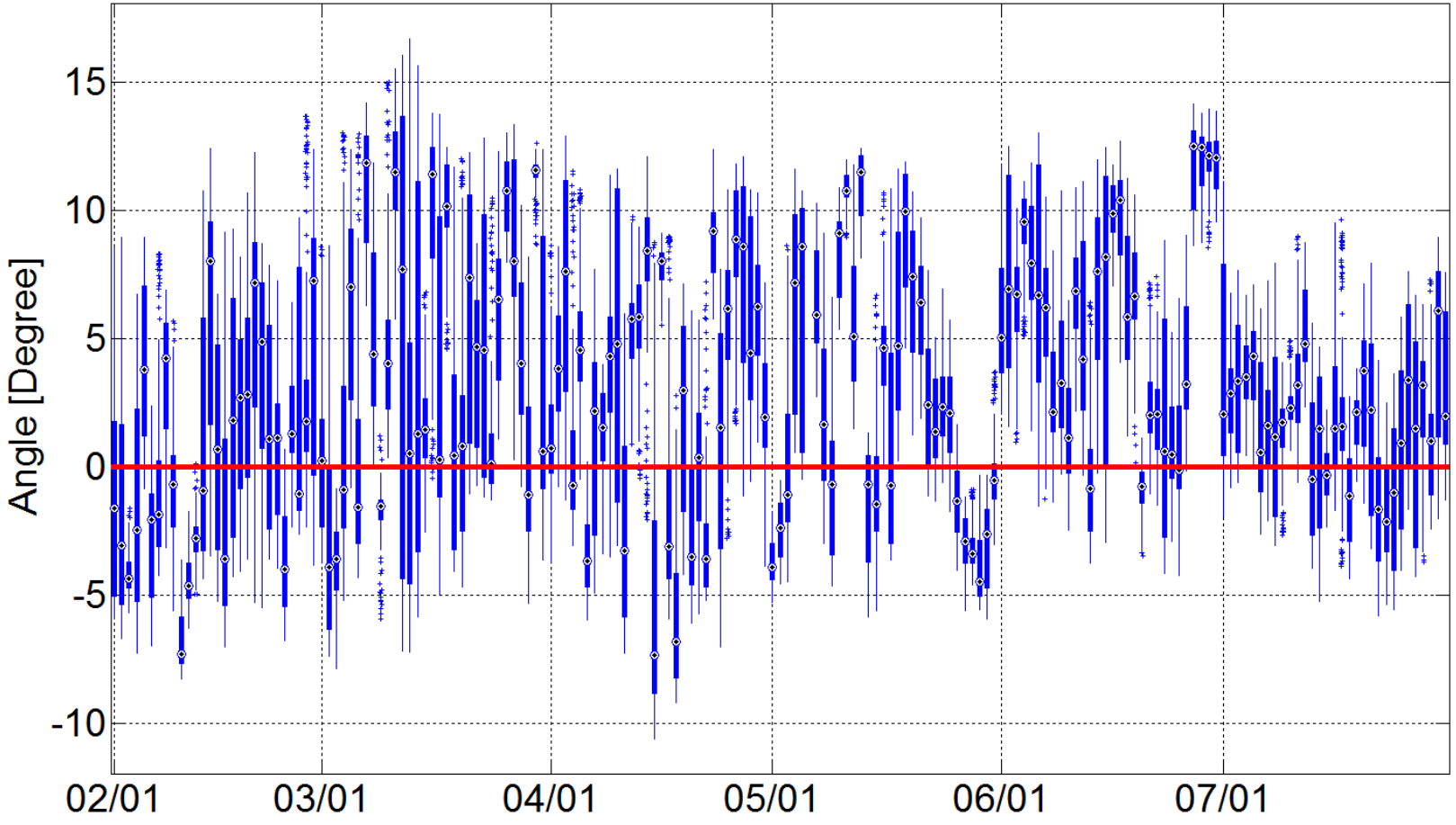
West 14-North 7



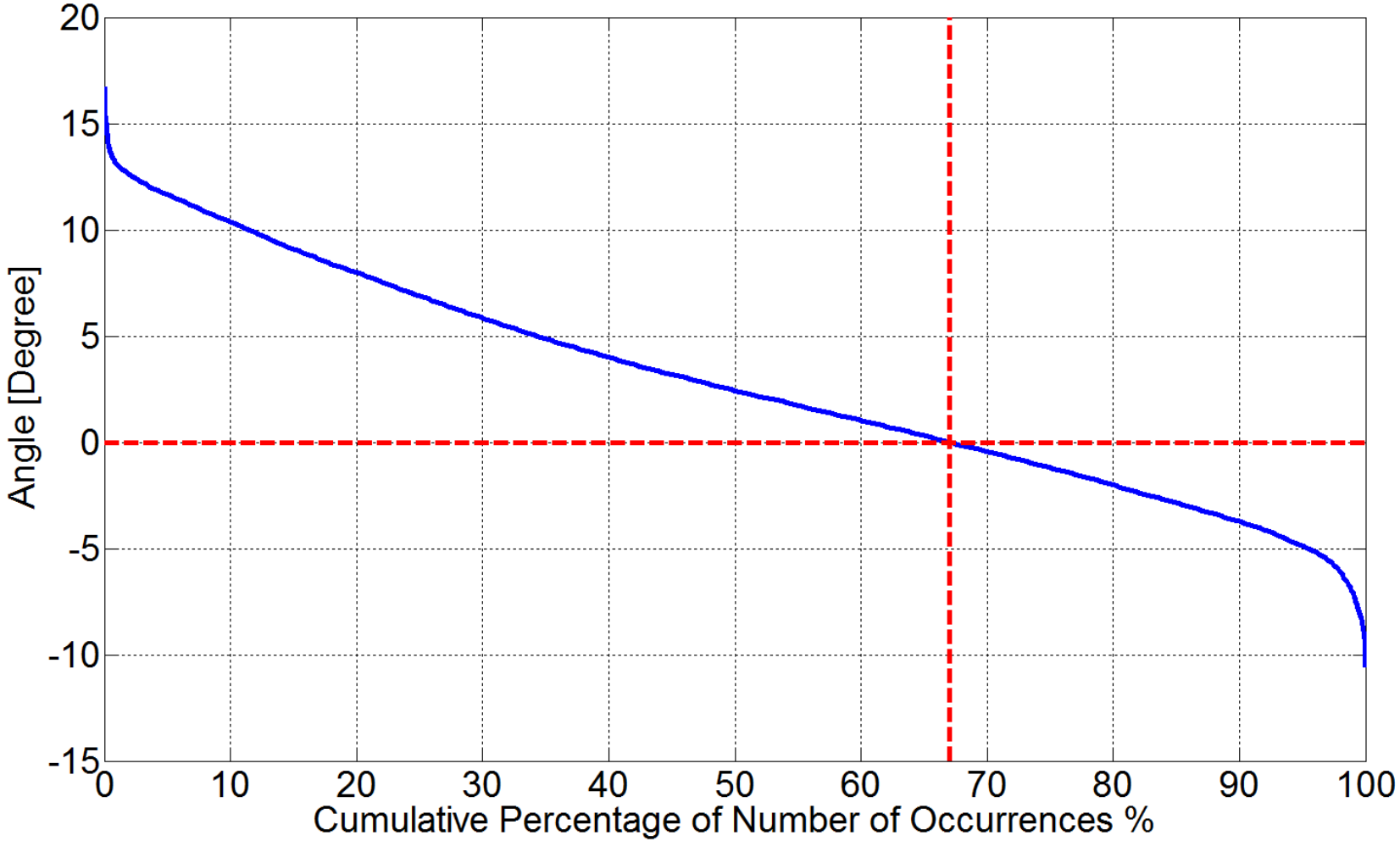
West 14-North 7



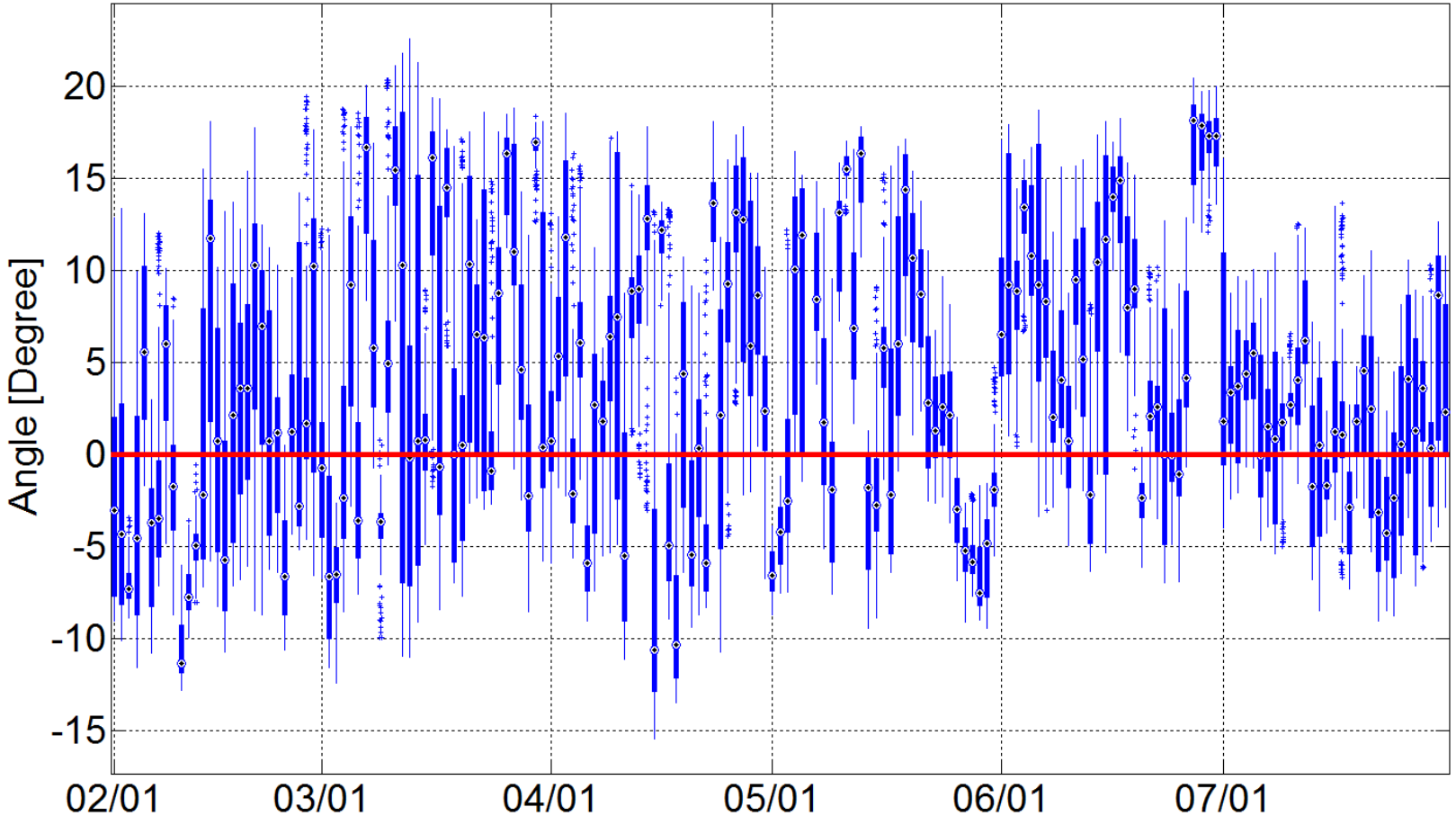
West 1-North 7



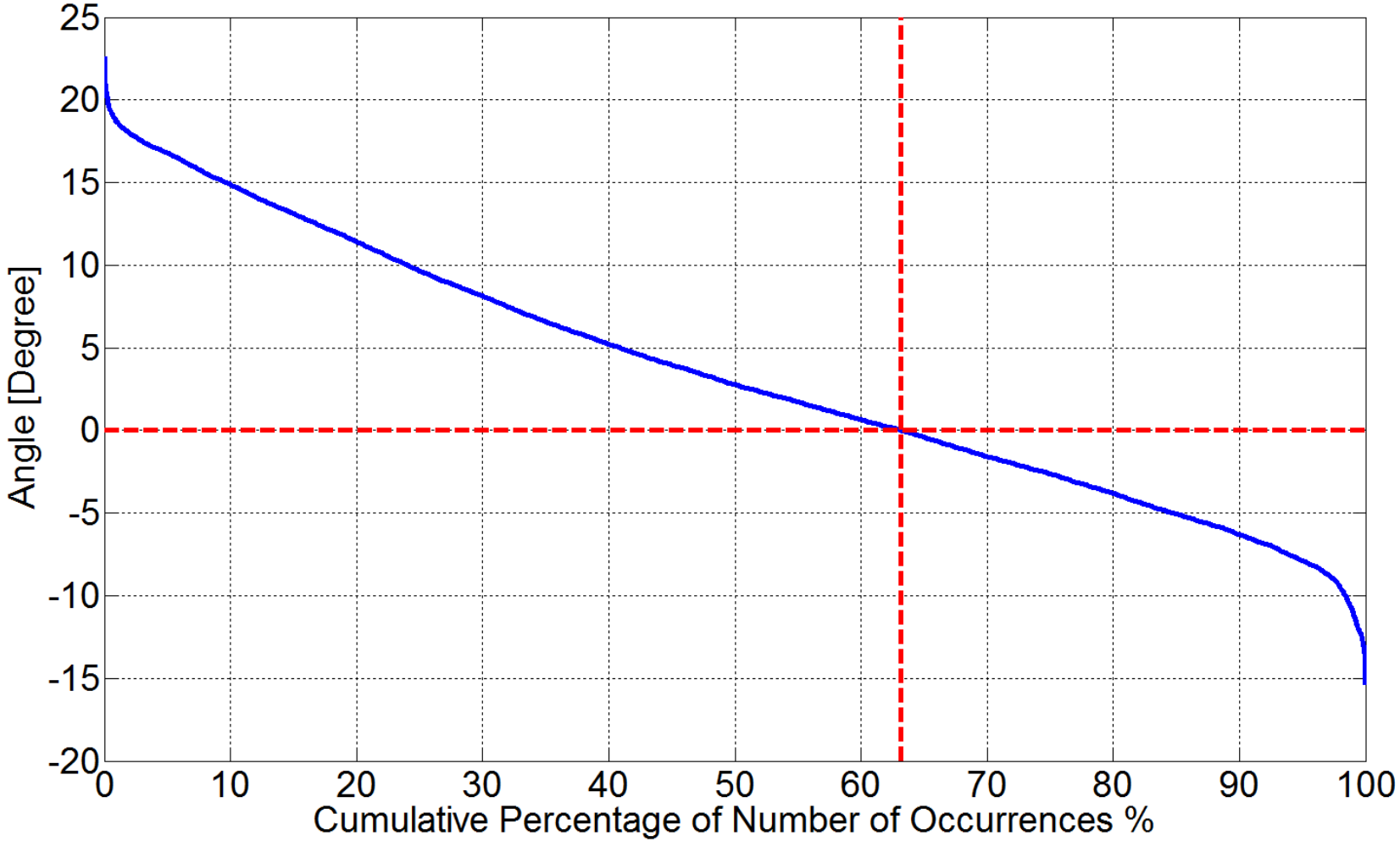
West 1-North 7



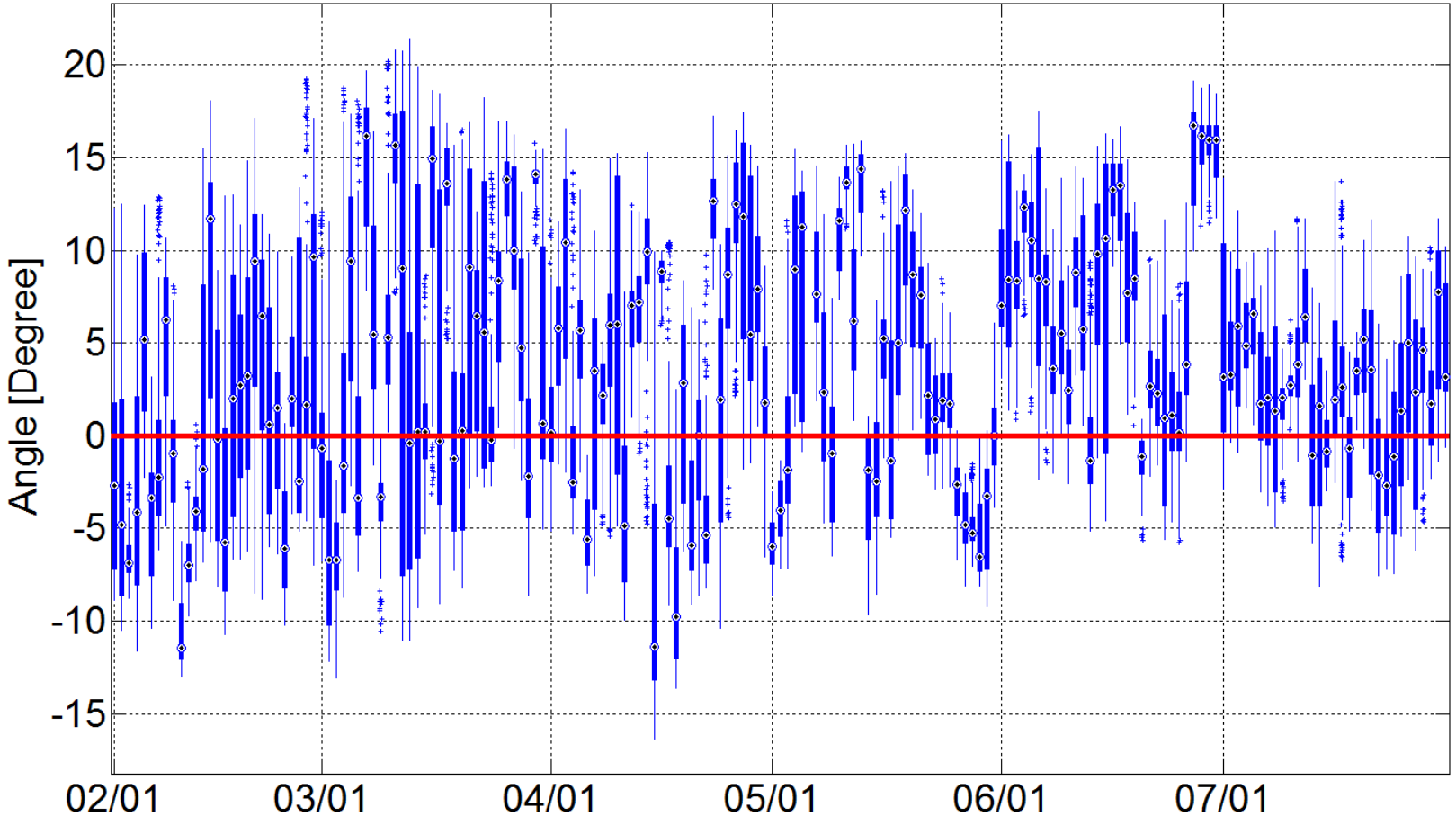
West 2-North 7



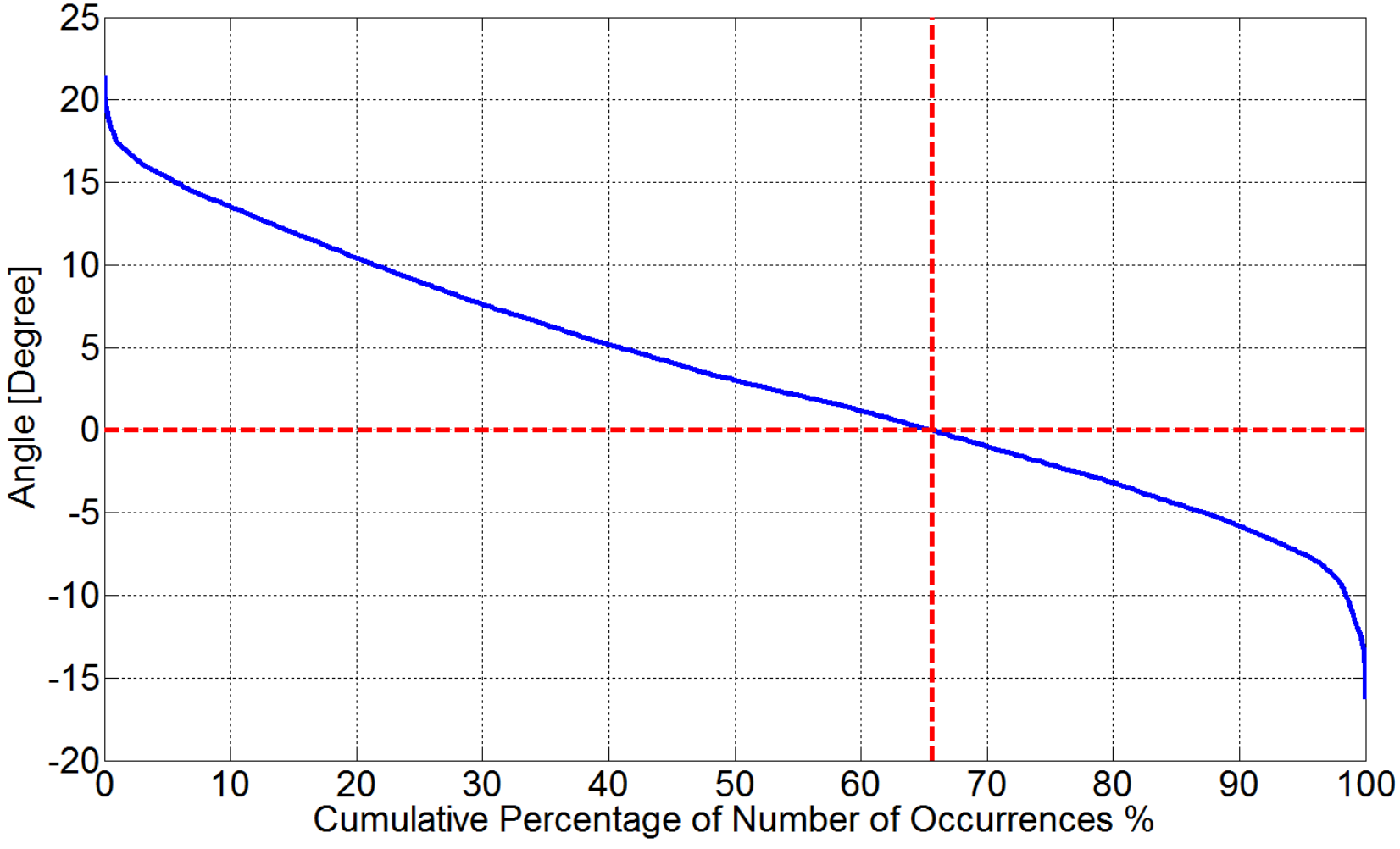
West 2-North 7



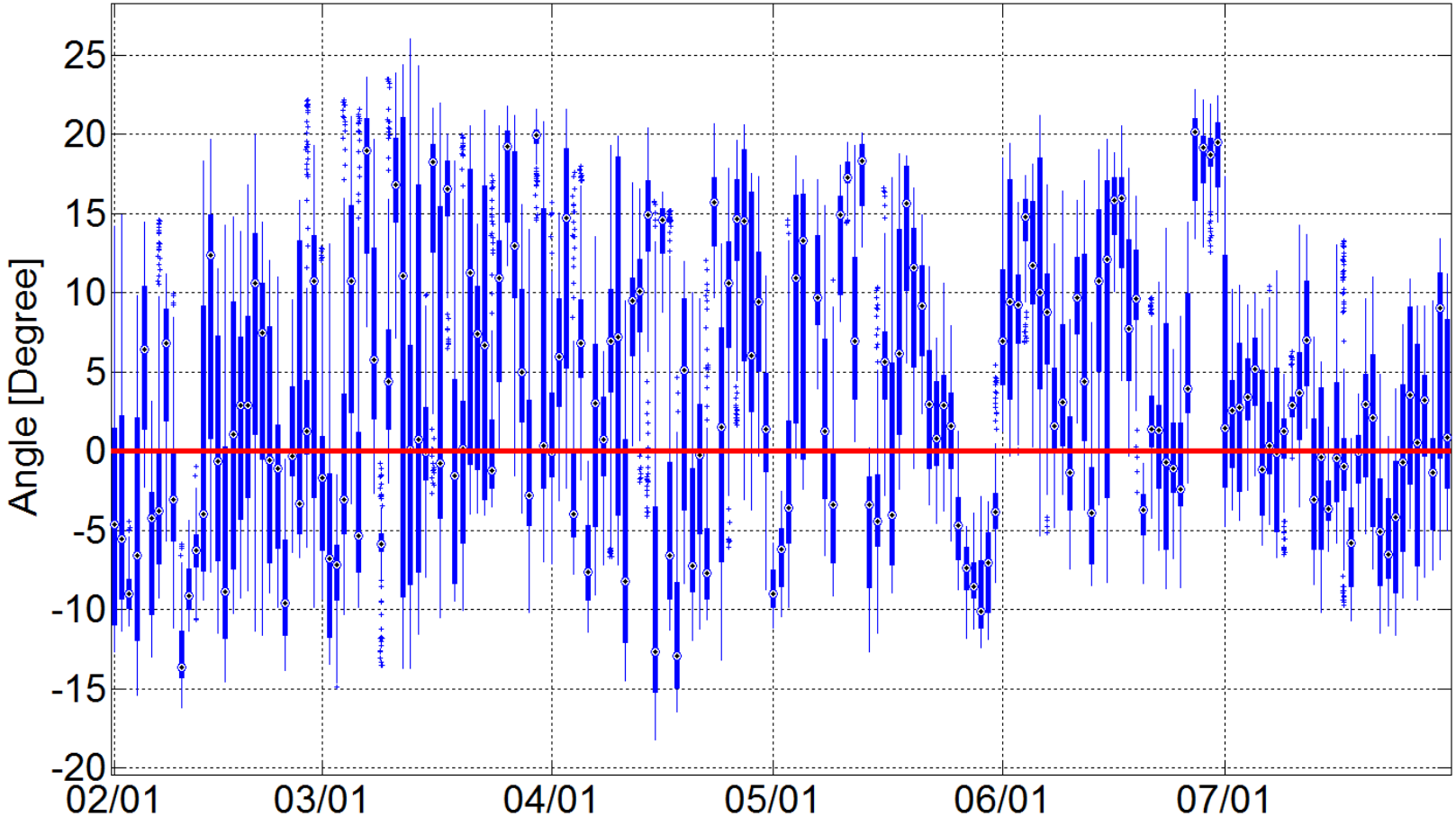
West 9-North 7



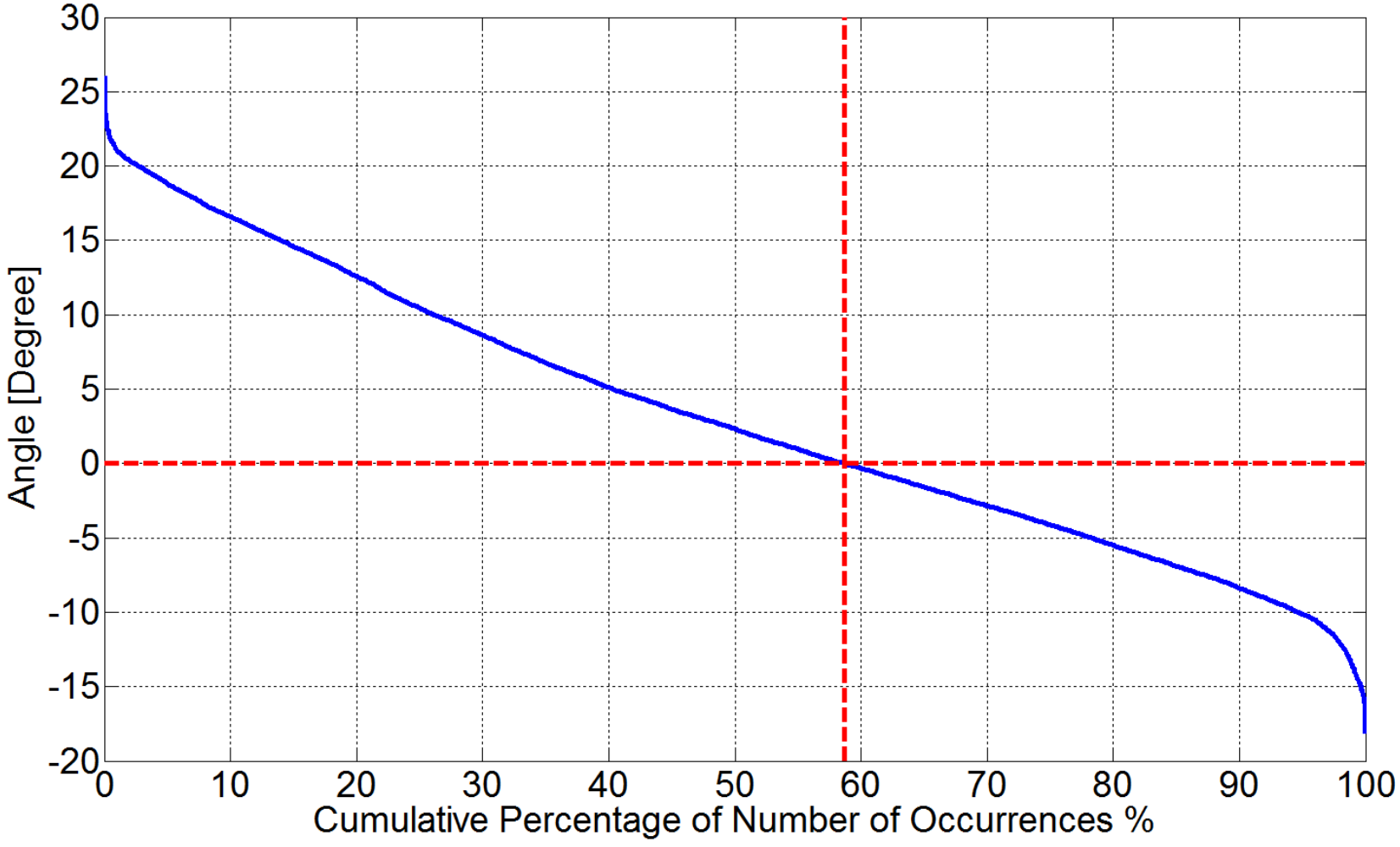
West 9-North 7



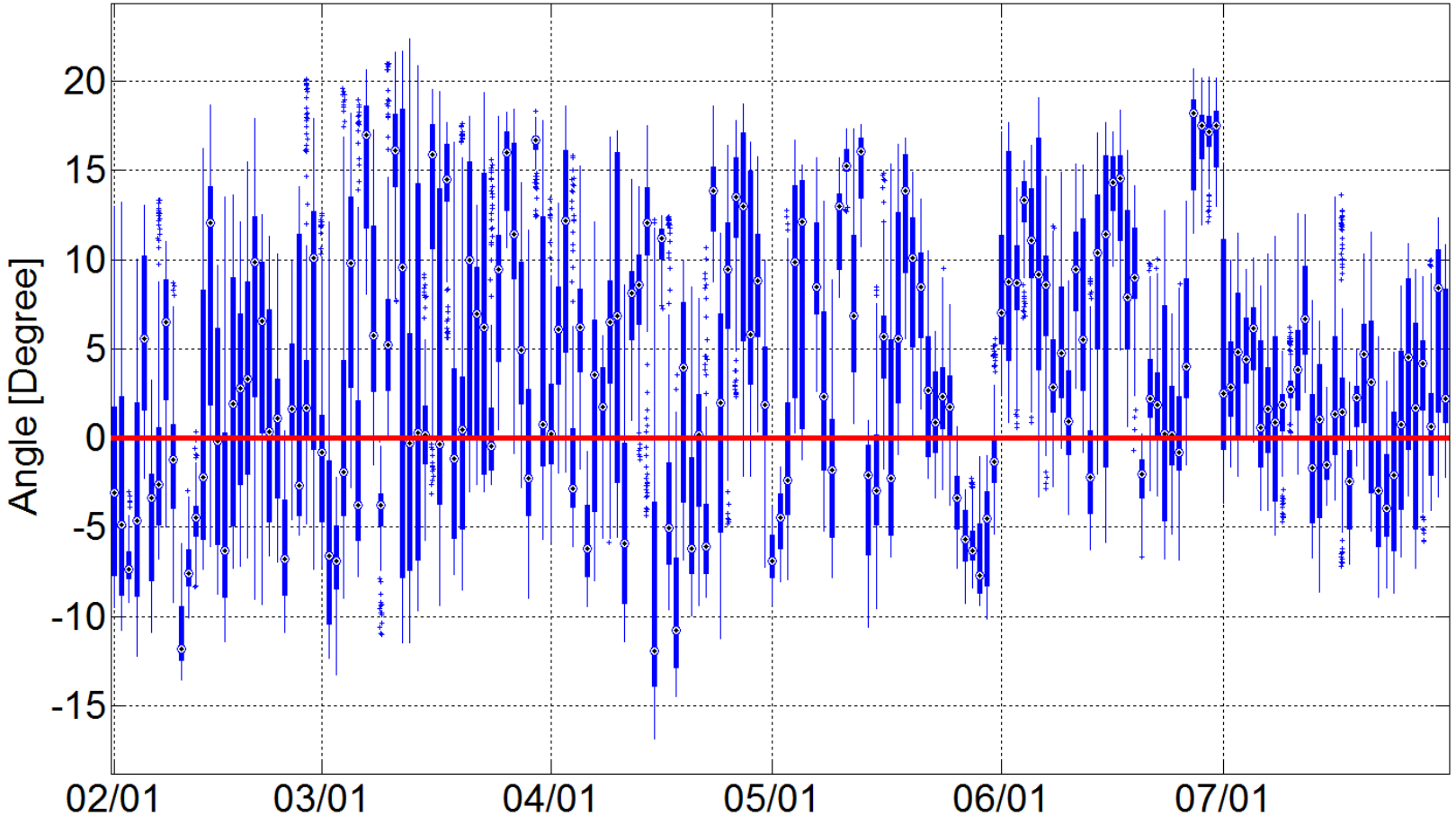
West 11-North 7



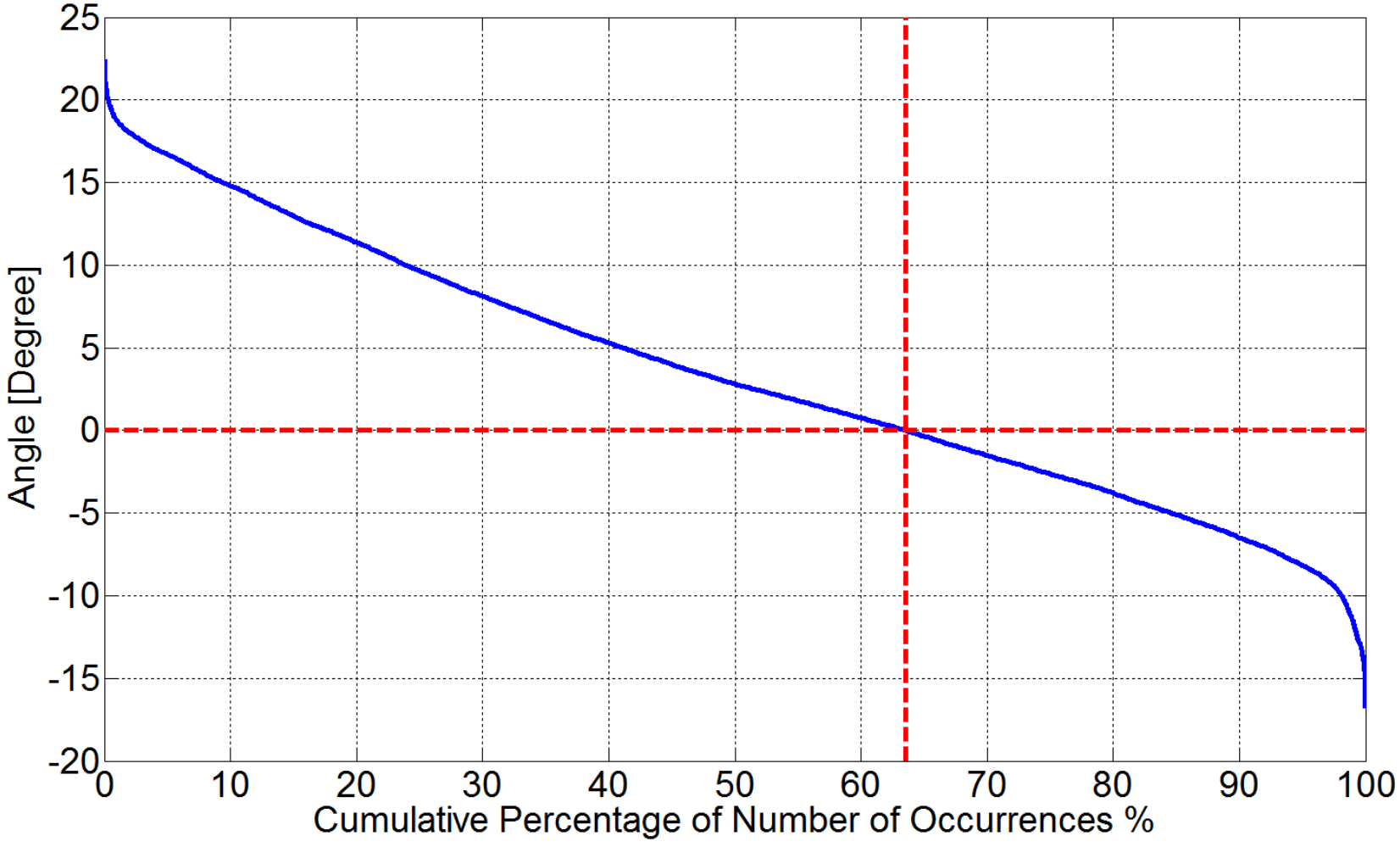
West 11-North 7



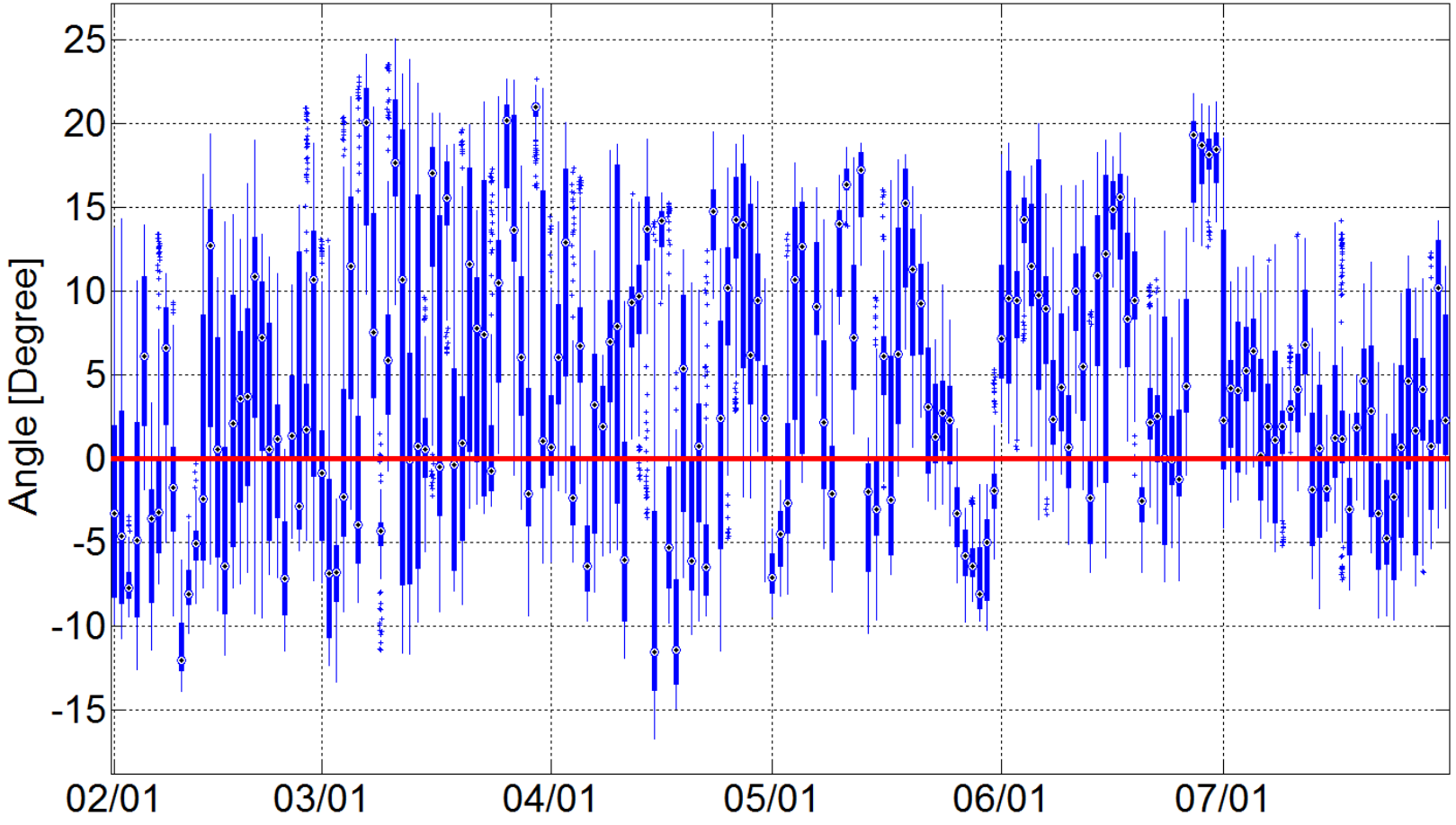
West 12-North 7



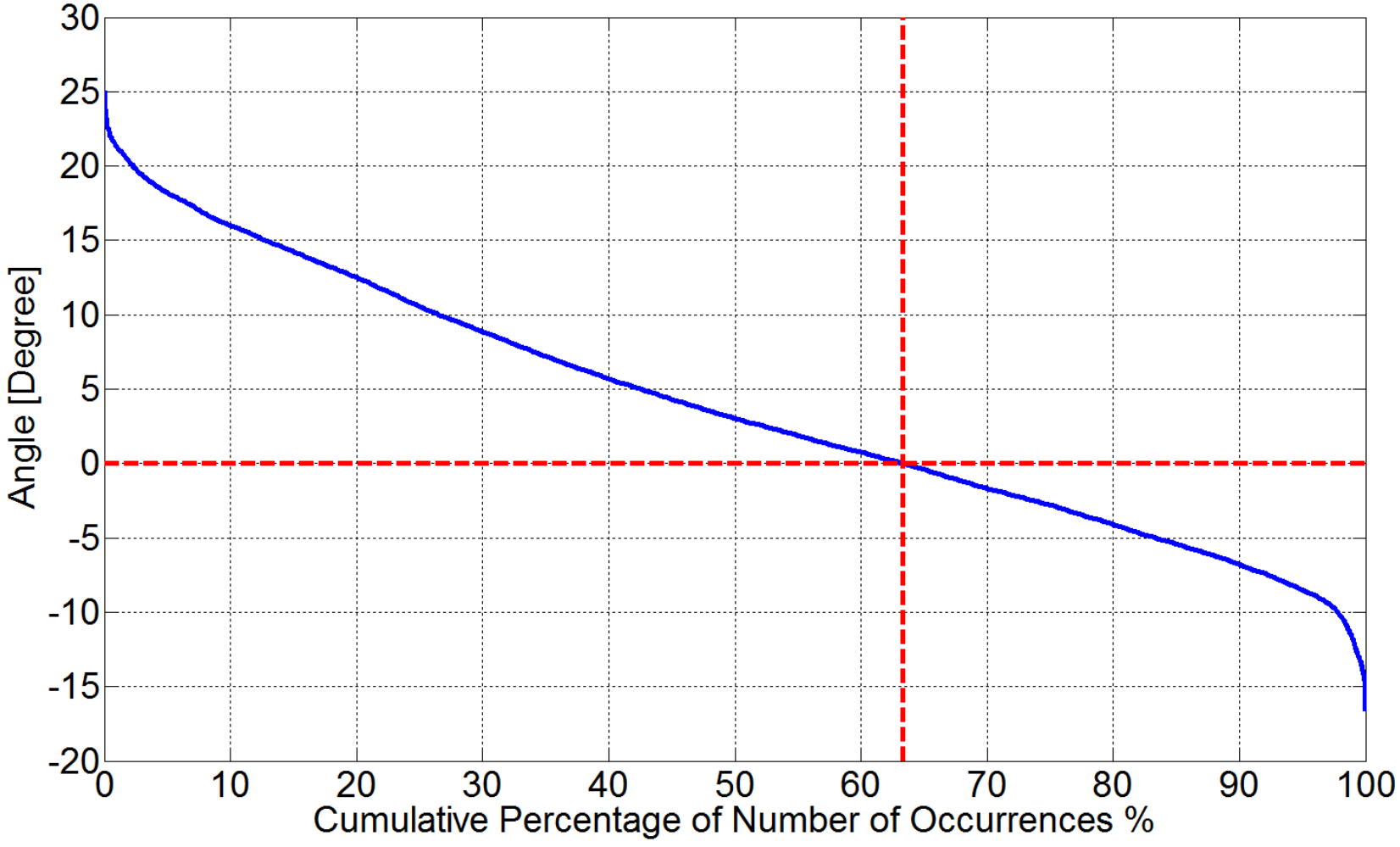
West 12-North 7



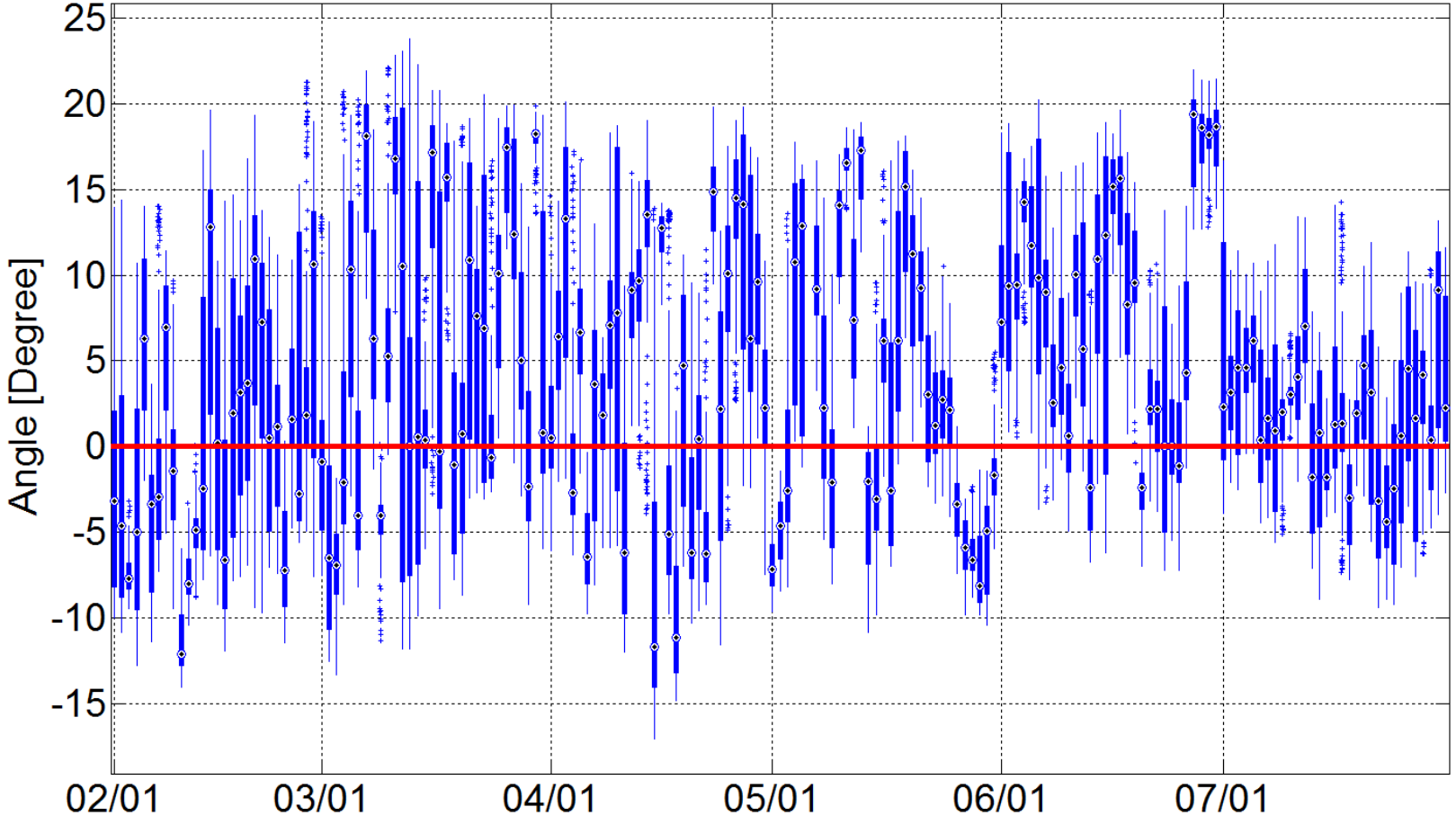
West 5-North 7



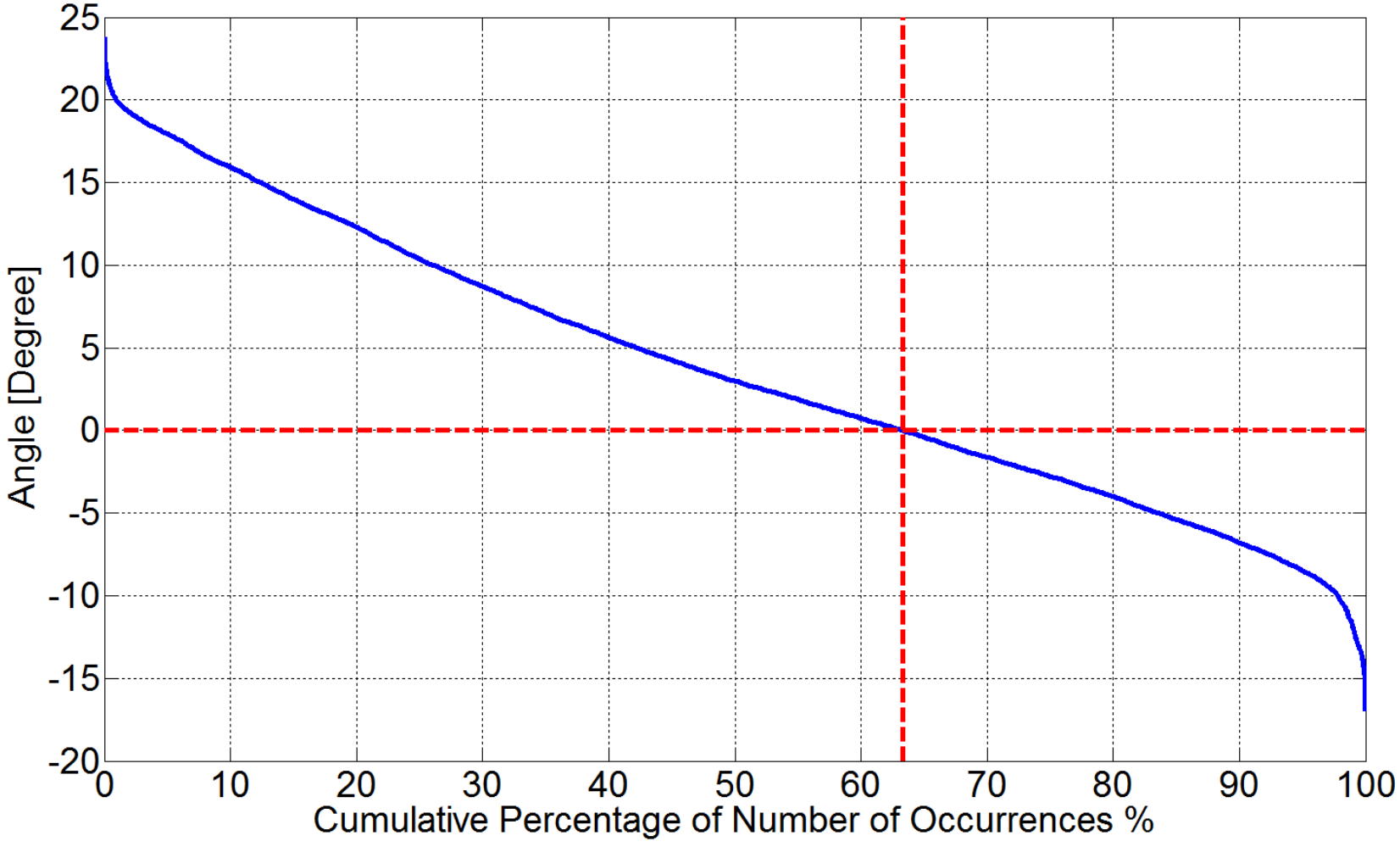
West 5-North 7



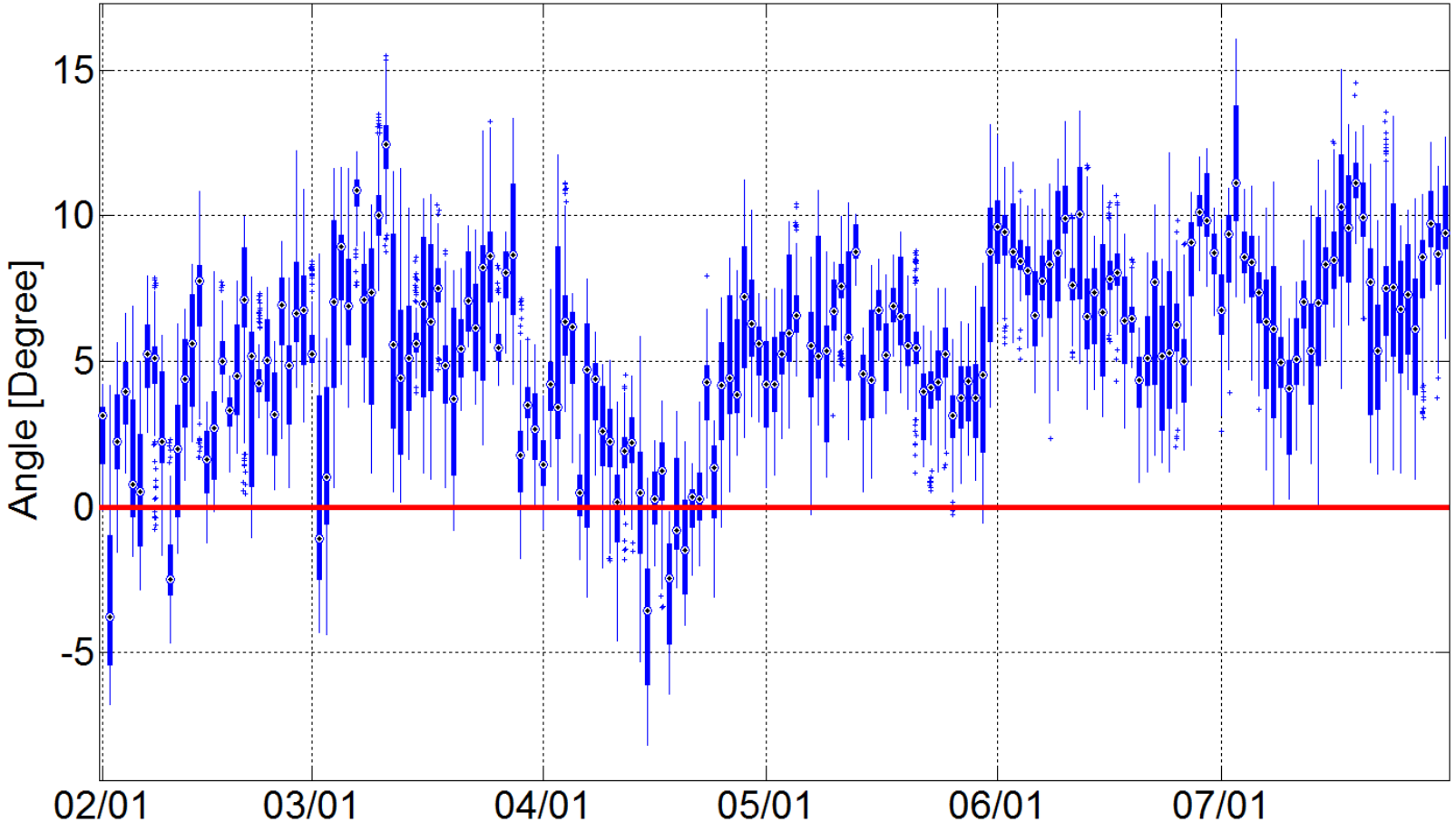
West 6-North 7



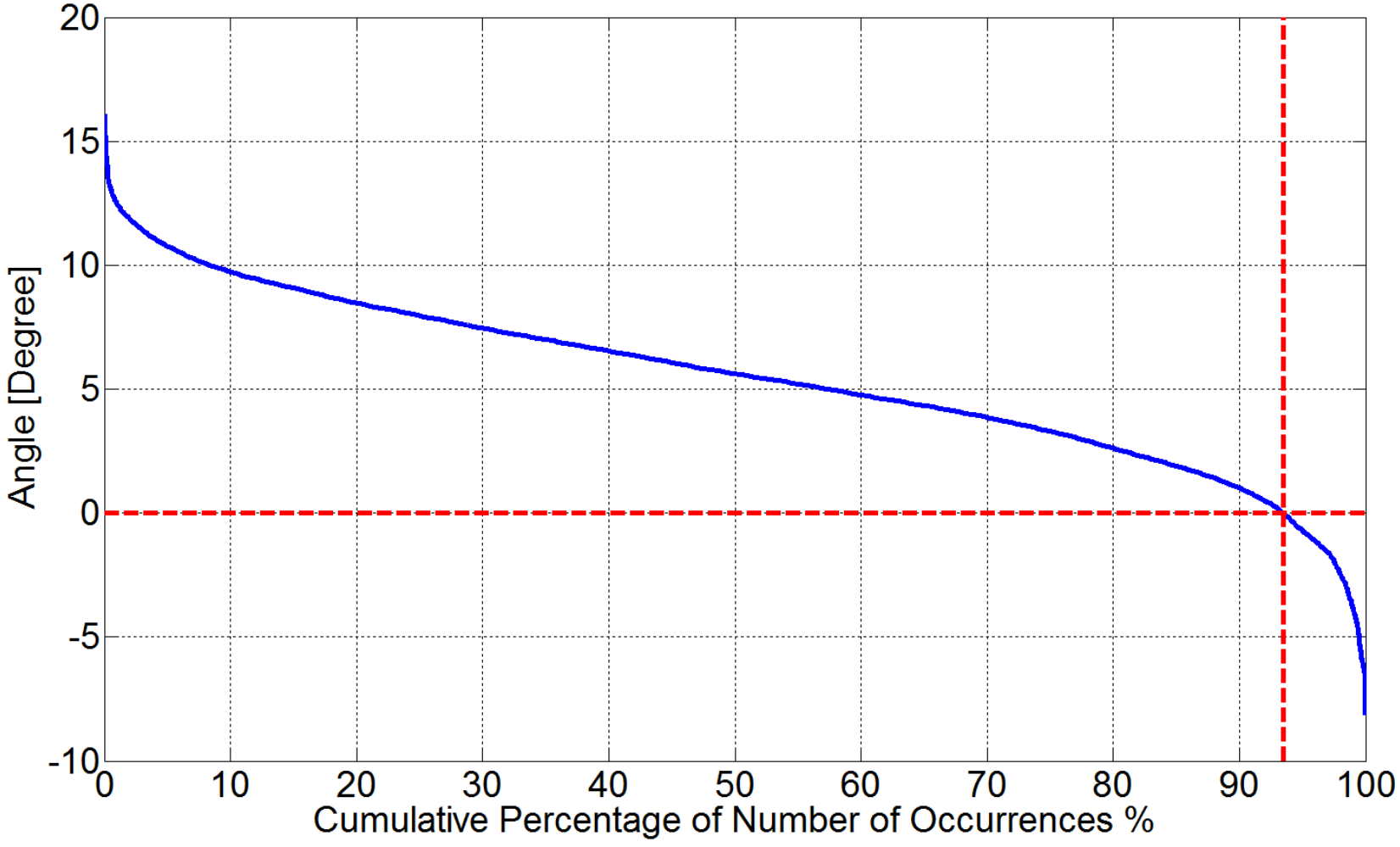
West 6-North 7



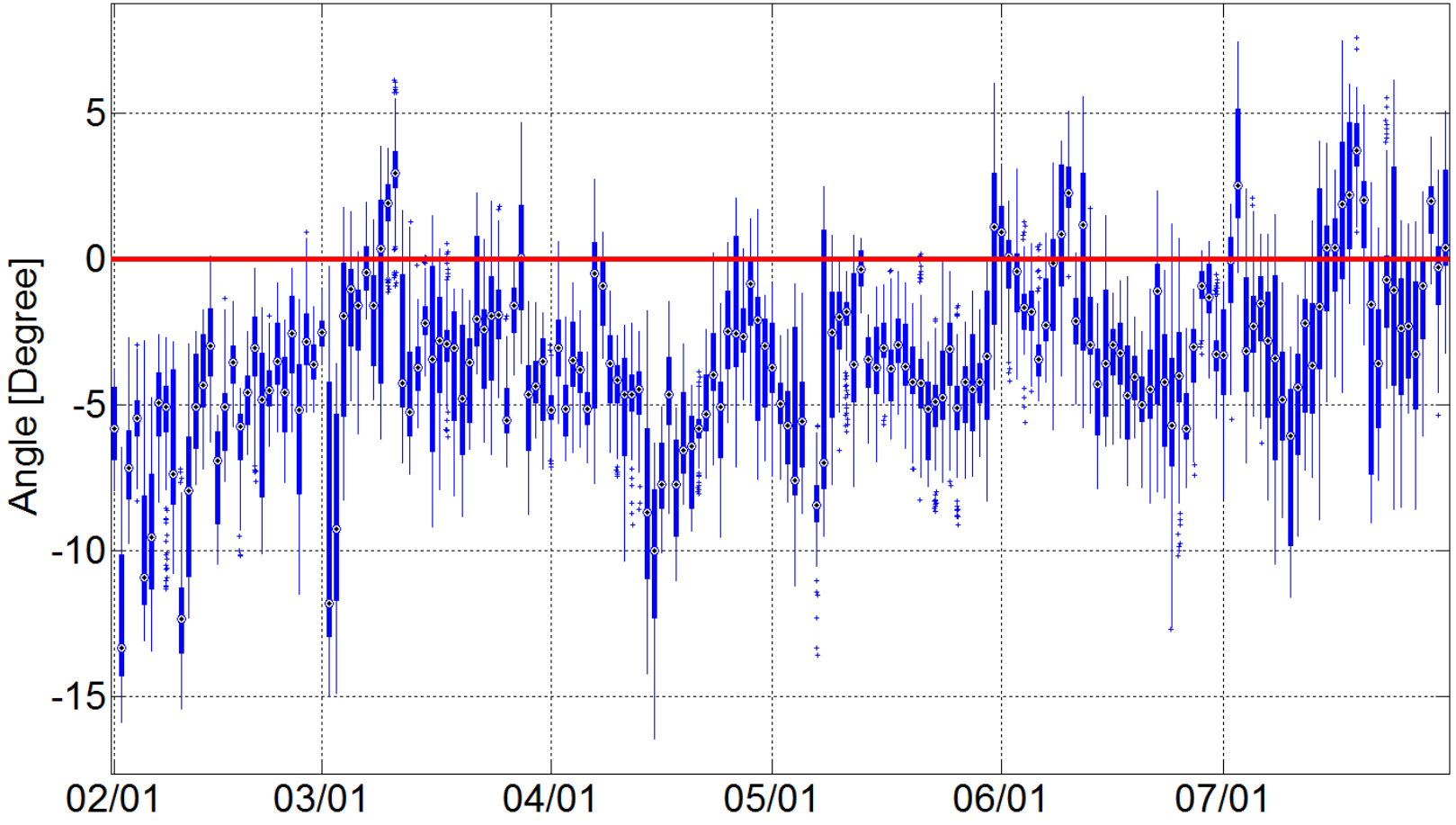
North 1-North 7



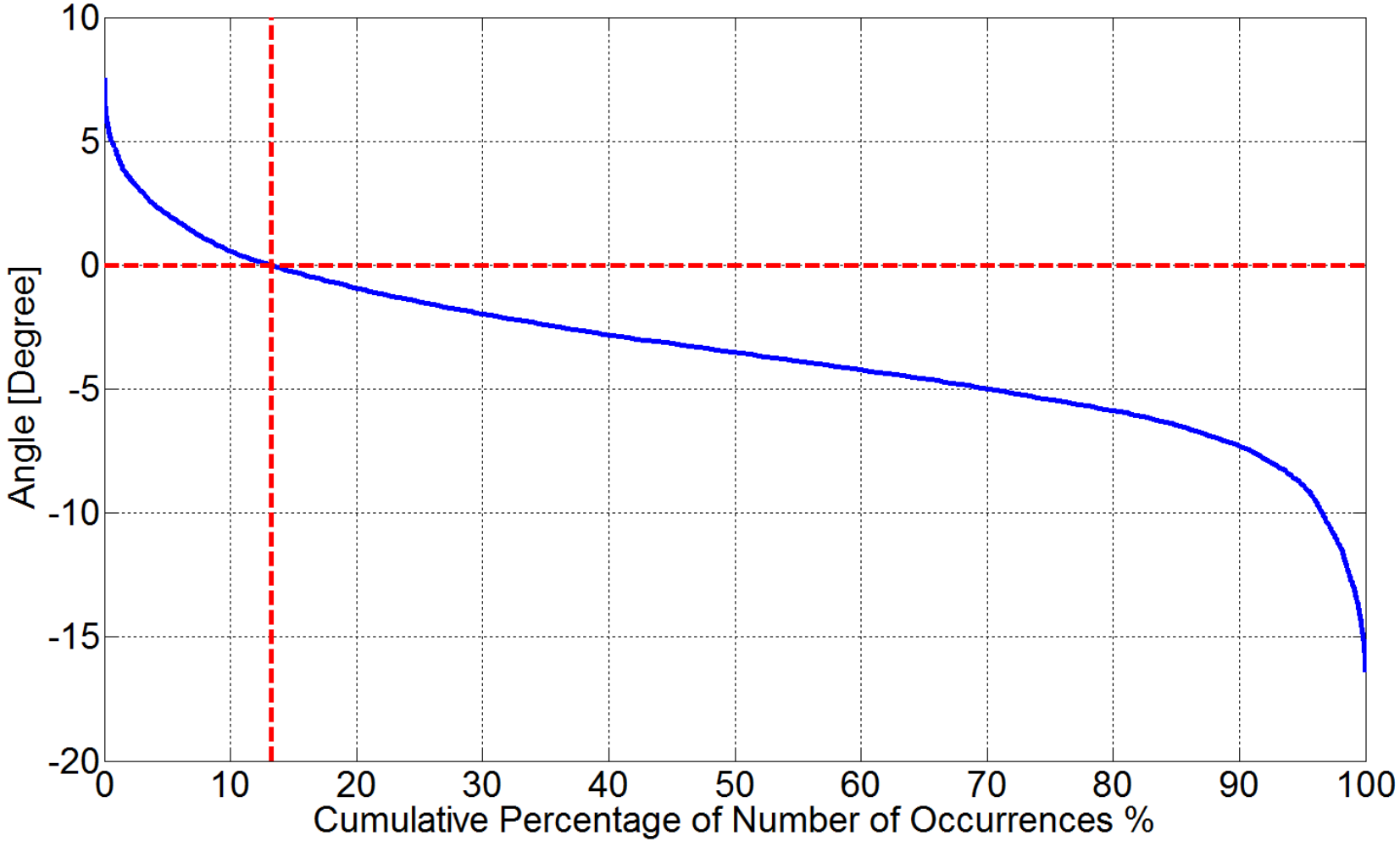
North 1-North 7



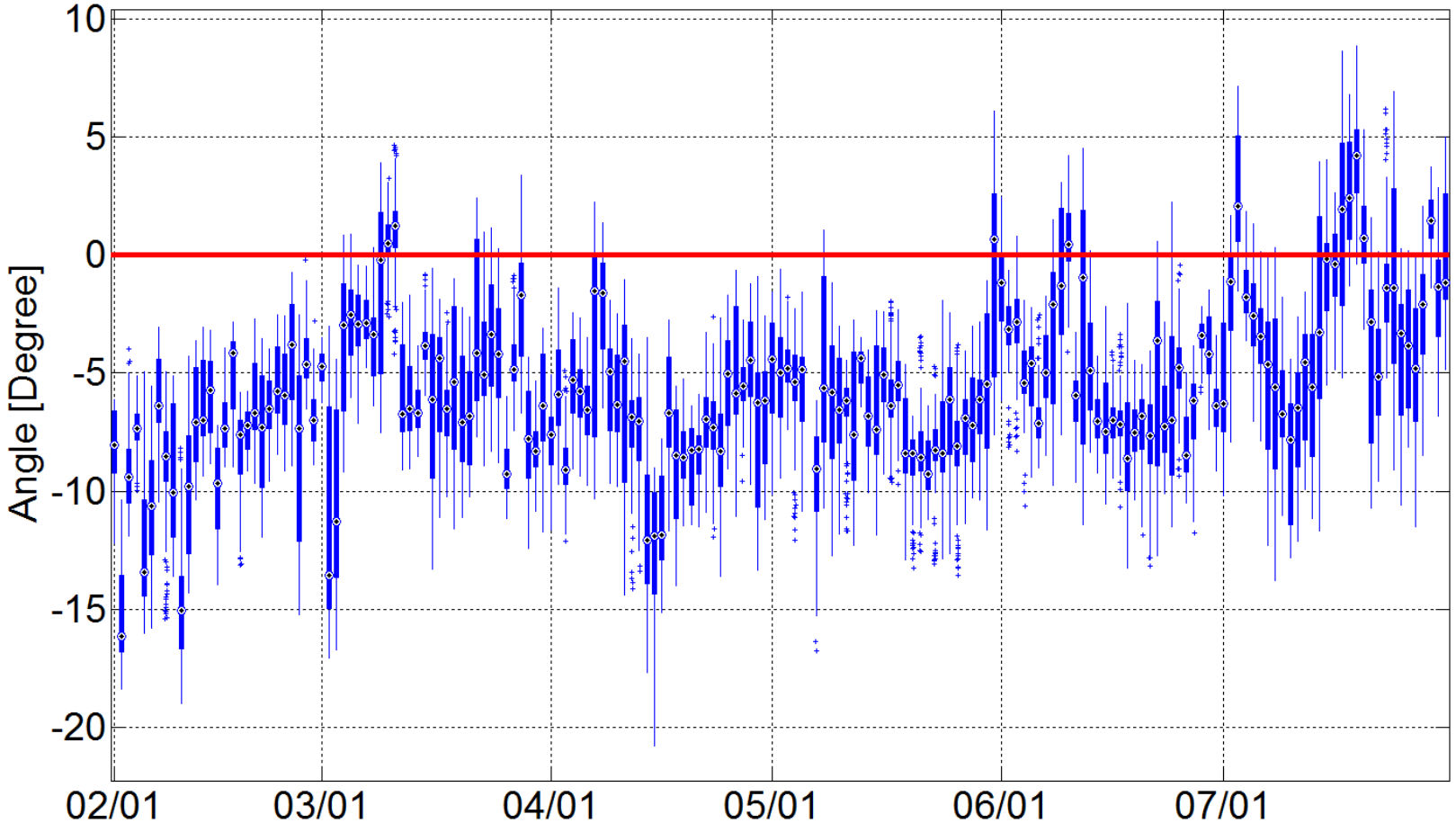
North 4-North 7



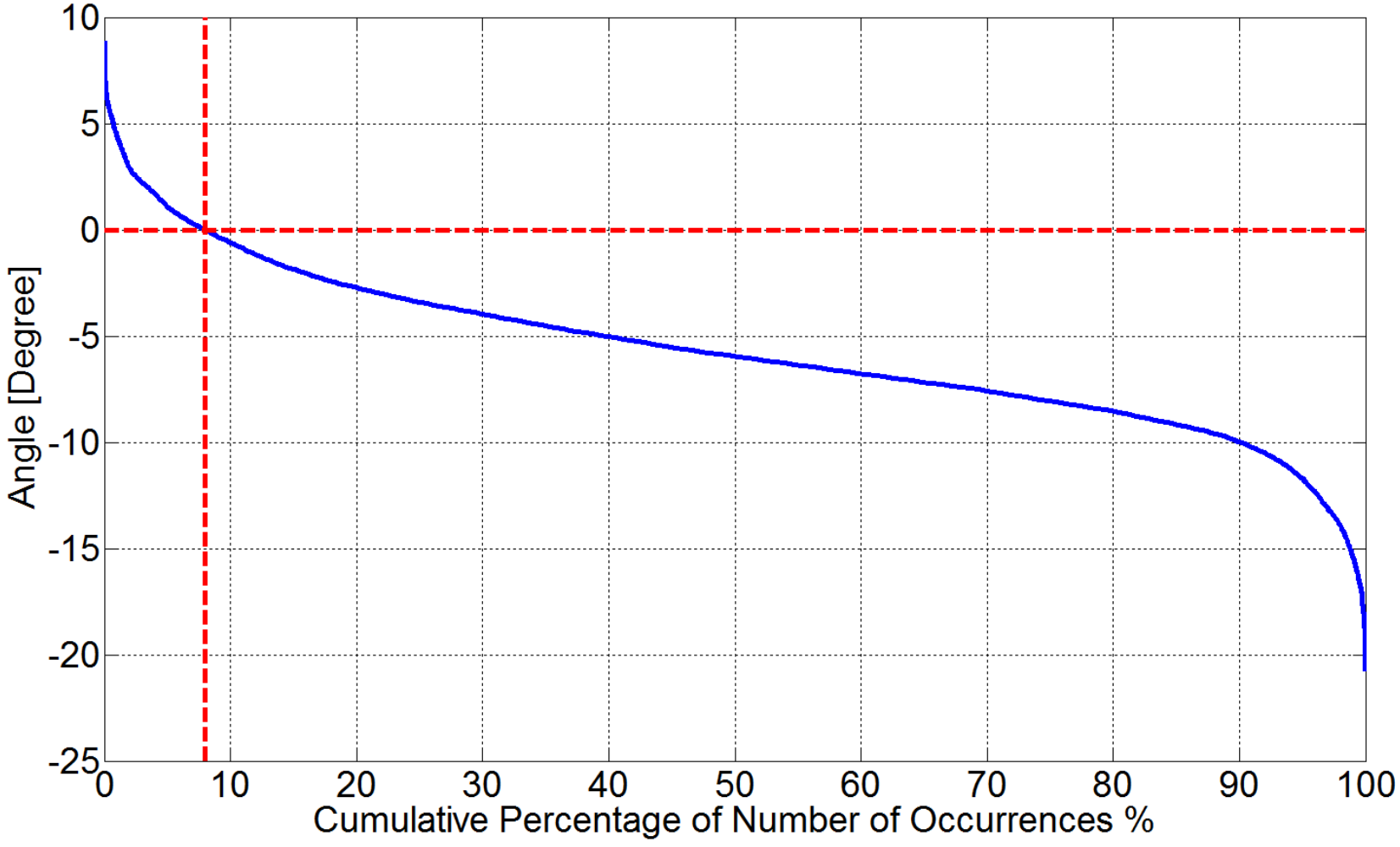
North 4-North 7



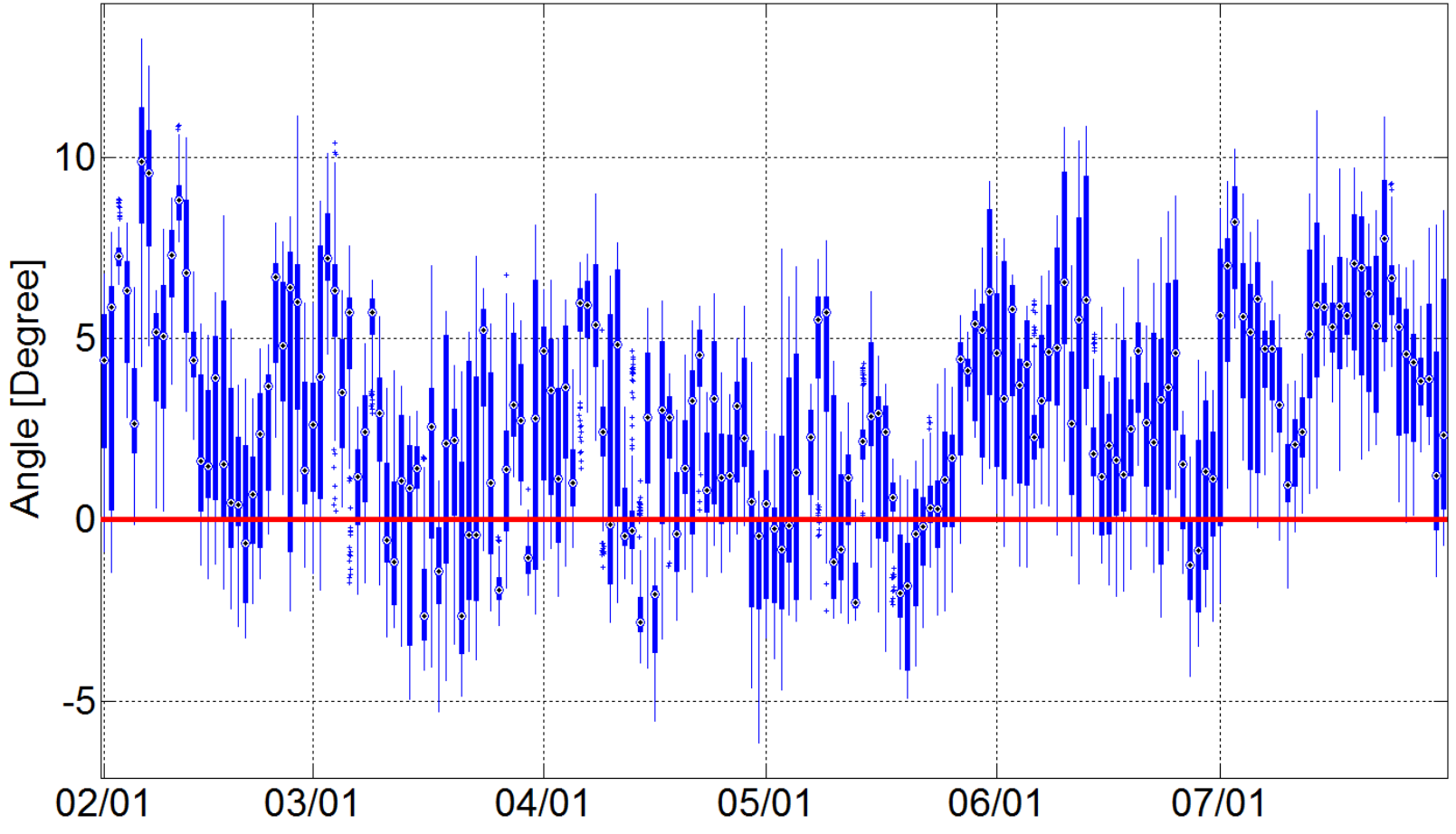
North 5-North 7



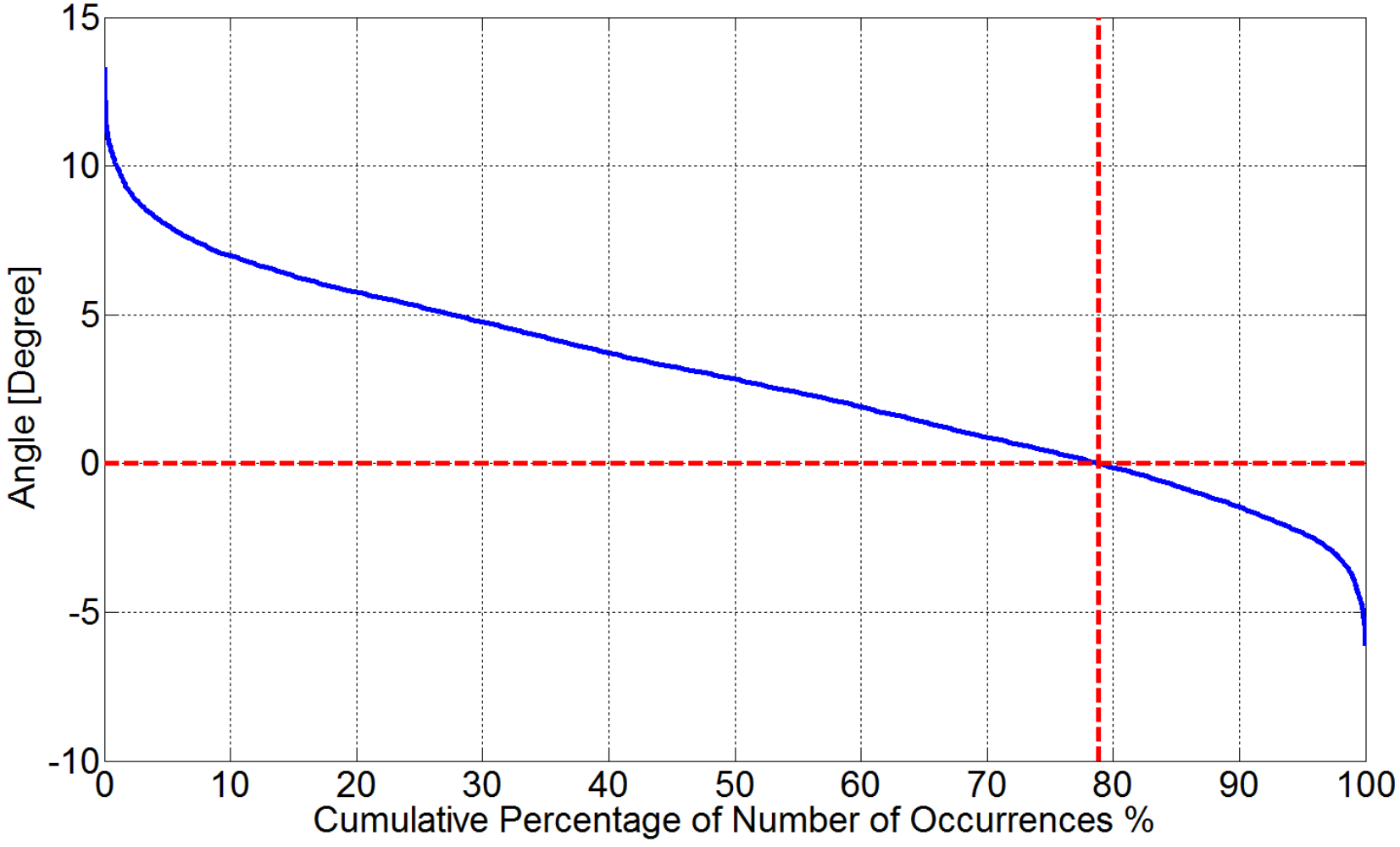
North 5-North 7



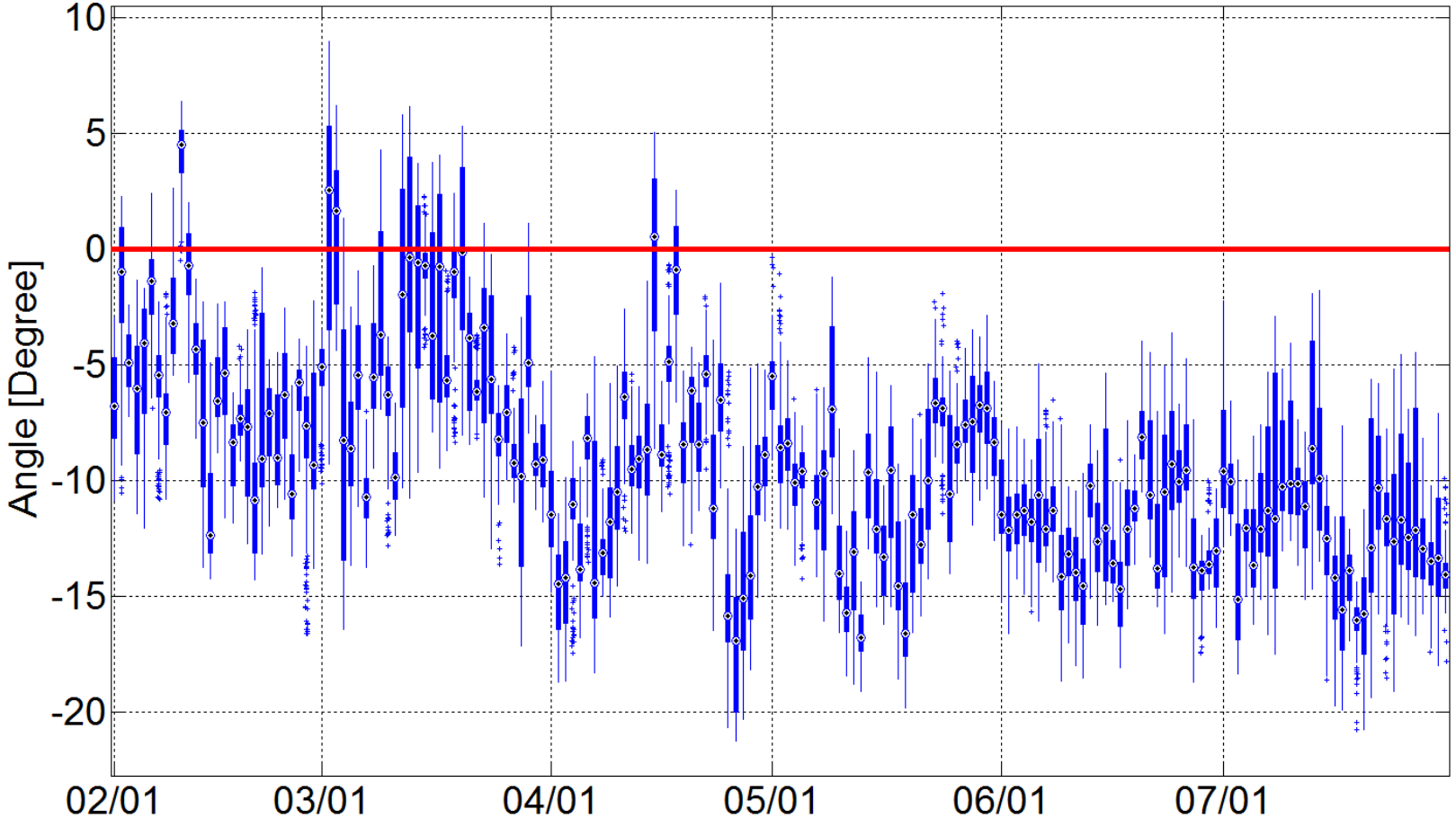
North 6-North 7



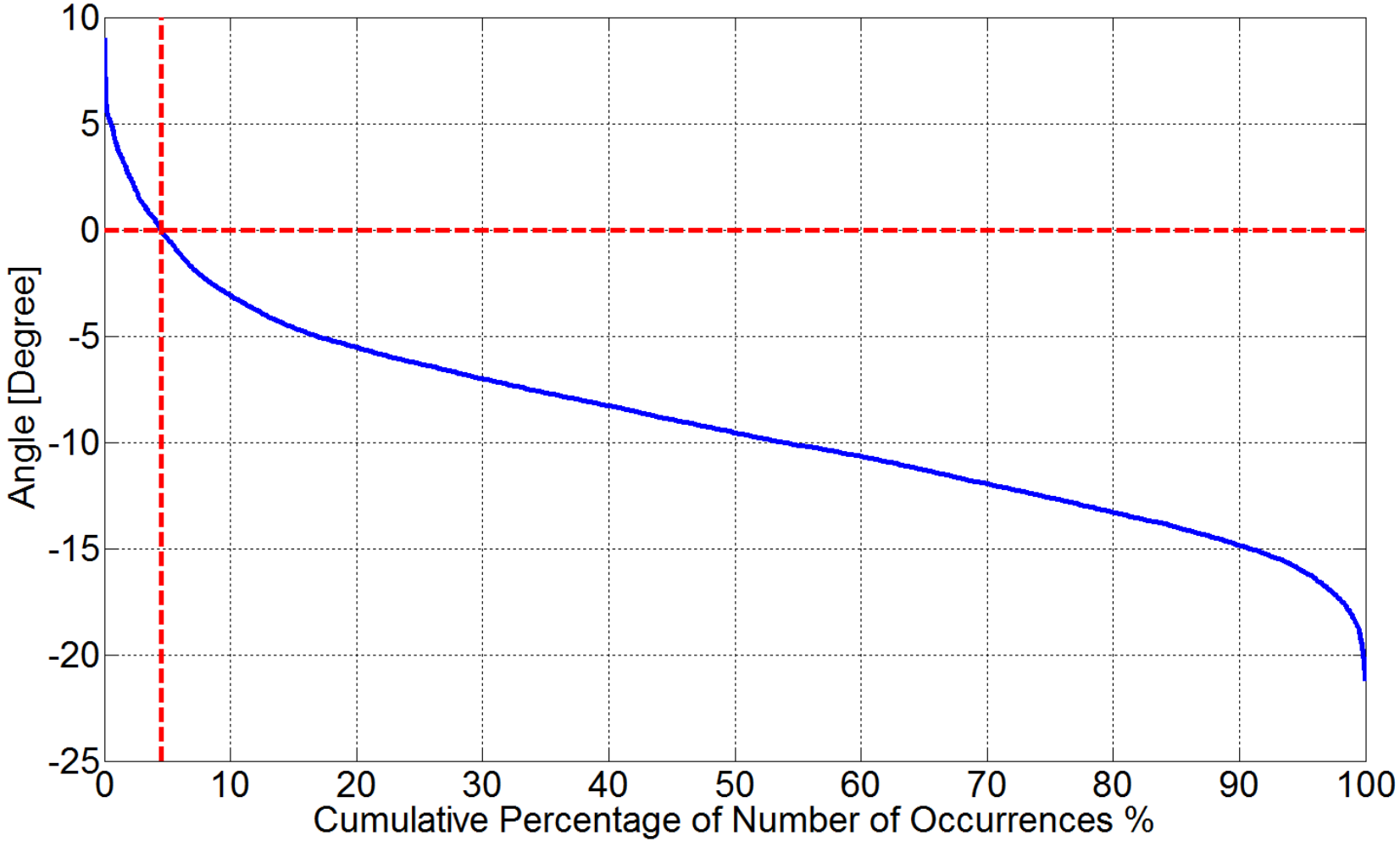
North 6-North 7



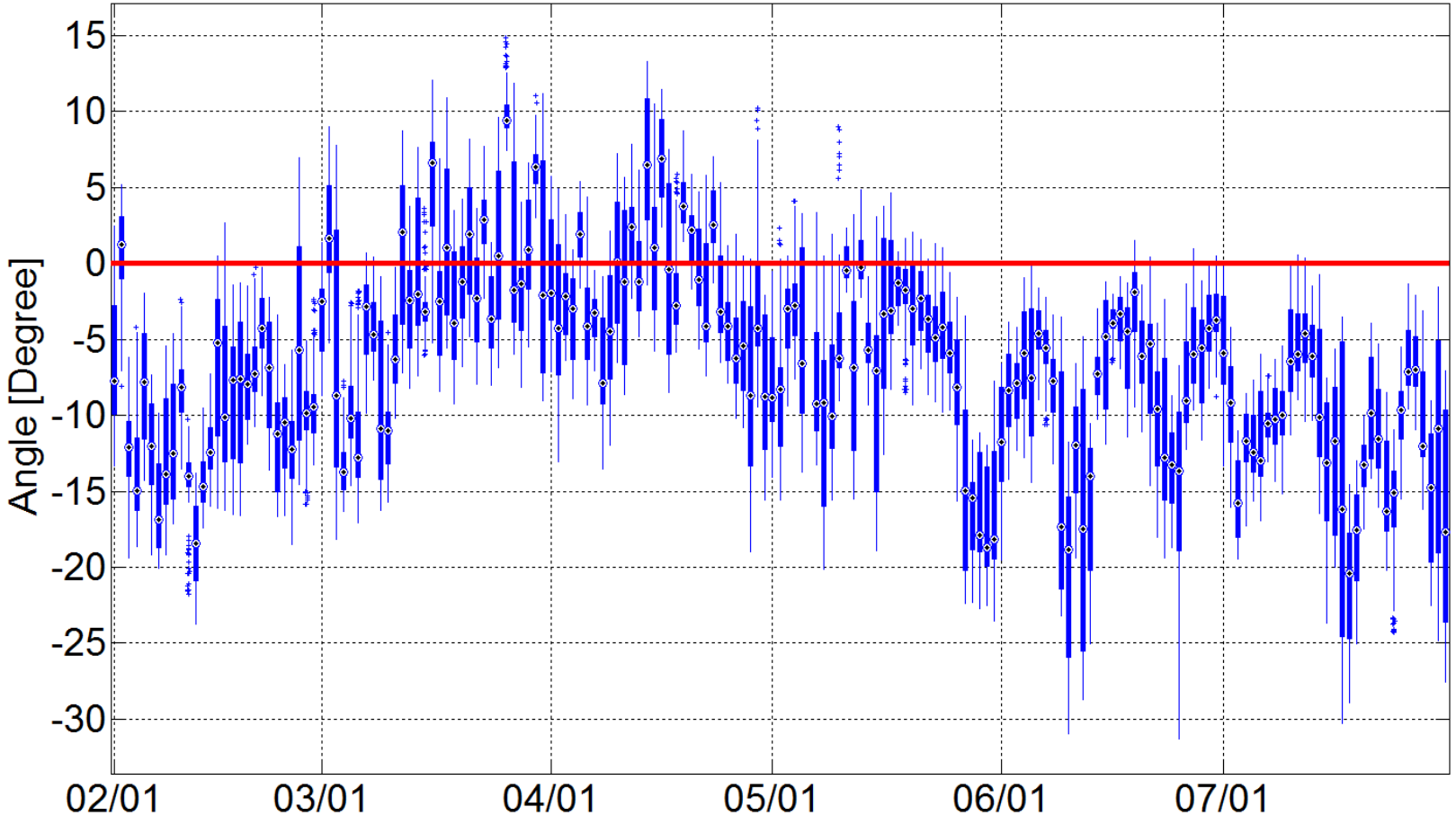
FarWest 2-North 7



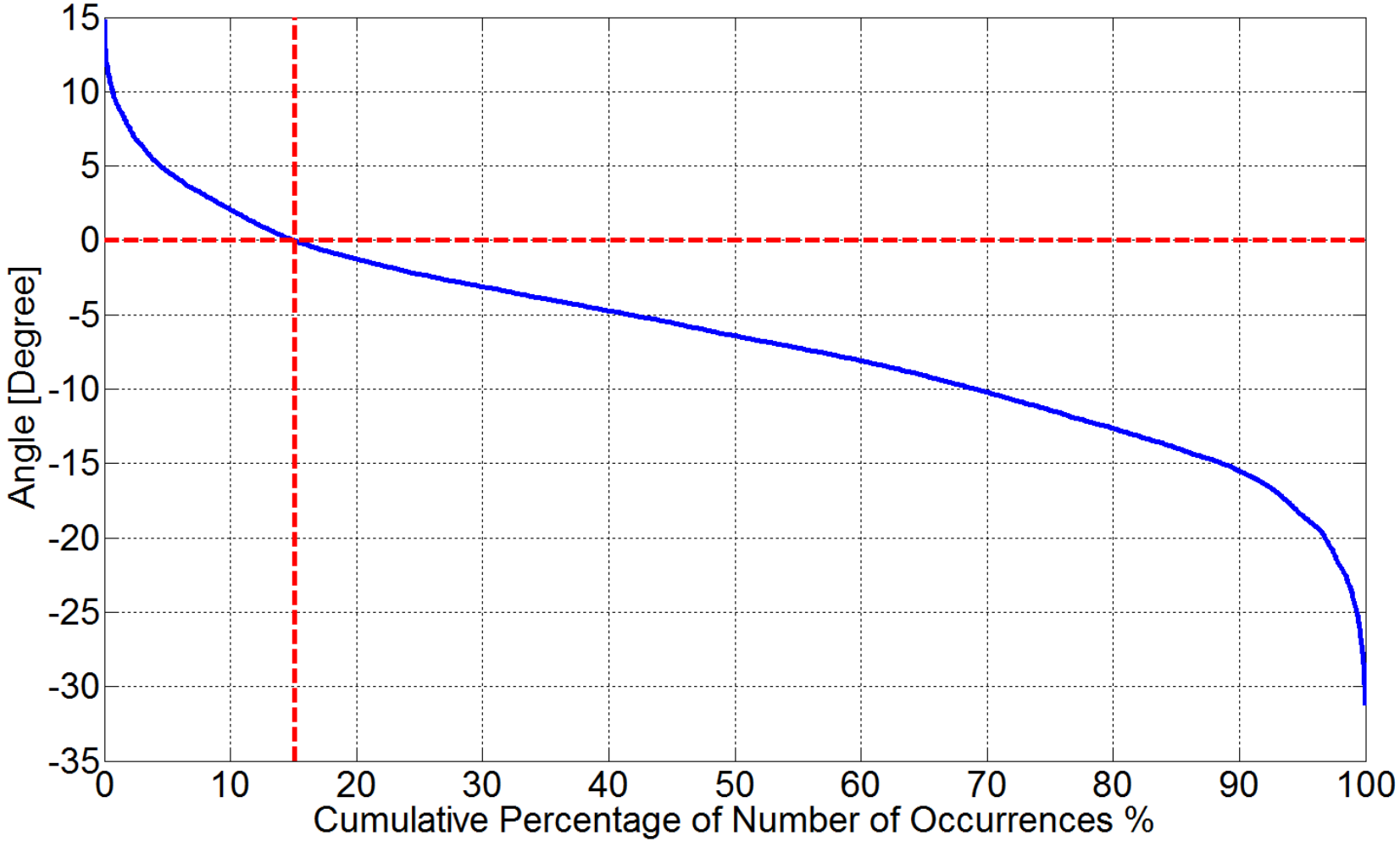
FarWest 2-North 7



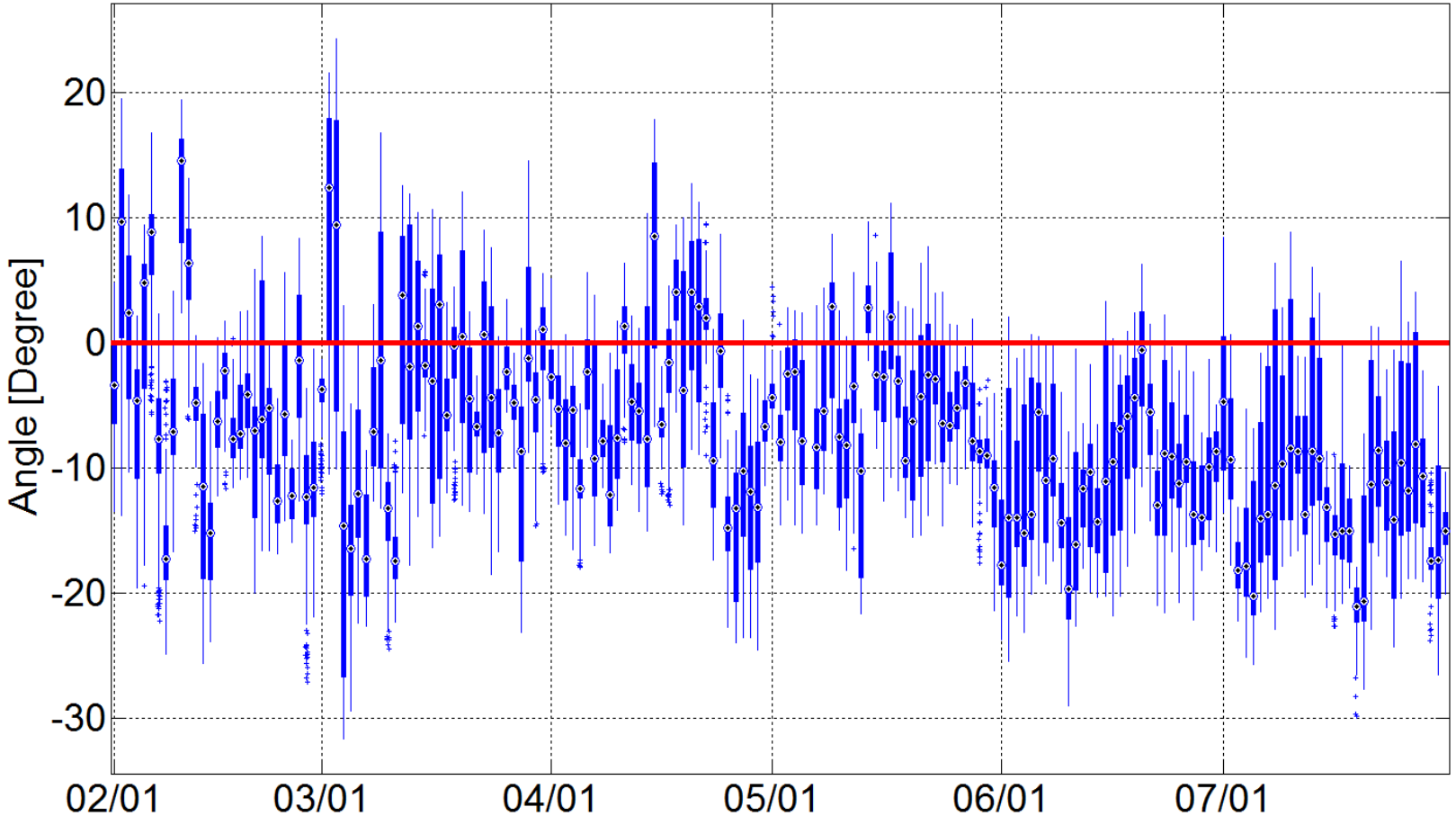
West 4-North 7



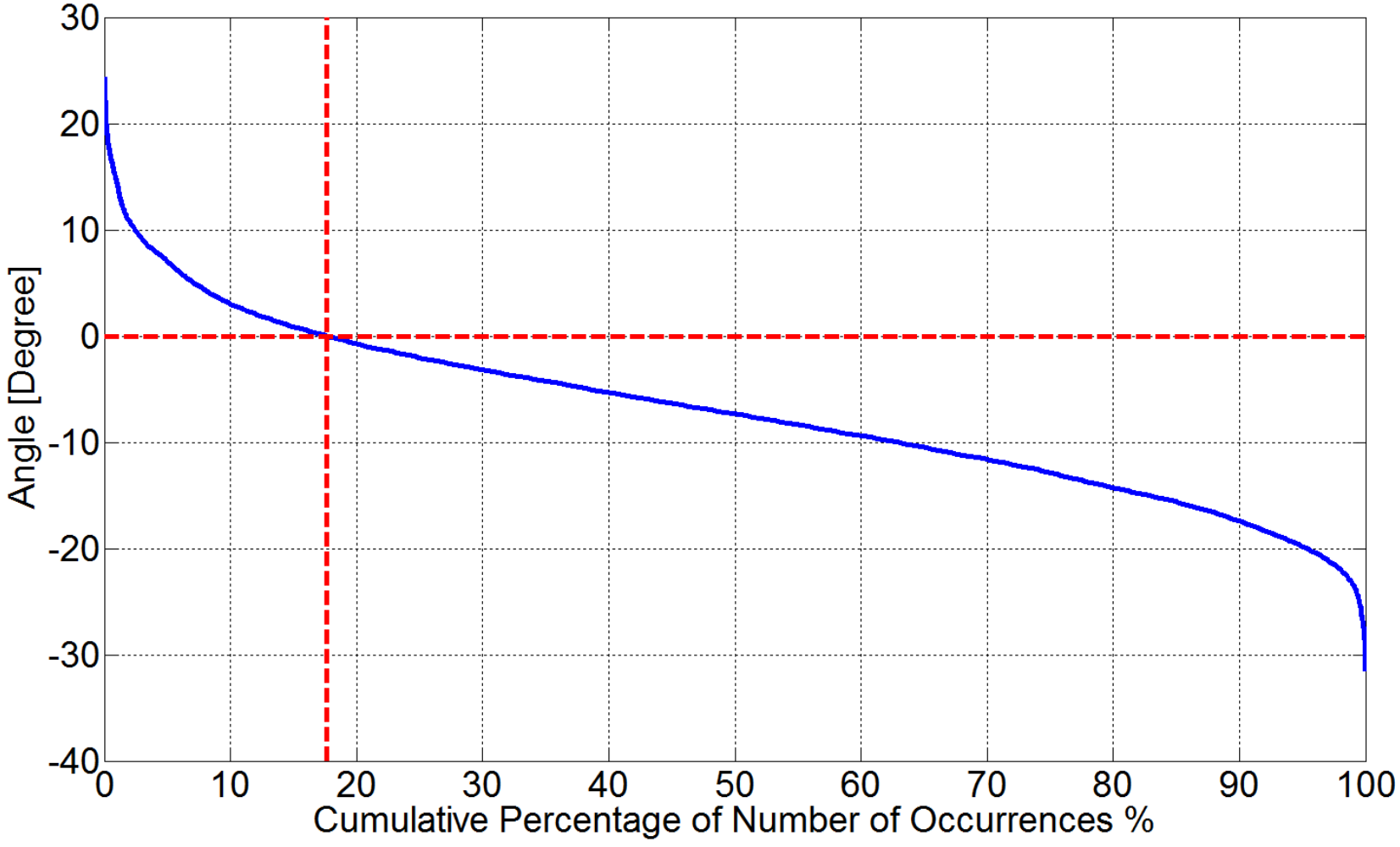
West 4-North 7



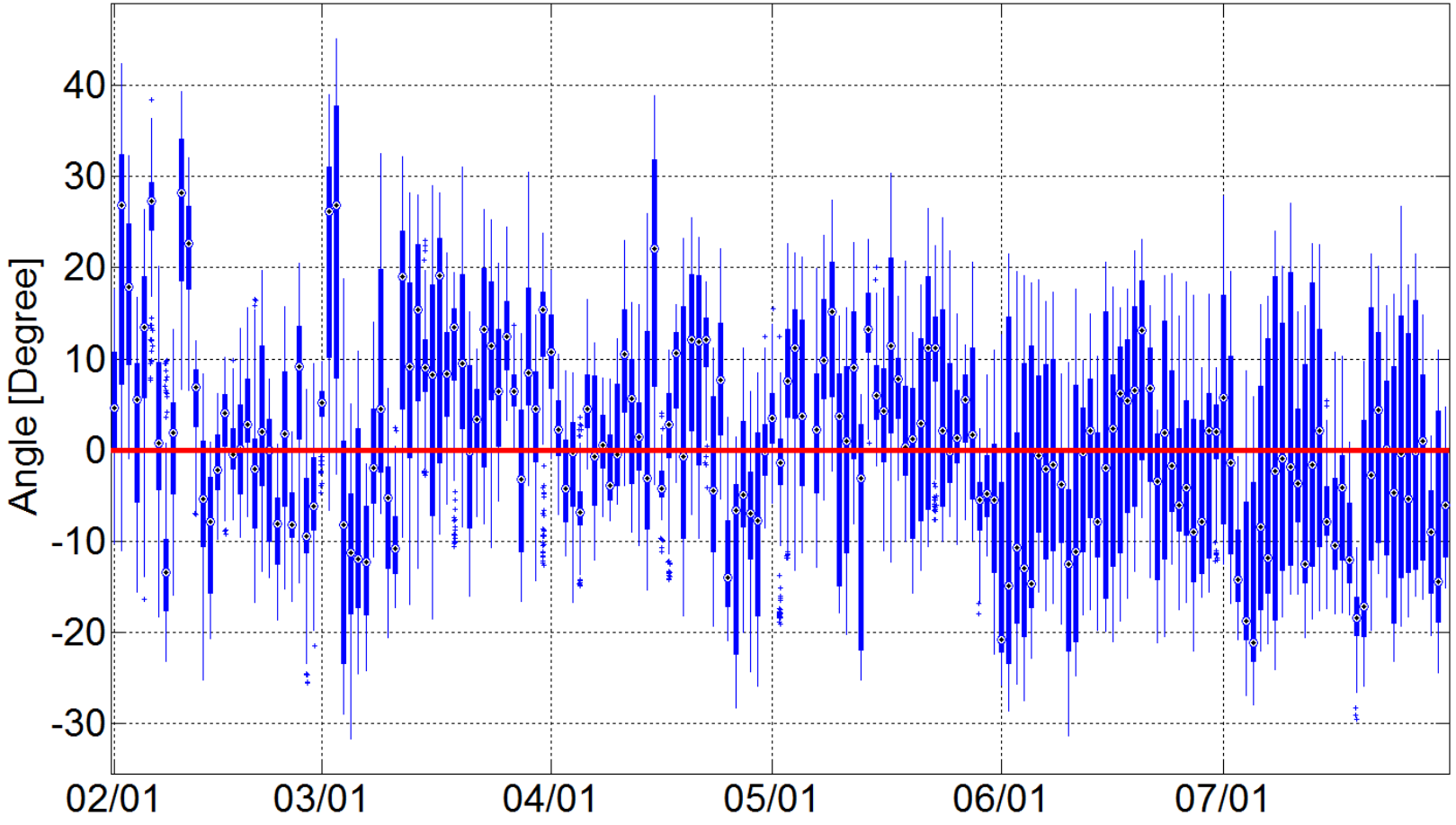
Coast 2-North 7



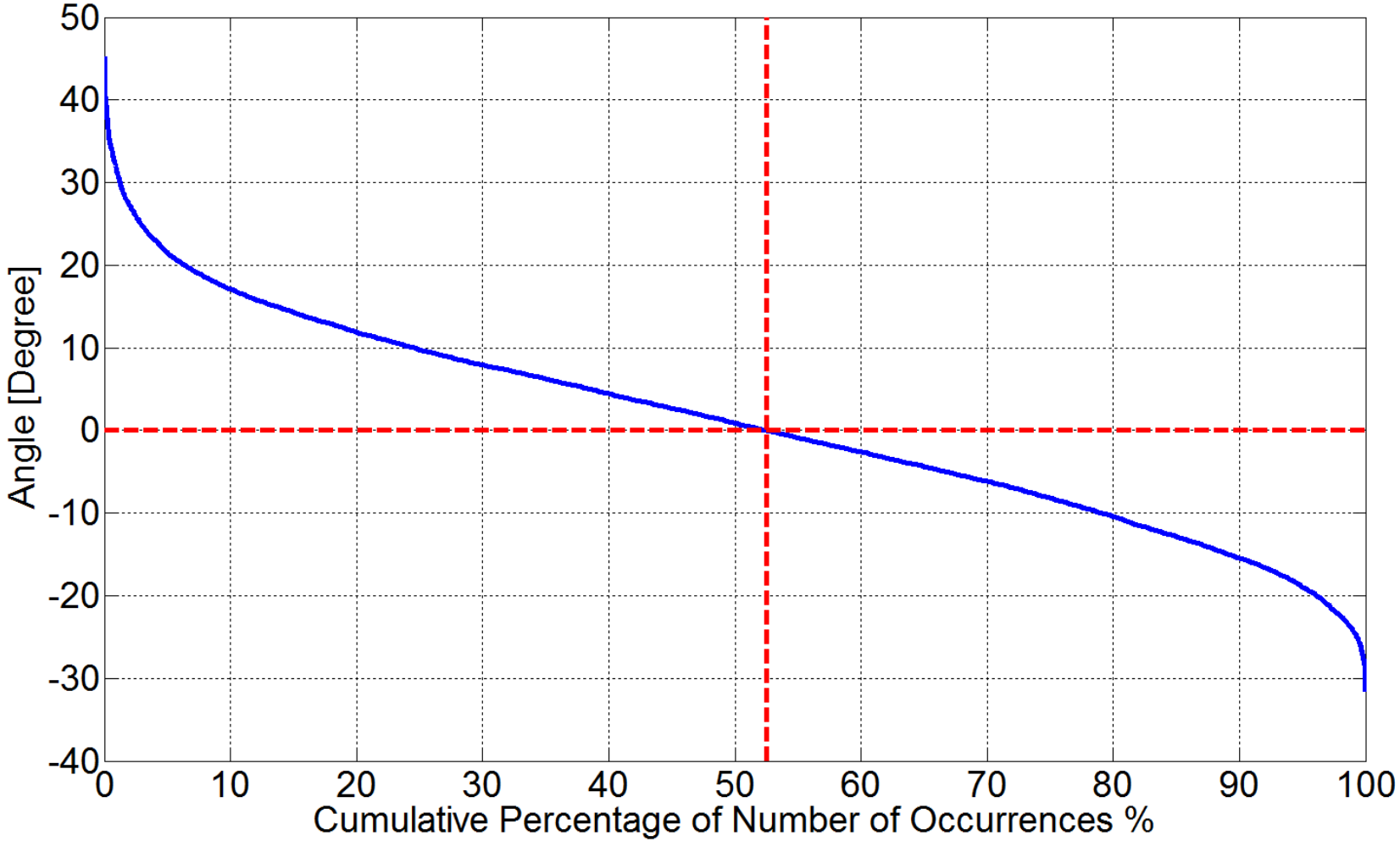
Coast 2-North 7



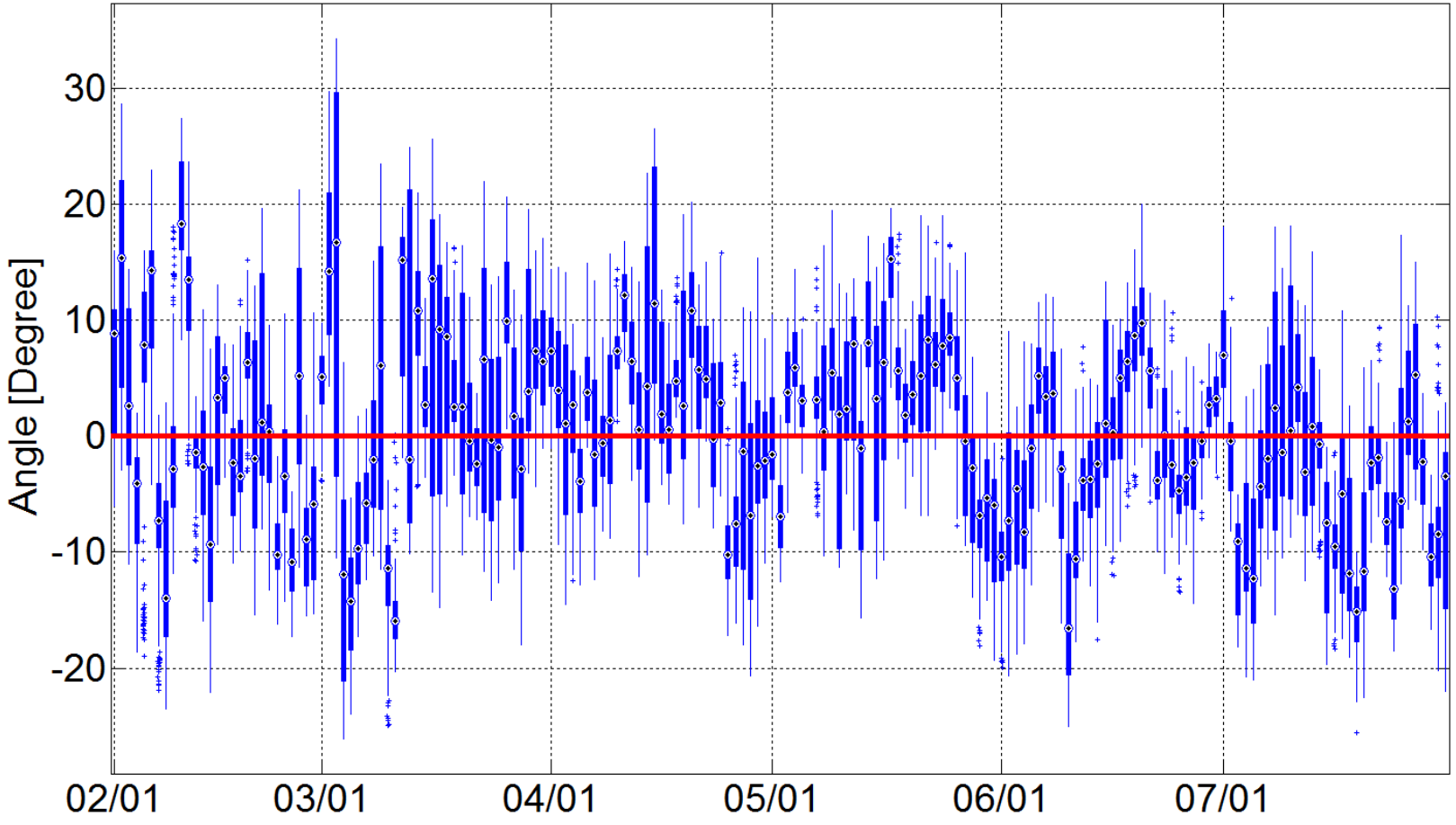
Coast 1-North 7



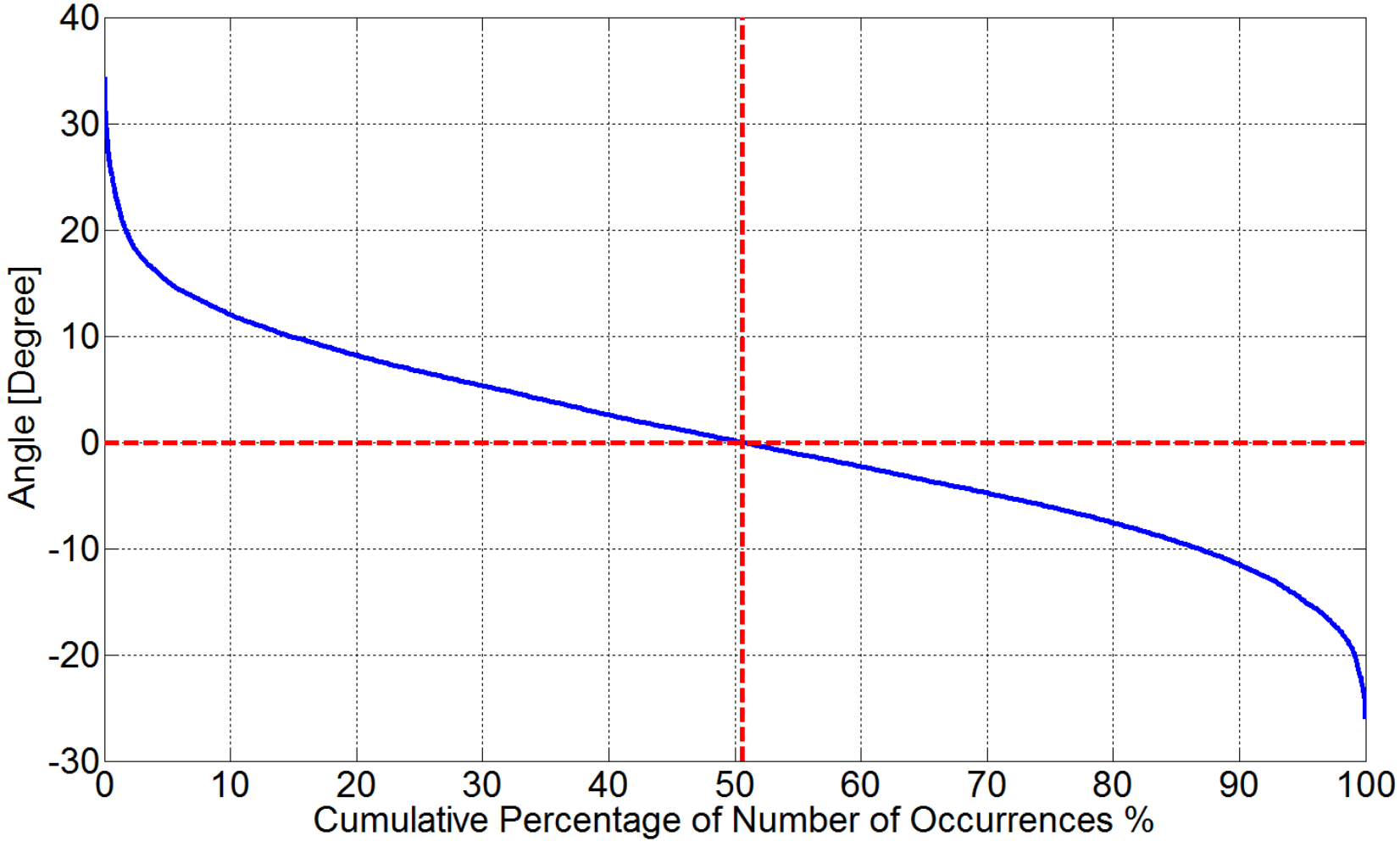
Coast 1-North 7



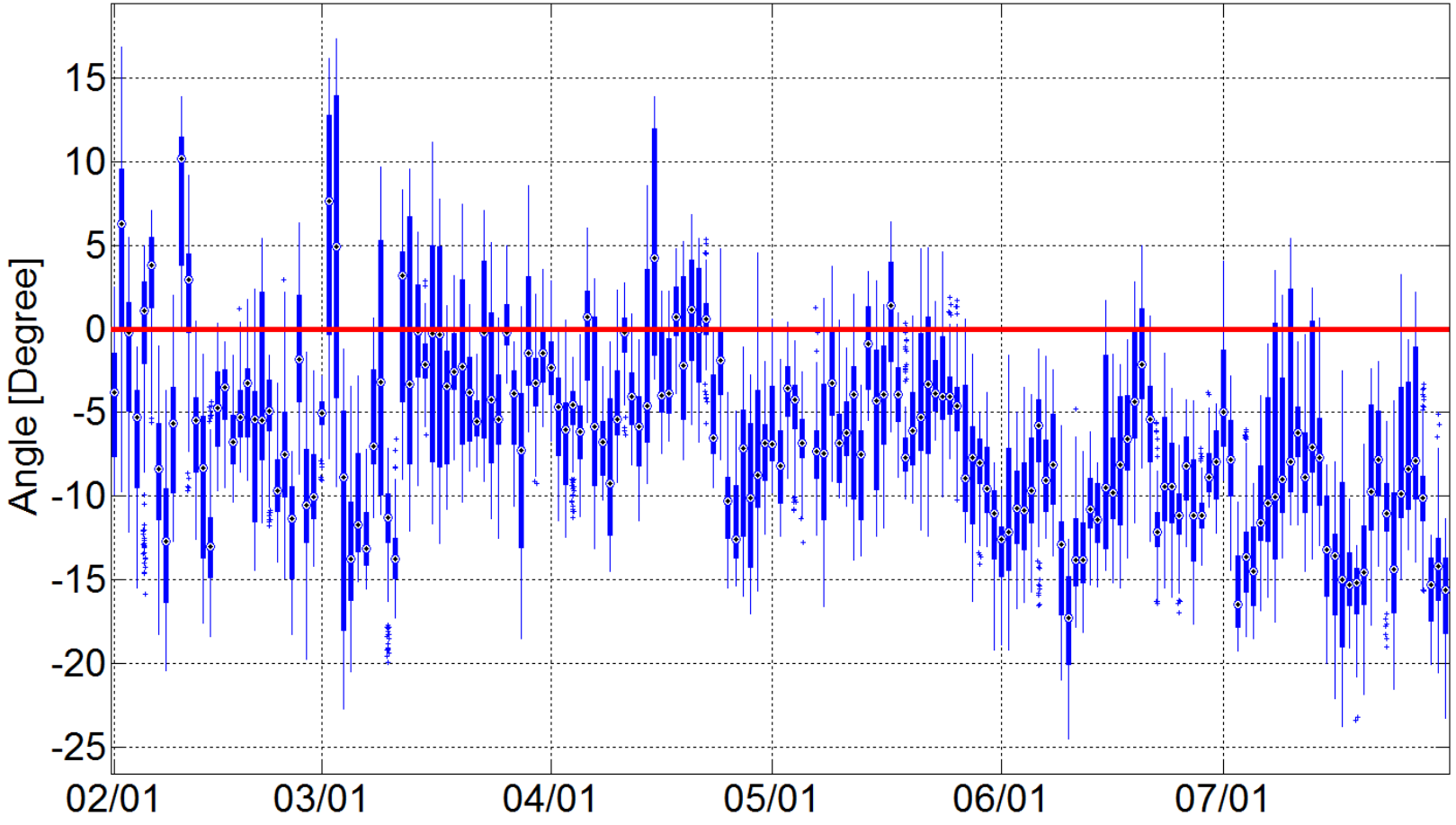
South 3-North 7



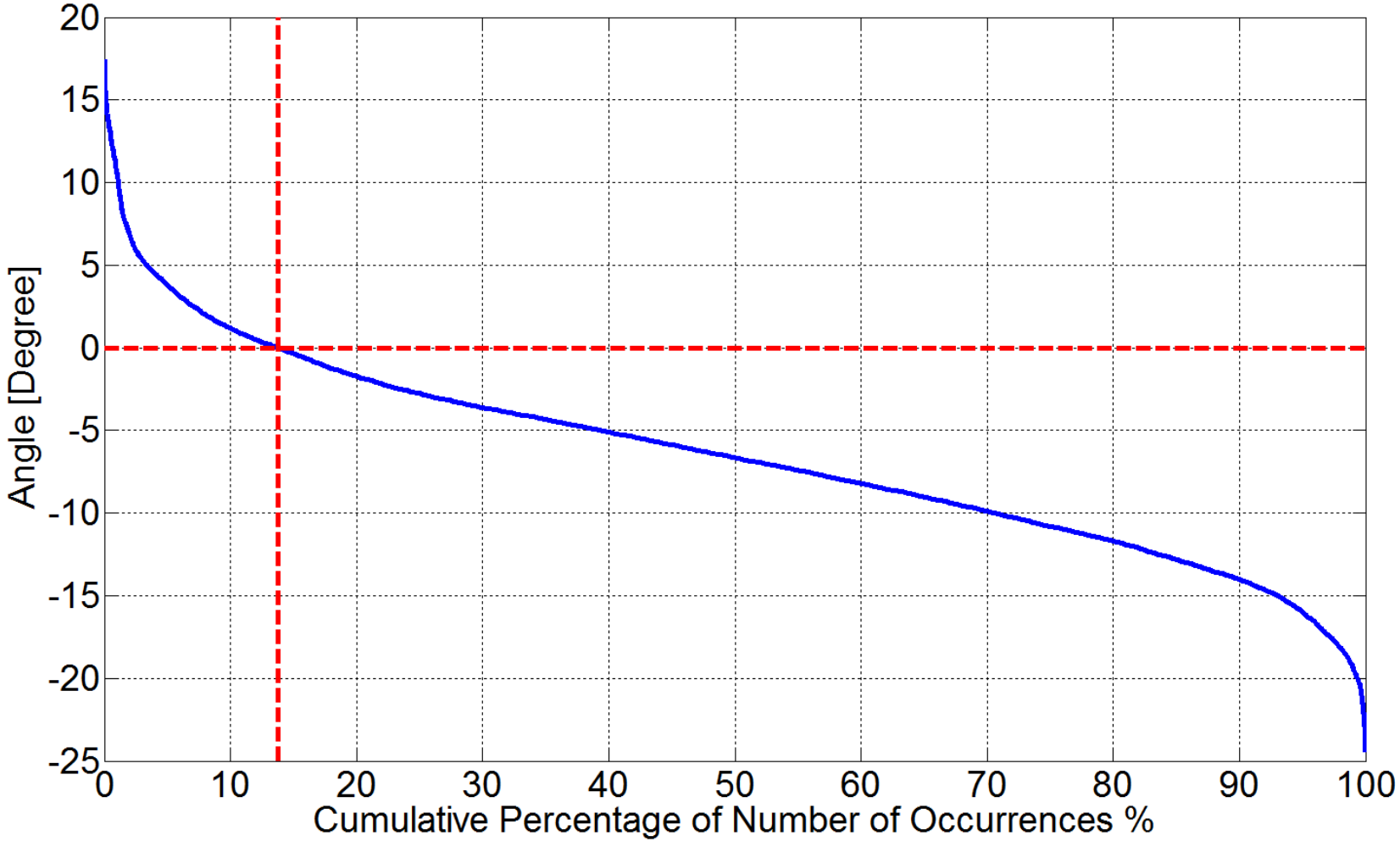
South 3-North 7



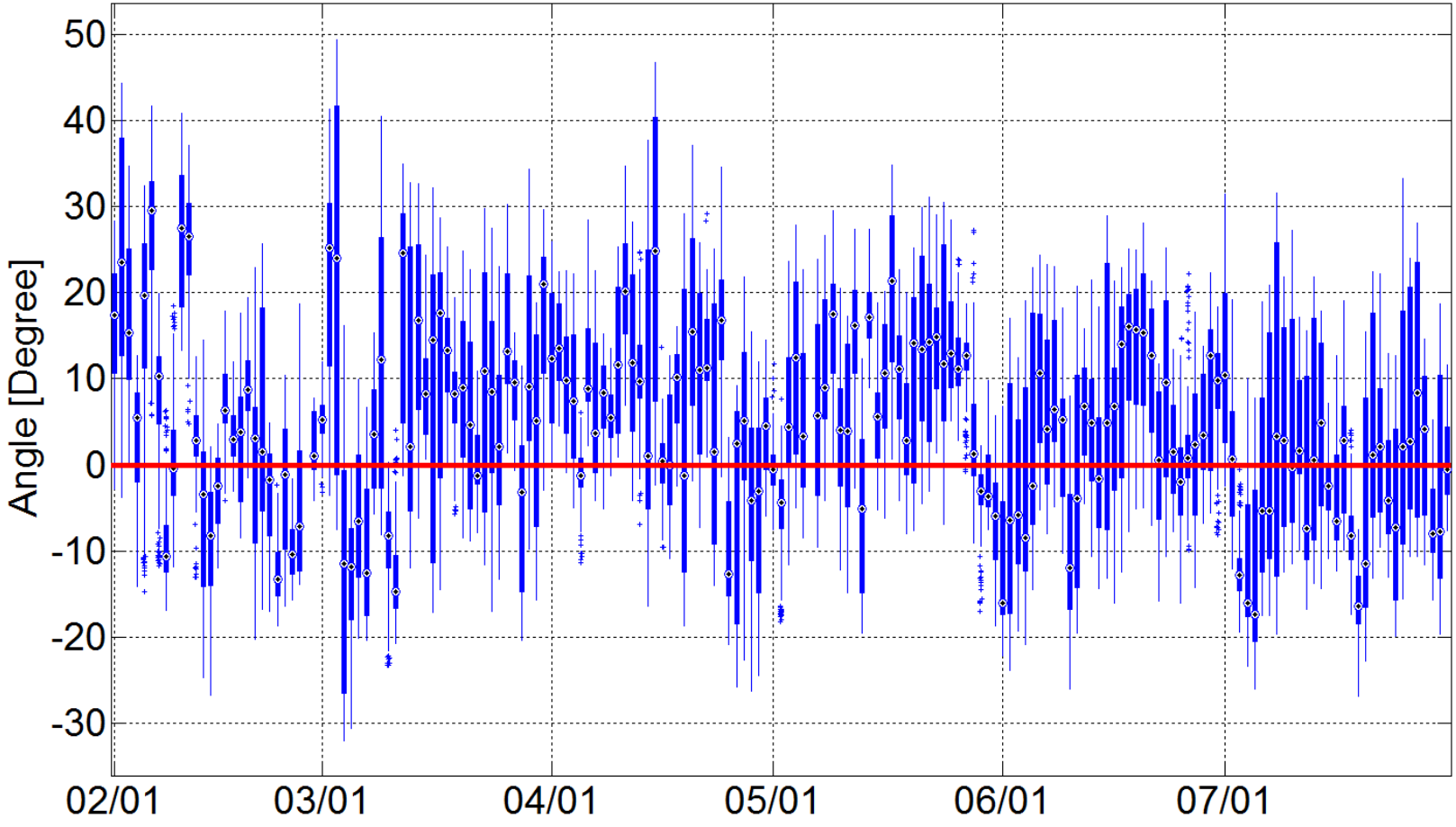
South 5-North 7



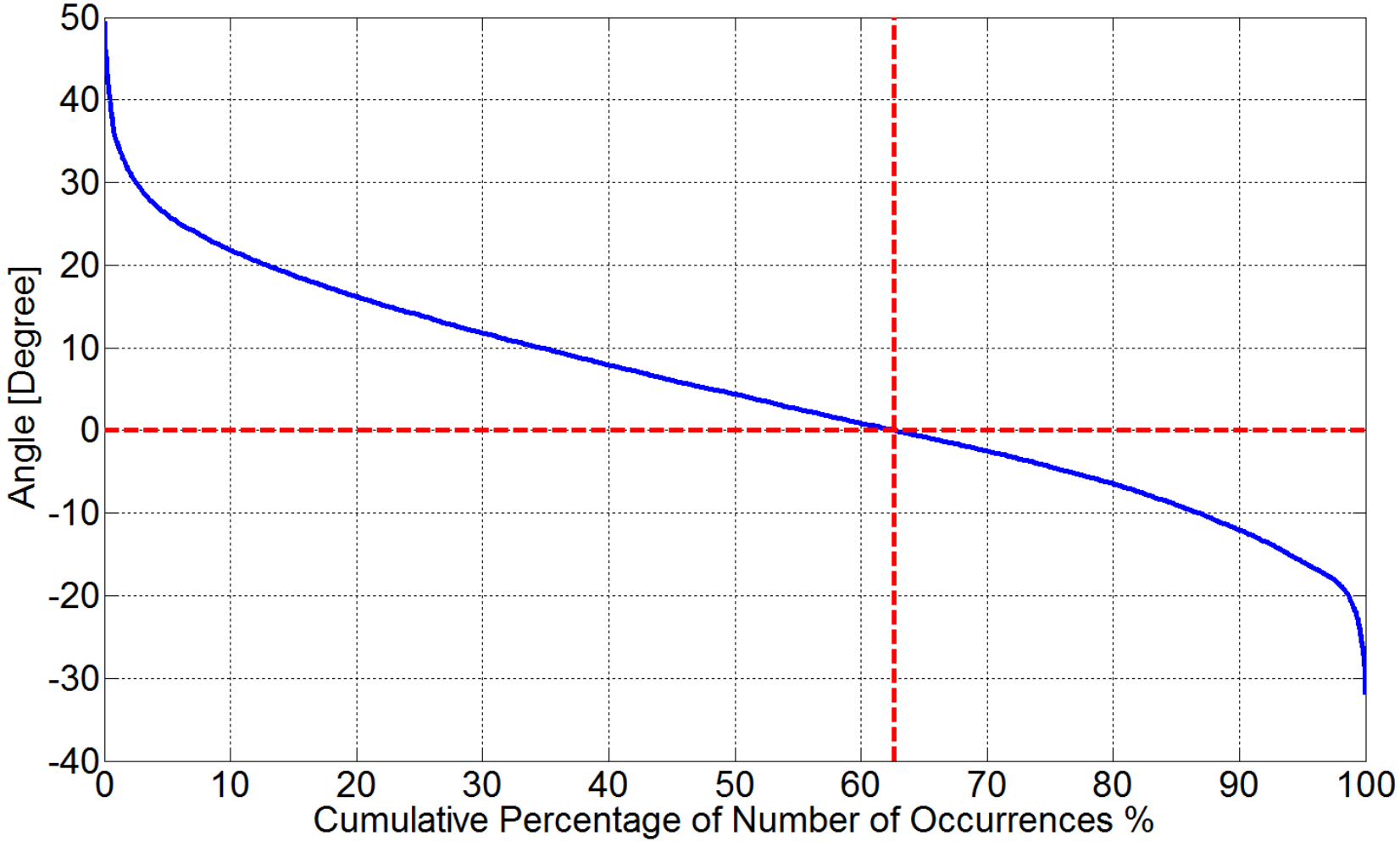
South 5-North 7



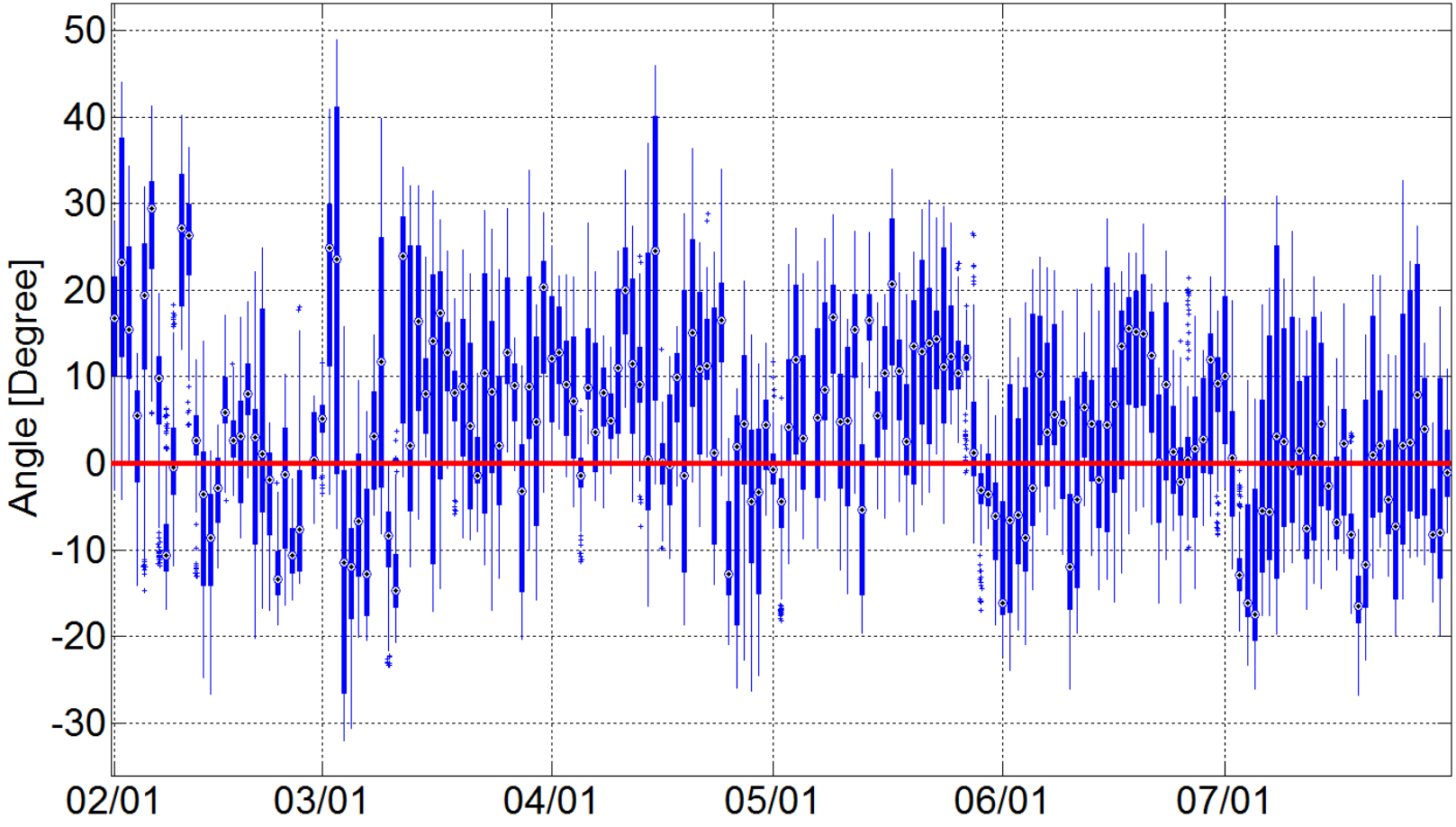
Coast 4-North 7



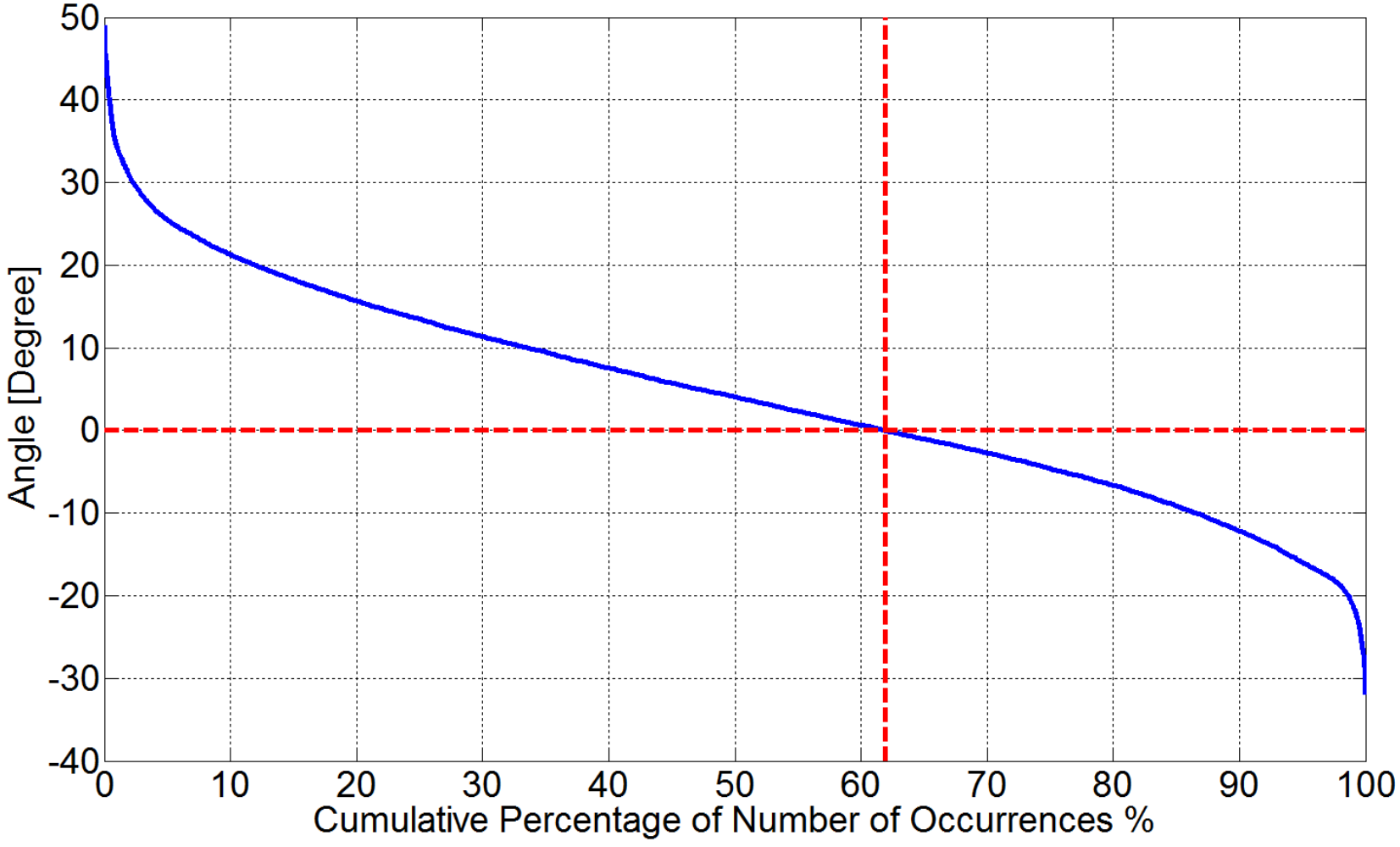
Coast 4-North 7



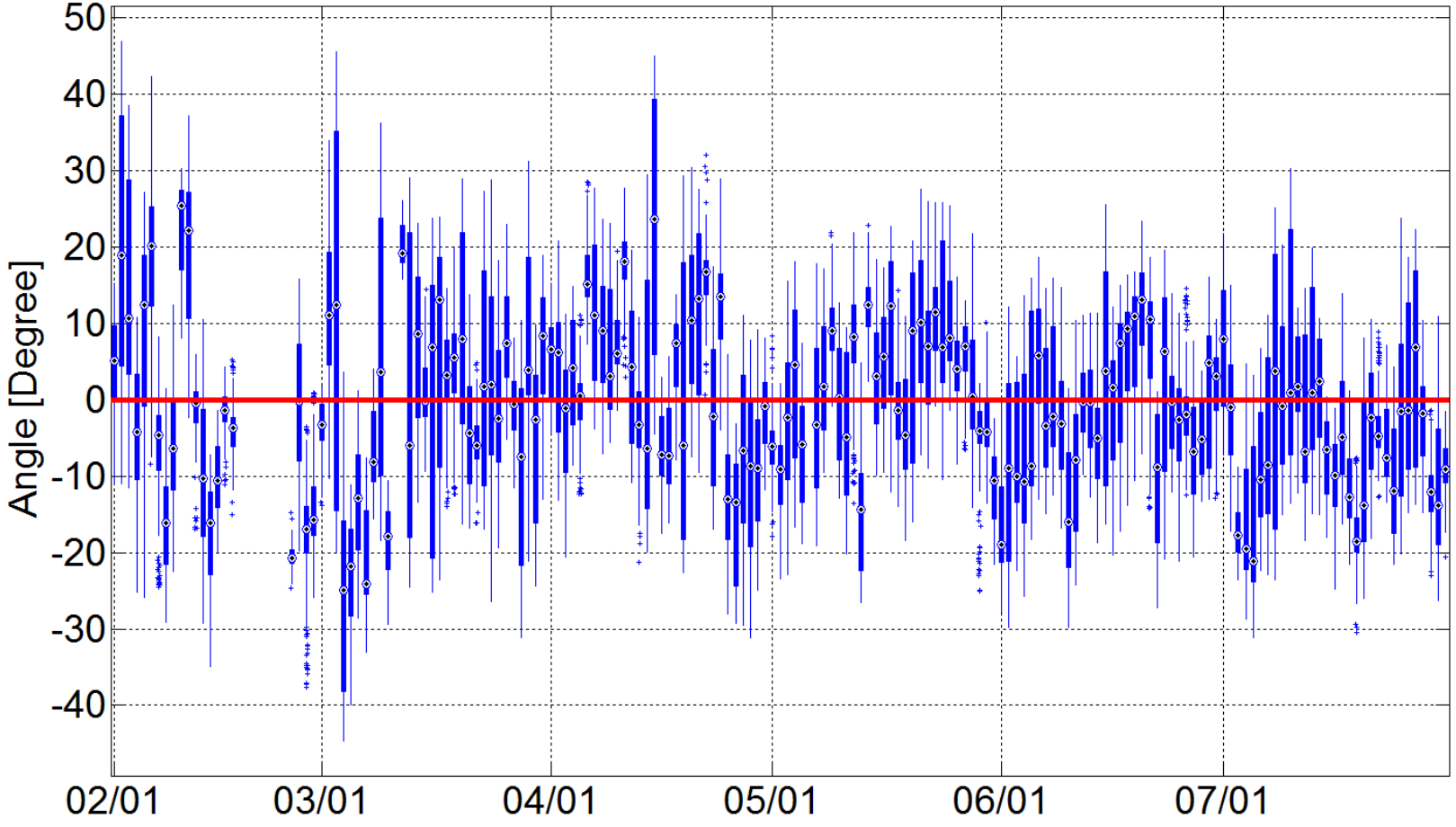
Coast 3-North 7



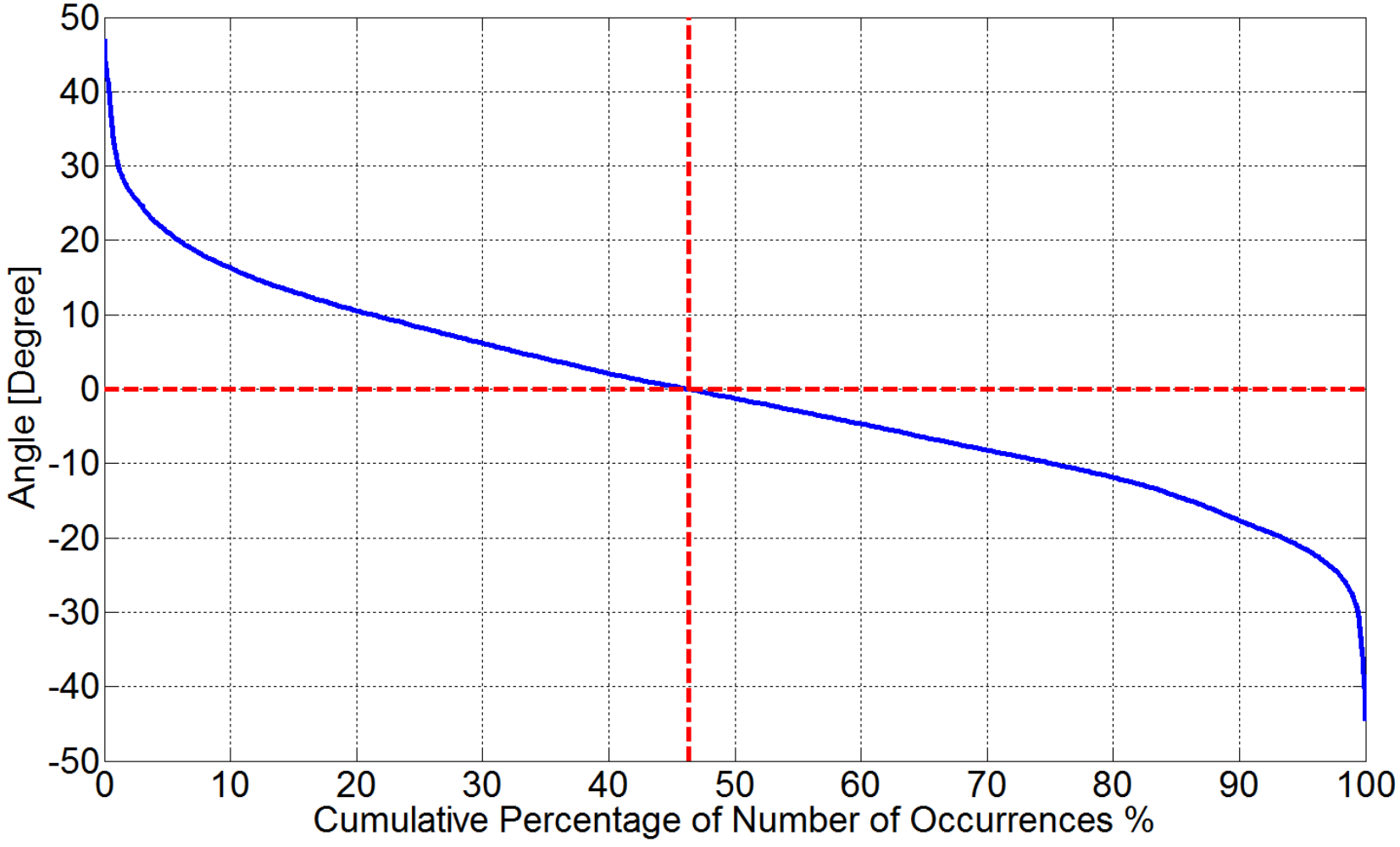
Coast 3-North 7



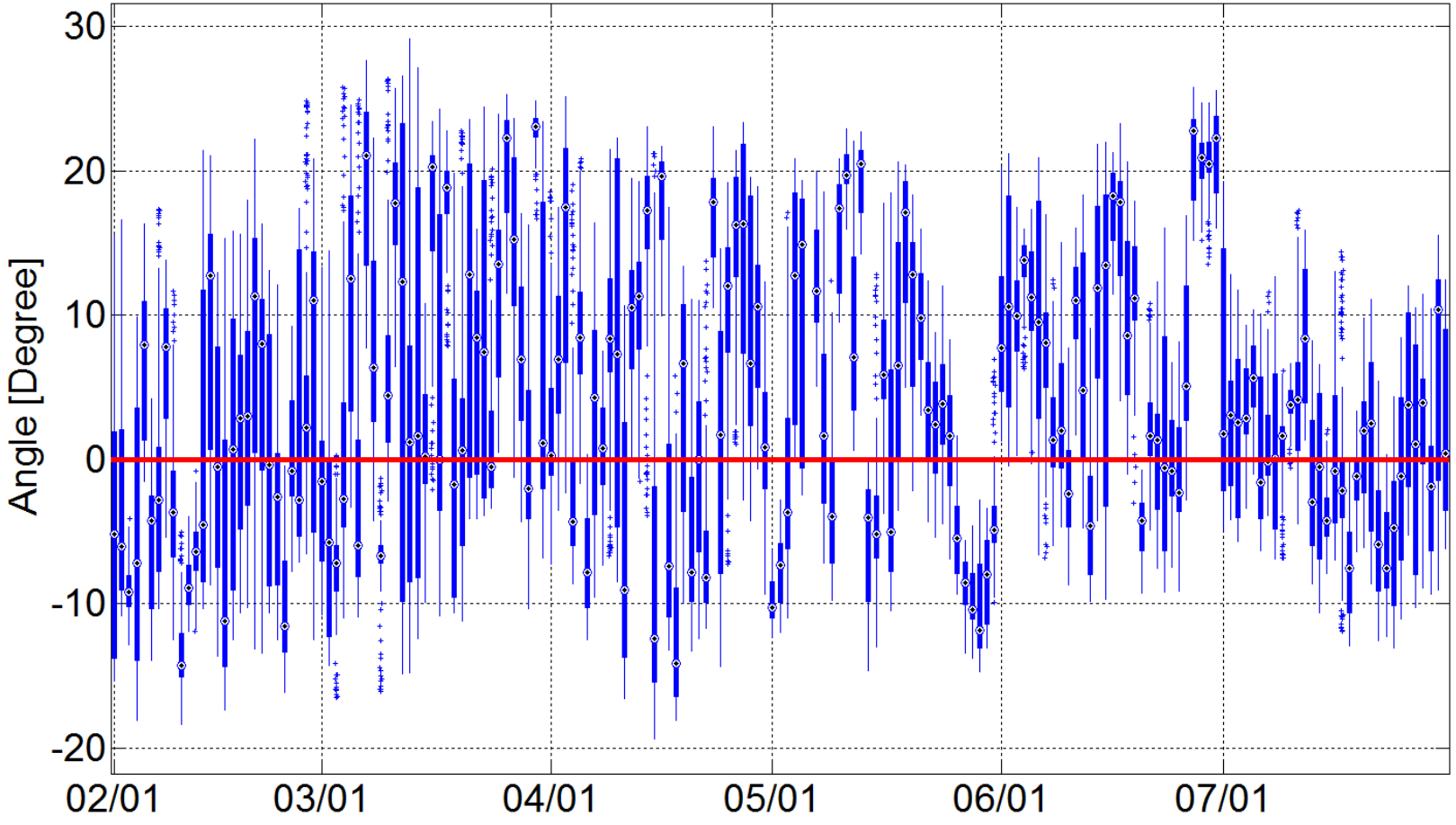
South 13-North 7



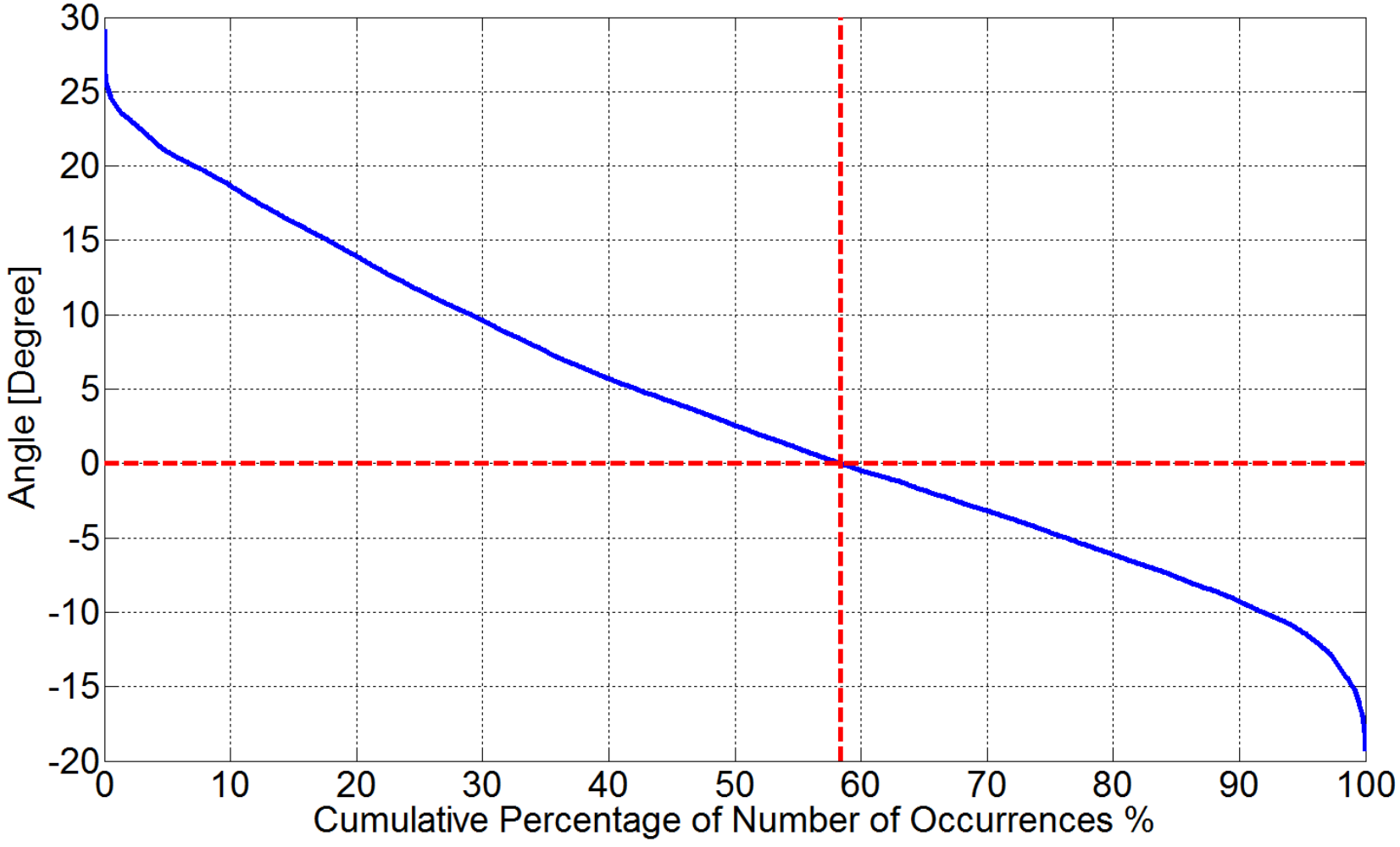
South 13-North 7



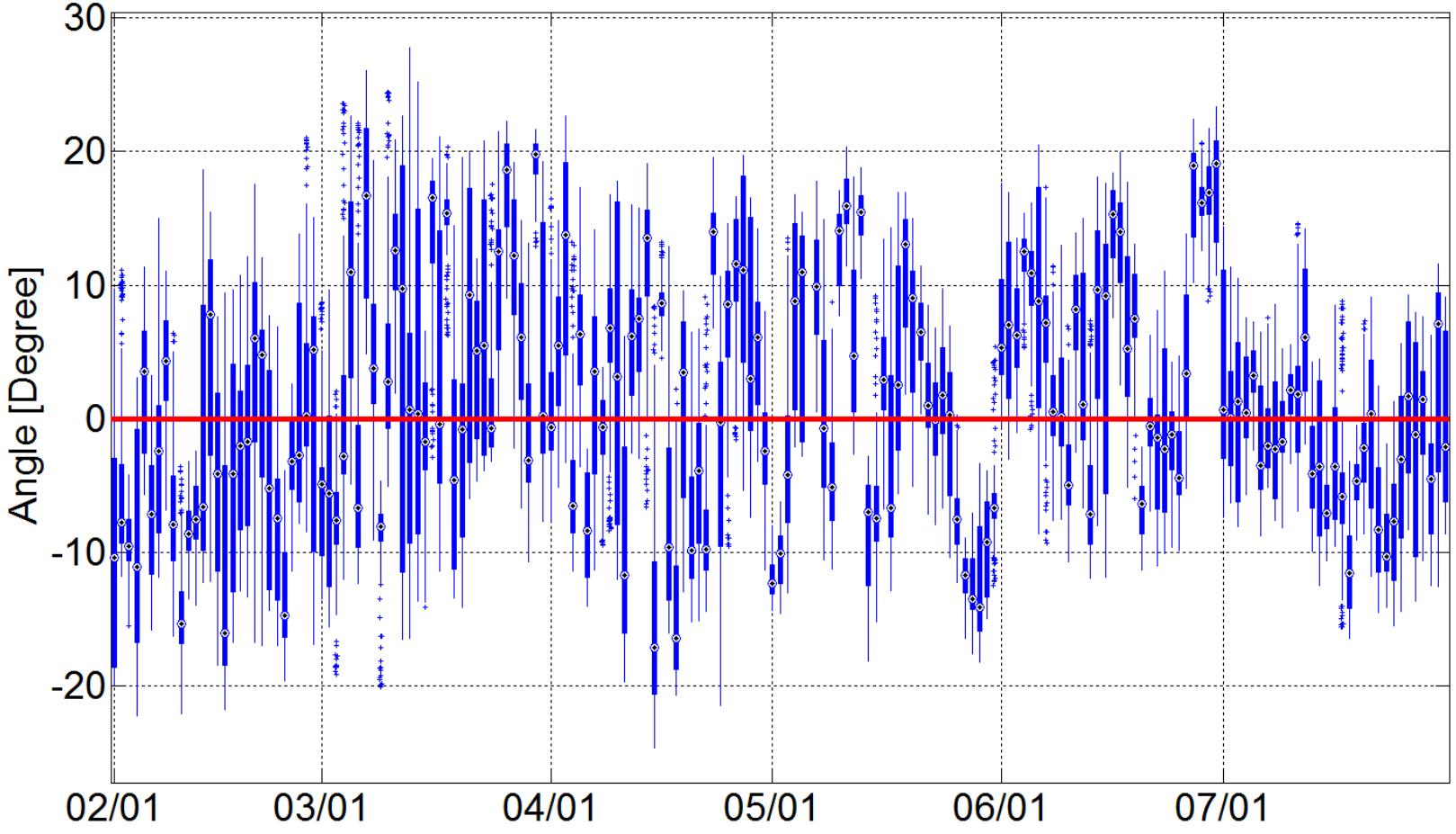
FarWest 4-North 7



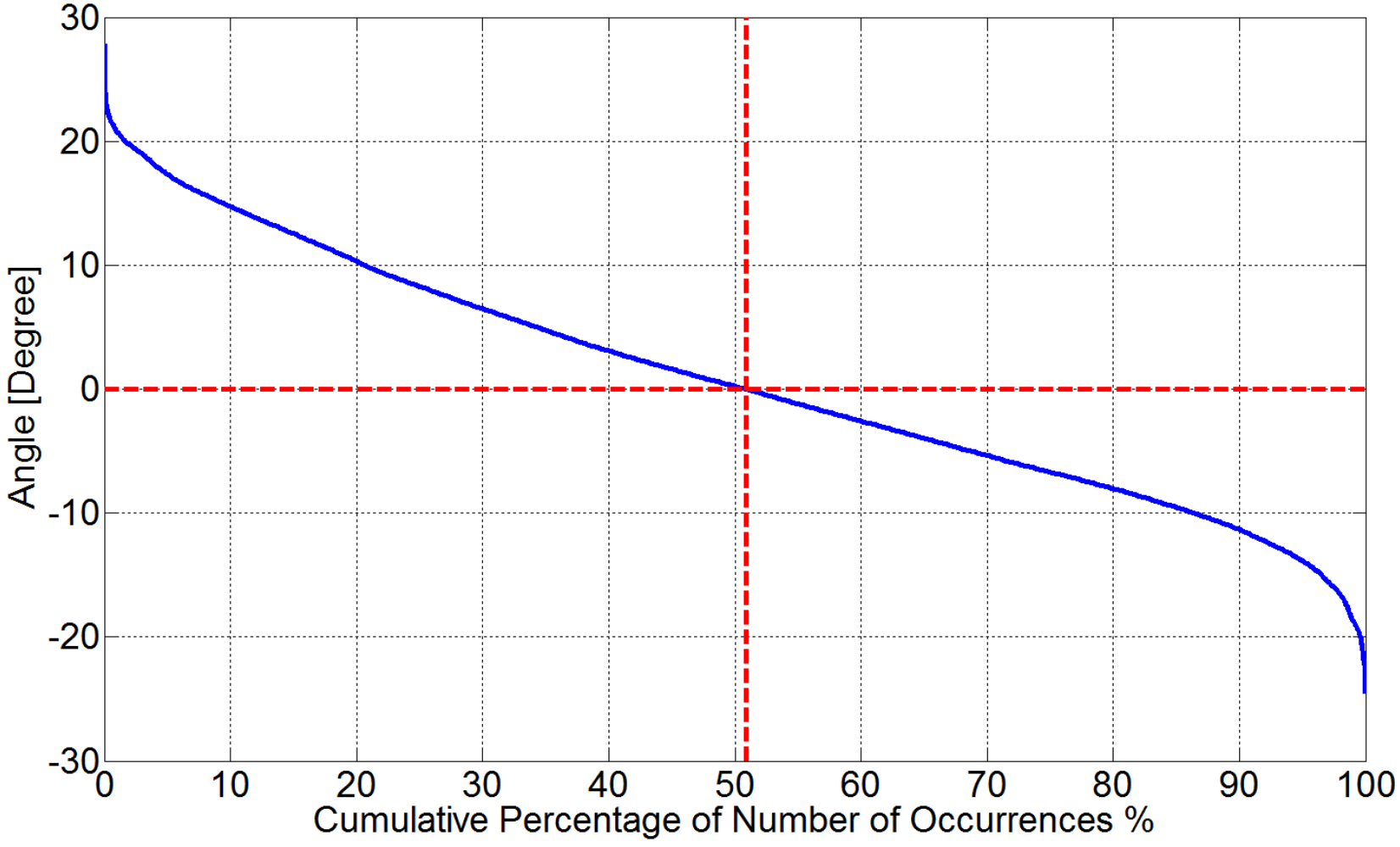
FarWest 4-North 7



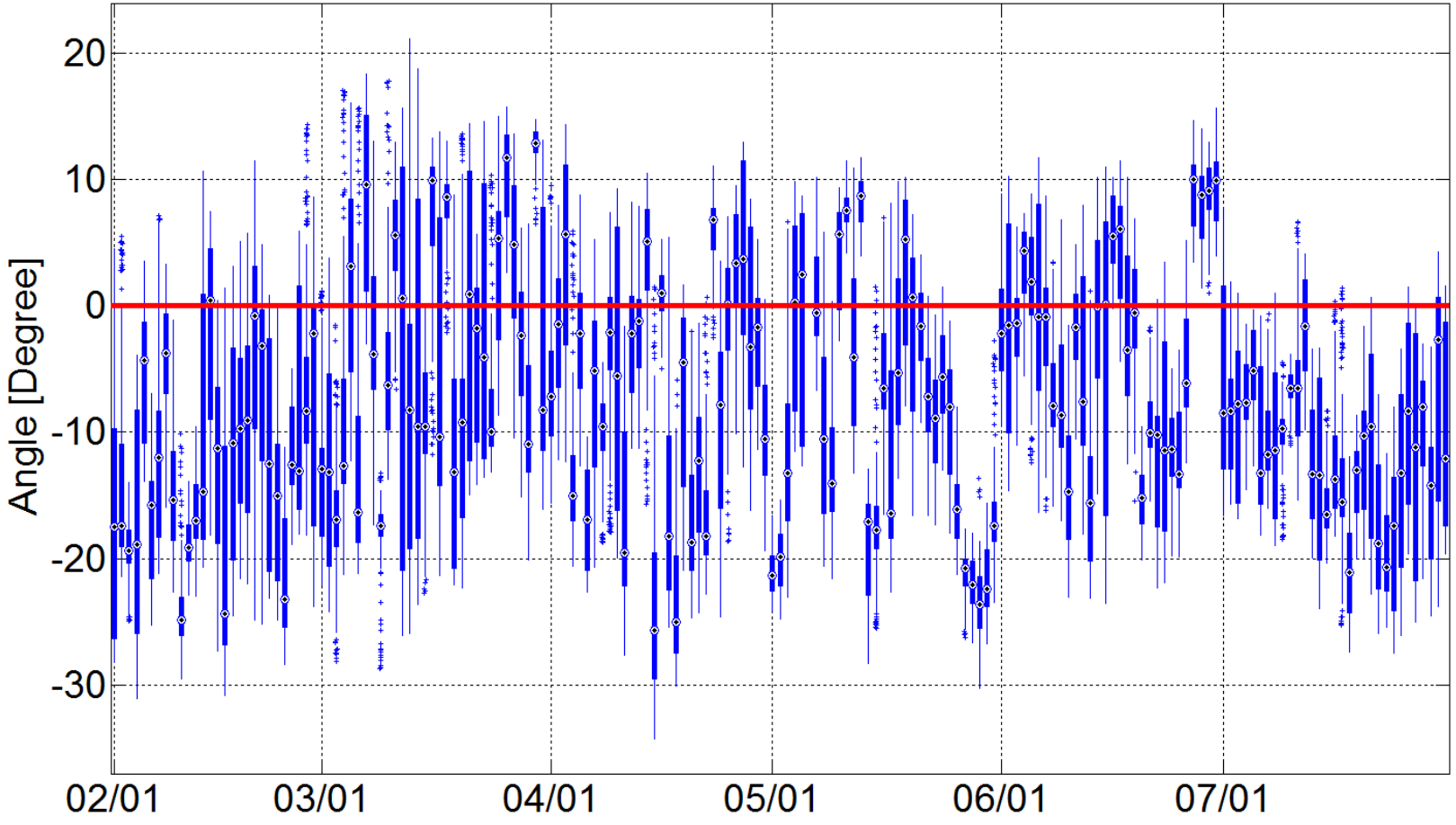
FarWest 7-North 7



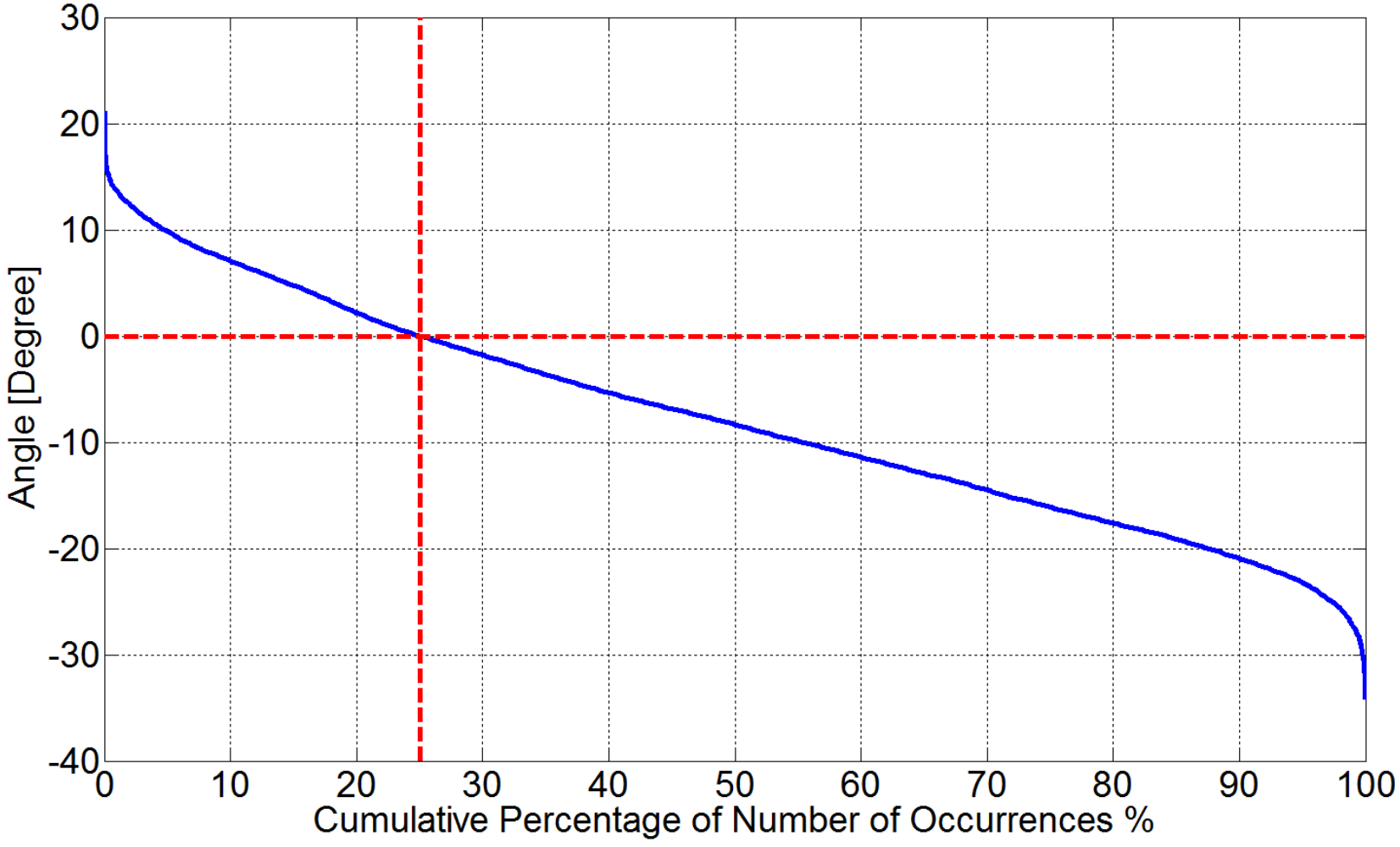
FarWest 7-North 7



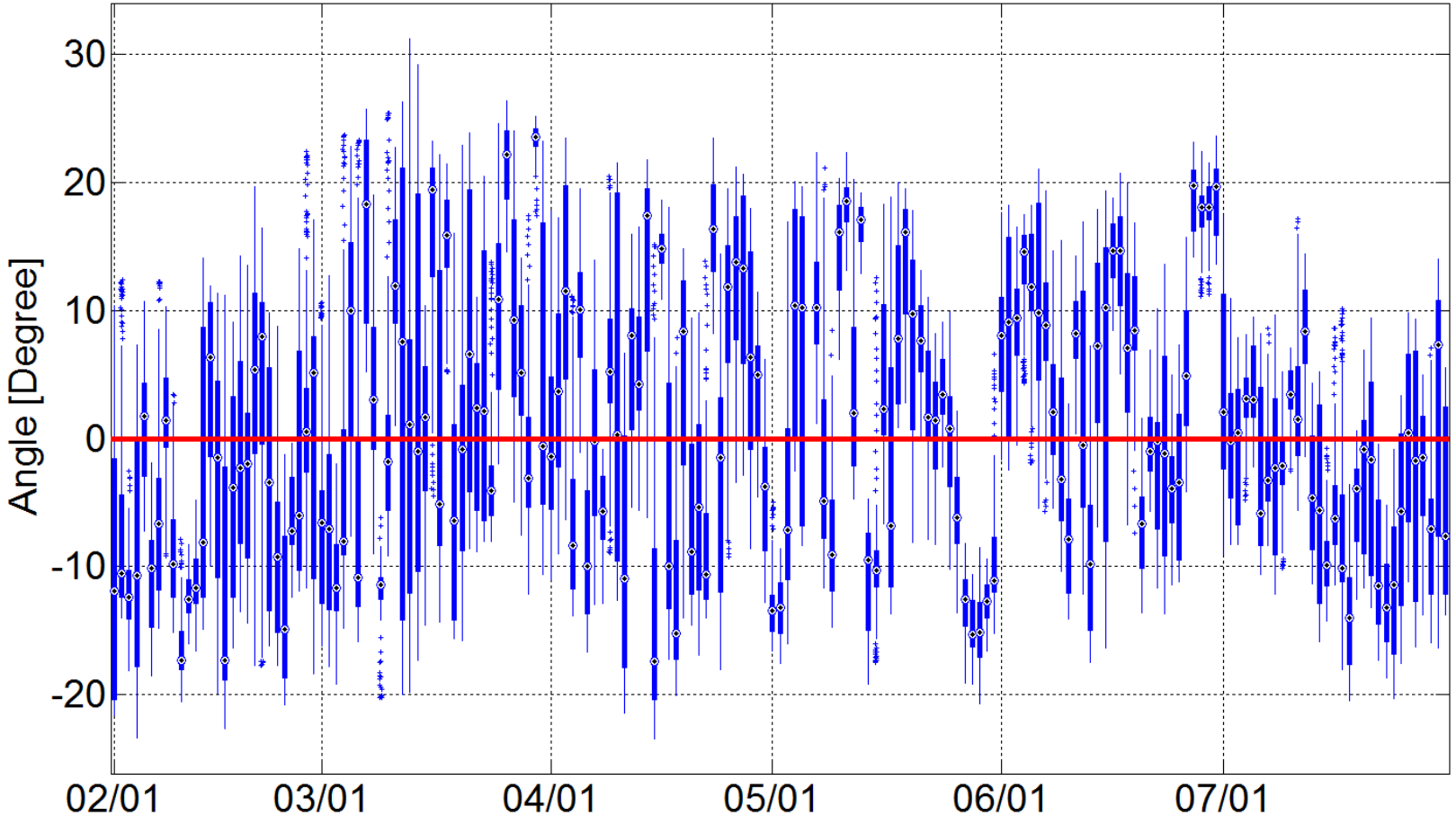
FarWest 8-North 7



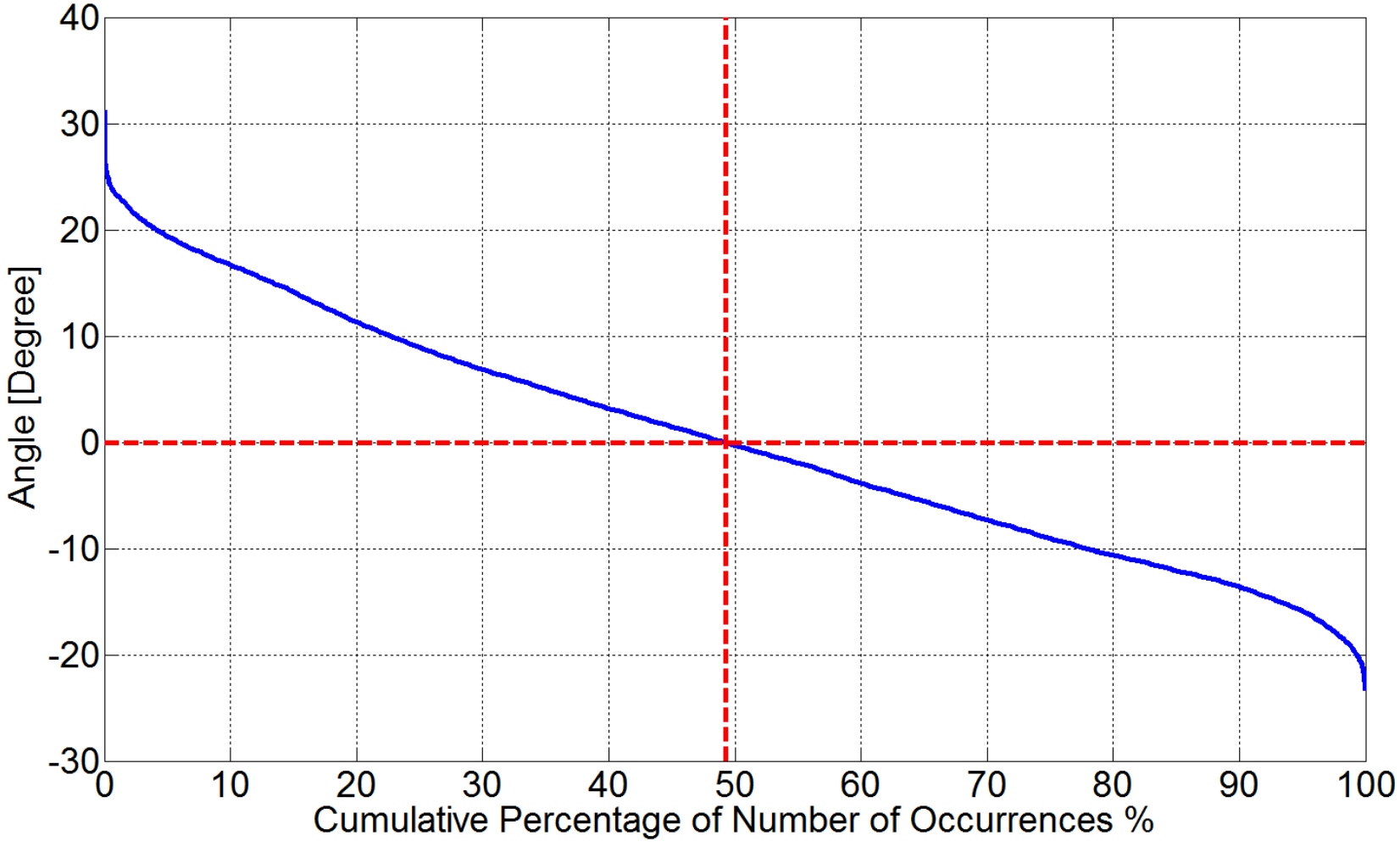
FarWest 8-North 7



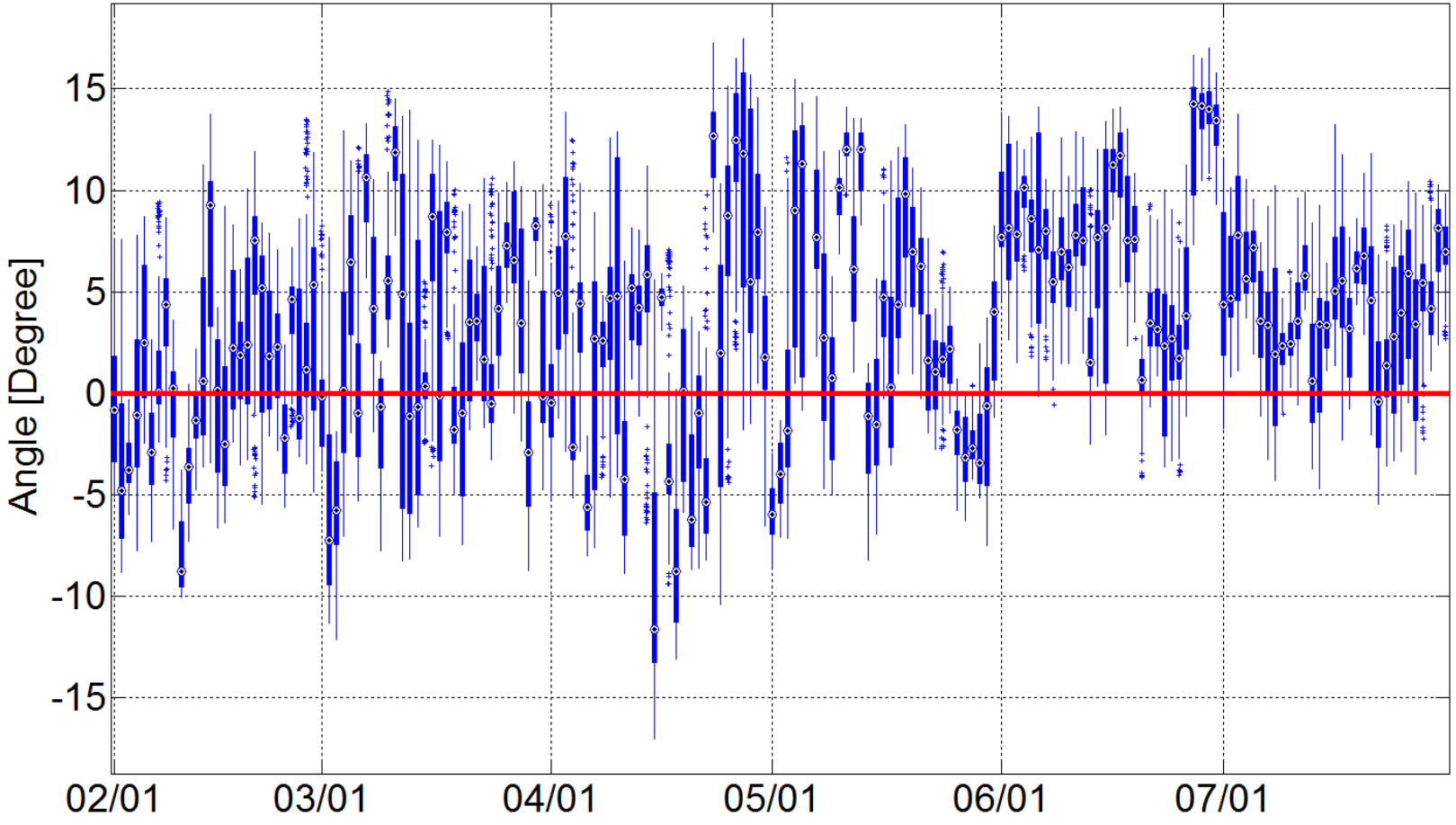
FarWest 9-North 7



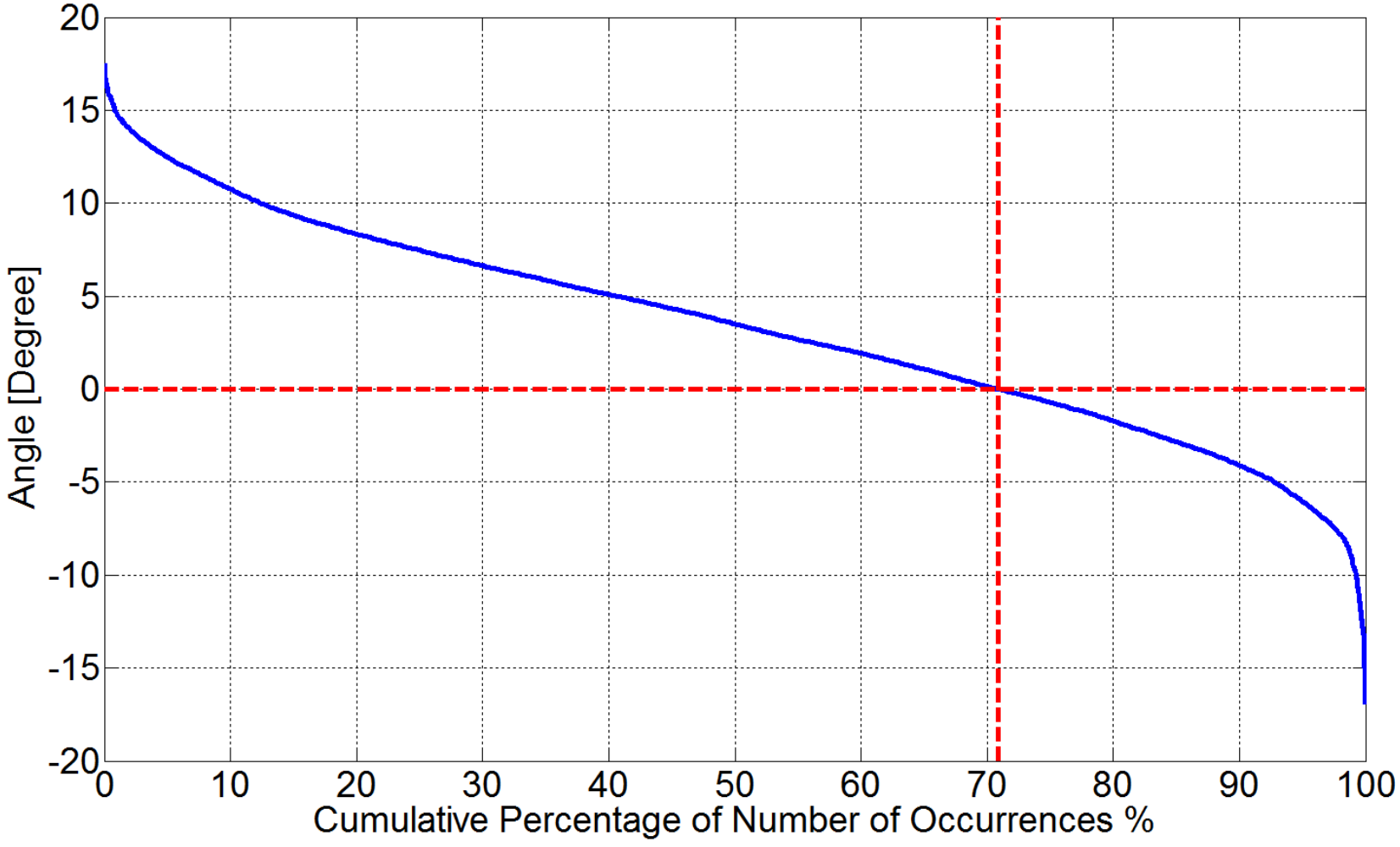
FarWest 9-North 7



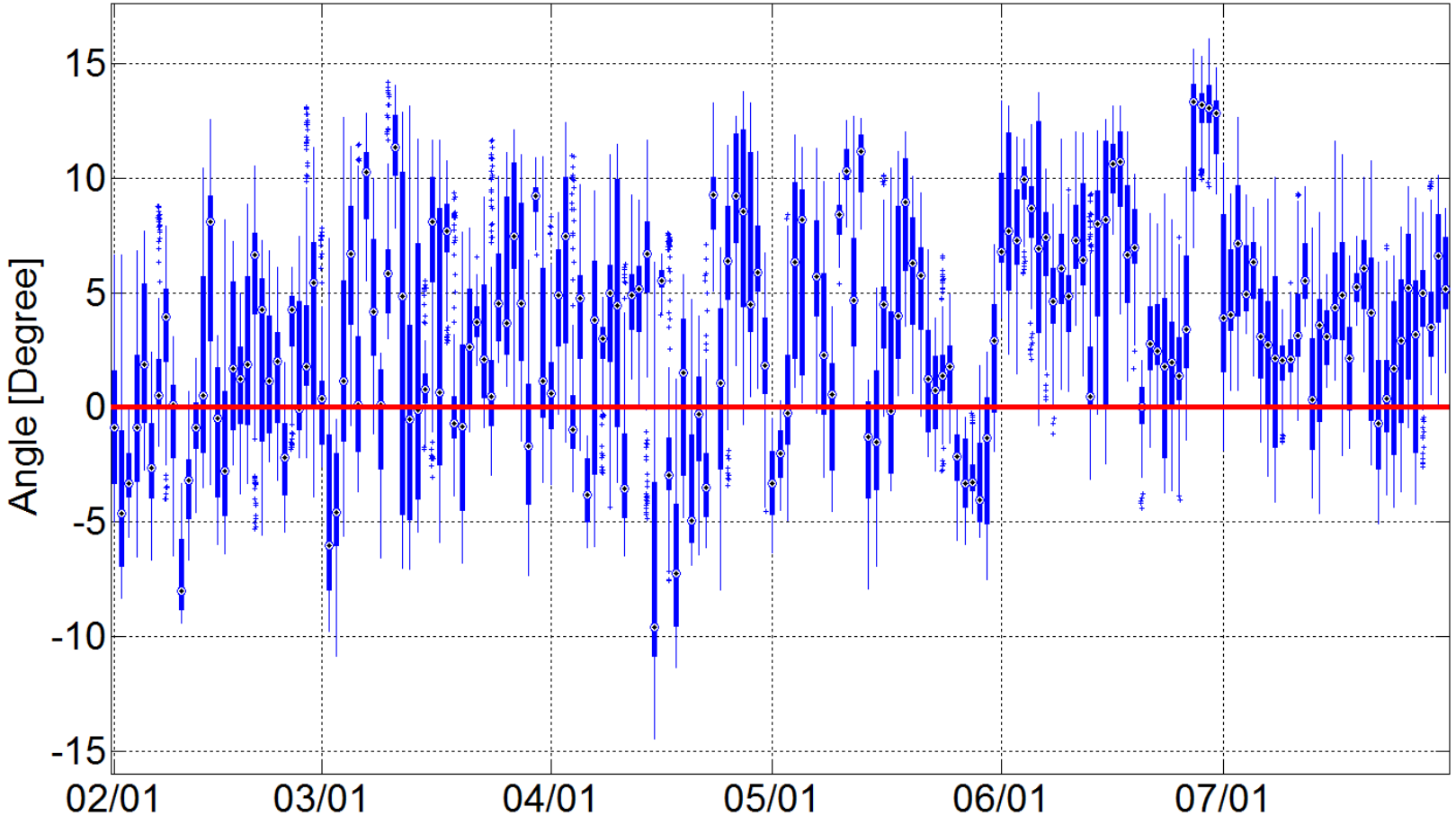
West 16-North 7



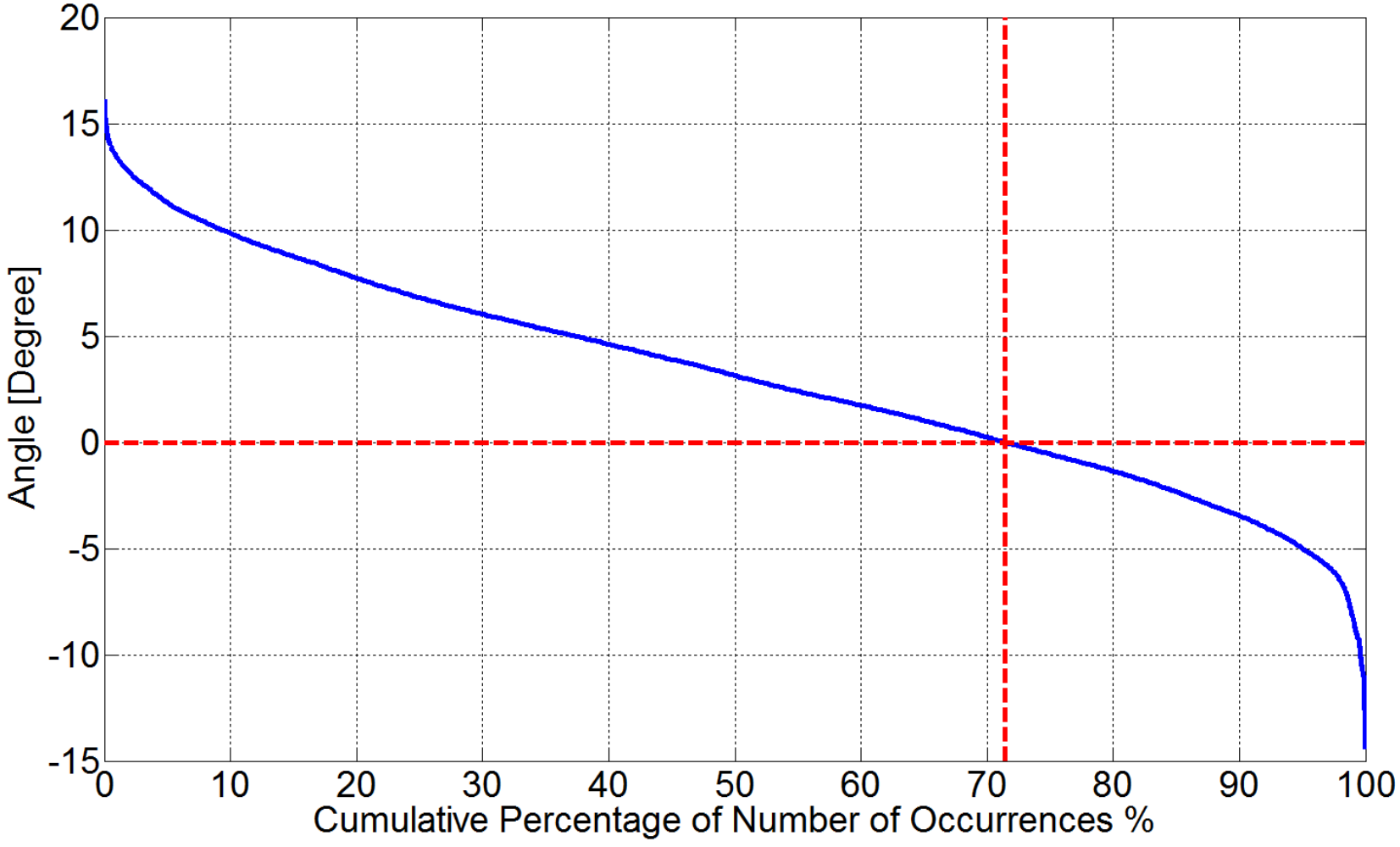
West 16-North 7



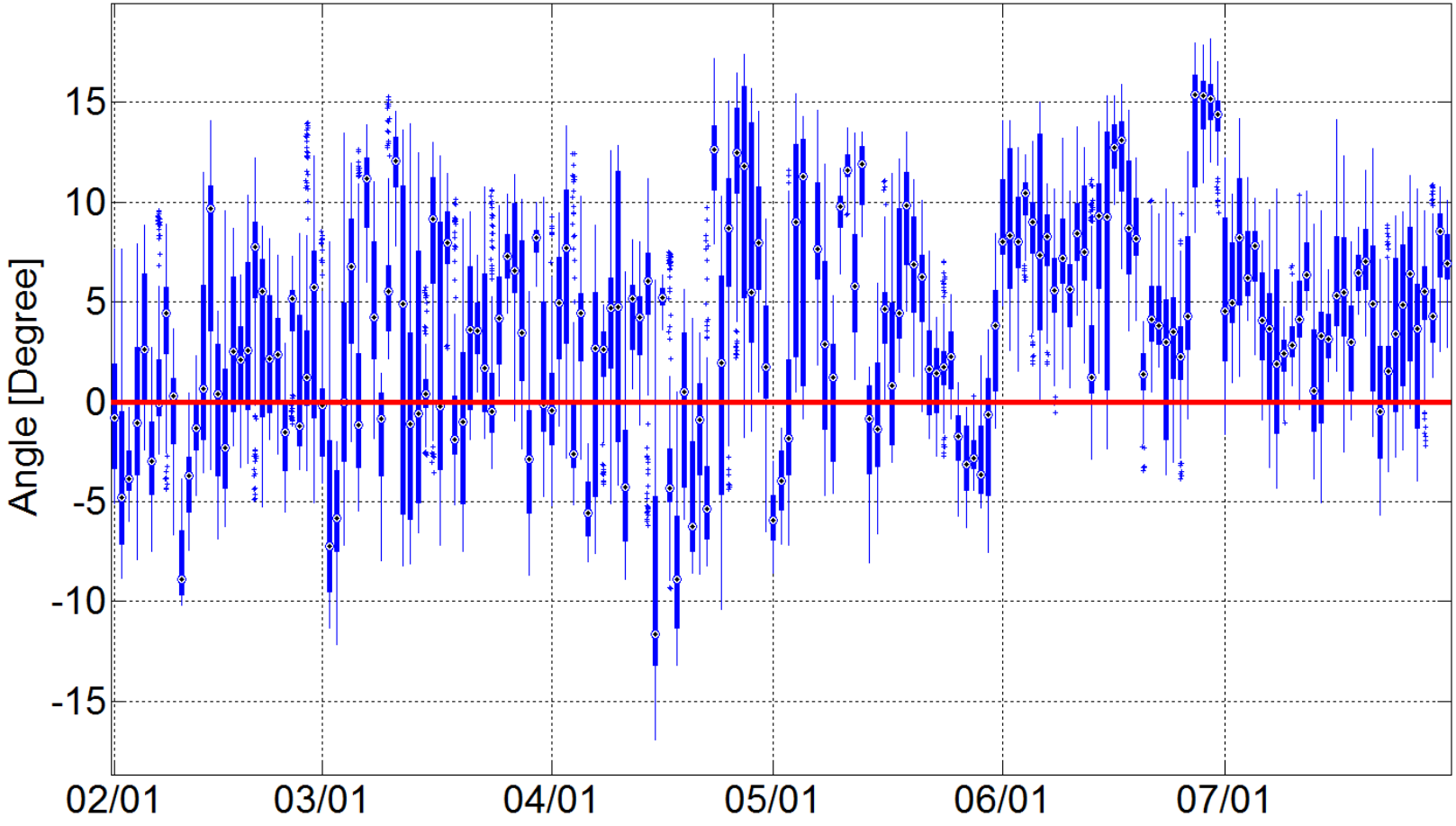
West 3*-North 7



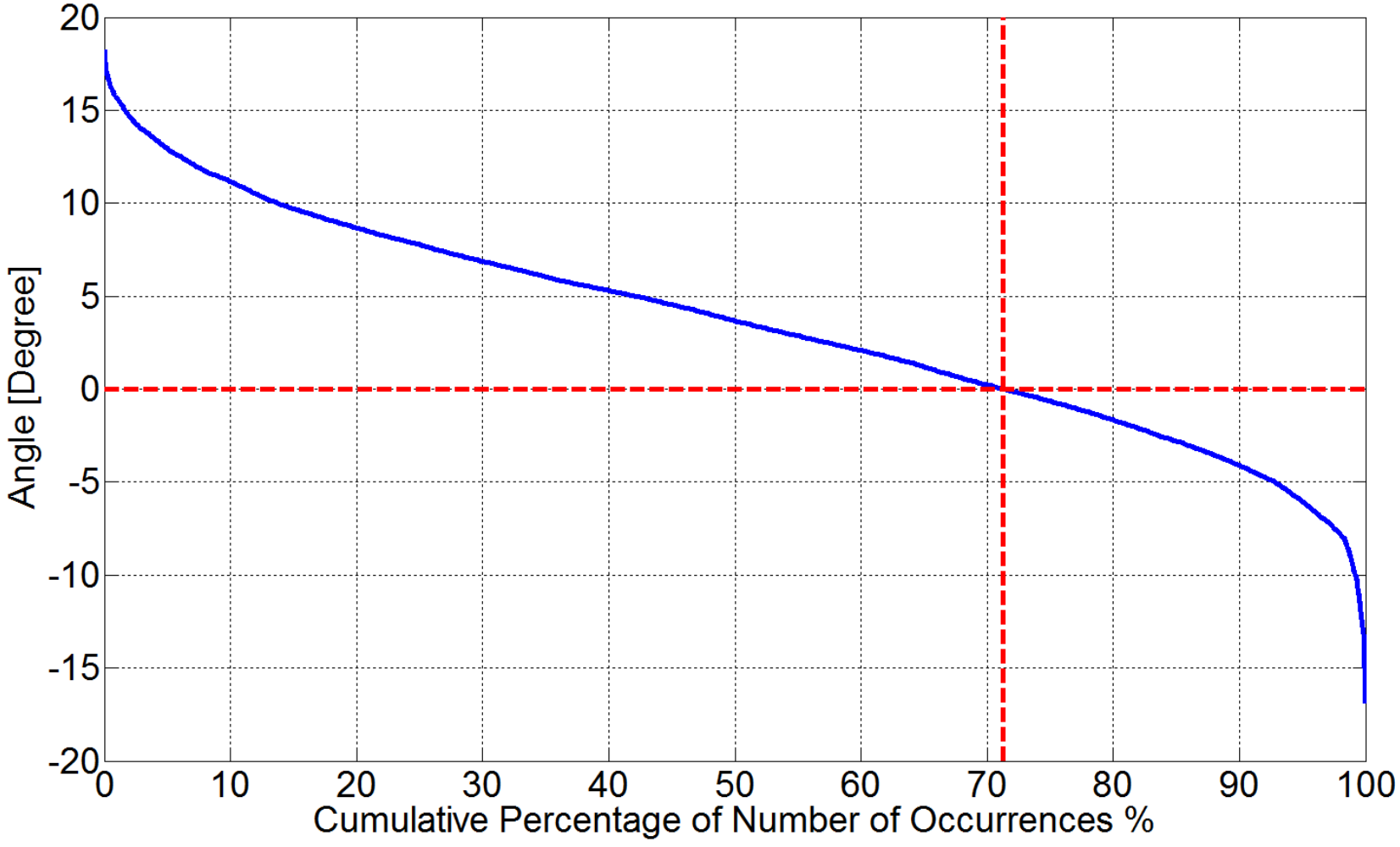
West 3*-North 7



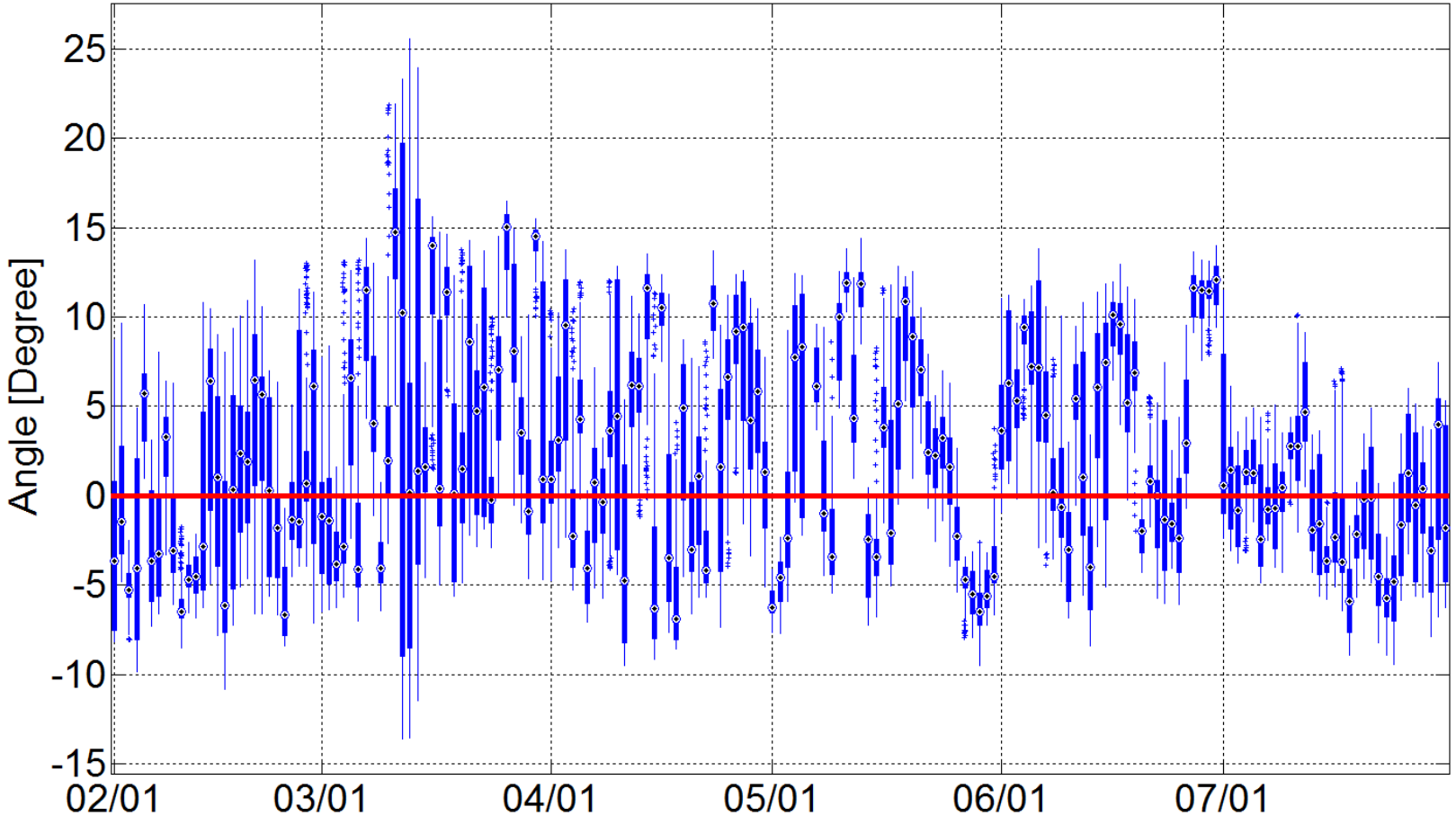
West 15-North 7



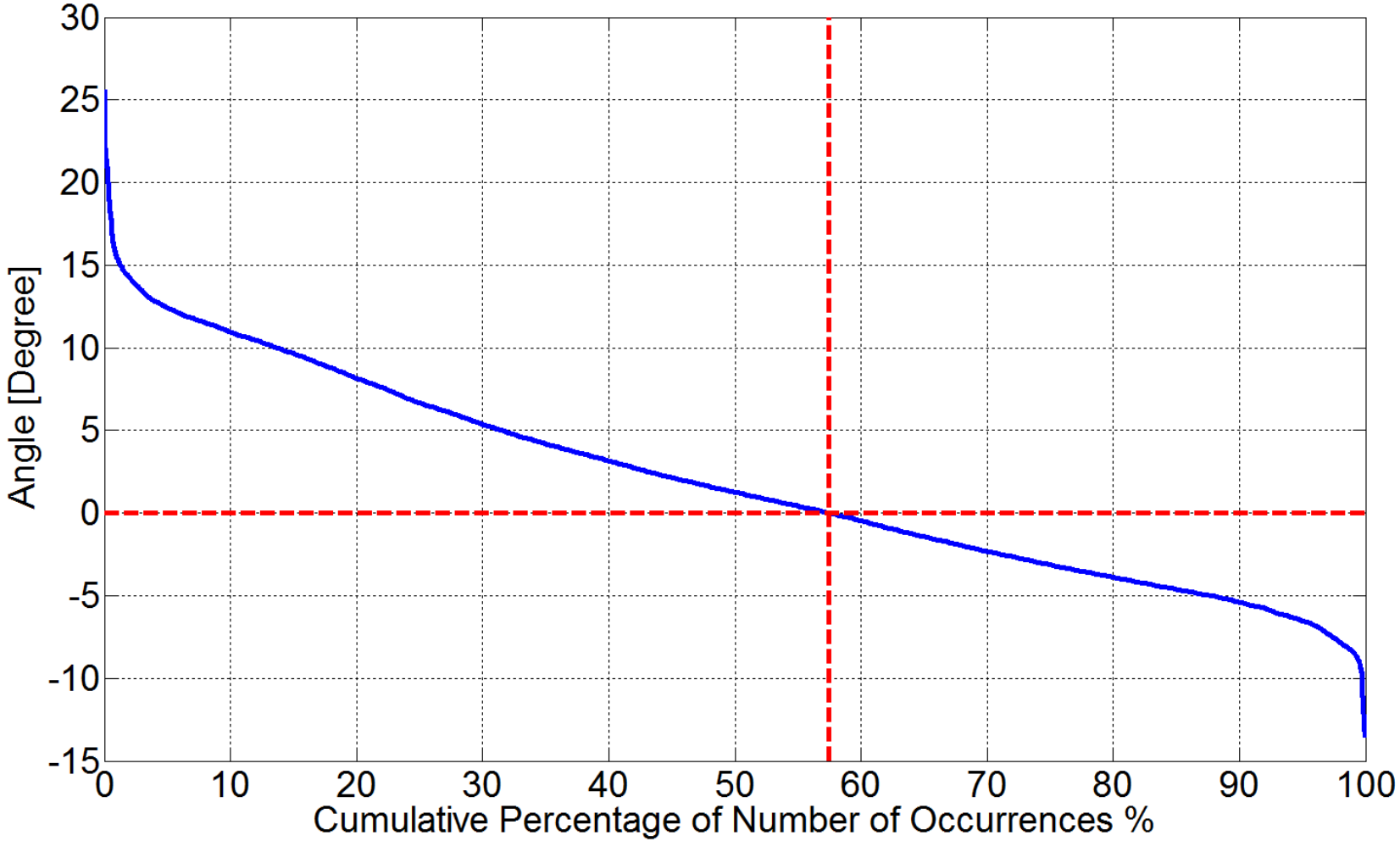
West 15-North 7



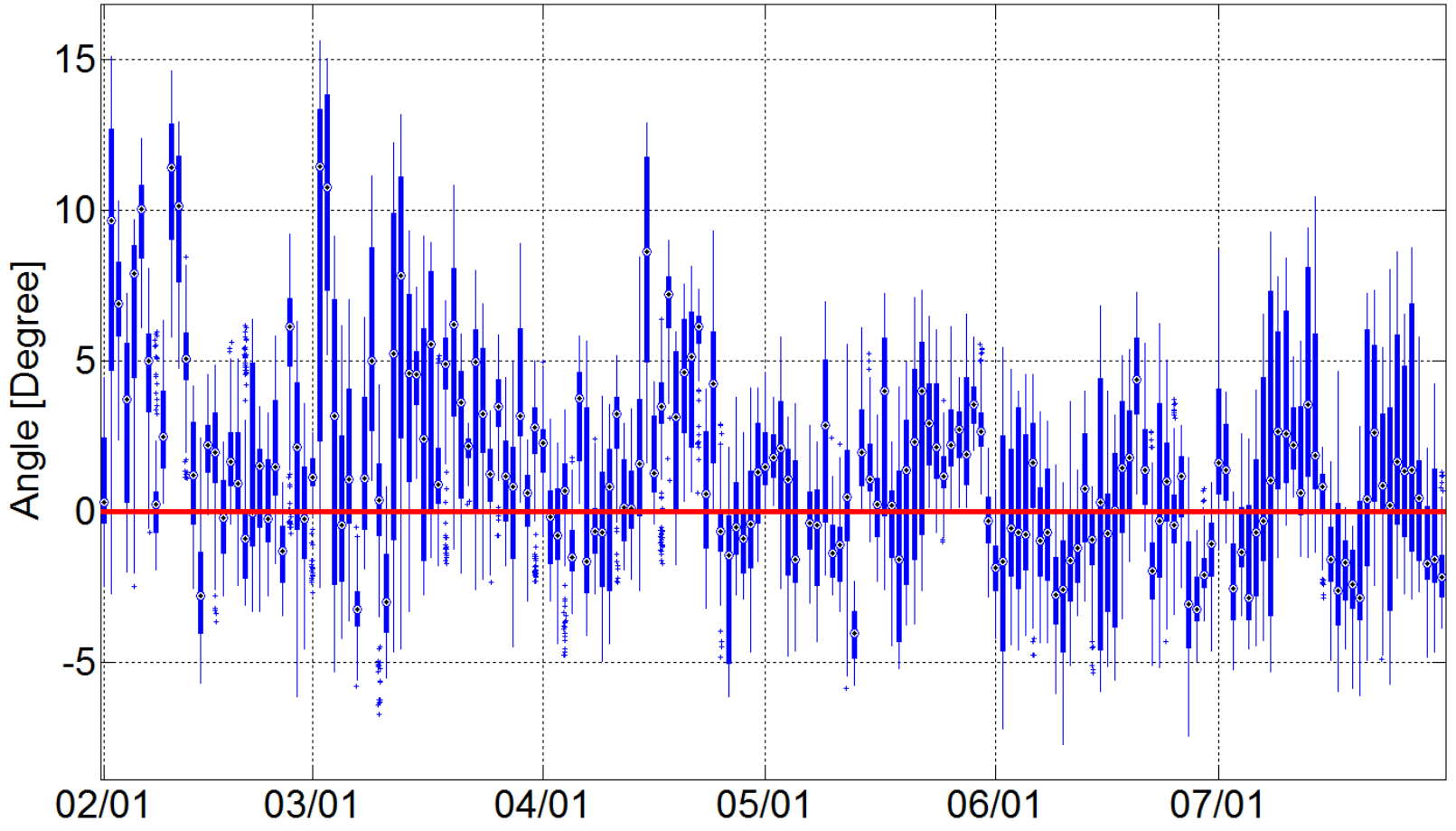
West 8*-North 7



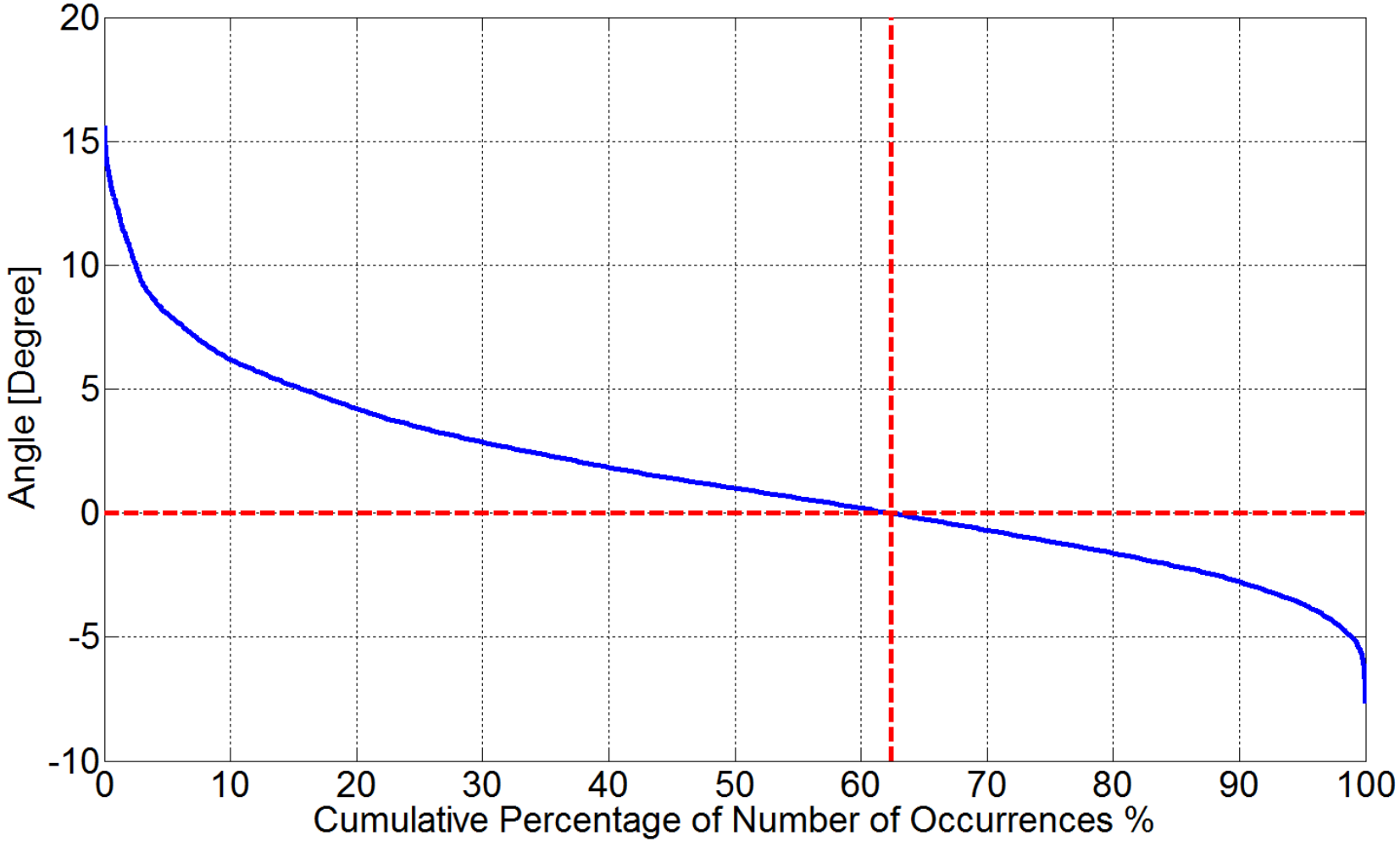
West 8*-North 7



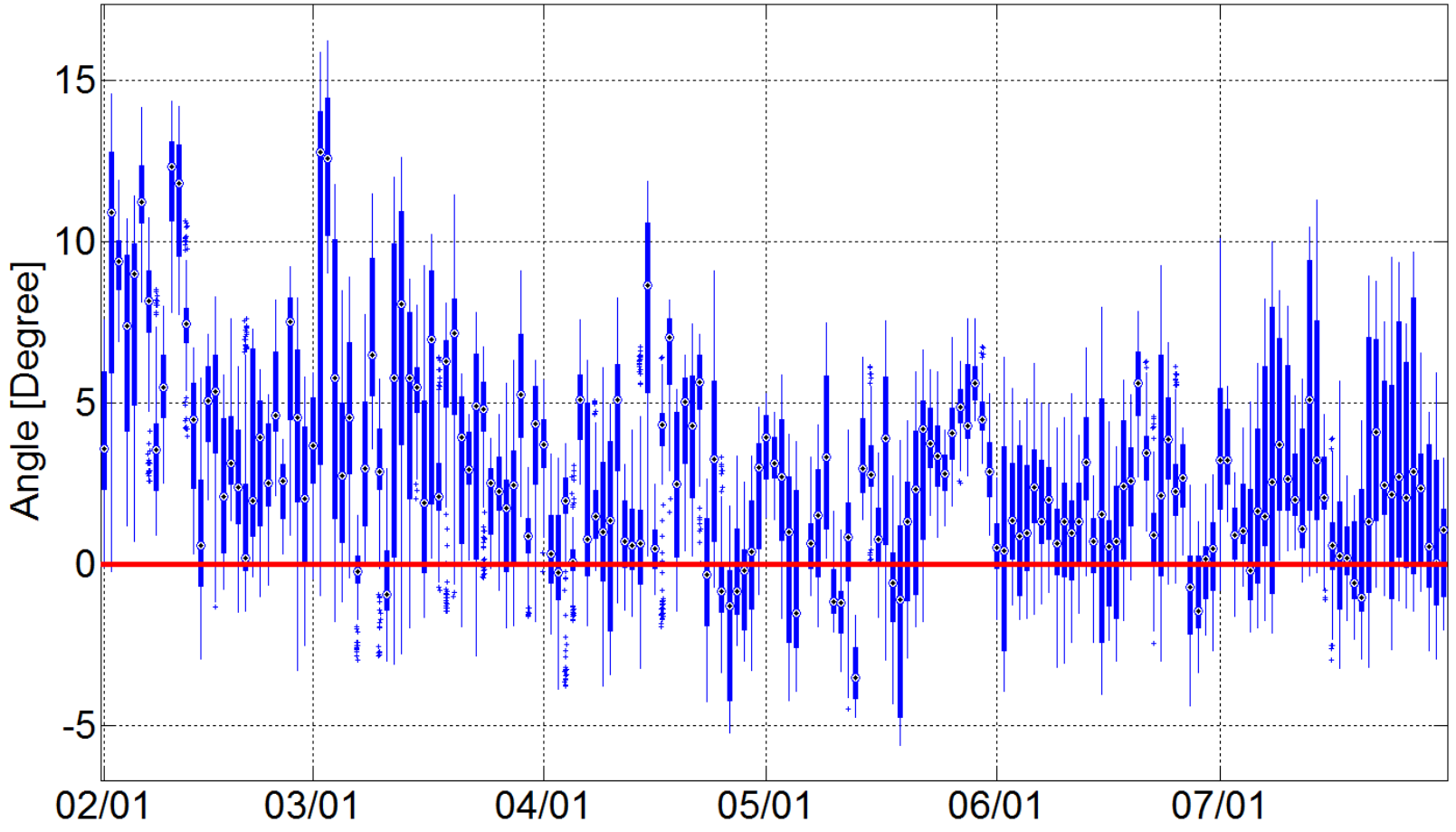
South 15*-North 7



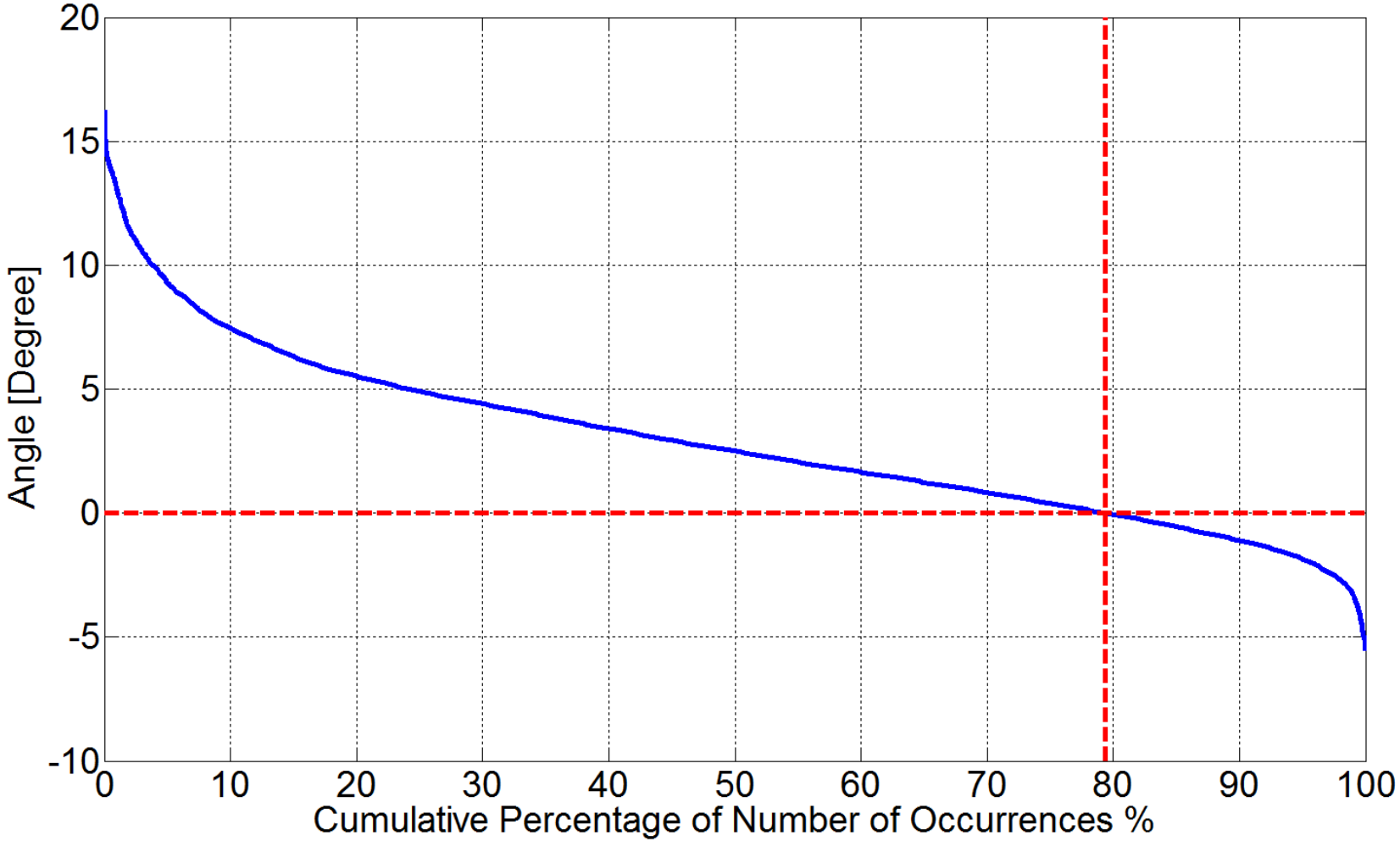
South 15*-North 7



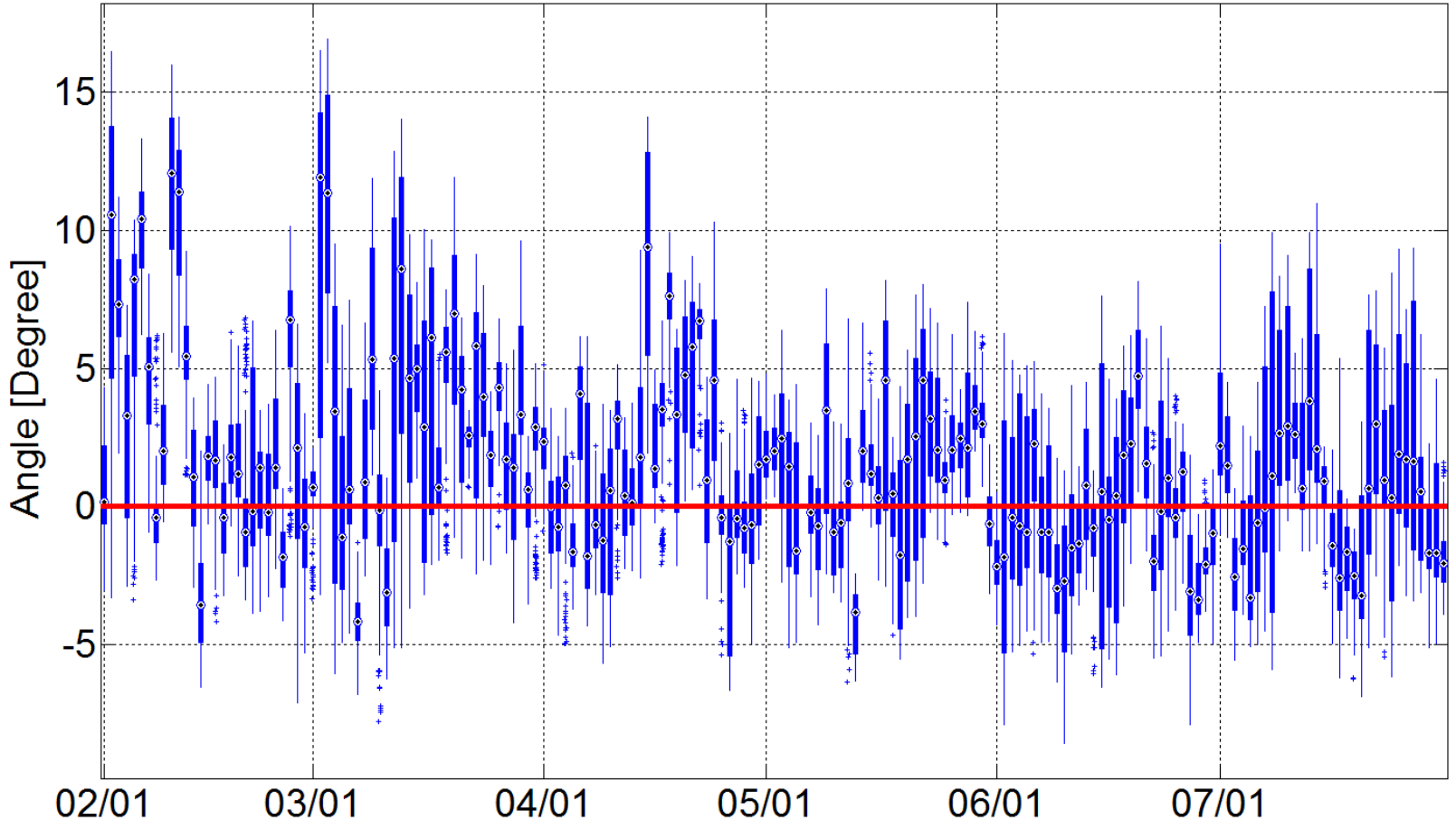
South 2*-North 7



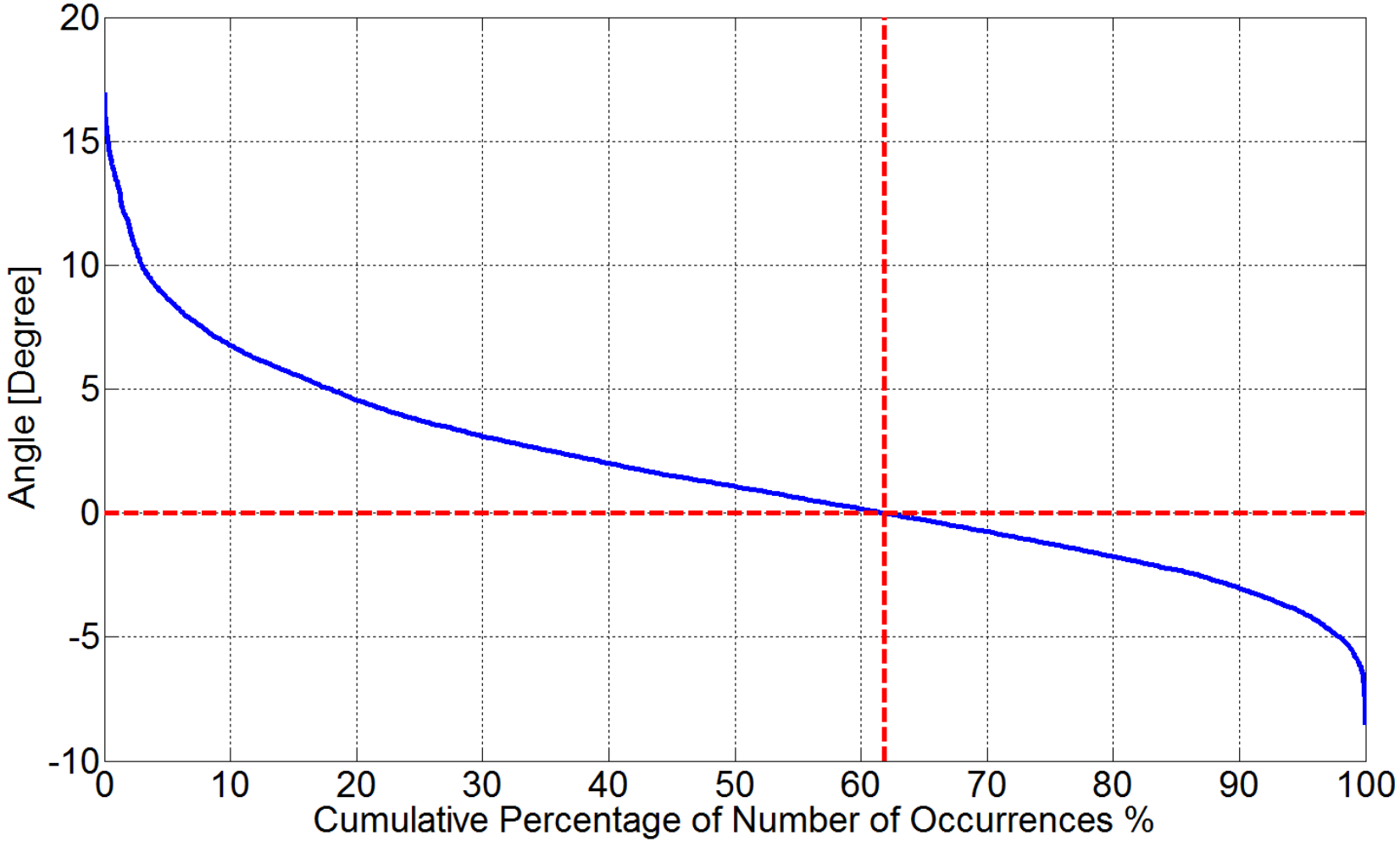
South 2*-North 7



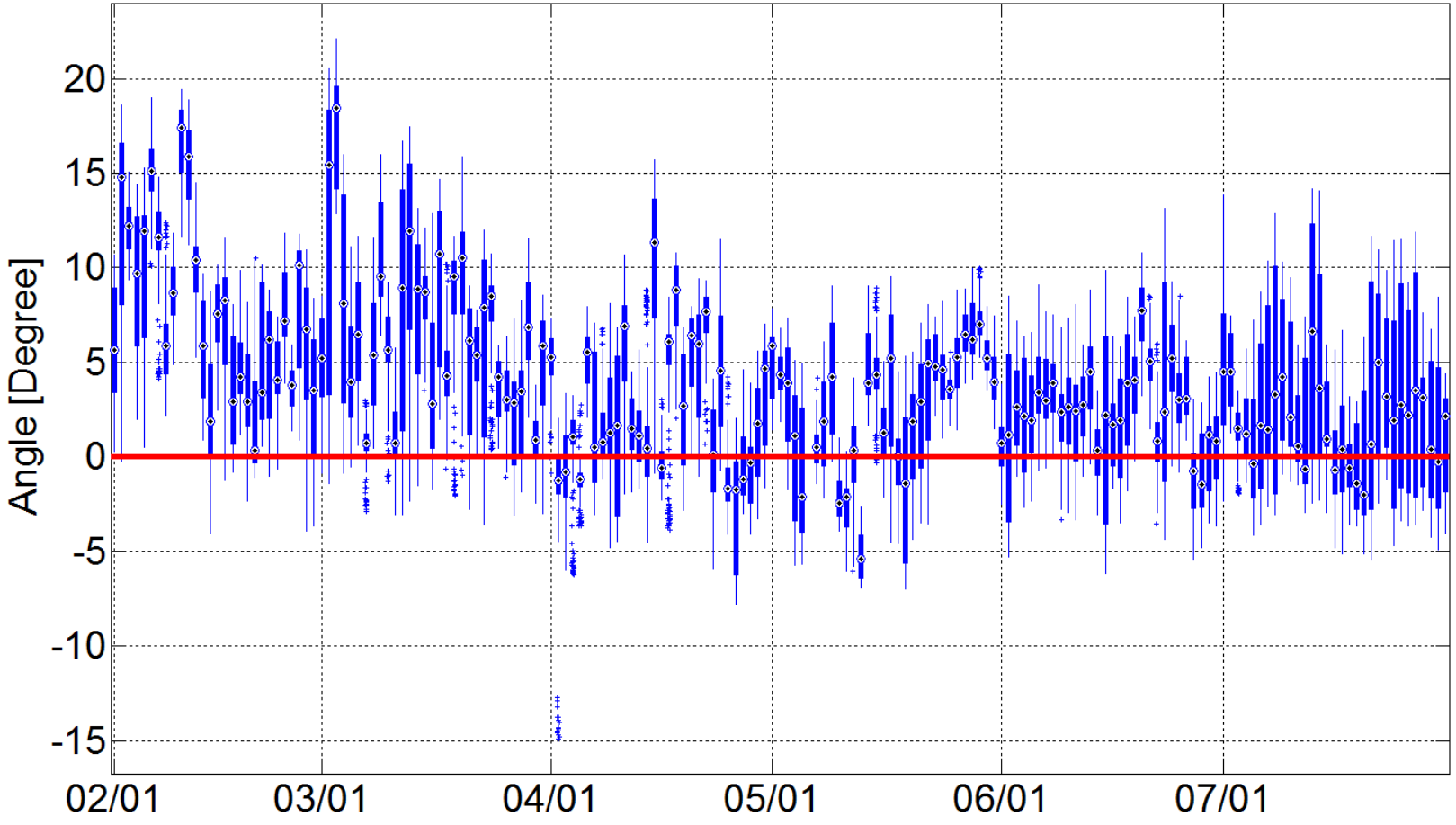
South 4*-North 7



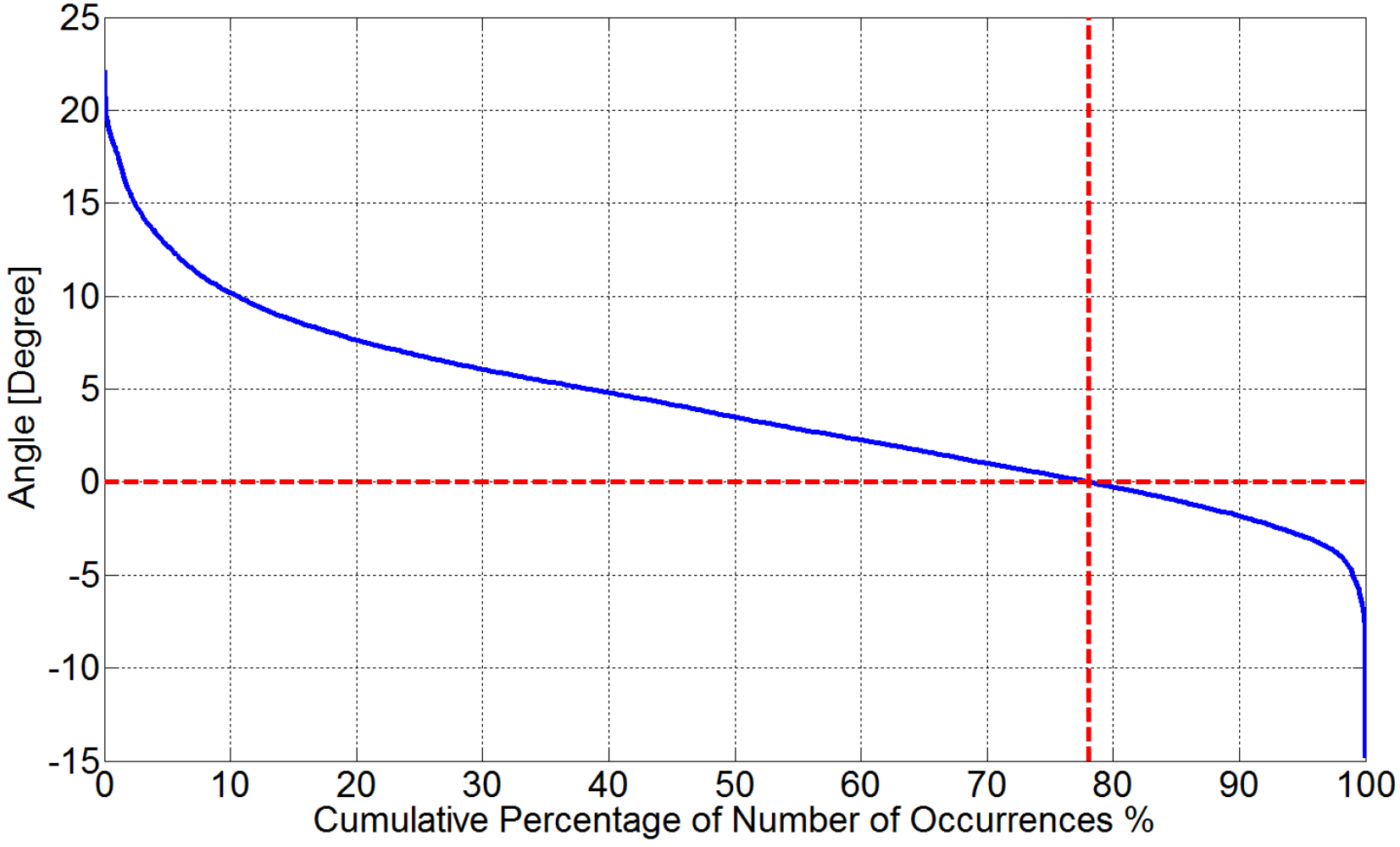
South 4*-North 7



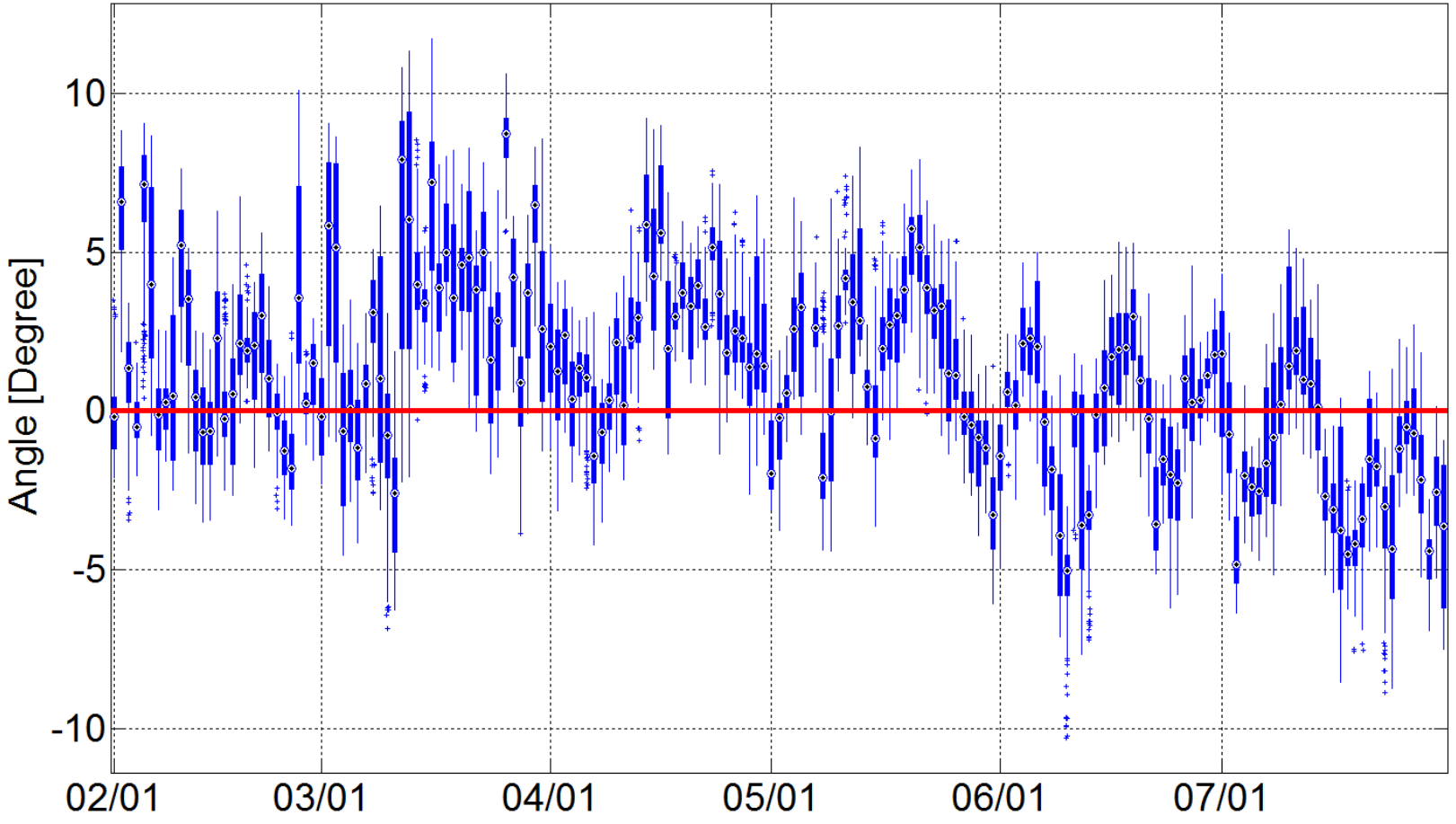
South 7*-North 7



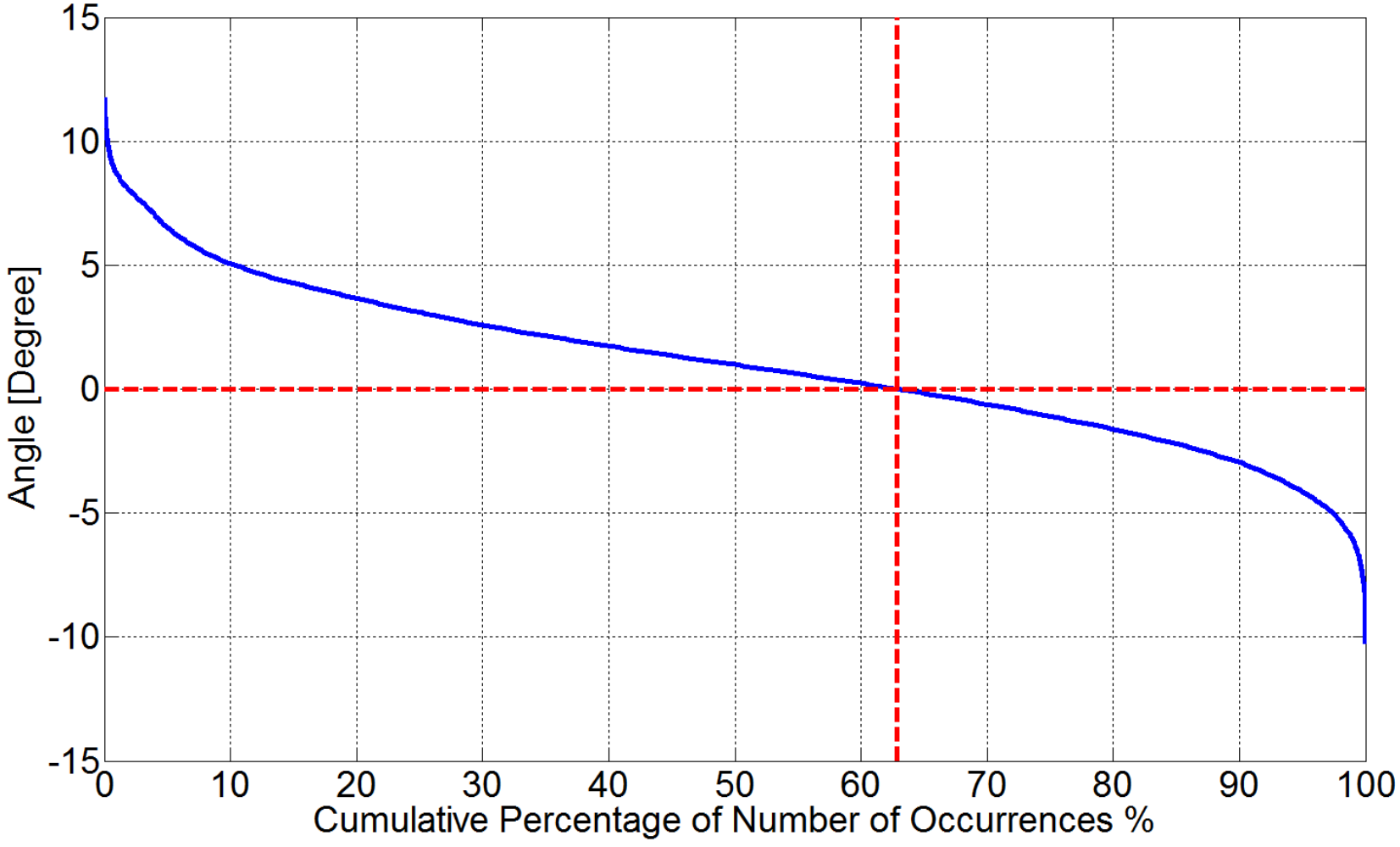
South 7*-North 7



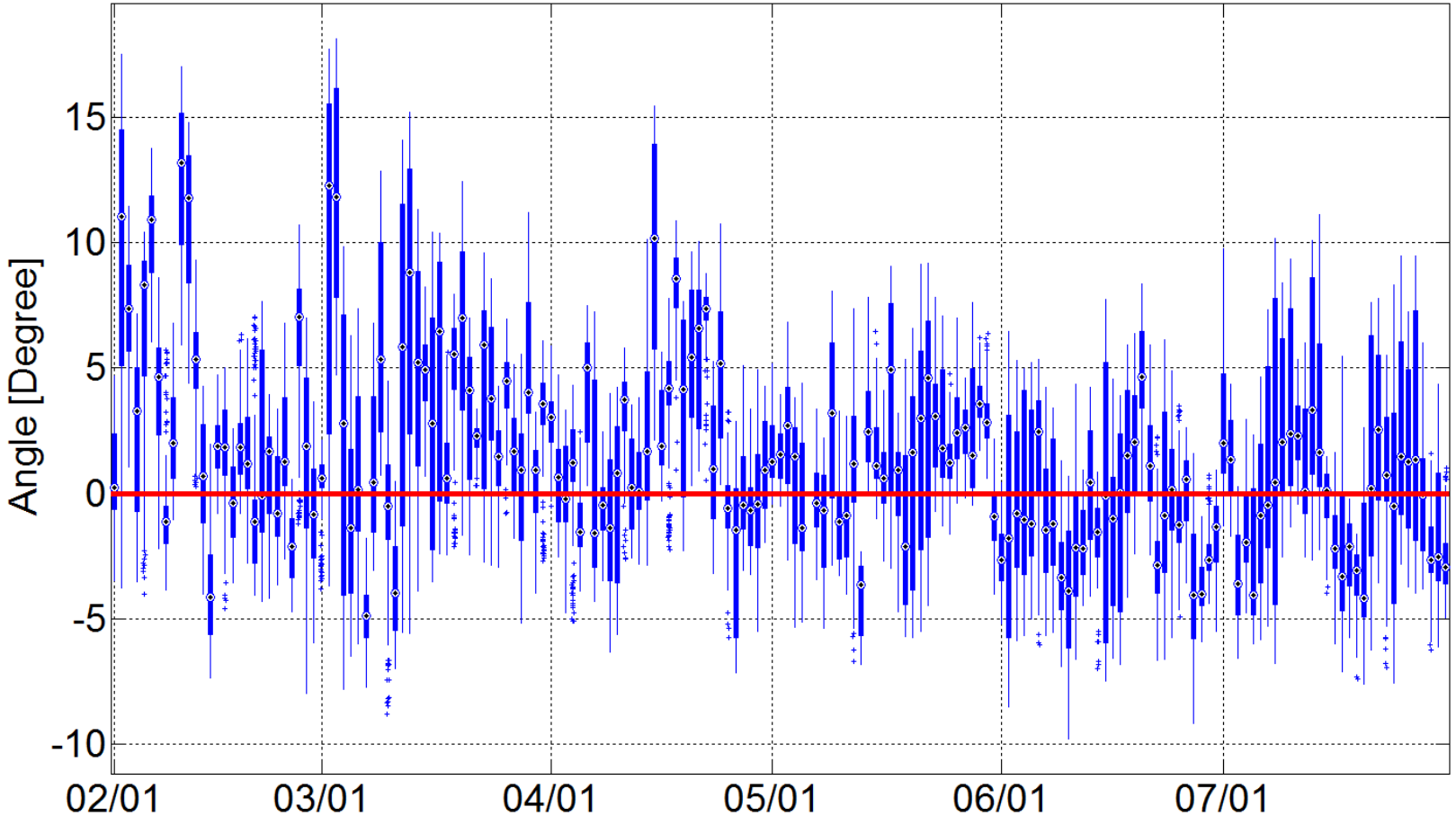
South 9*-North 7



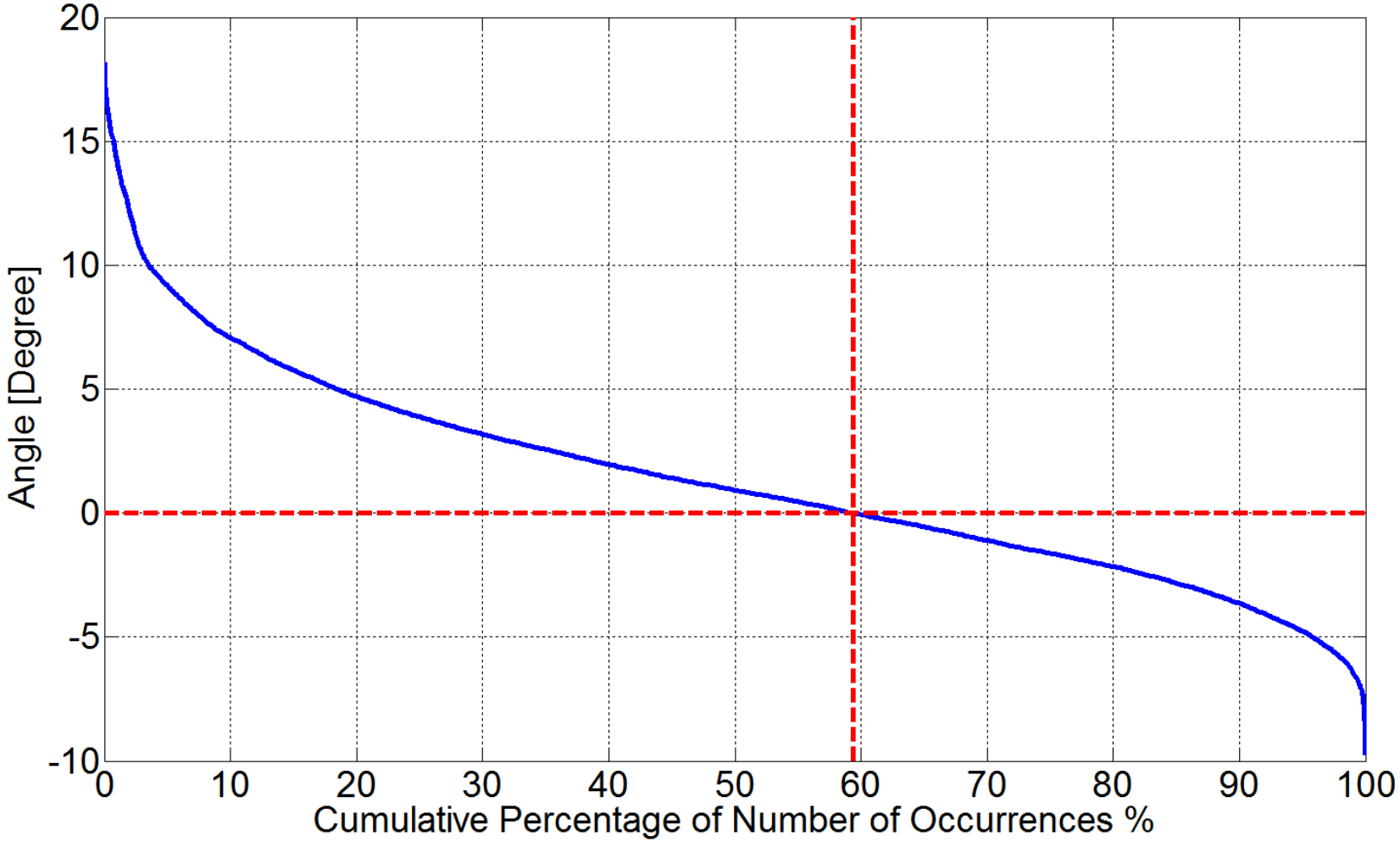
South 9*-North 7



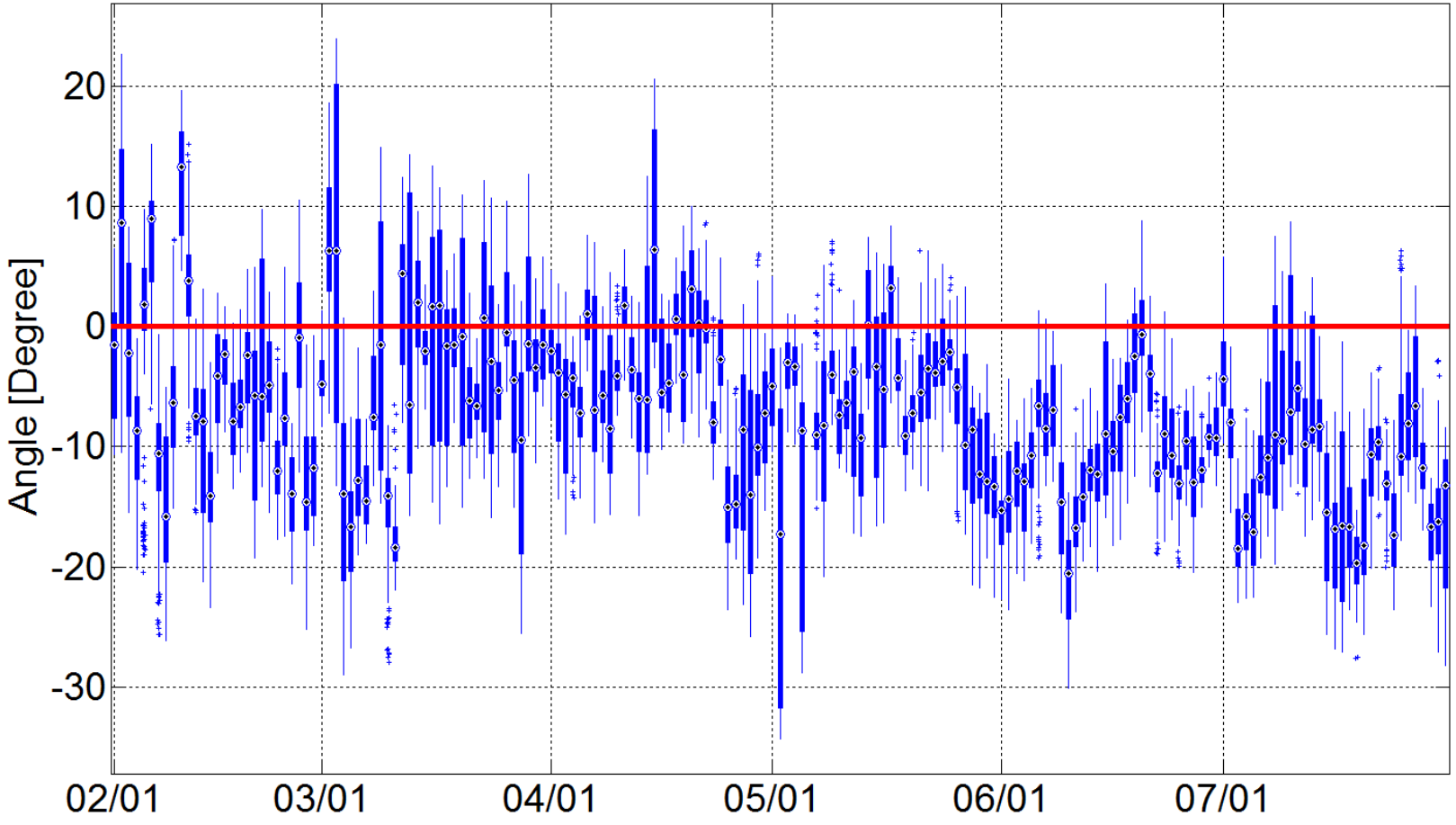
South 11*-North 7



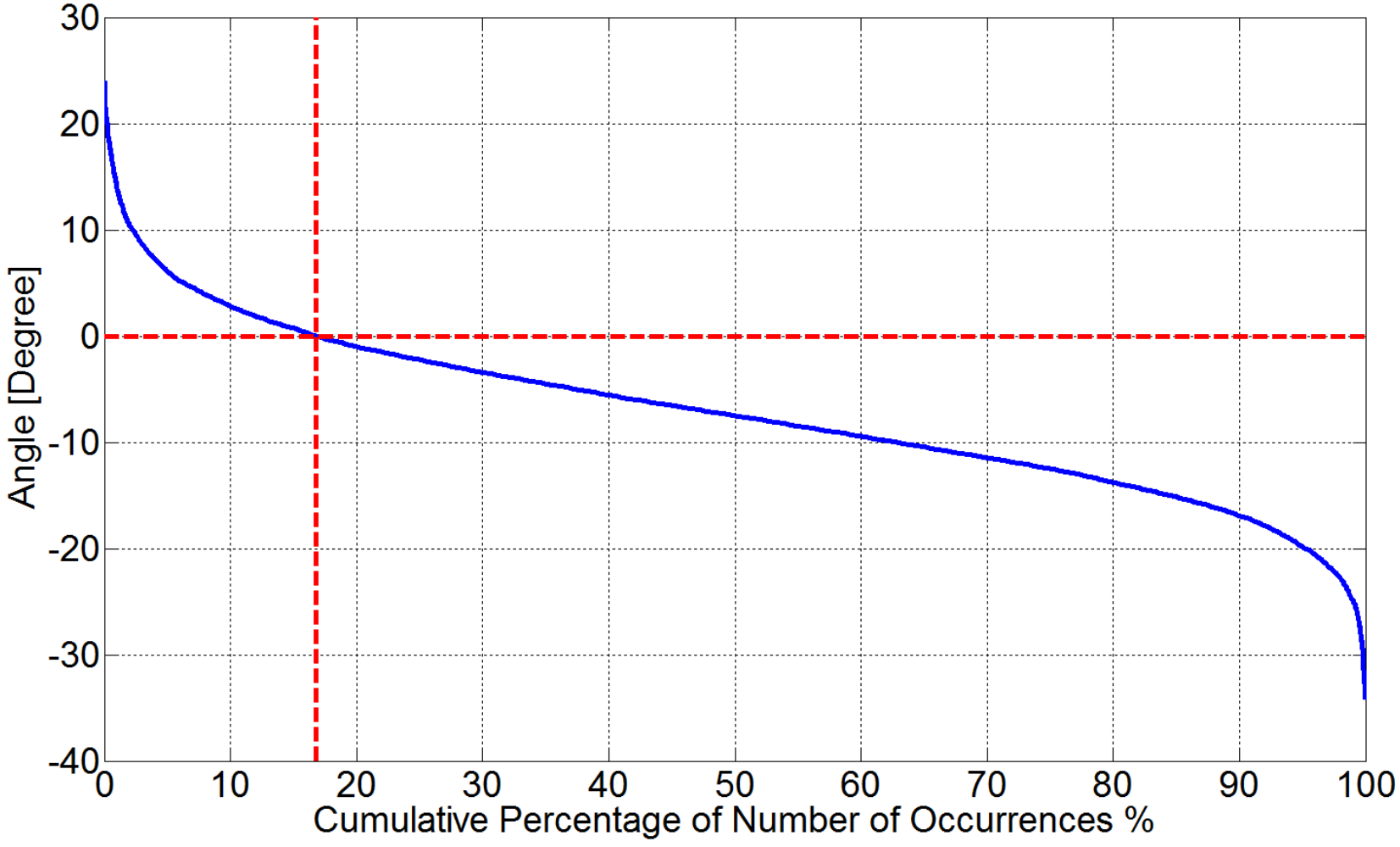
South 11*-North 7



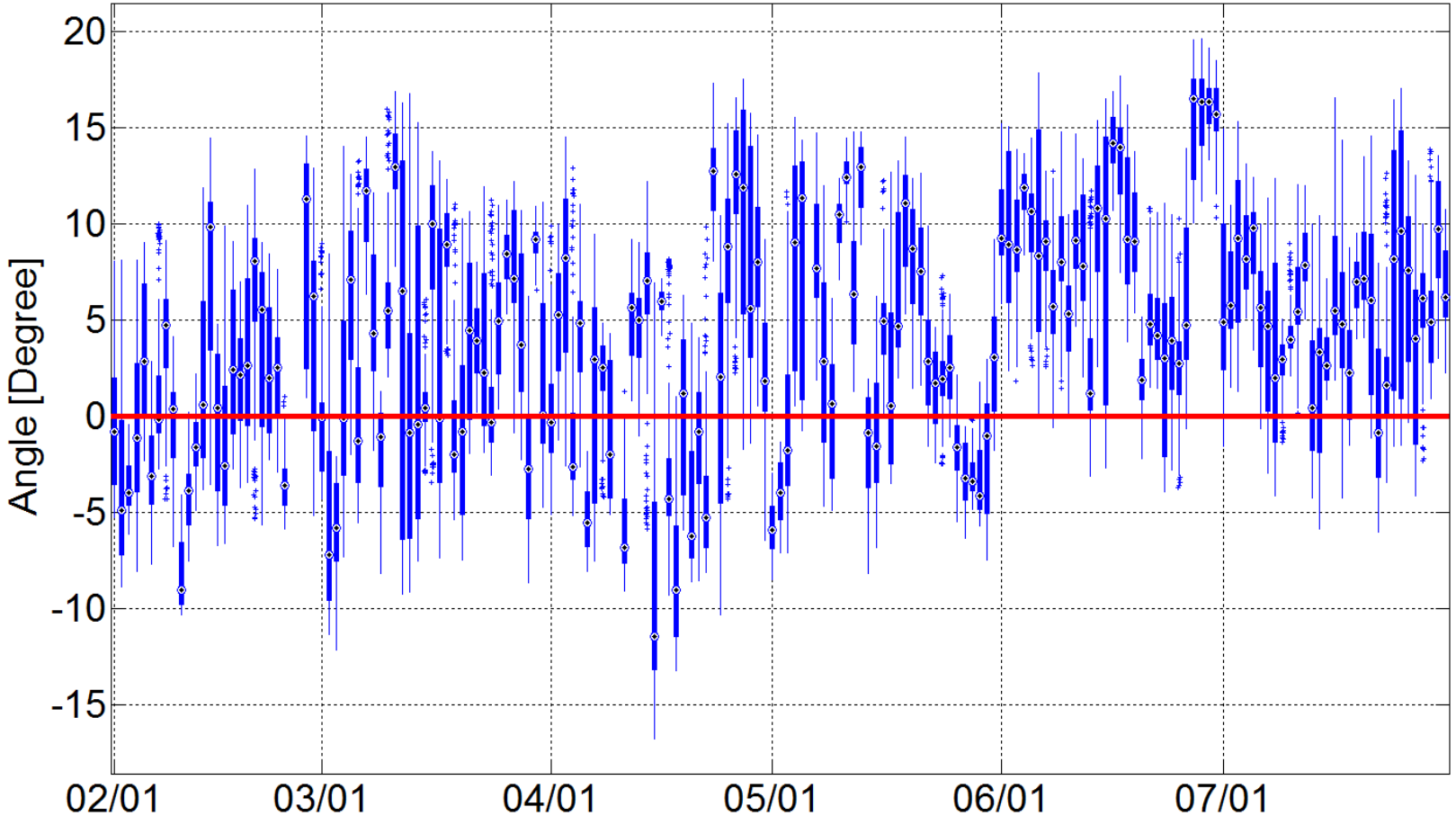
South 10*-North 7



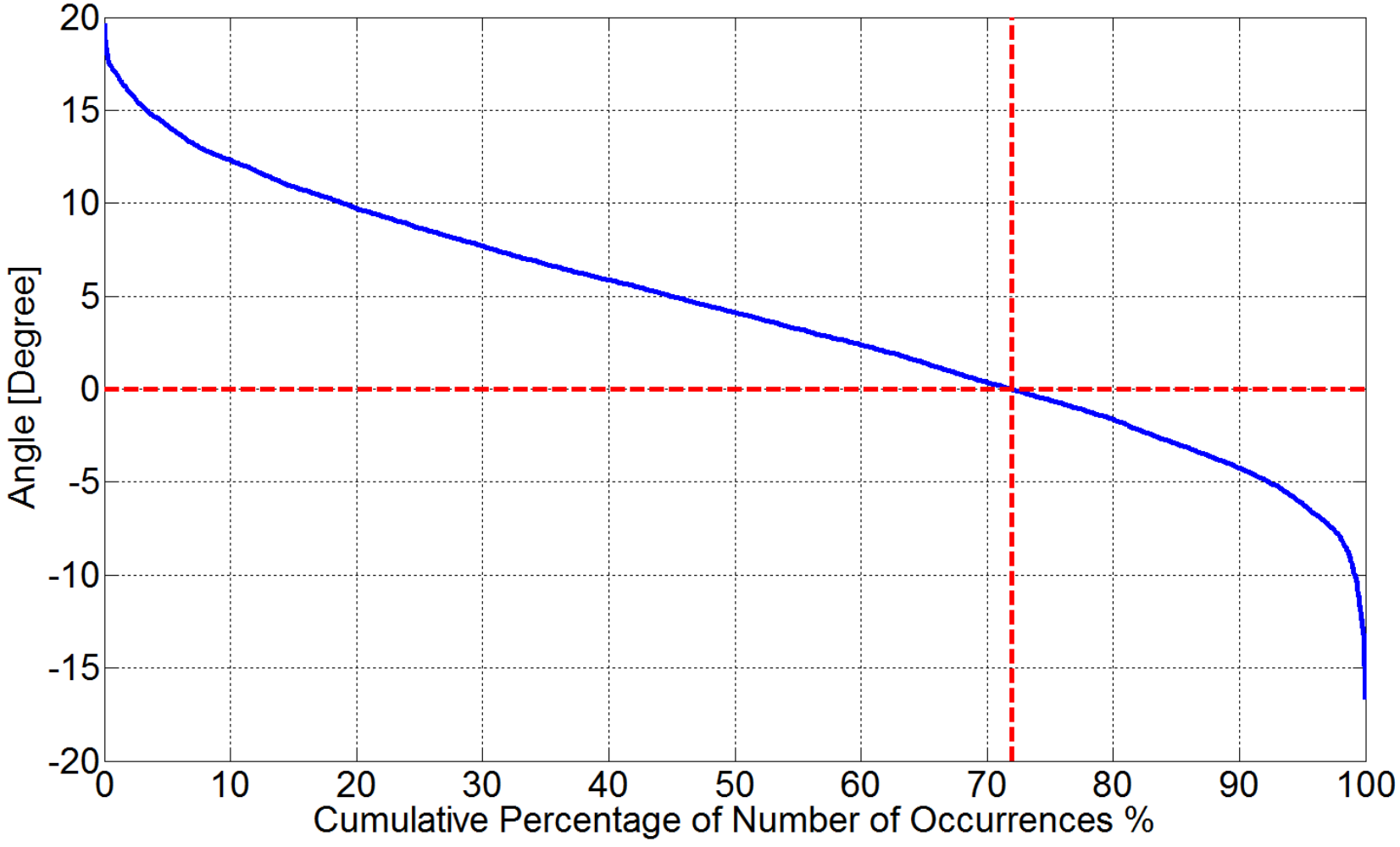
South 10*-North 7



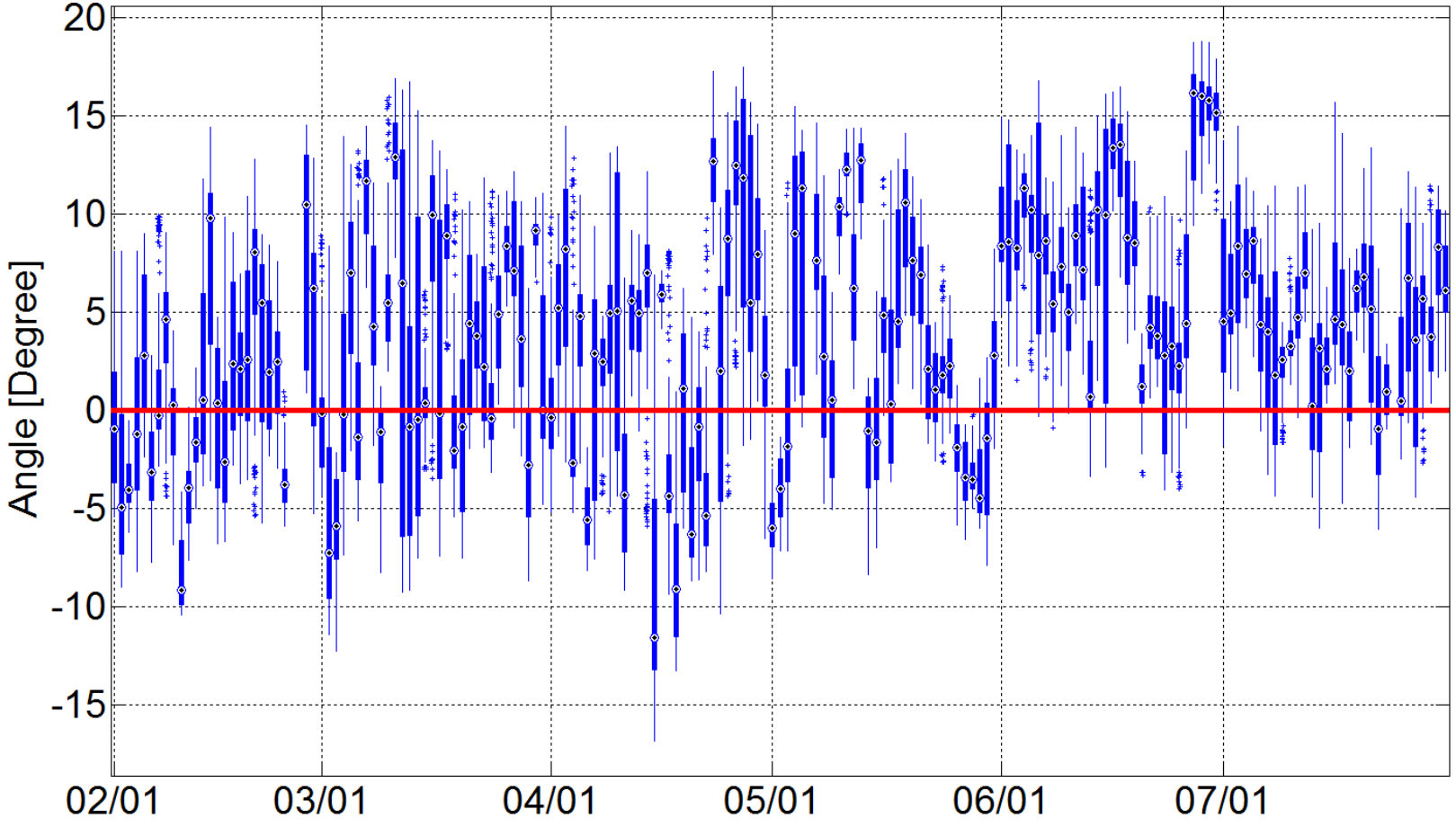
West 17*-North 7



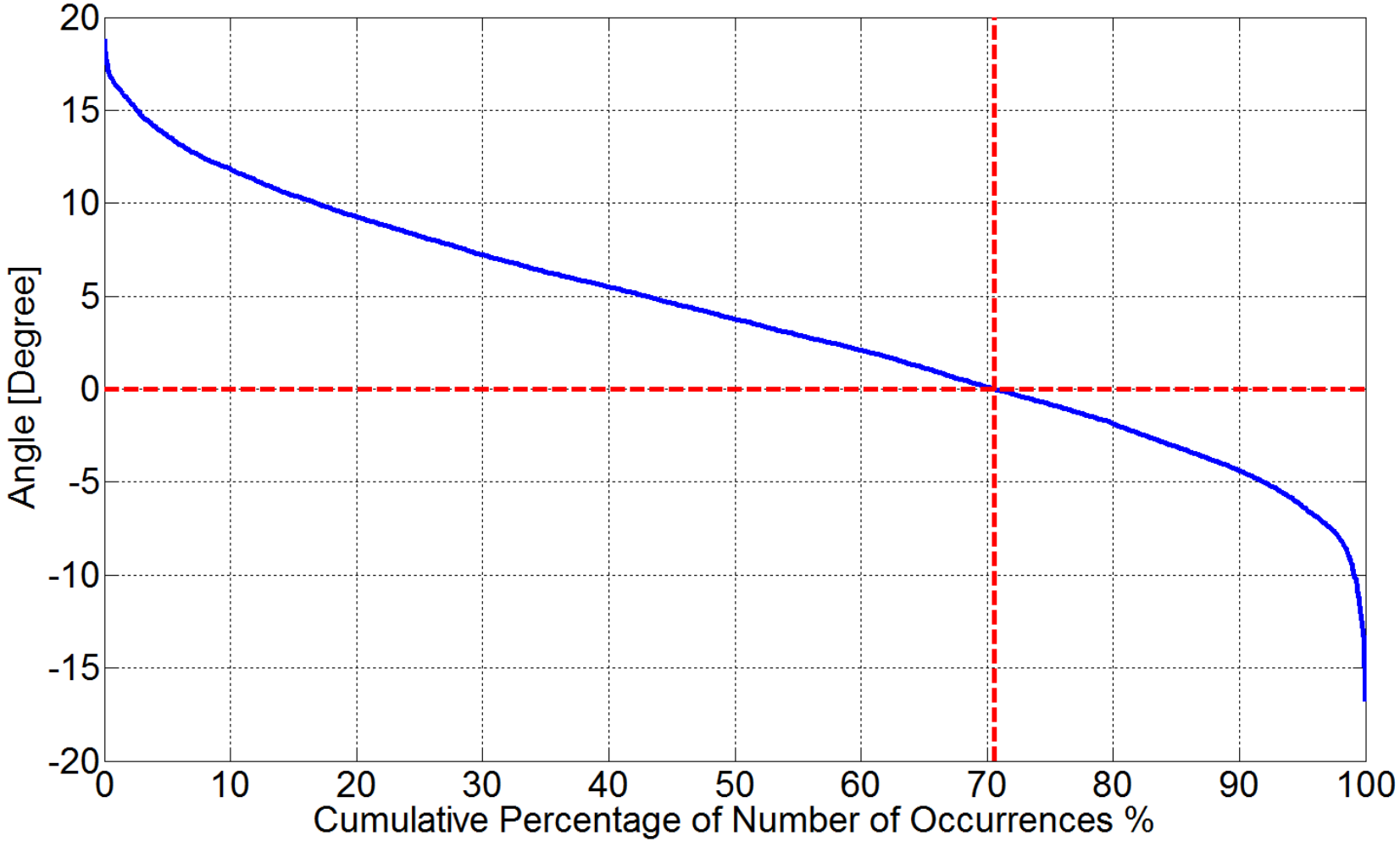
West 17*-North 7



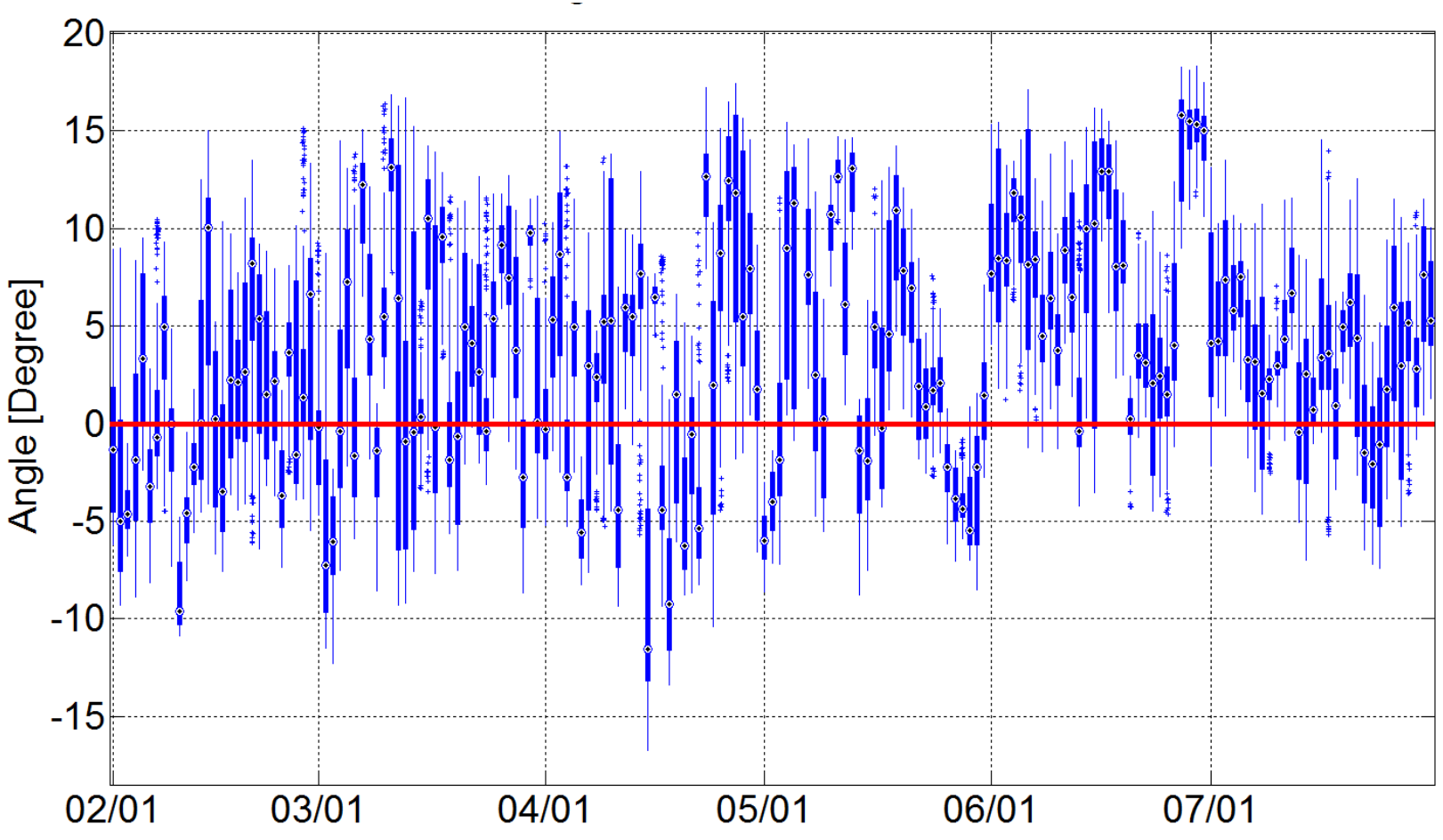
West 13*-North 7



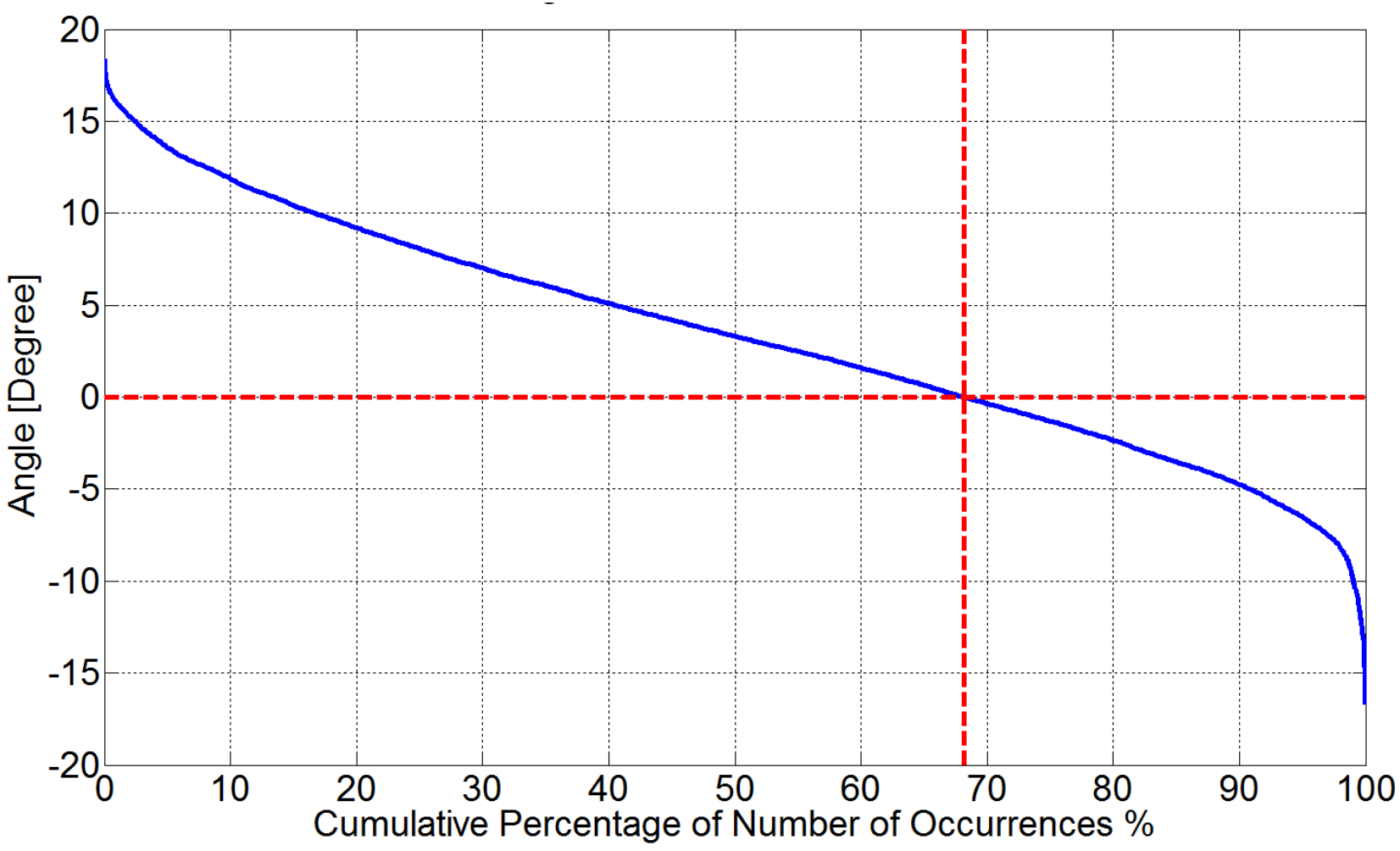
West 13*-North 7



West 19-North 7



West 19-North 7



Appendix A – Part 2
CCET Discovery Across Texas project

Baseline Analysis Update - Voltage Angles (Reference: North 7)

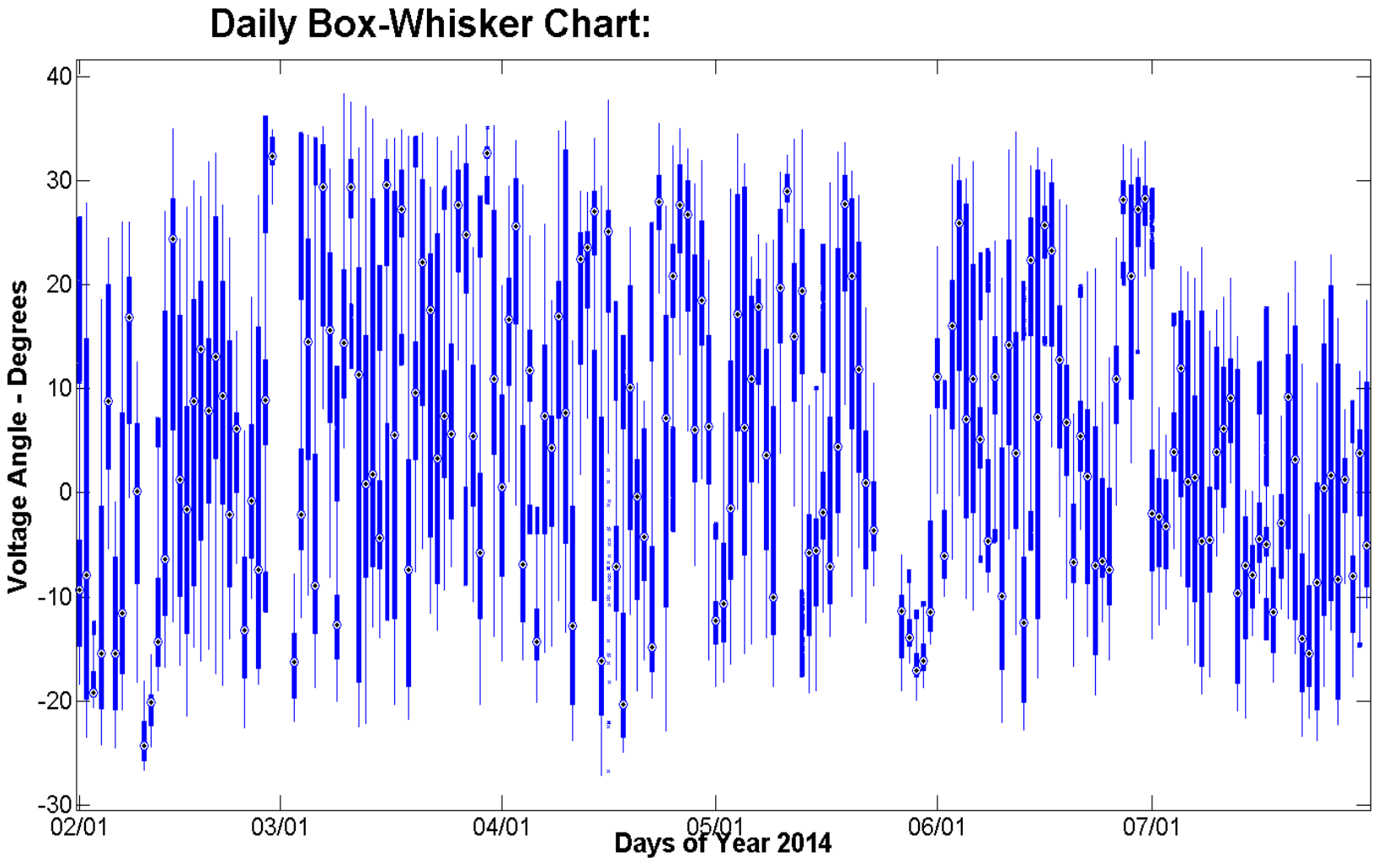
Phasor Data: February to July 2014
Box-Whisker Plots and Time Duration Curves

Electric Power Group

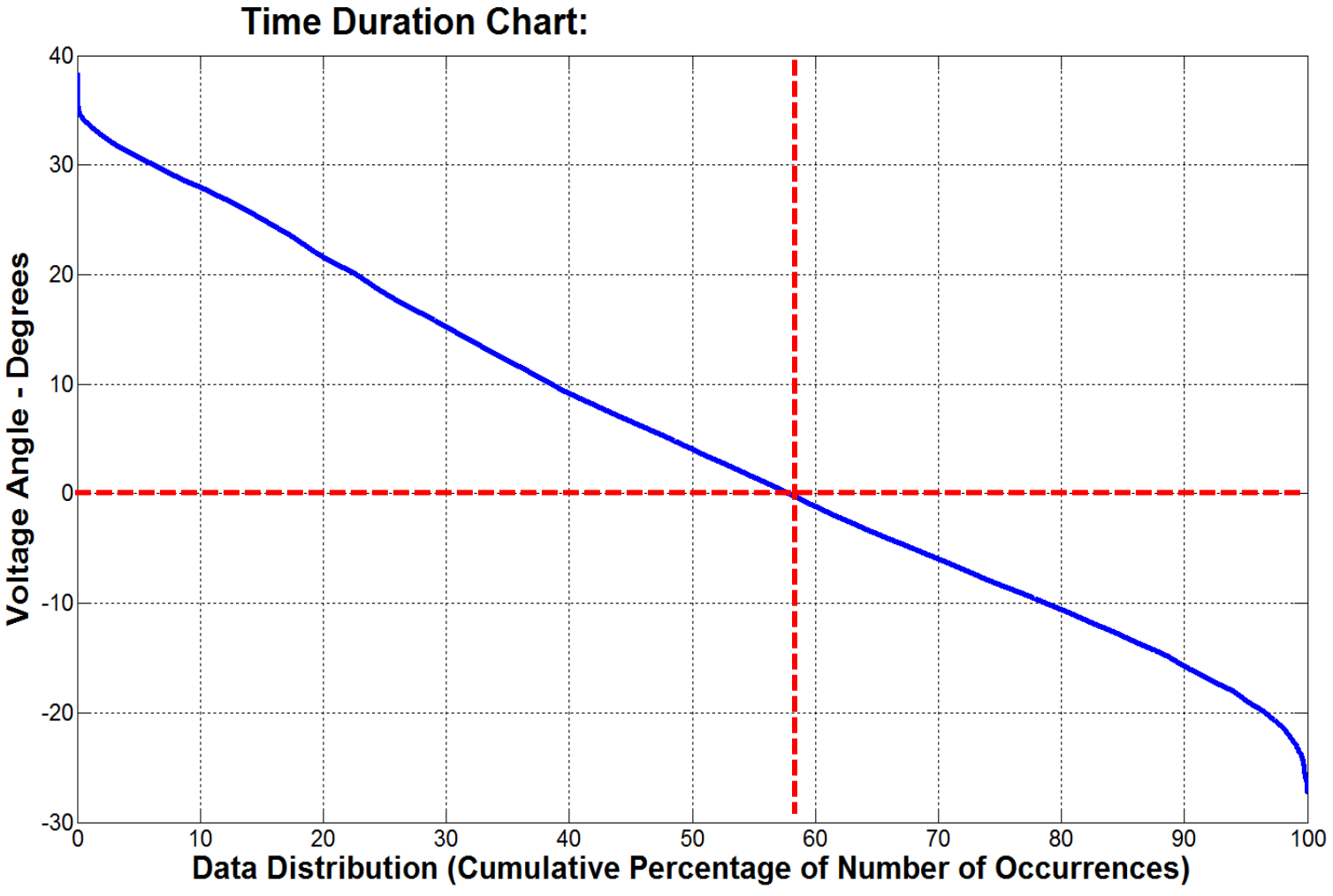
CCET

ERCOT

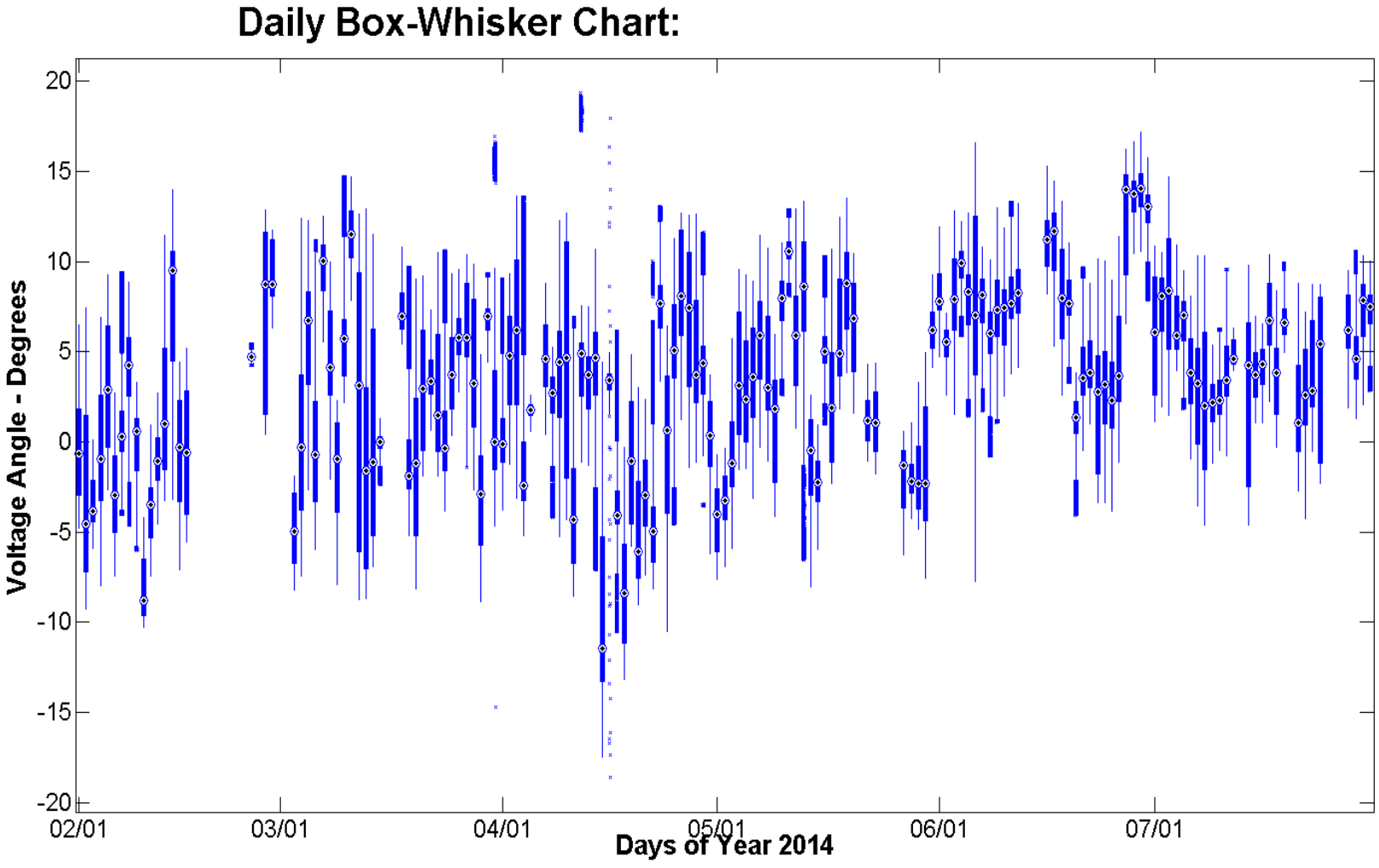
West 10


Daily Box-Whisker Chart:
Voltage Angle - Degrees
40
30
20
10
0
-10
-20
-30
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

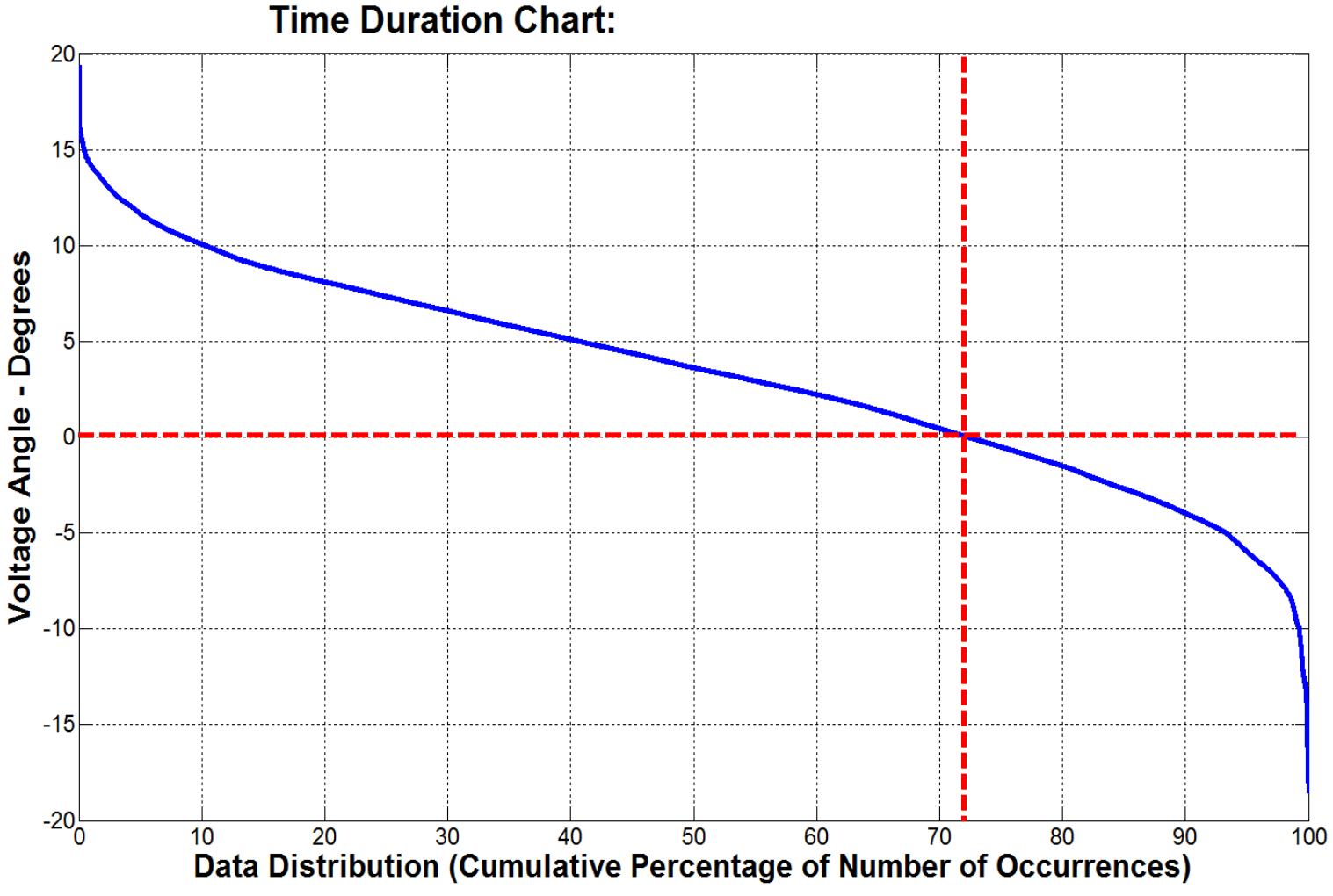
West 10


Time Duration Chart:
Voltage Angle - Degrees
40
30
20
10
0
-10
-20
-30
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

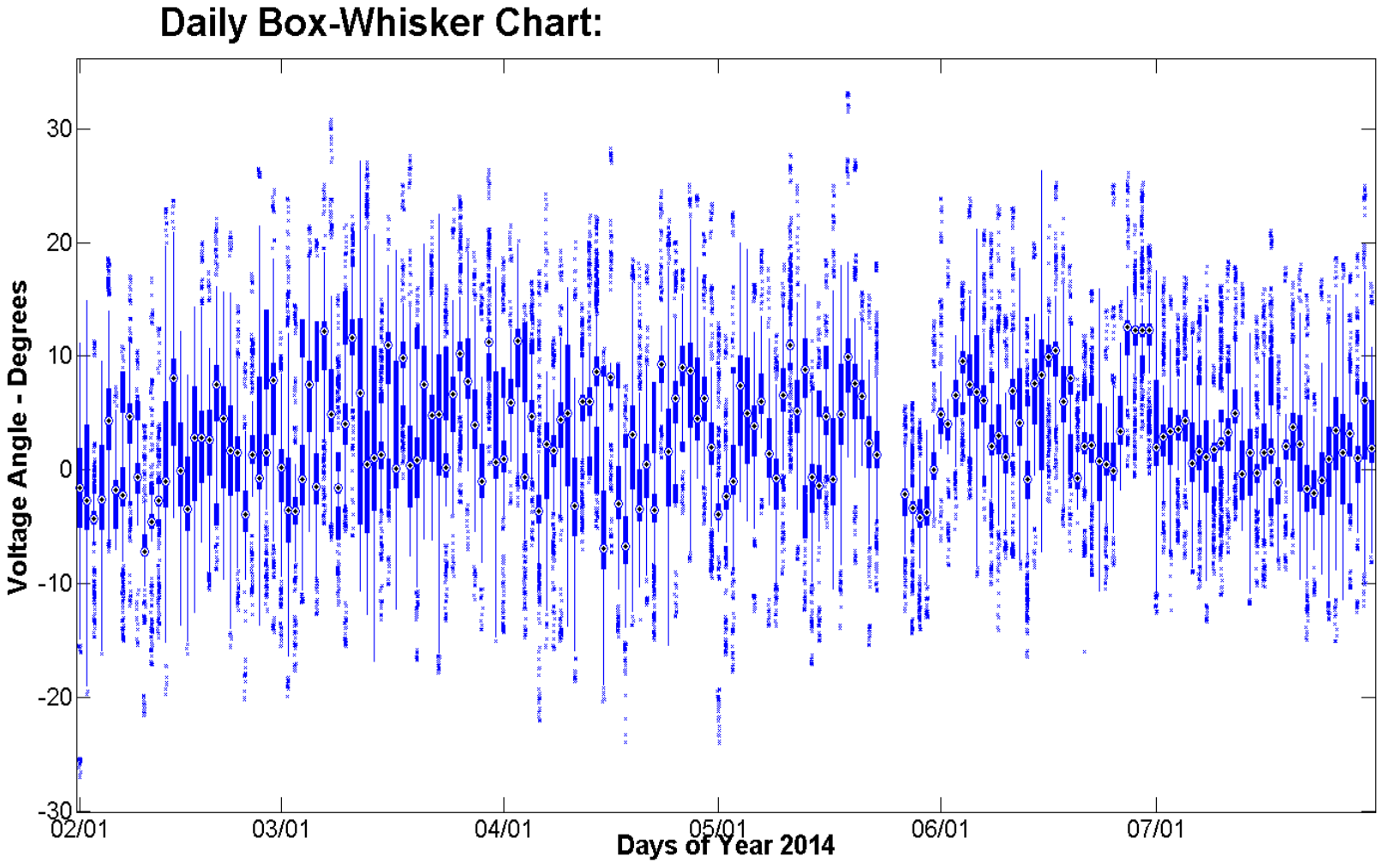
West 14


Daily Box-Whisker Chart:
Voltage Angle - Degrees
20
15
10
5
0
-5
-10
-15
-20
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

West 14

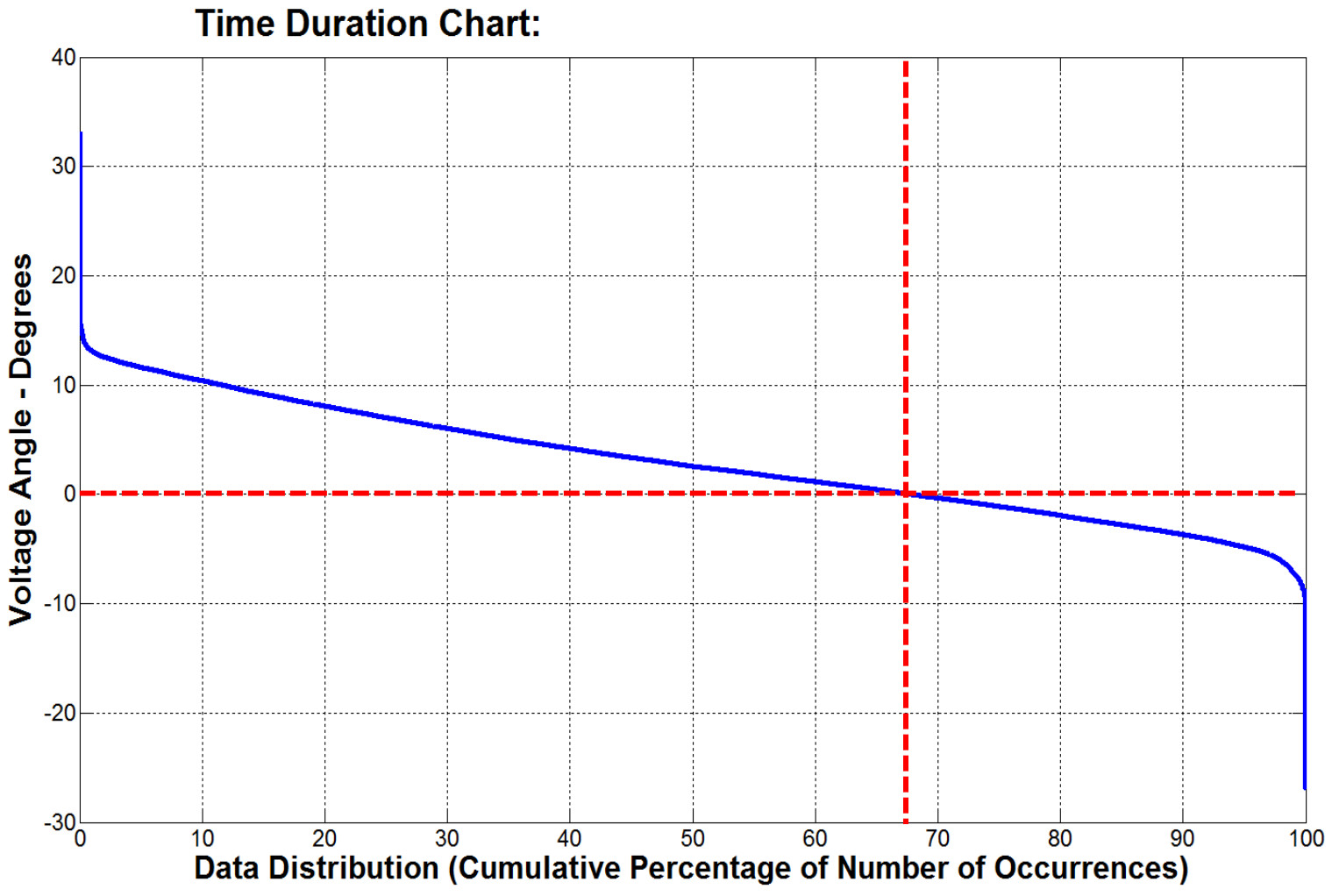

Time Duration Chart:
Voltage Angle - Degrees
20
15
10
5
0
-5
-10
-15
-20
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

West 1*

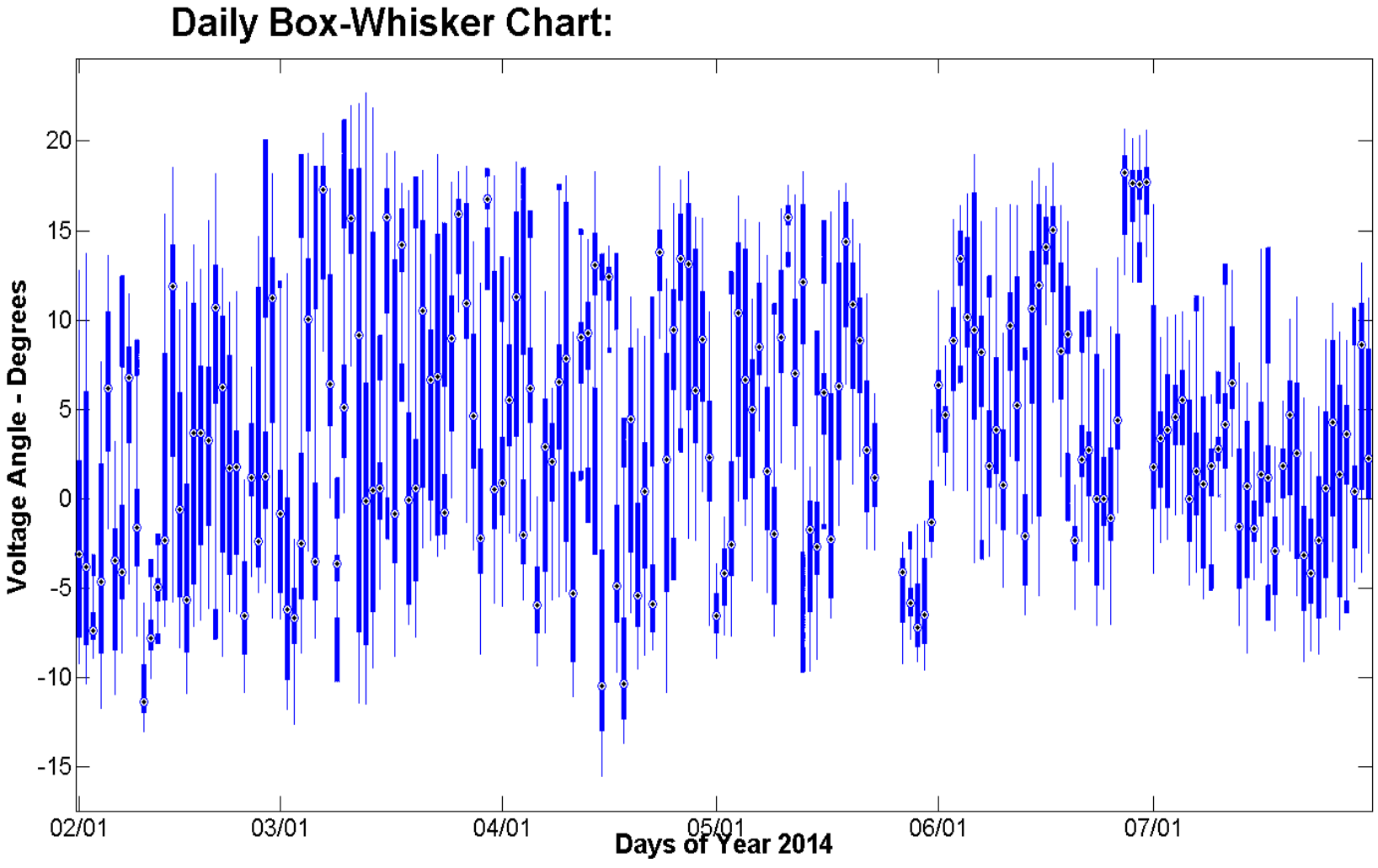


* West 1 PMU has noisy signal

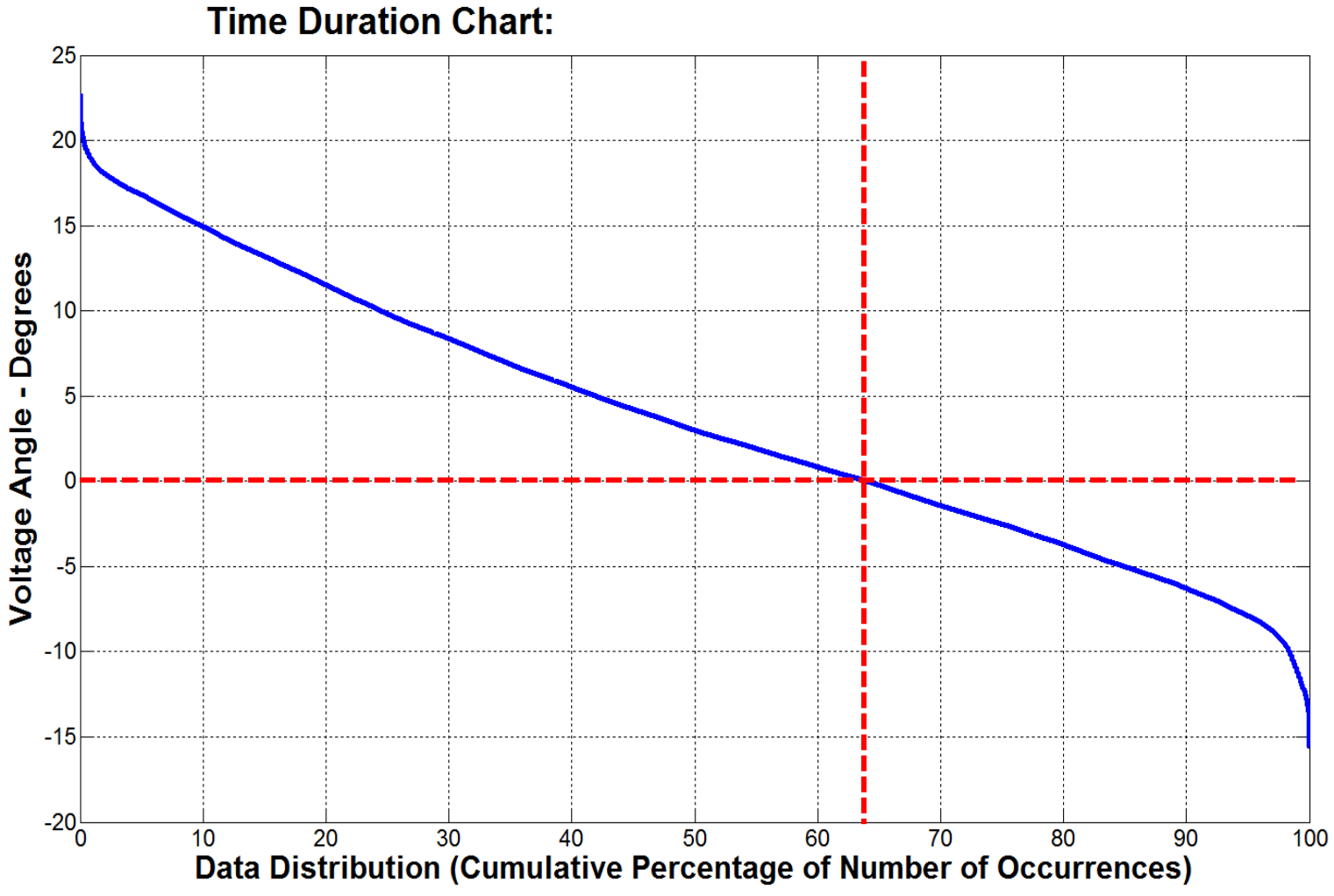
West 1


Time Duration Chart:
Voltage Angle - Degrees
Data Distribution (Cumulative Percentage of Number of Occurrences)
40
30
20
10
0
-10
-20
-30
0
10
20
30
40
50
60
70
80
90
100

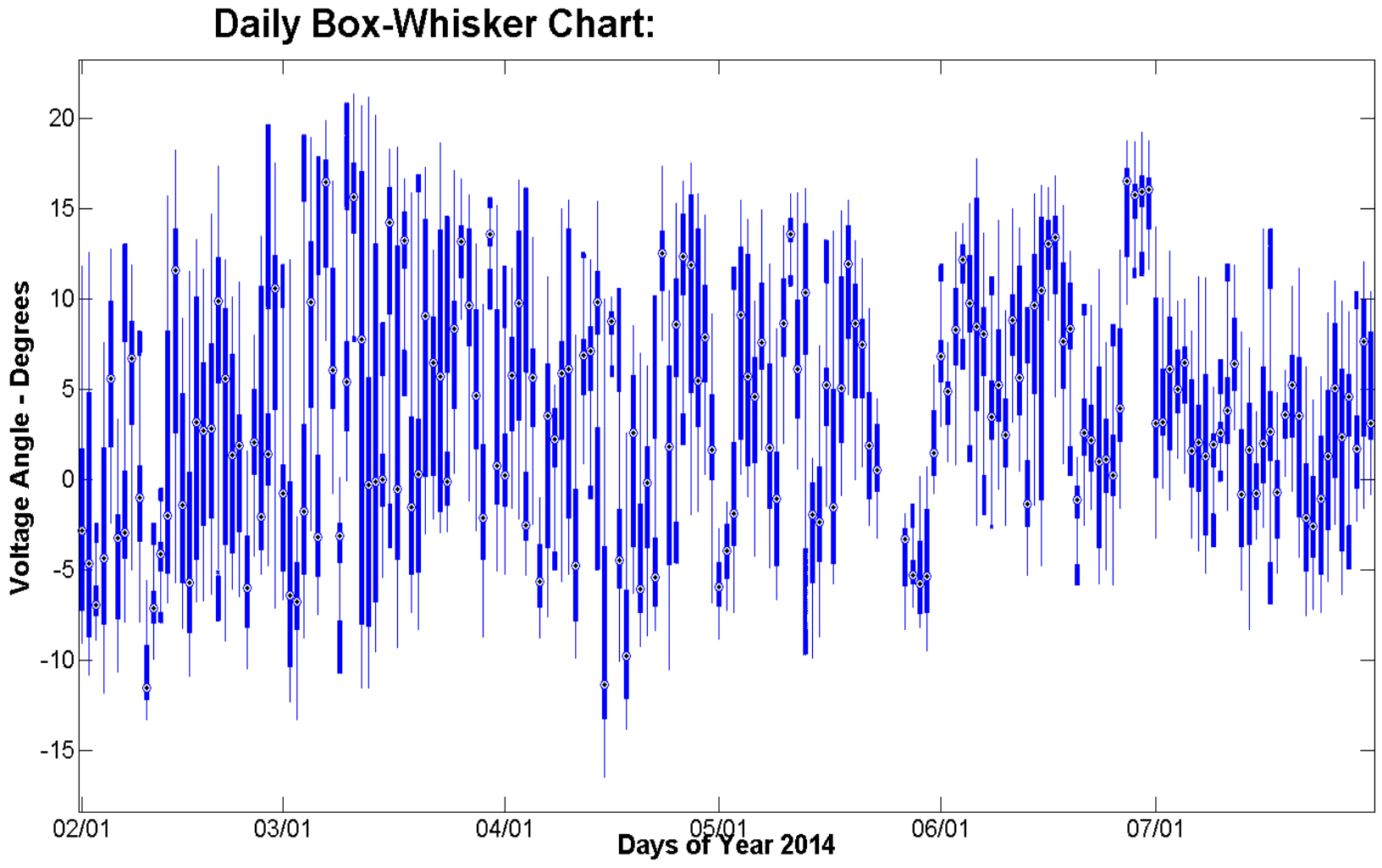
West 2


Daily Box-Whisker Chart:
Voltage Angle - Degrees
20
15
10
5
0
-5
-10
-15
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

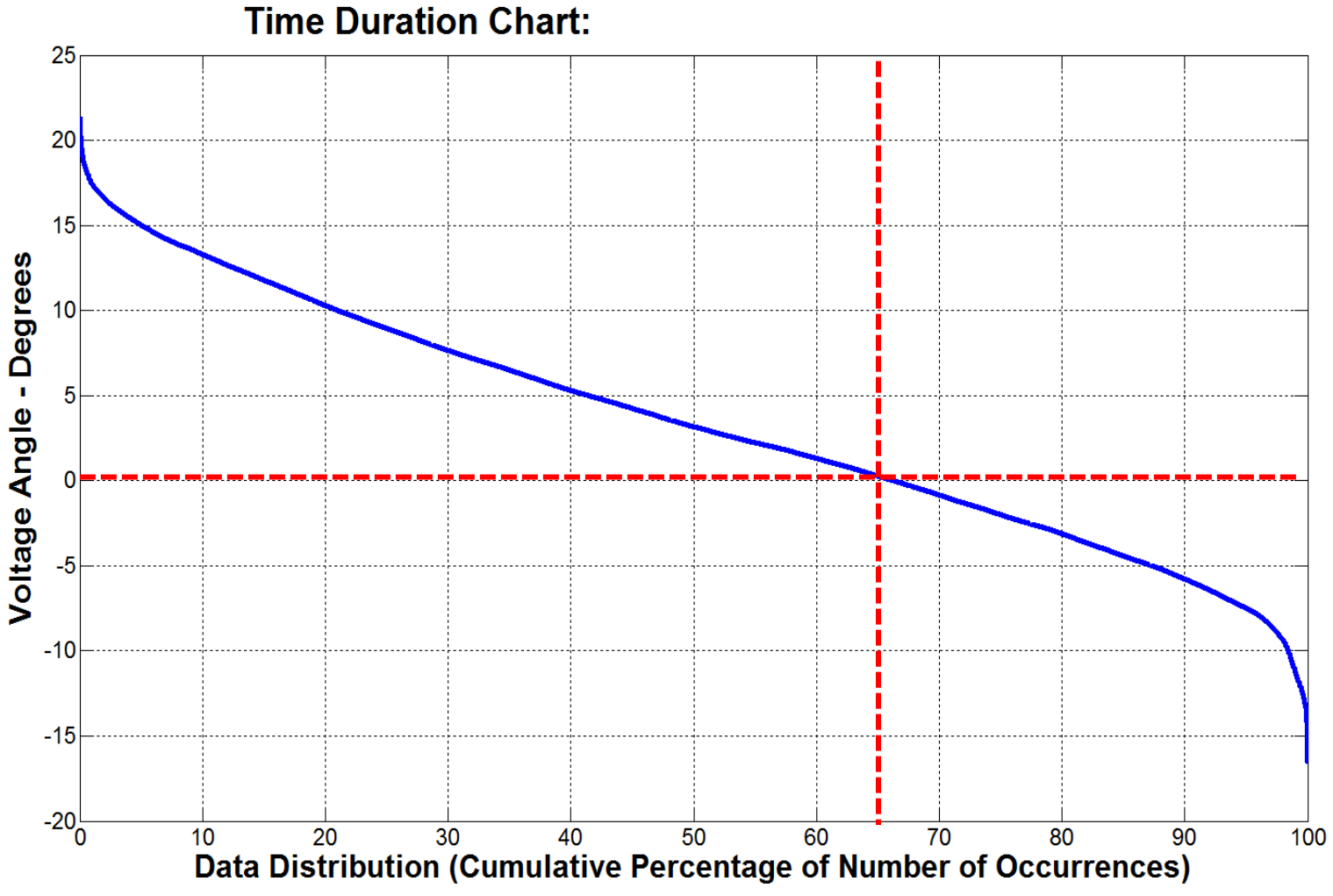
West 2


Time Duration Chart:
Voltage Angle - Degrees
25
20
15
10
5
0
-5
-10
-15
-20
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

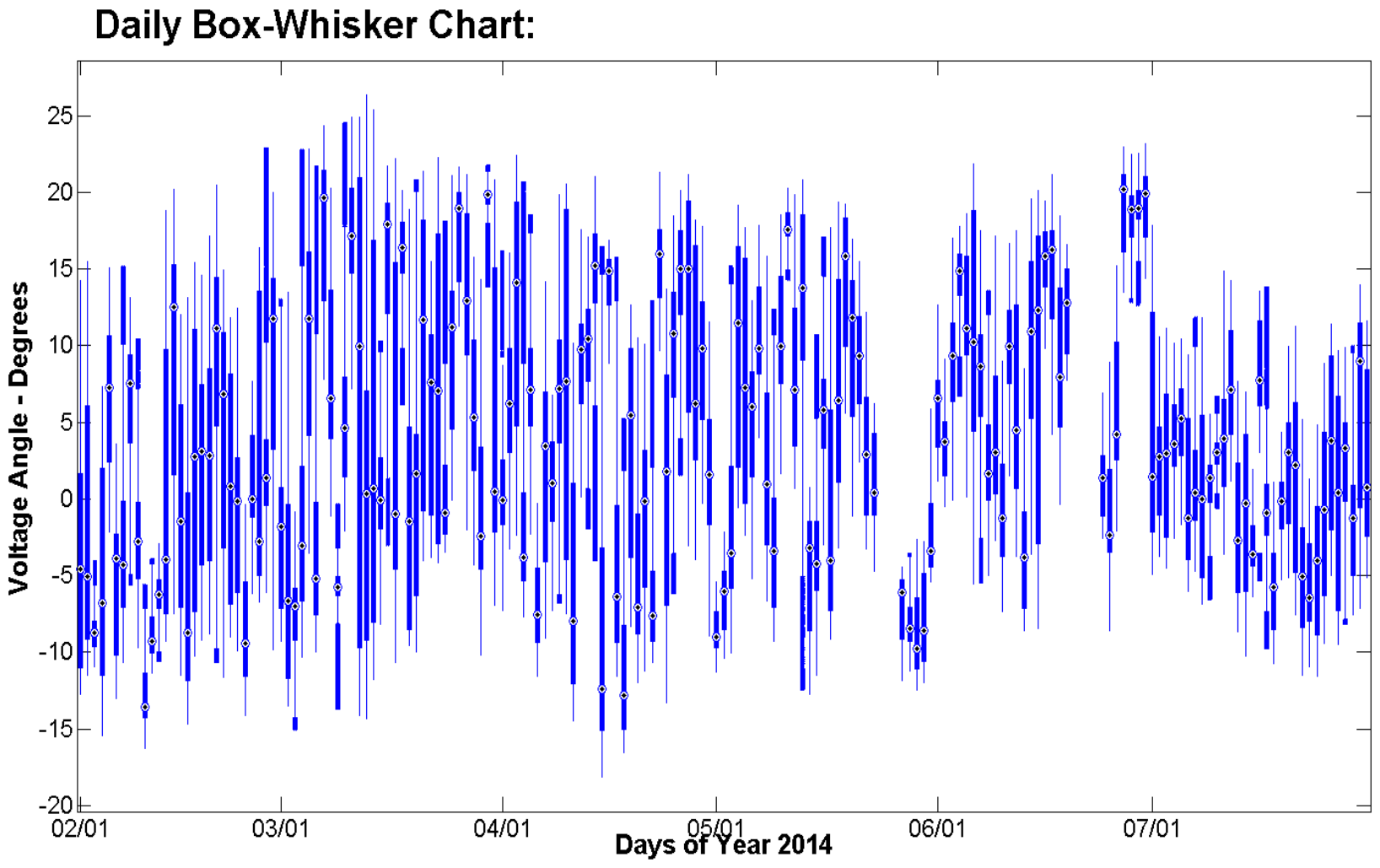
West 9


Daily Box-Whisker Chart:
Voltage Angle - Degrees
20
15
10
5
0
-5
-10
-15
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

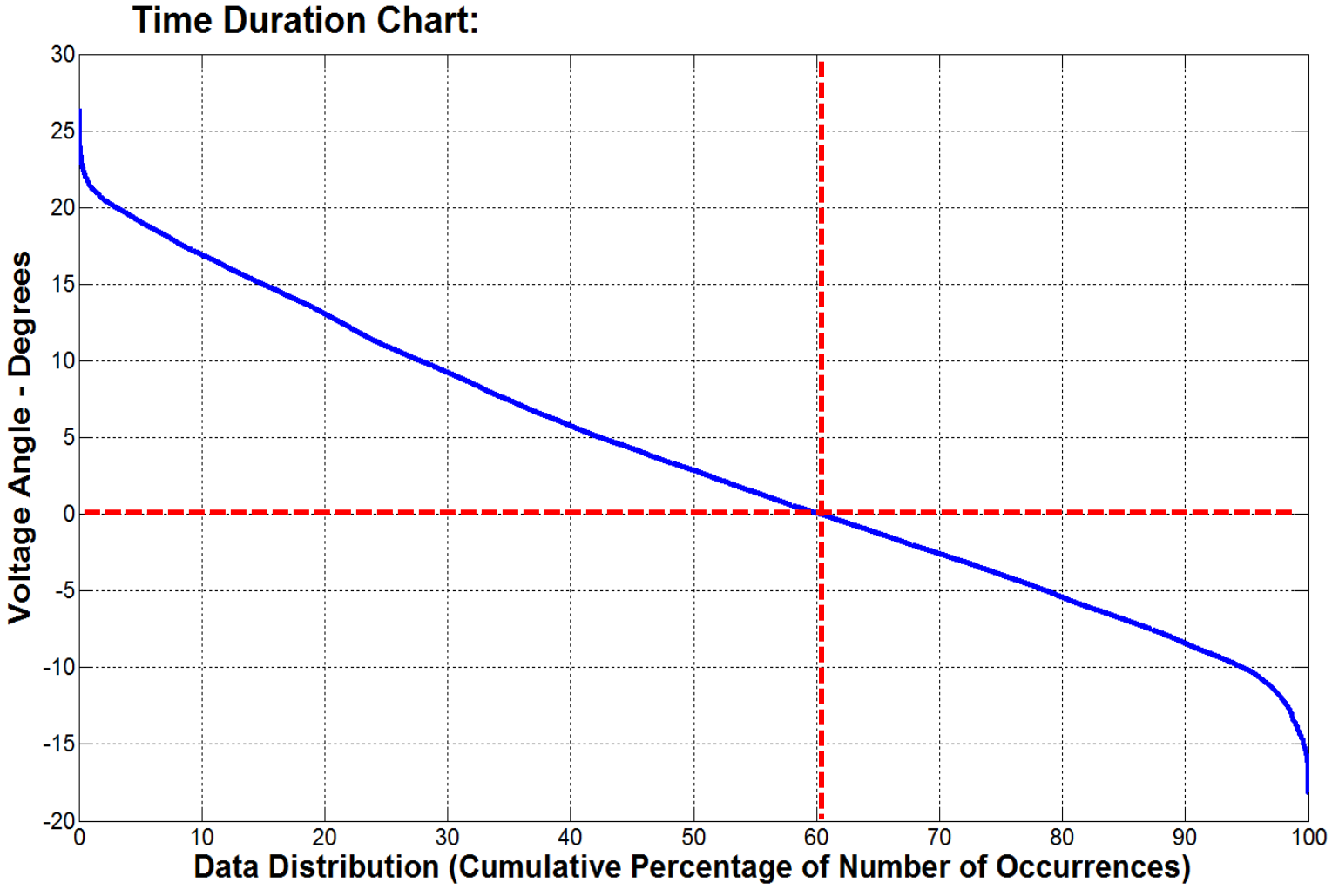
West 9


Time Duration Chart:
Voltage Angle - Degrees
25
20
15
10
5
0
-5
-10
-15
-20
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

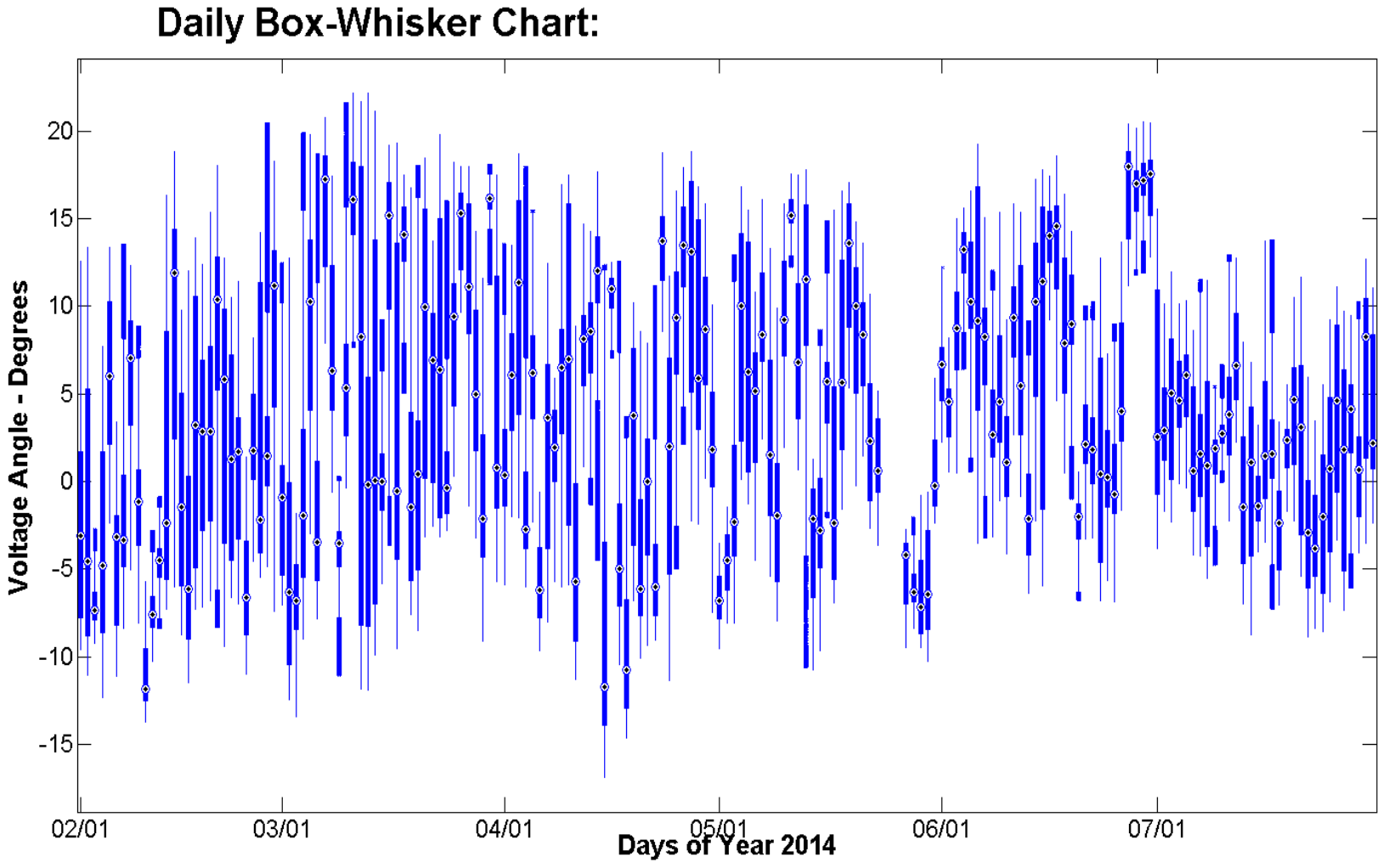
West 11


Daily Box-Whisker Chart:
Voltage Angle - Degrees
25
20
15
10
5
0
-5
-10
-15
-20
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

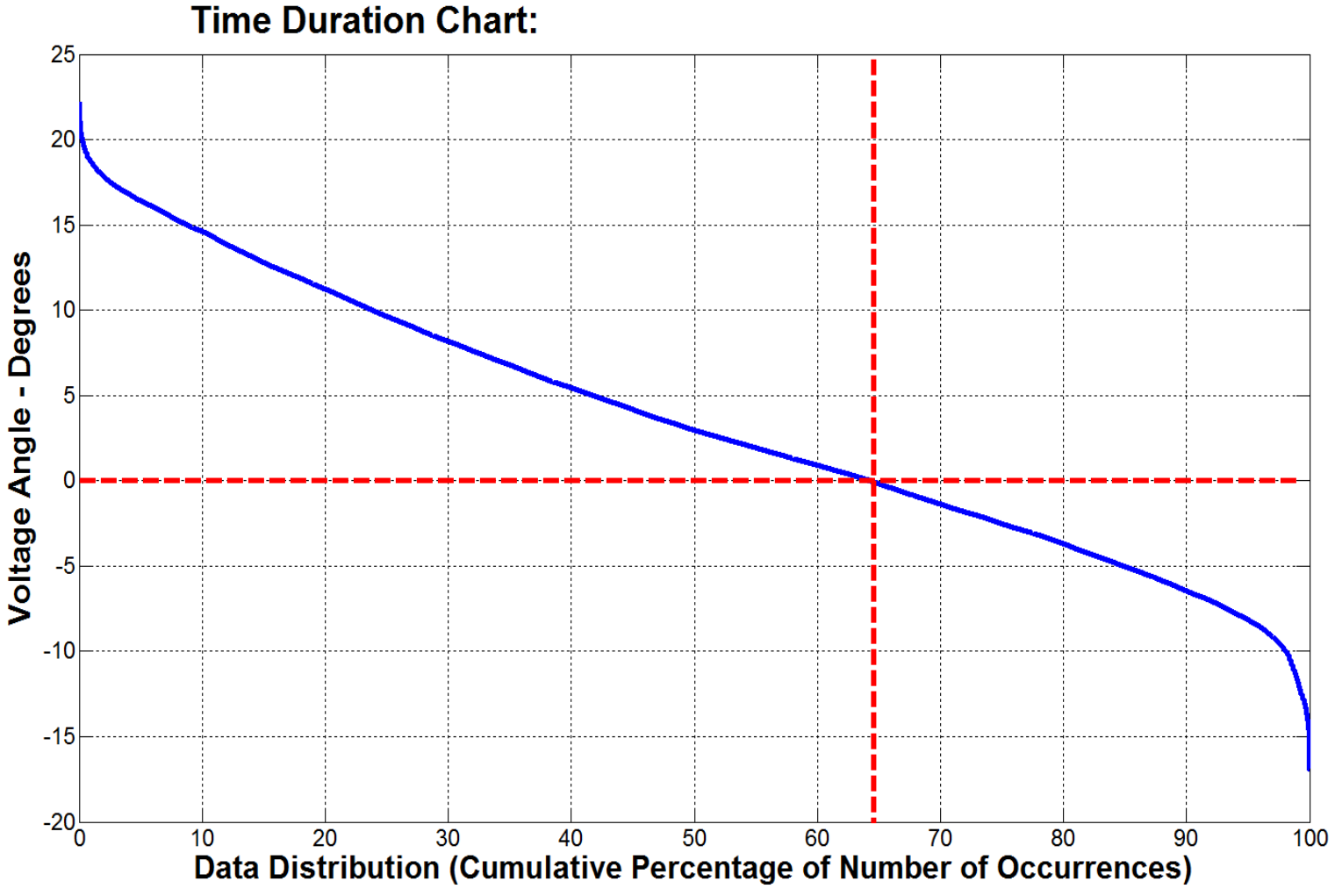
West 11


Time Duration Chart:
Voltage Angle - Degrees
30
25
20
15
10
5
0
-5
-10
-15
-20
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

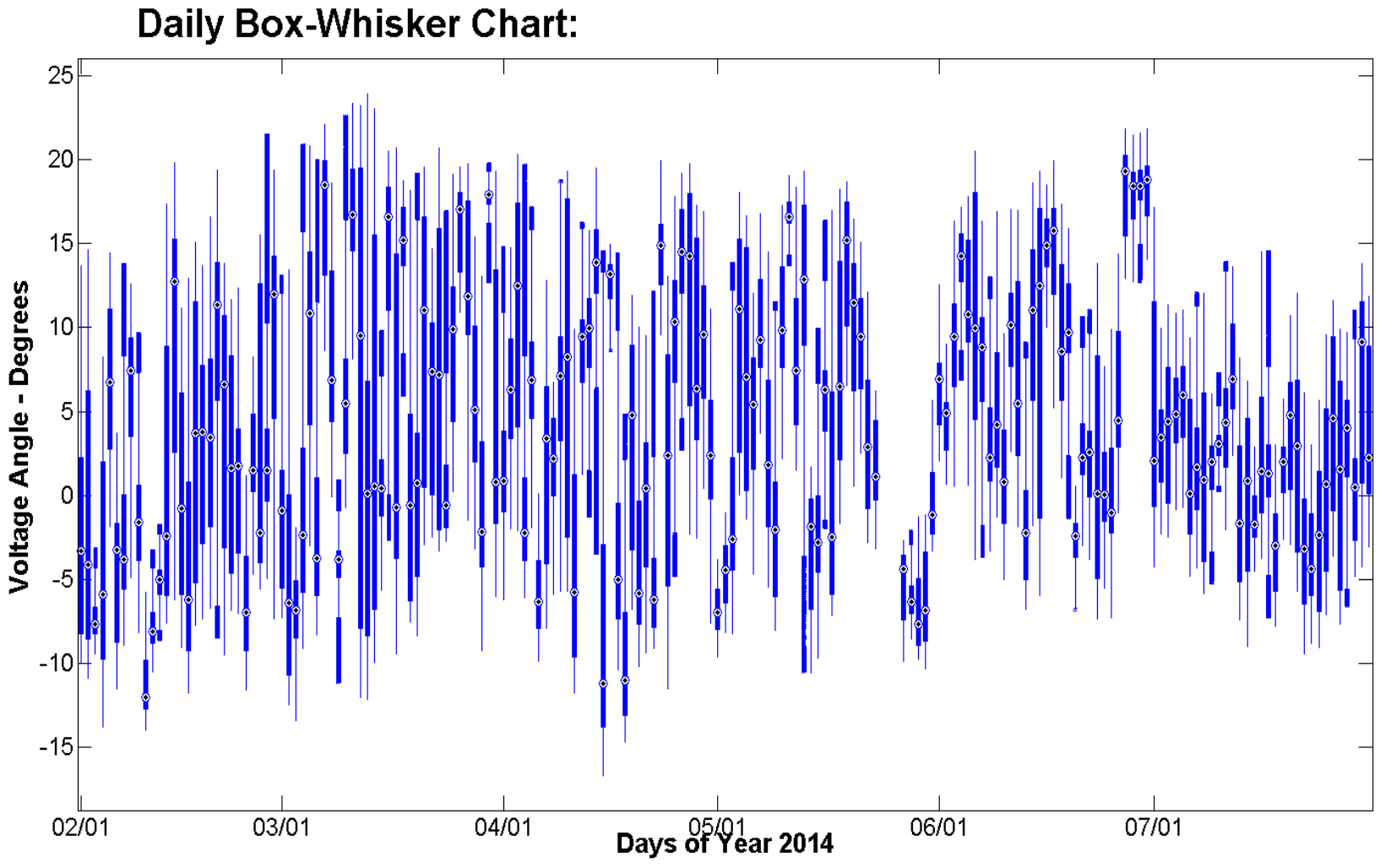
West 12


Daily Box-Whisker Chart:
Voltage Angle - Degrees
20
15
10
5
0
-5
-10
-15
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

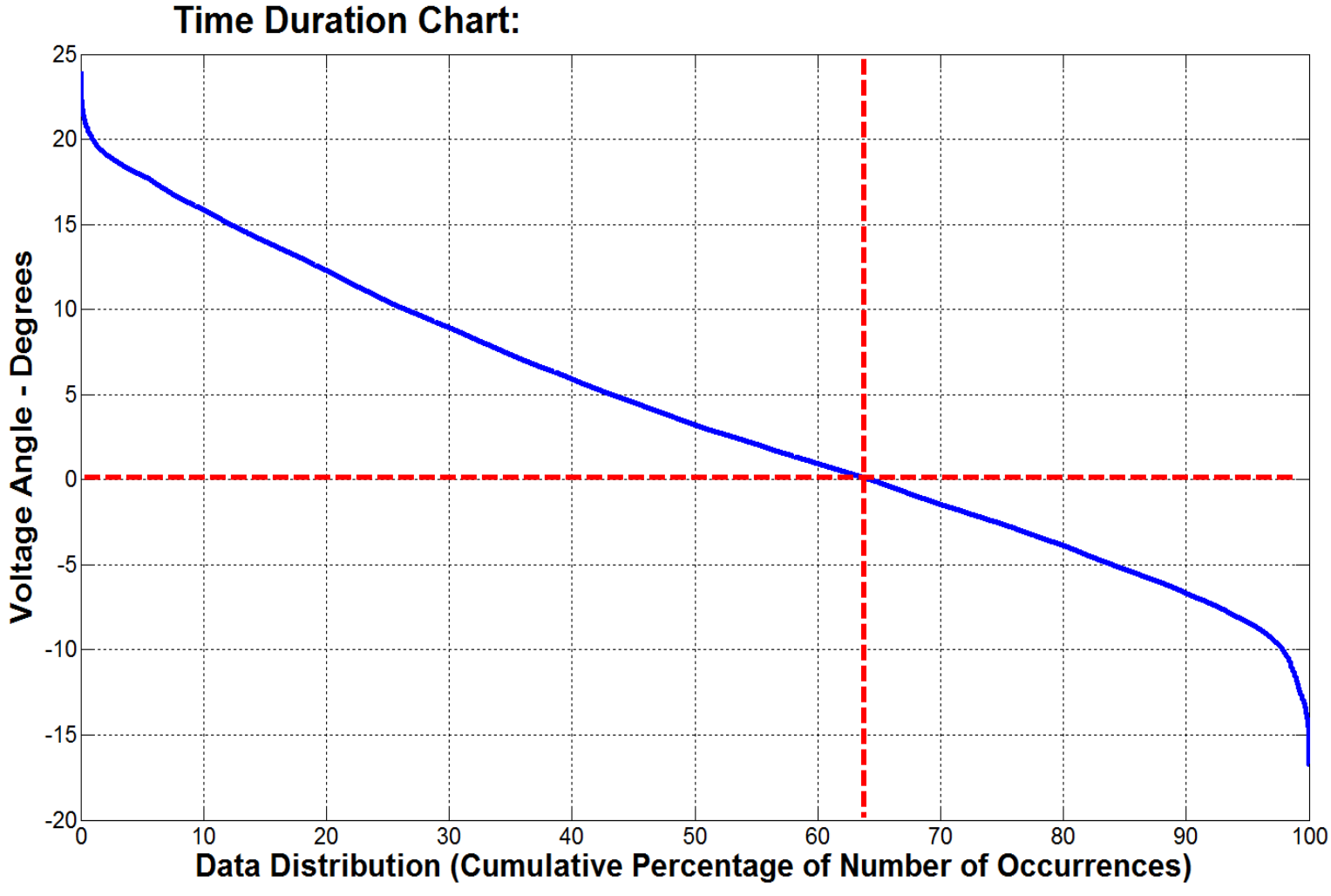
West 12


Time Duration Chart:
Voltage Angle - Degrees
25
20
15
10
5
0
-5
-10
-15
-20
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

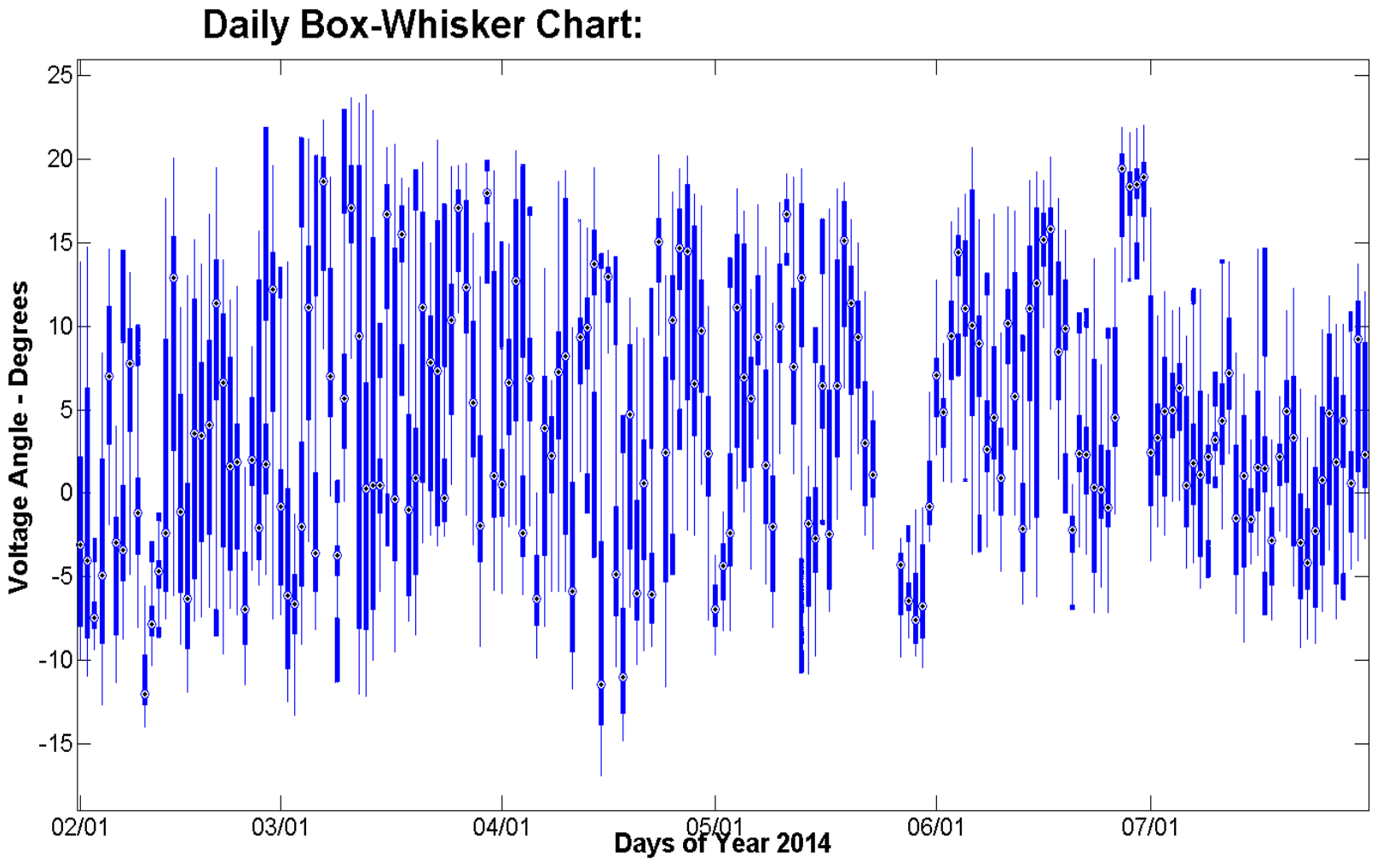
West 5


Daily Box-Whisker Chart:
Voltage Angle - Degrees
25
20
15
10
5
0
-5
-10
-15
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

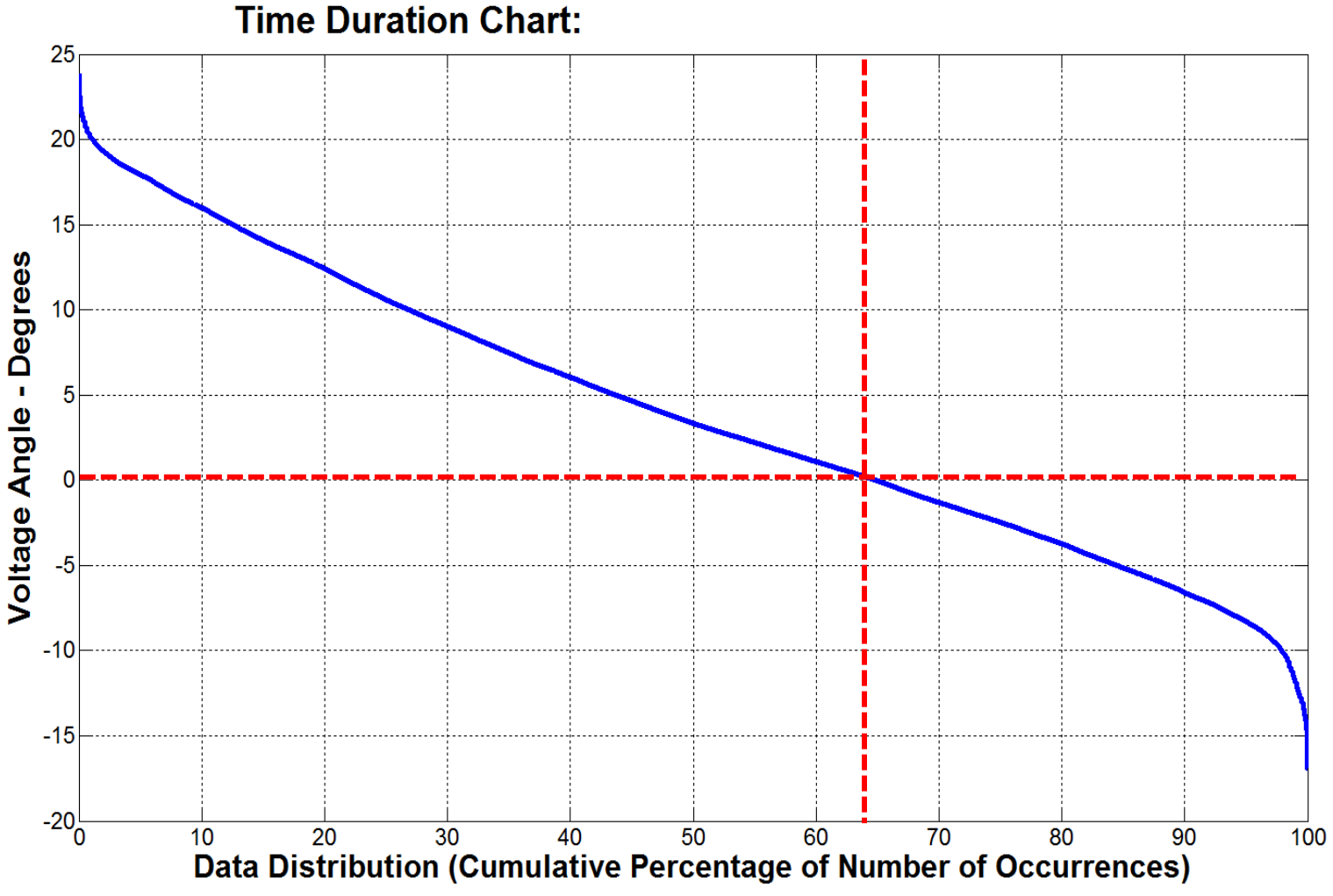
West 5


Time Duration Chart:
Voltage Angle - Degrees
25
20
15
10
5
0
-5
-10
-15
-20
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

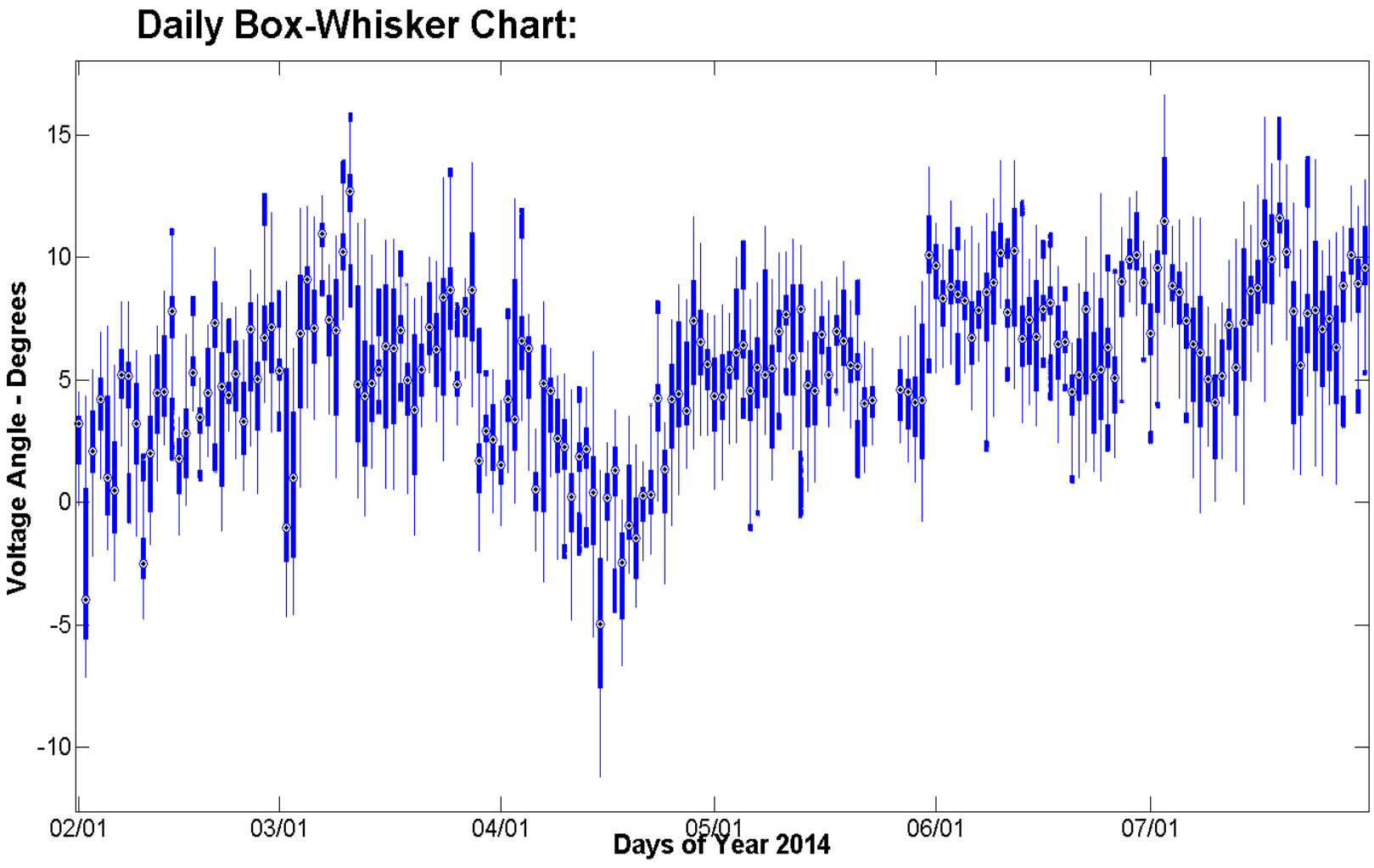
West 6


Daily Box-Whisker Chart:
Voltage Angle - Degrees
25
20
15
10
5
0
-5
-10
-15
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

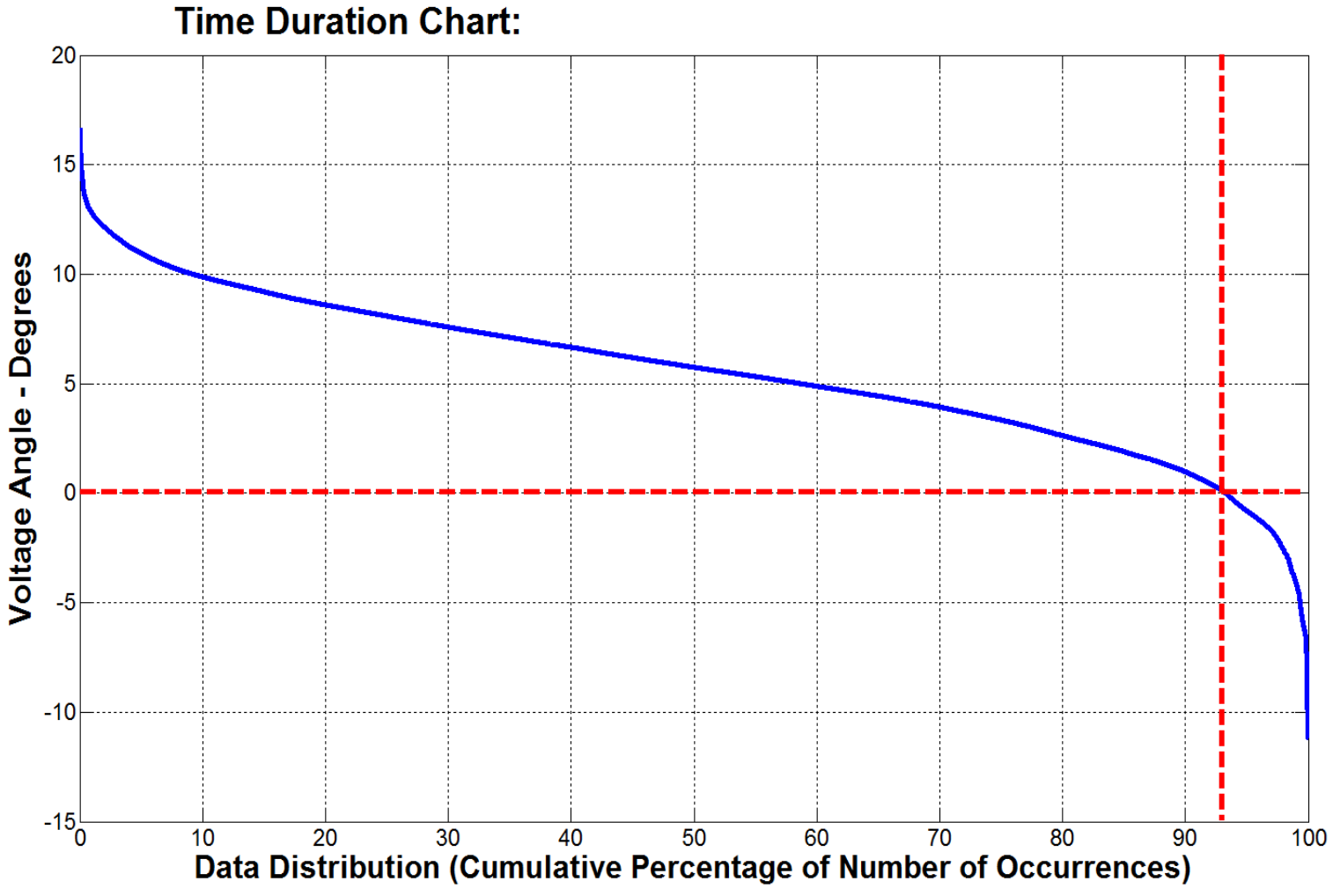
West 6


Time Duration Chart:
Voltage Angle - Degrees
25
20
15
10
5
0
-5
-10
-15
-20
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

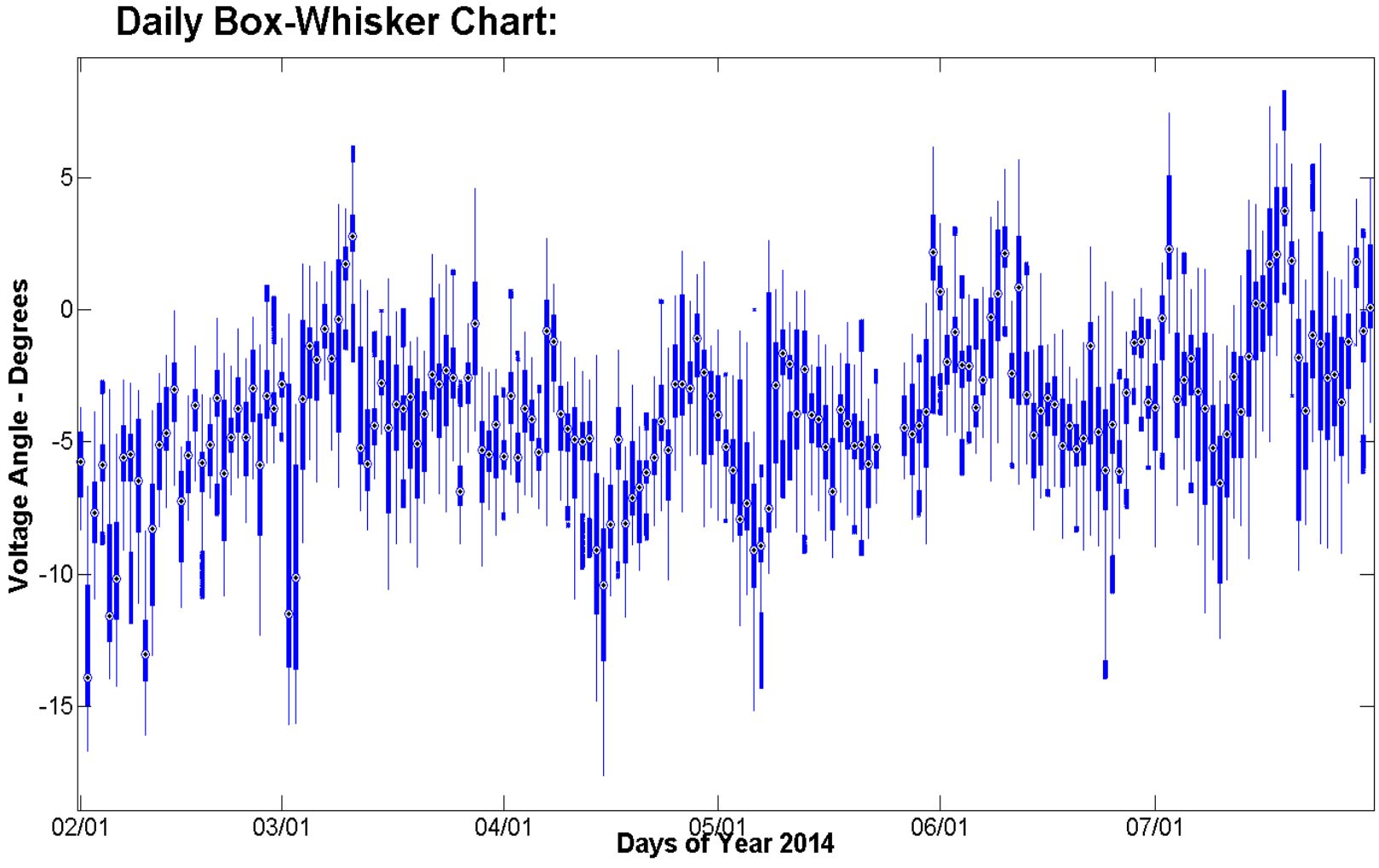
North 1


Daily Box-Whisker Chart:
Voltage Angle - Degrees
15
10
5
0
-5
-10
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

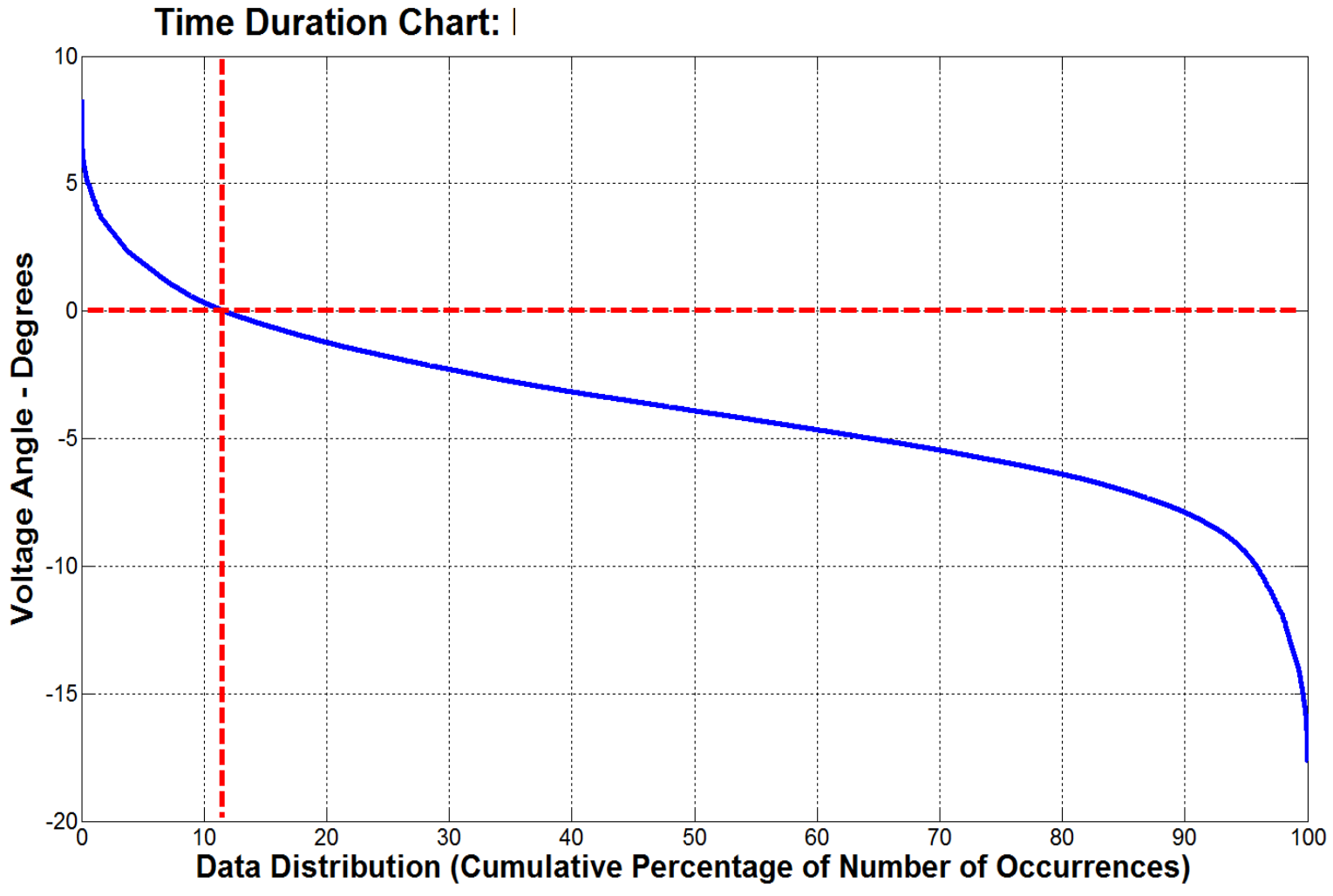
North 1


Time Duration Chart:
Voltage Angle - Degrees
20
15
10
5
0
-5
-10
-15
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

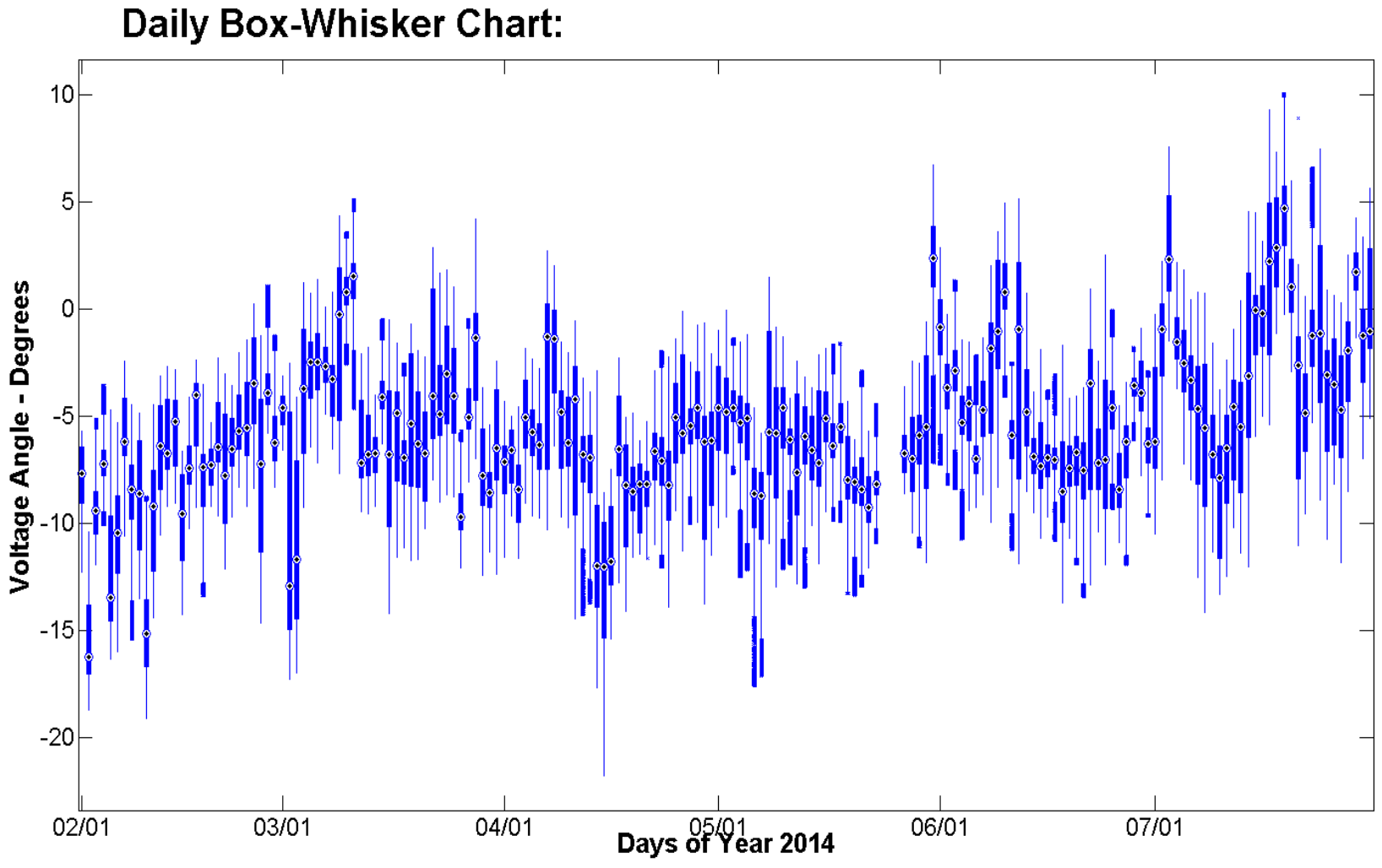
North 4


Daily Box-Whisker Chart:
Voltage Angle - Degrees
5
0
-5
-10
-15
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

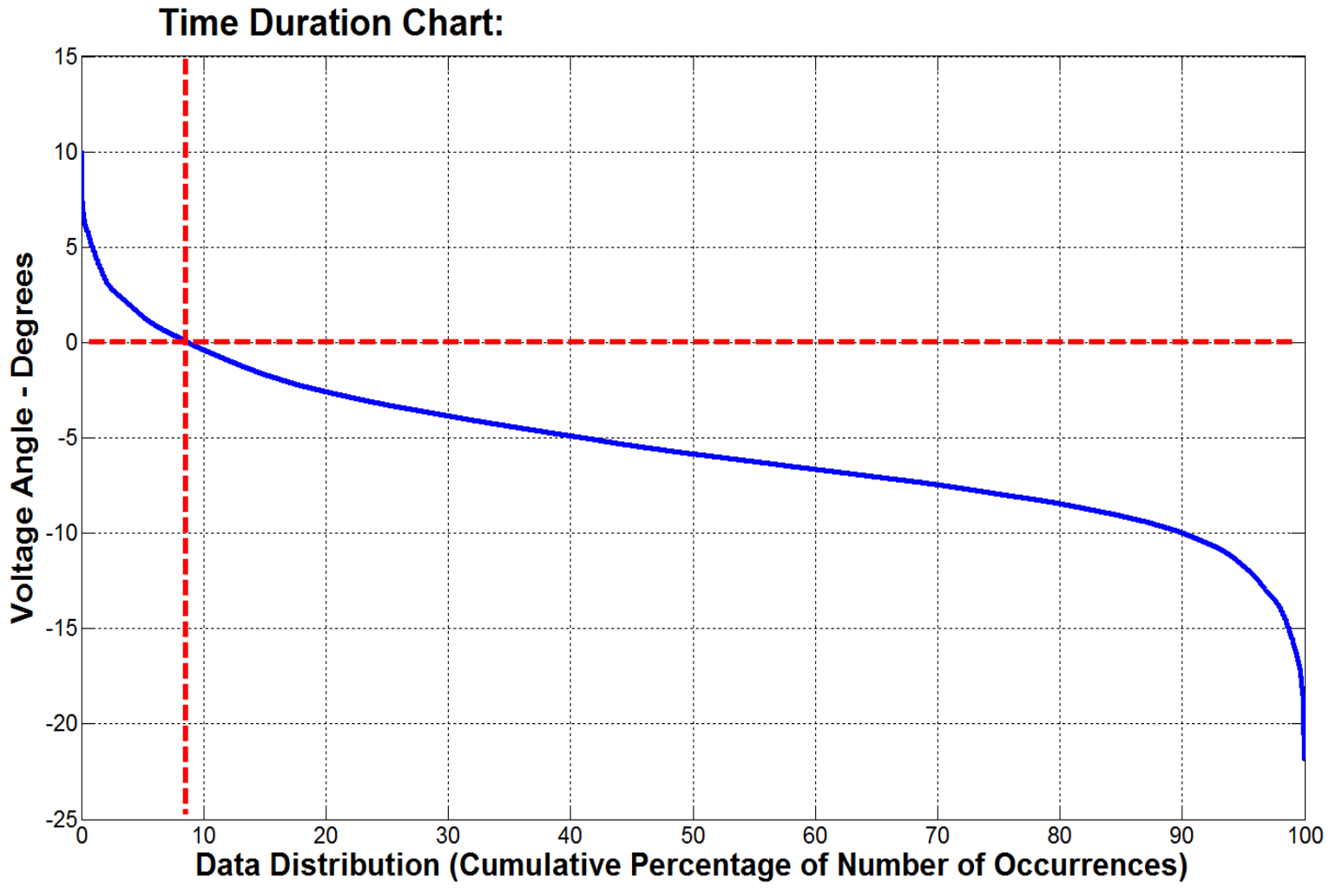
North 4


Time Duration Chart:
Voltage Angle - Degrees
10
5
0
-5
-10
-15
-20
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

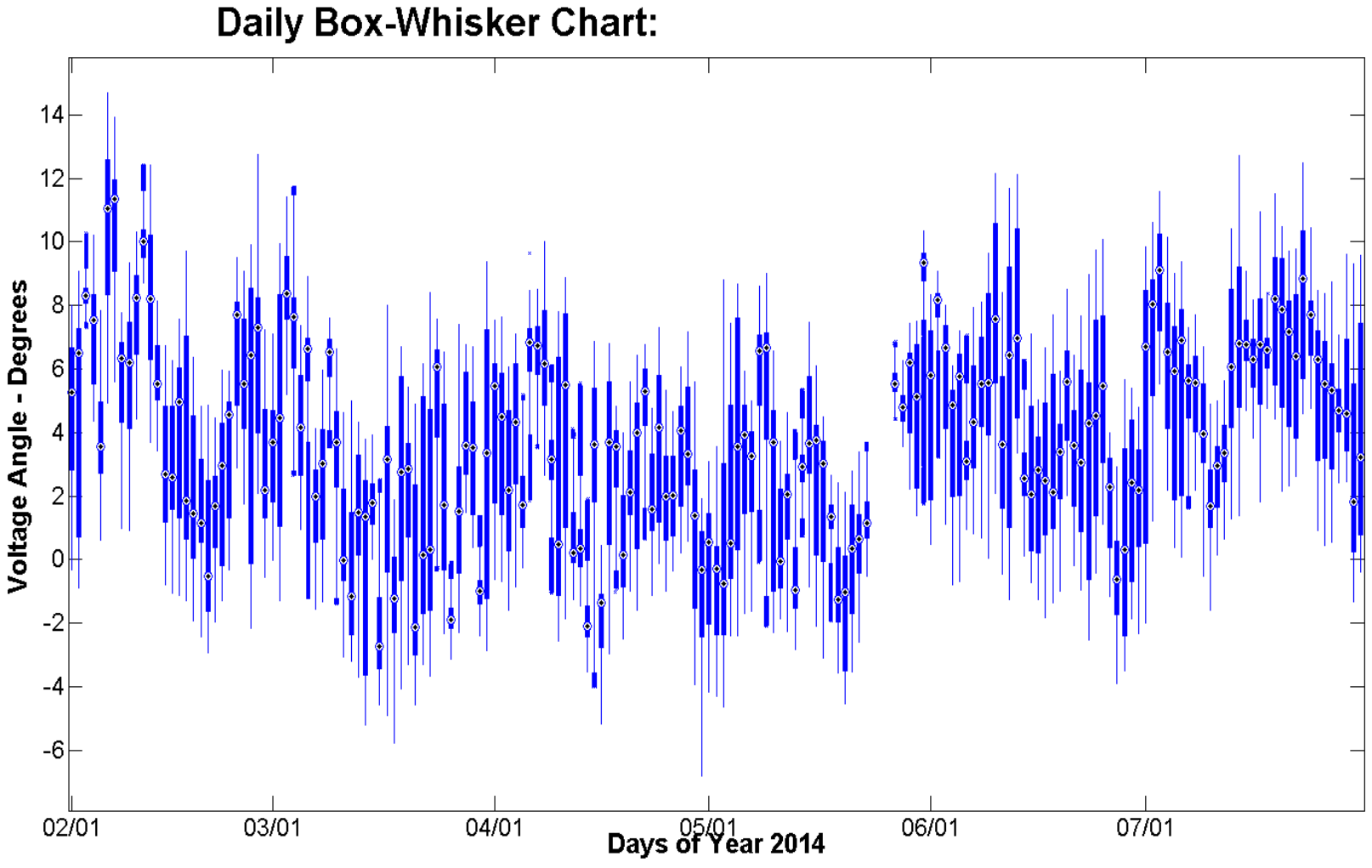
North 5


Daily Box-Whisker Chart:
Voltage Angle - Degrees
10
5
0
-5
-10
-15
-20
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

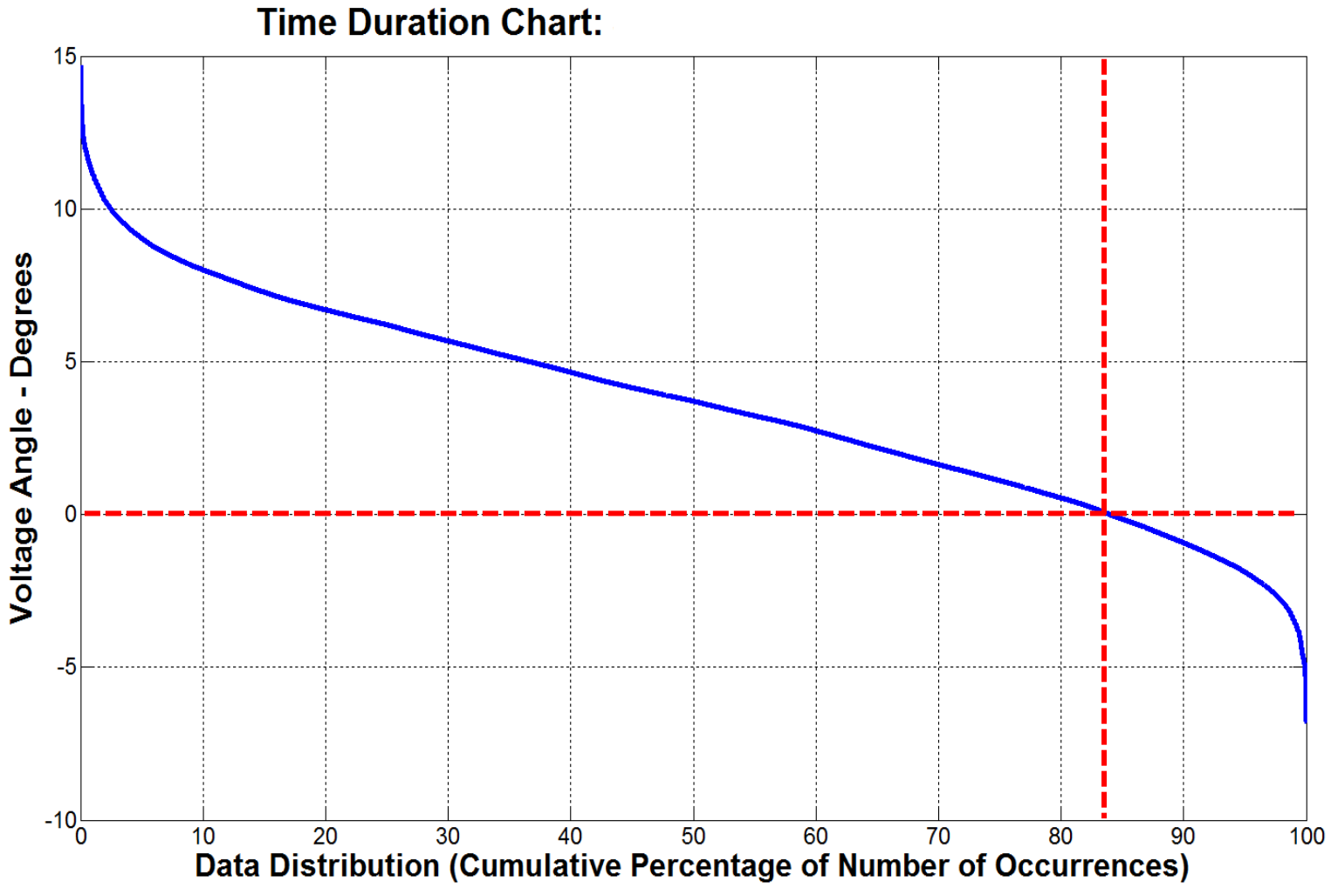
North 5


Time Duration Chart:
Voltage Angle - Degrees
15
10
5
0
-5
-10
-15
-20
-25
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

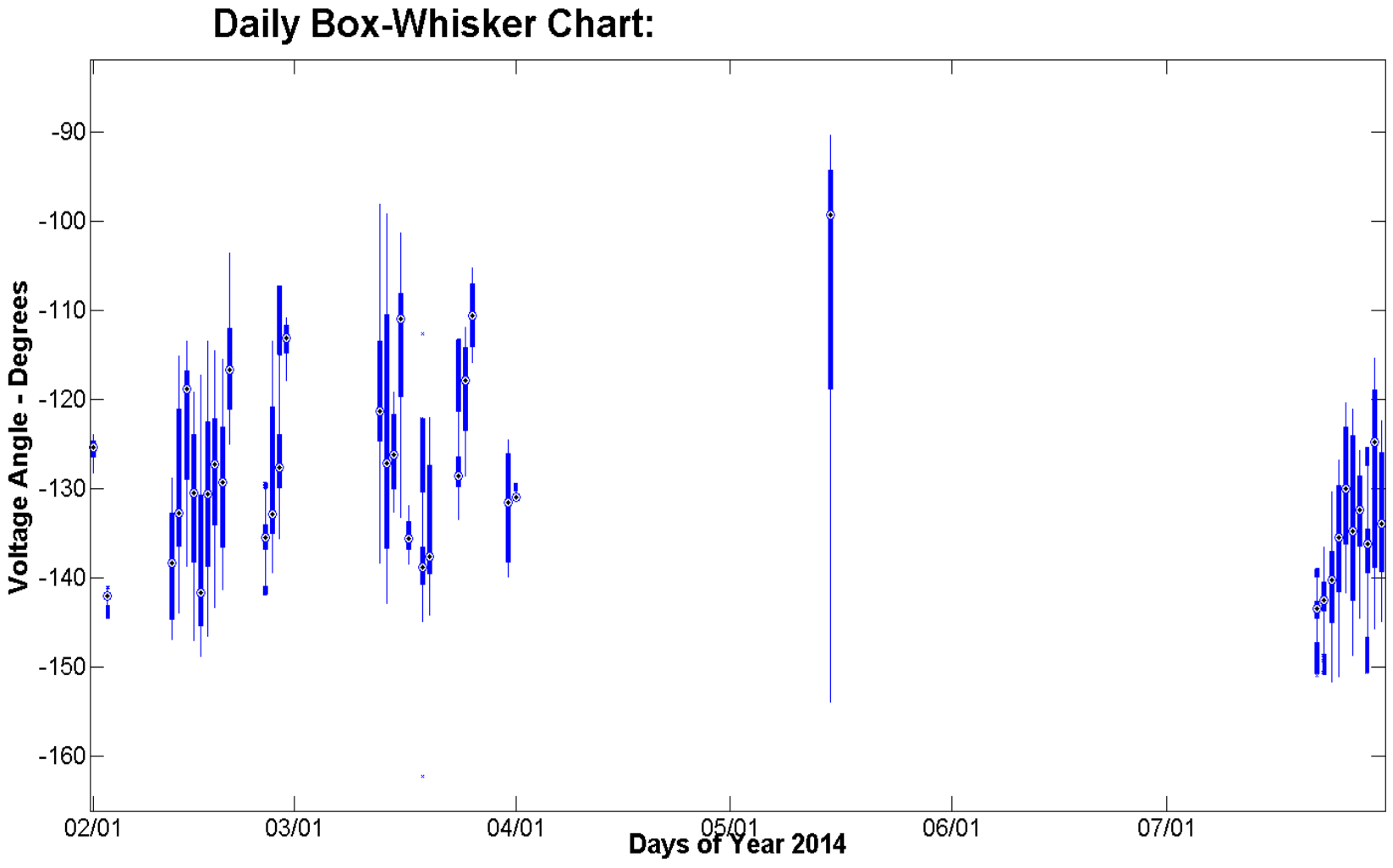
North 6


Daily Box-Whisker Chart:
Voltage Angle - Degrees
14
12
10
8
6
4
2
0
-2
-4
-6
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

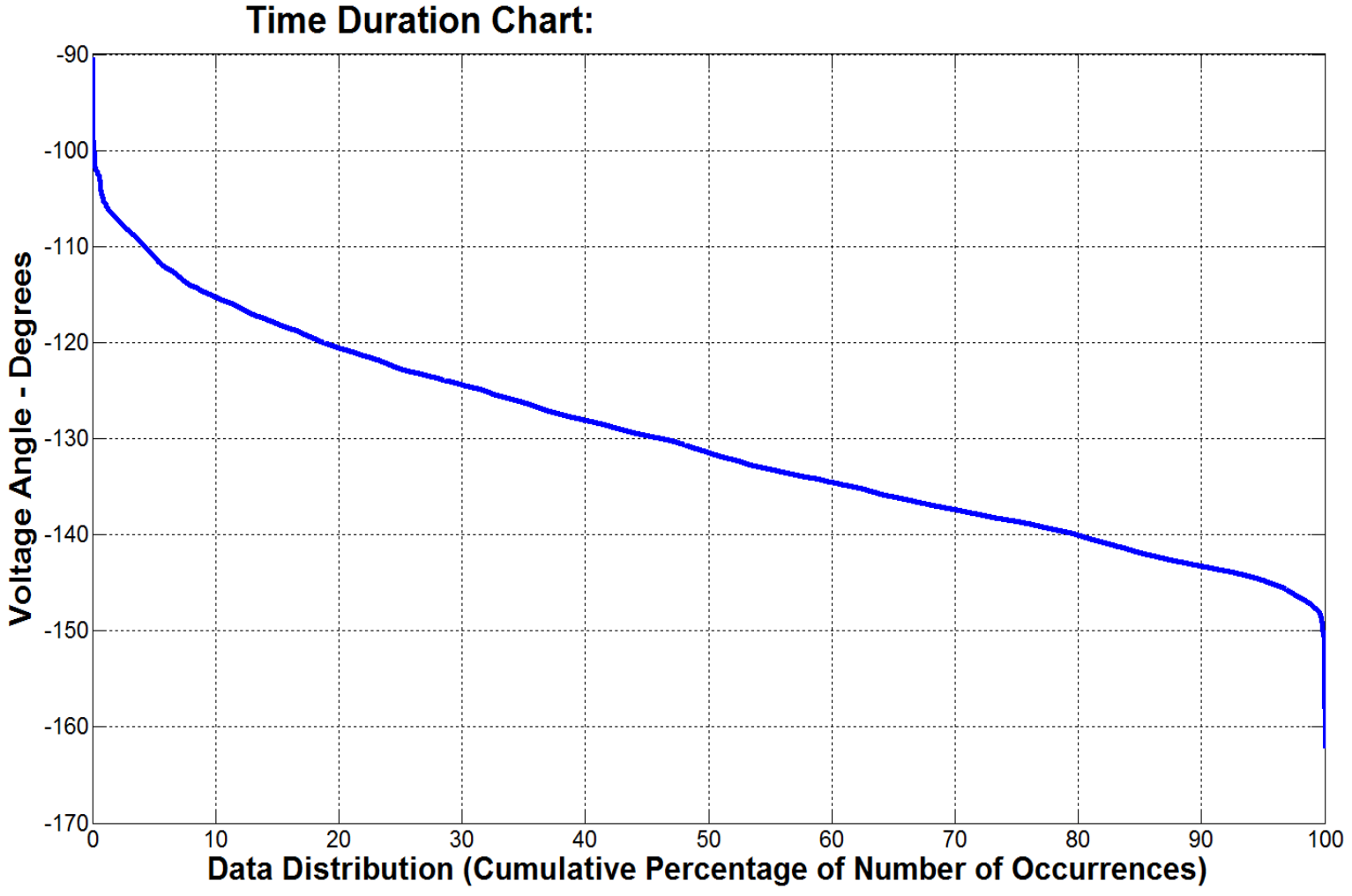
North 6


Time Duration Chart:
Voltage Angle - Degrees
15
10
5
0
-5
-10
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

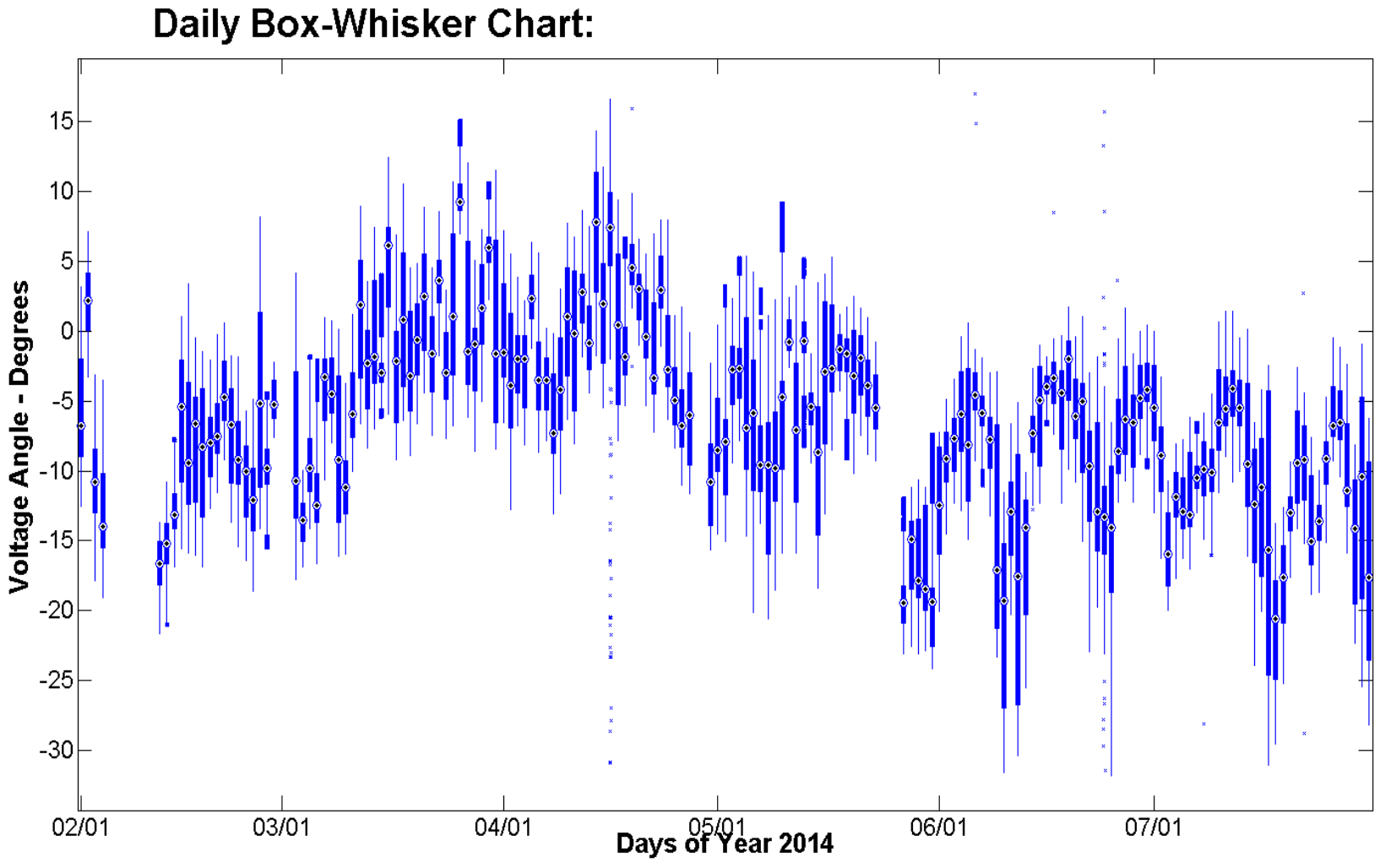
FarWest 2


Daily Box-Whisker Chart:
Voltage Angle - Degrees
-90
-100
-110
-120
-130
-140
-150
-160
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

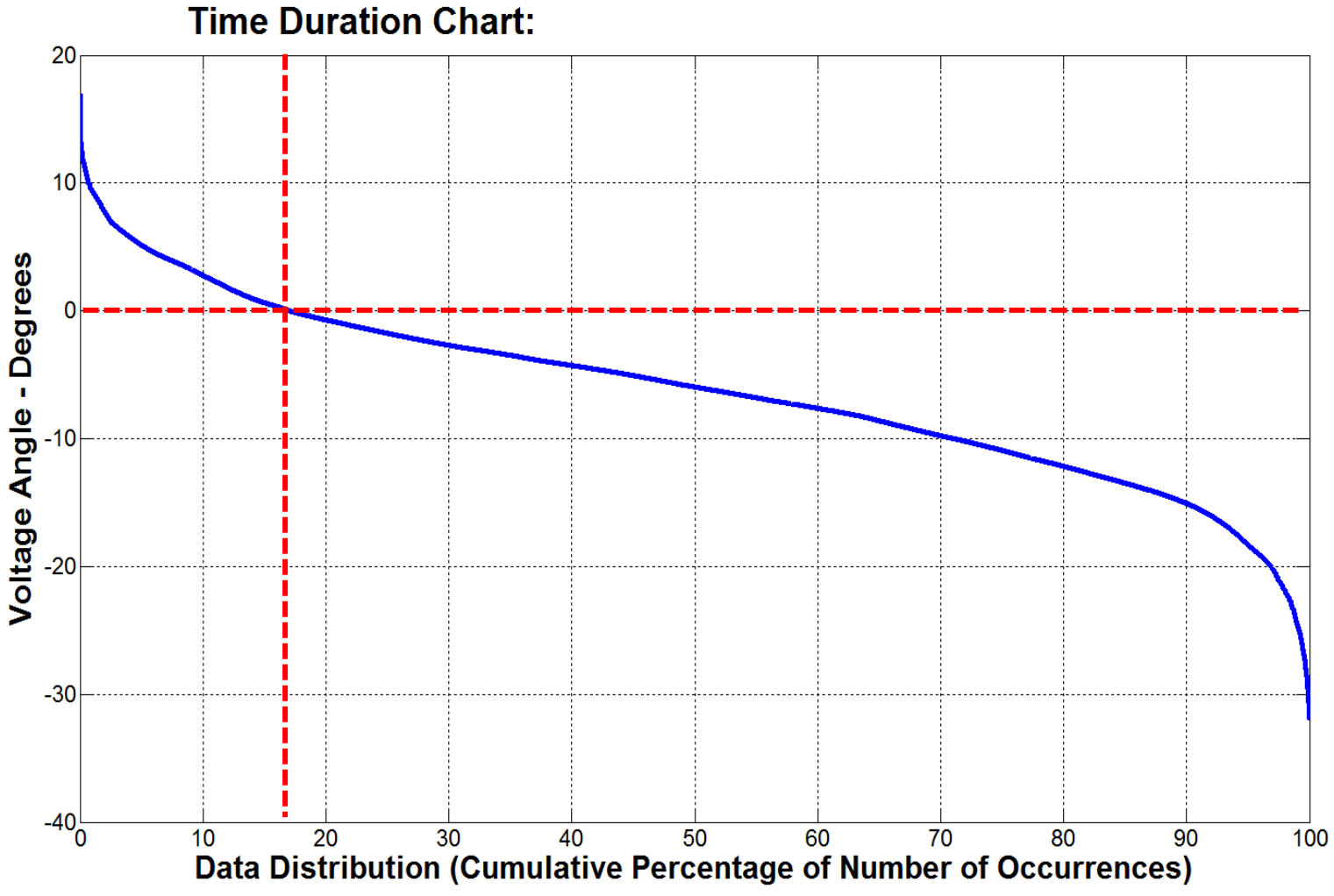
FarWest 2


Time Duration Chart:
Voltage Angle - Degrees
-90
-100
-110
-120
-130
-140
-150
-160
-170
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

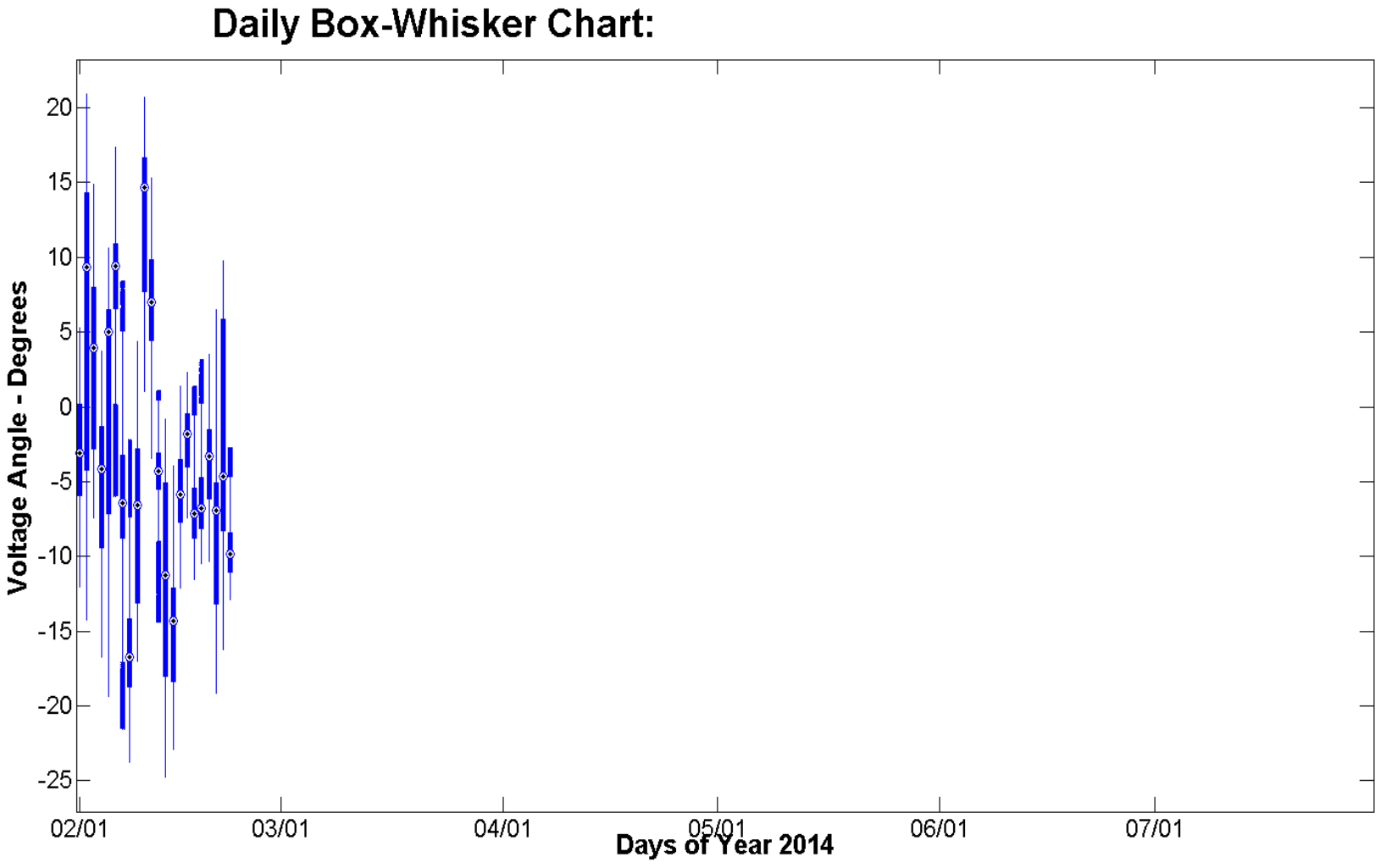
West 4


Daily Box-Whisker Chart:
Voltage Angle - Degrees
15
10
5
0
-5
-10
-15
-20
-25
-30
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

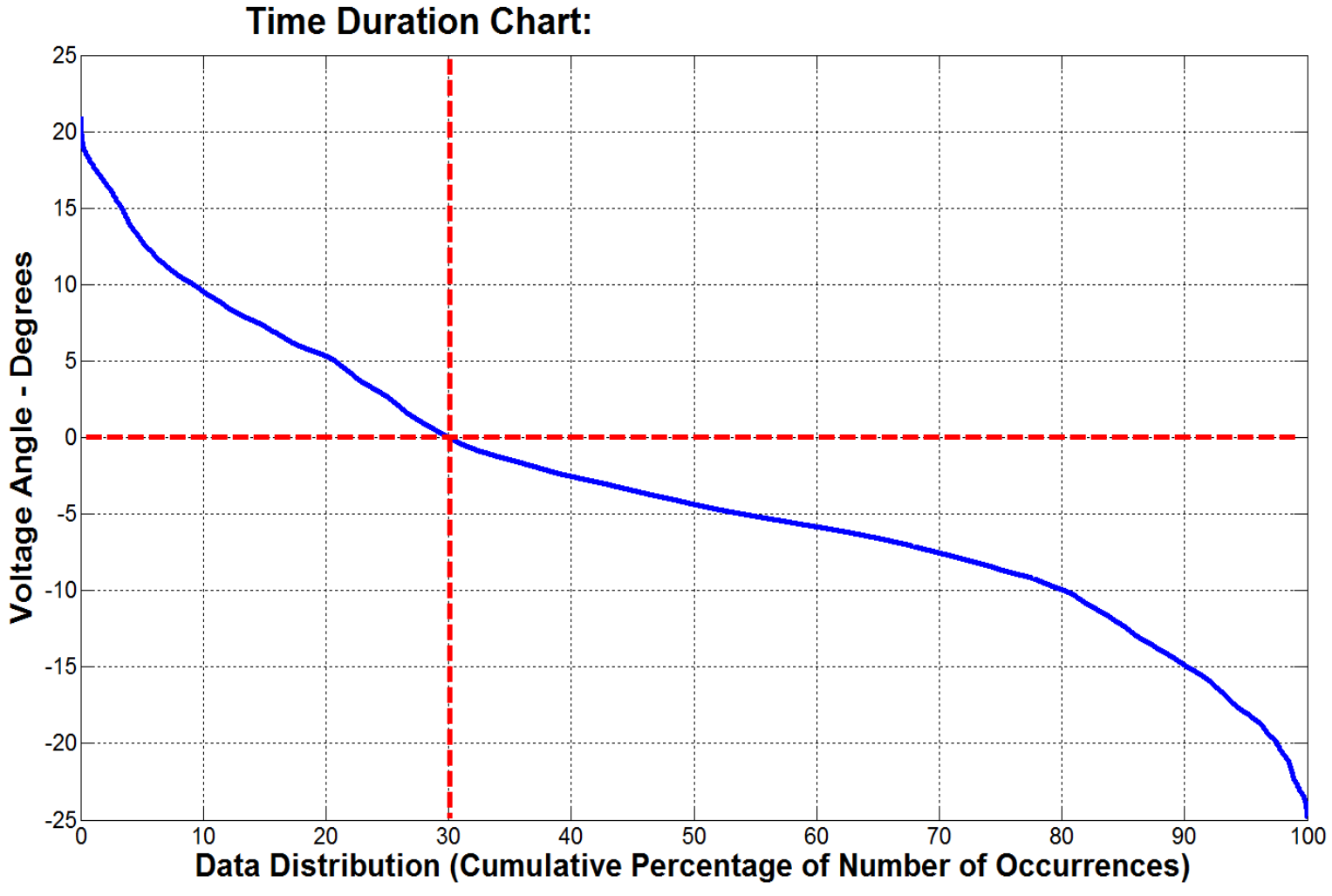
West 4


Time Duration Chart:
Voltage Angle - Degrees
20
10
0
-10
-20
-30
-40
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

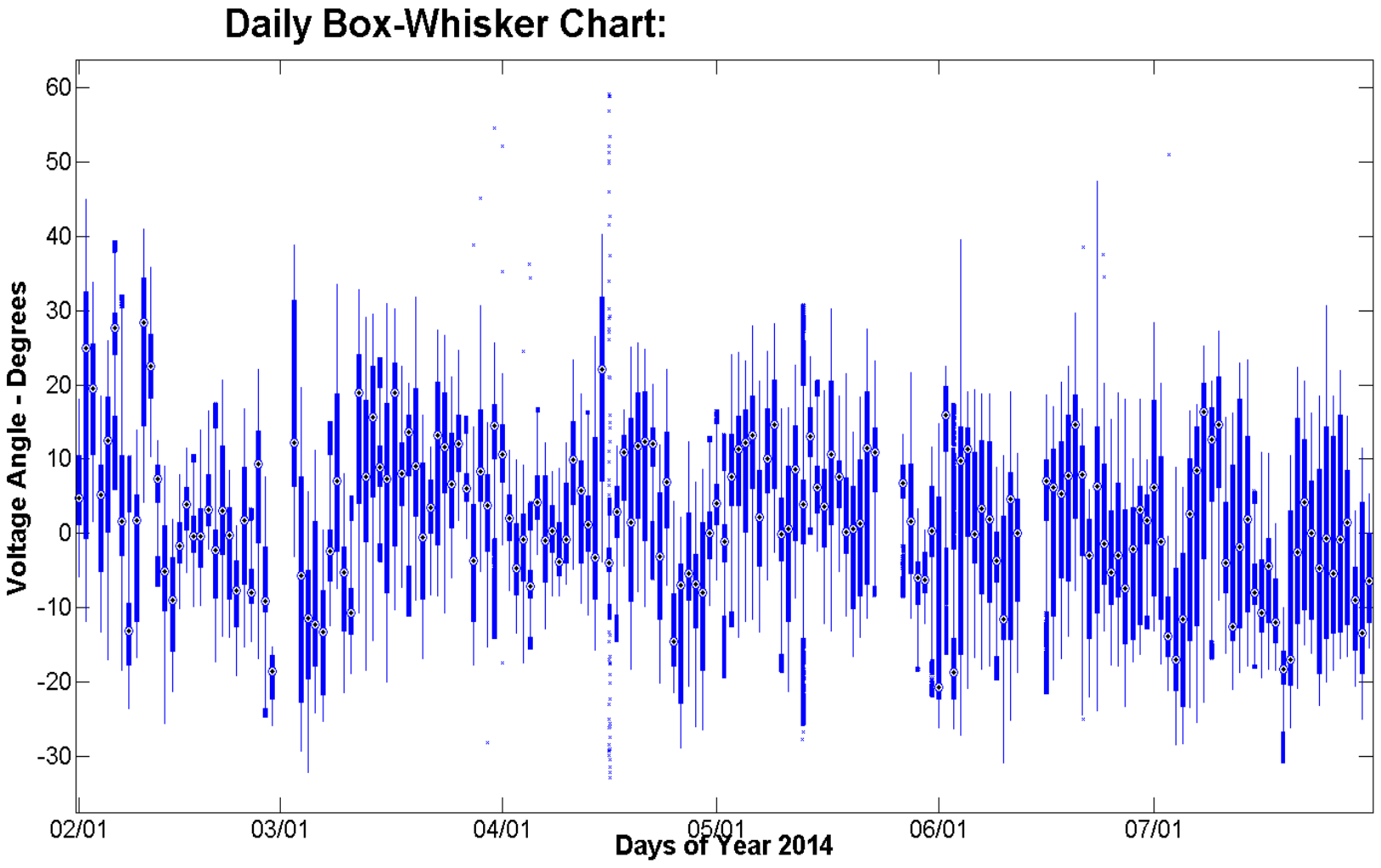
Coast 2


Daily Box-Whisker Chart:
Voltage Angle - Degrees
20
15
10
5
0
-5
-10
-15
-20
-25
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

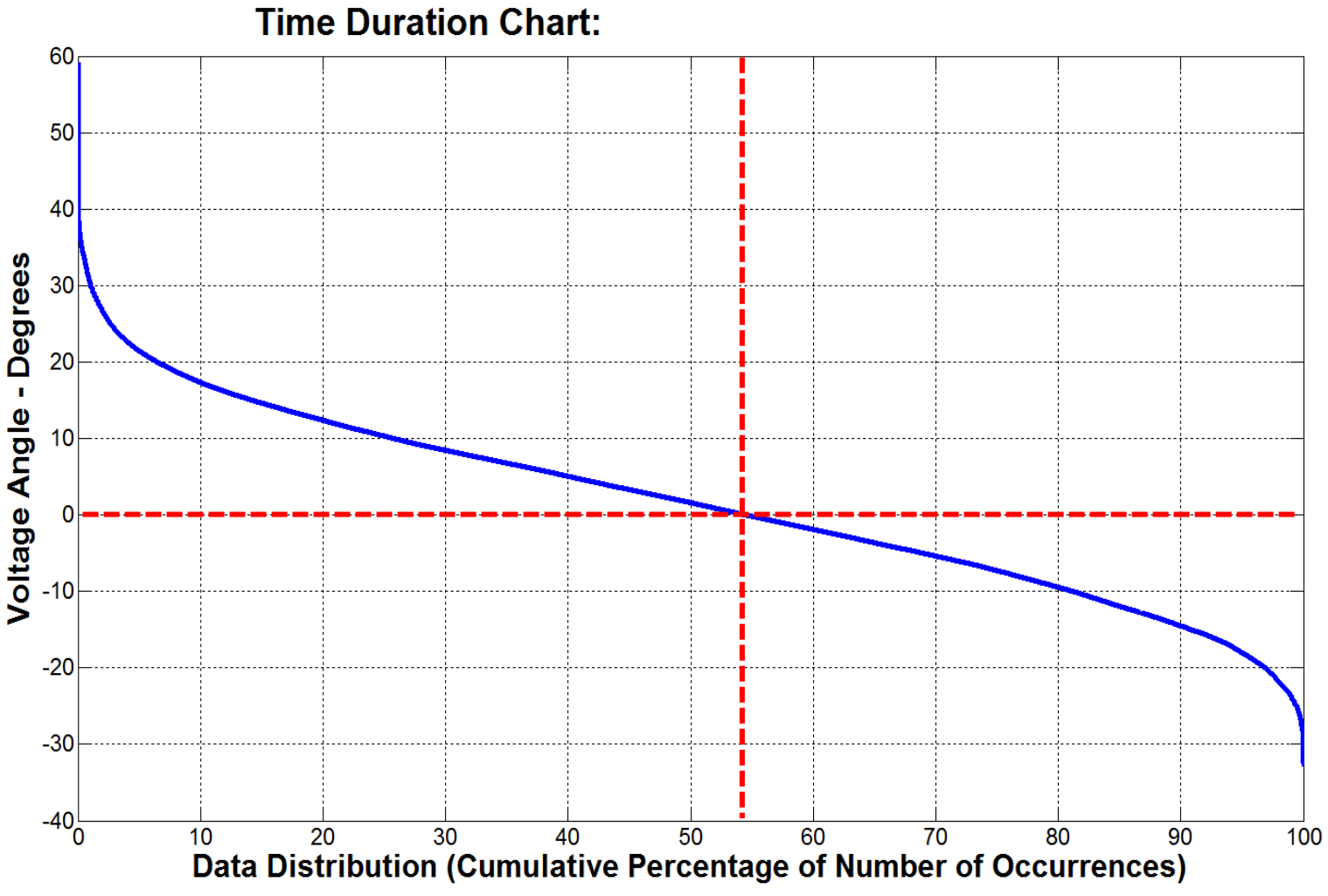
Coast 2


Time Duration Chart:
Voltage Angle - Degrees
25
20
15
10
5
0
-5
-10
-15
-20
-25
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

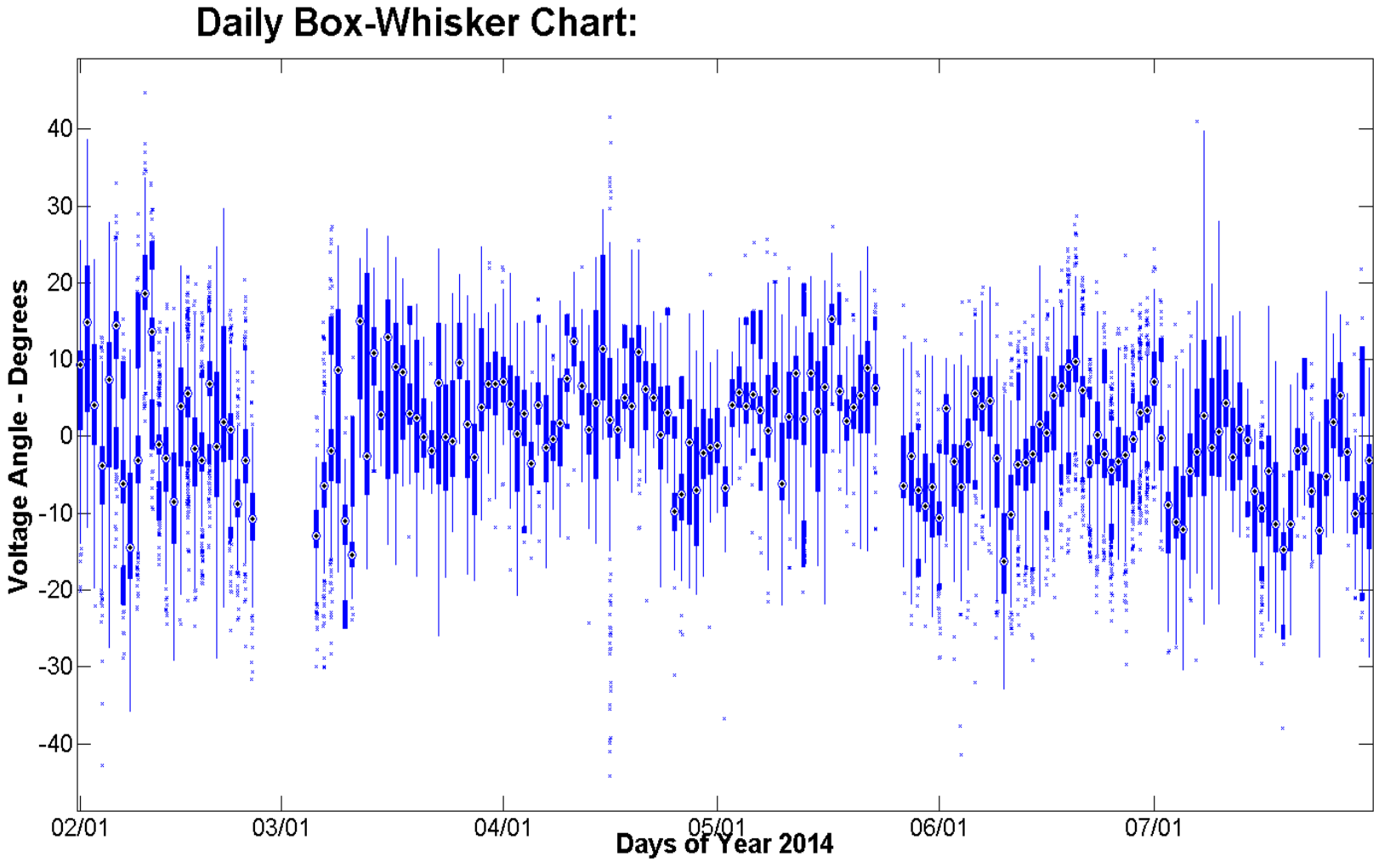
Coast 1


Daily Box-Whisker Chart:
Voltage Angle - Degrees
60
50
40
30
20
10
0
-10
-20
-30
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

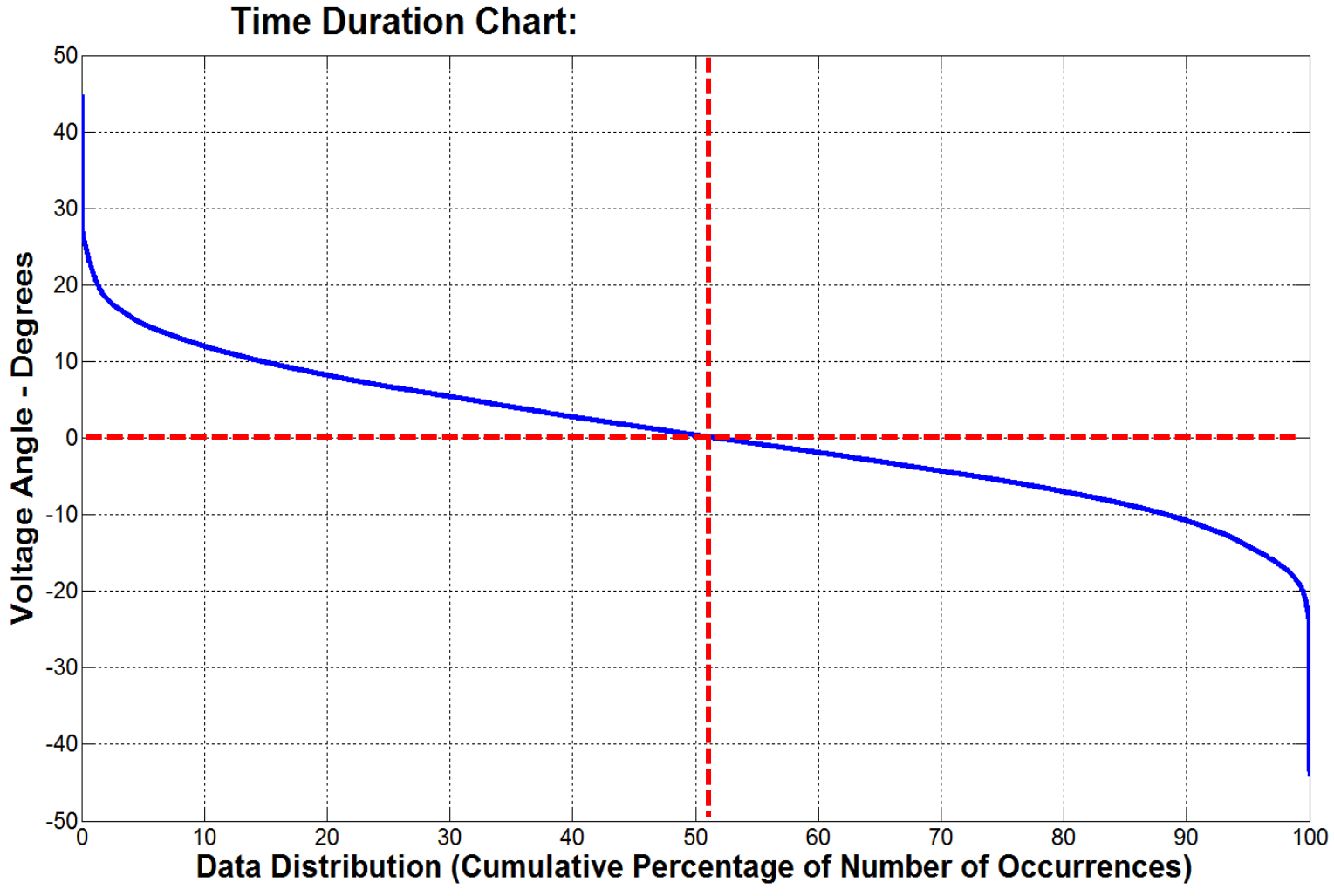
Coast 1


Time Duration Chart:
Voltage Angle - Degrees
60
50
40
30
20
10
0
-10
-20
-30
-40
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

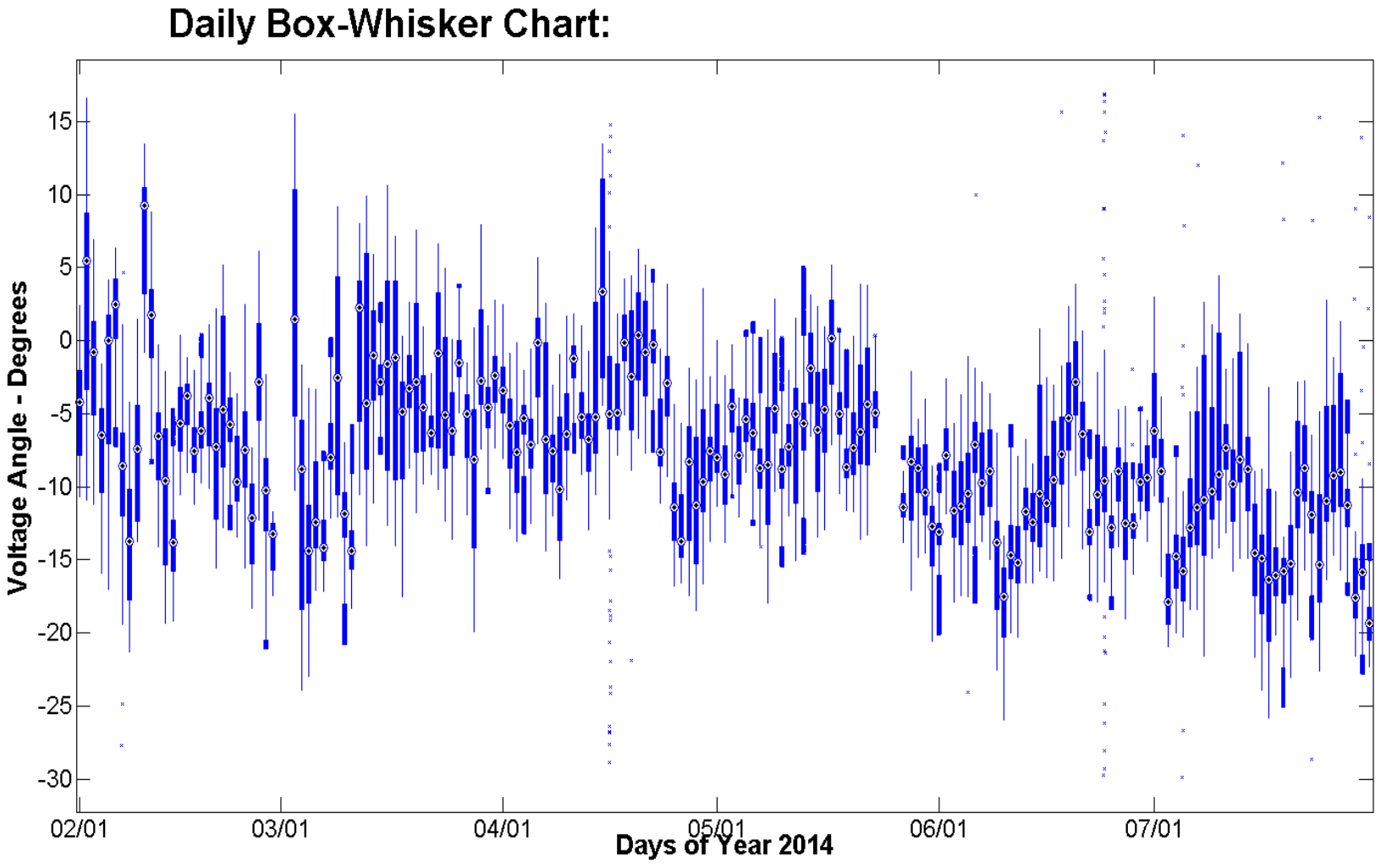
South 3


Daily Box-Whisker Chart:
Voltage Angle - Degrees
40
30
20
10
0
-10
-20
-30
-40
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

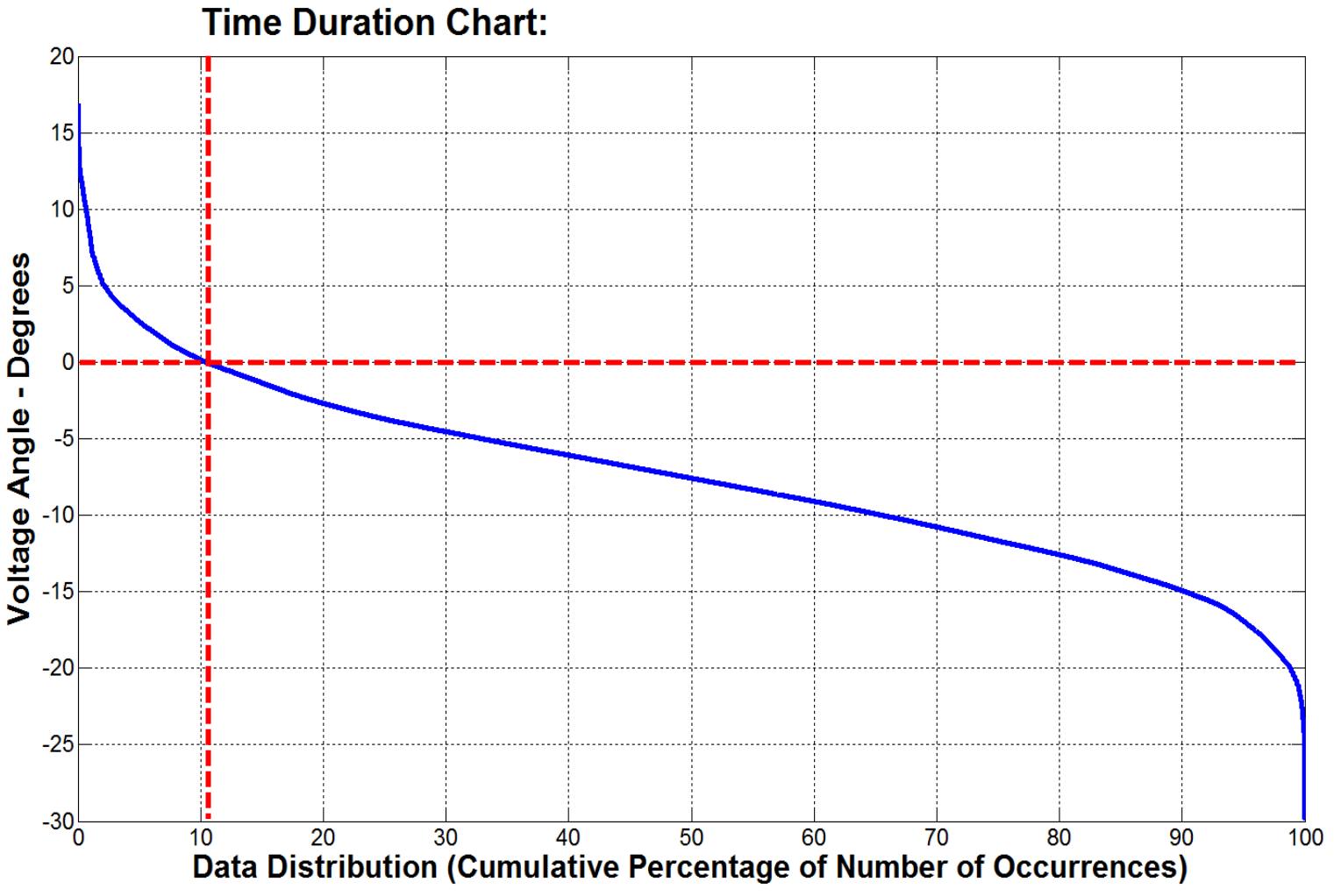
South 3


Time Duration Chart:
Voltage Angle - Degrees
Data Distribution (Cumulative Percentage of Number of Occurrences)
50
40
30
20
10
0
-10
-20
-30
-40
-50
0
10
20
30
40
50
60
70
80
90
100

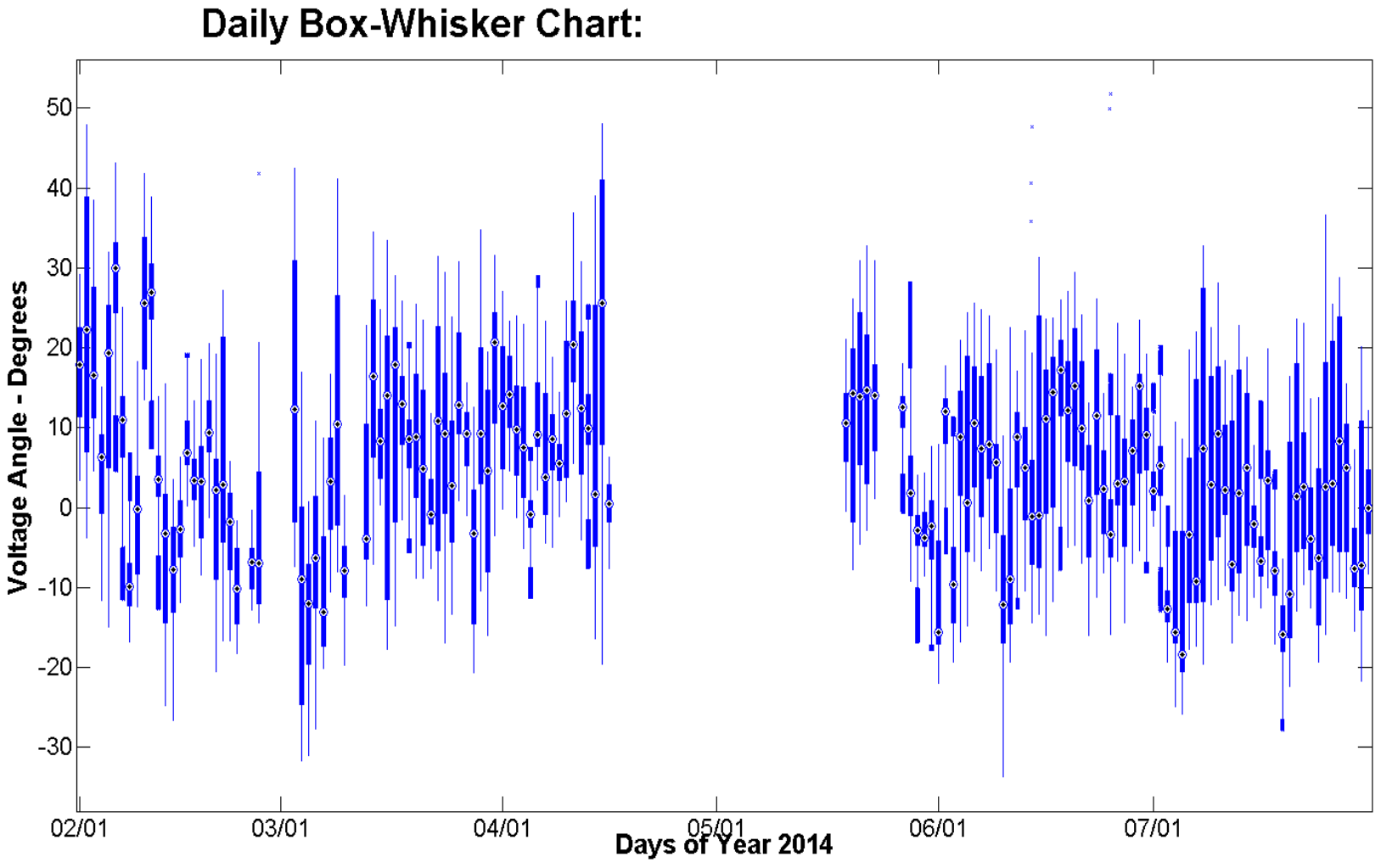
South 5


Daily Box-Whisker Chart:
Voltage Angle - Degrees
15
10
5
0
-5
-10
-15
-20
-25
-30
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

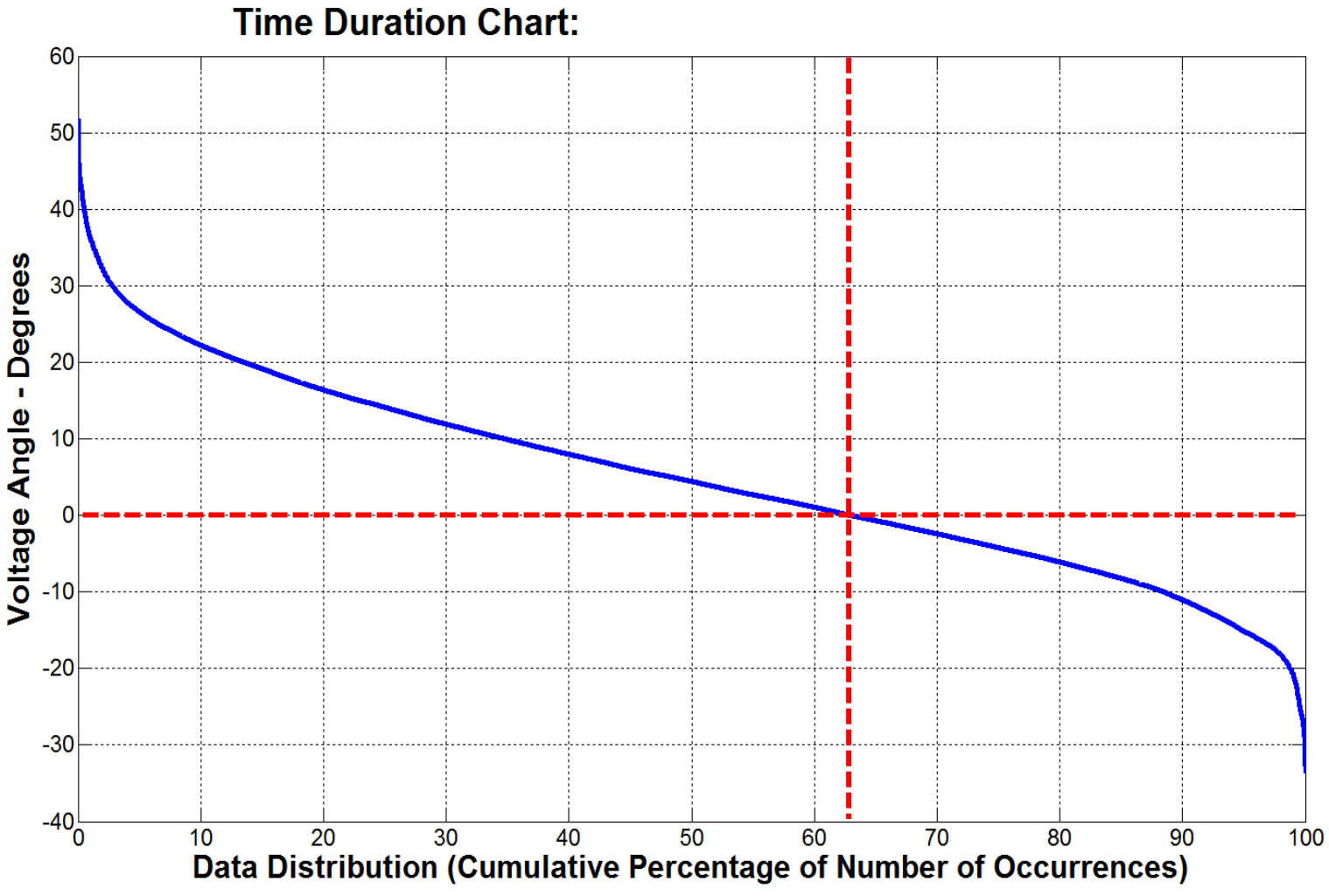
South 5


Time Duration Chart:
Voltage Angle - Degrees
Data Distribution (Cumulative Percentage of Number of Occurrences)
20
15
10
5
0
-5
-10
-15
-20
-25
-30
0
10
20
30
40
50
60
70
80
90
100

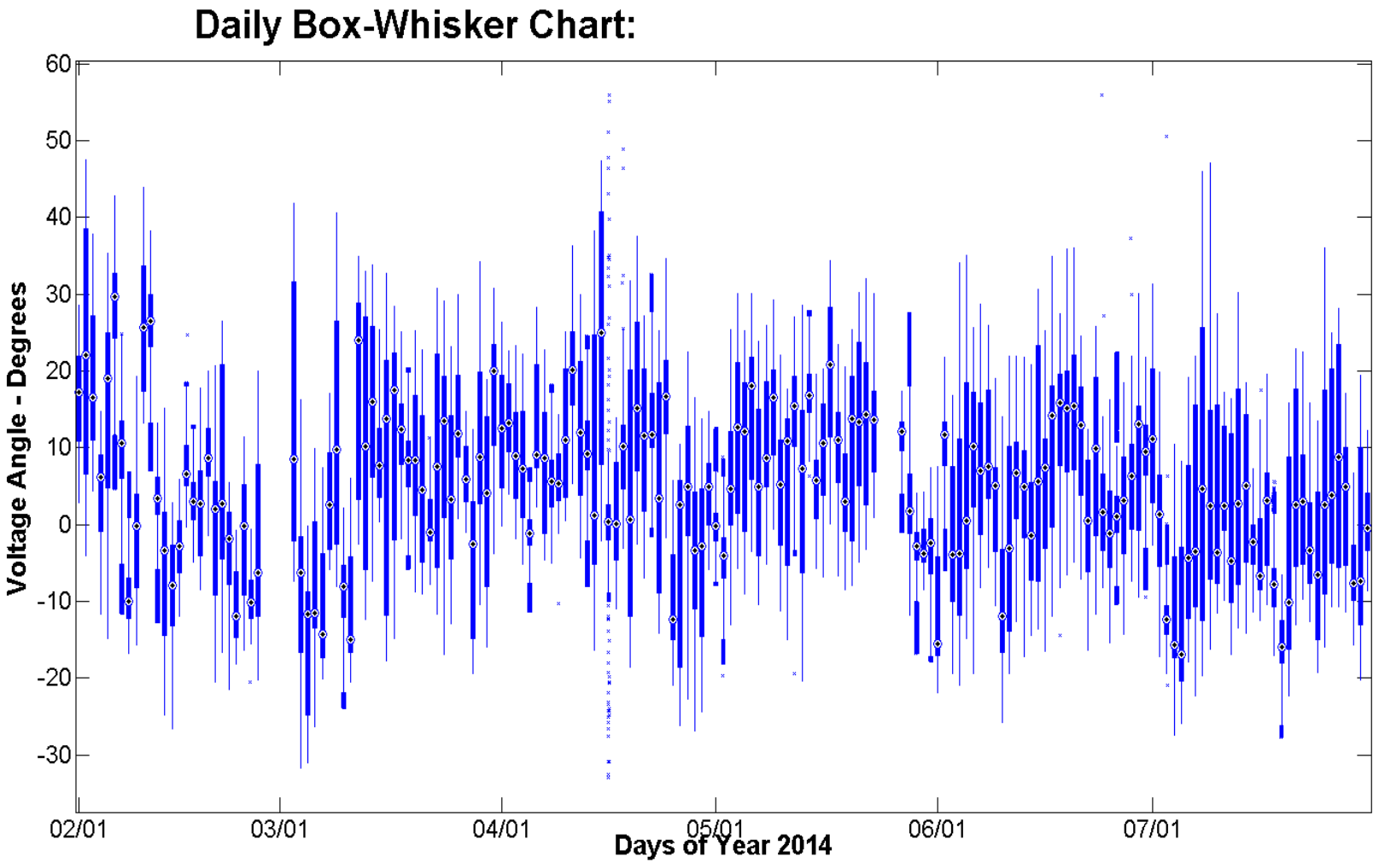
Coast 4


Daily Box-Whisker Chart:
Voltage Angle - Degrees
50
40
30
20
10
0
-10
-20
-30
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

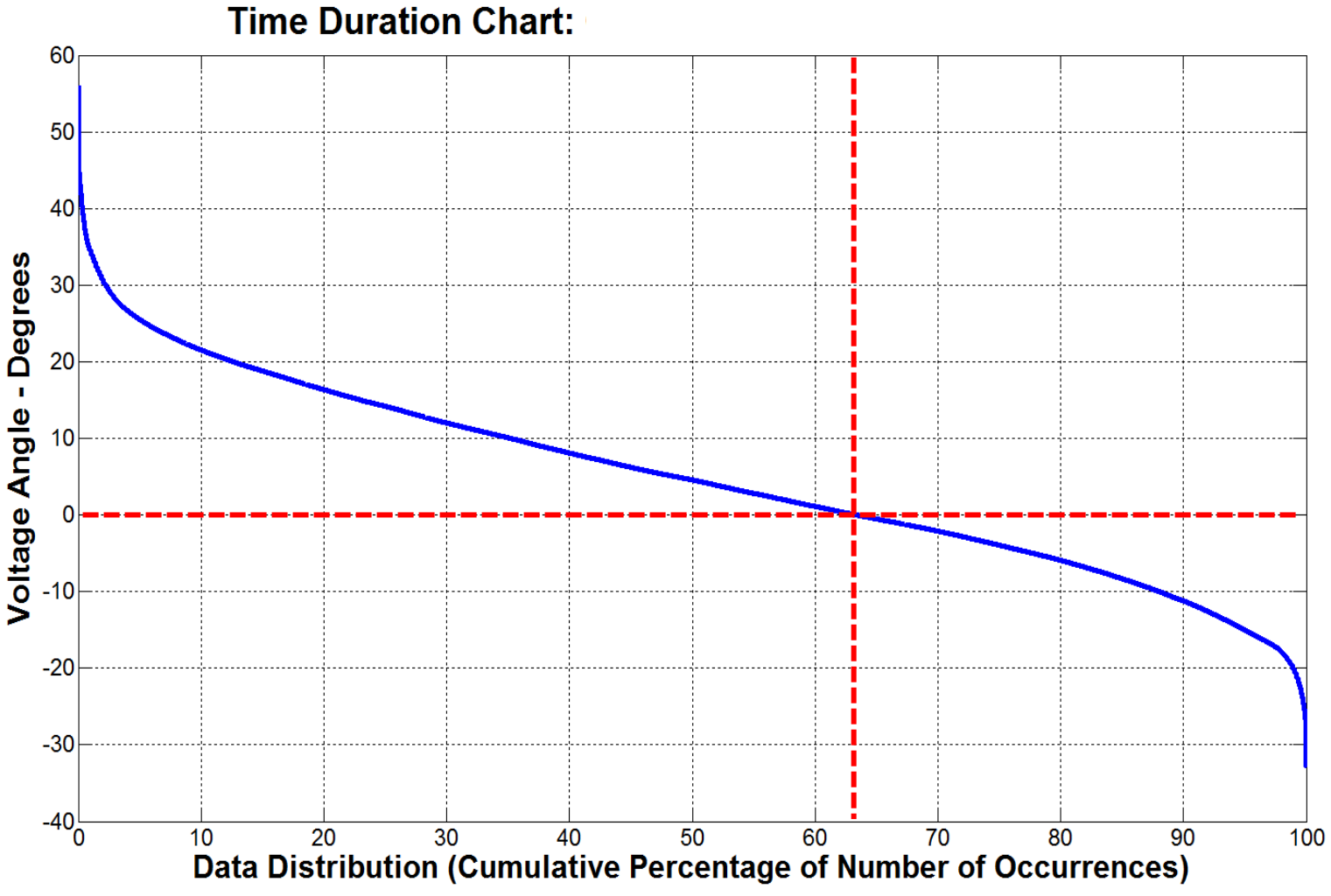
Coast 4


Time Duration Chart:
Voltage Angle - Degrees
60
50
40
30
20
10
0
-10
-20
-30
-40
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

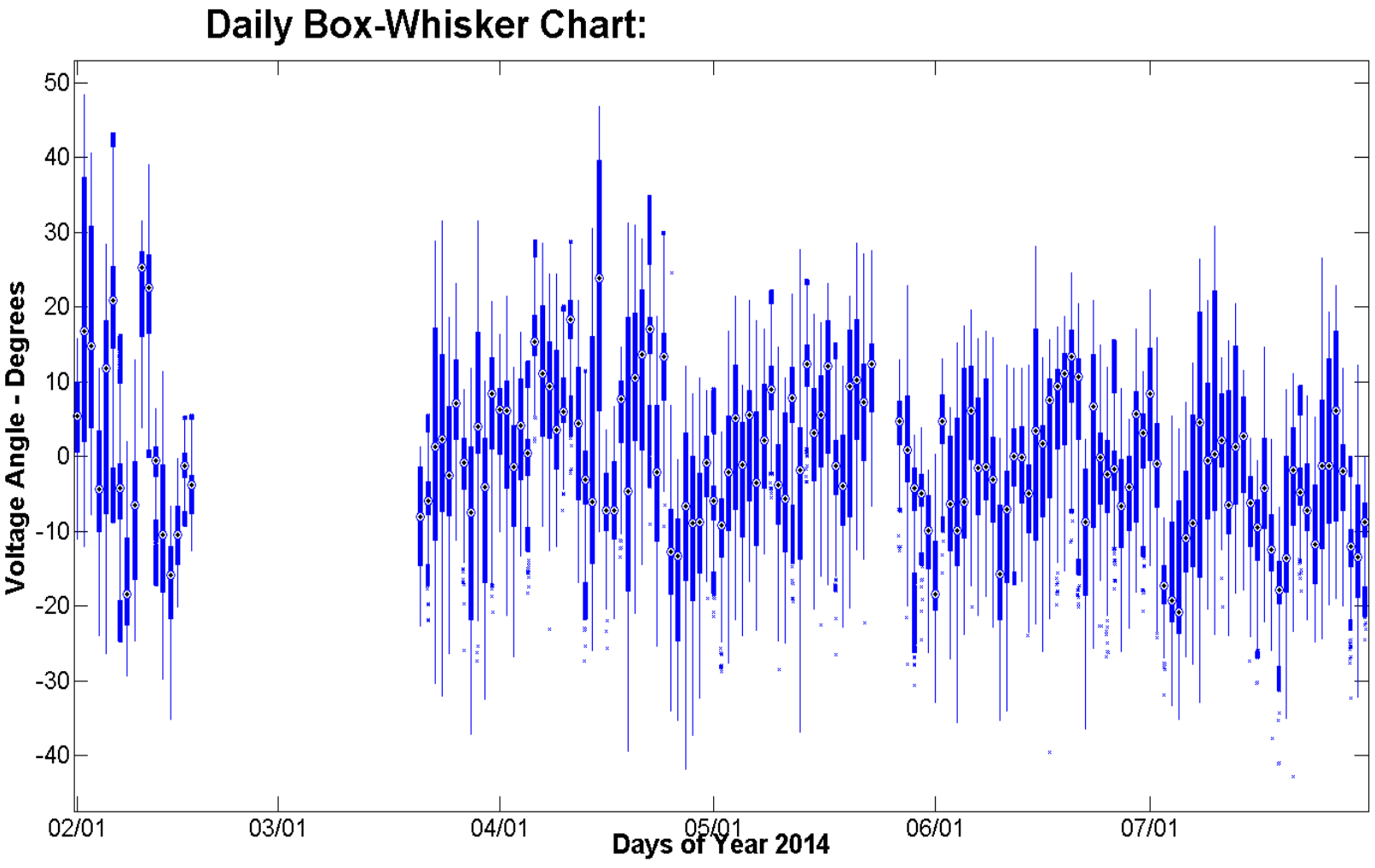
Coast 3


Daily Box-Whisker Chart:
Voltage Angle - Degrees
60
50
40
30
20
10
0
-10
-20
-30
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

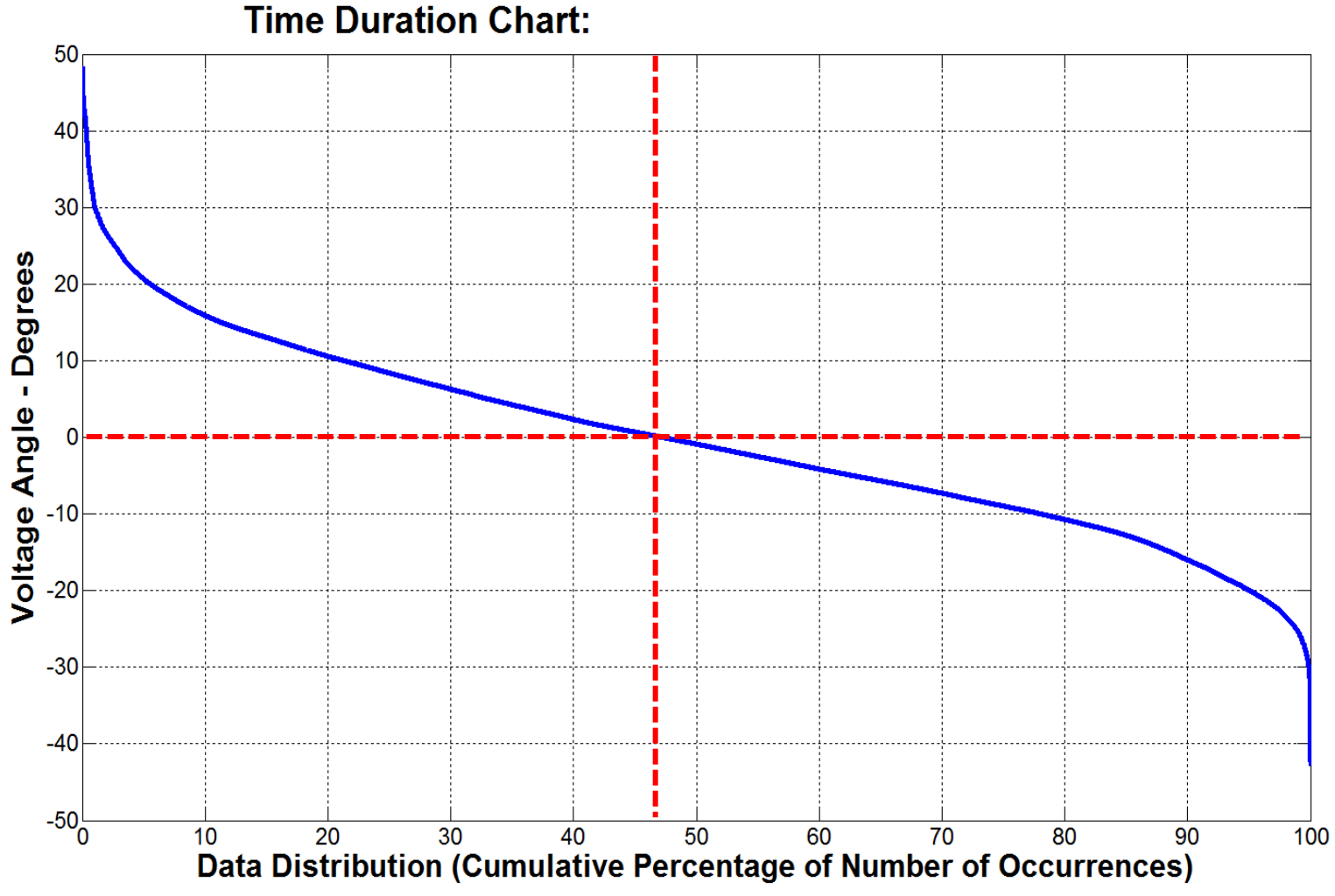
Coast 3


Time Duration Chart:
Voltage Angle - Degrees
60
50
40
30
20
10
0
-10
-20
-30
-40
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

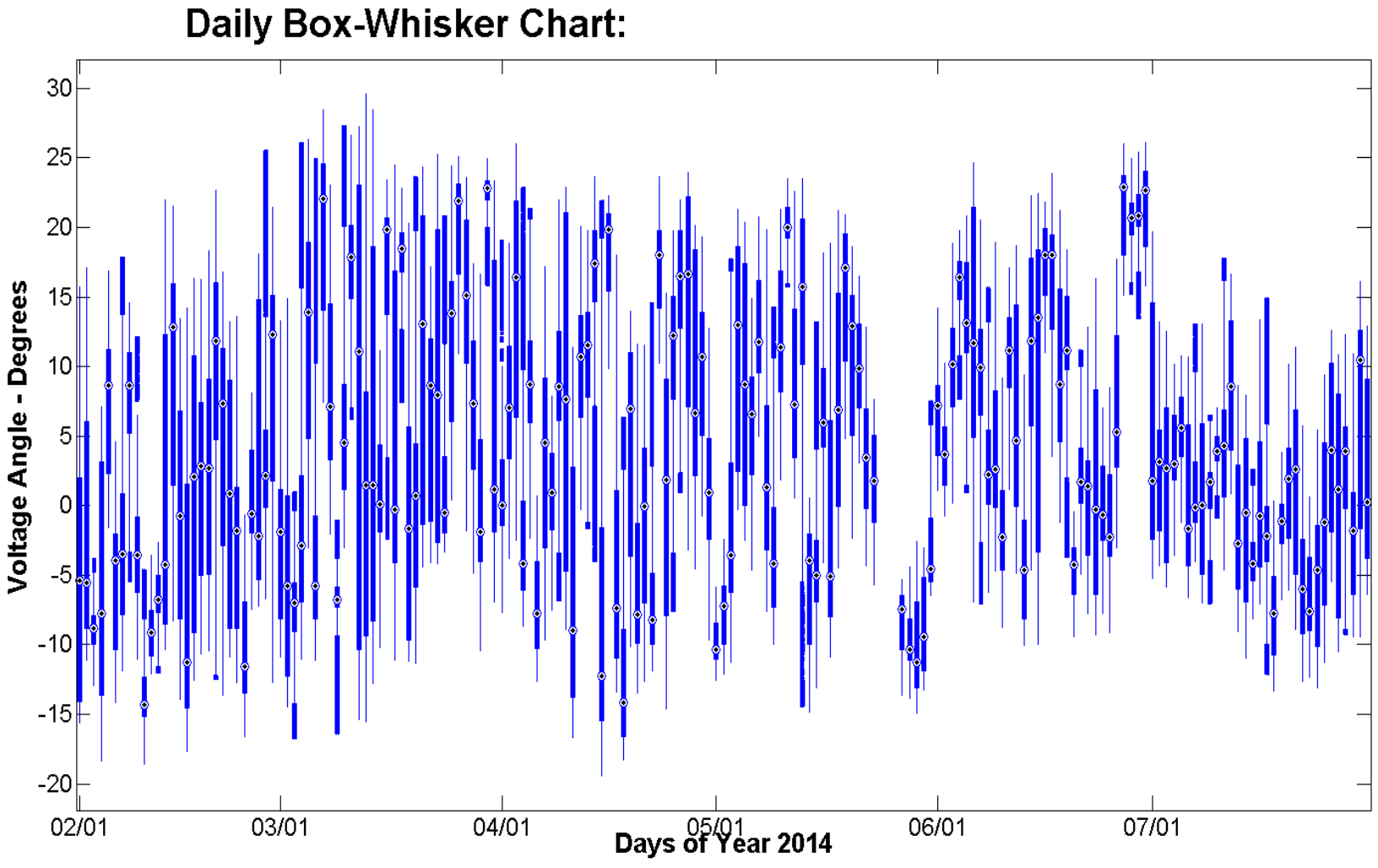
South 13


Daily Box-Whisker Chart:
Voltage Angle - Degrees
50
40
30
20
10
0
-10
-20
-30
-40
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

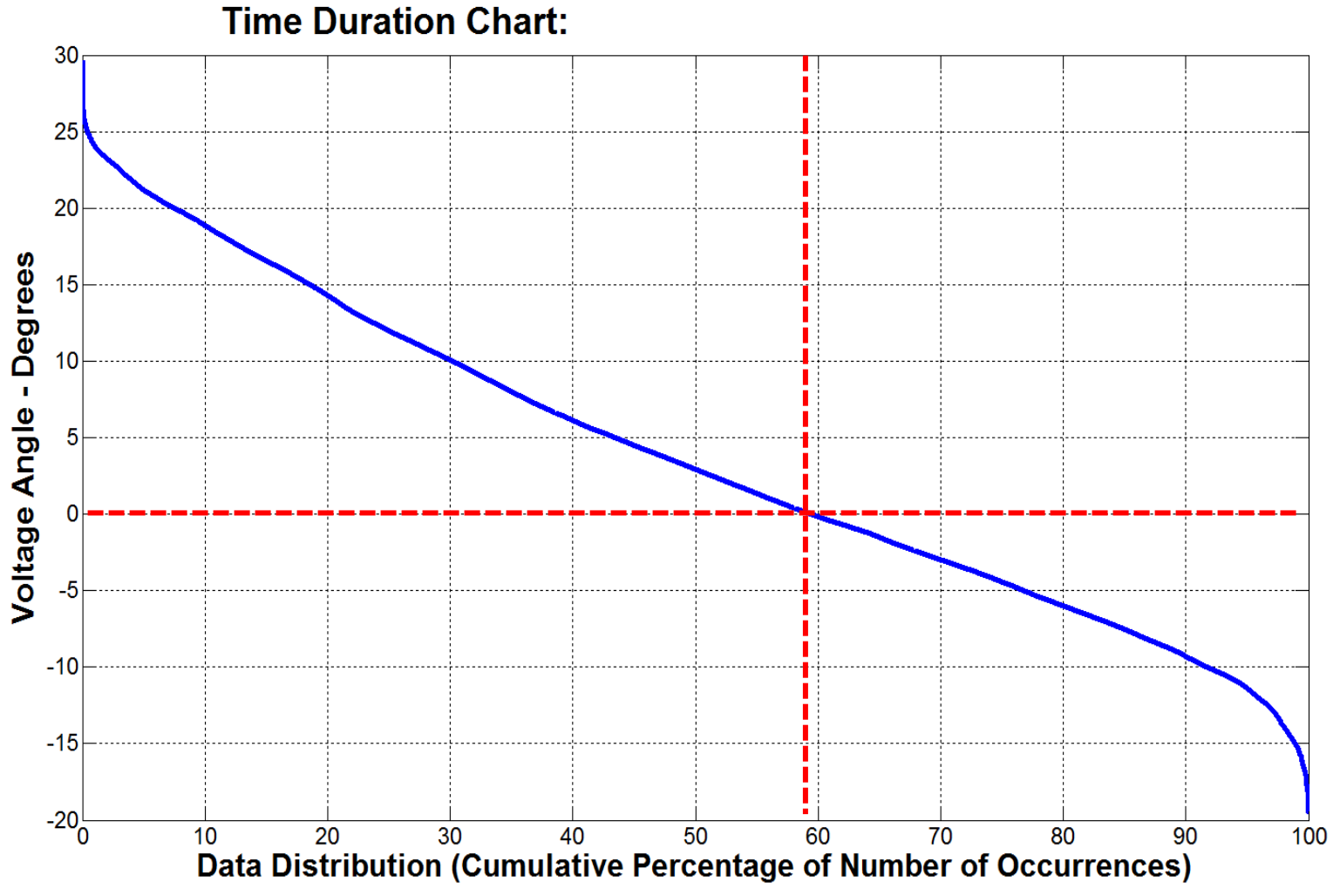
South 13


Time Duration Chart:
Voltage Angle - Degrees
50
40
30
20
10
0
-10
-20
-30
-40
-50
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

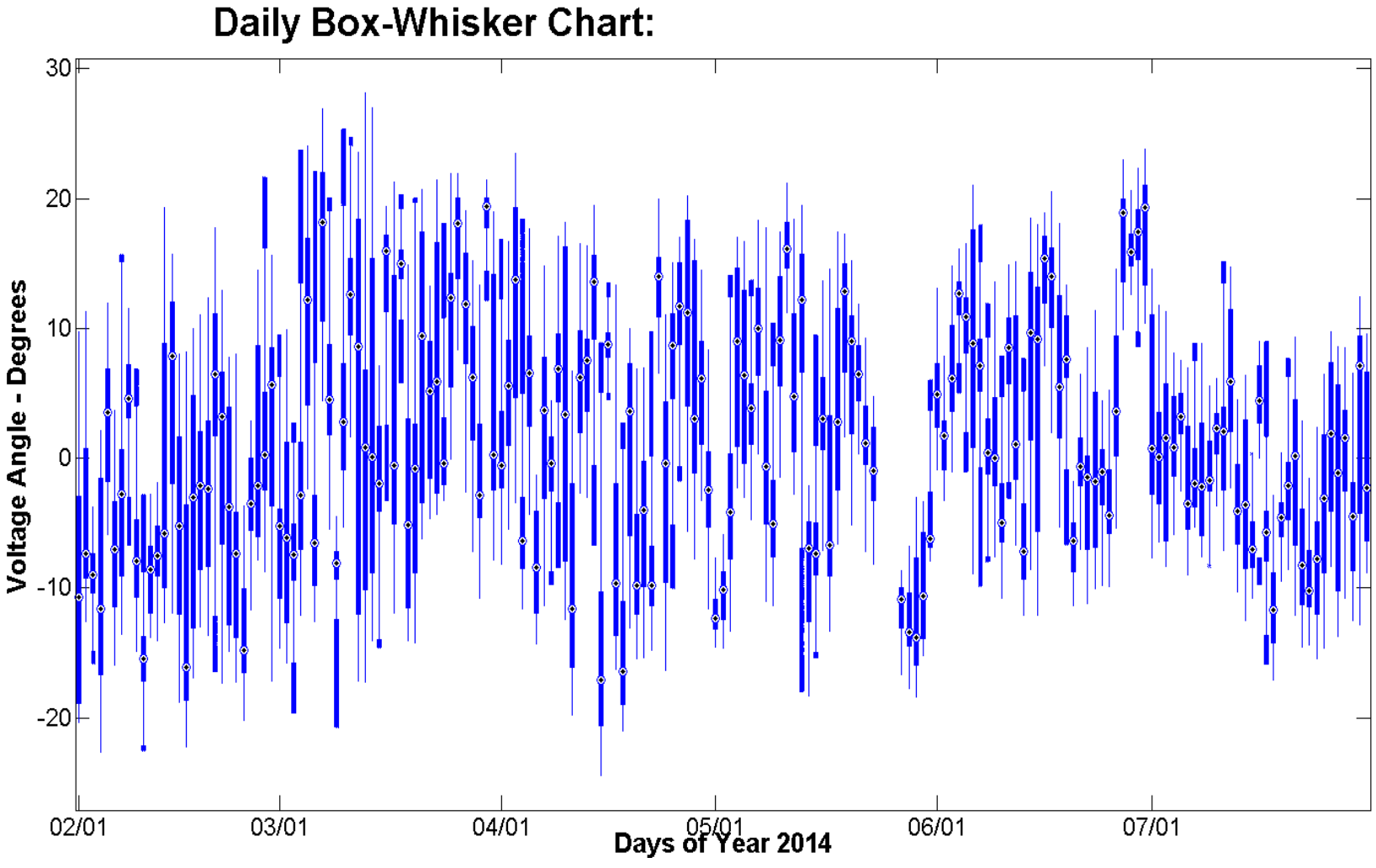
FarWest 4


Daily Box-Whisker Chart:
Voltage Angle - Degrees
30
25
20
15
10
5
0
-5
-10
-15
-20
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

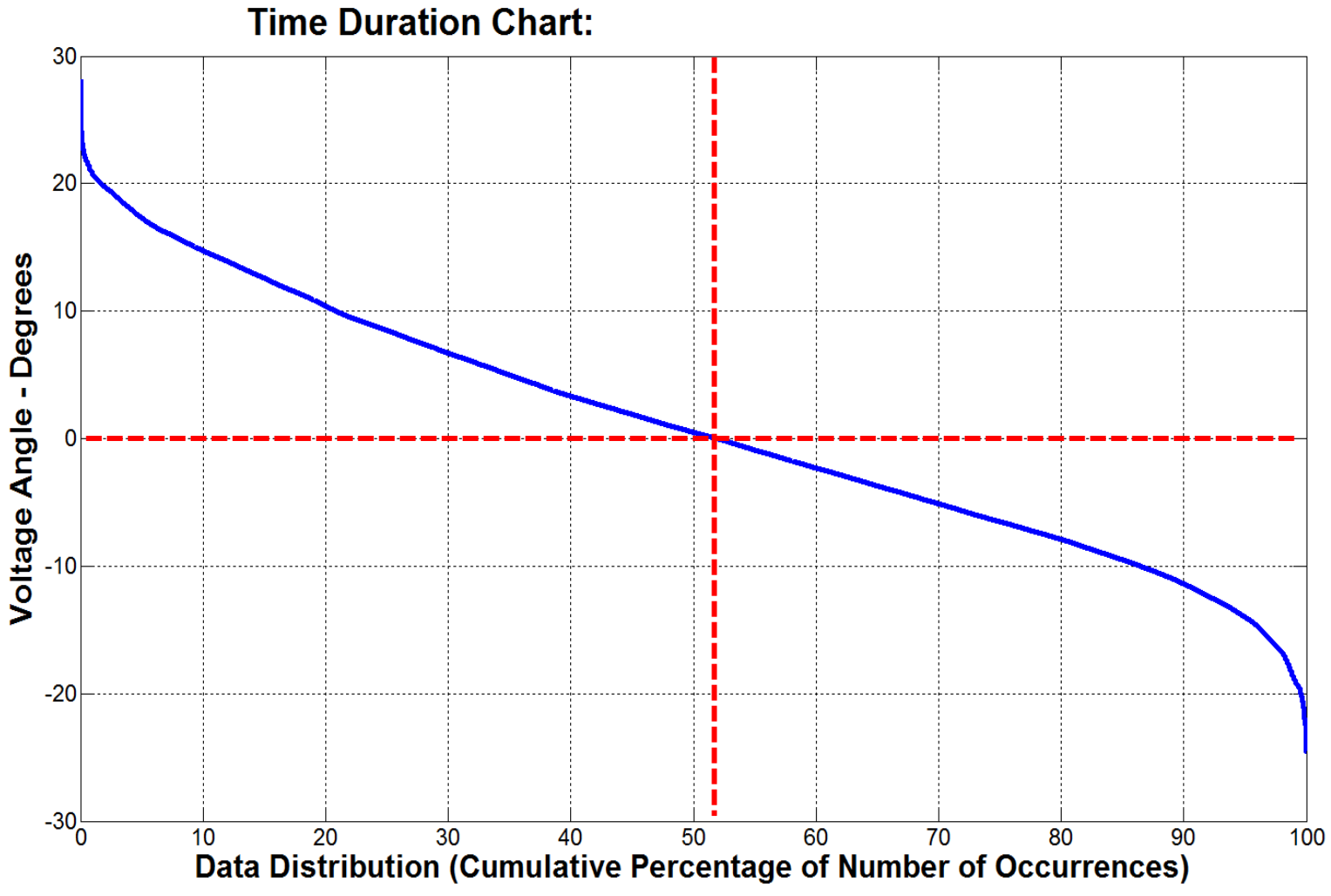
FarWest 4


Time Duration Chart:
Voltage Angle - Degrees
30
25
20
15
10
5
0
-5
-10
-15
-20
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

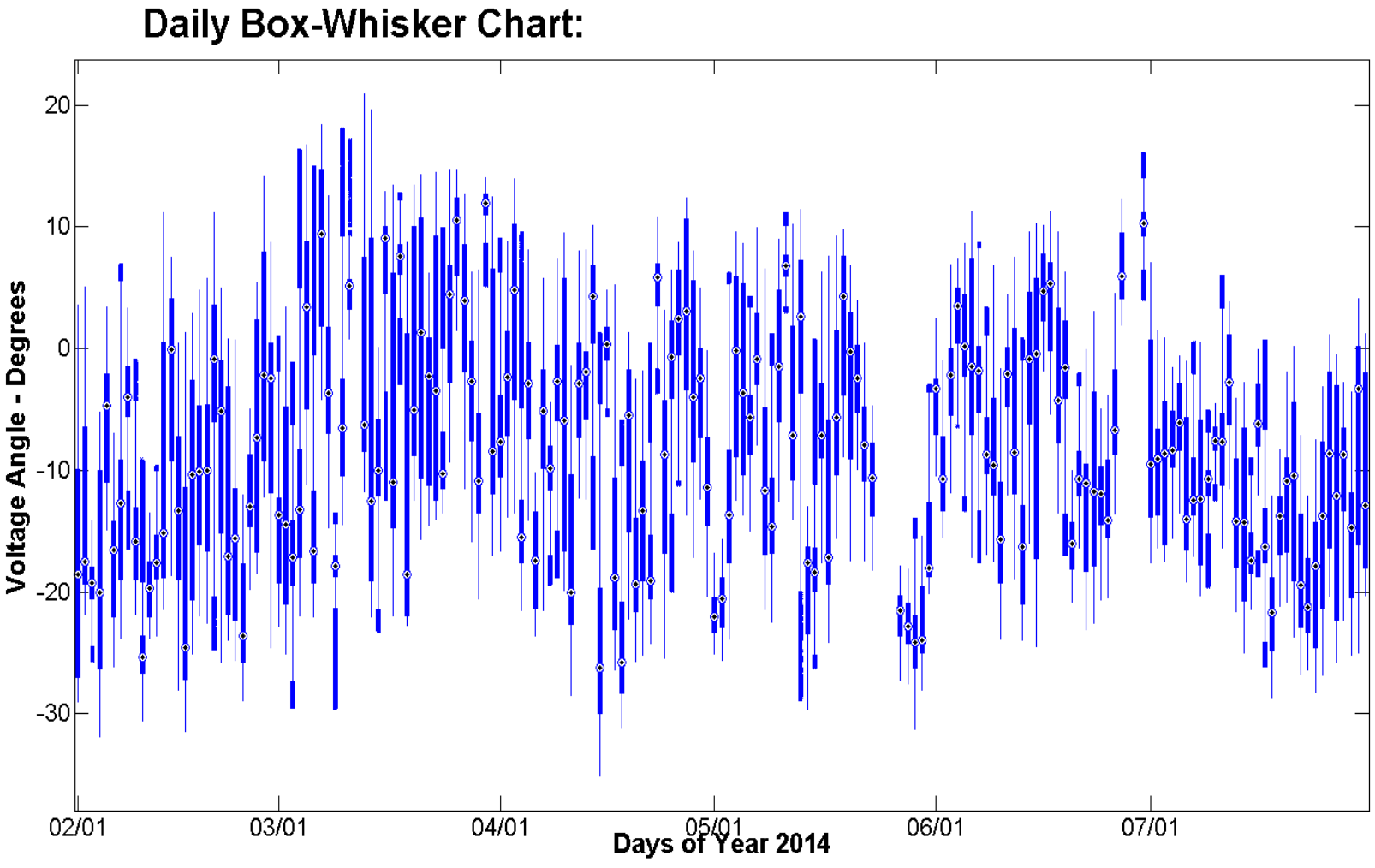
FarWest 7


Daily Box-Whisker Chart:
Voltage Angle - Degrees
30
20
10
0
-10
-20
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

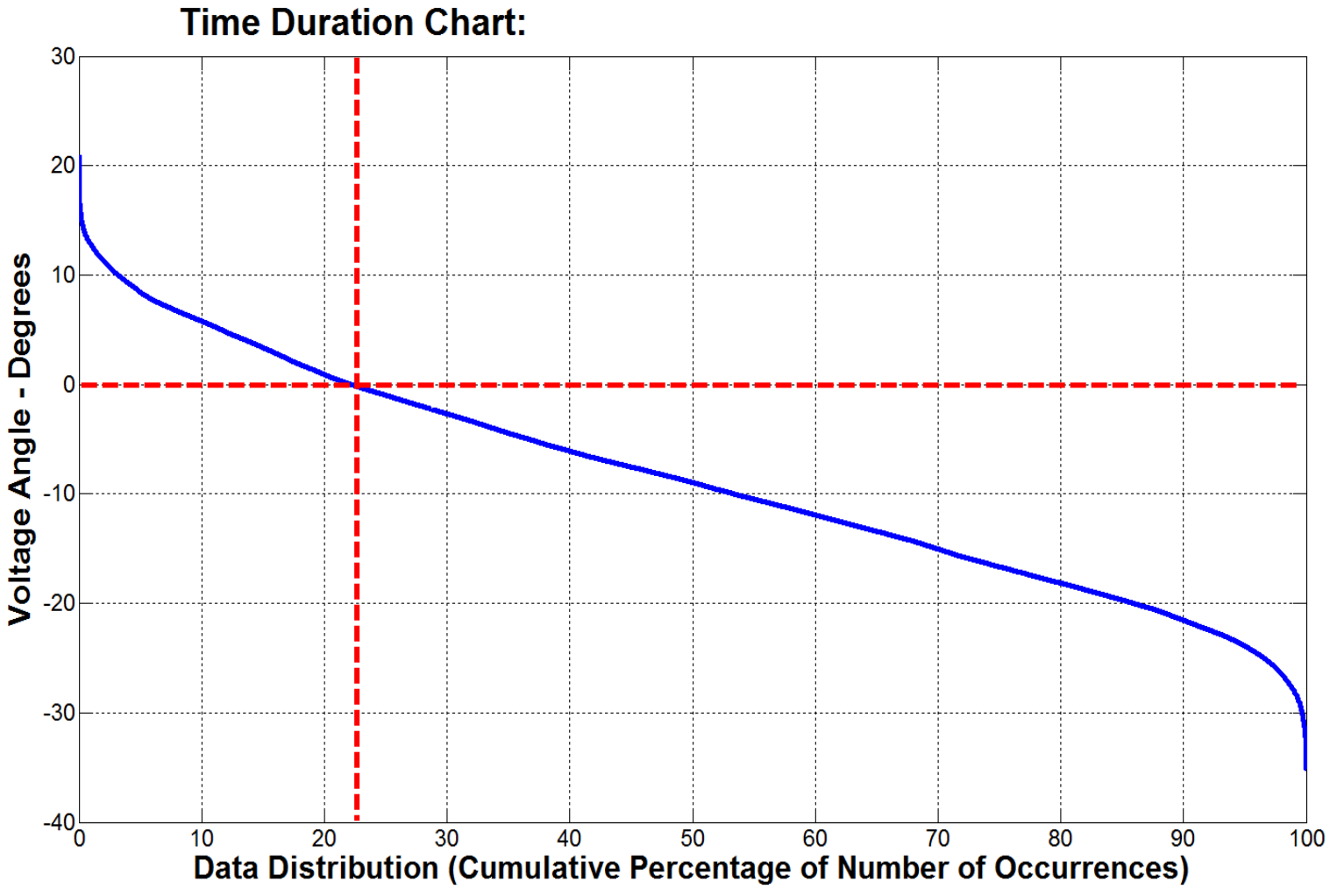
FarWest 7


Time Duration Chart:
Voltage Angle - Degrees
30
20
10
0
-10
-20
-30
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

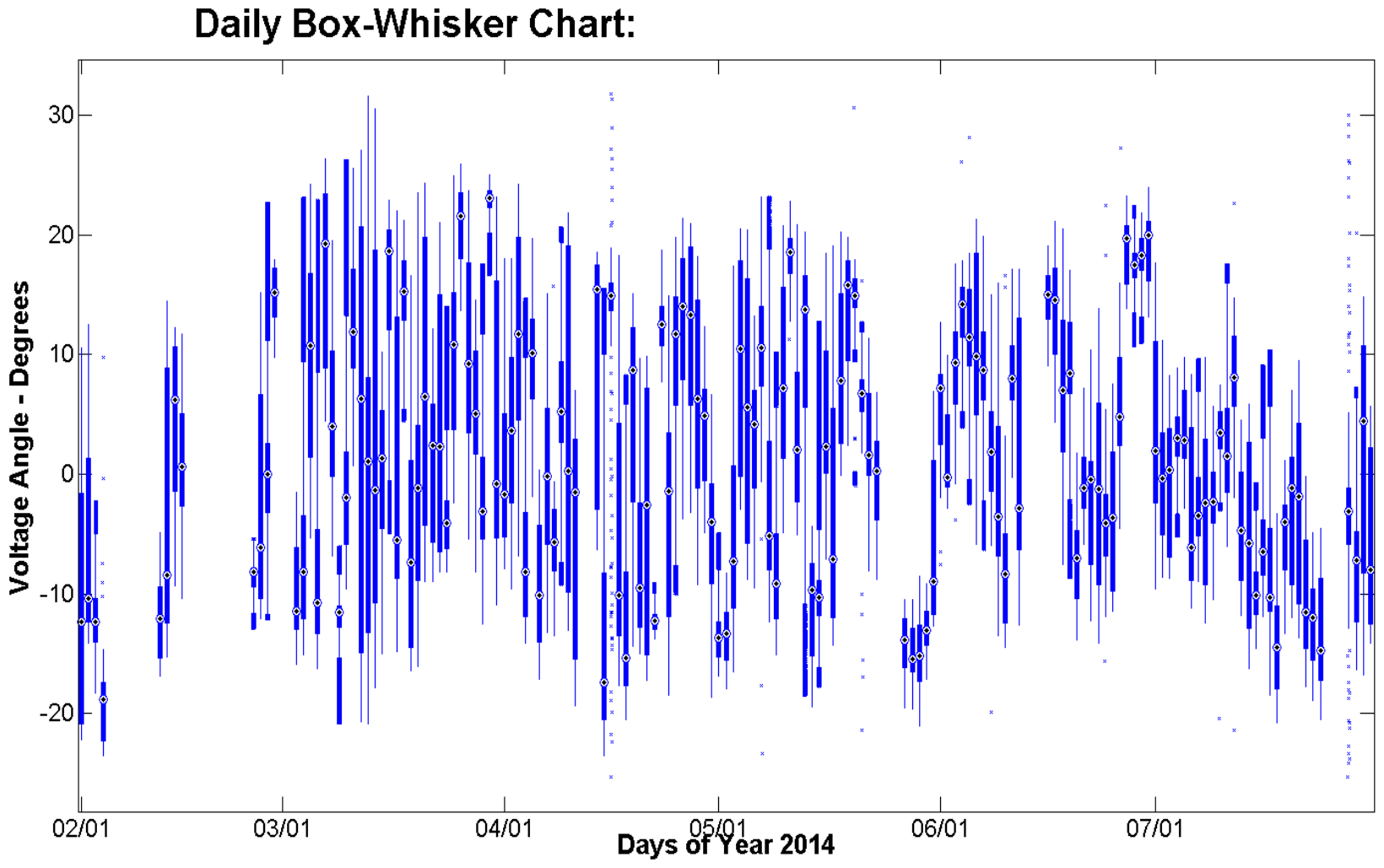
FarWest 8


Daily Box-Whisker Chart:
Voltage Angle - Degrees
20
10
0
-10
-20
-30
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

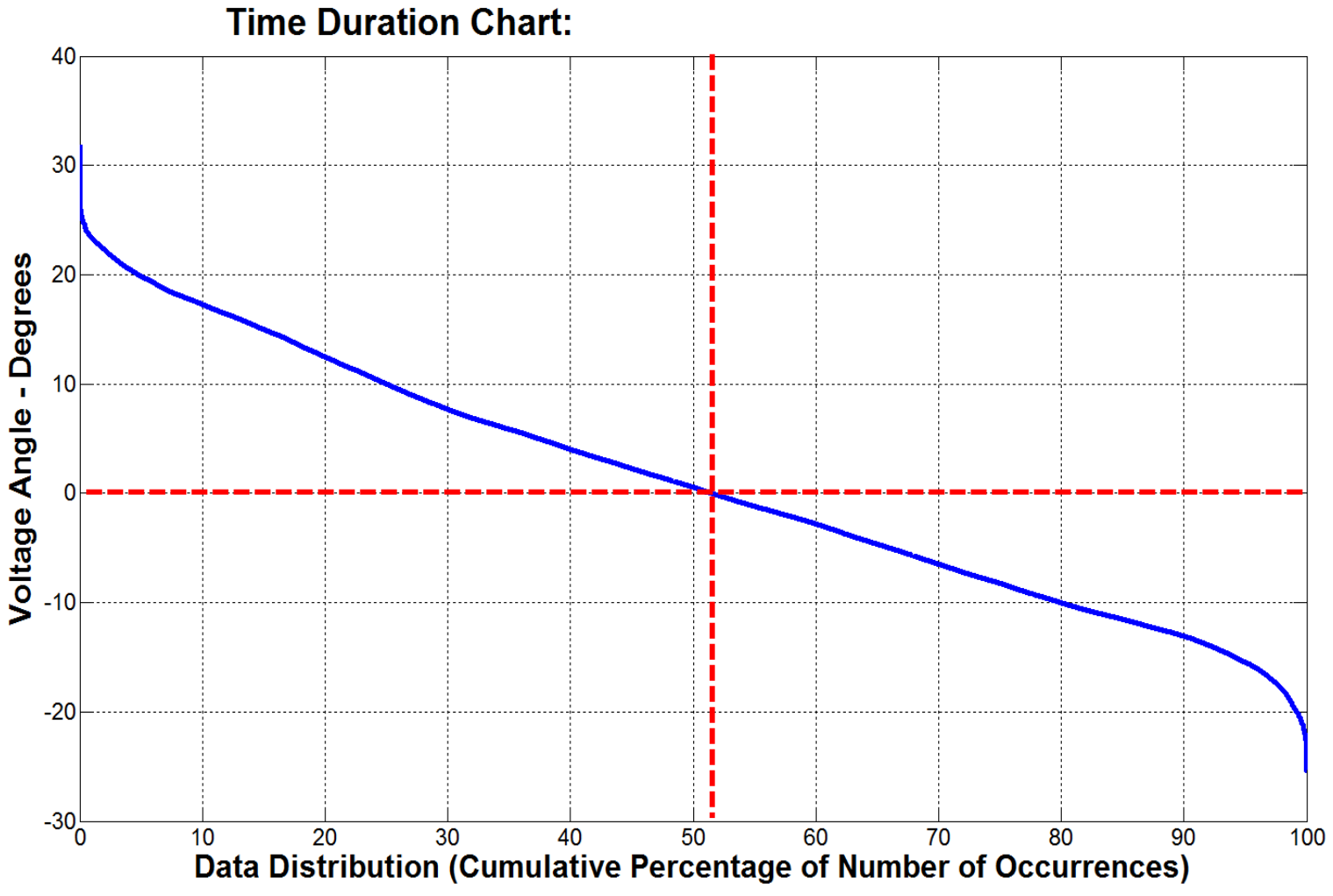
FarWest 8


Time Duration Chart:
Voltage Angle - Degrees
30
20
10
0
-10
-20
-30
-40
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

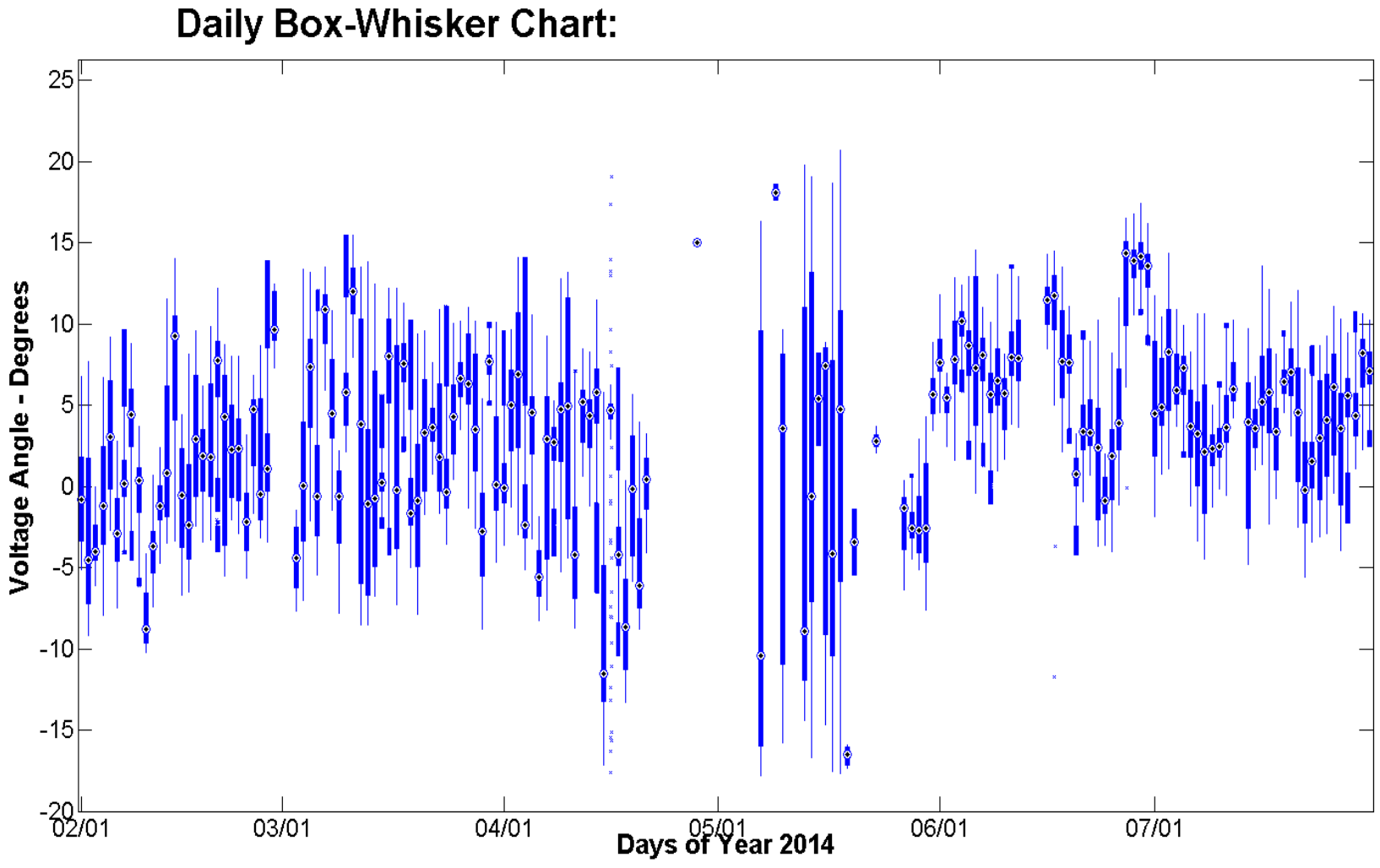
FarWest 9


Daily Box-Whisker Chart:
Voltage Angle - Degrees
30
20
10
0
-10
-20
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

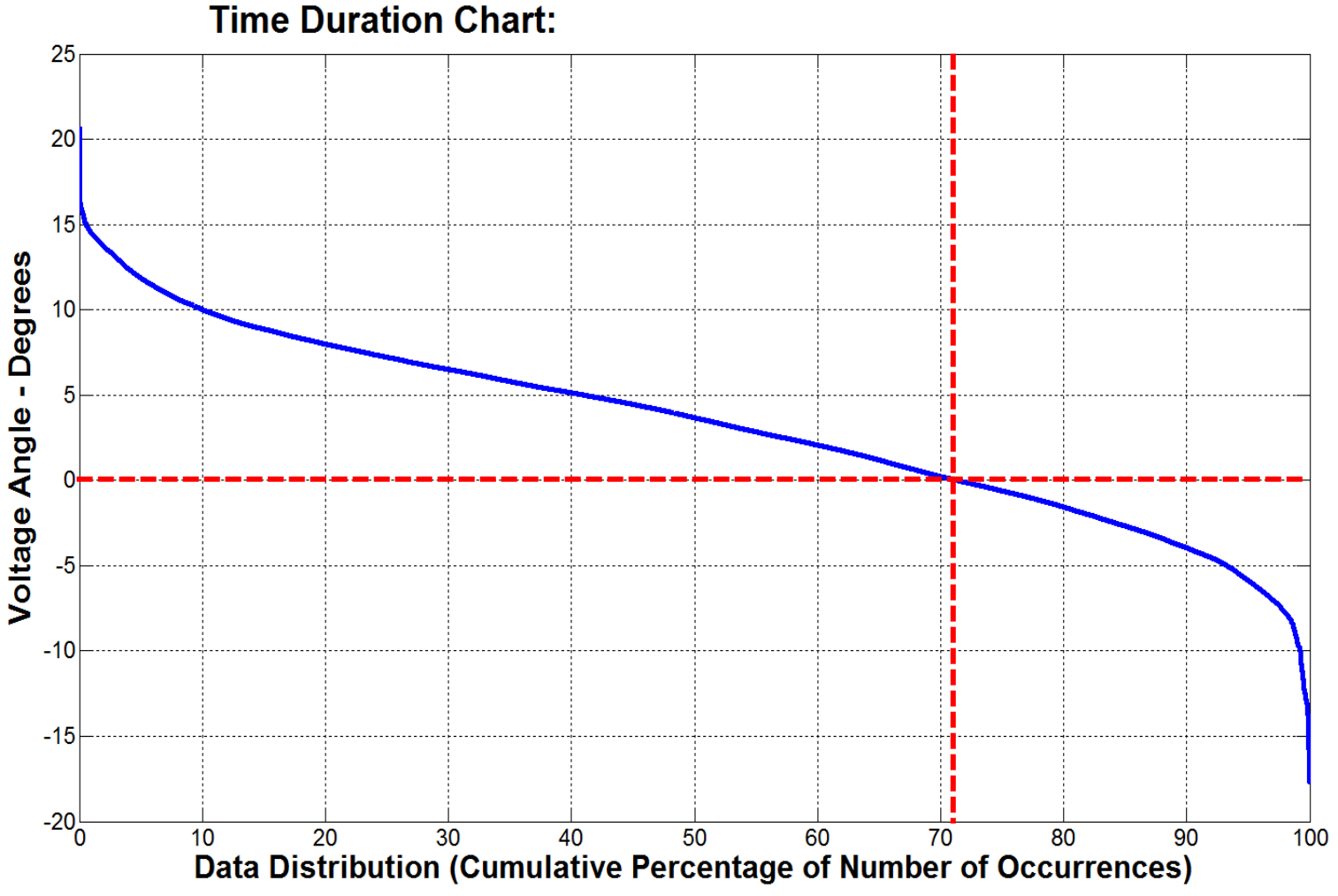
FarWest 9


Time Duration Chart:
Voltage Angle - Degrees
40
30
20
10
0
-10
-20
-30
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

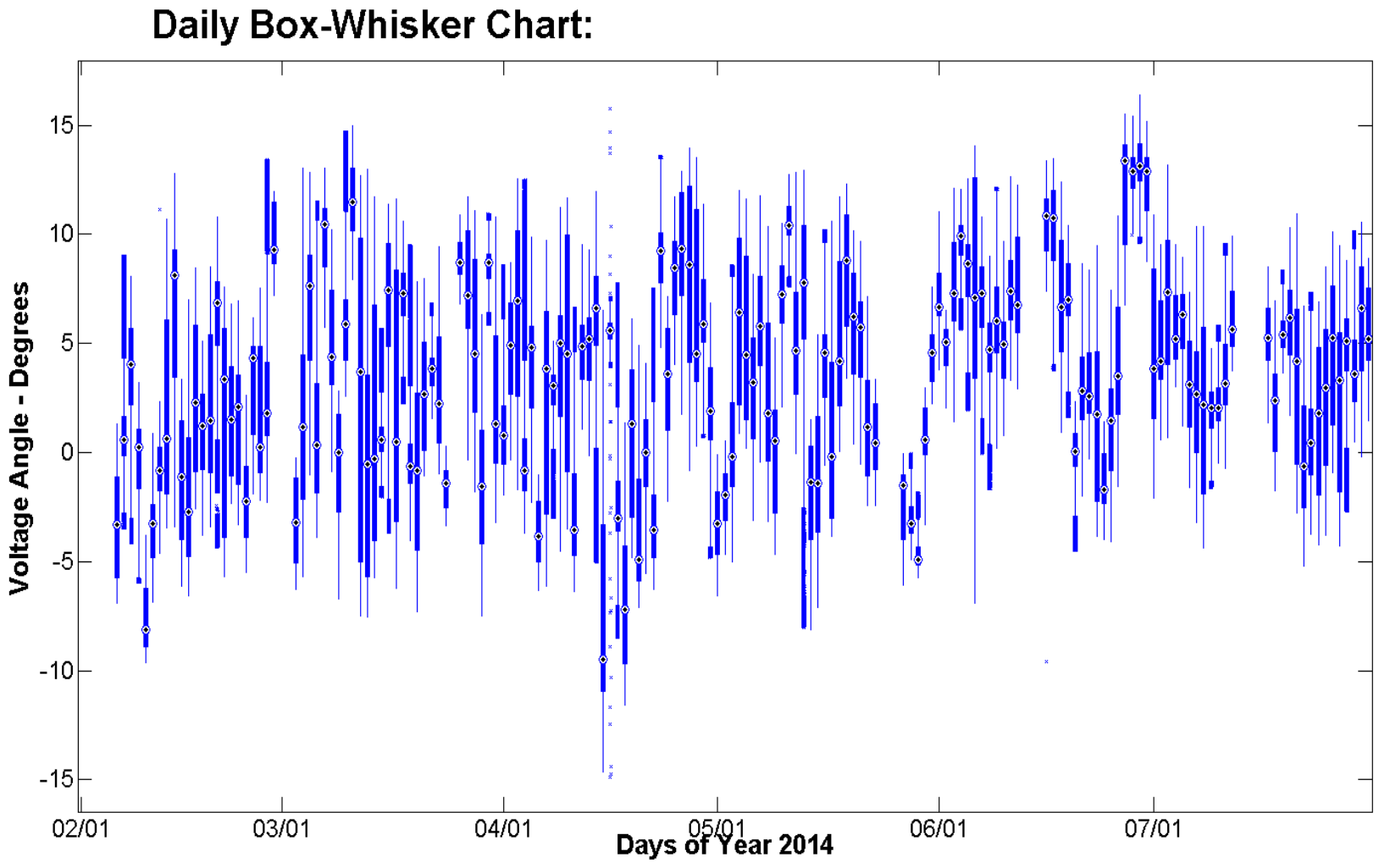
West 16


Daily Box-Whisker Chart:
Voltage Angle - Degrees
25
20
15
10
5
0
-5
-10
-15
-20
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

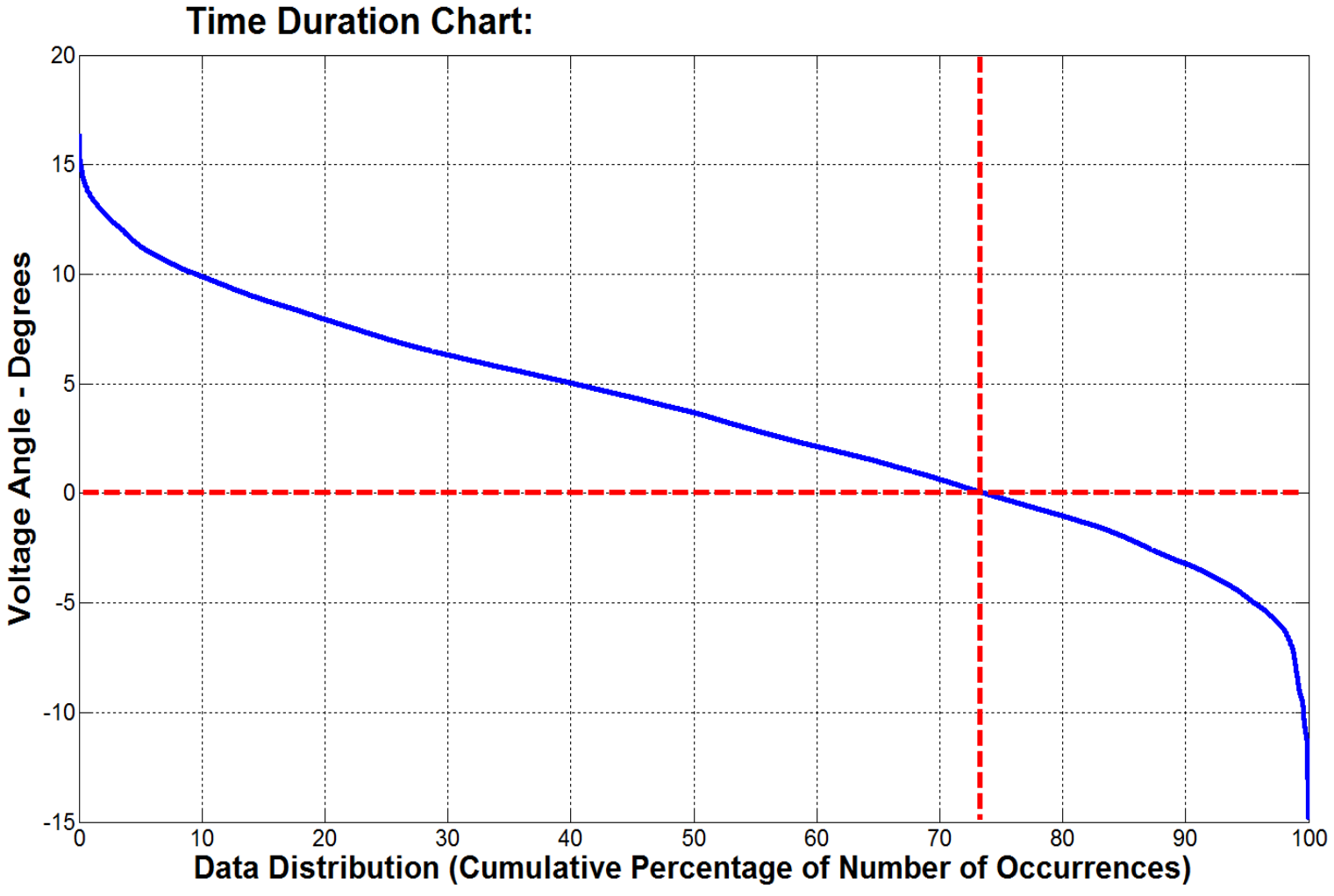
West 16


Time Duration Chart:
Voltage Angle - Degrees
25
20
15
10
5
0
-5
-10
-15
-20
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

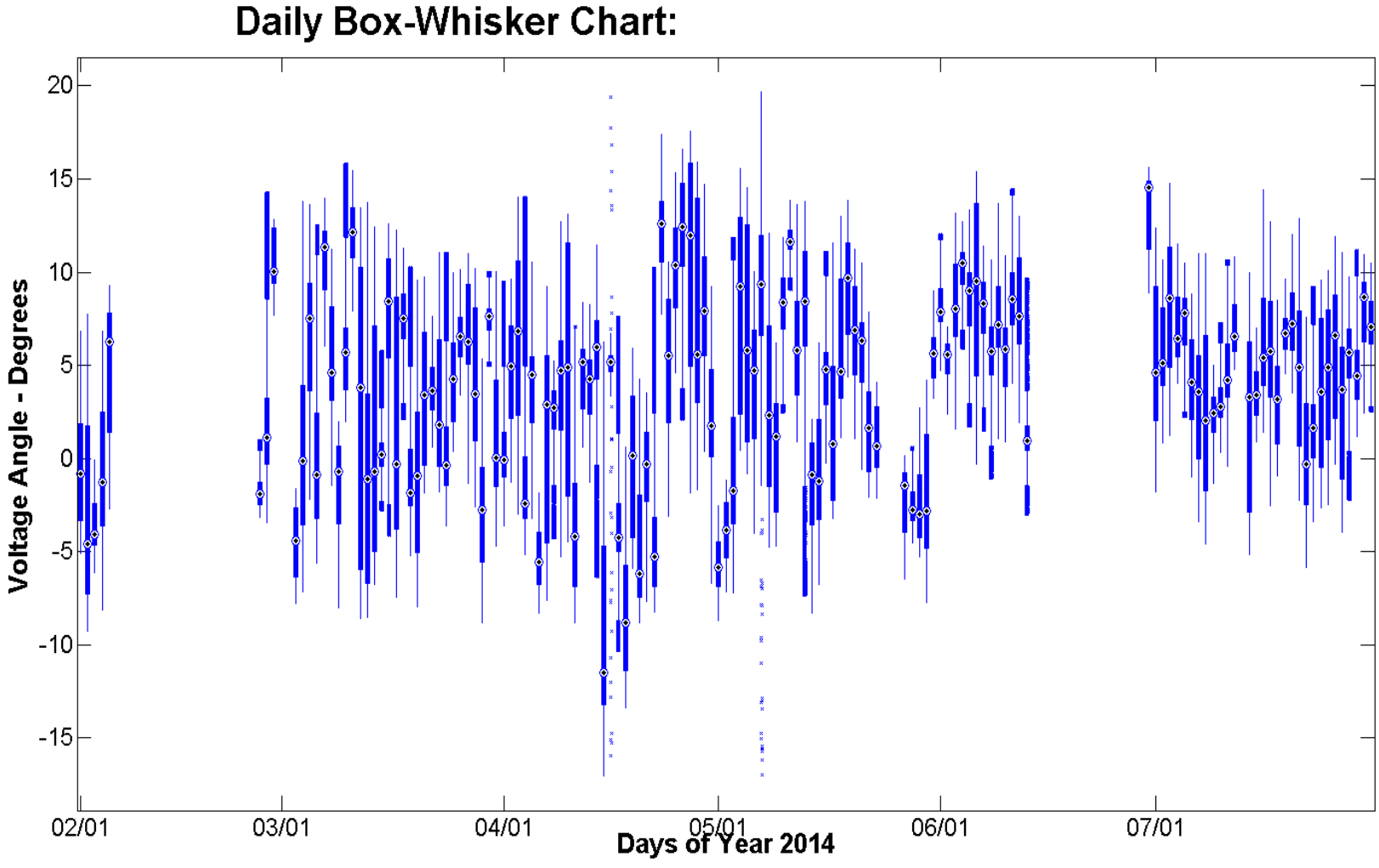
West 3


Daily Box-Whisker Chart:
Voltage Angle - Degrees
15
10
5
0
-5
-10
-15
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

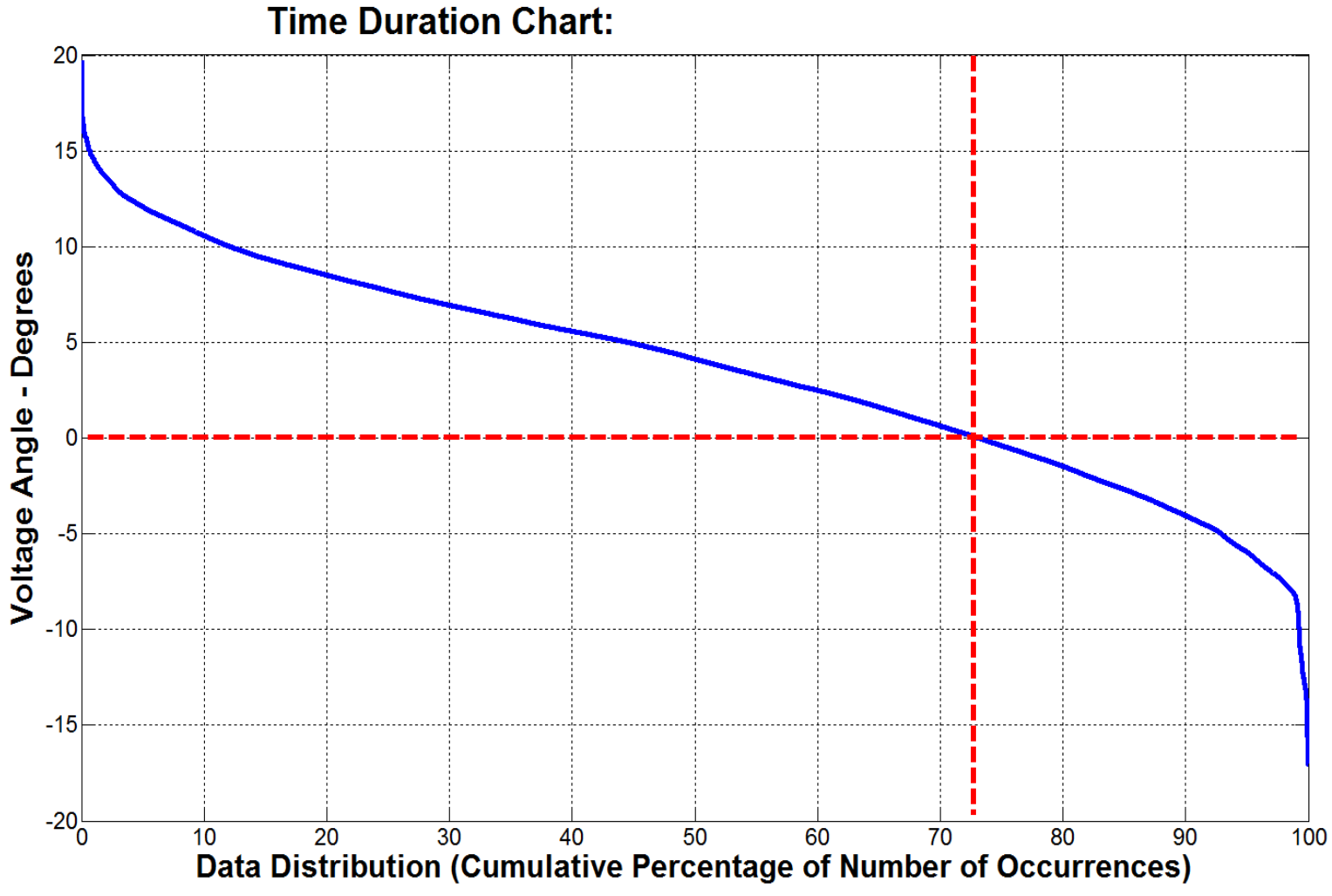
West 3


Time Duration Chart:
Voltage Angle - Degrees
Data Distribution (Cumulative Percentage of Number of Occurrences)
20
15
10
5
0
-5
-10
-15
0
10
20
30
40
50
60
70
80
90
100

West 15


Daily Box-Whisker Chart:
Voltage Angle - Degrees
20
15
10
5
0
-5
-10
-15
02/01
03/01
04/01
05/01
06/01
07/01
Days of Year 2014

West 15


Time Duration Chart:
Voltage Angle - Degrees
20
15
10
5
0
-5
-10
-15
-20
0
10
20
30
40
50
60
70
80
90
100
Data Distribution (Cumulative Percentage of Number of Occurrences)

Appendix B – Part 1
CCET Discovery Across Texas project

Baseline Analysis Update – Angle Differences

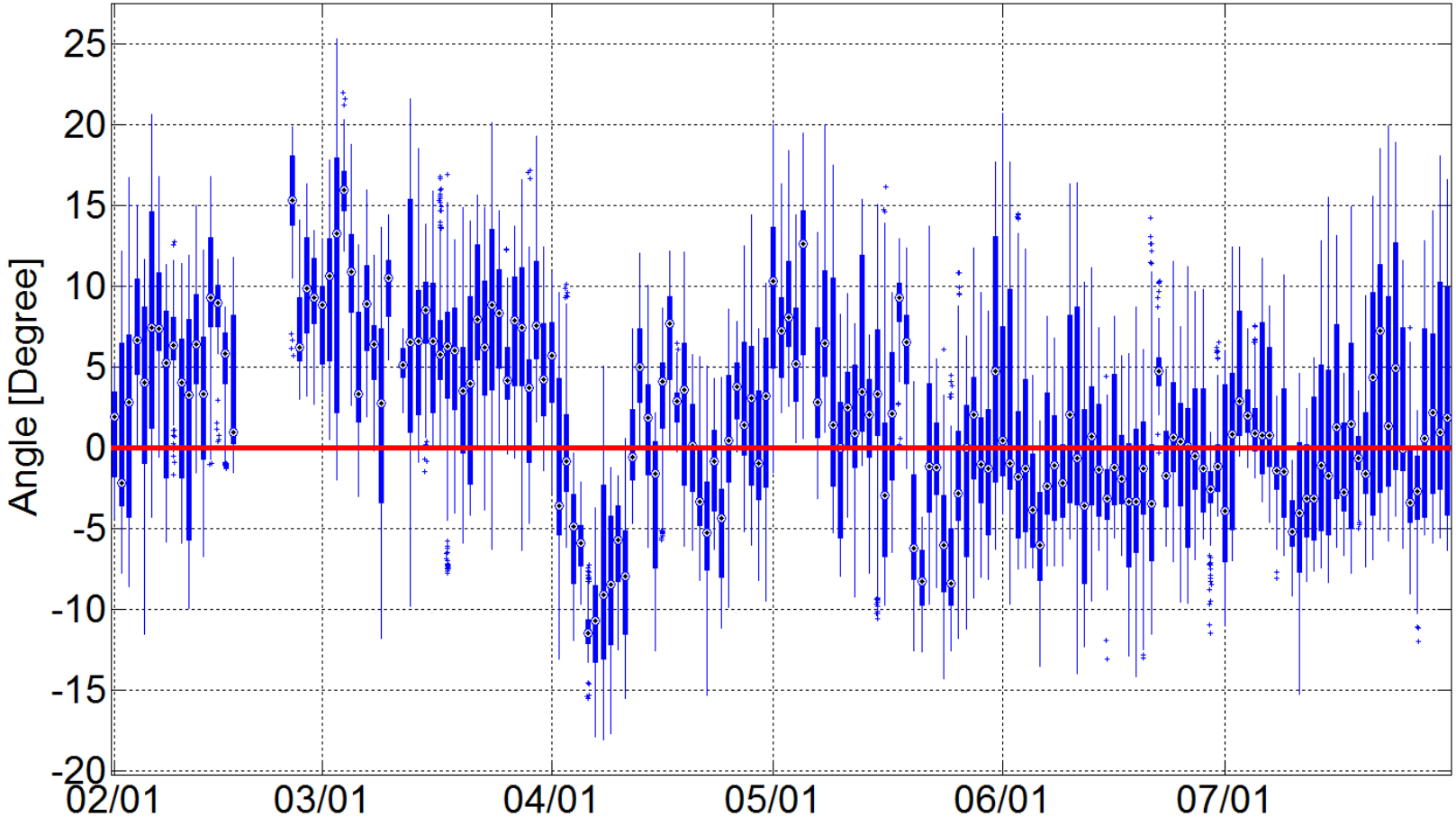
State Estimator Data: February to July 2014
Box-Whisker Plots and Time Duration Curves

Electric Power Group

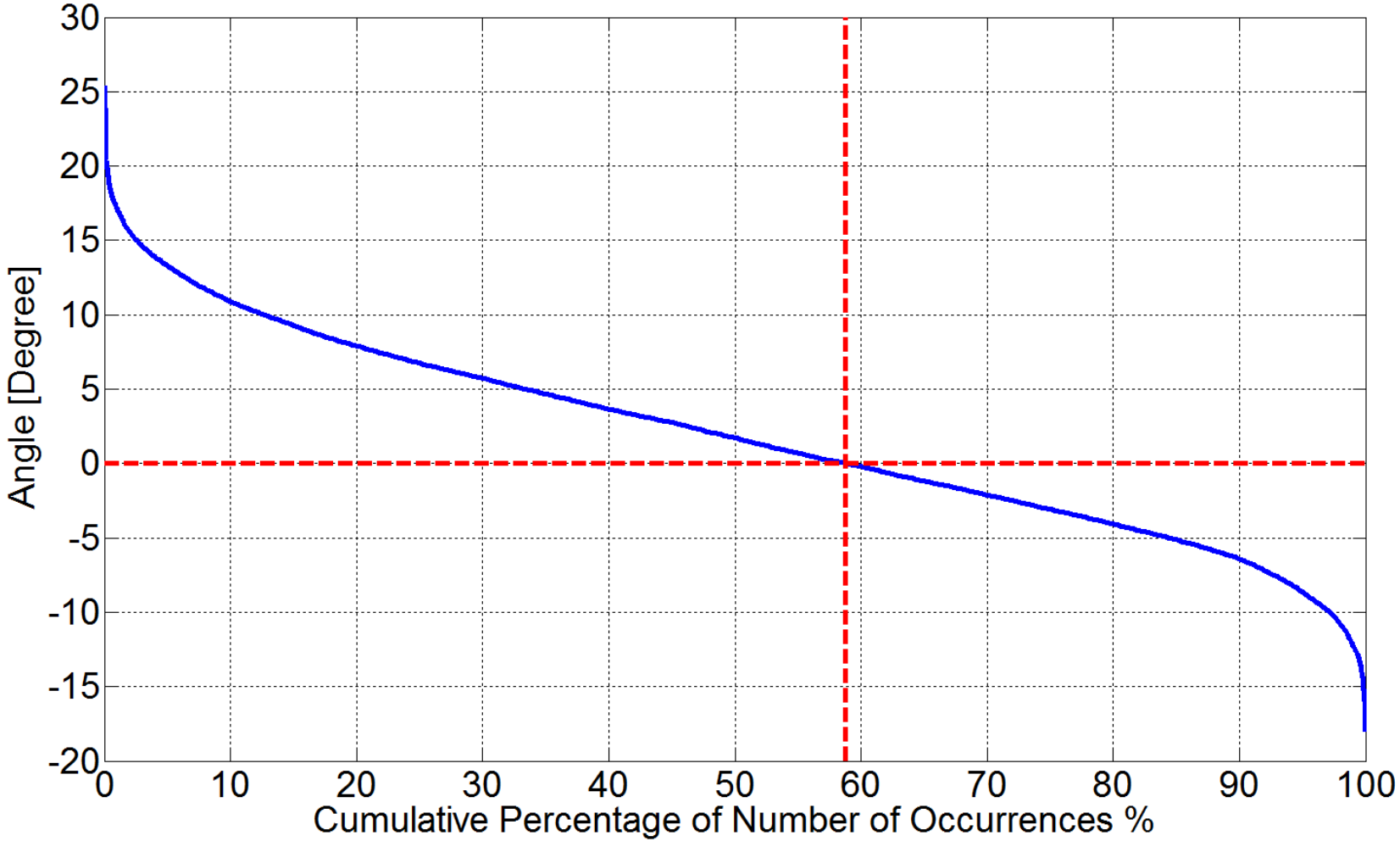
CCET

ERCOT

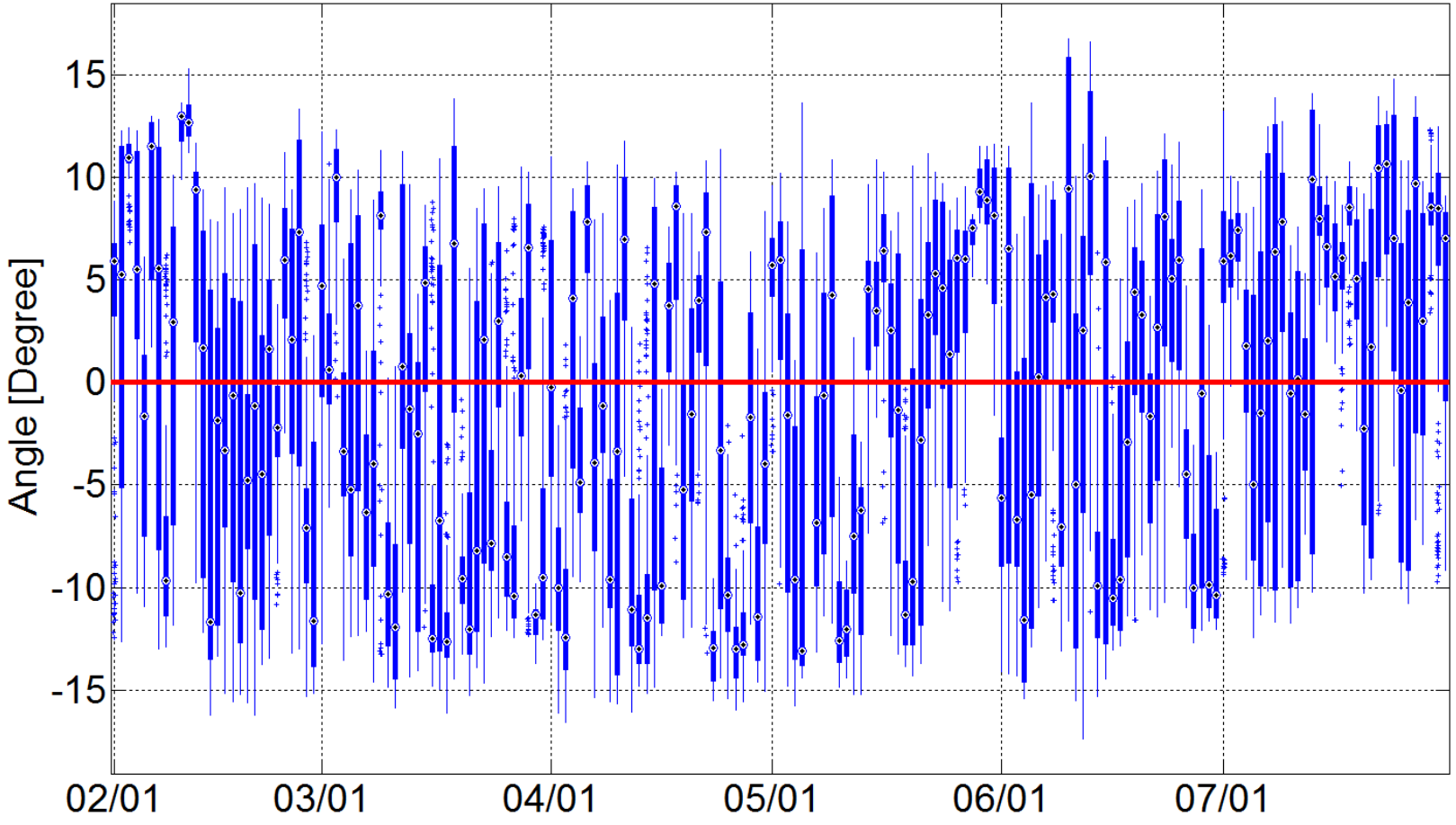
Coast 1-South 13



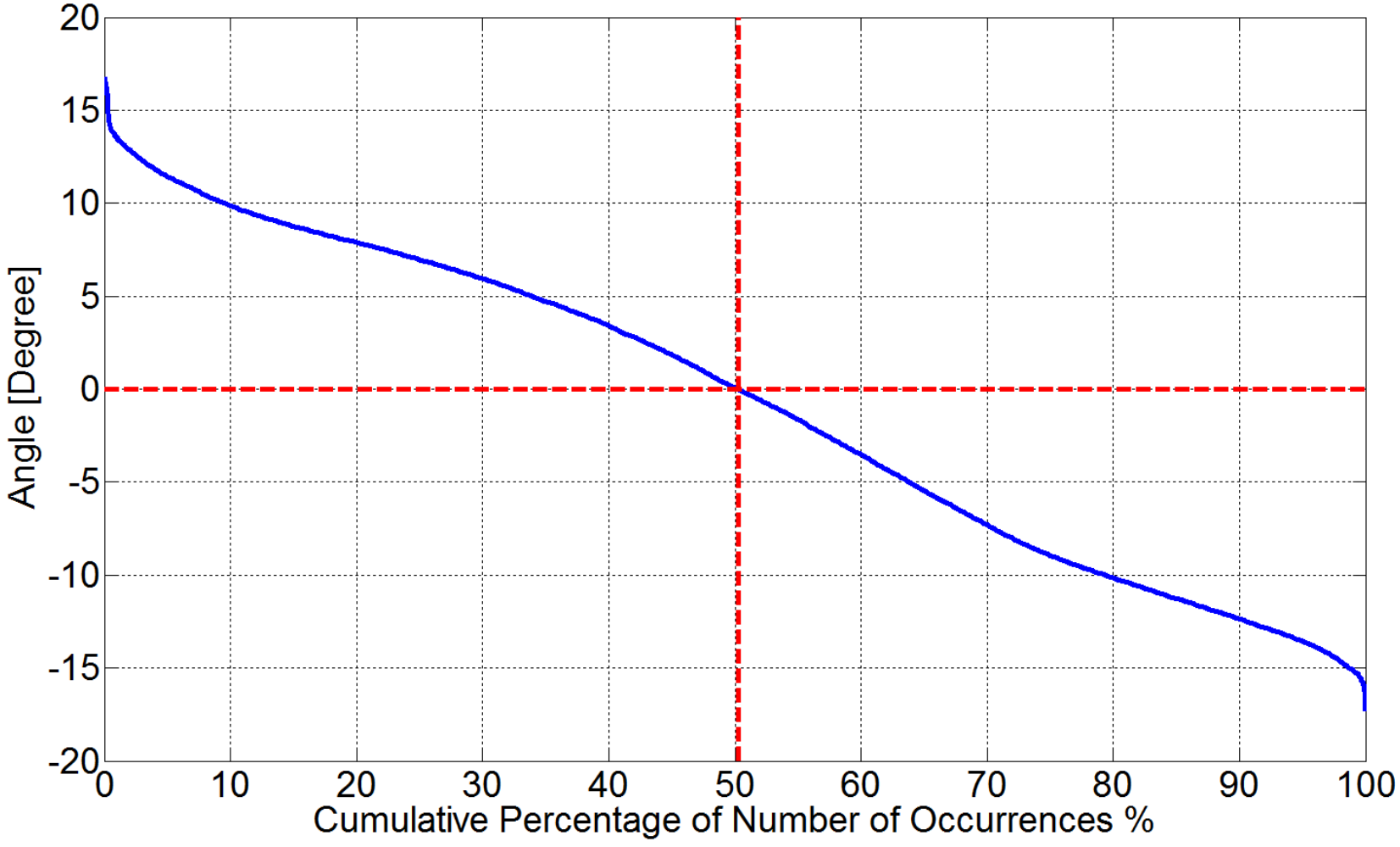
Coast 1-South 13



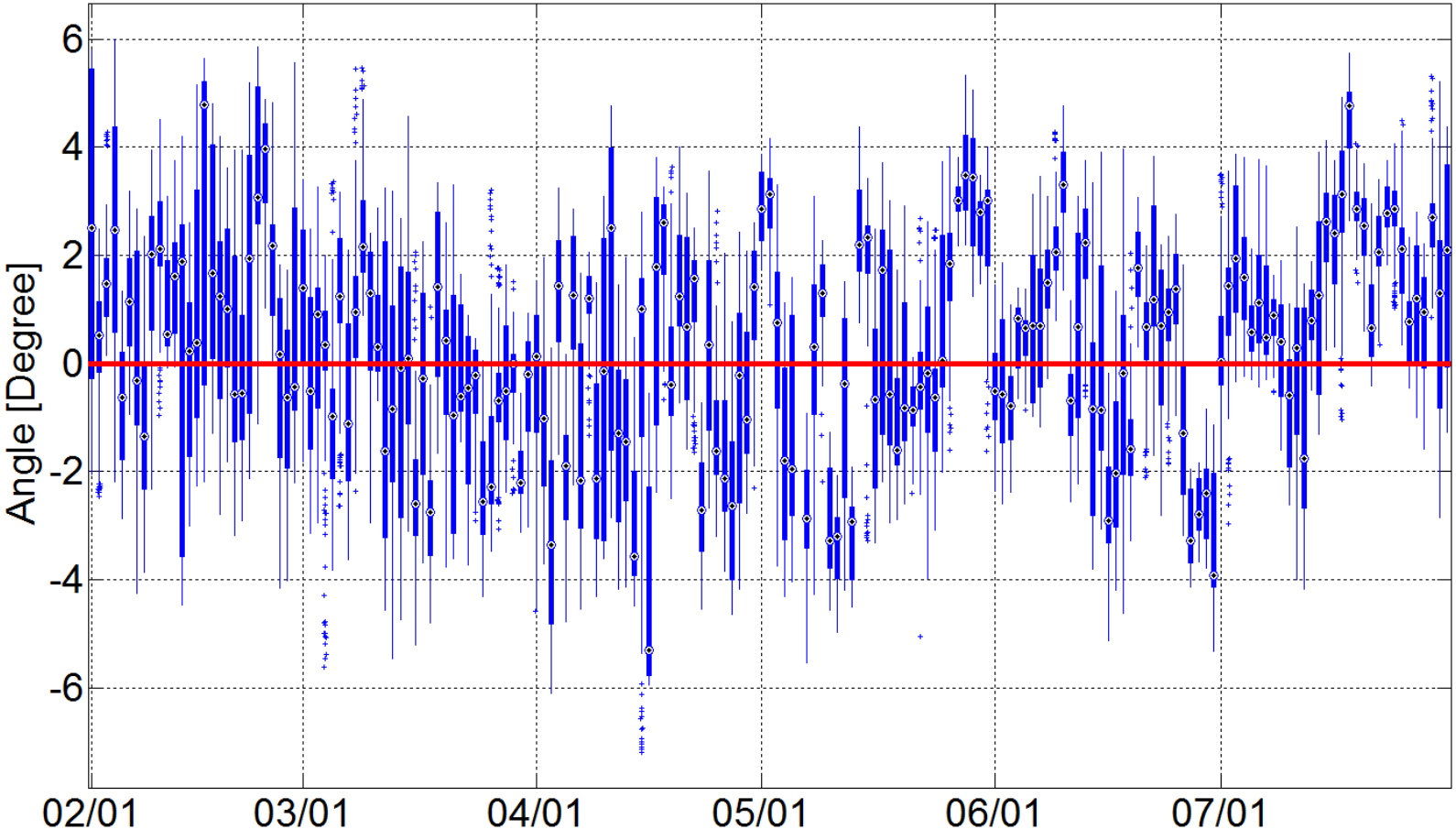
West 5-West 10



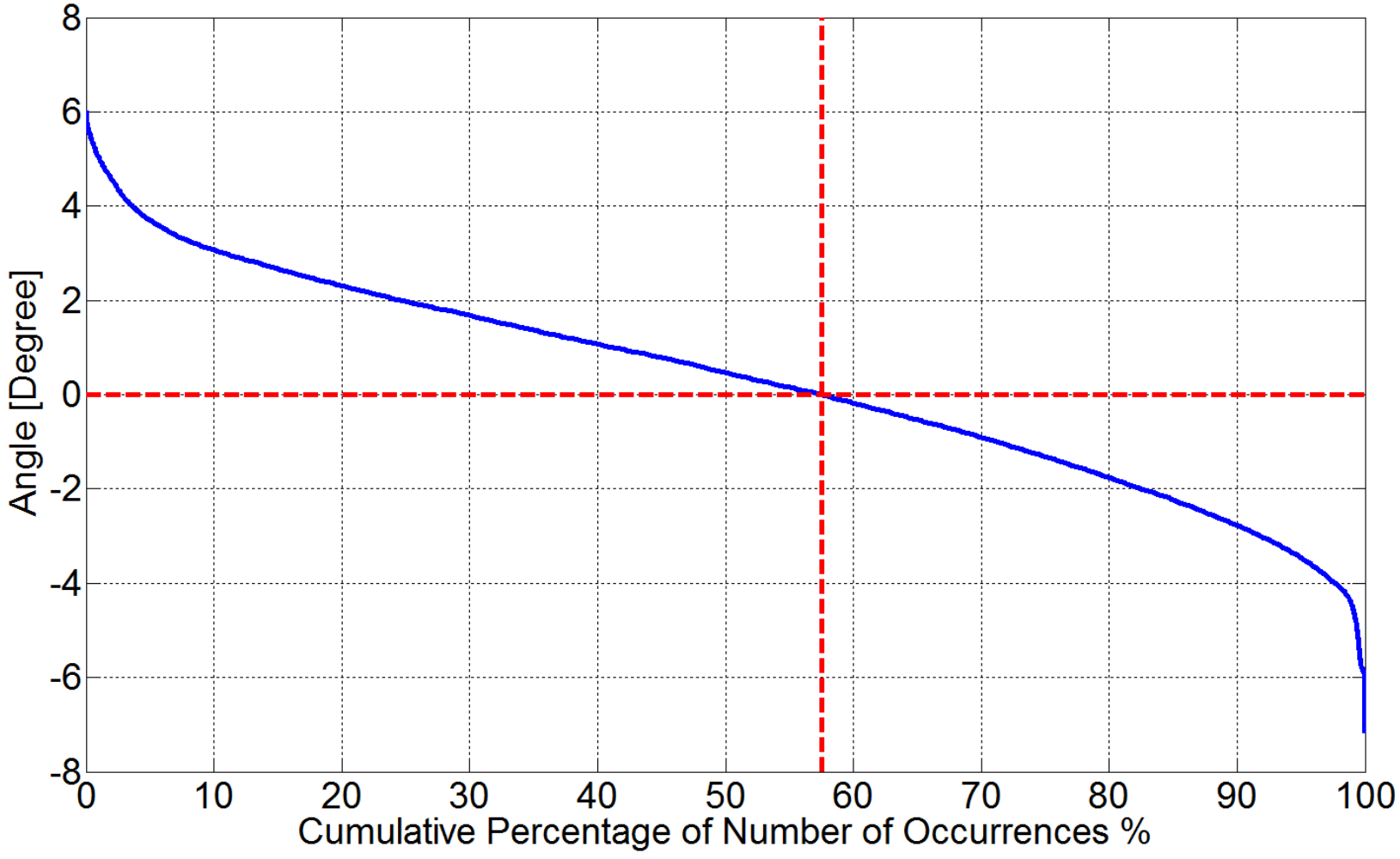
West 5-West 10



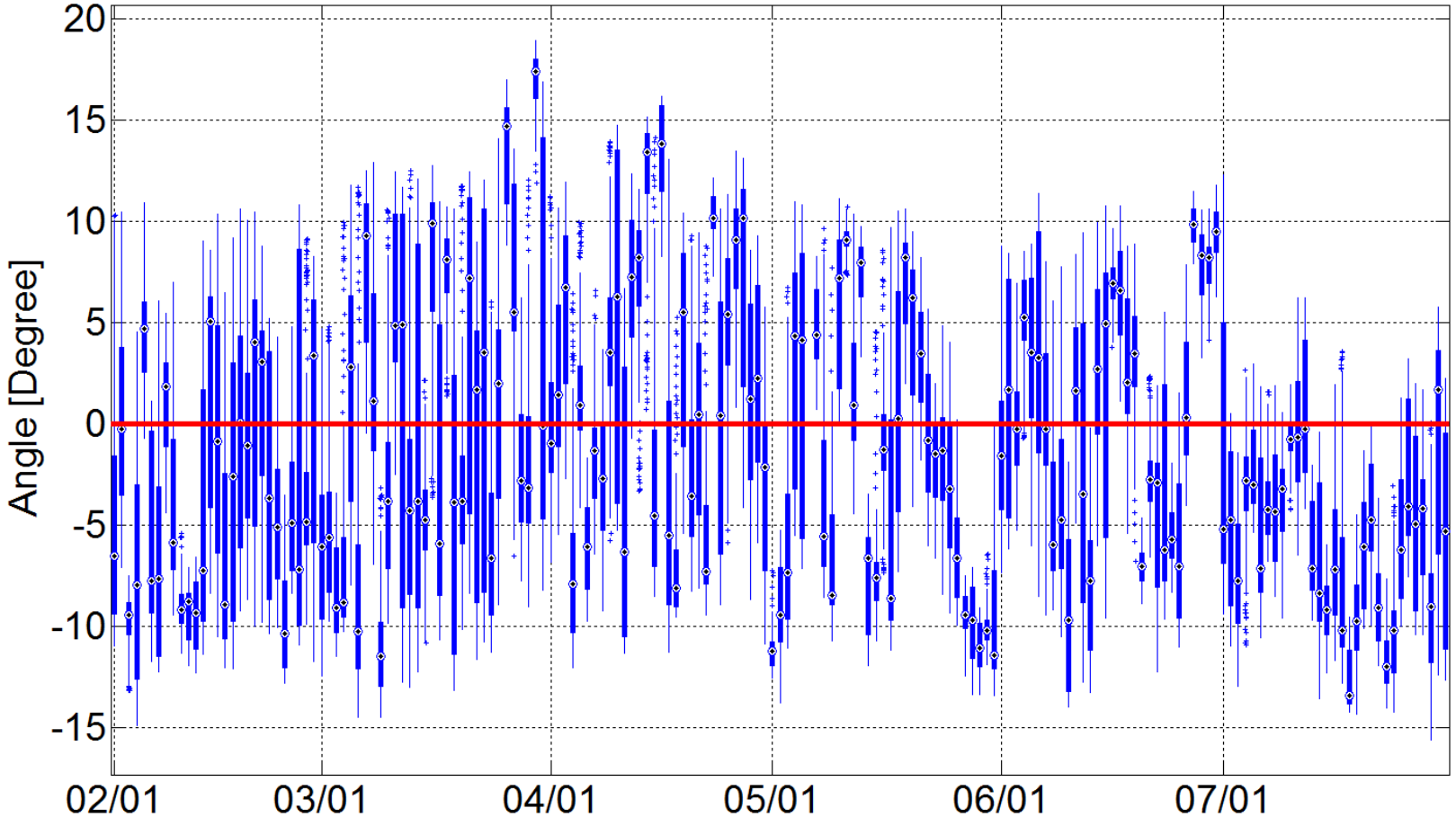
West 5-FarWest 4



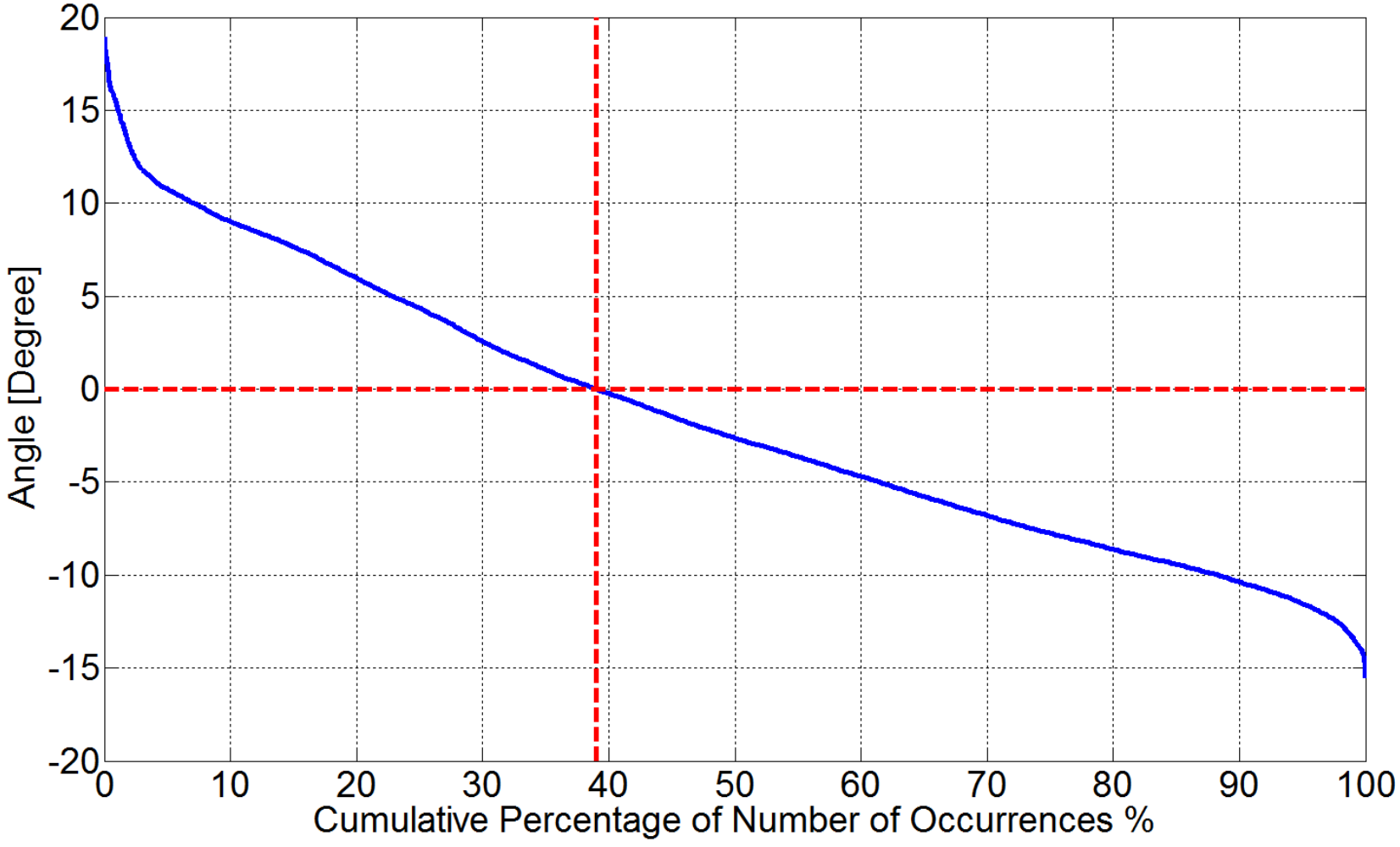
West 5-FarWest 4



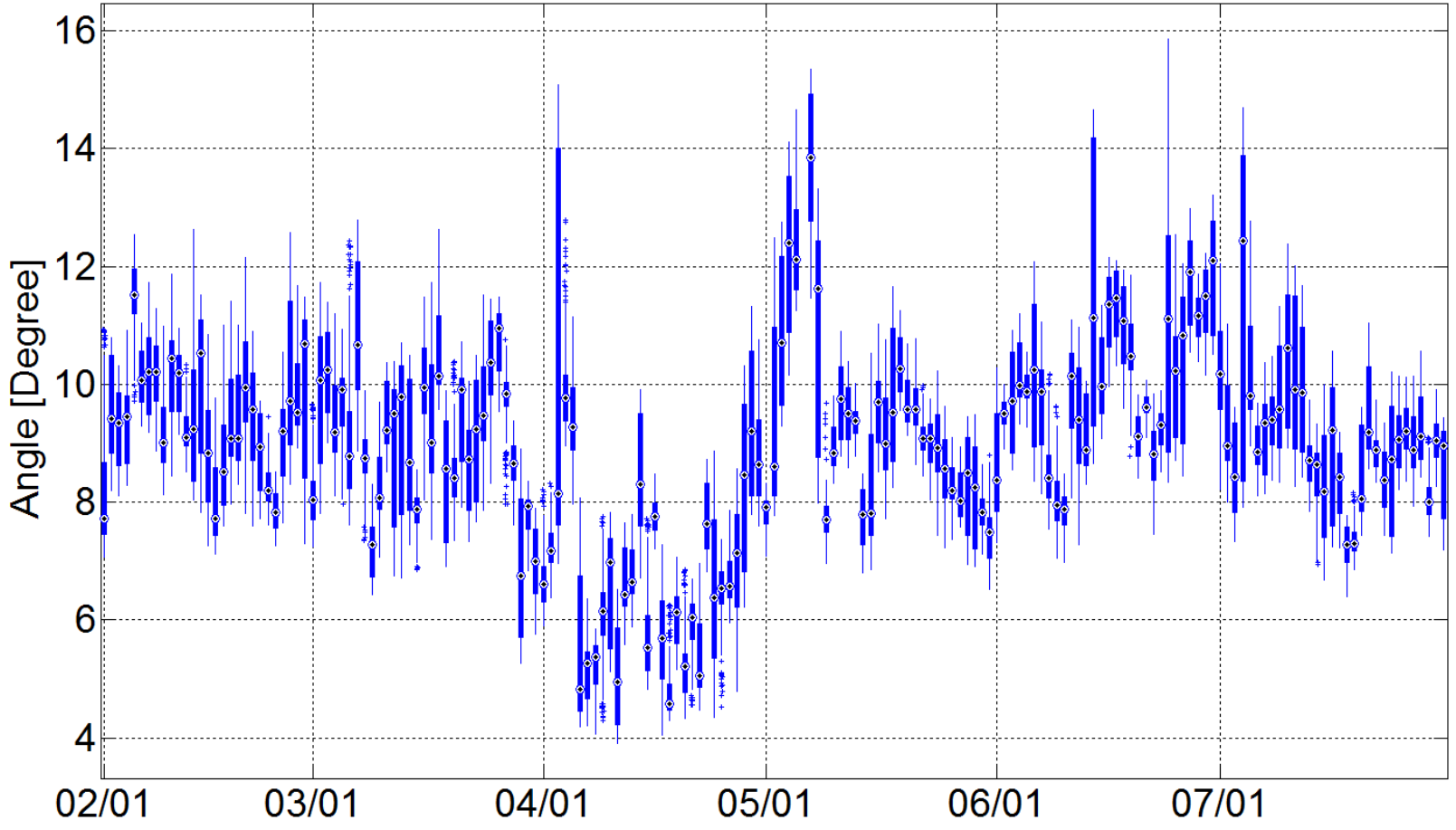
West 5-North 1



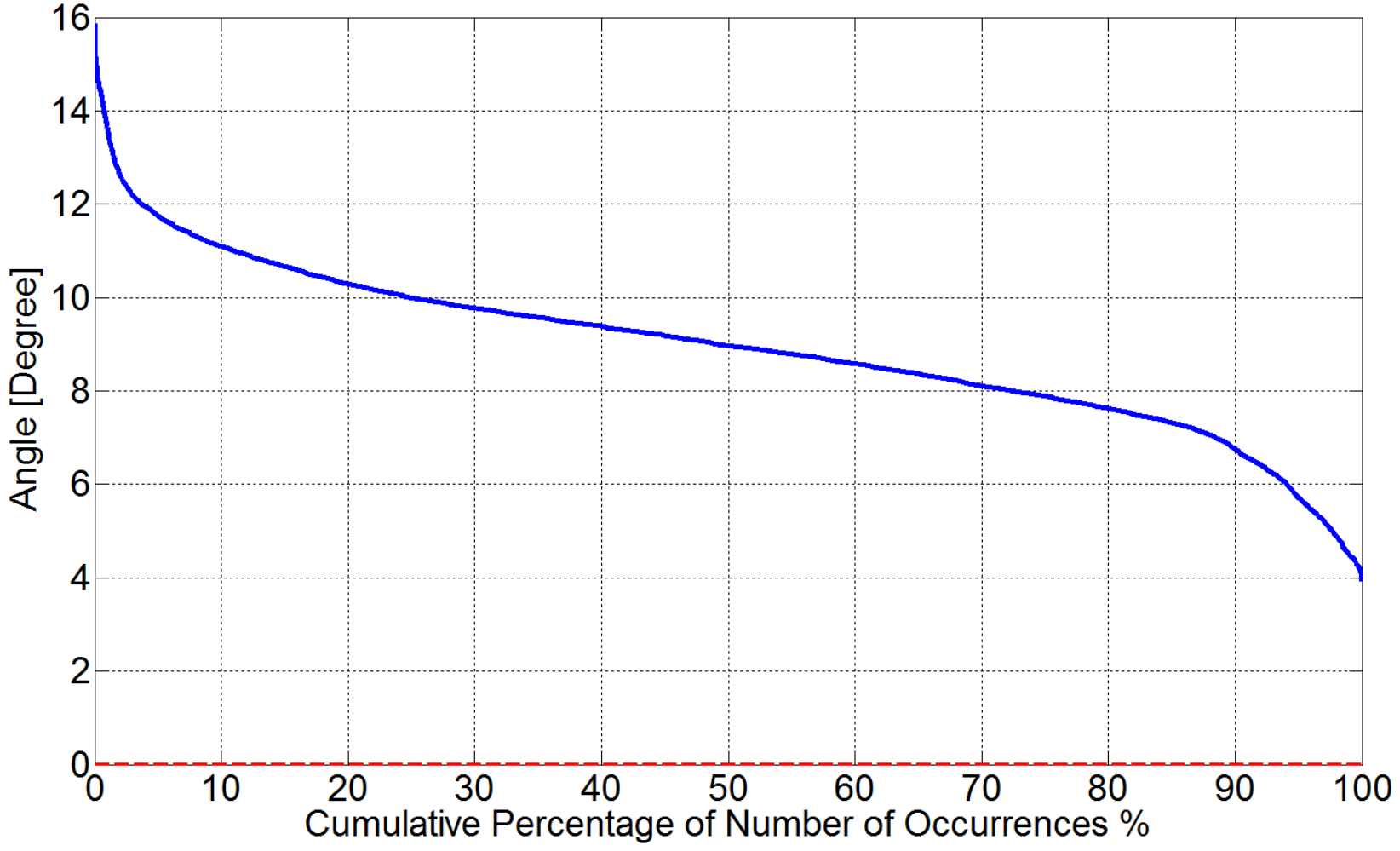
West 5-North 1



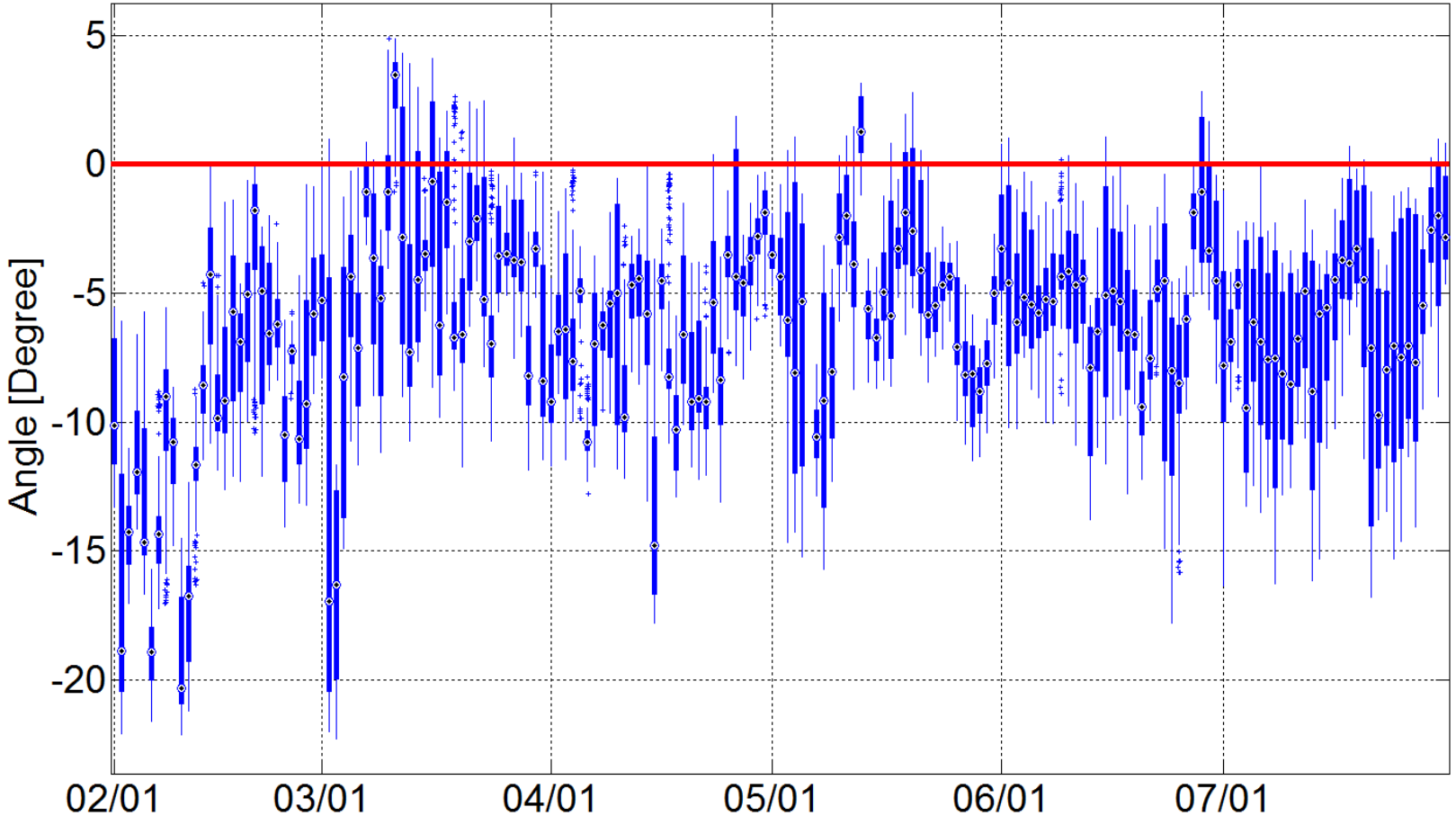
North 1-North 4



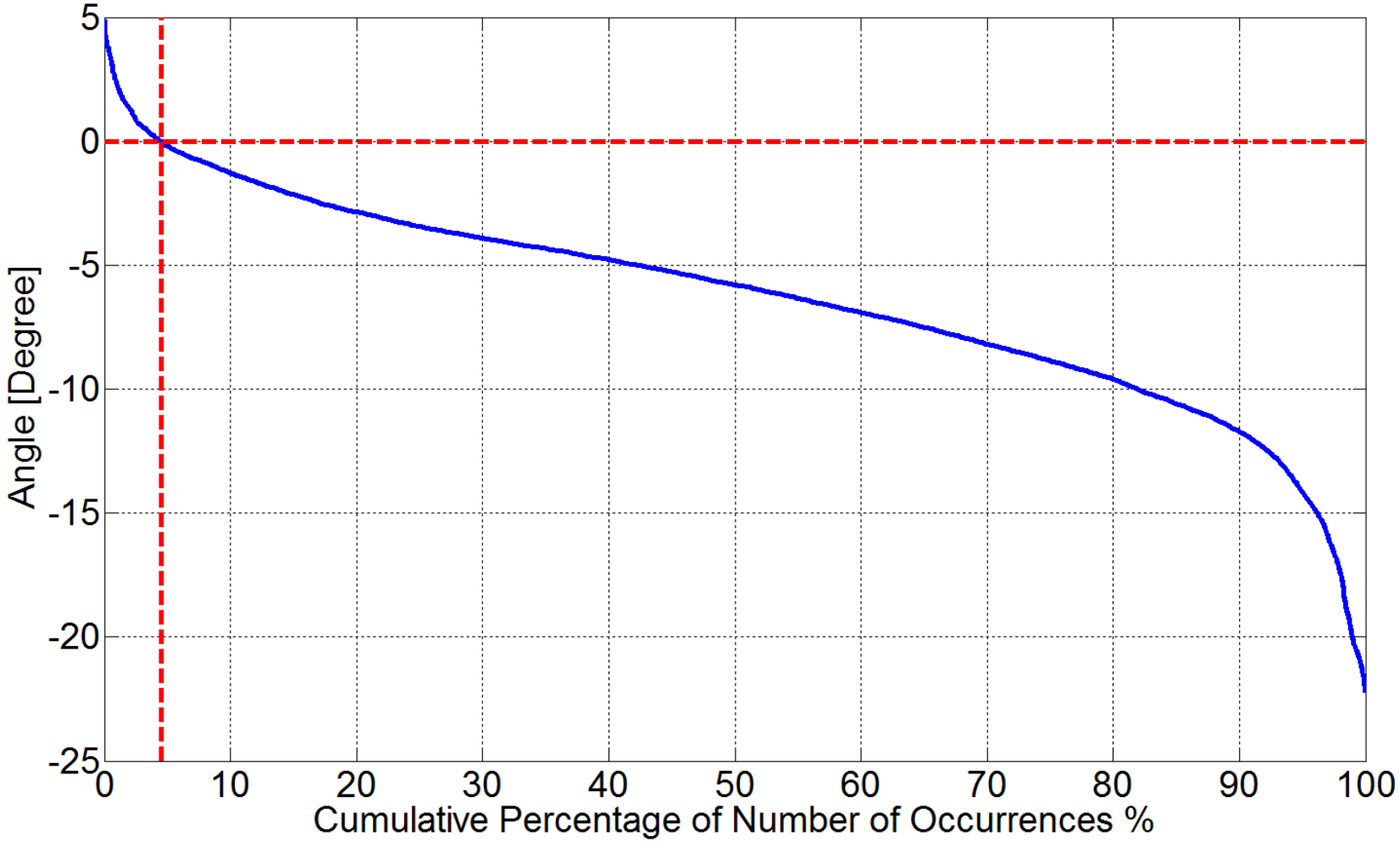
North 1-North 4



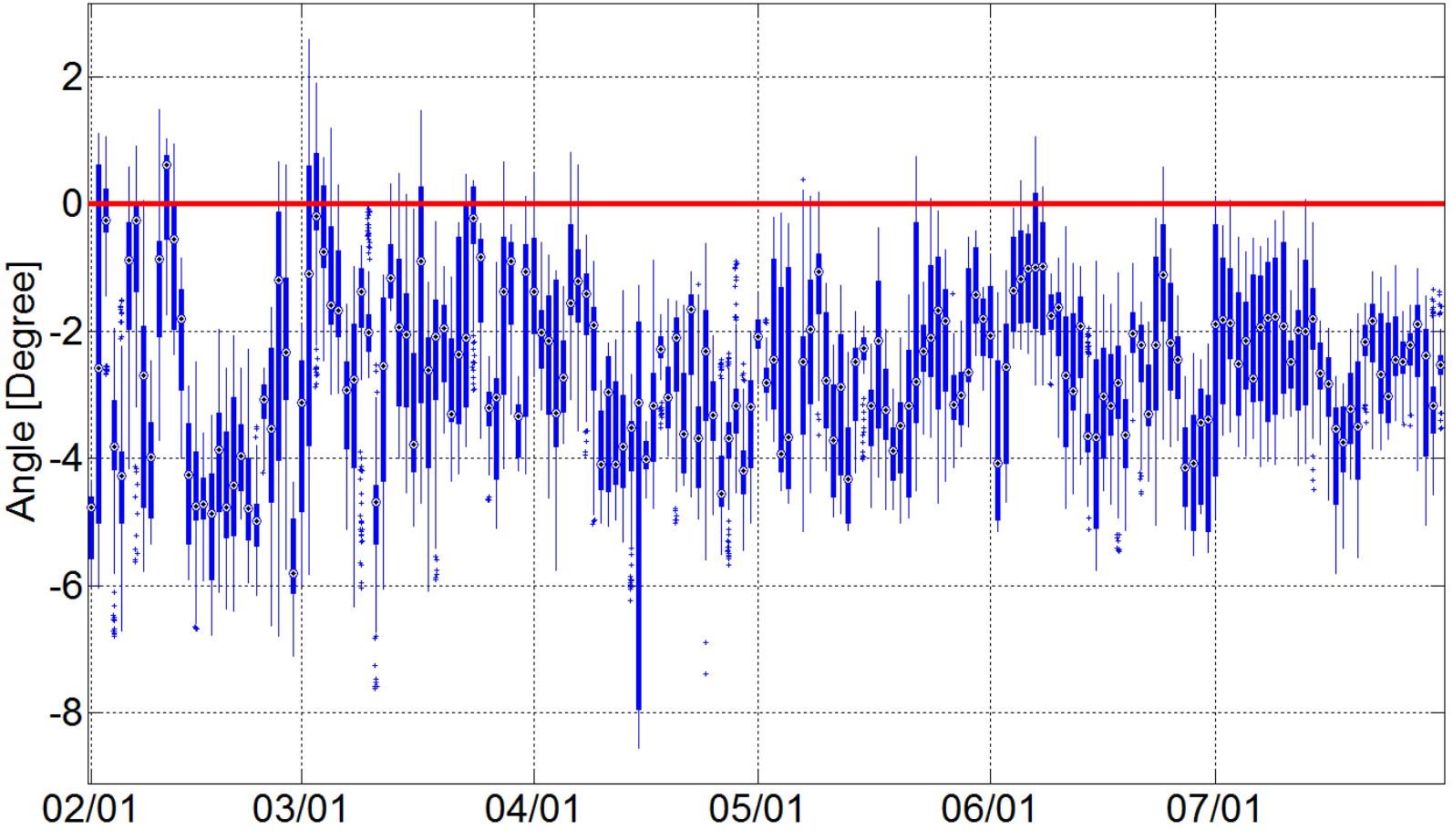
North 4-North 6



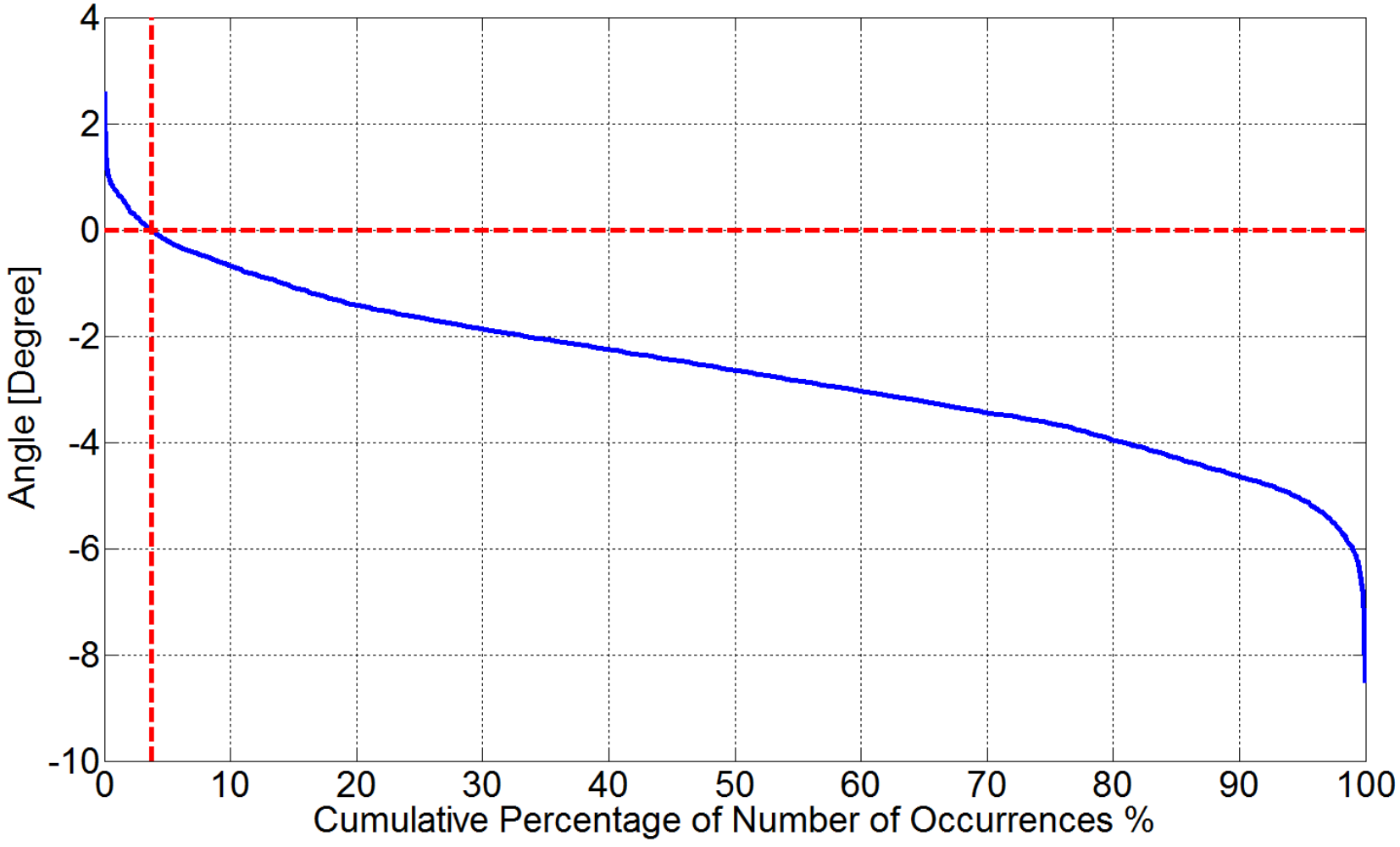
North 4-North 6



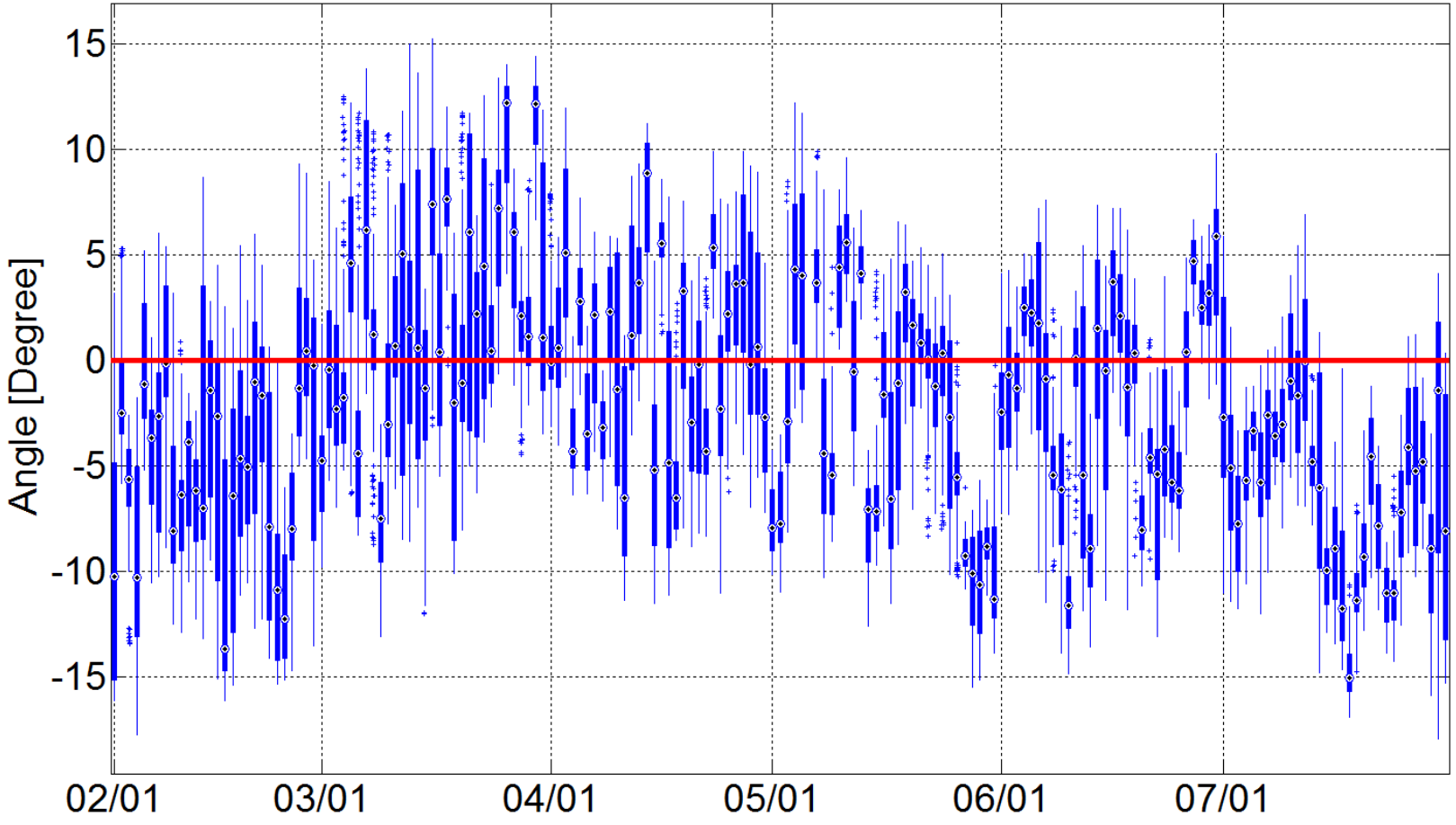
FarWest 7-FarWest 4



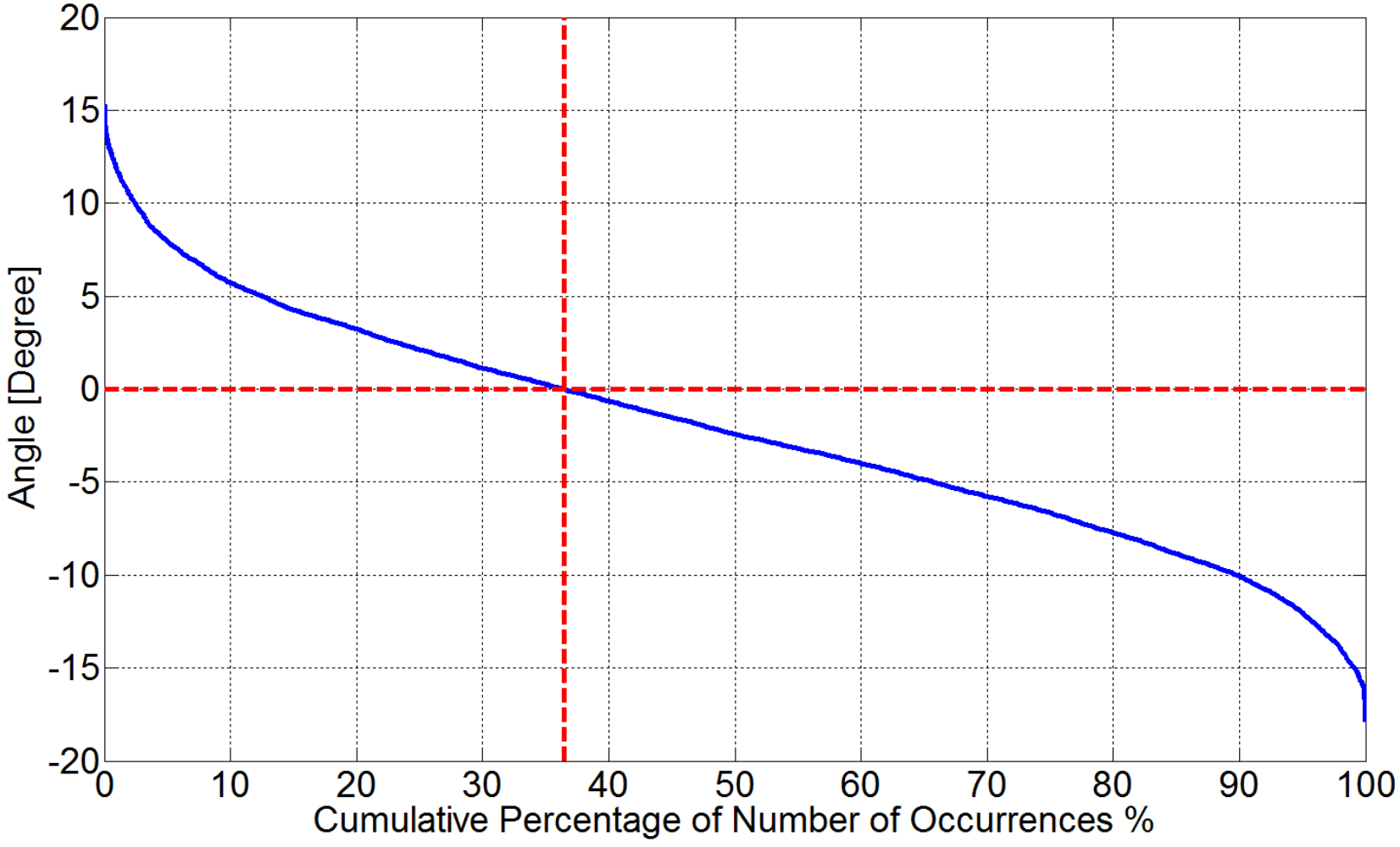
FarWest 7-FarWest 4



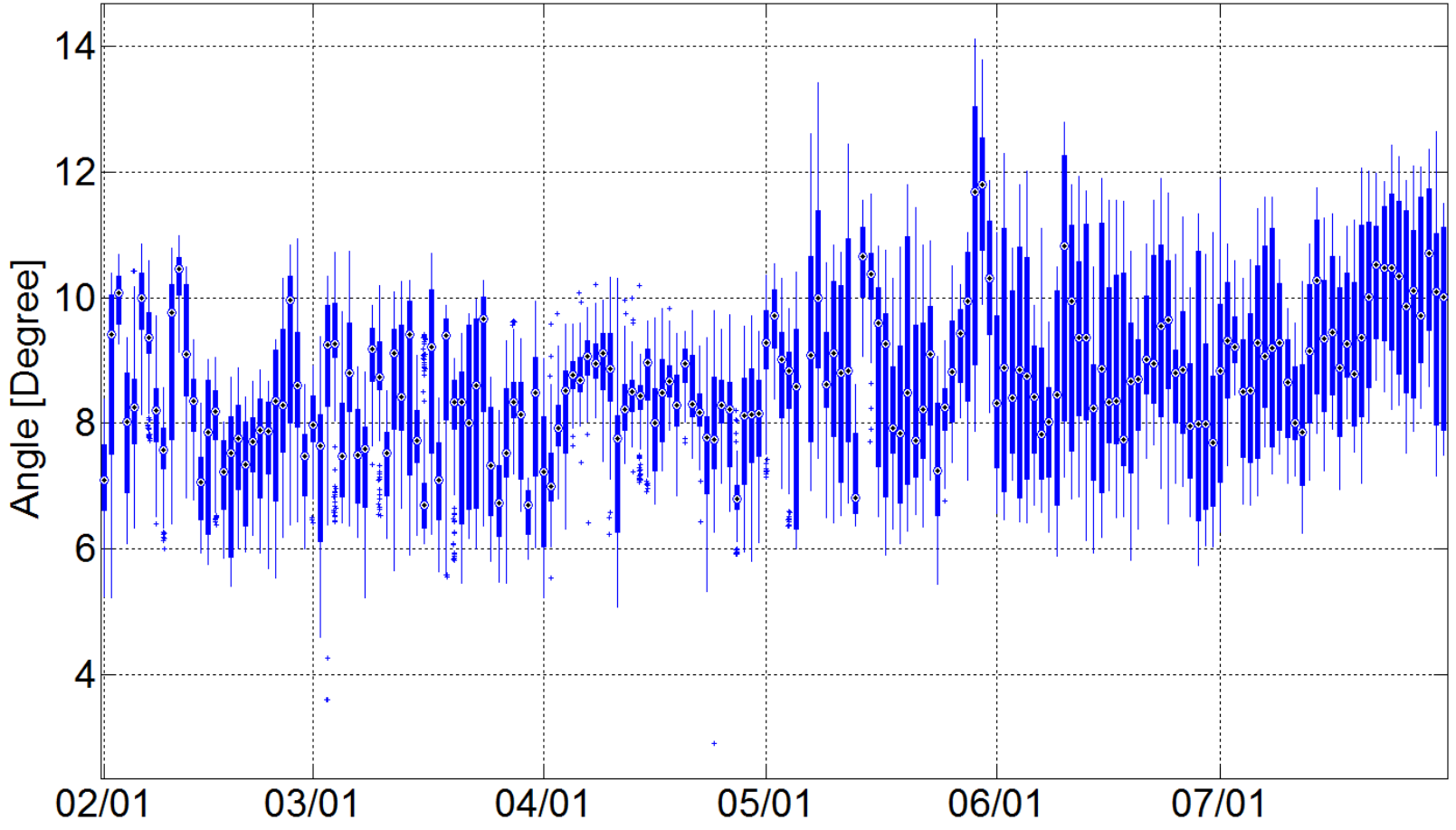
FarWest 7-West 14



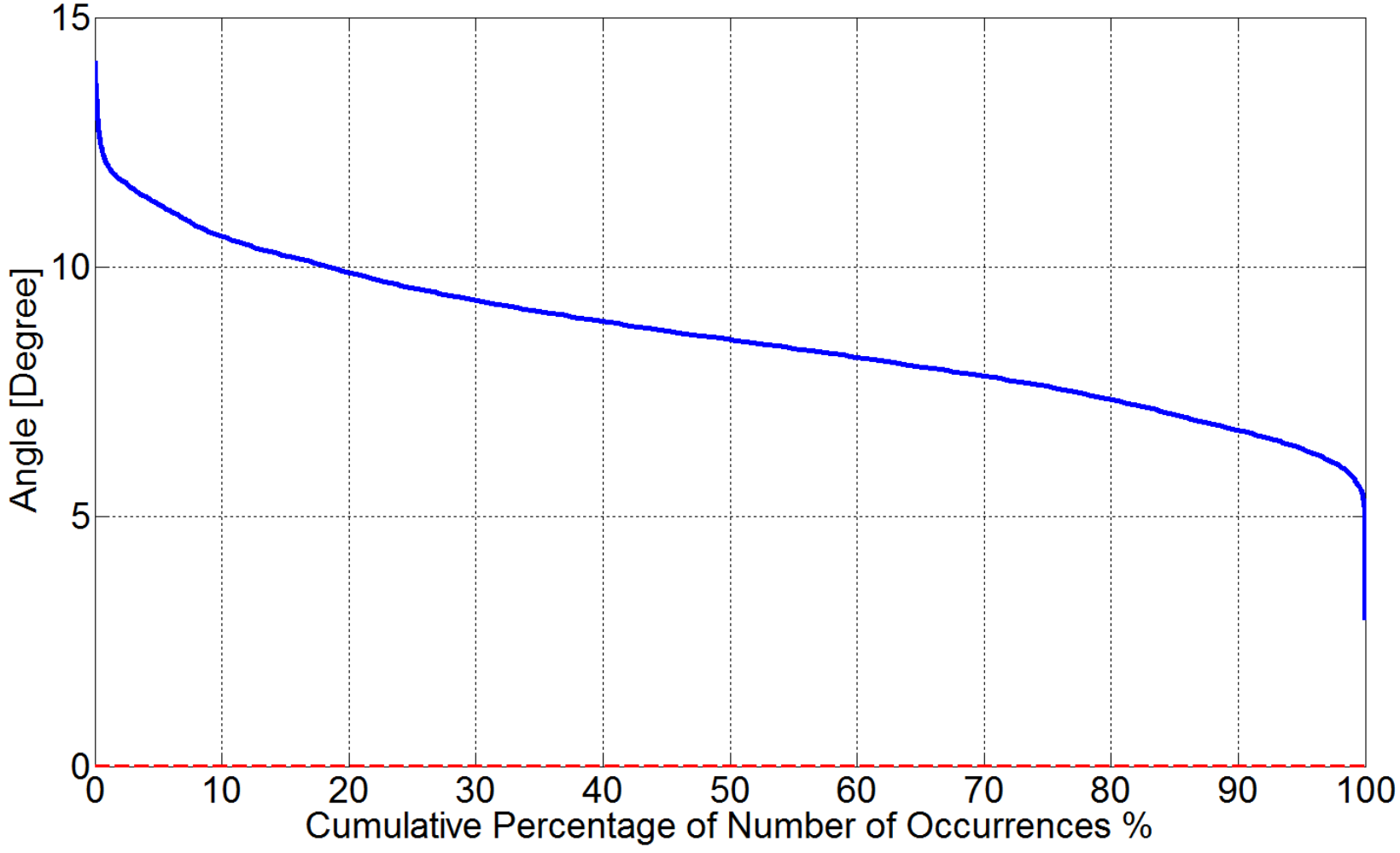
FarWest 7-West 14



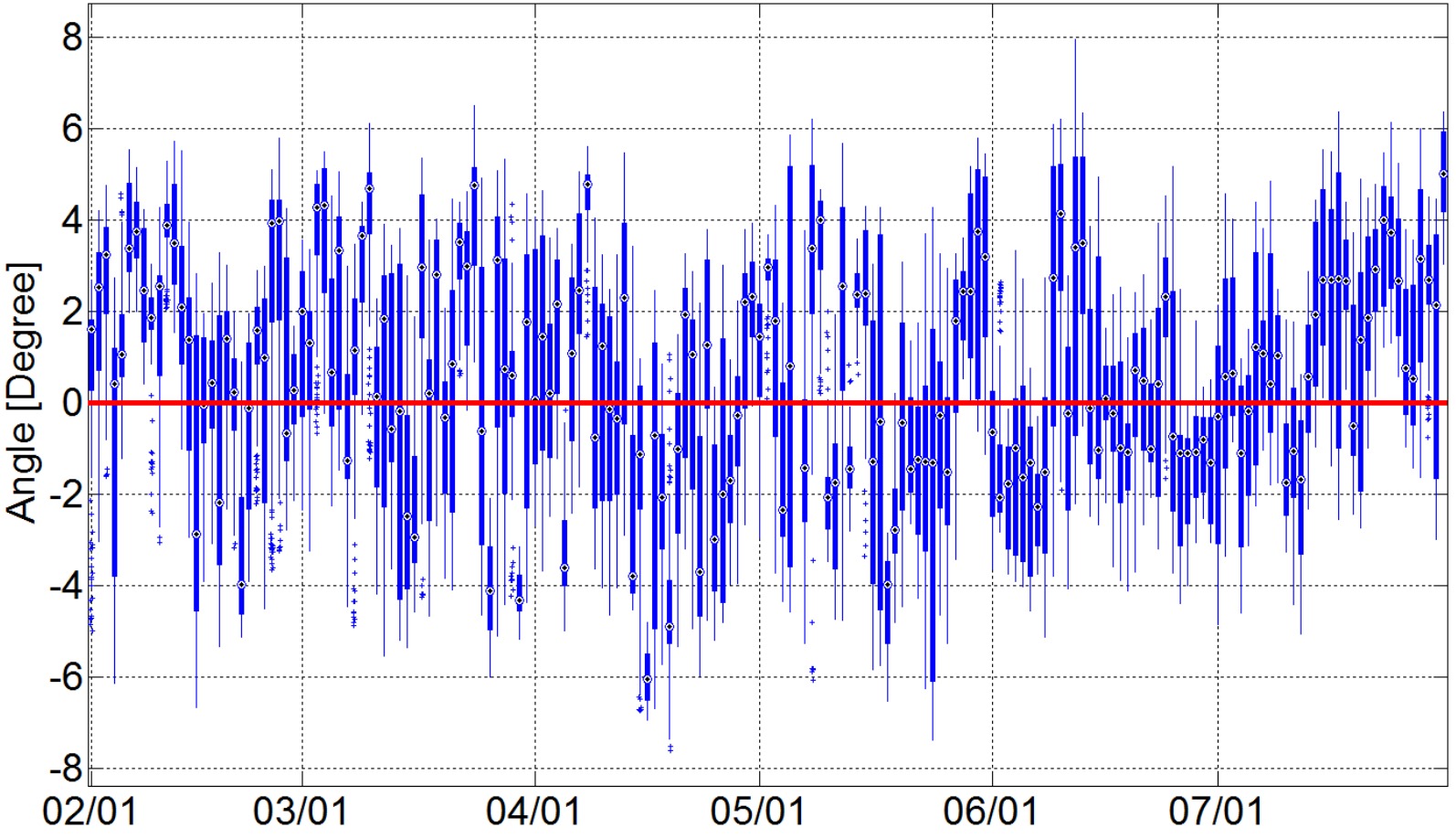
FarWest 7-FarWest 8



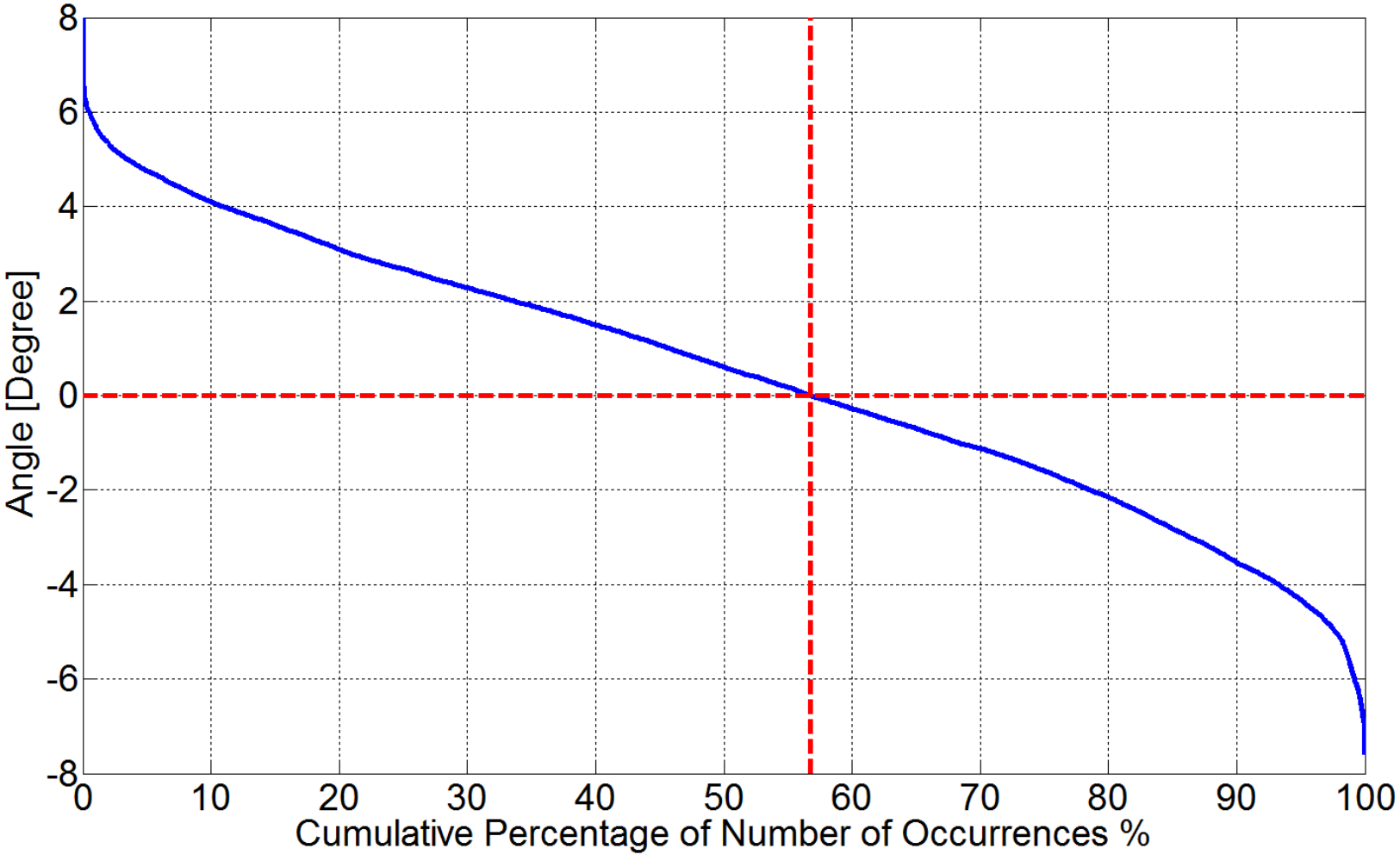
FarWest 7-FarWest 8



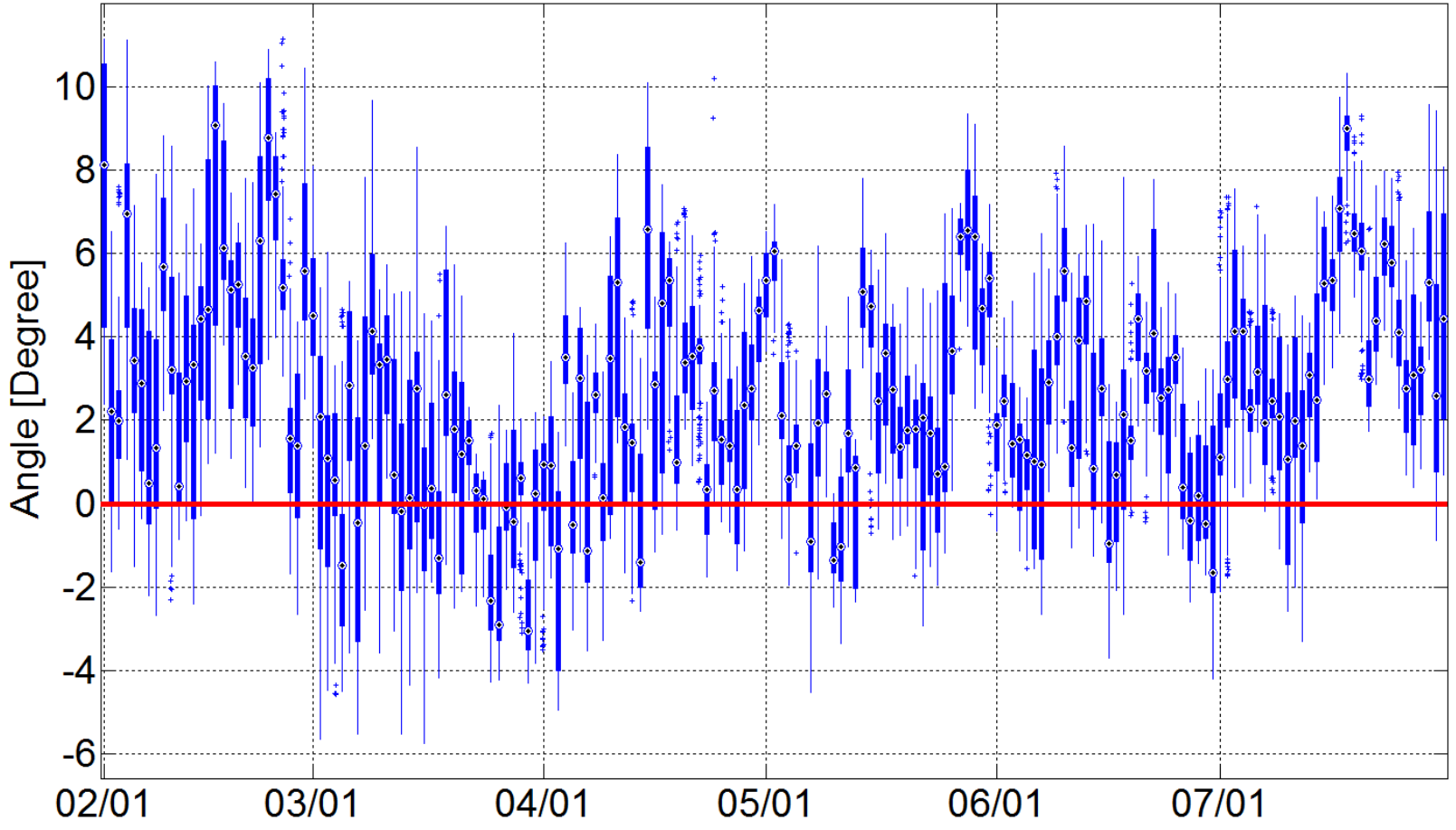
FarWest 7-FarWest 9



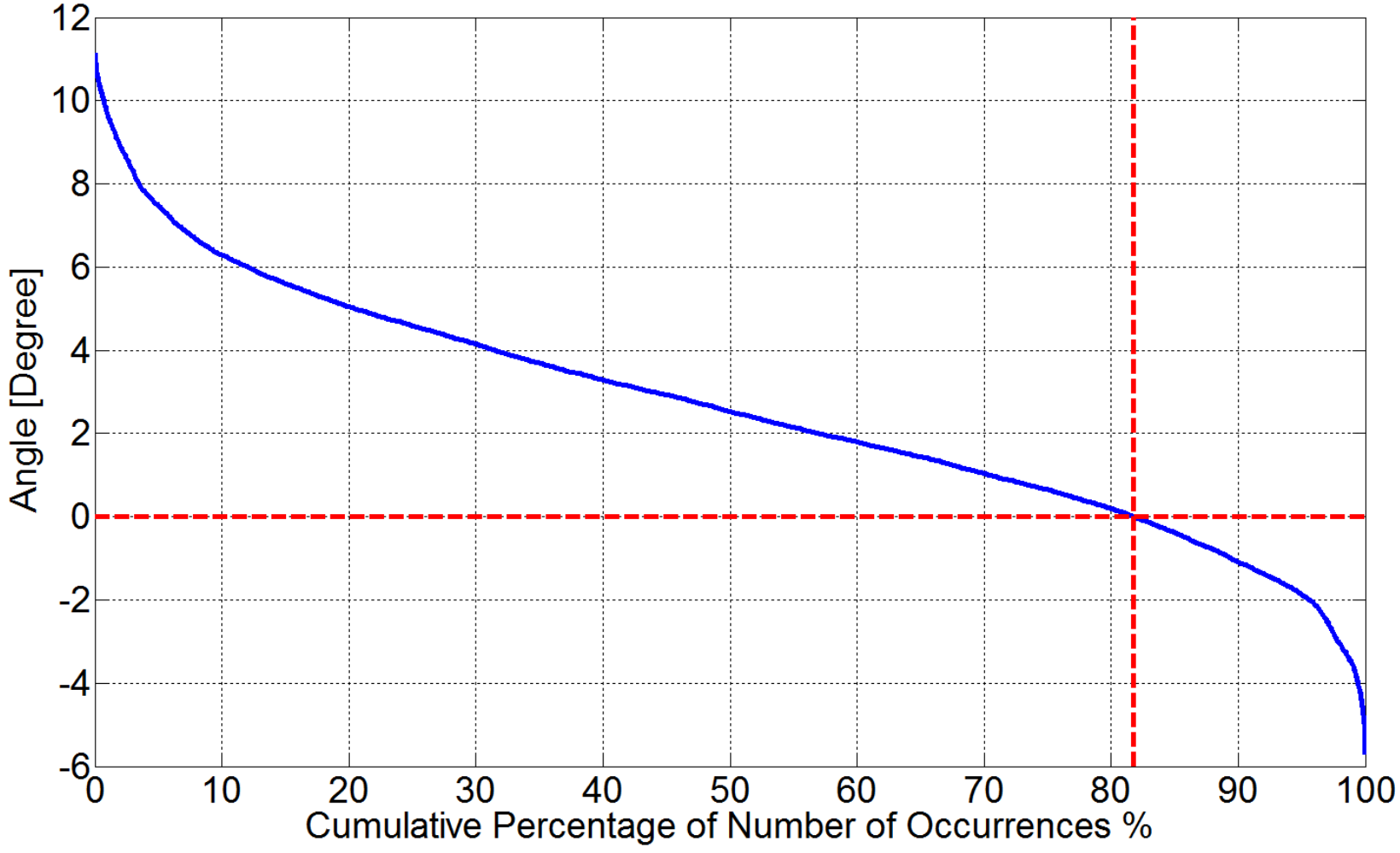
FarWest 7-FarWest 9



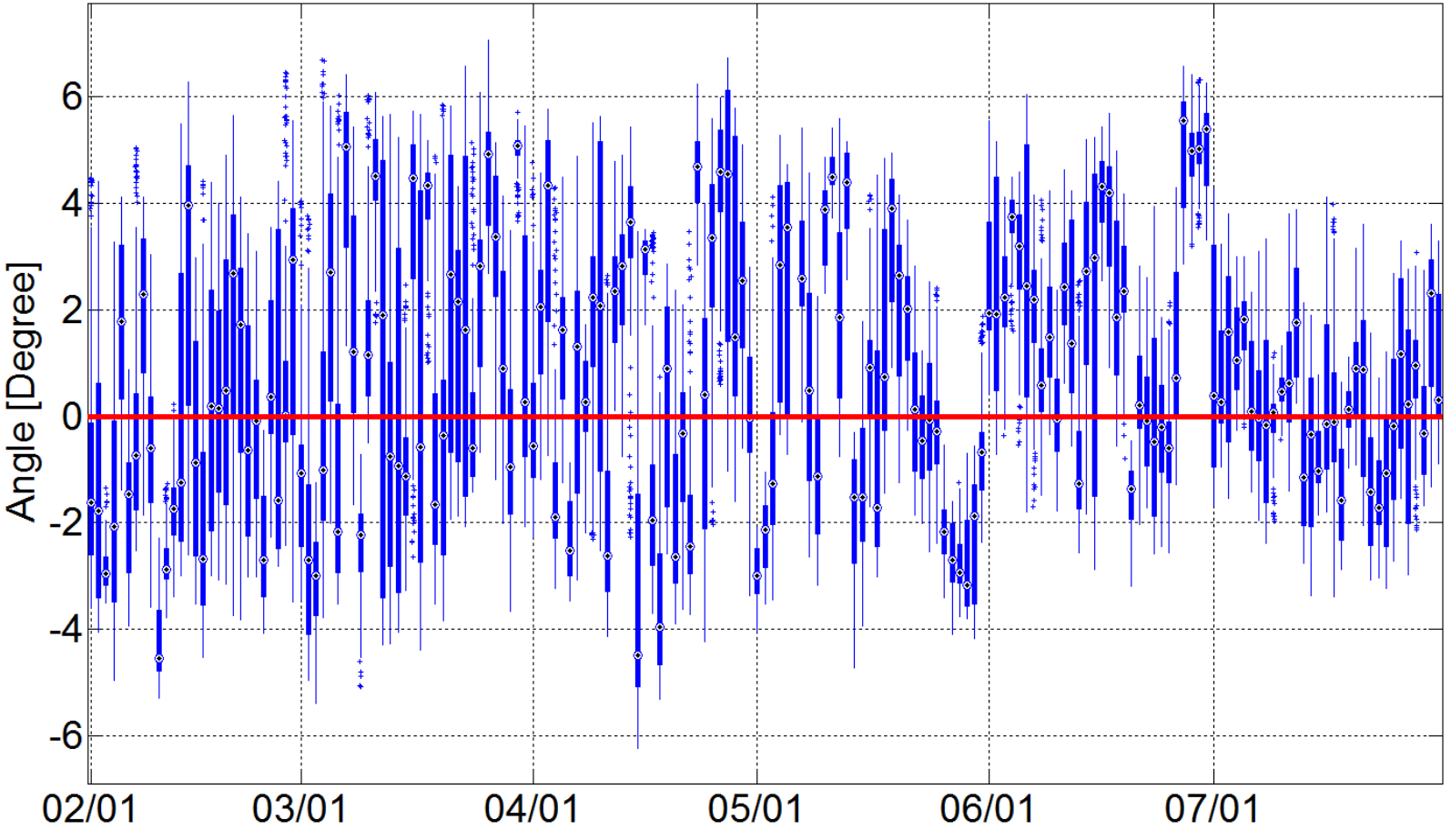
West 12-FarWest 7



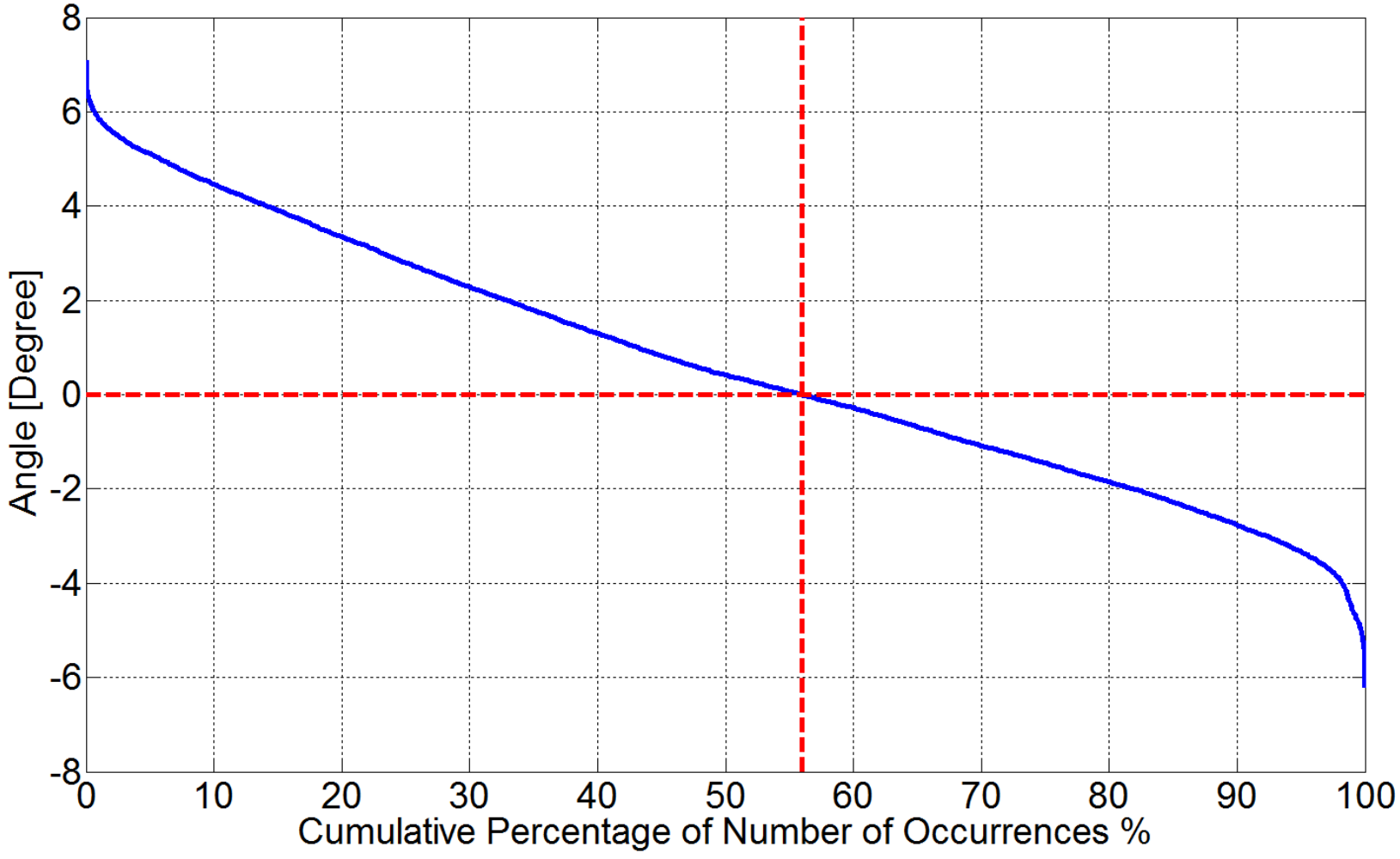
West 12-FarWest 7



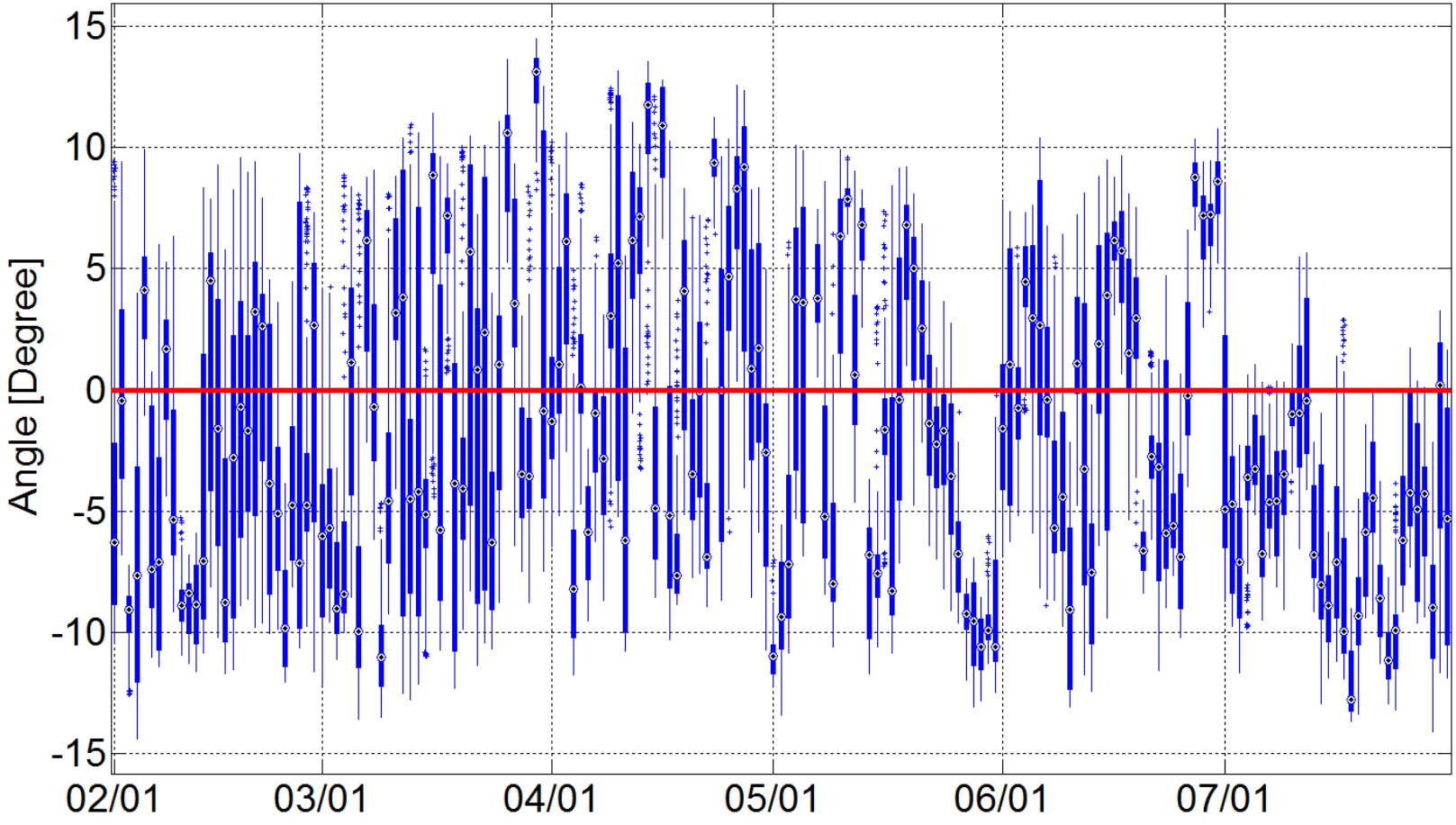
West 12-West 1



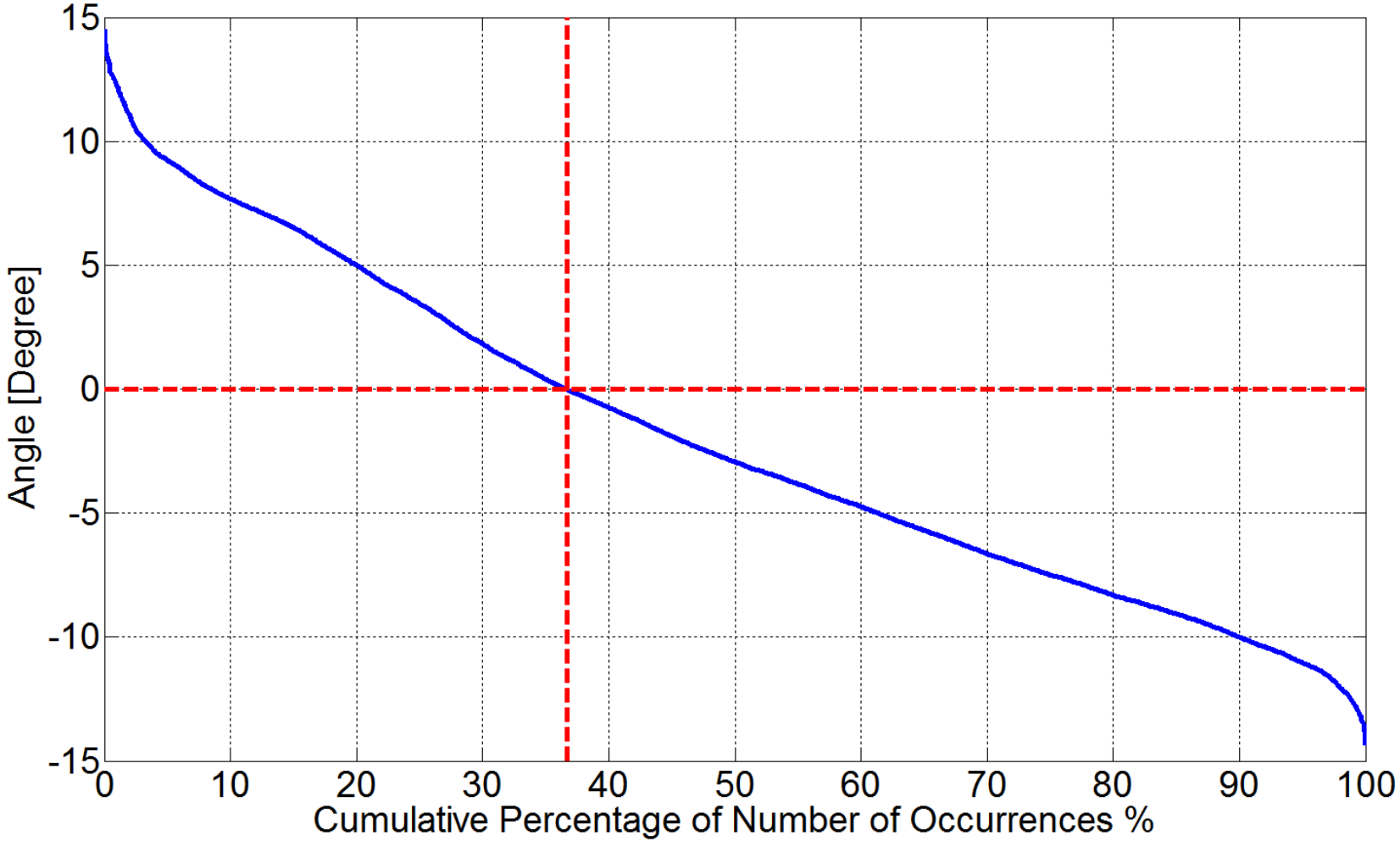
West 12-West 1



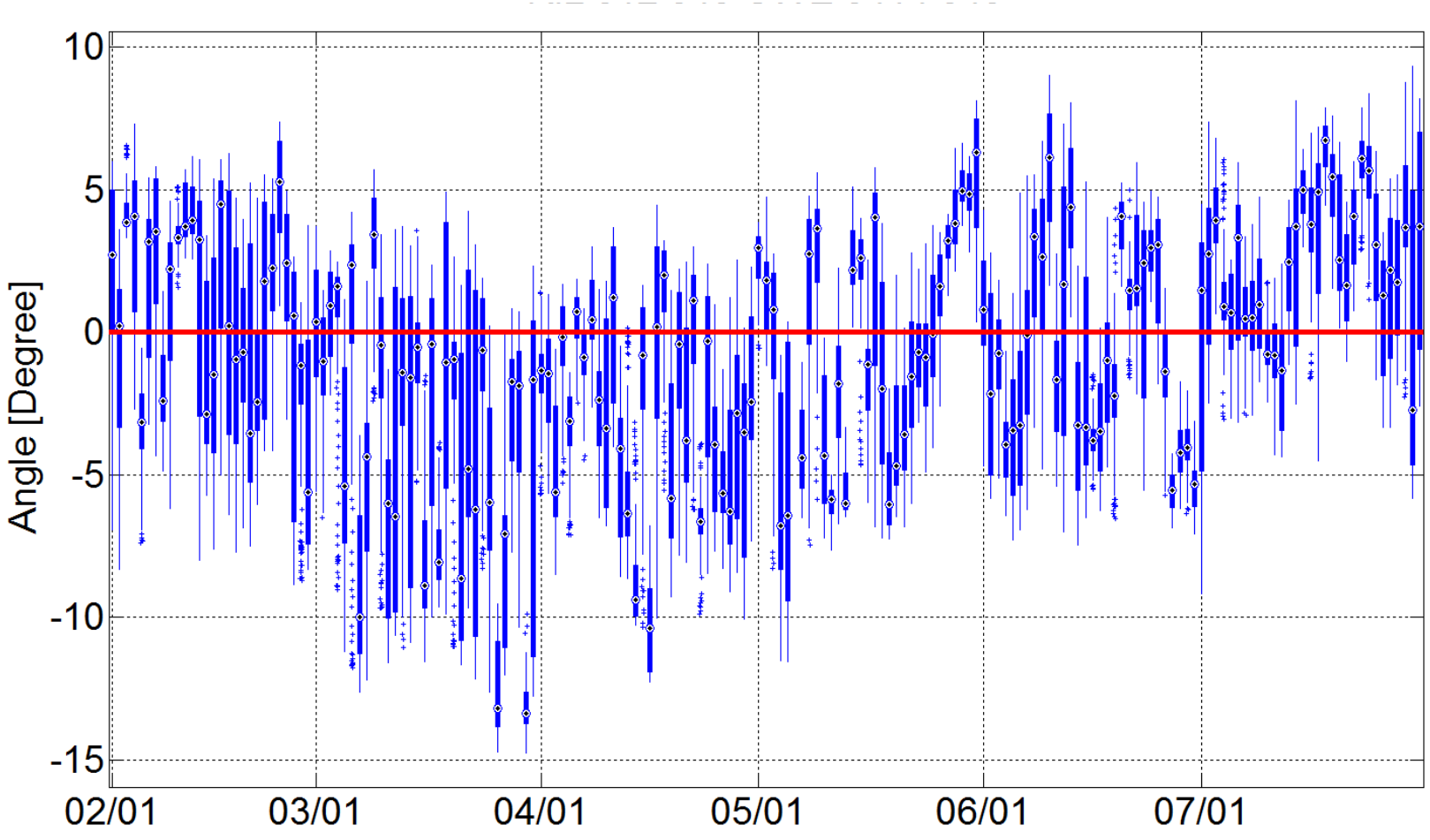
West 12-North 1



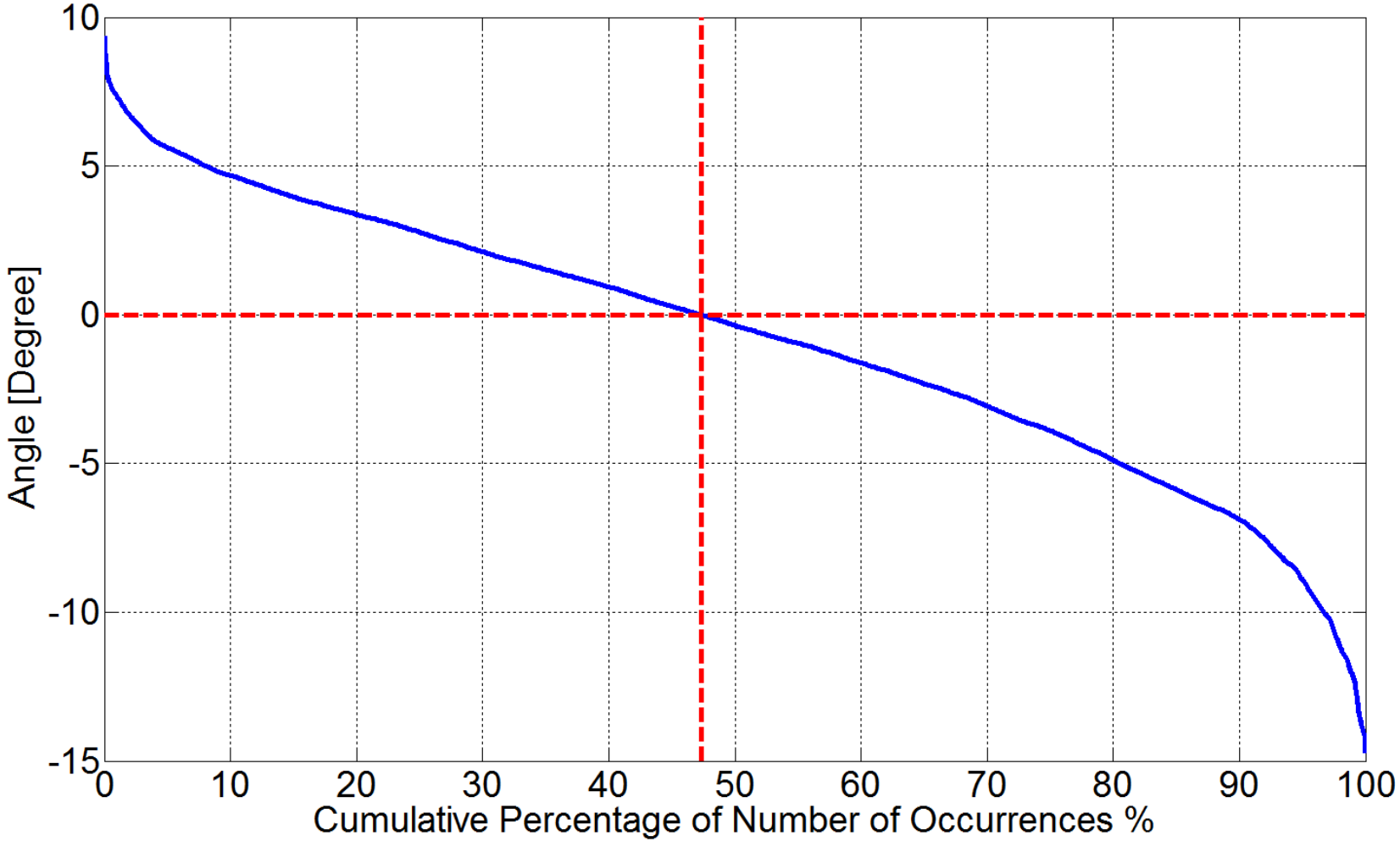
West 12-North 1



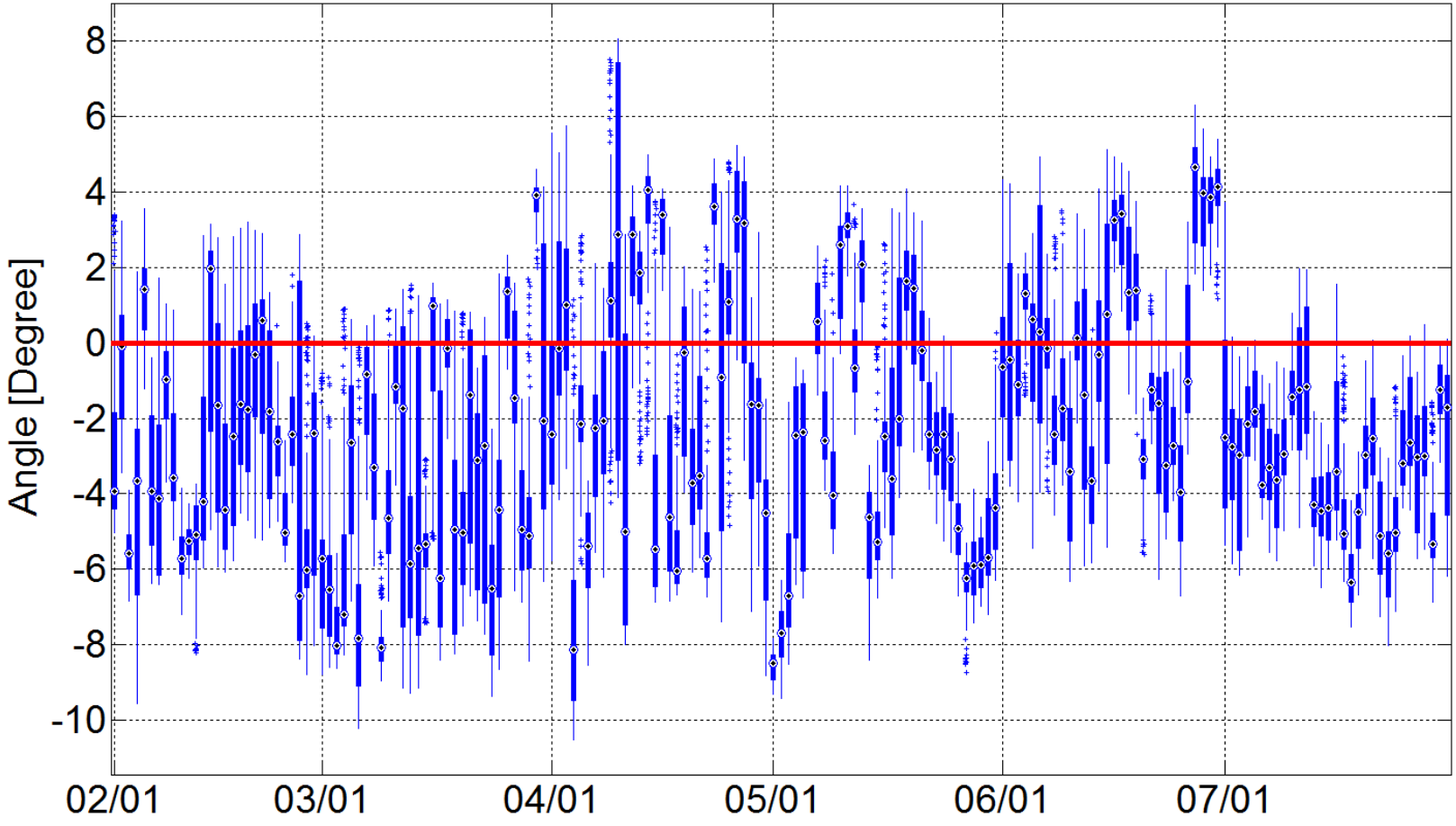
West 14-West 5



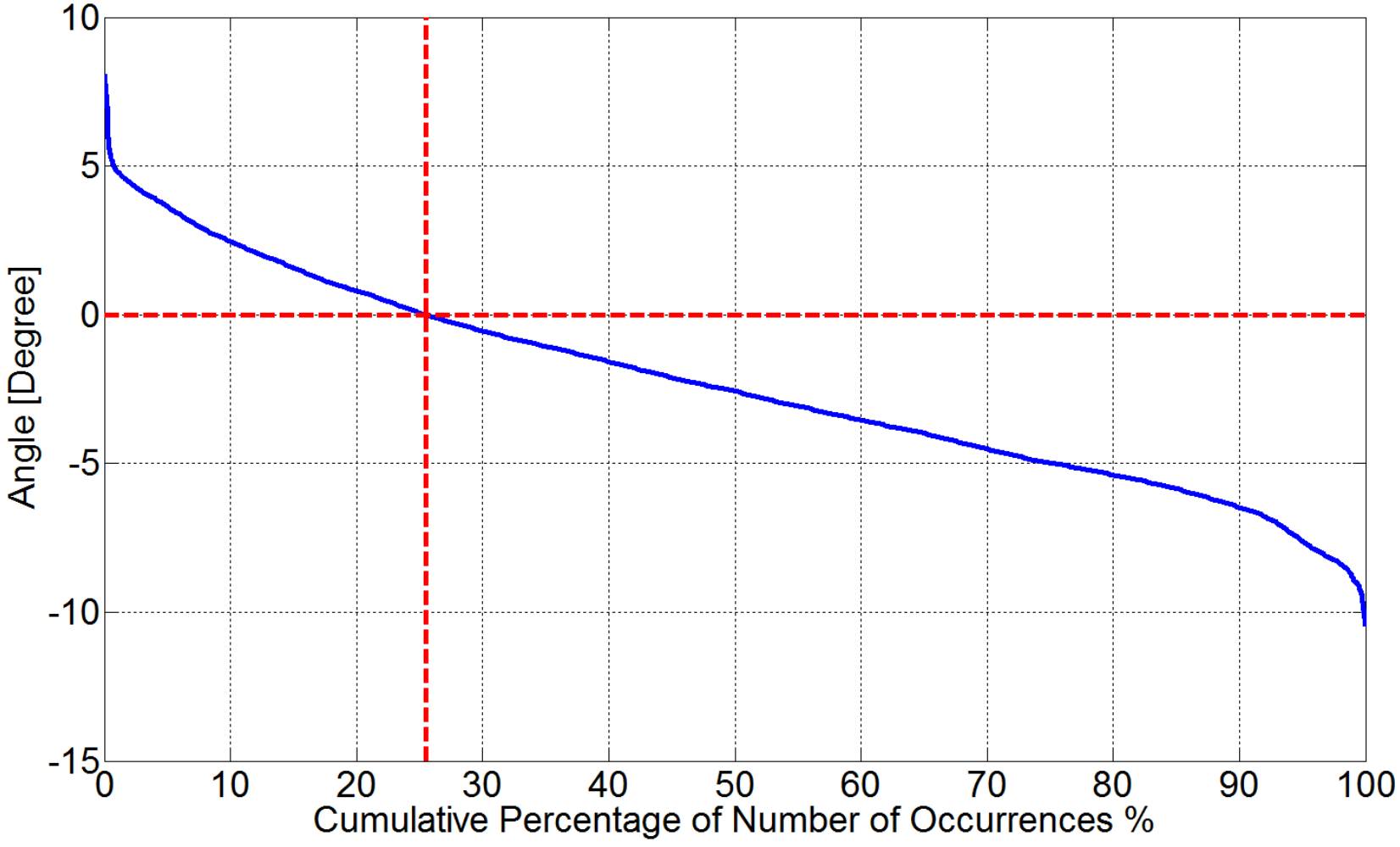
West 14-West 5



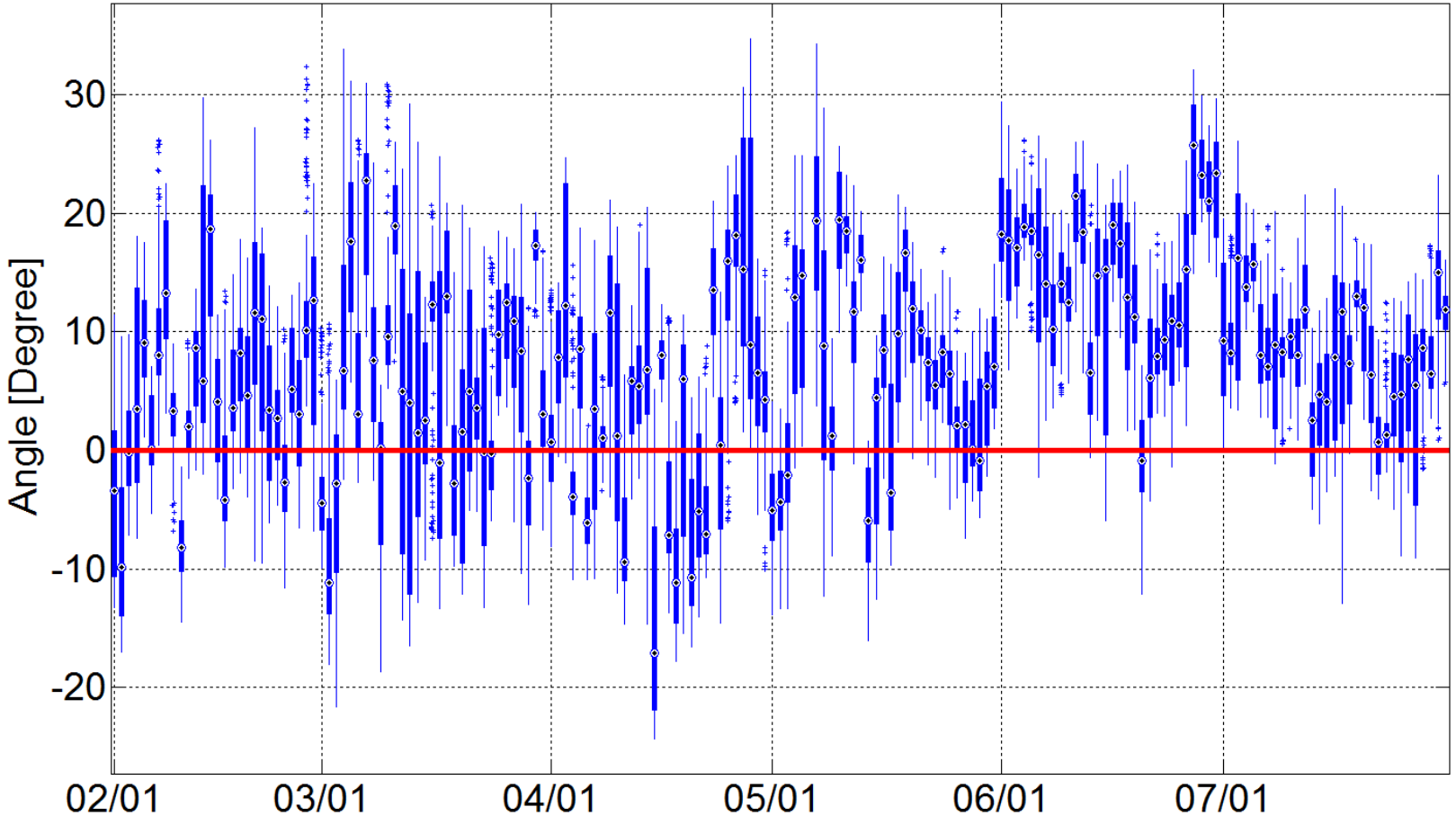
West 14-North 1



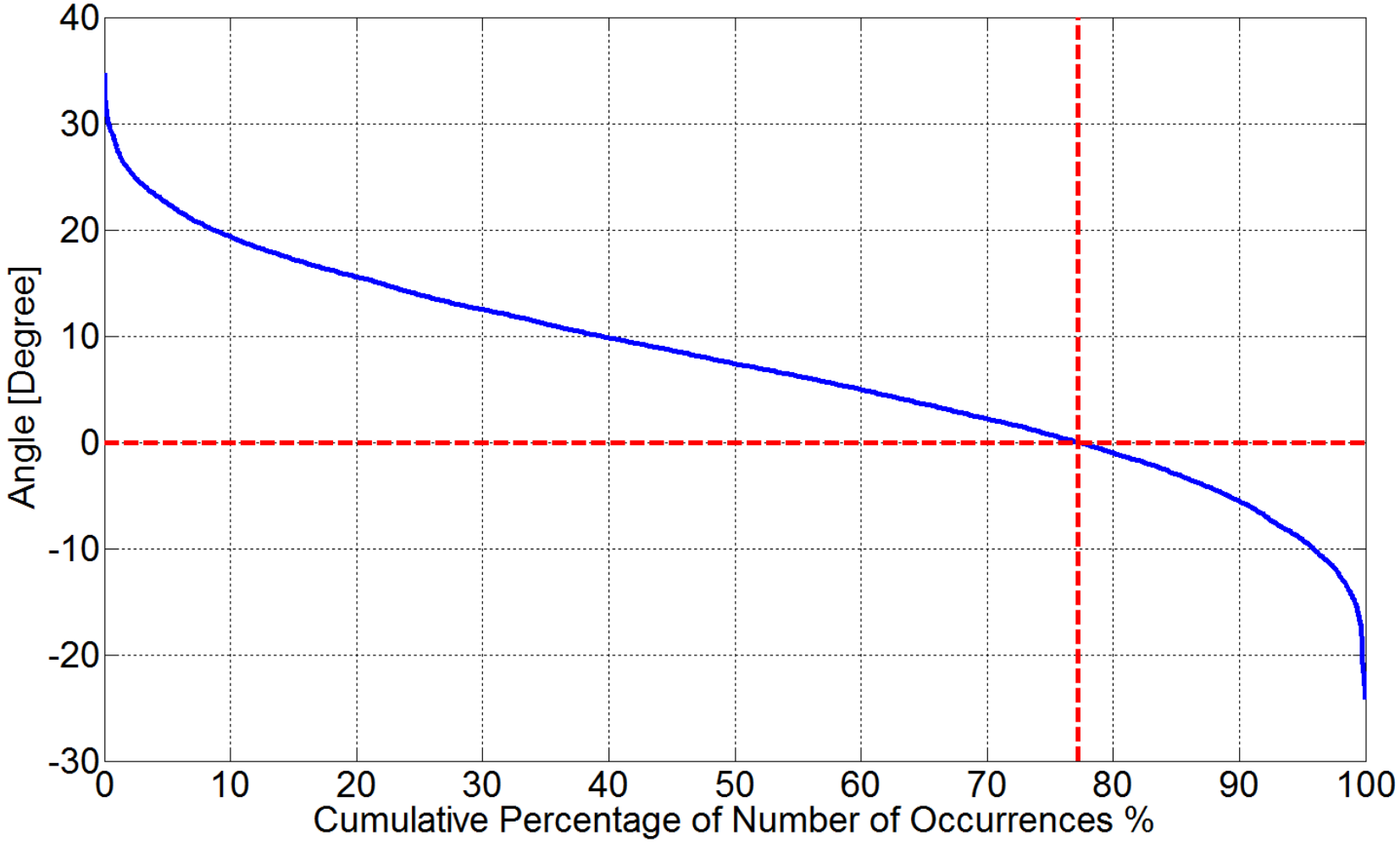
West 14-North 1



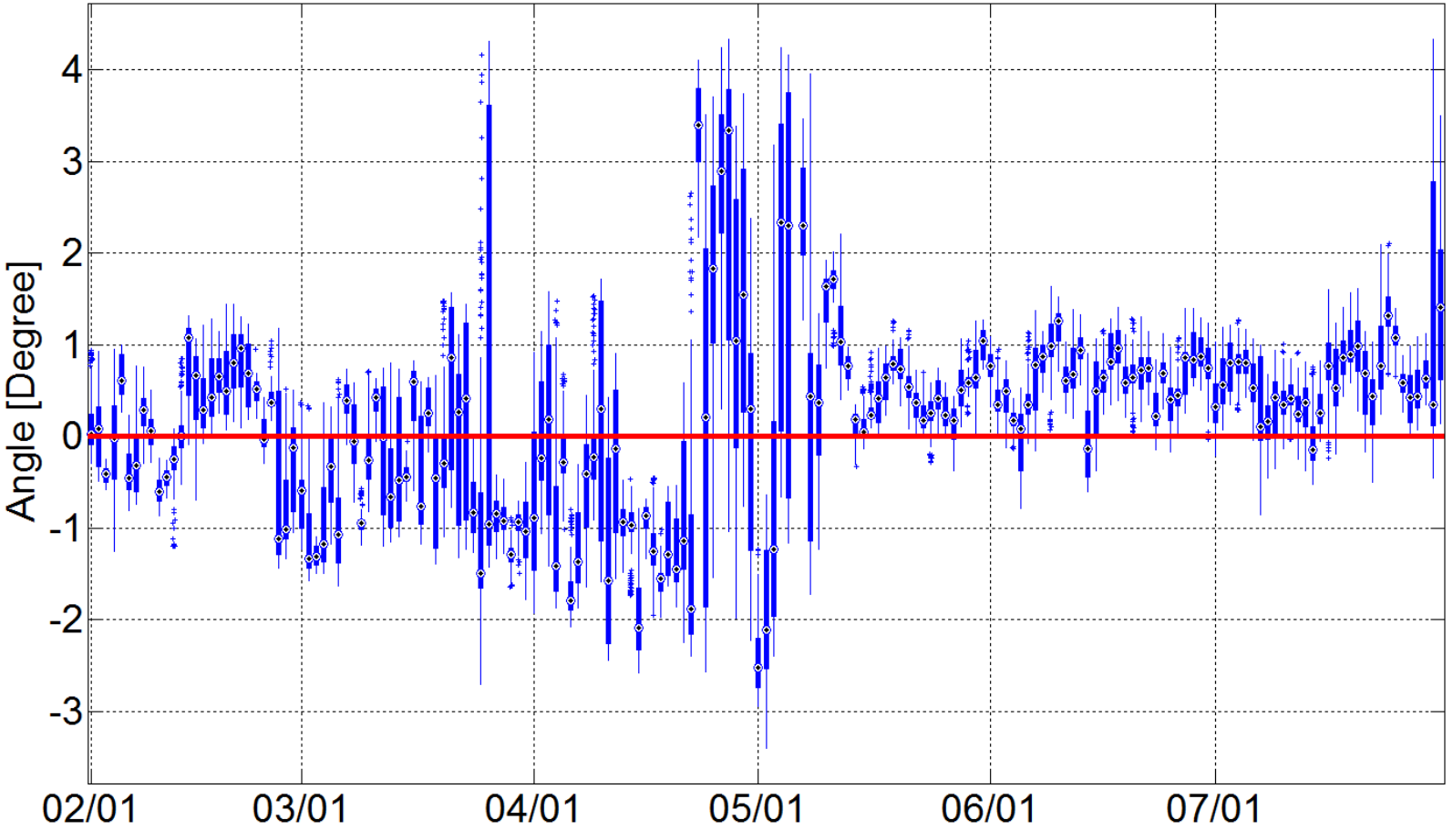
FarWest 9-West 4



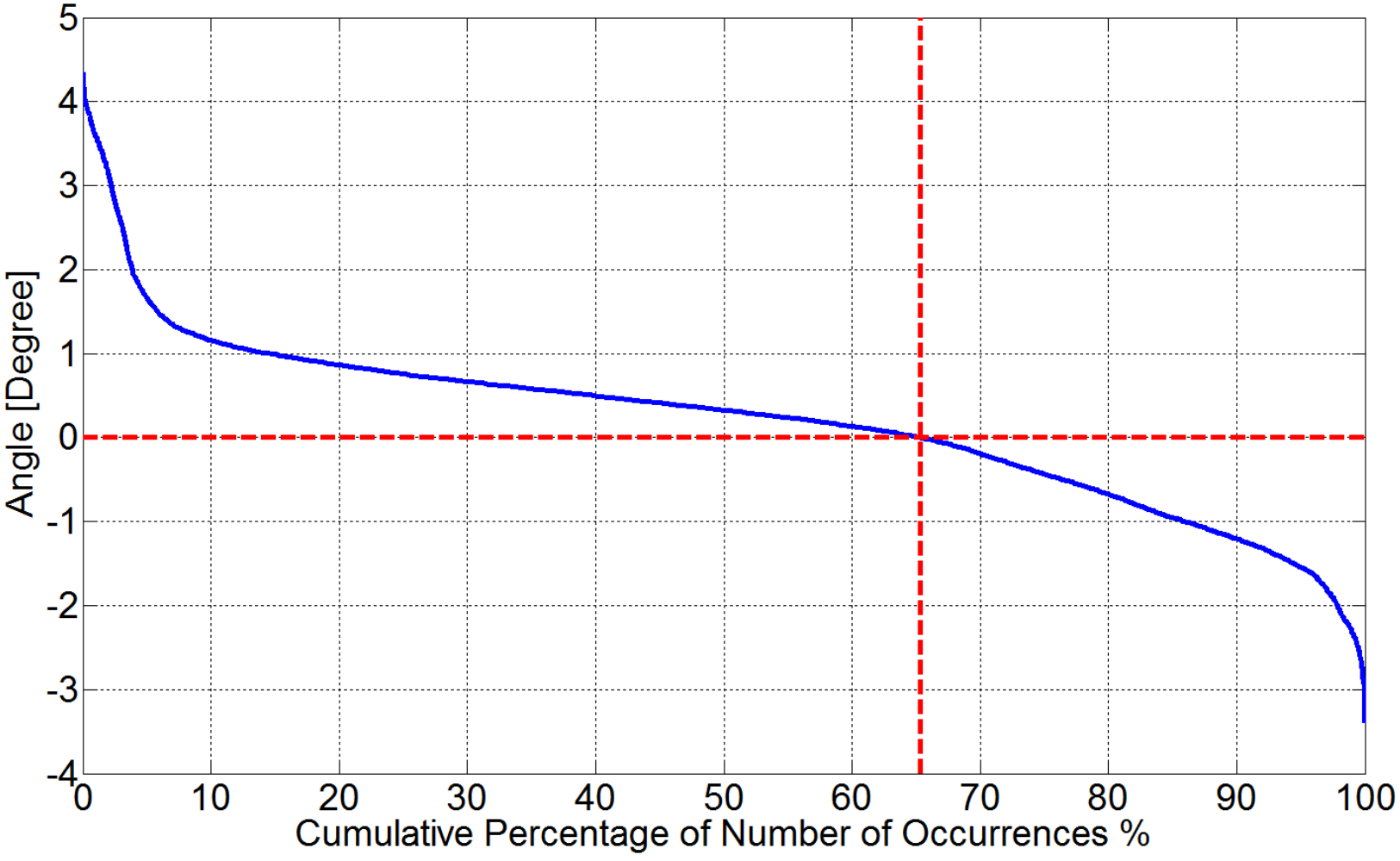
FarWest 9-West 4



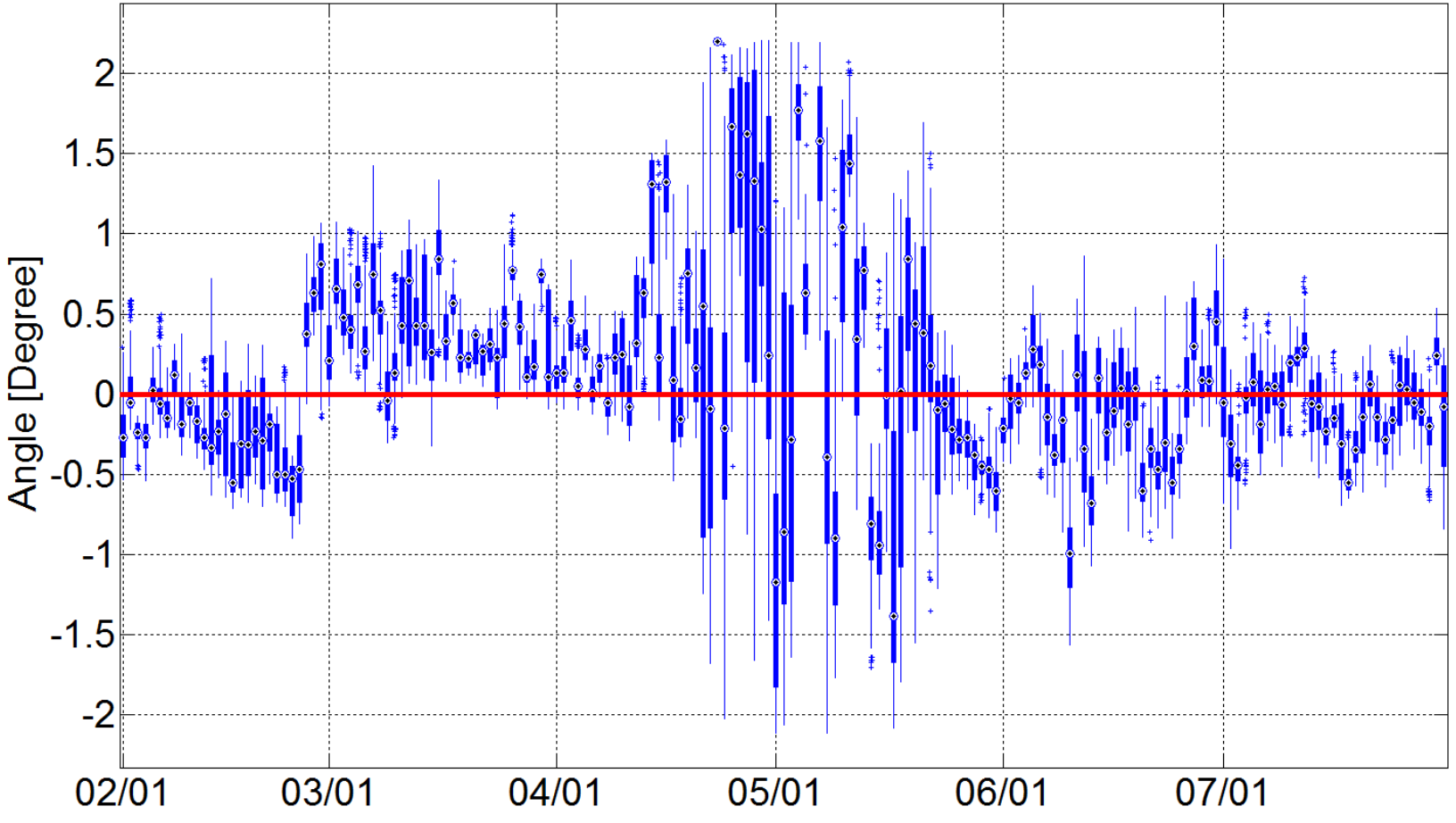
West 16-West 3



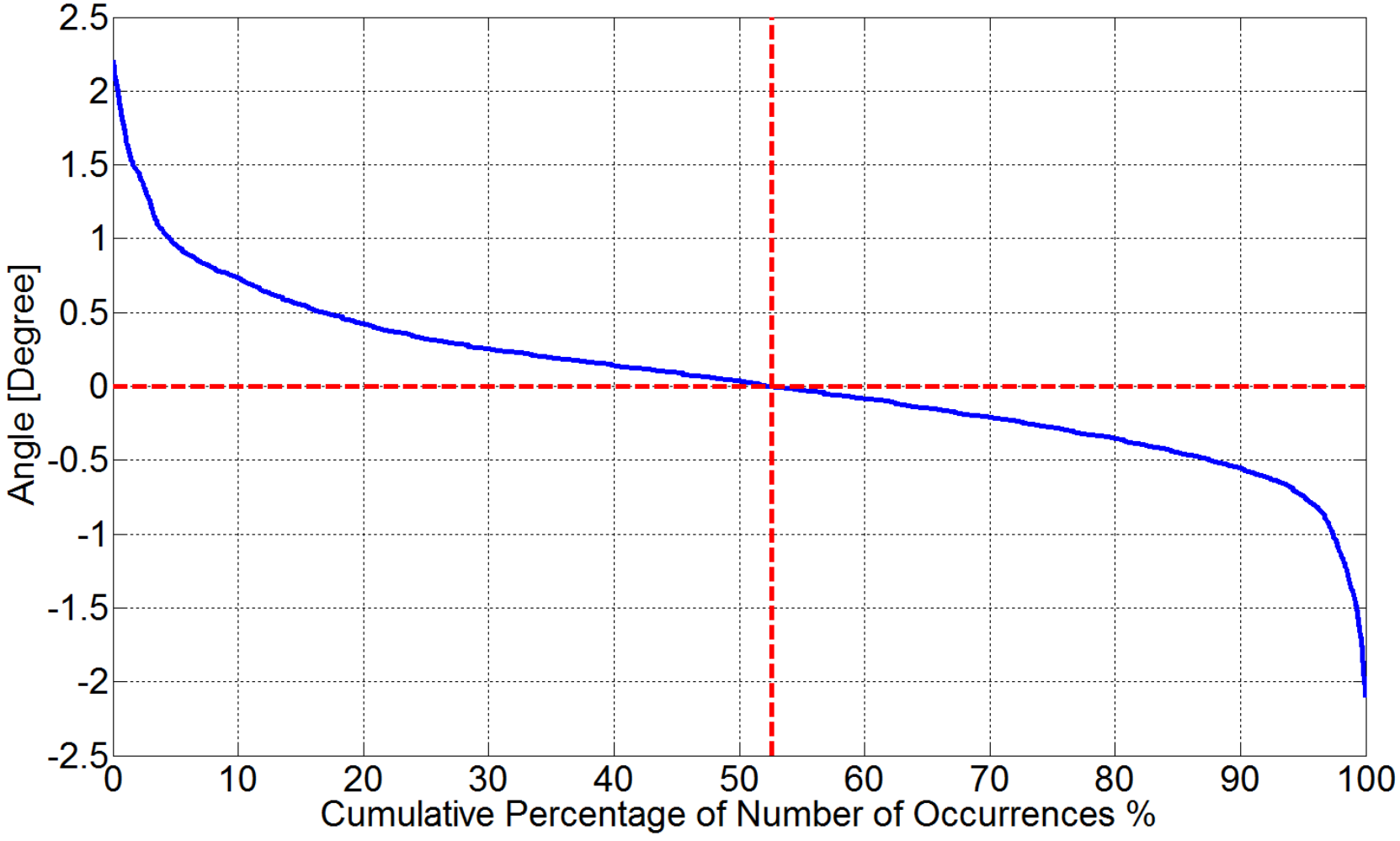
West 16-West 3



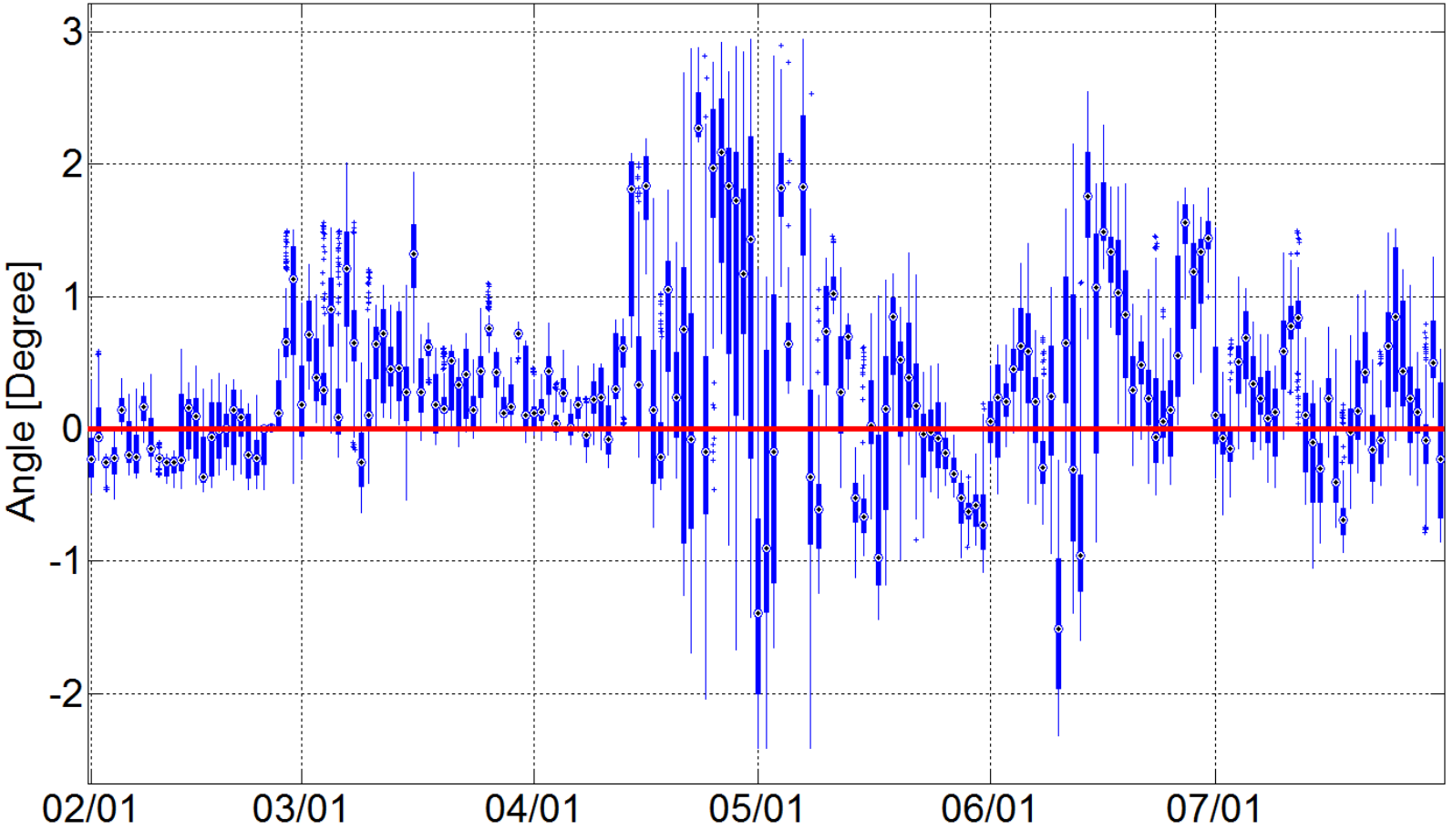
West 16-West 14



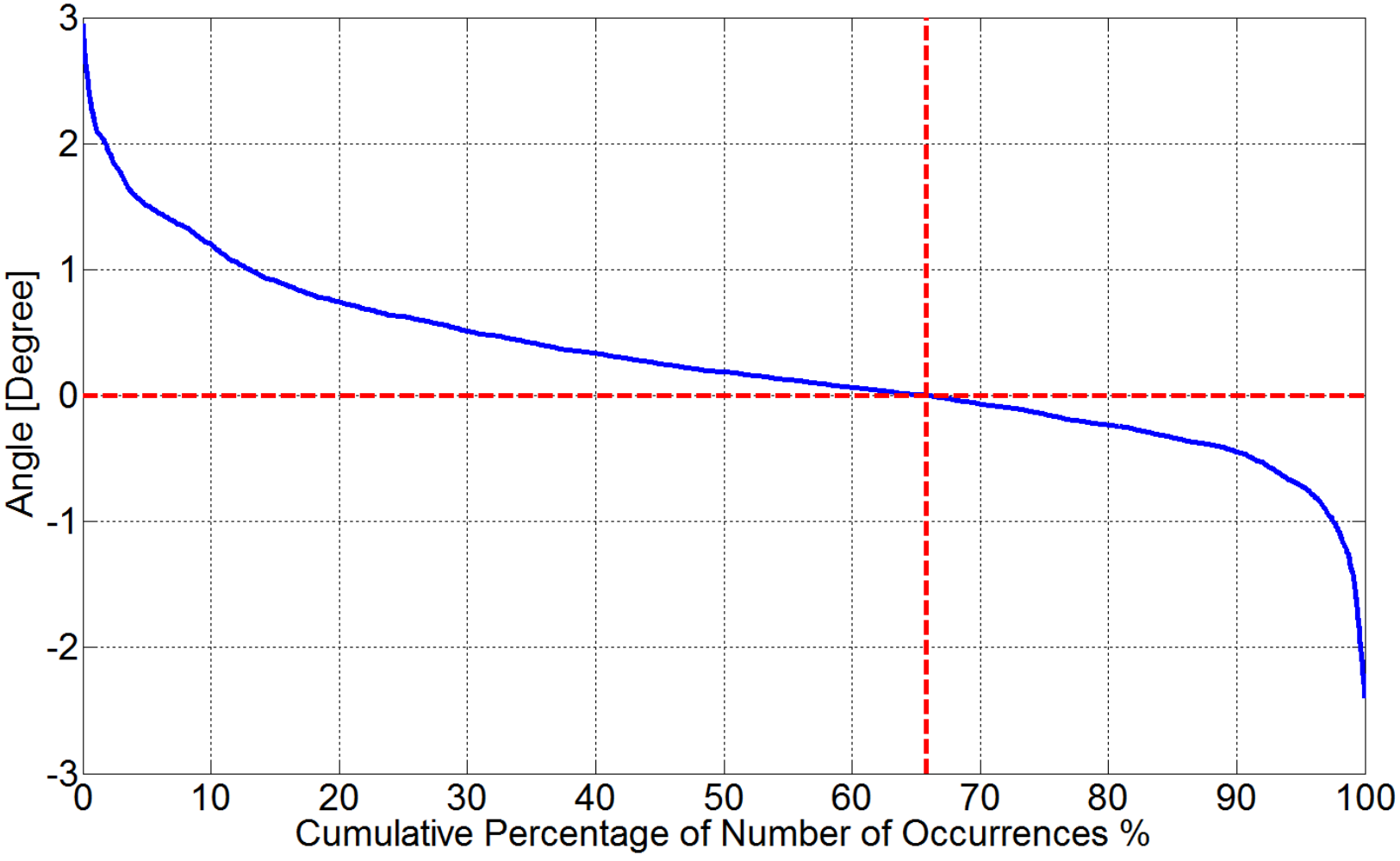
West 16-West 14



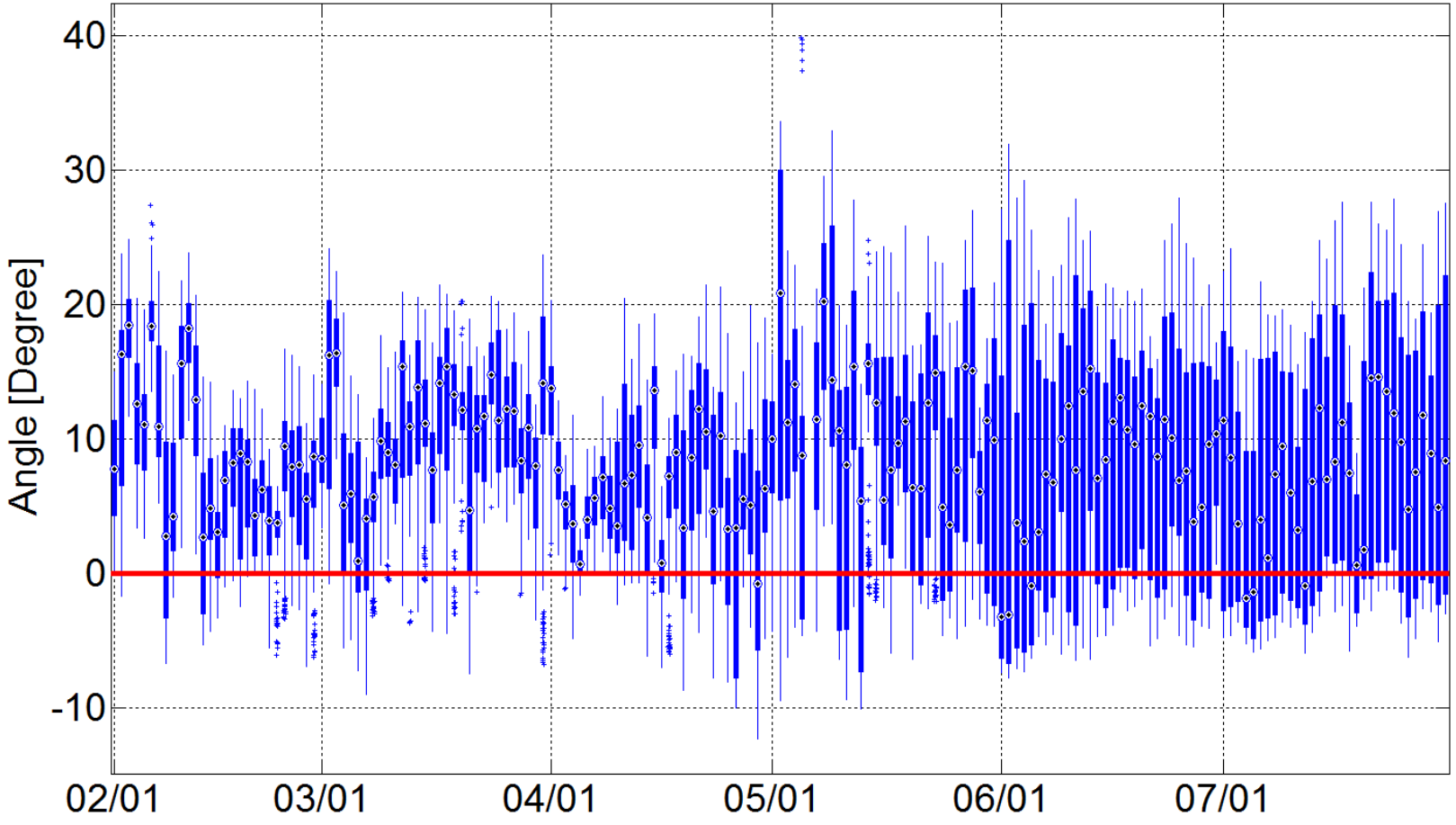
West 15-West 14



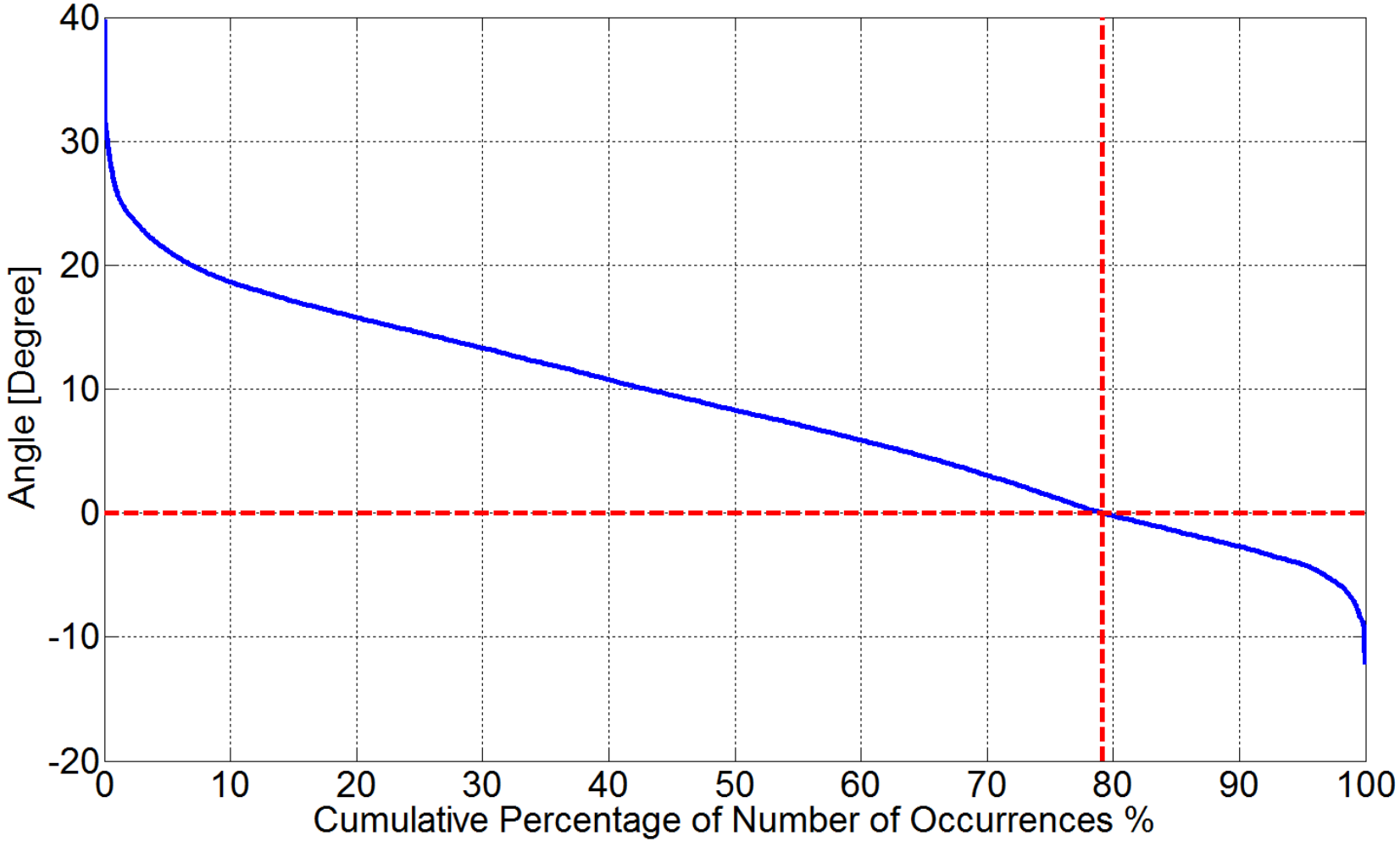
West 15-West 14



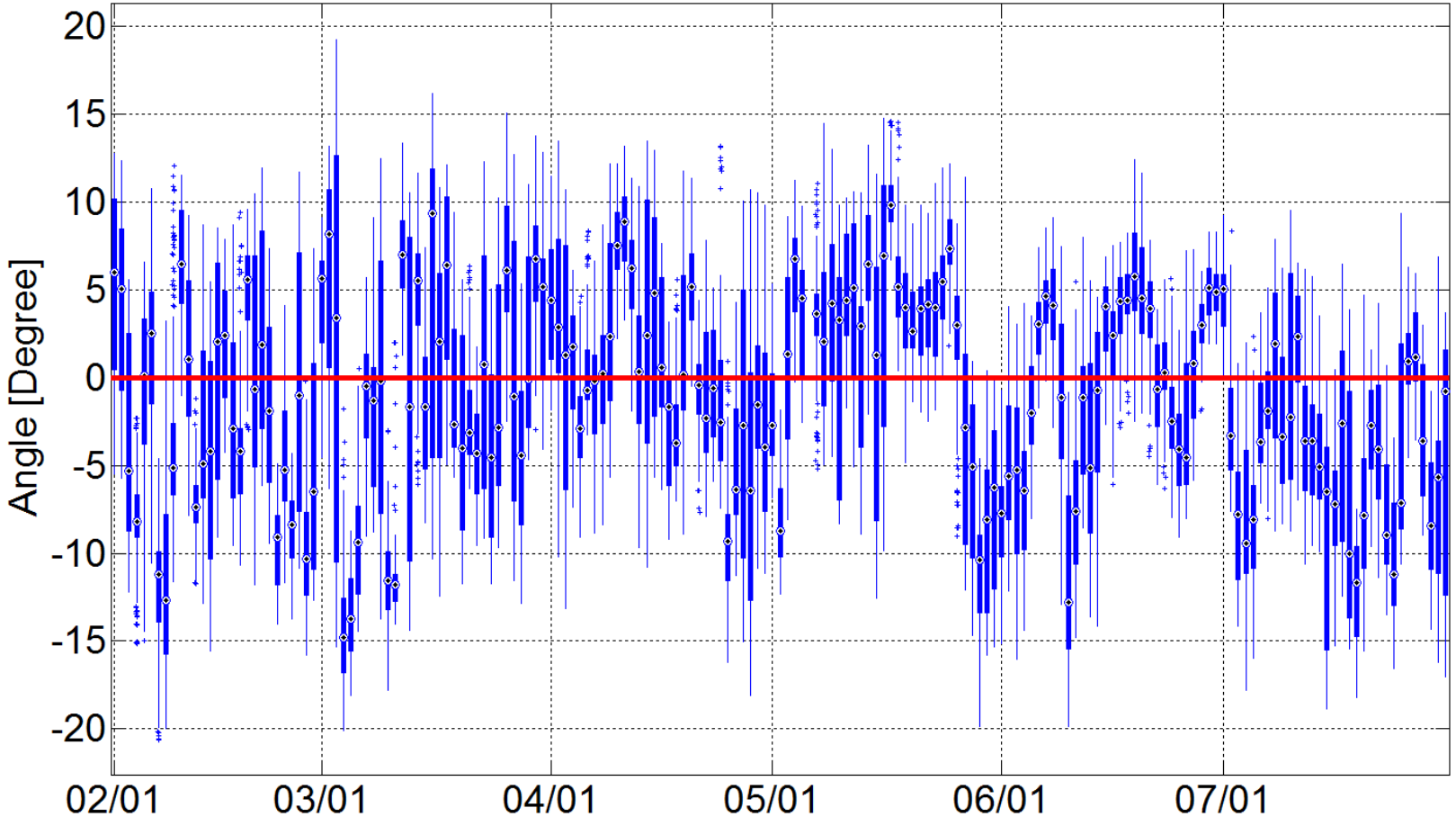
Coast 1-South 10*



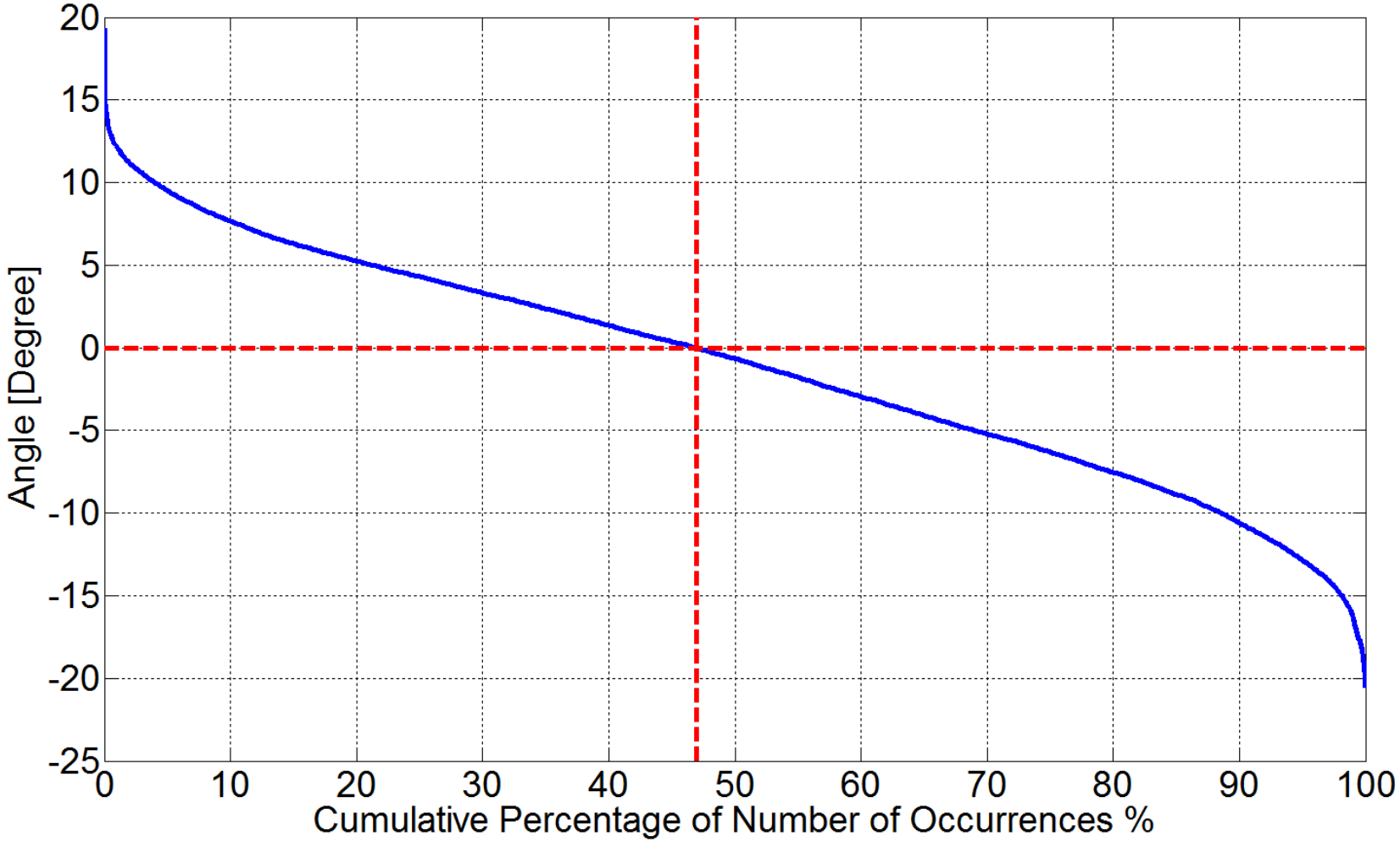
Coast 1-South 10*



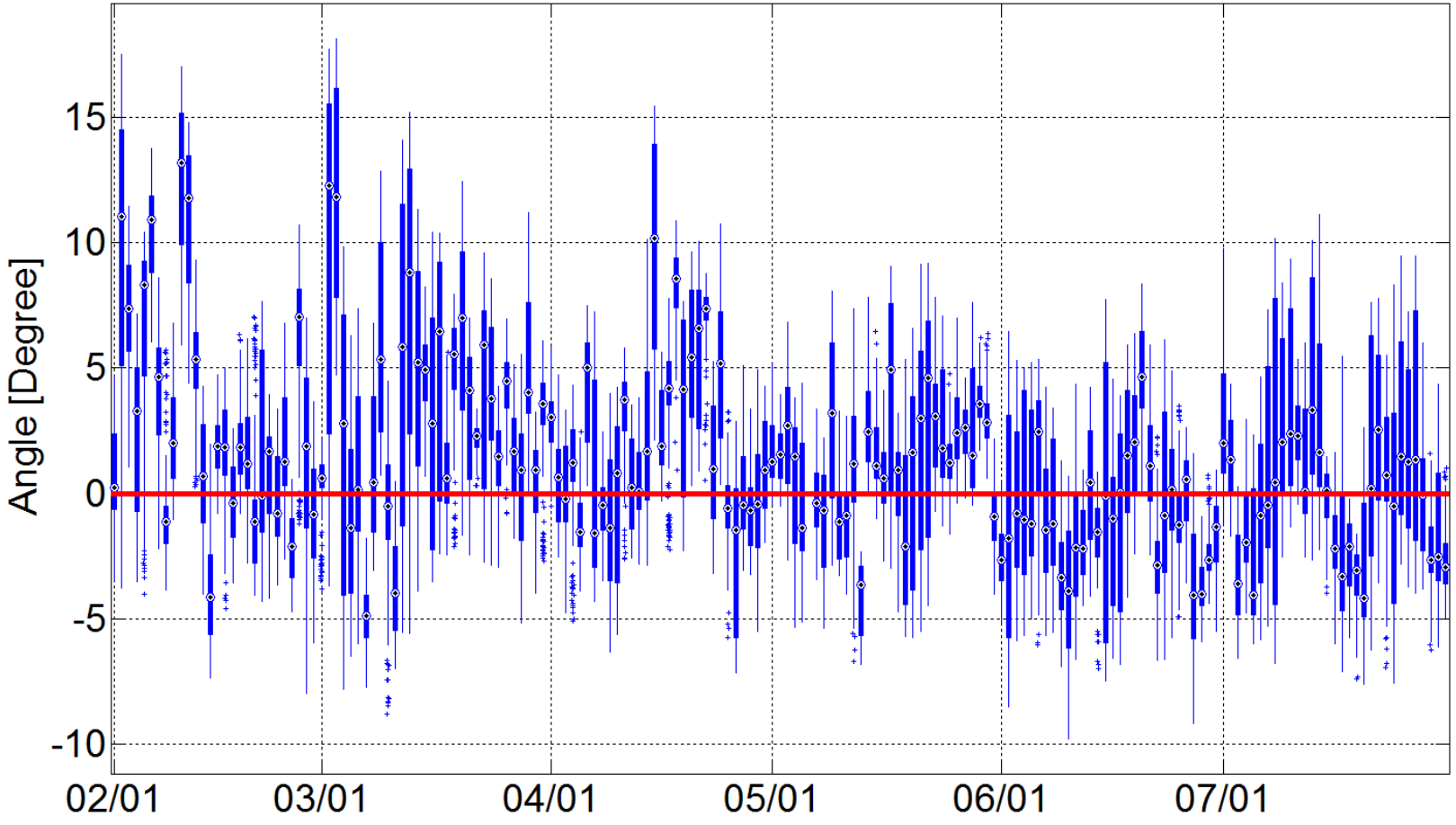
South 3*-South 11*



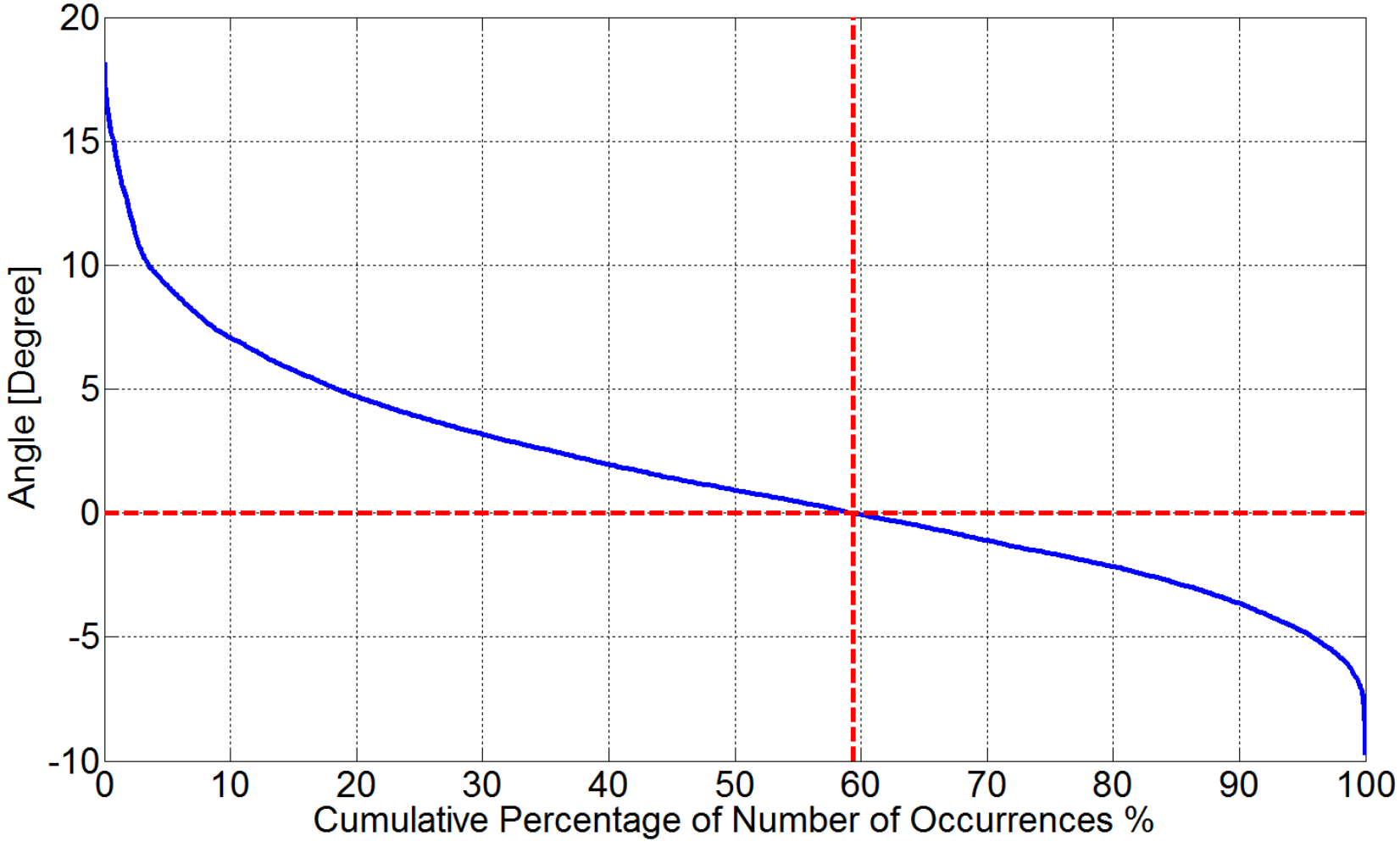
South 3*-South 11*



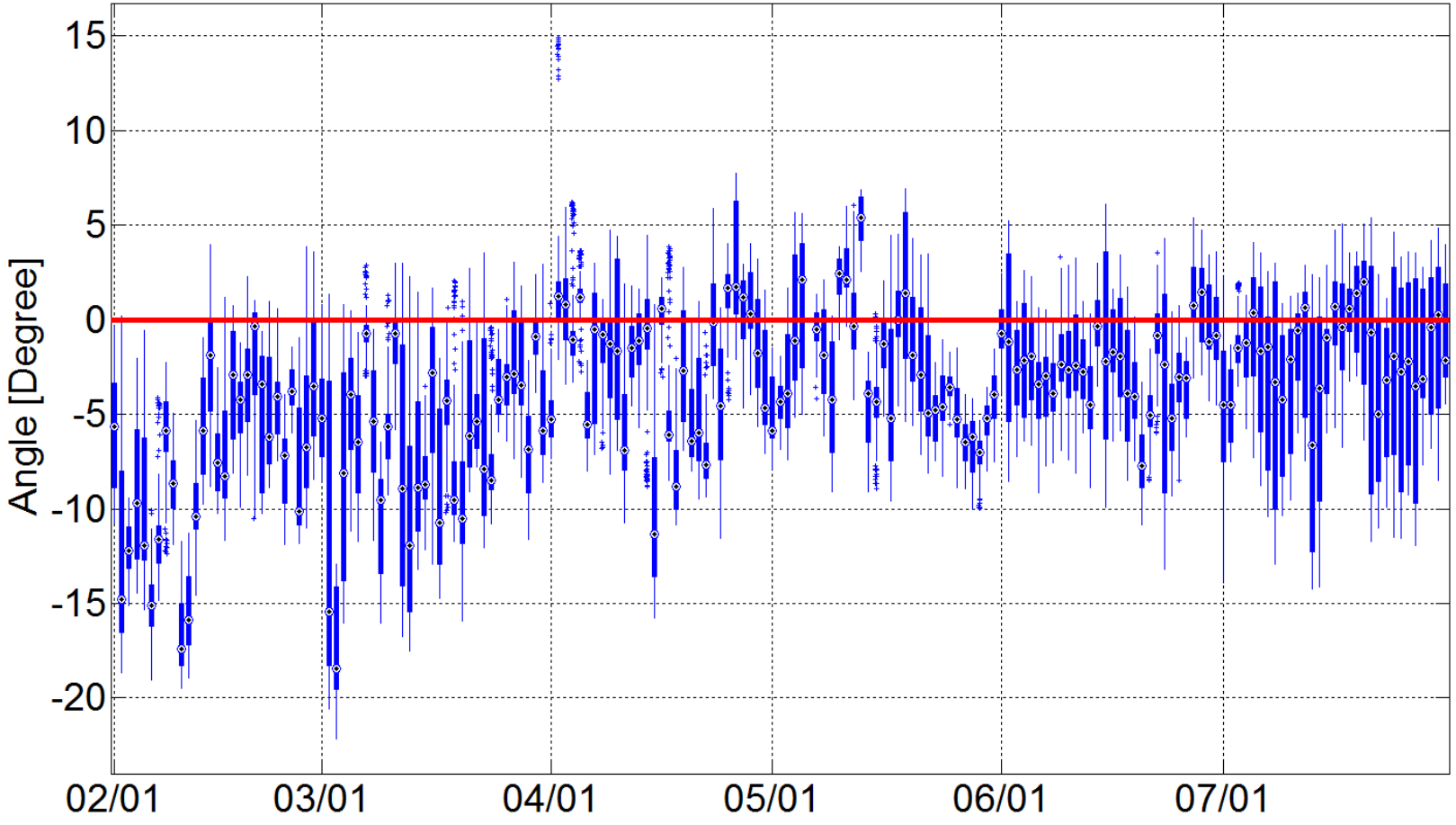
South 11*-North 7



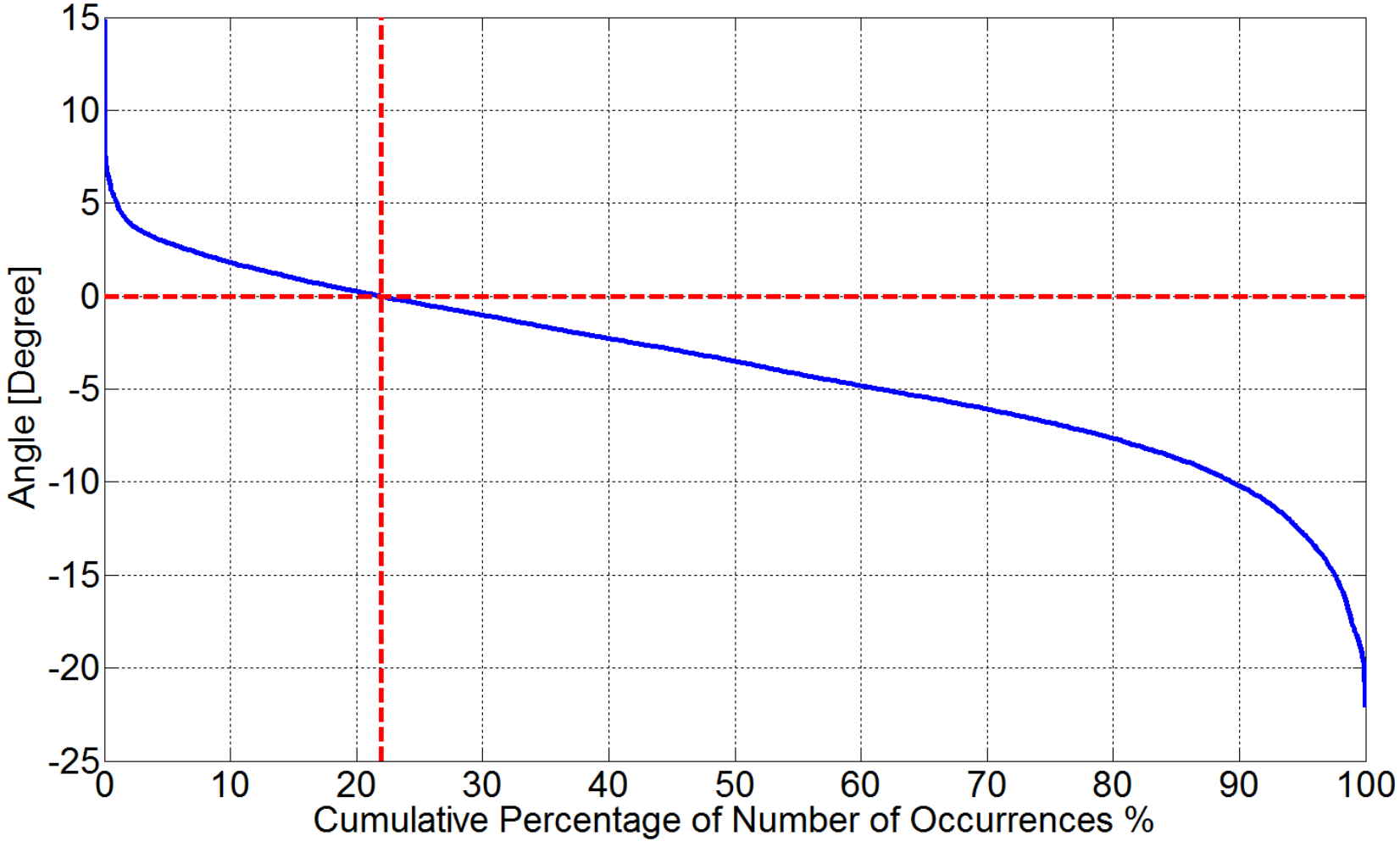
South 11*-North 7



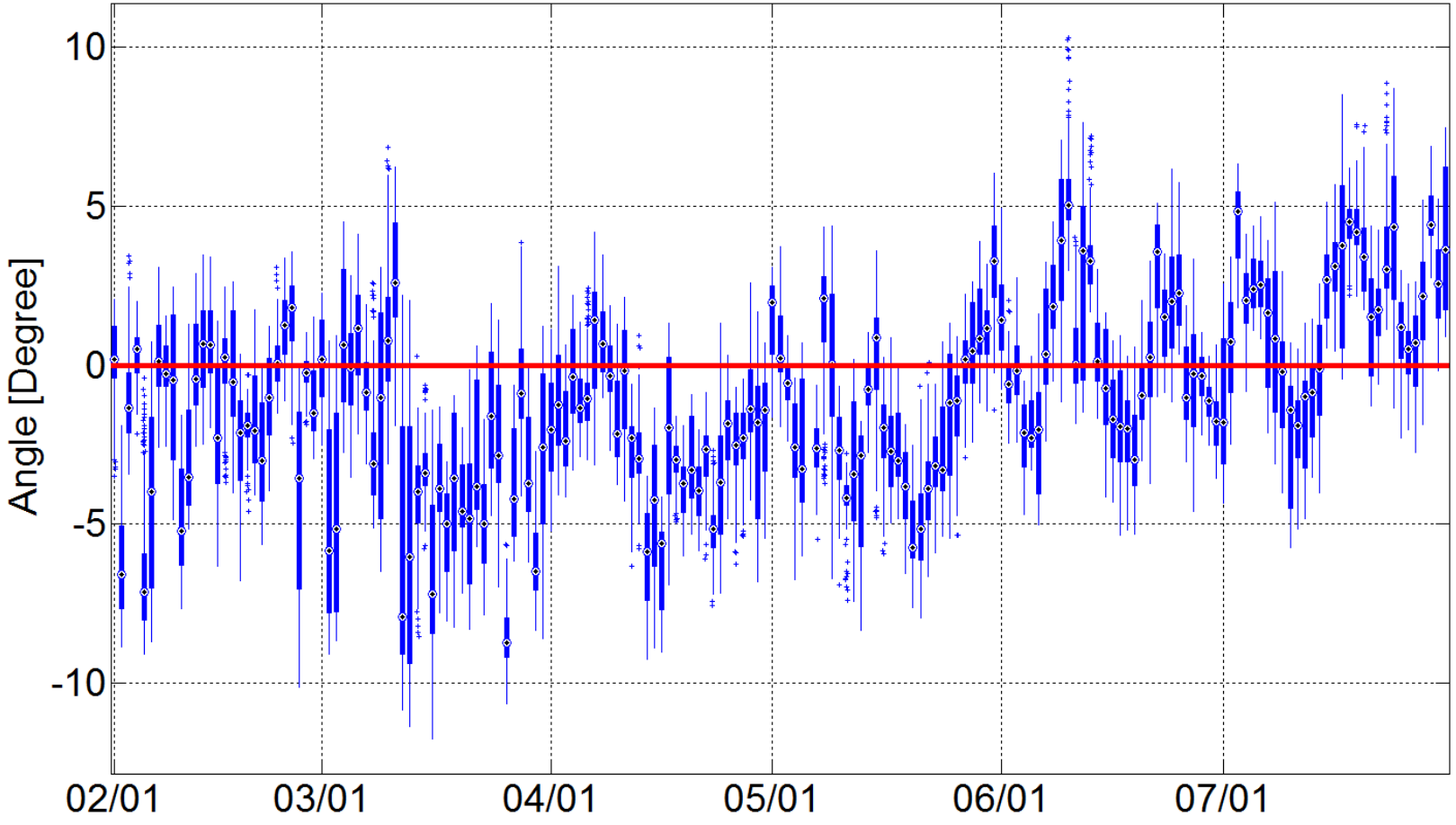
North 7-South 7*



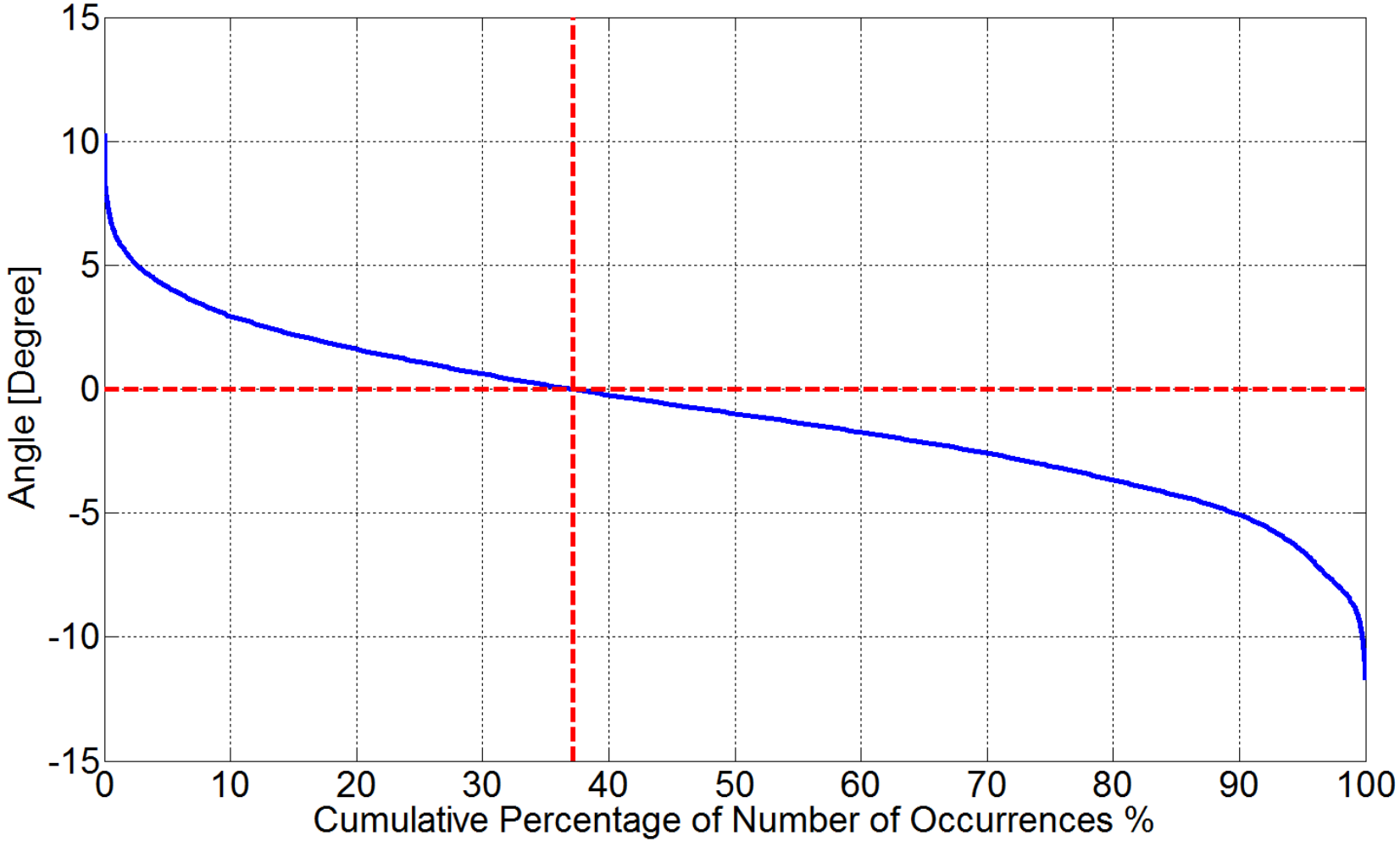
North 7-South 7*



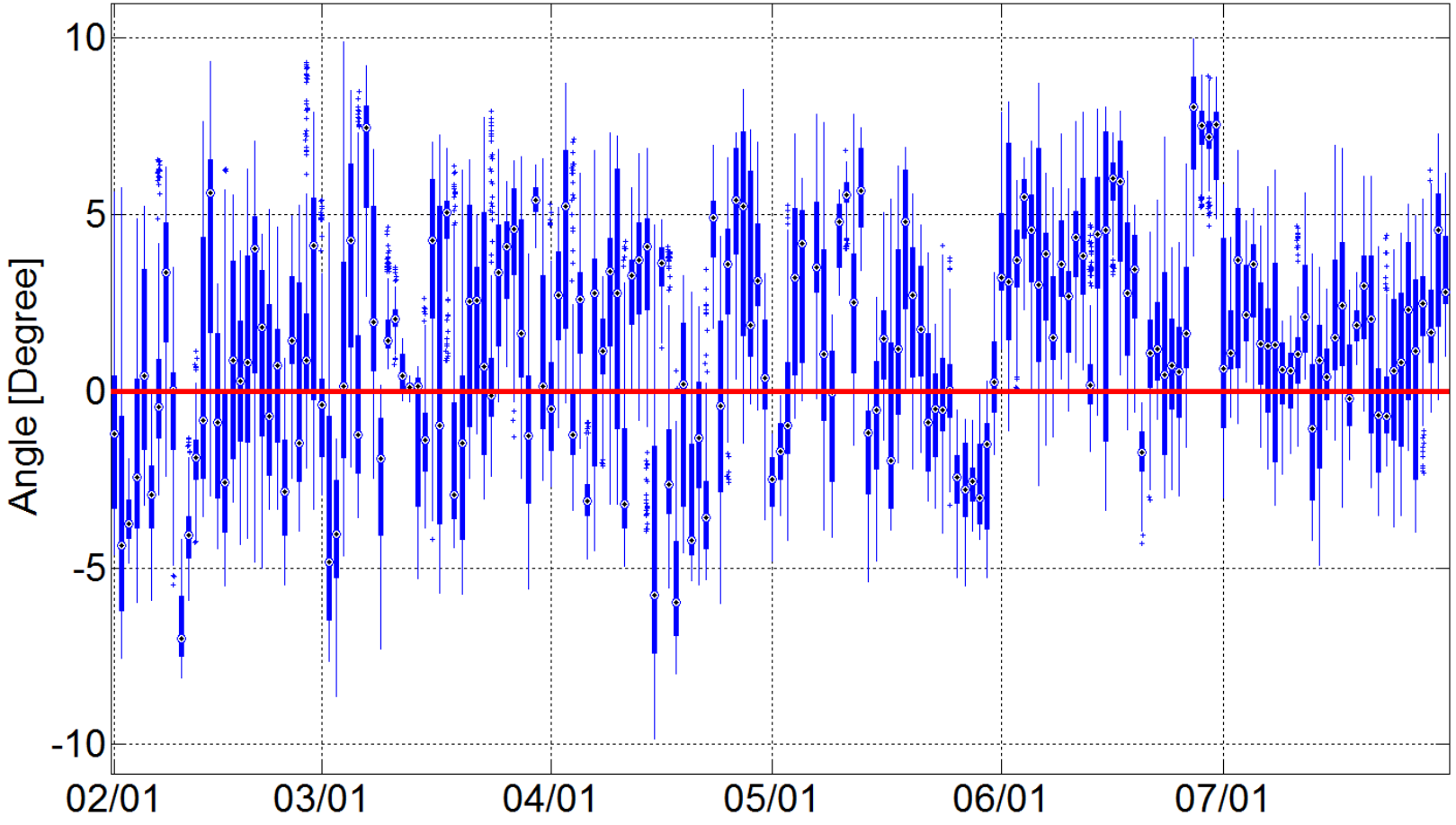
North 7-South 9*



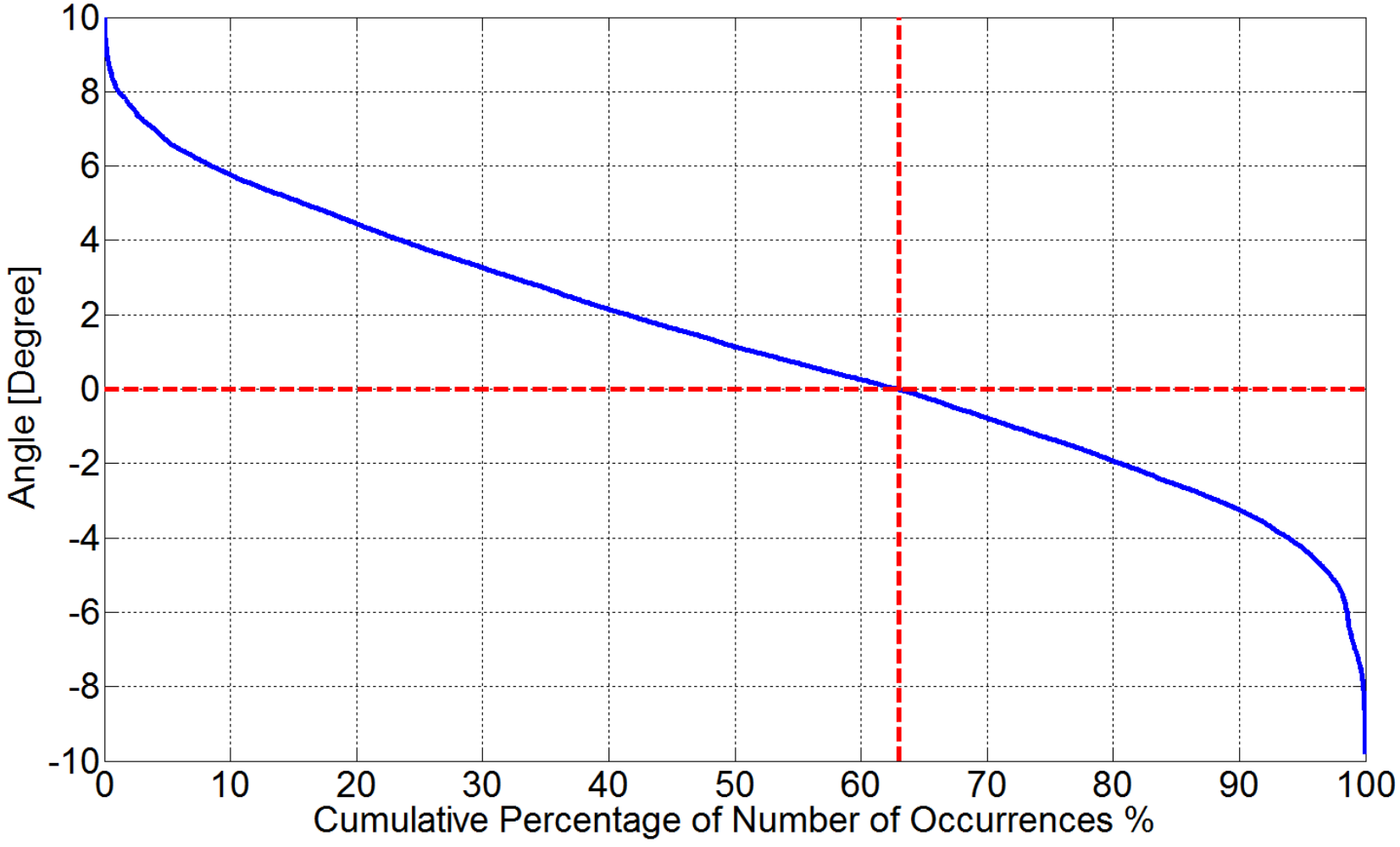
North 7-South 9*



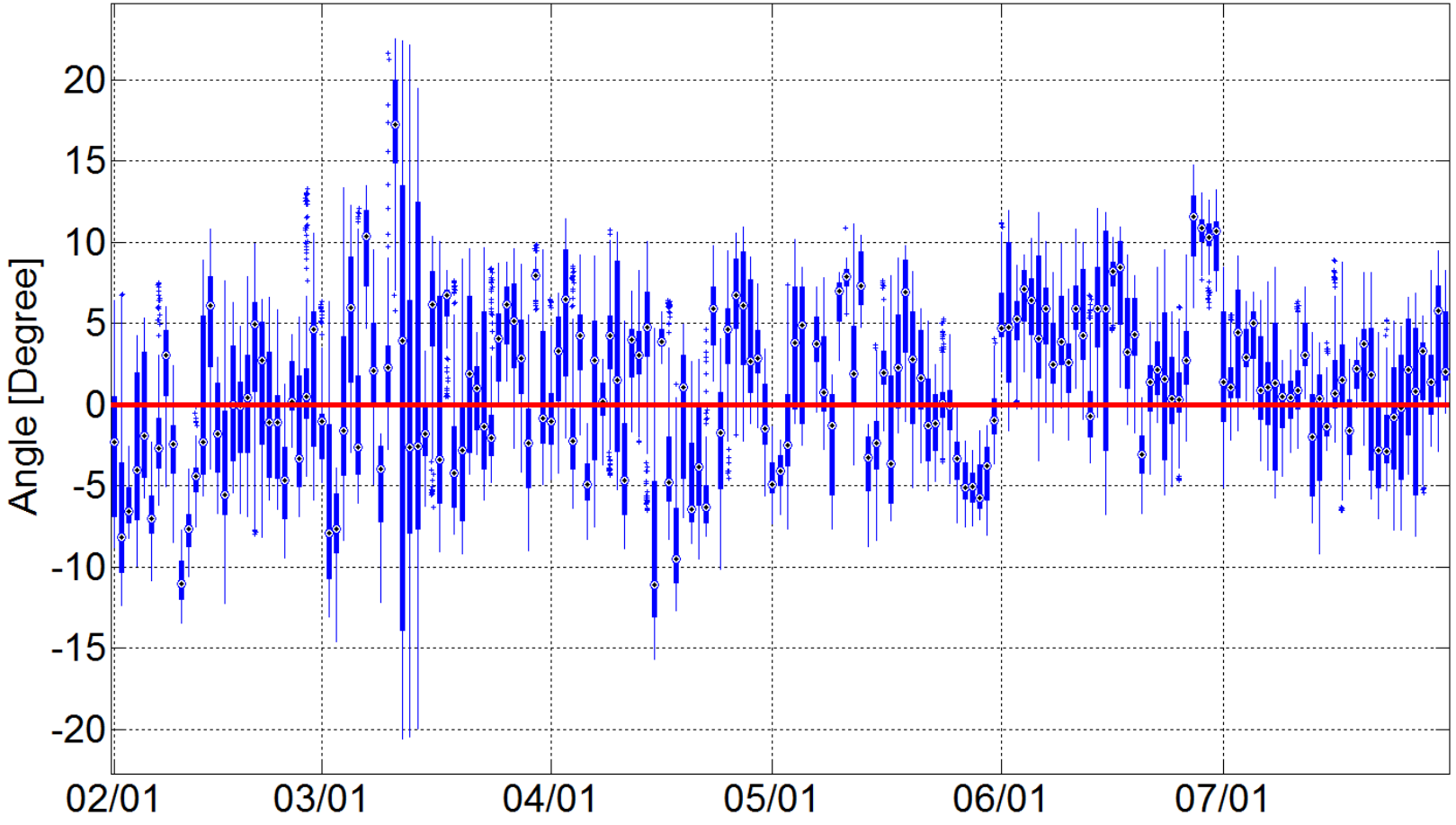
West 11-West 8*



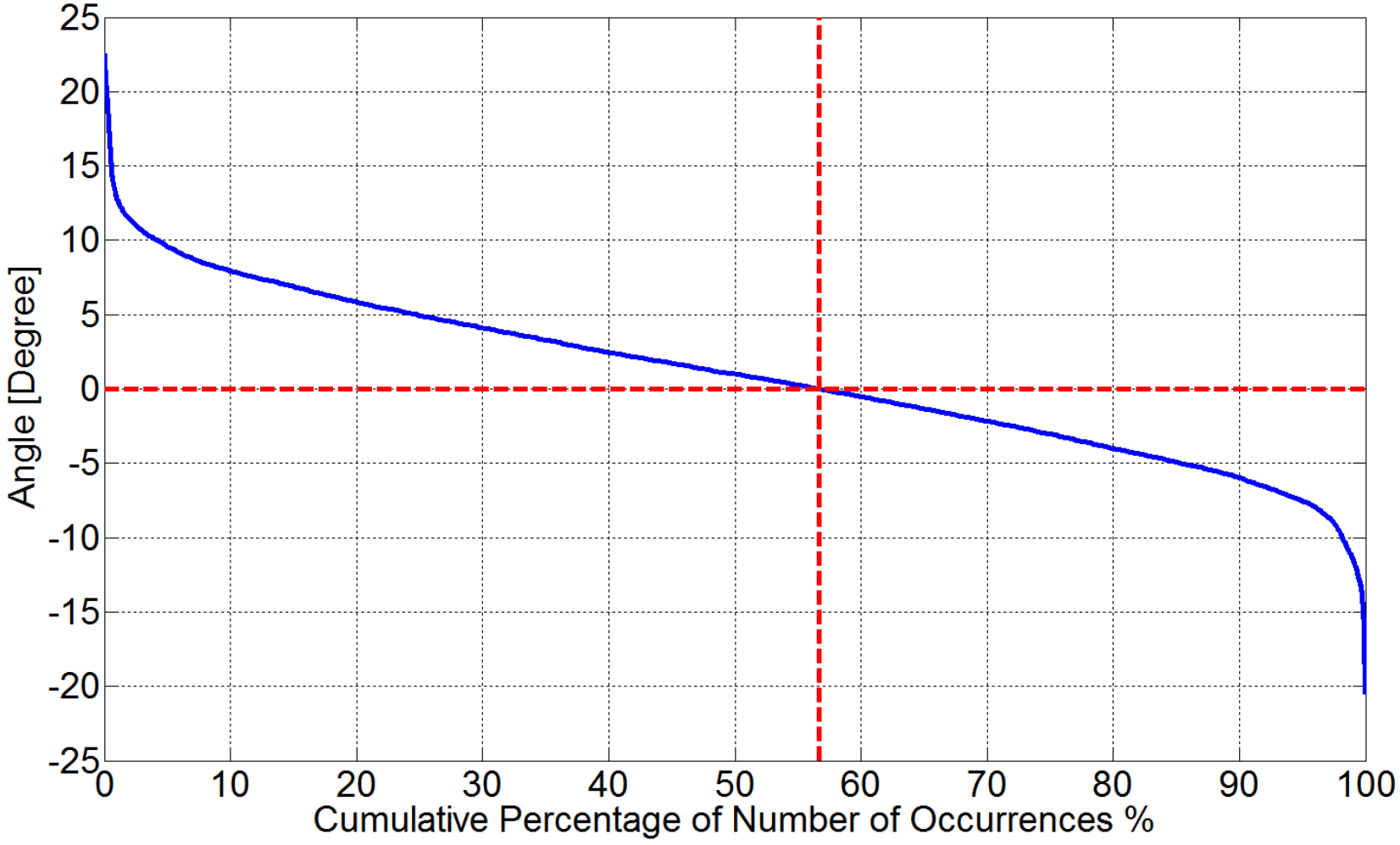
West 11-West 8*



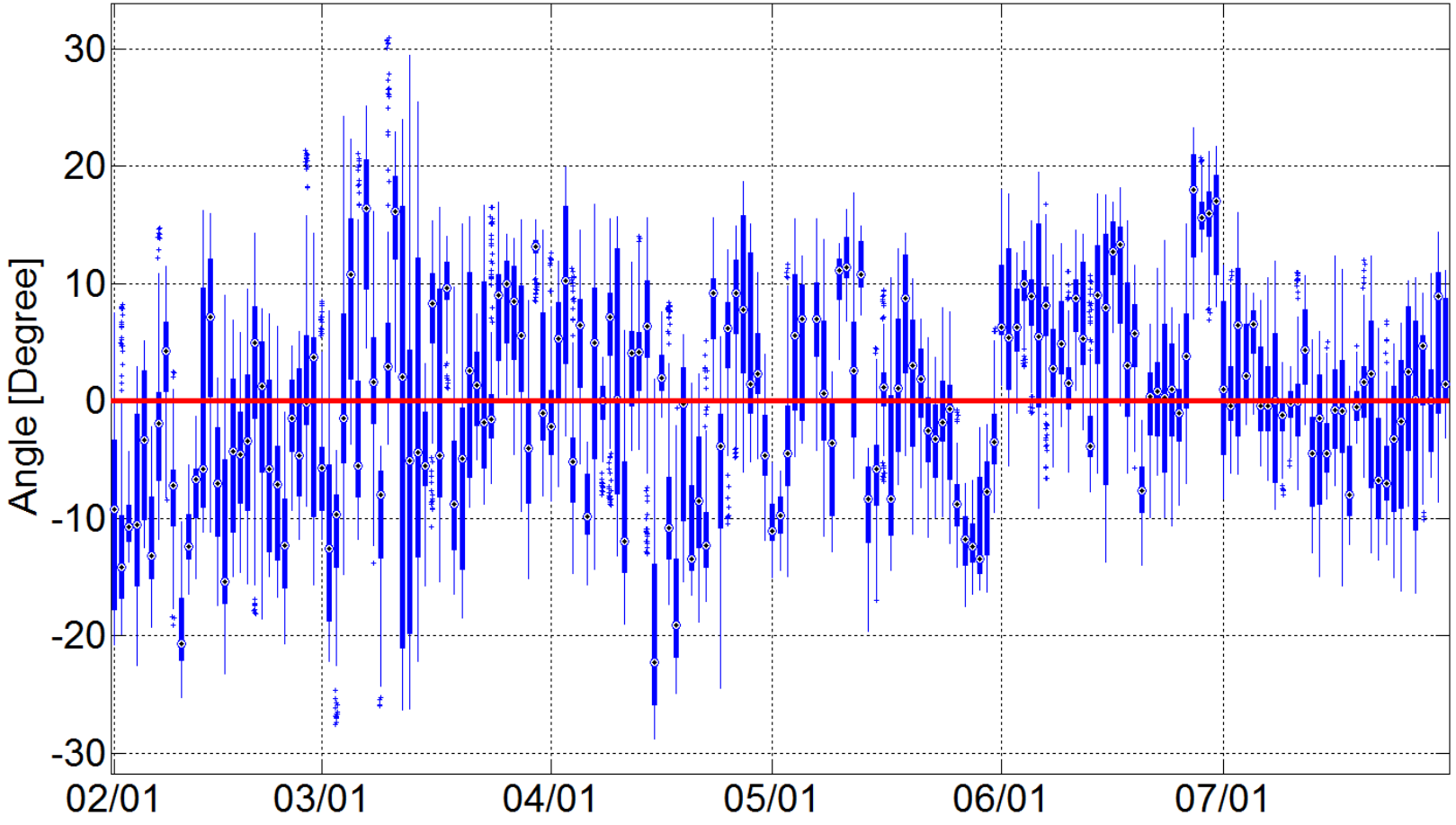
West 8*-South 9*



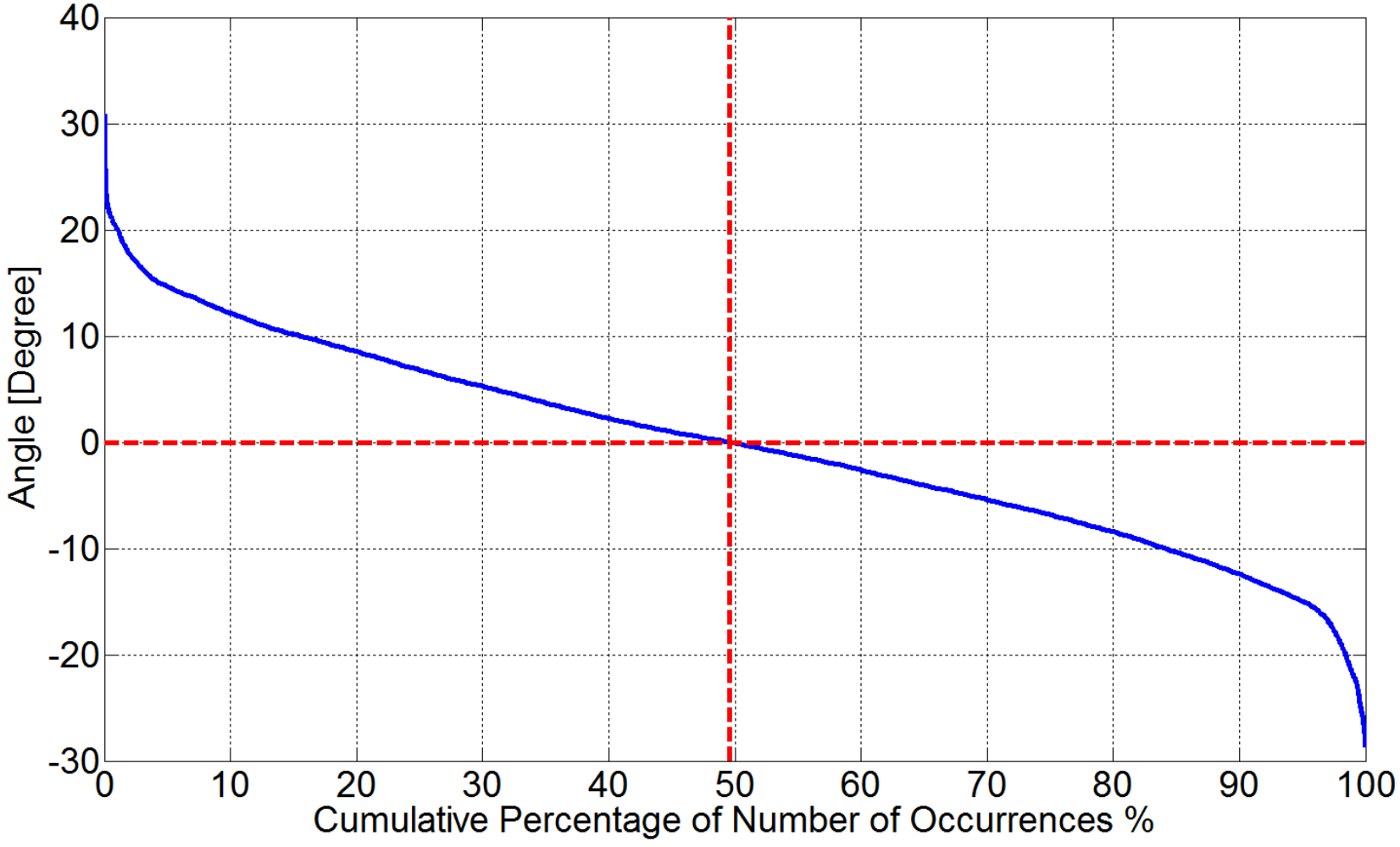
West 8*-South 9*



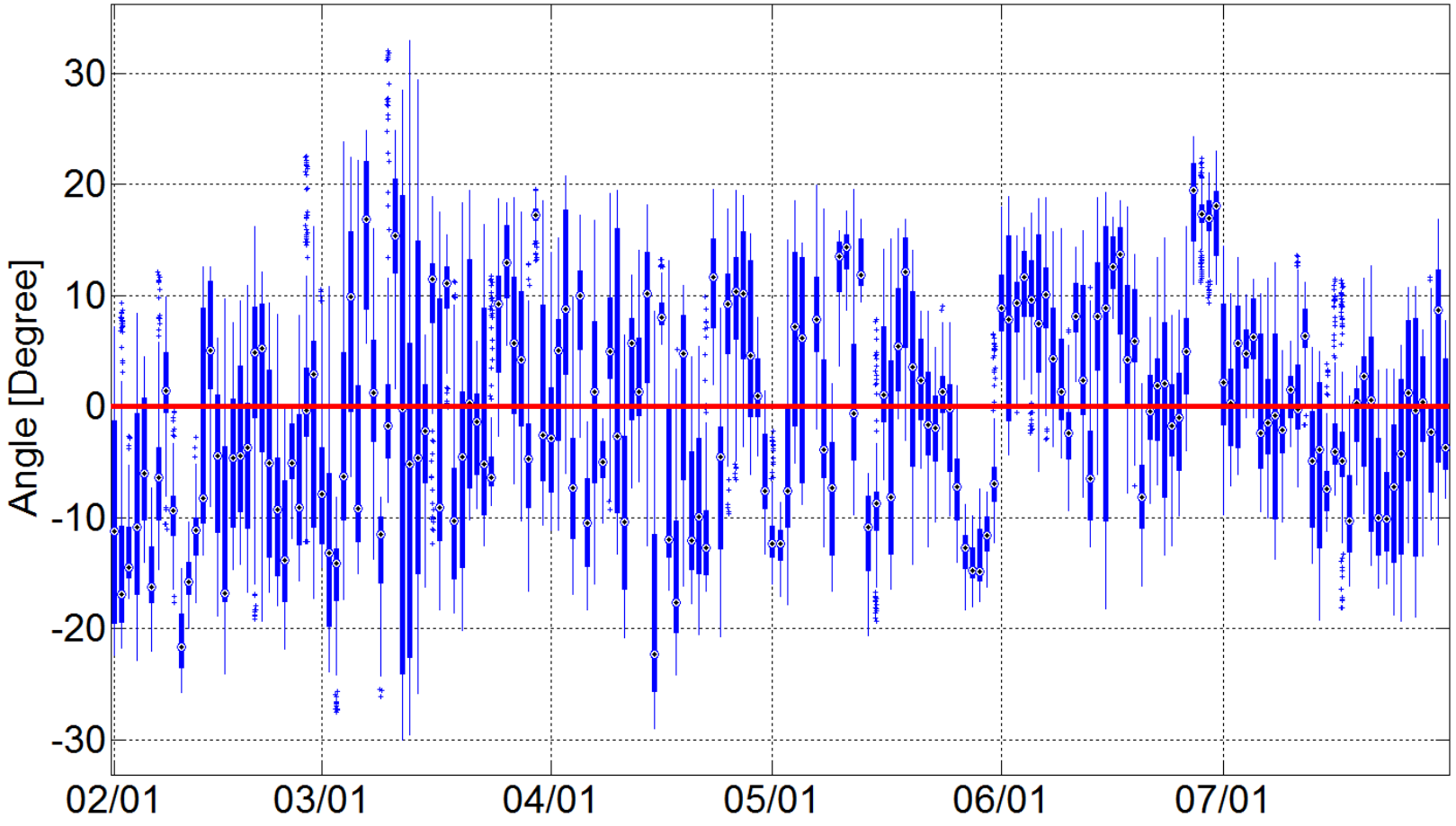
FarWest 7-South 9*



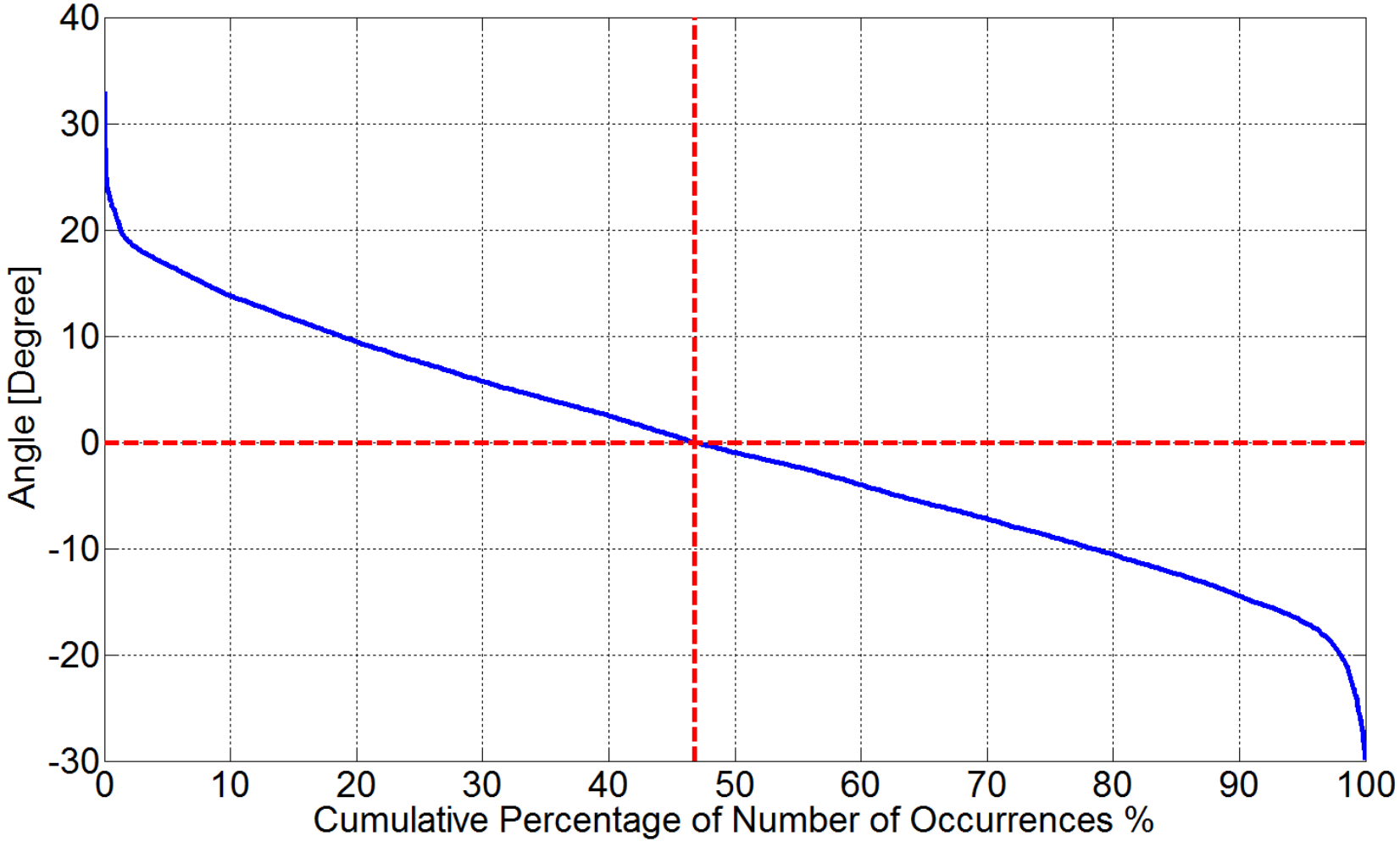
FarWest 7-South 9*



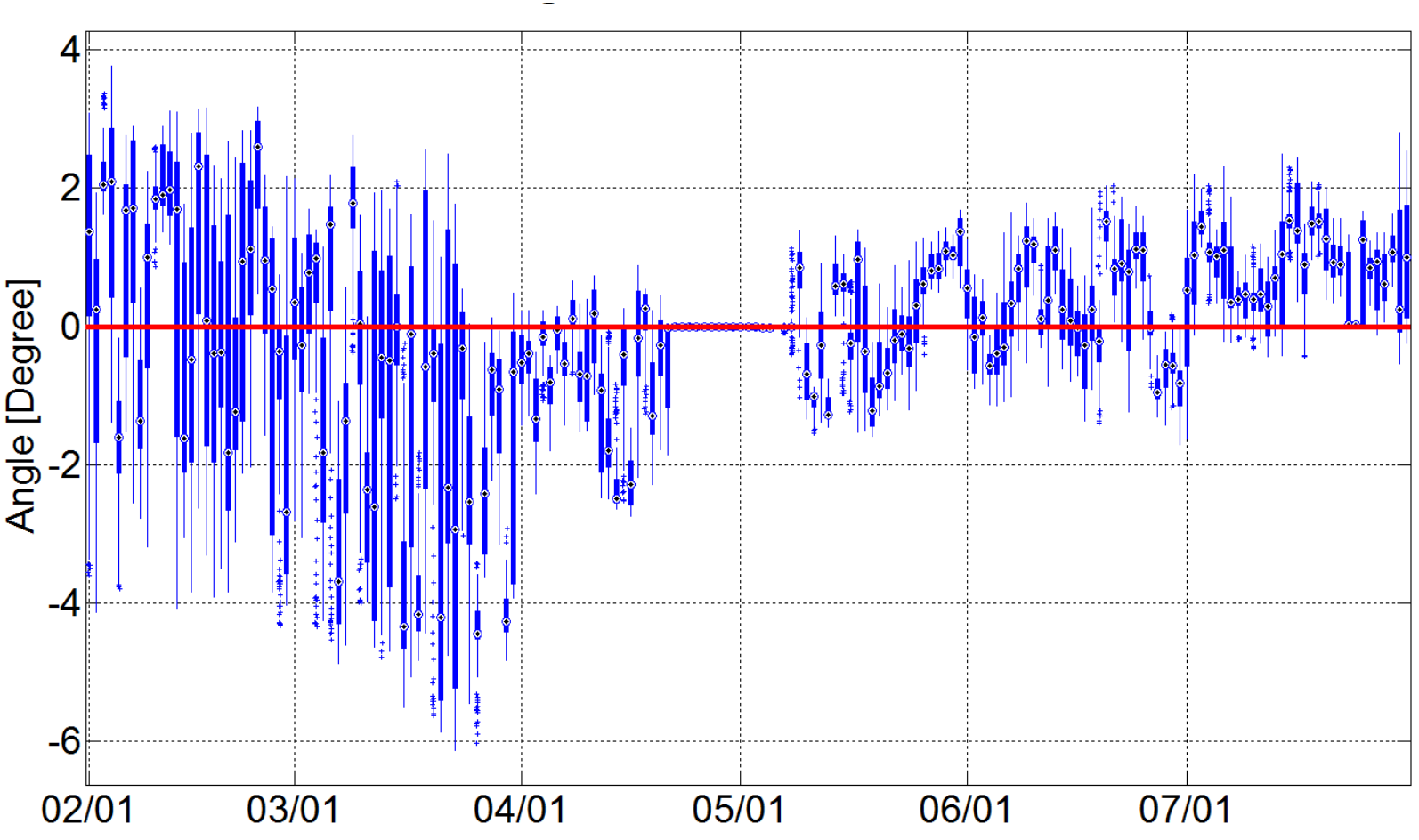
FarWest 9-South 9*



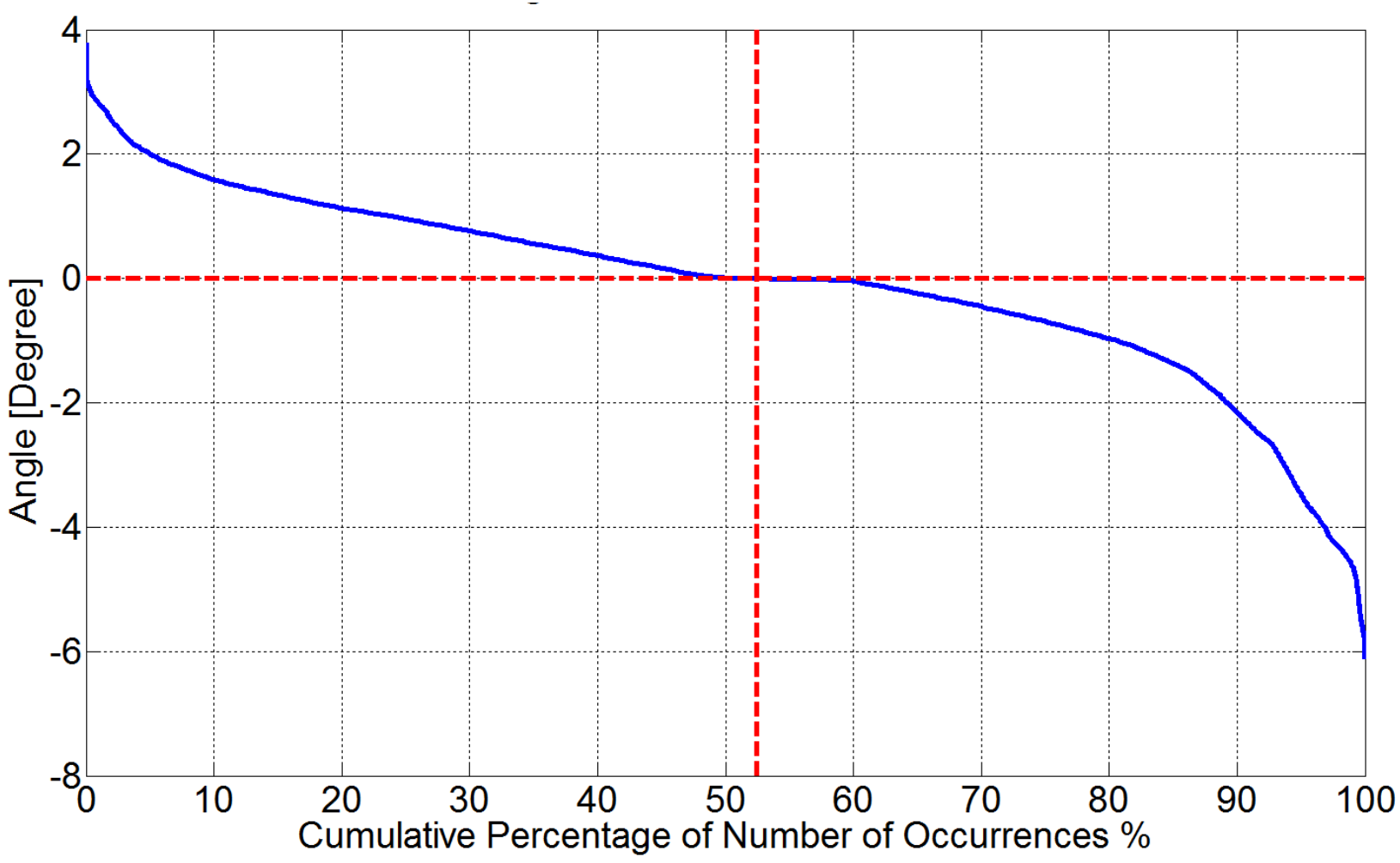
FarWest 9-South 9*



West 19*-West 9



West 19*-West 9



Appendix B – Part 2
CCET Discovery Across Texas project

Baseline Analysis Update – Angle Differences

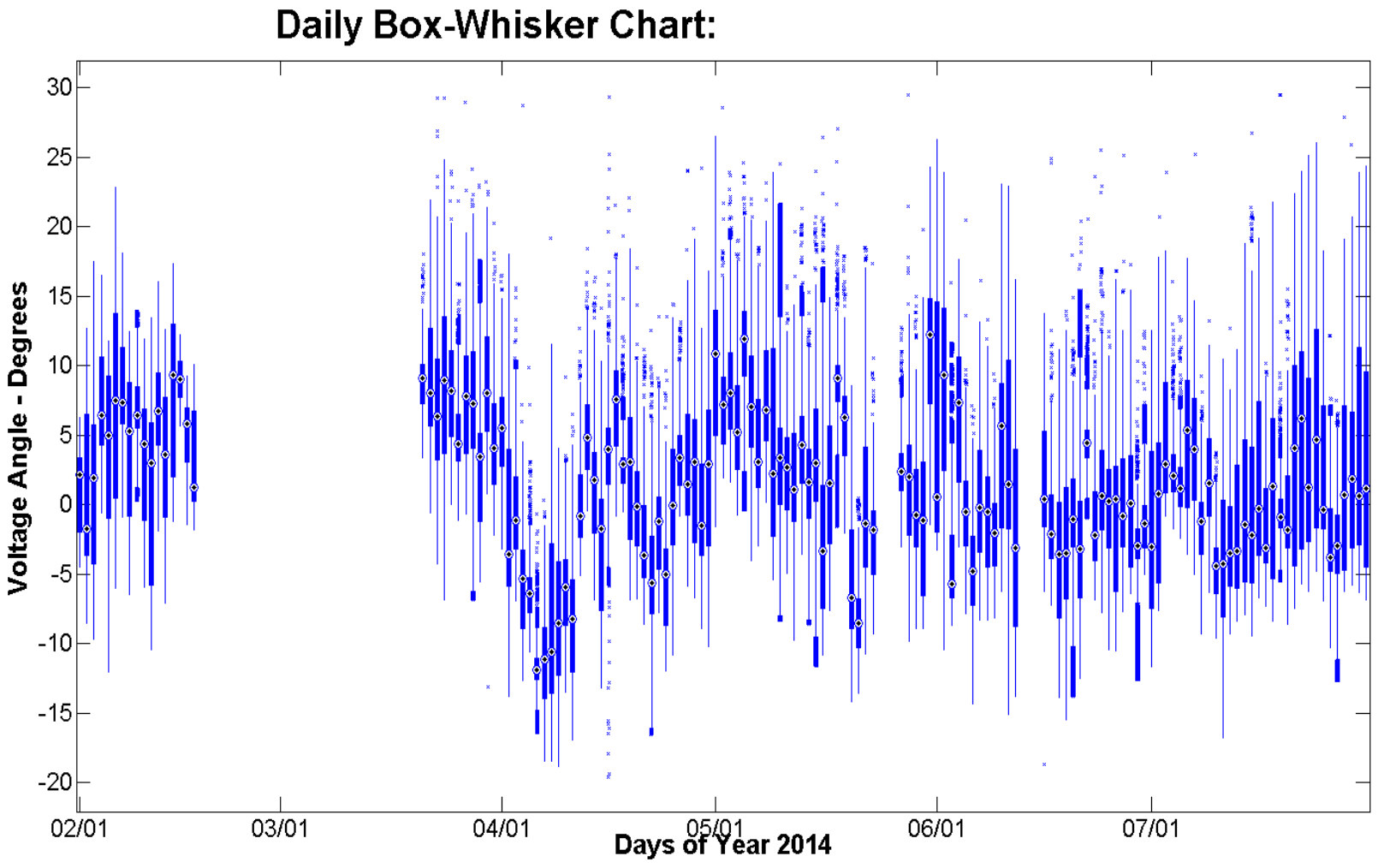
Phasor Data: February to July 2014
Box-Whisker Plots and Time Duration Curves

Electric Power Group

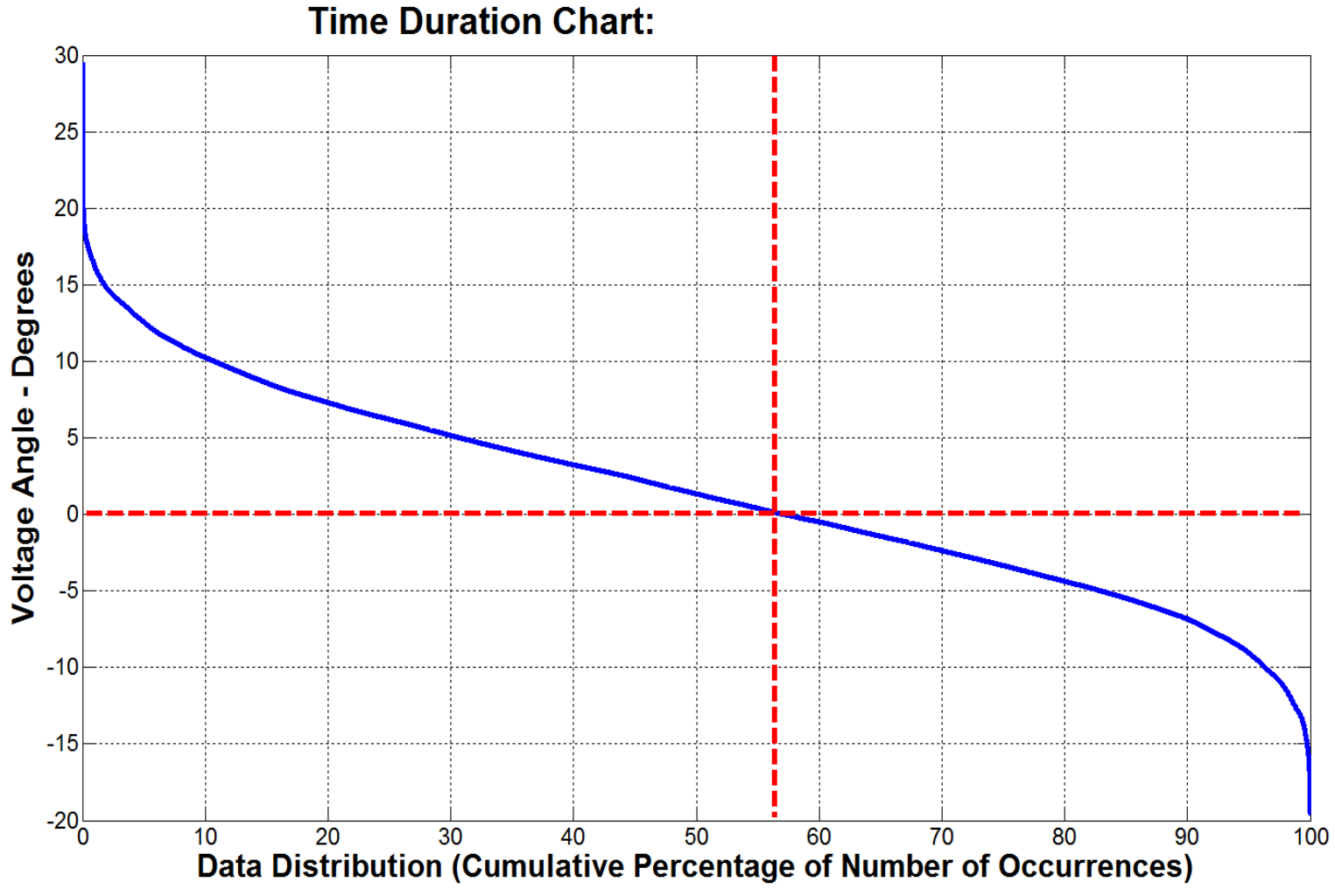
CCET

ERCOT

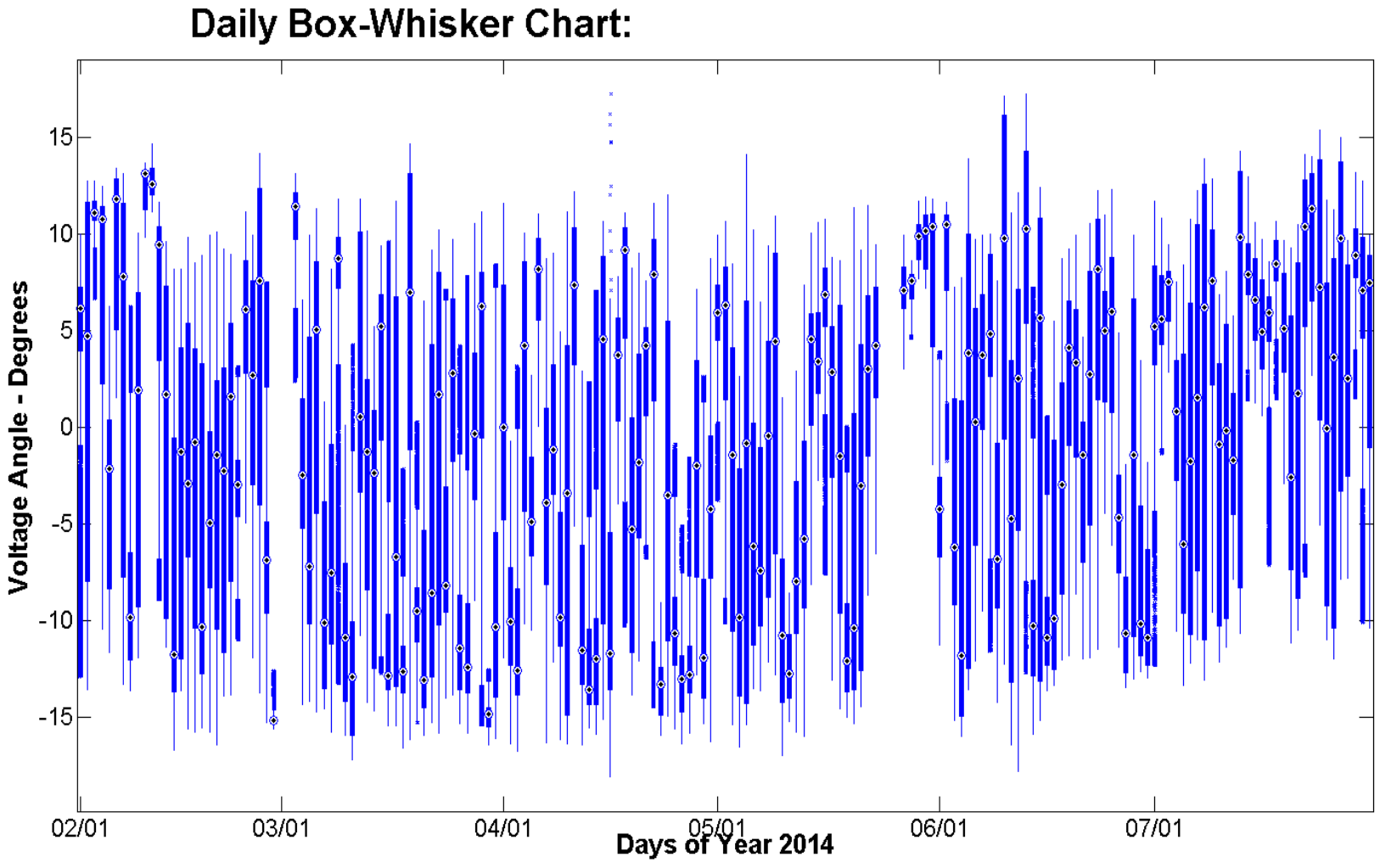
Coast 1 - South 13



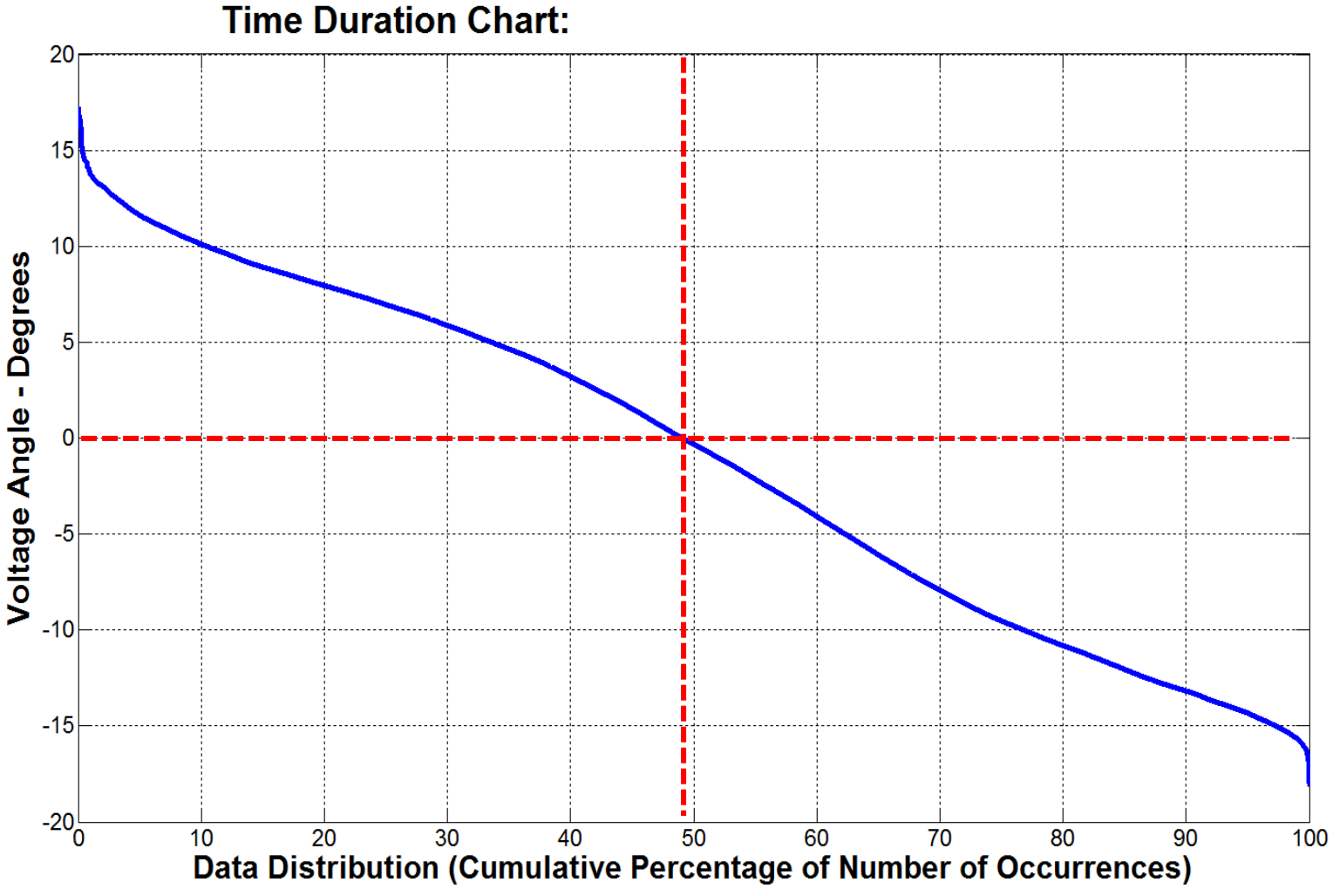
Coast 1 - South 13



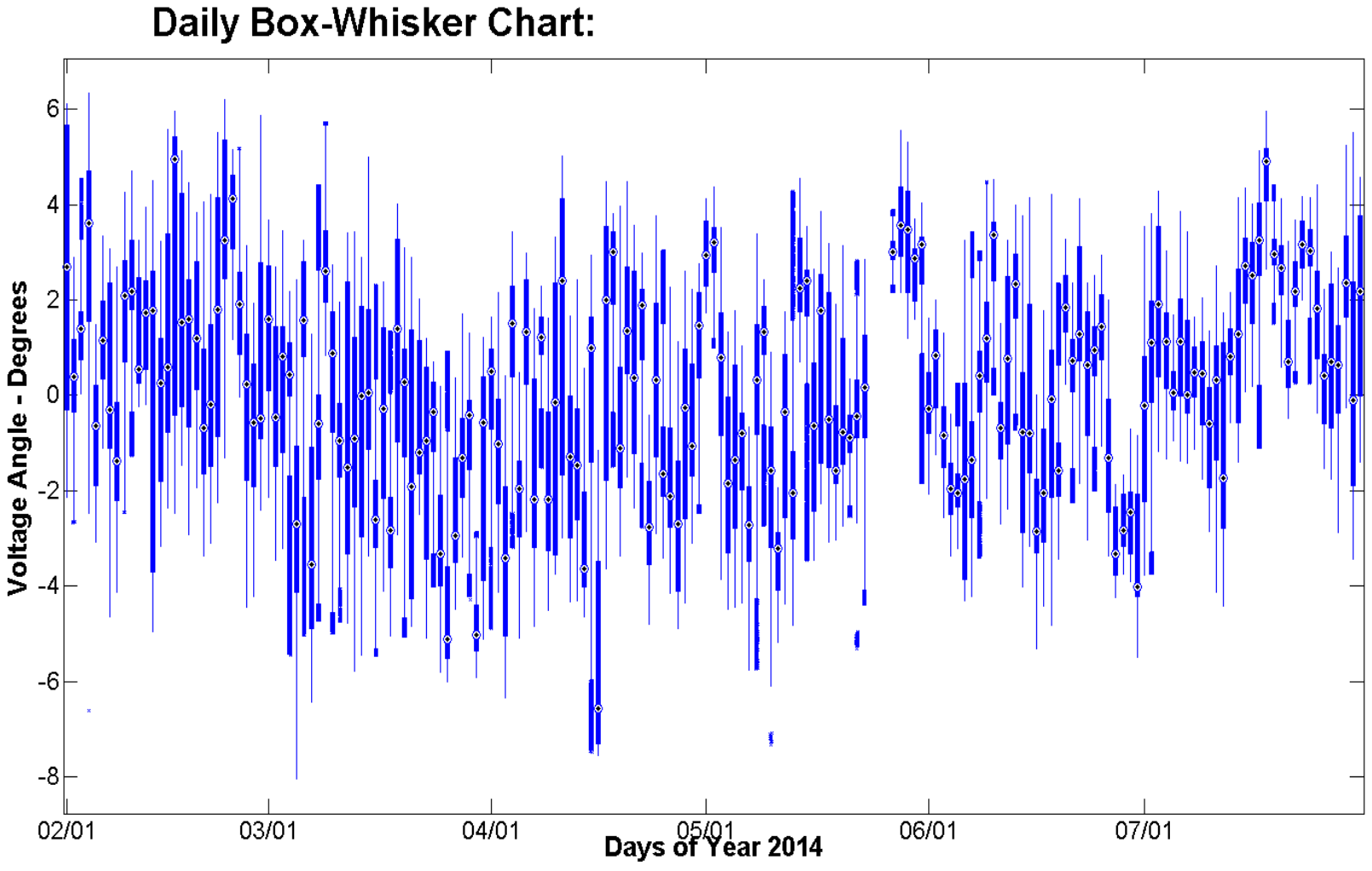
West 5 – West 10



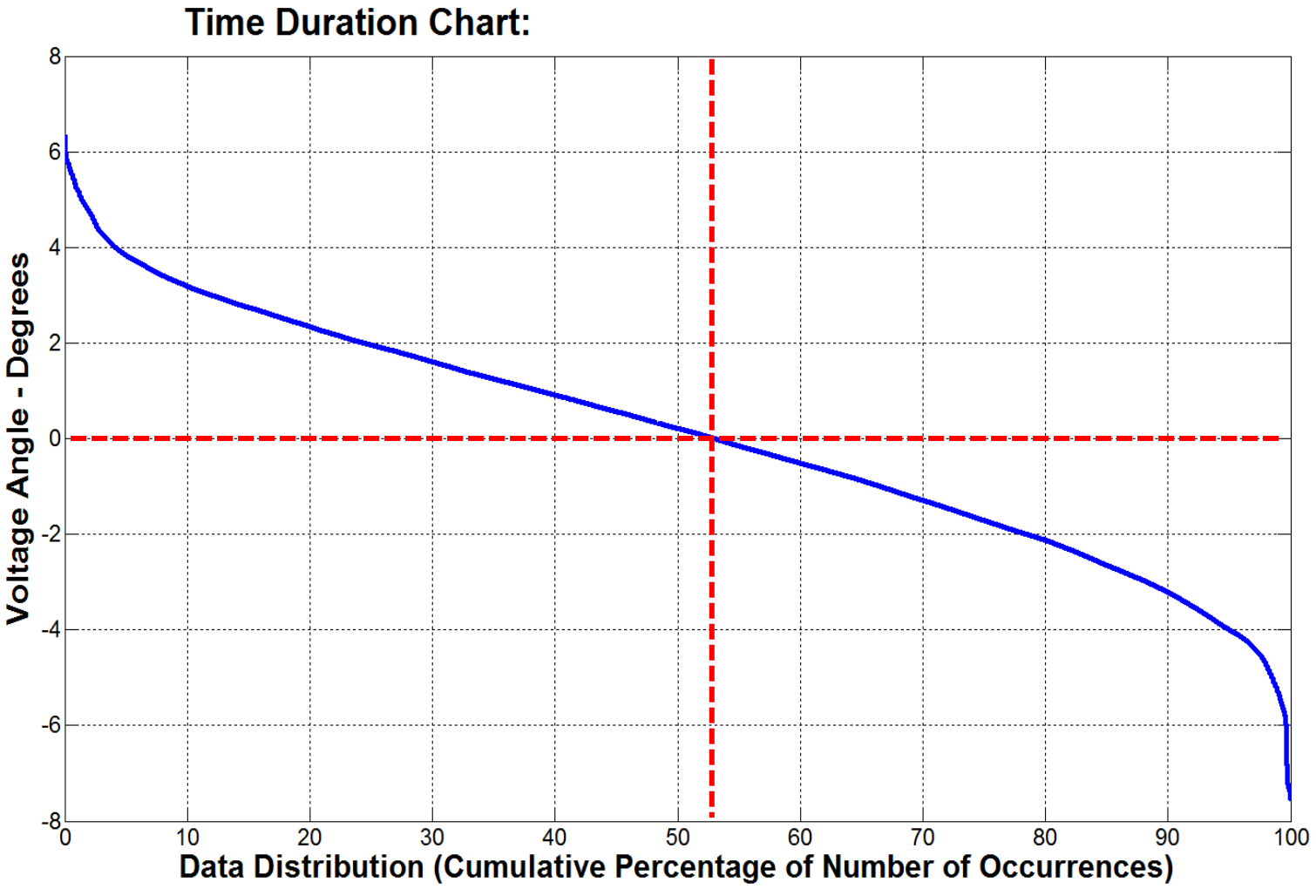
West 5 – West 10



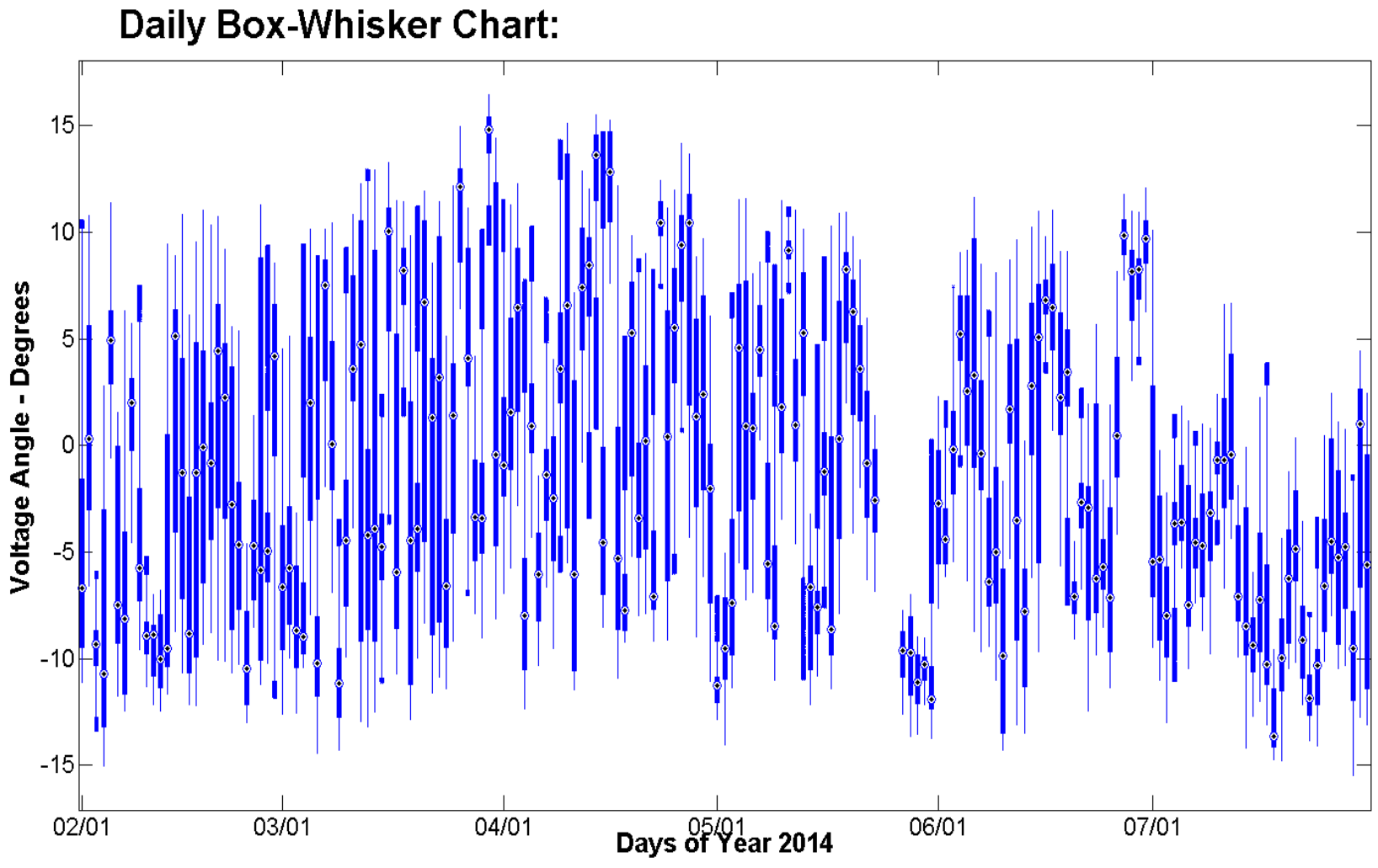
West 5 – FarWest 4



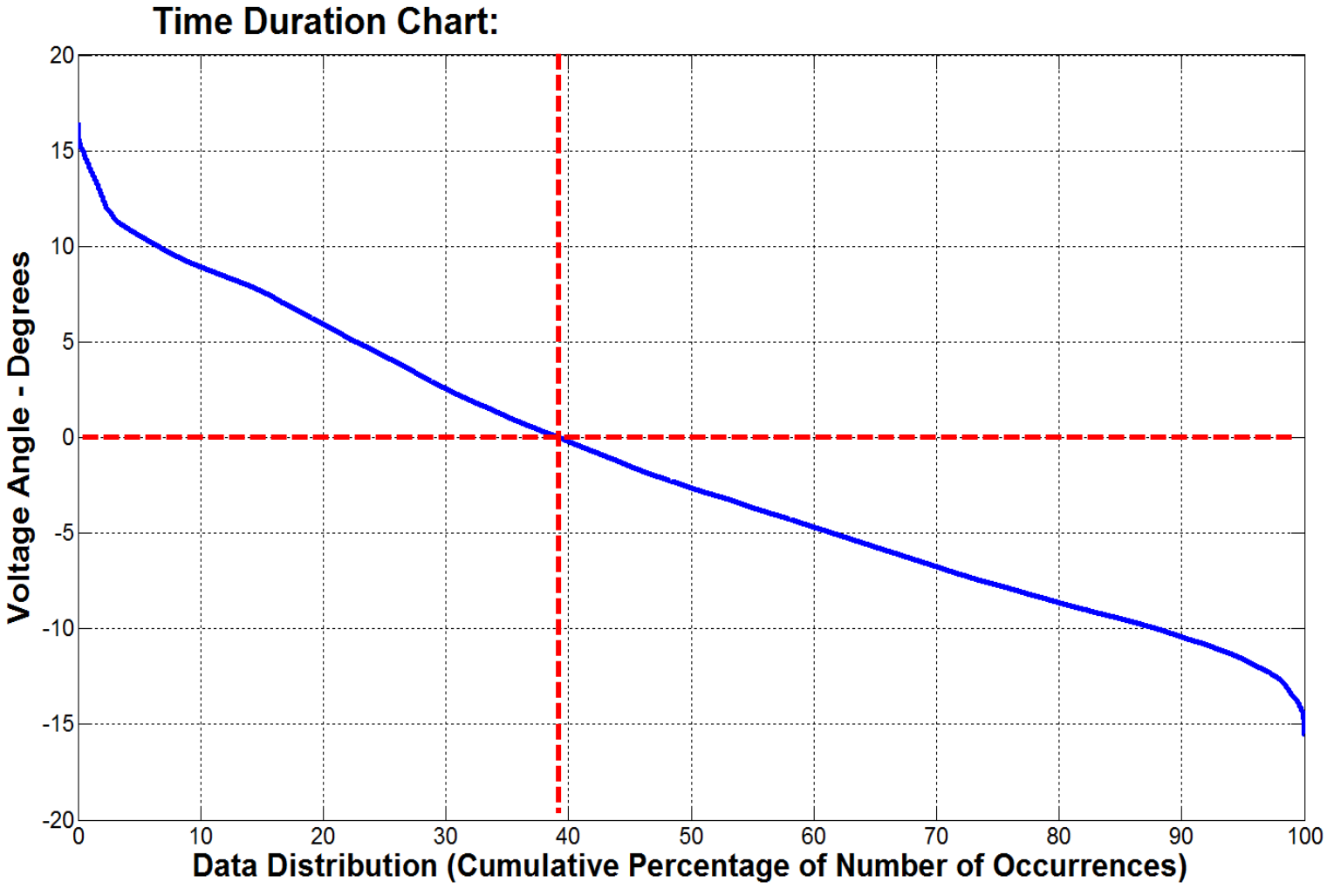
West 5 – FarWest 4



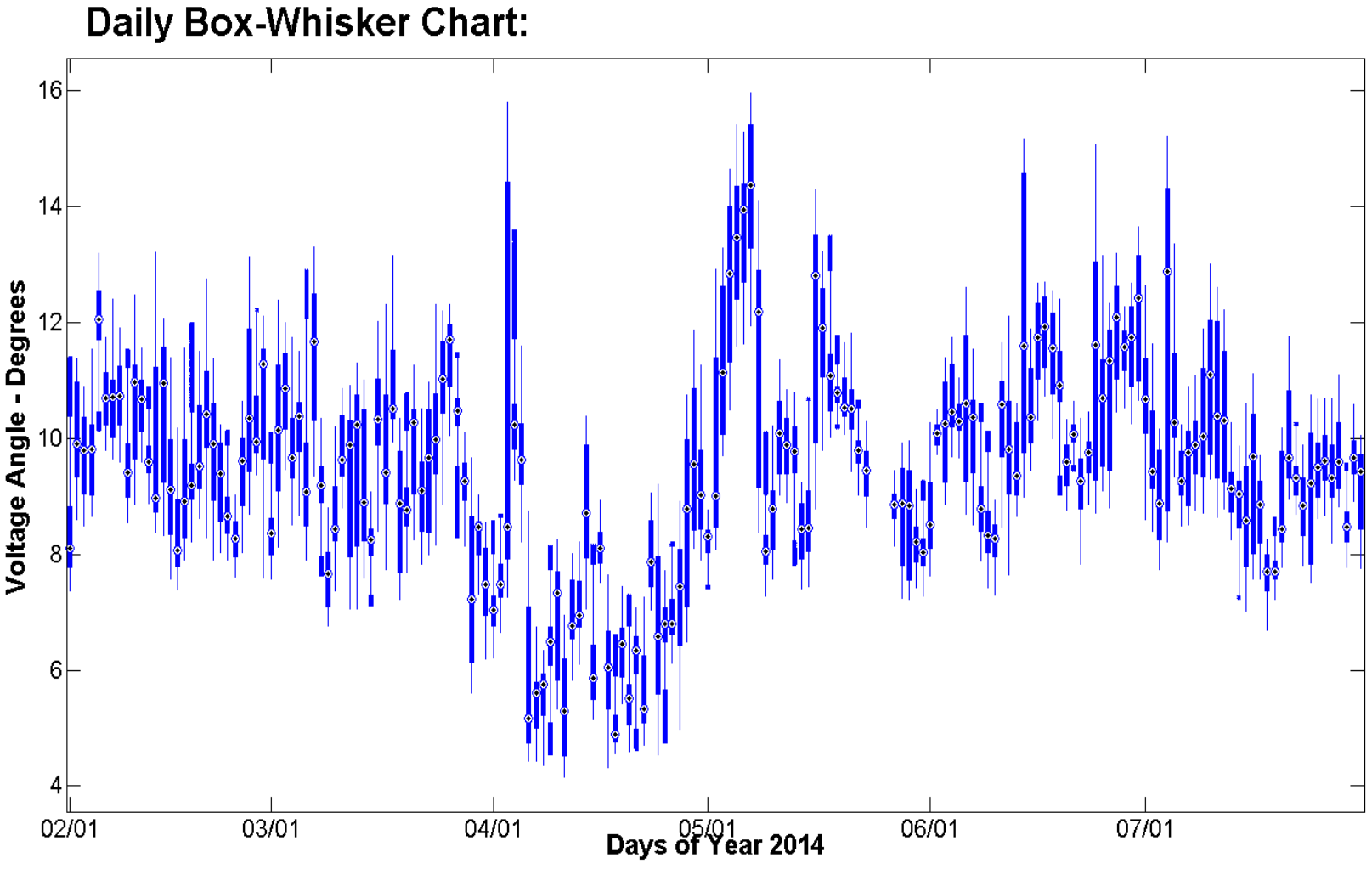
West 5 – North 1



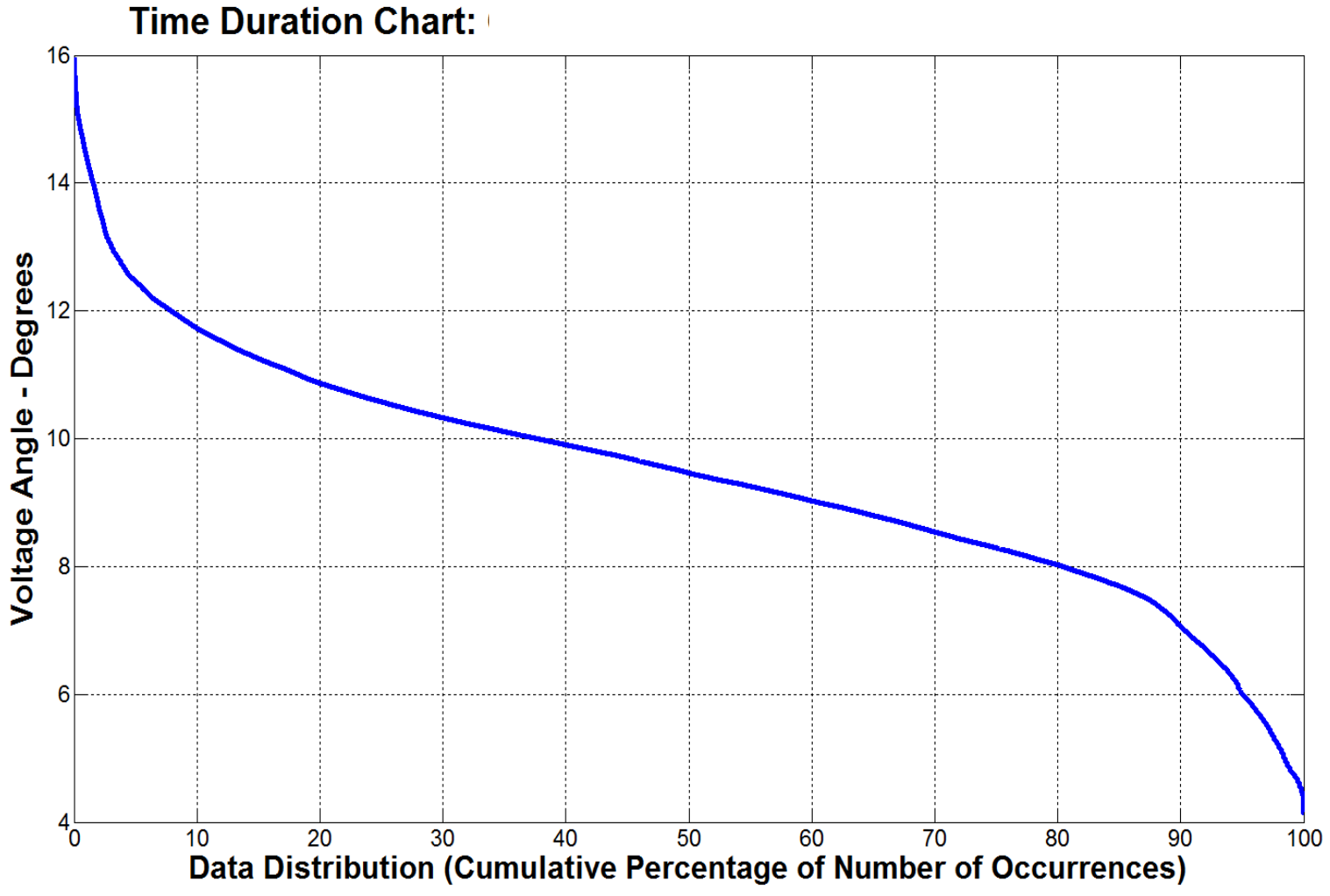
West 5 – North 1



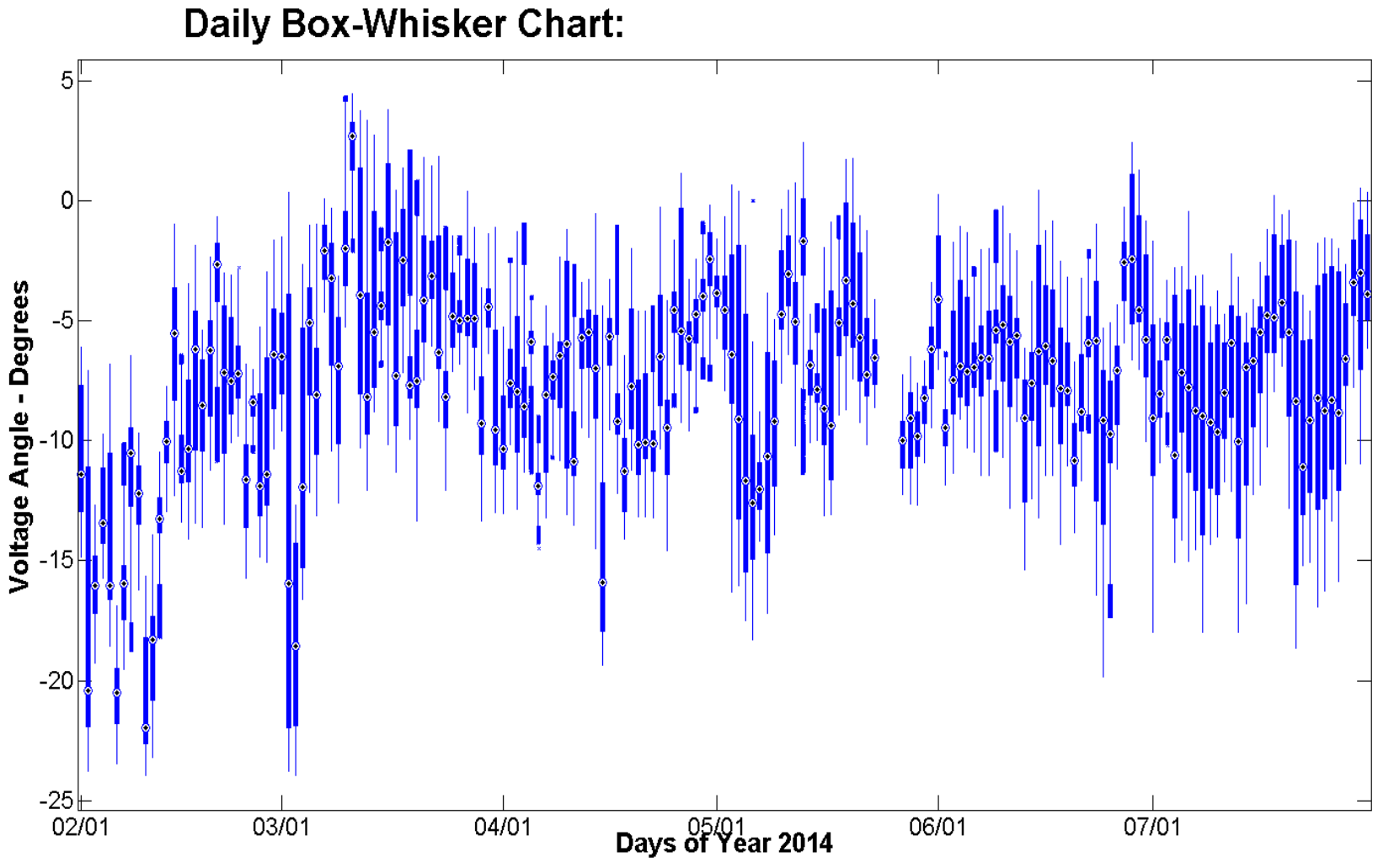
North 1 – North 4



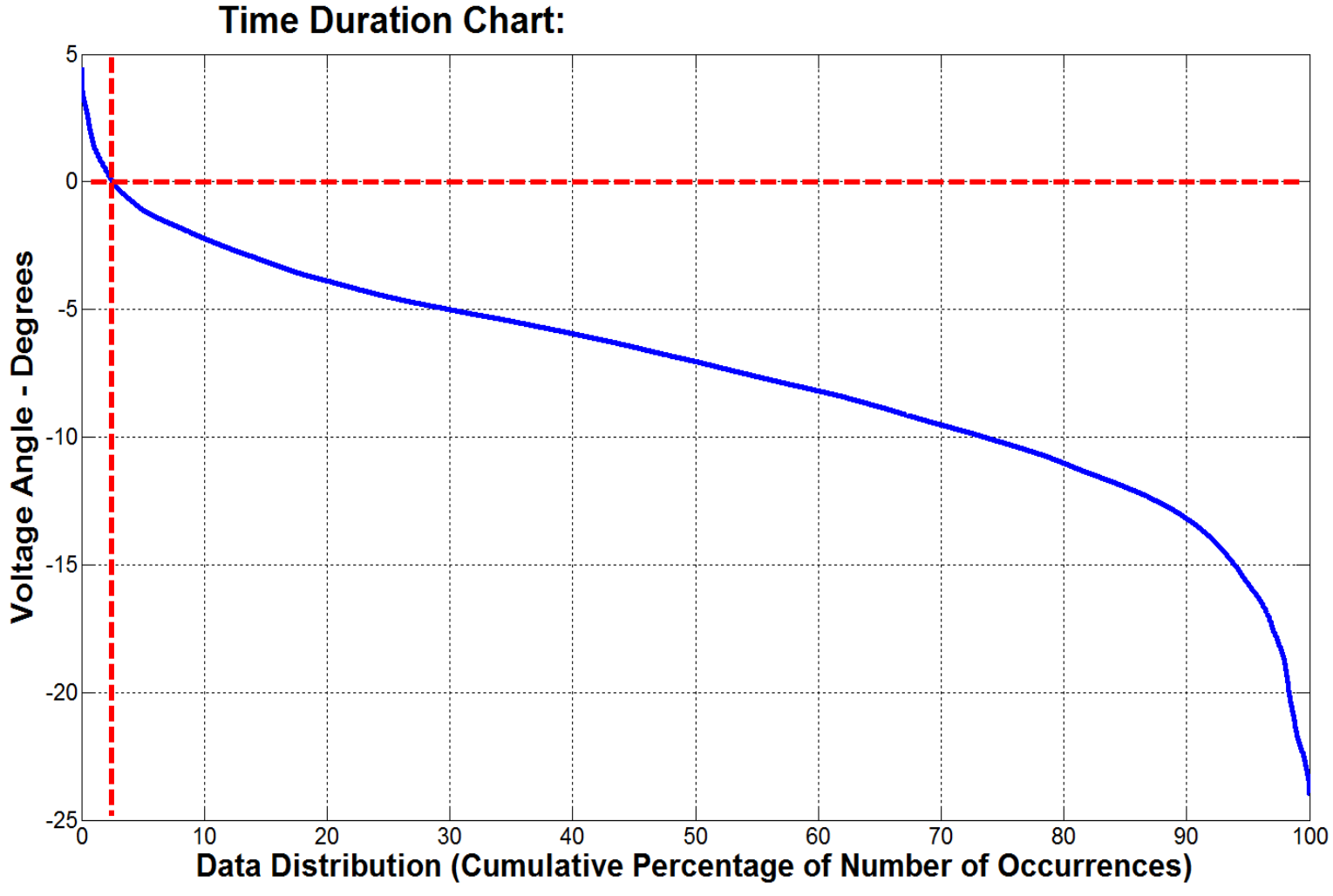
North 1 – North 4



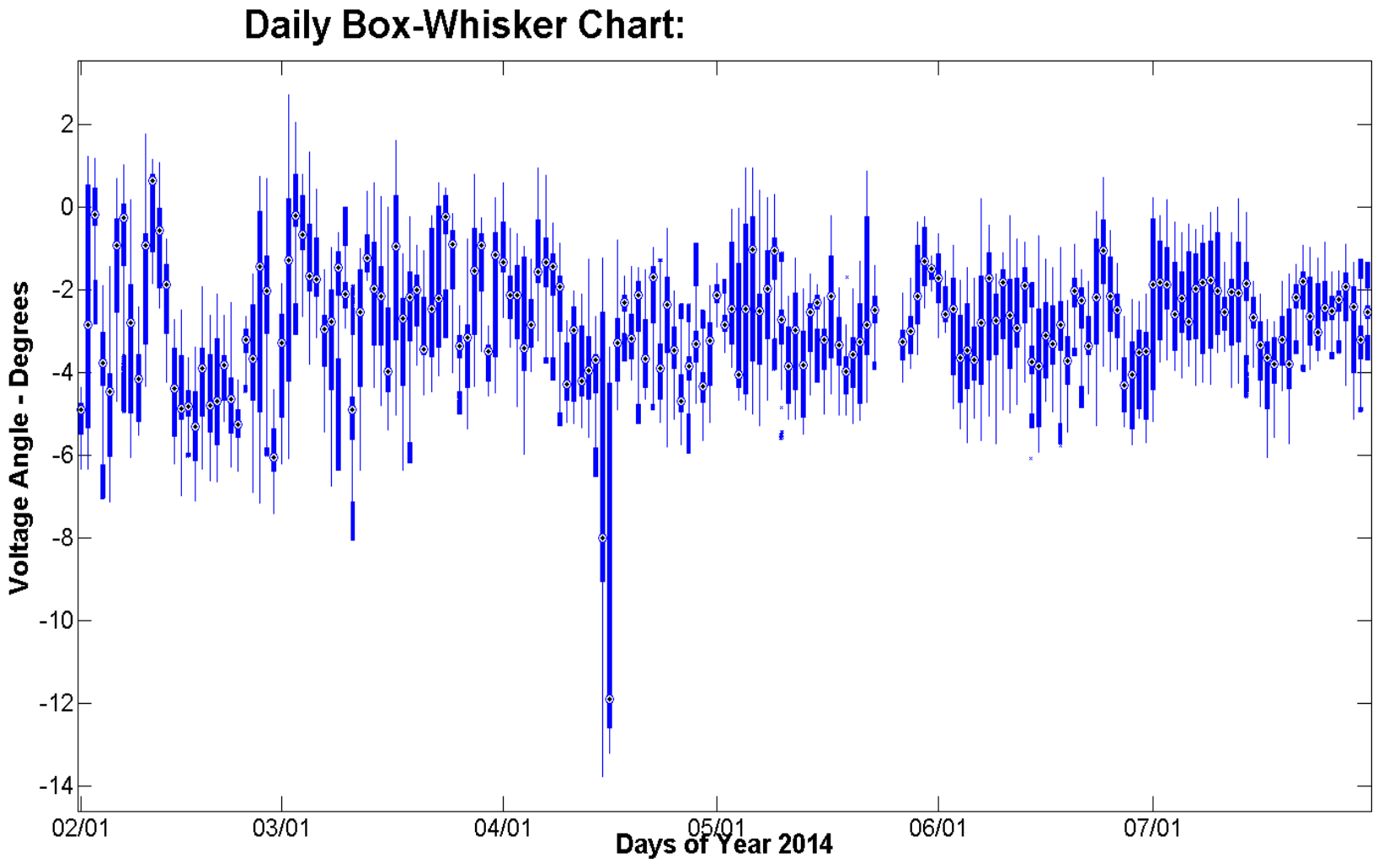
North 4 – North 6



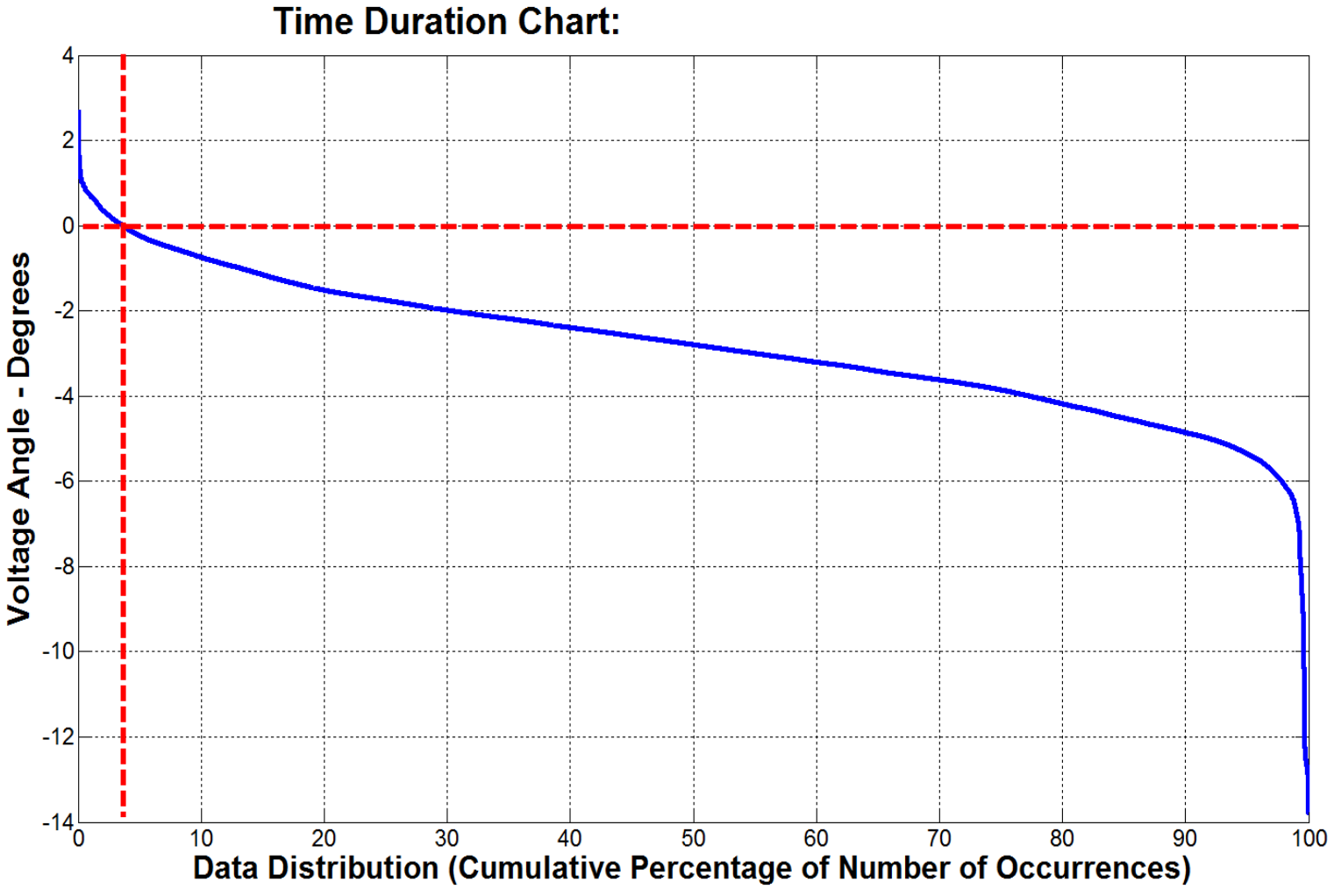
North 4 – North 6



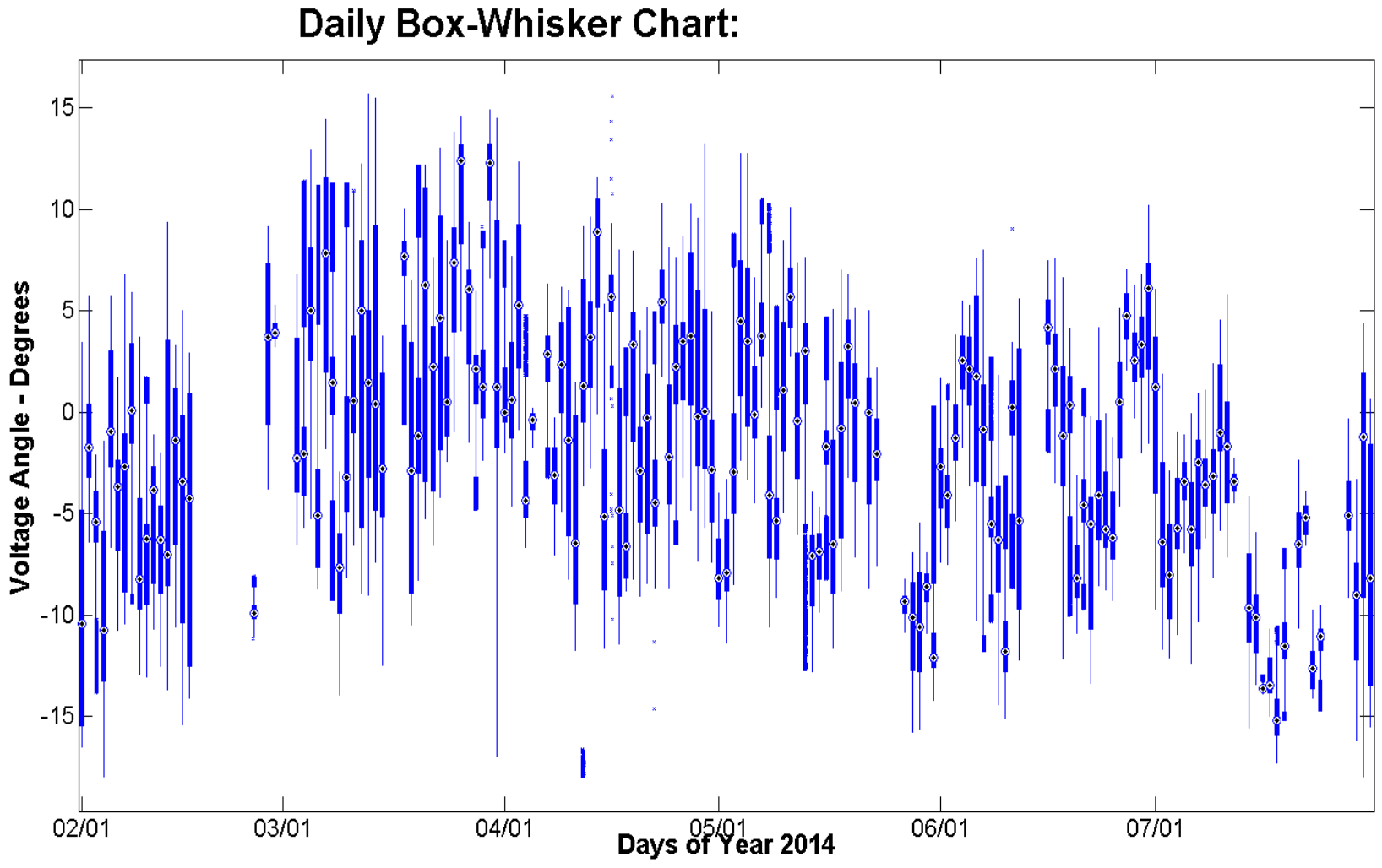
FarWest 7 – FarWest 4



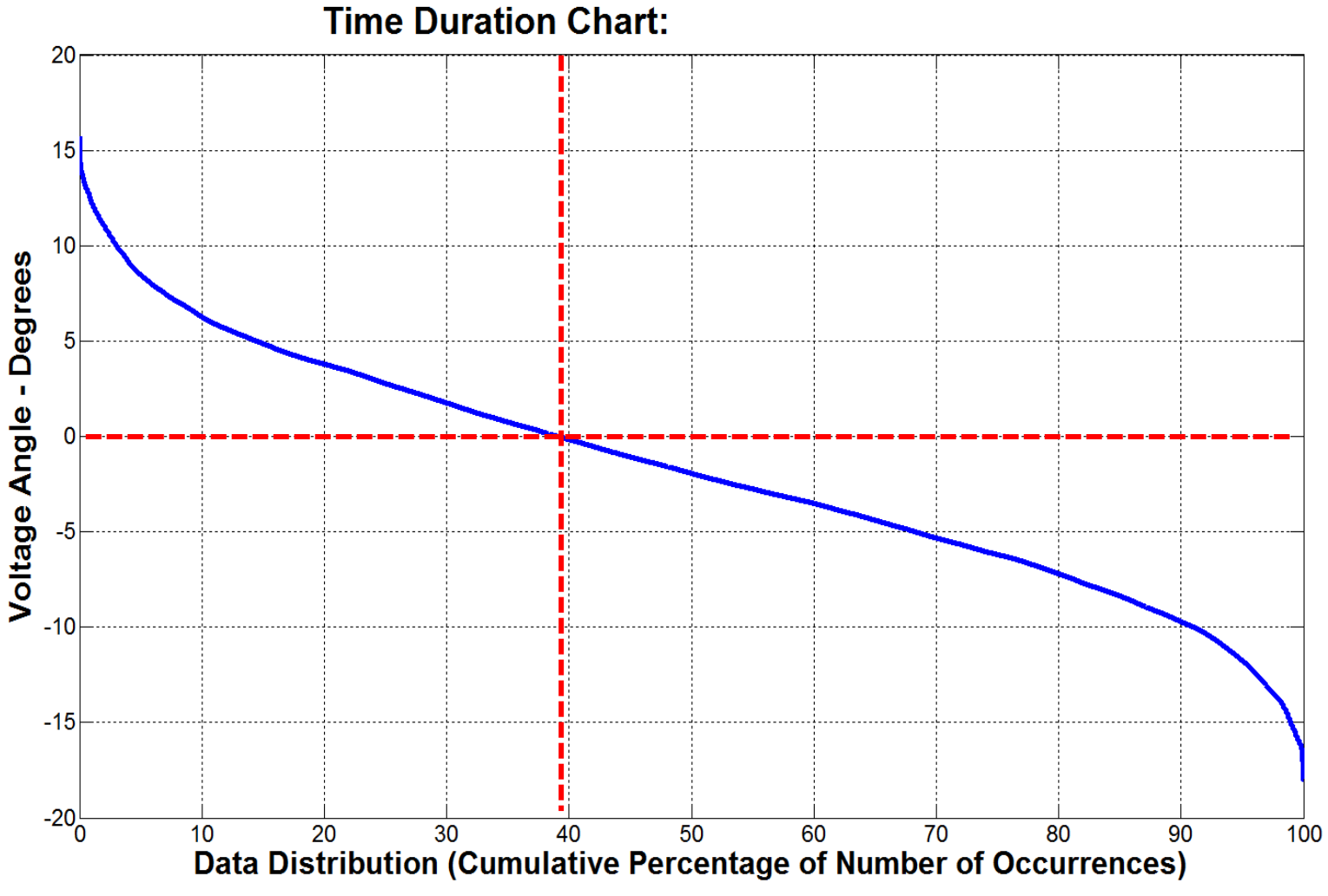
FarWest 7 – FarWest 4



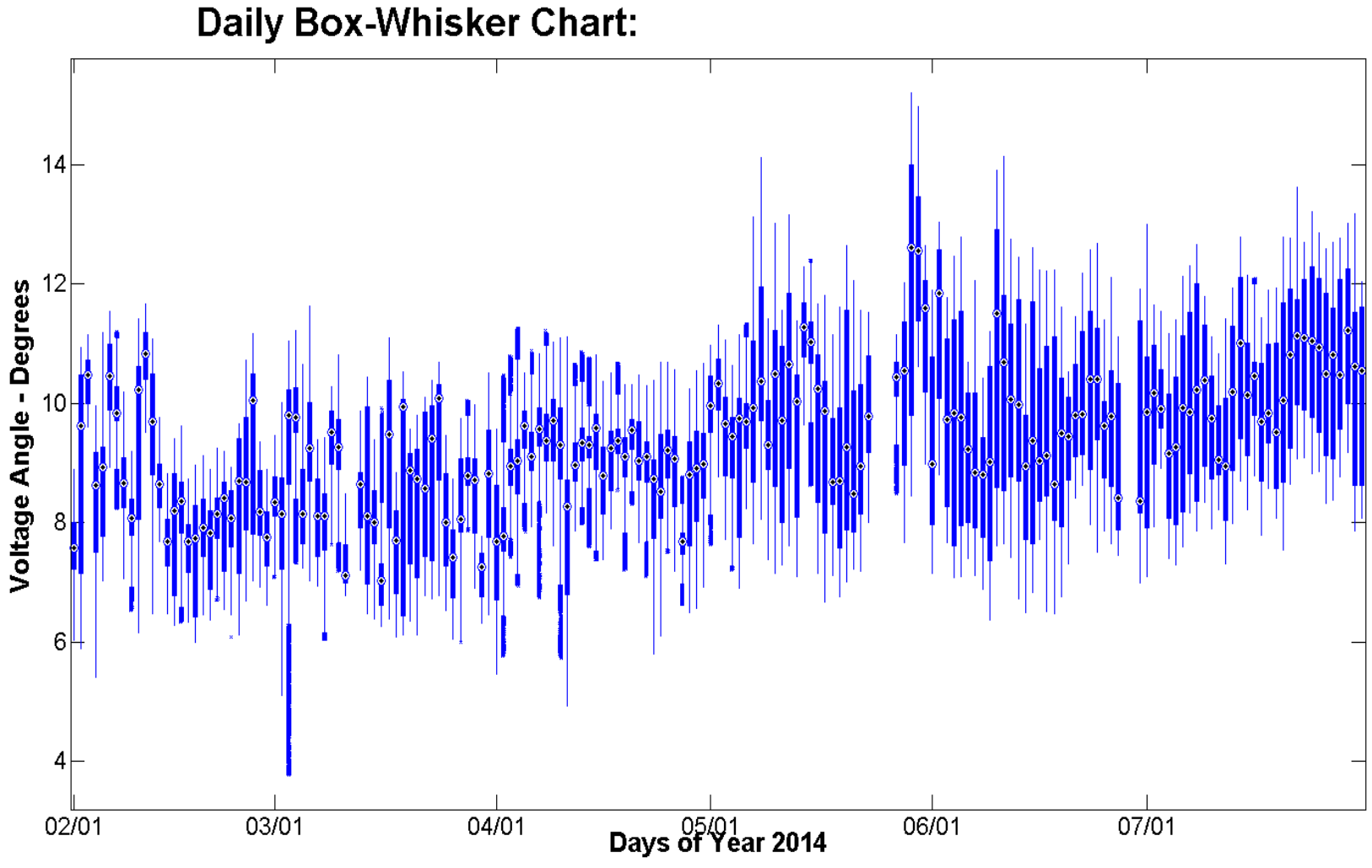
FarWest 7 – West 14



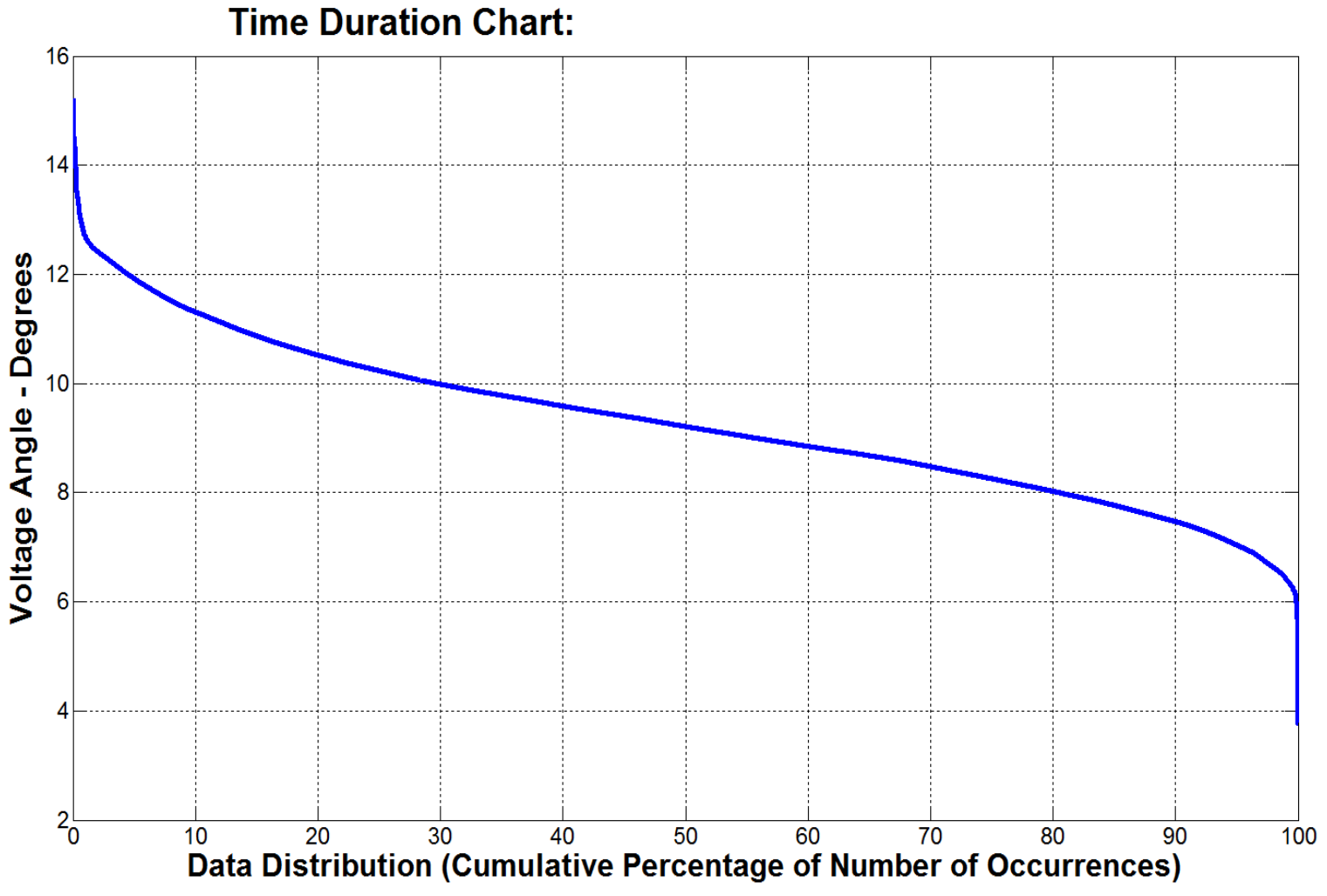
FarWest 7 – West 14



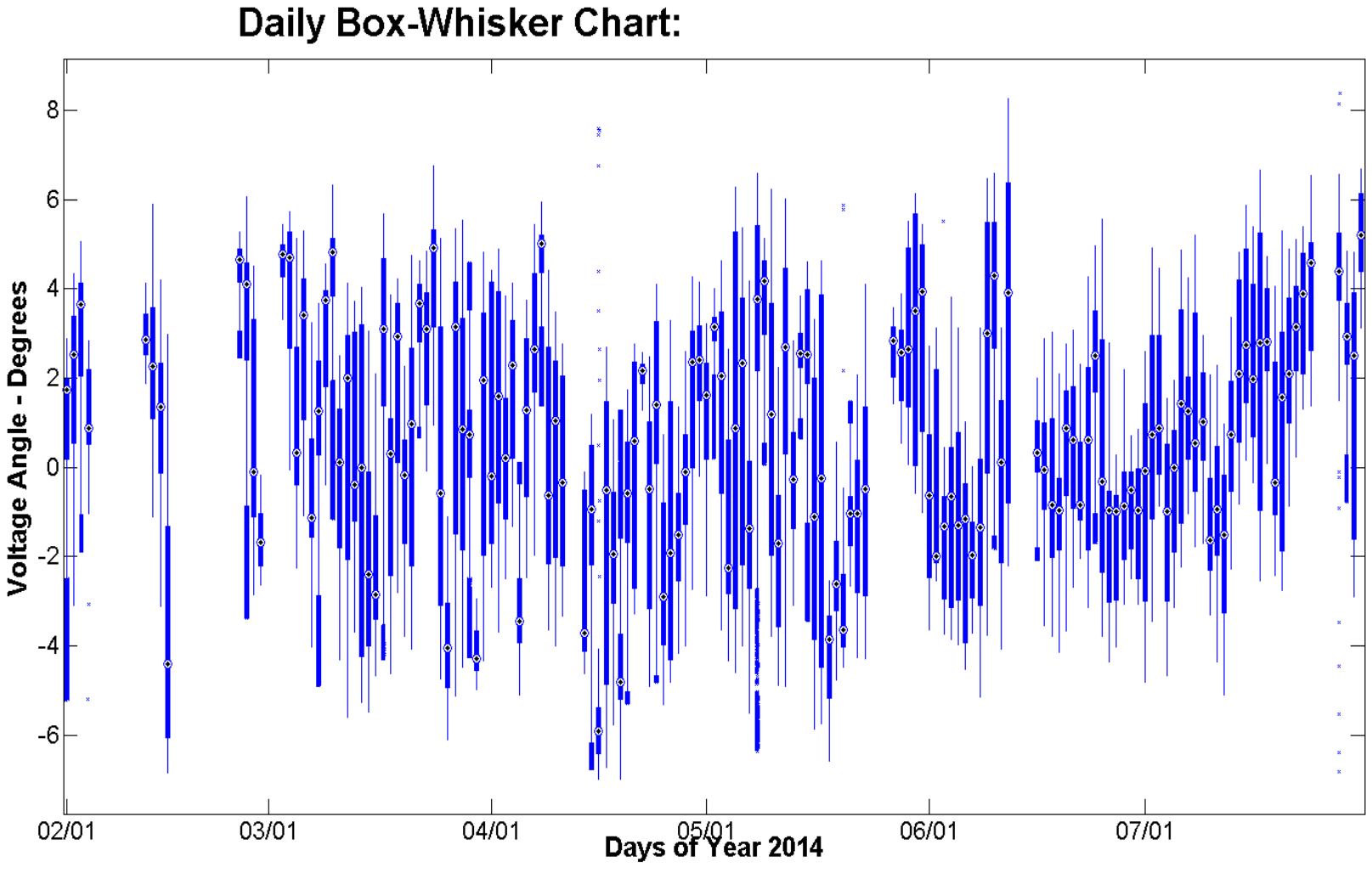
FarWest 7 – FarWest 8



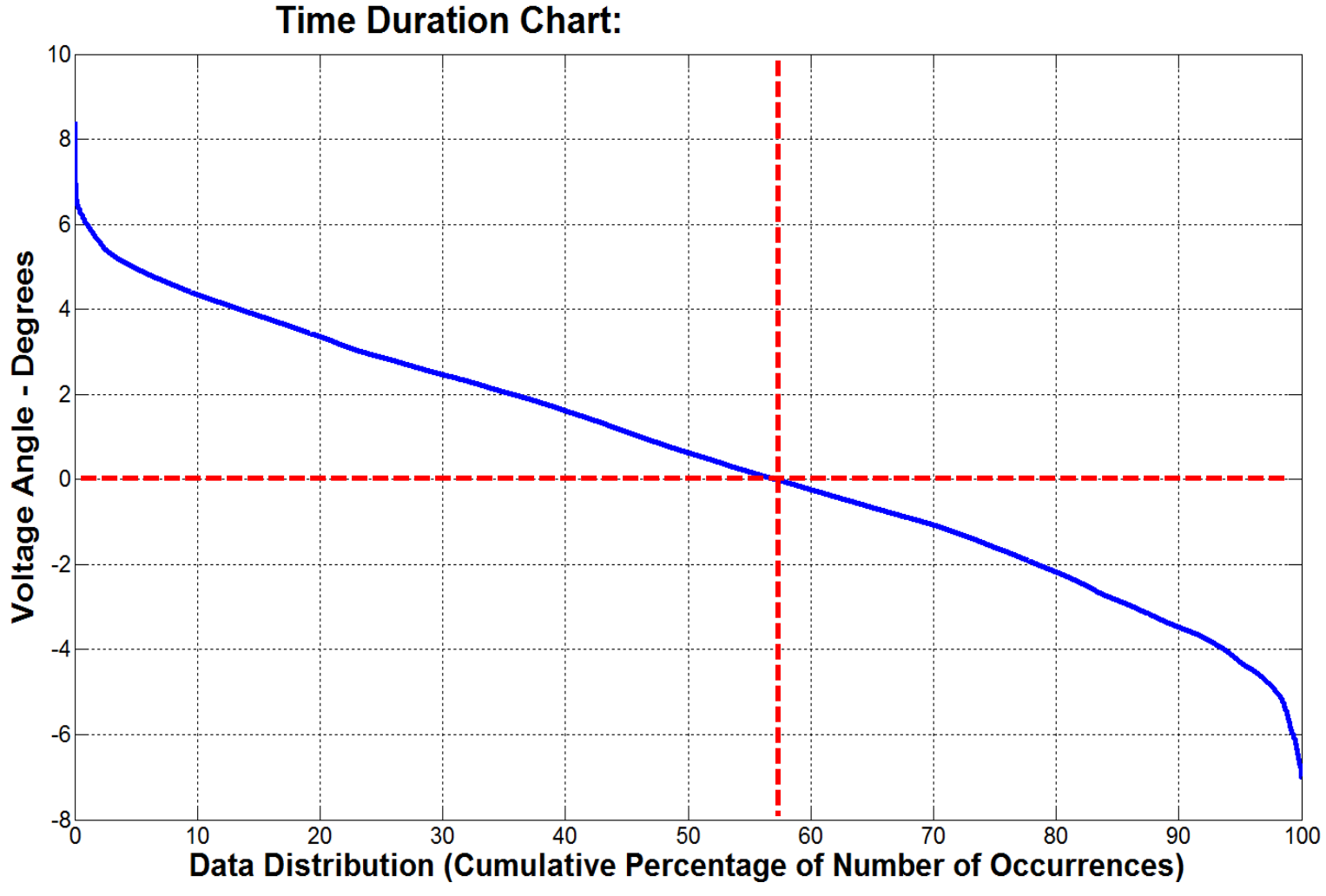
FarWest 7 – FarWest 8



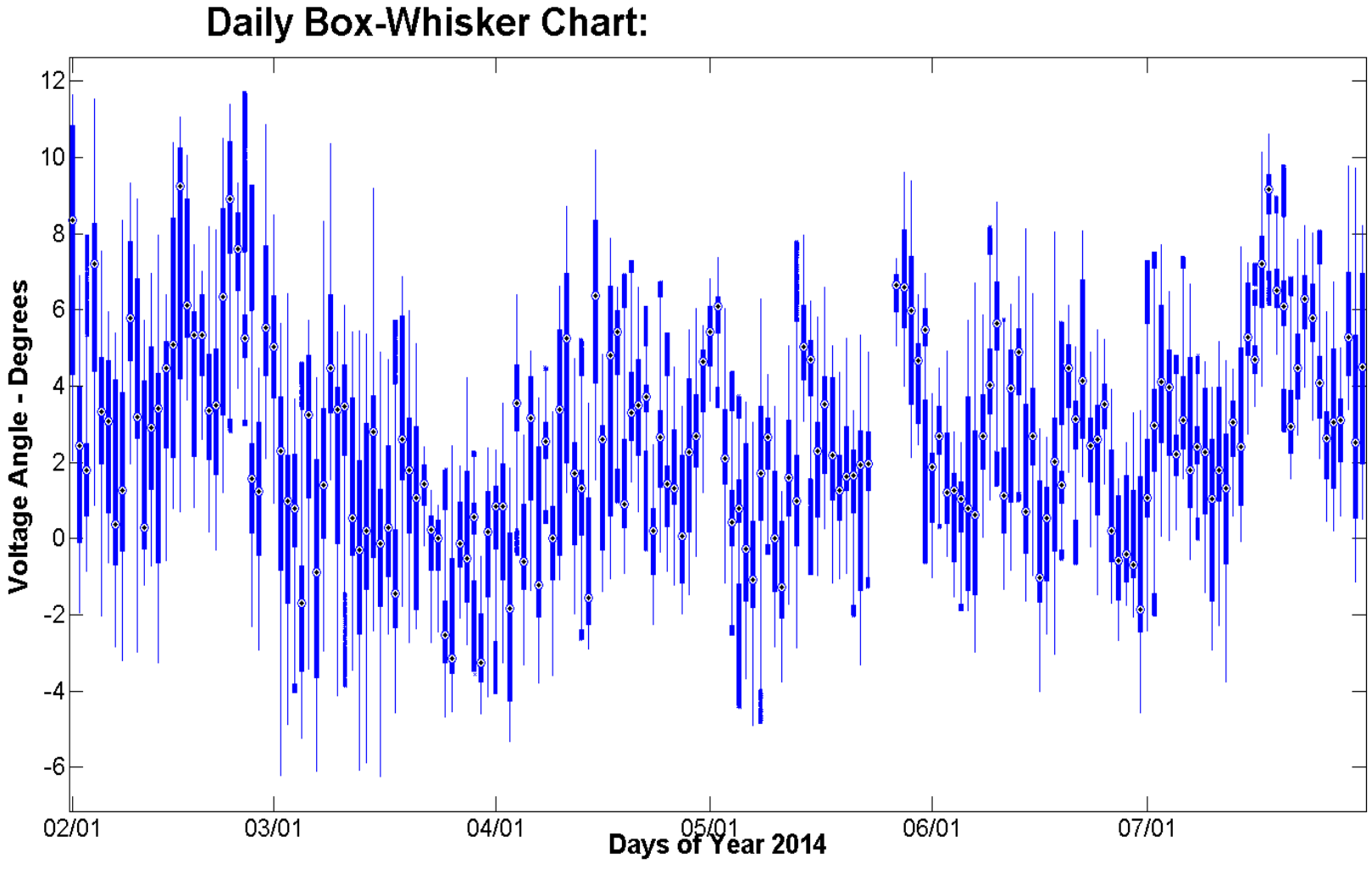
FarWest 7 – FarWest 9



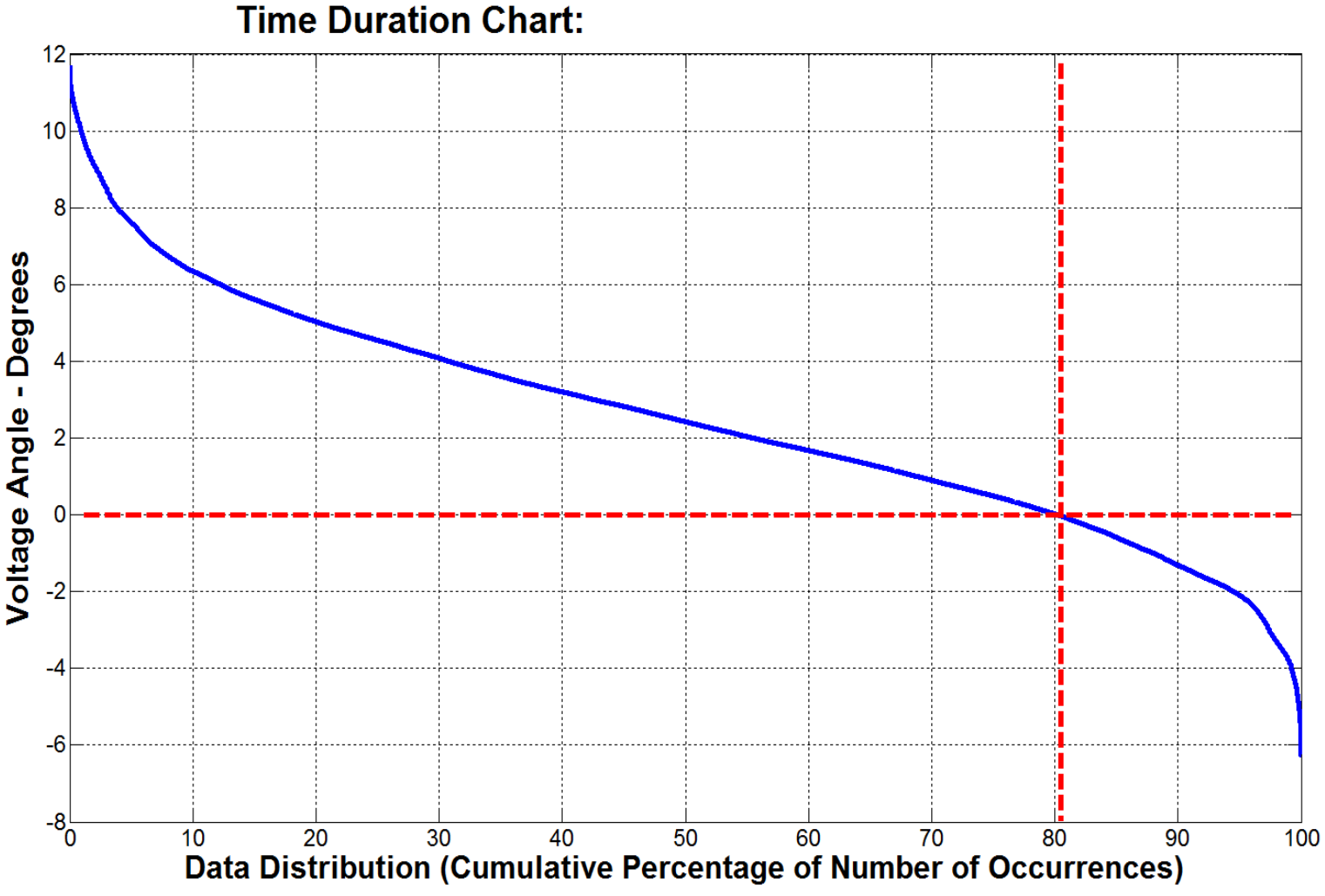
FarWest 7 – FarWest 9



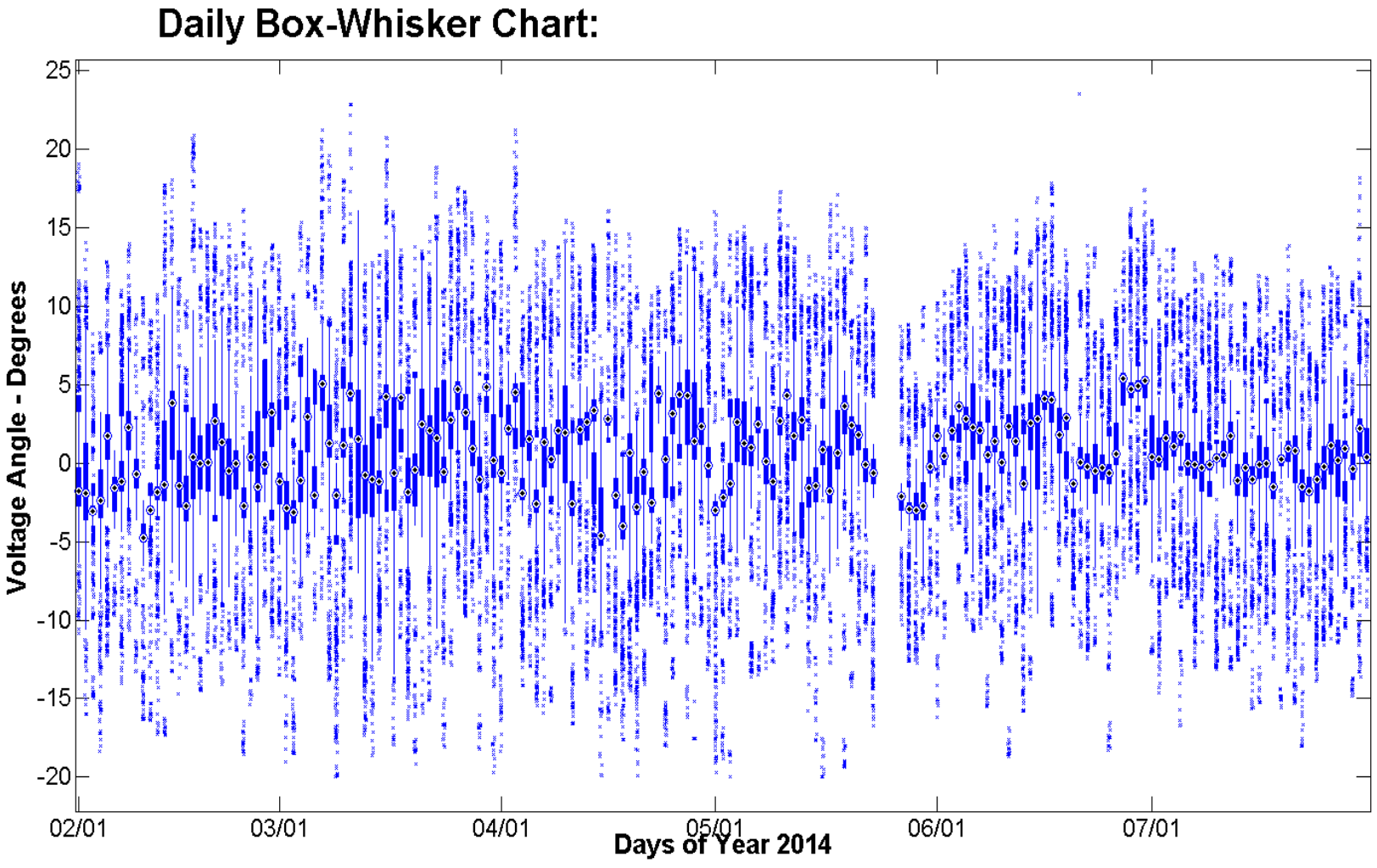
West 12 – FarWest 7



West 12 – FarWest 7

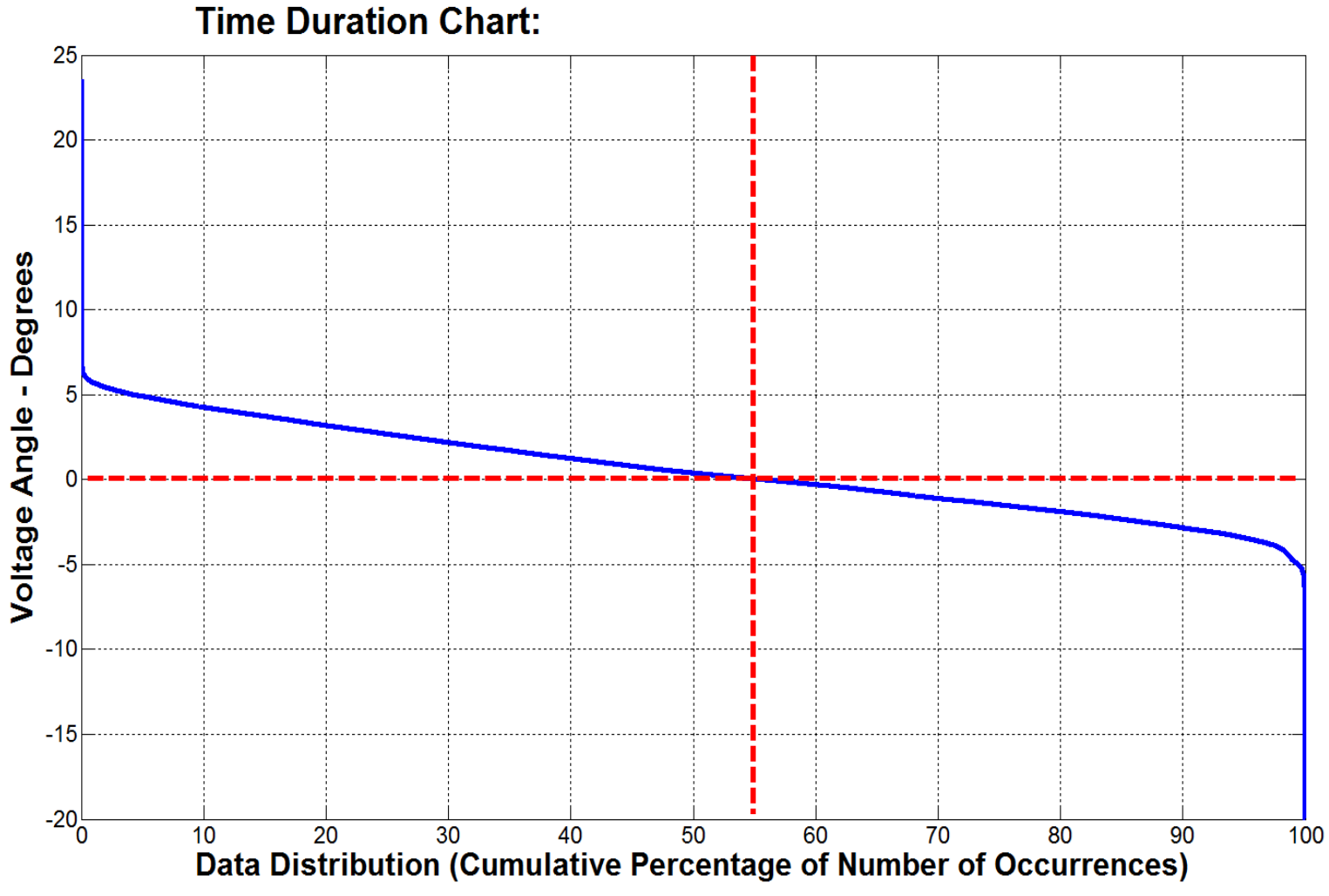


West 12 – West 1*

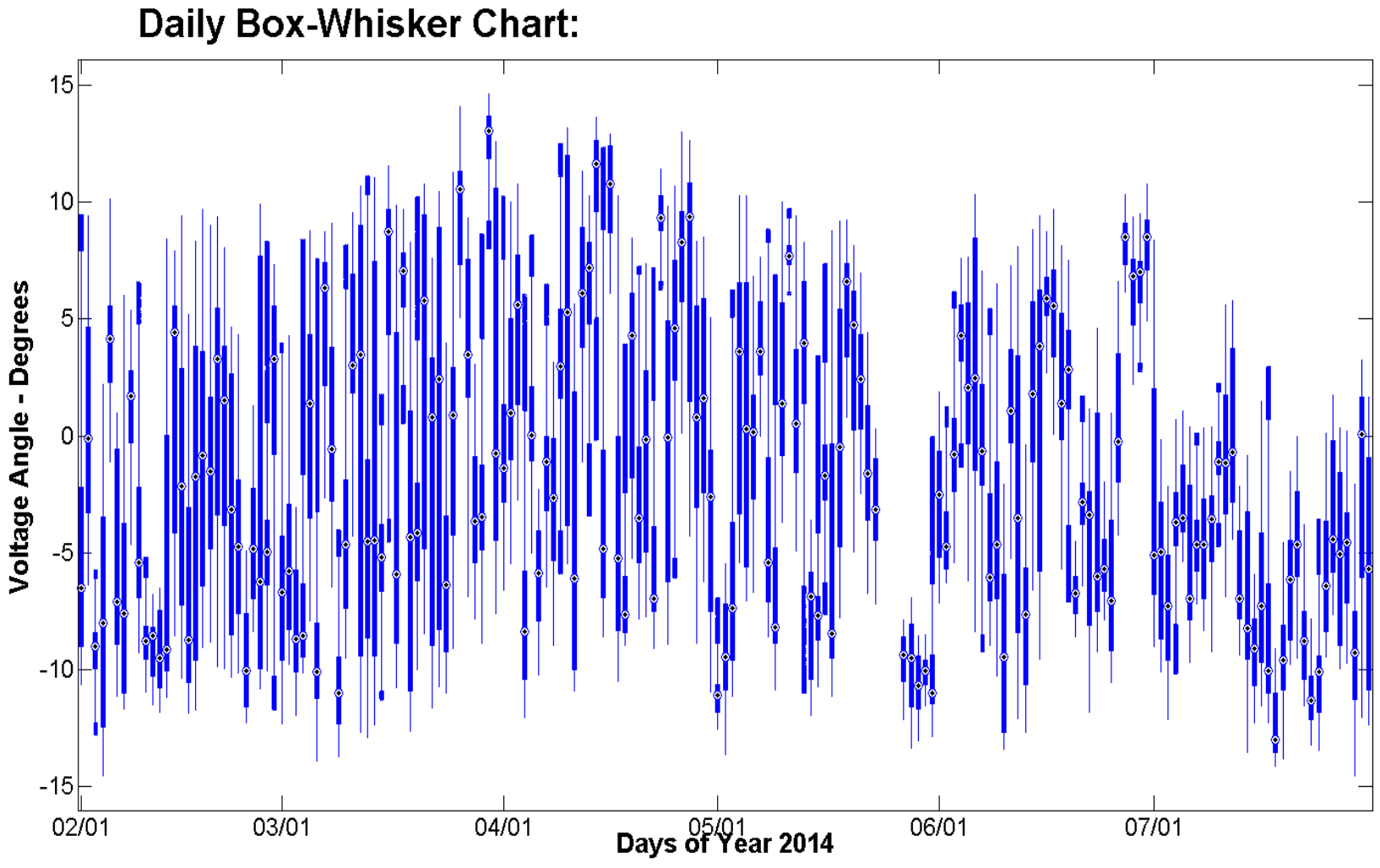


* West 1 PMU has noisy signal

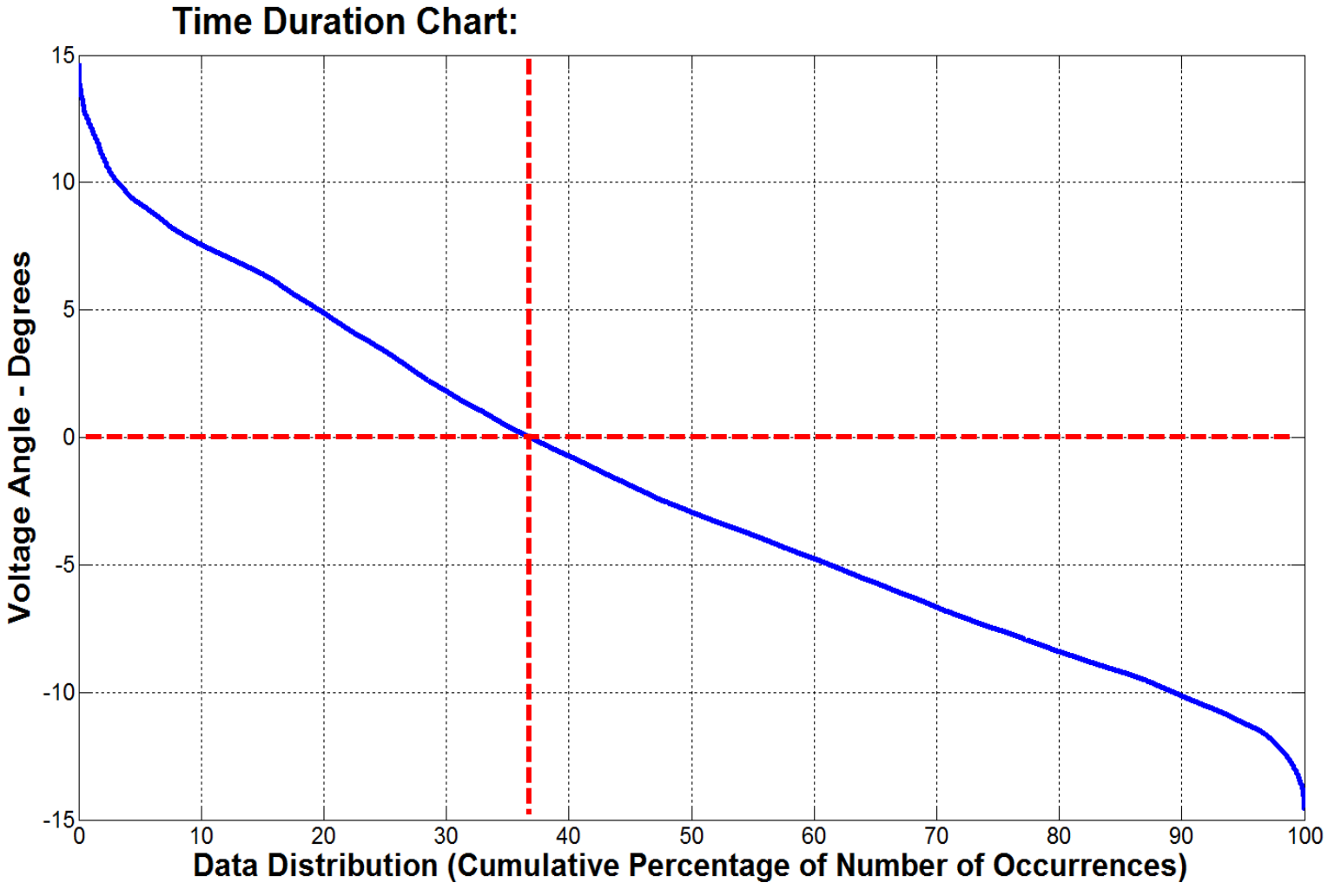
West 12 – West 1



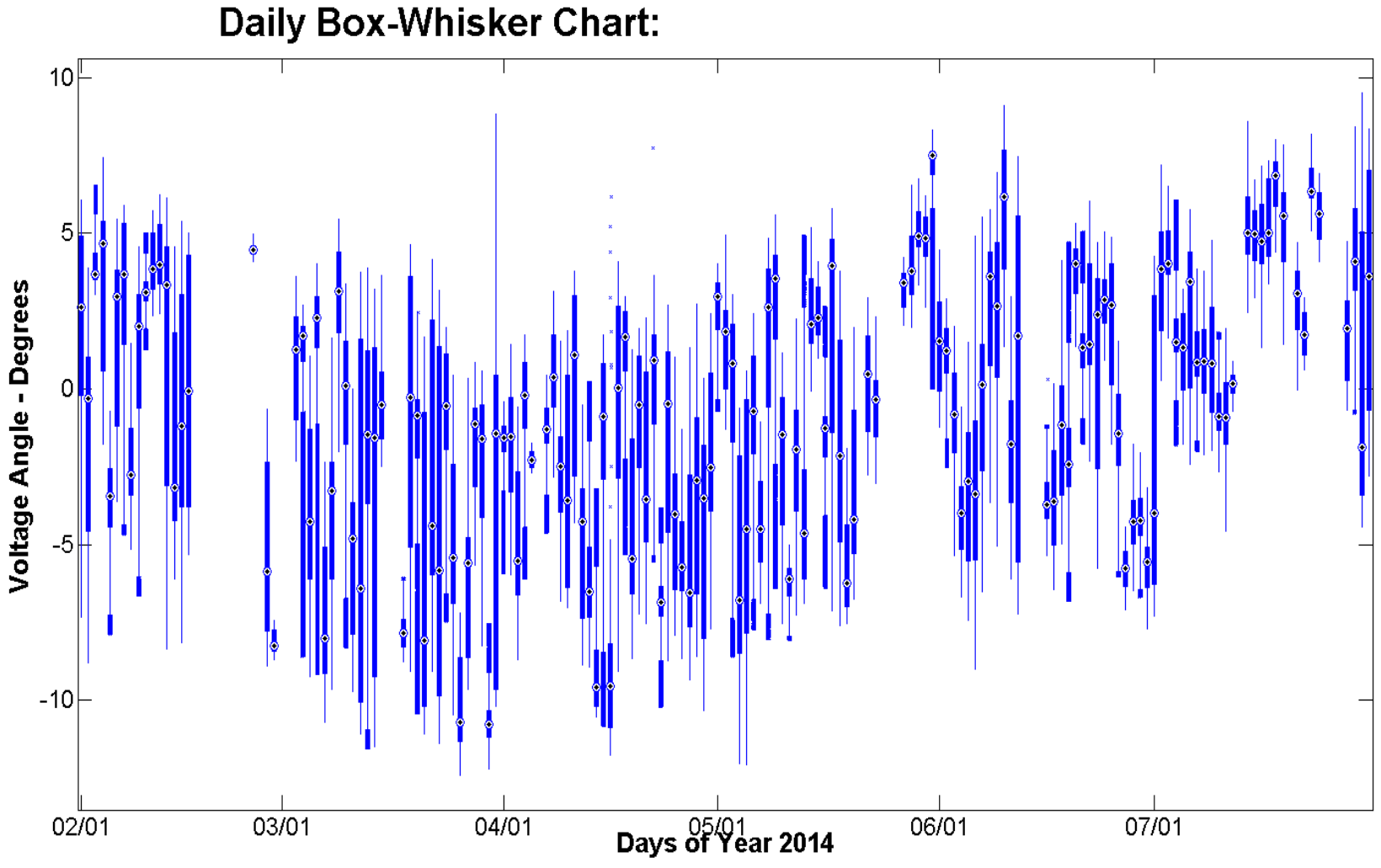
West 12 – North 1



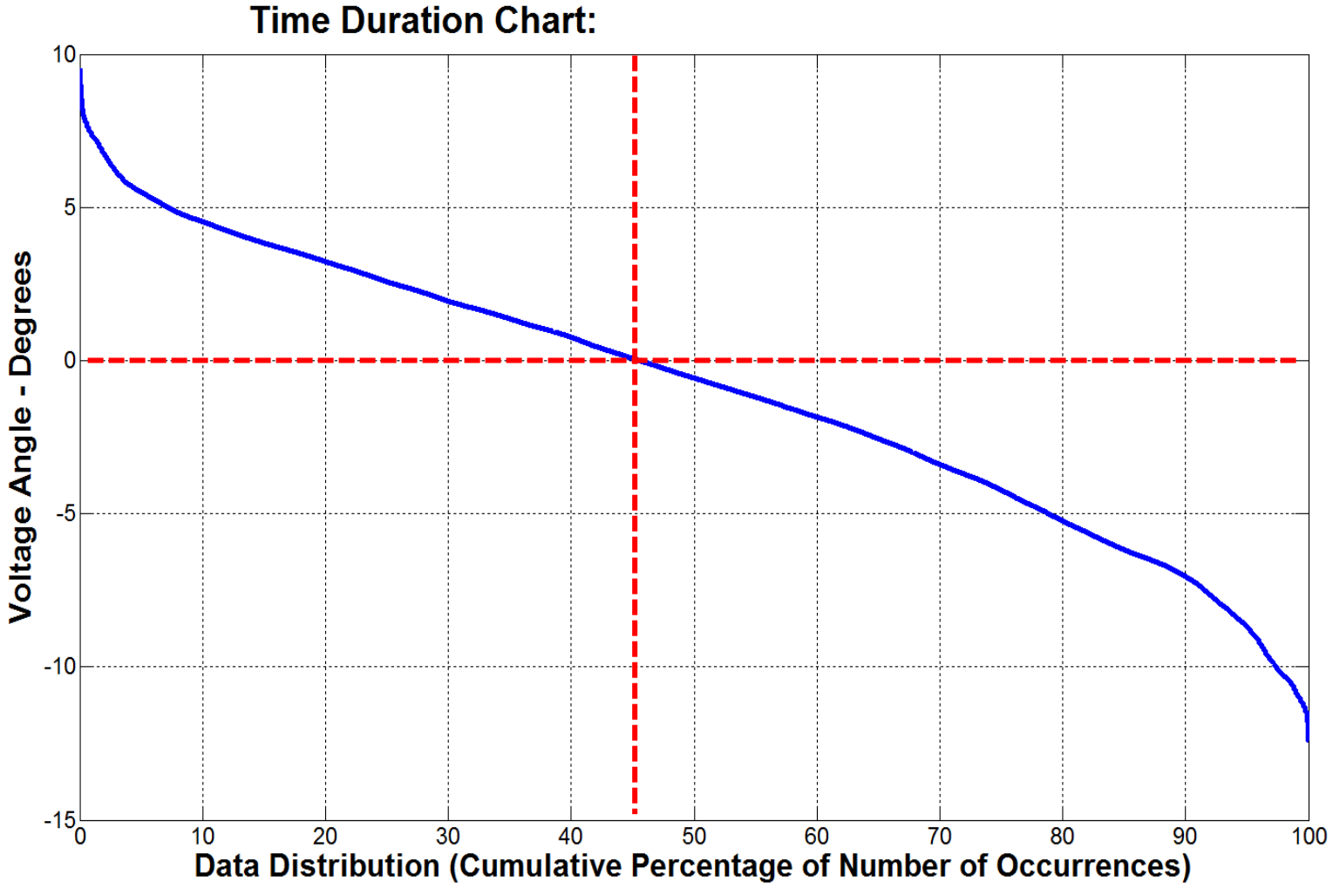
West 12 – North 1



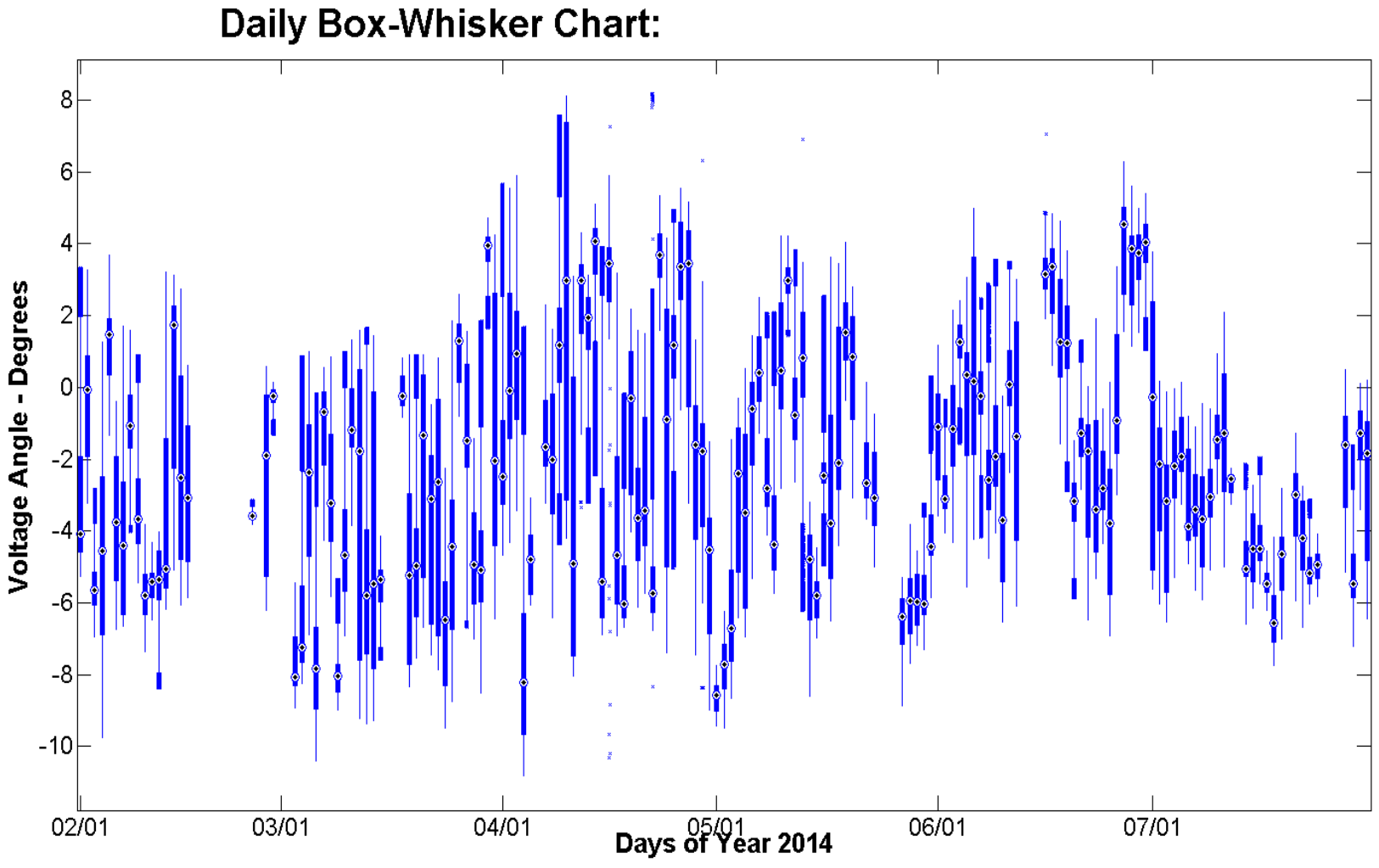
West 14 – West 5



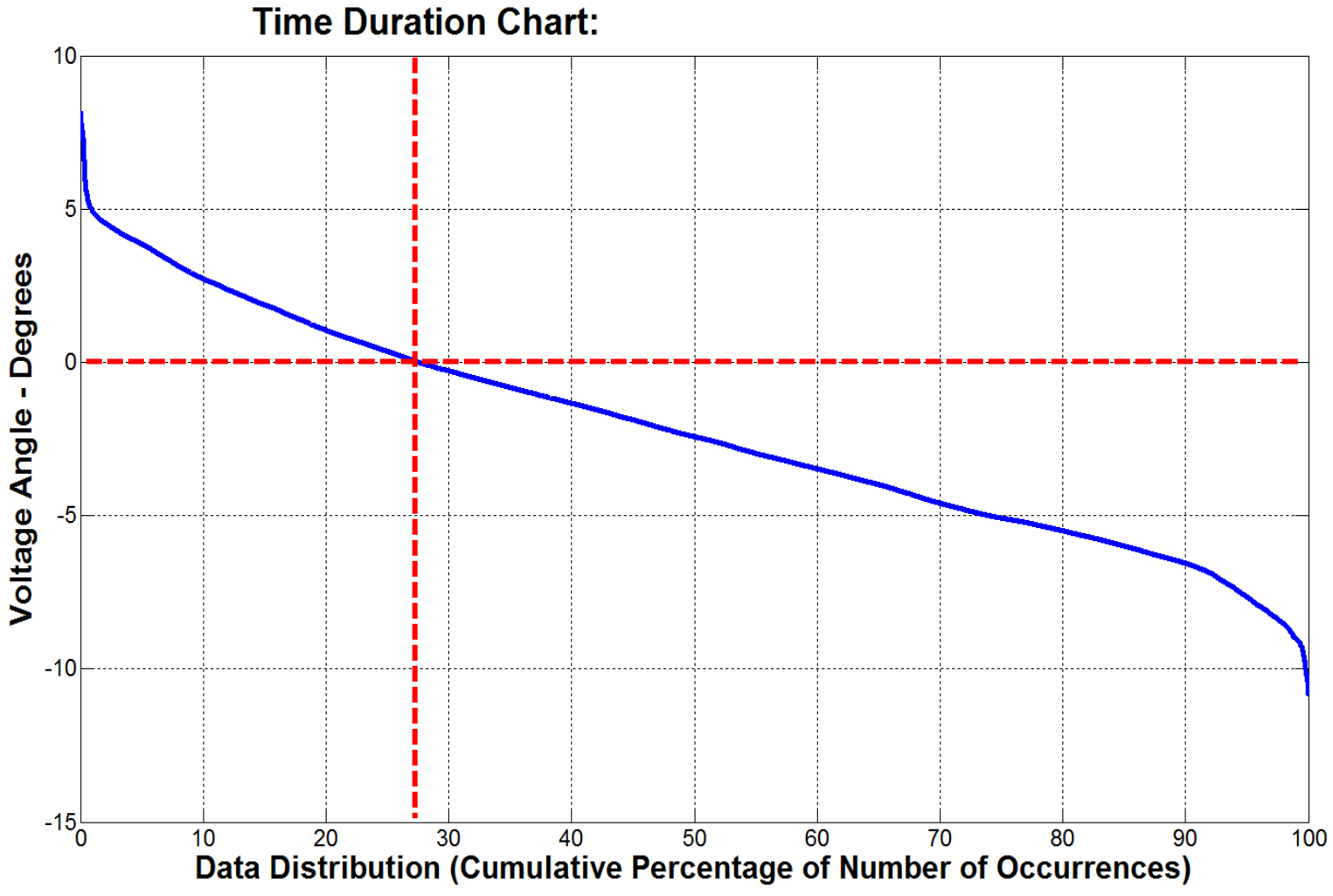
West 14 – West 5



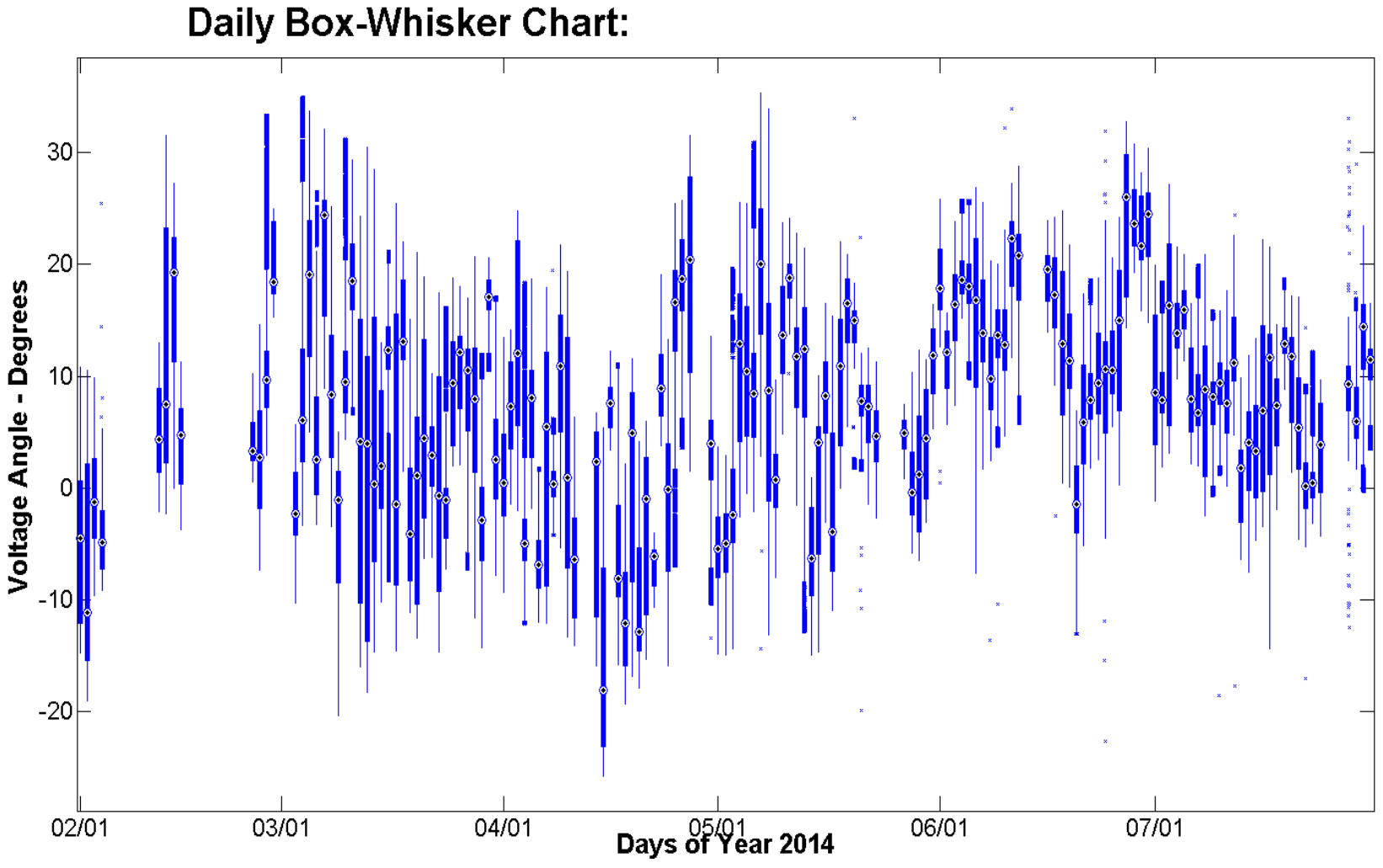
West 14 – North 1



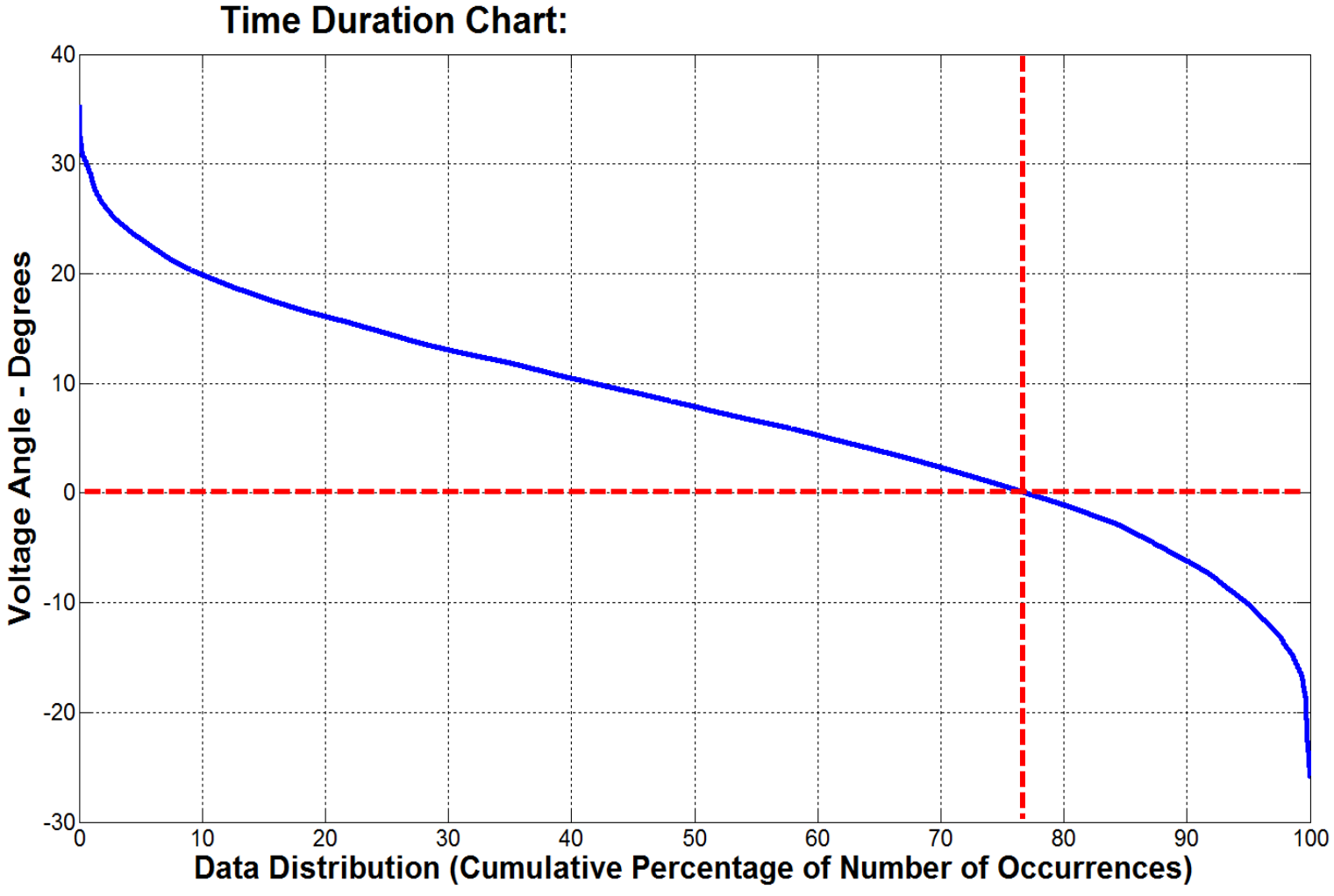
West 14 – North 1



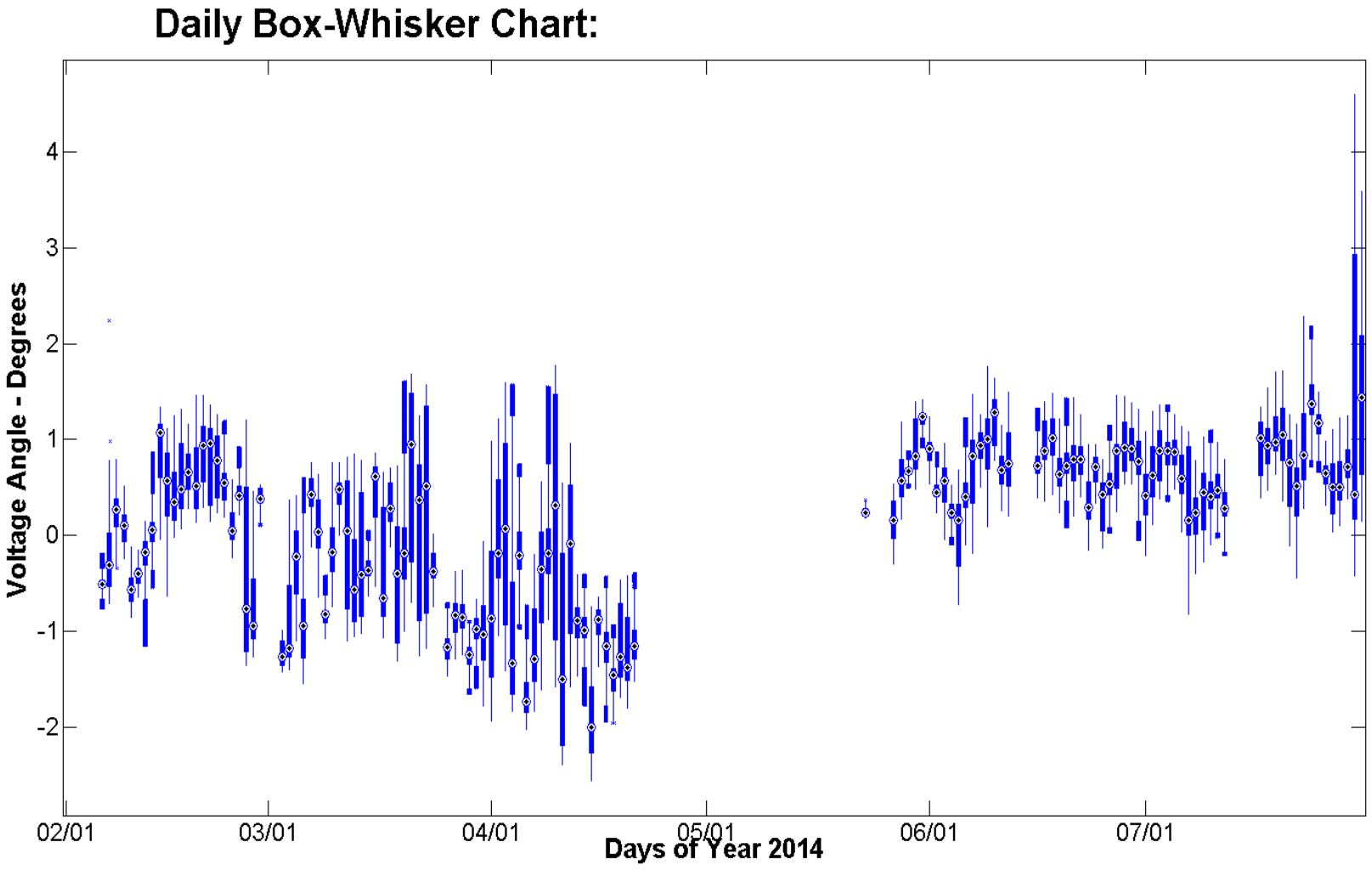
FarWest 9 – West 4



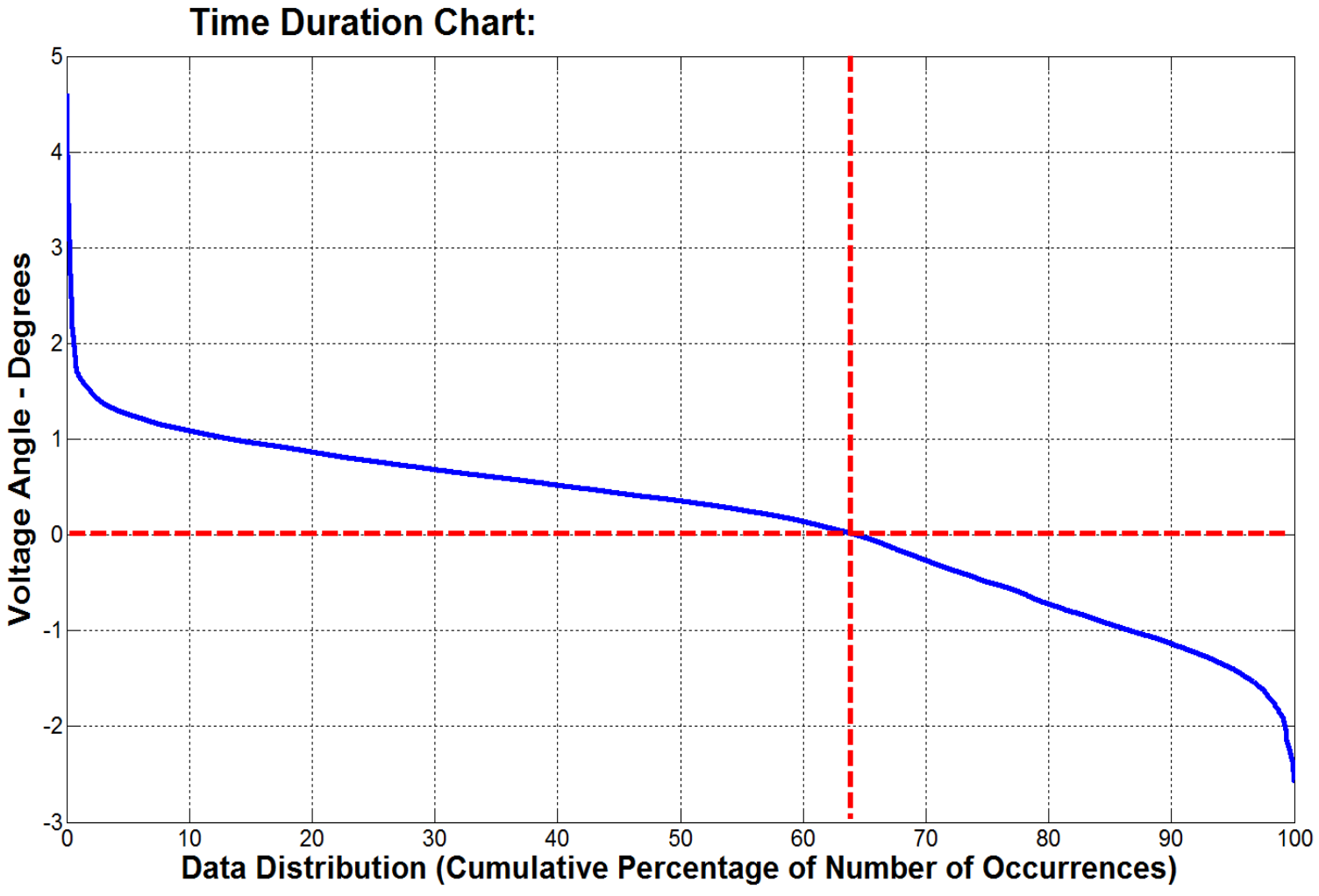
FarWest 9 – West 4



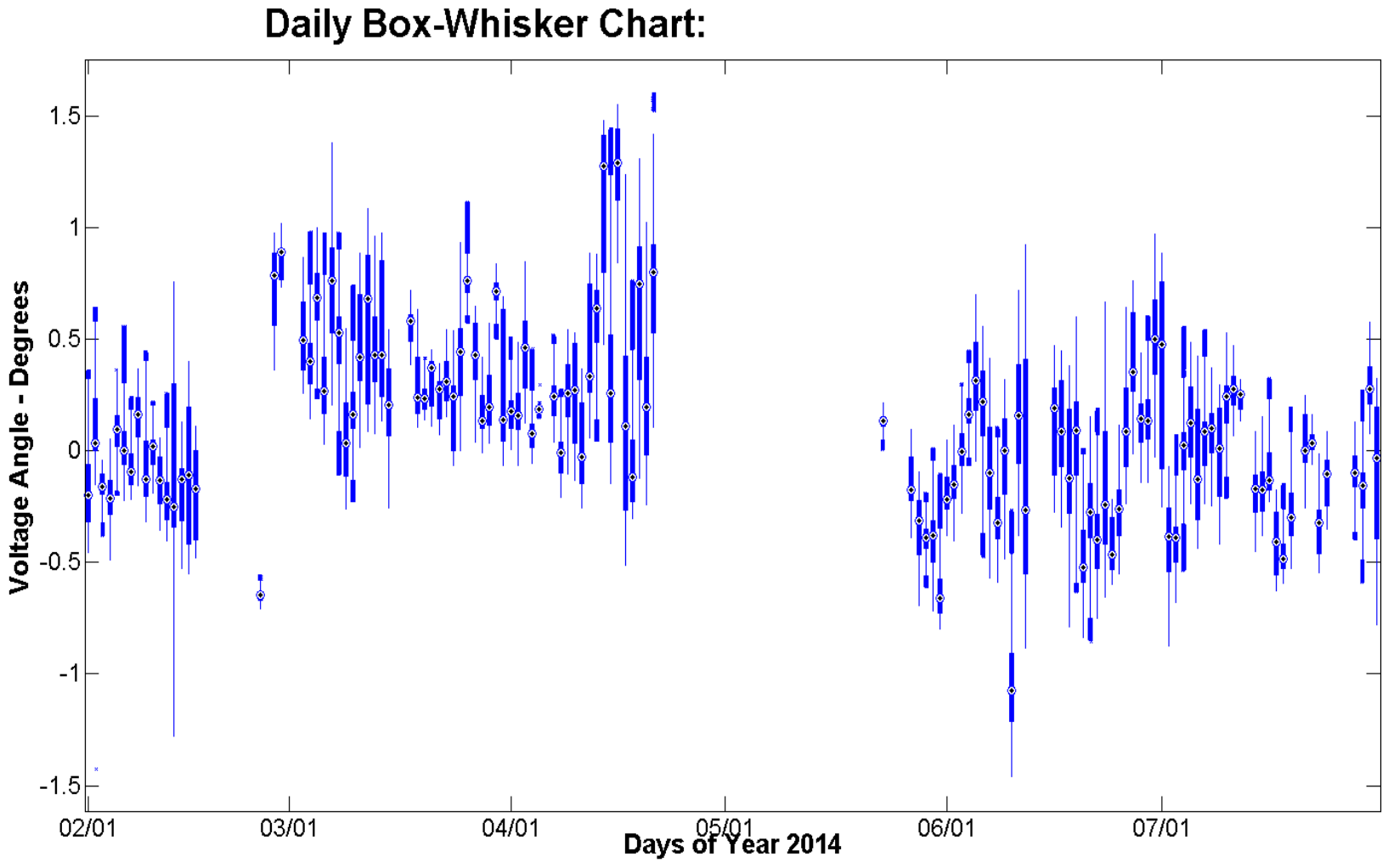
West 16 – West 3



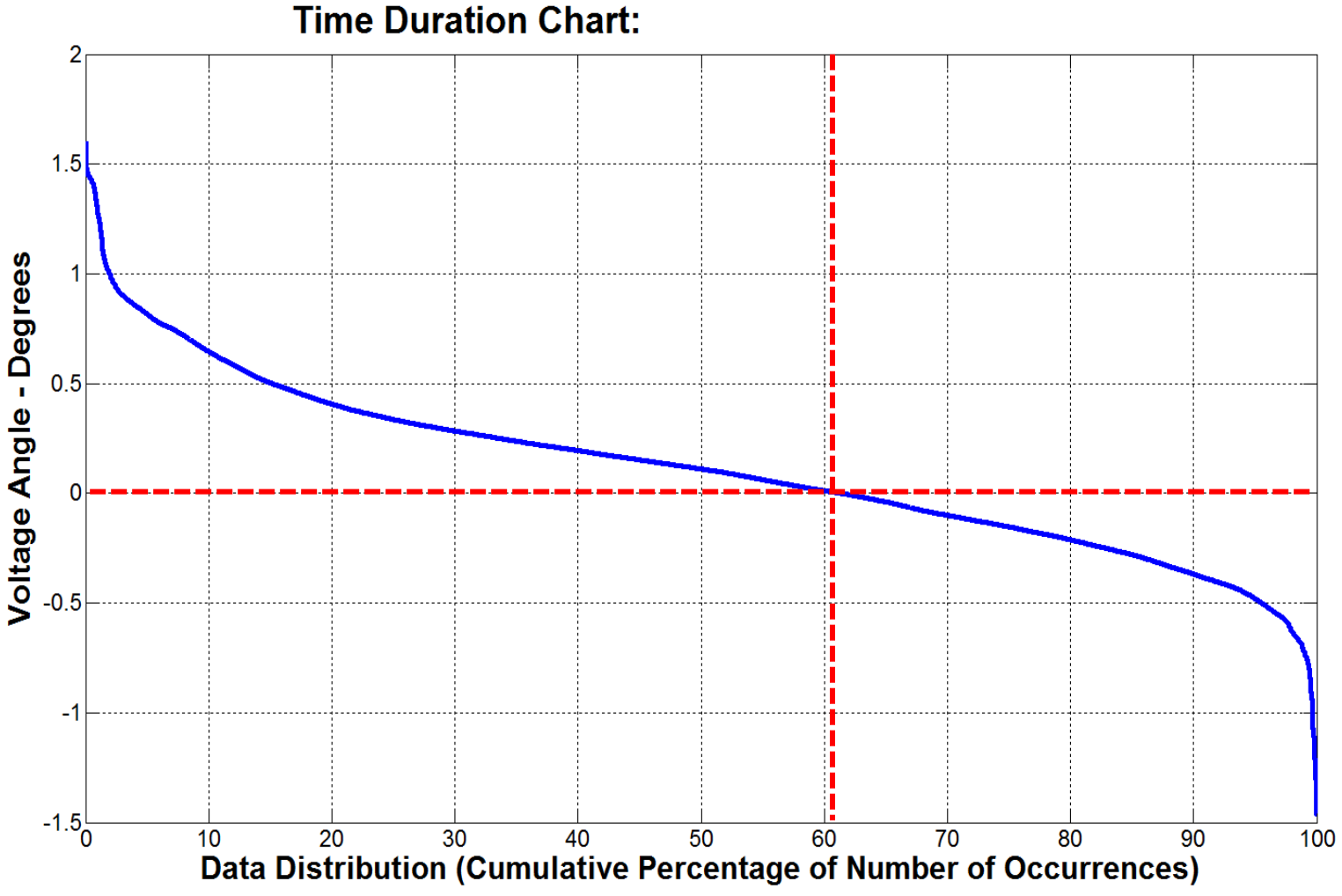
West 16 – West 3



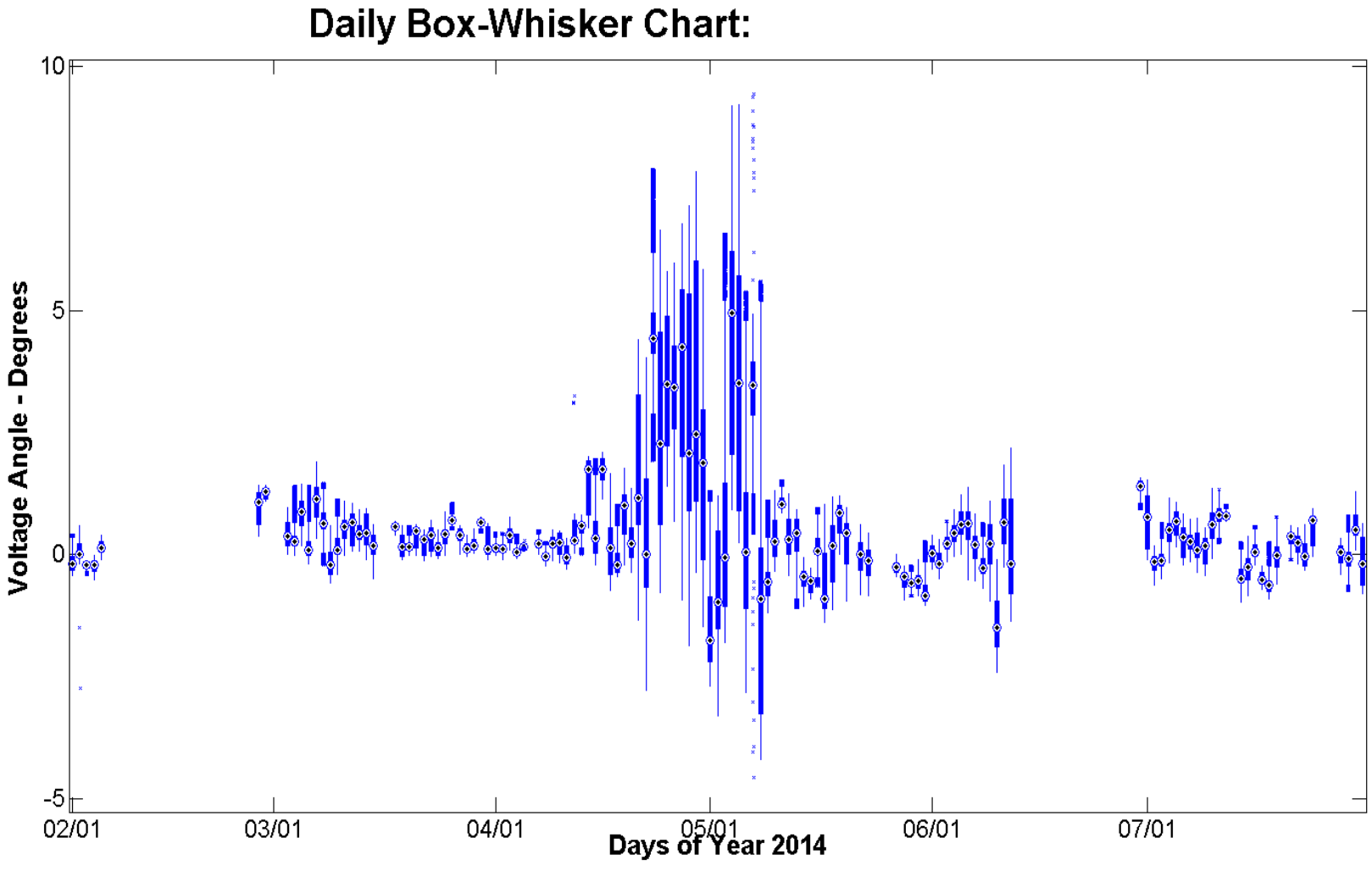
West 16 – West 14



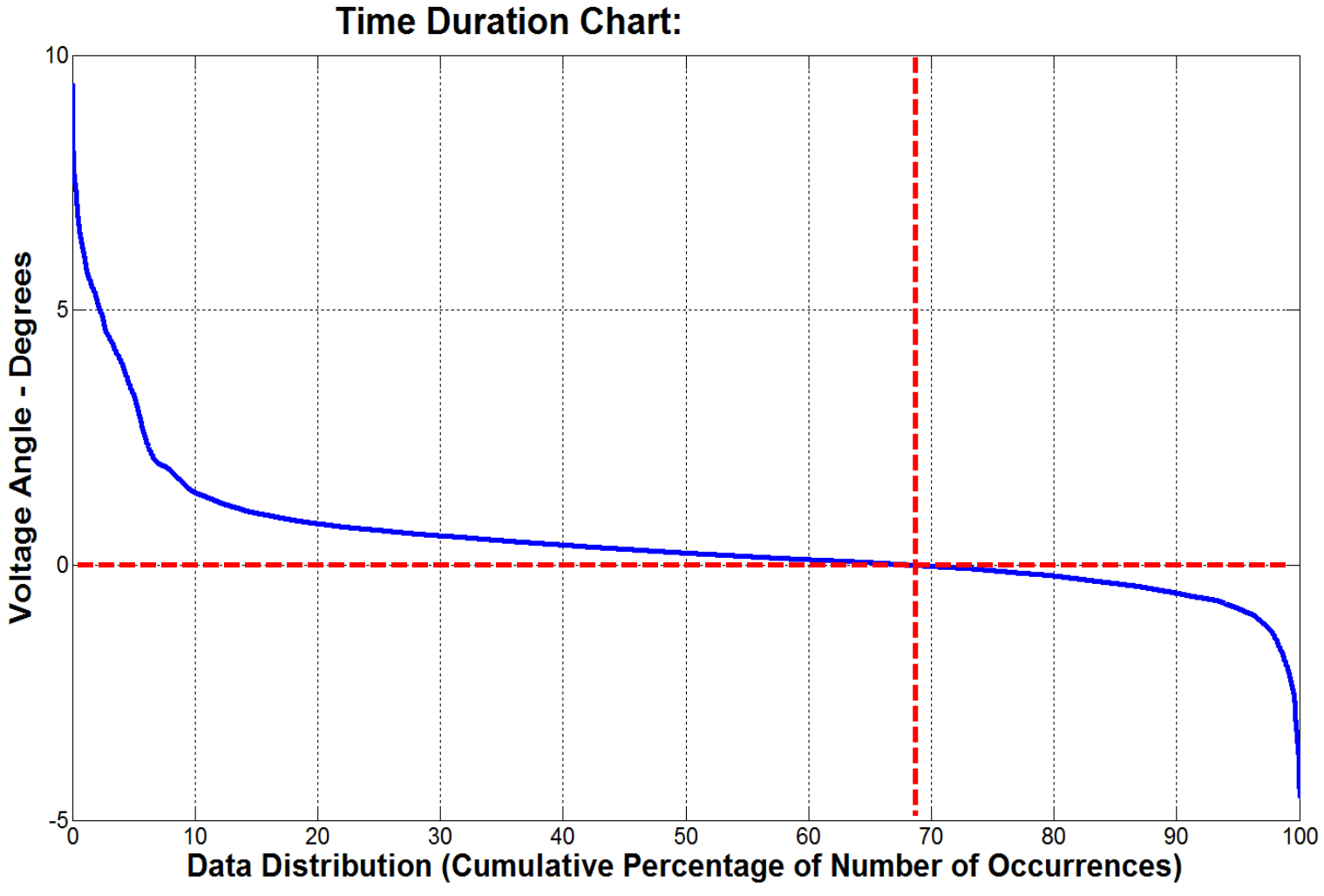
West 16 – West 14



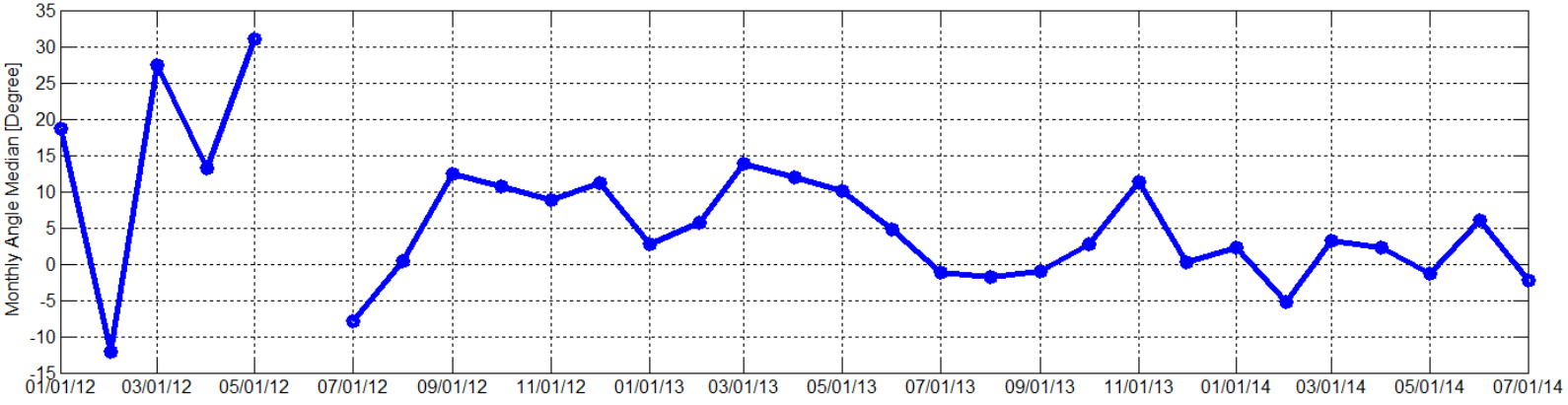
West 15 – West 14

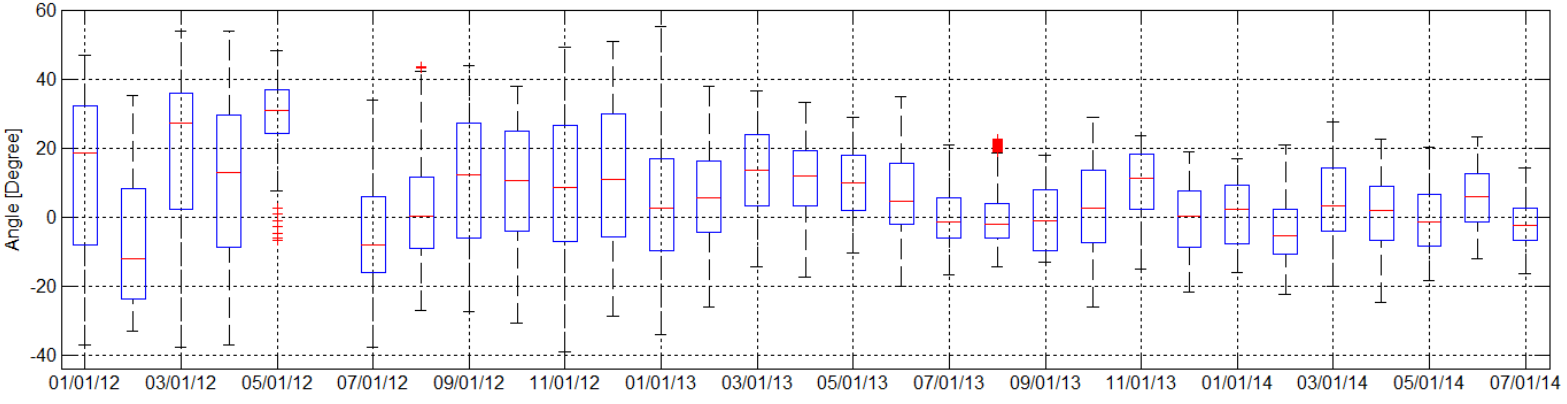


West 15 – West 14

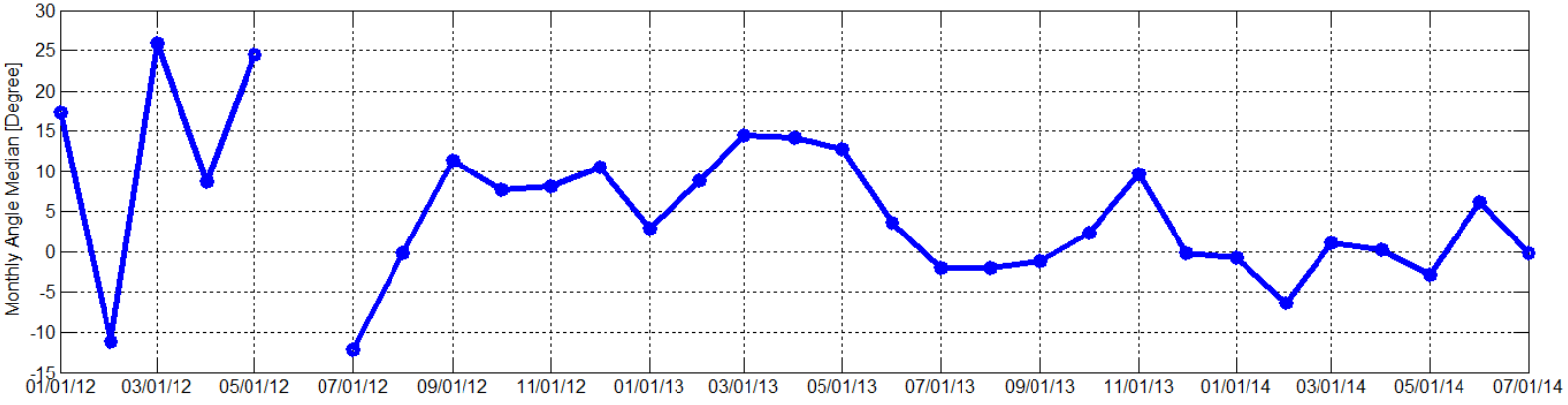


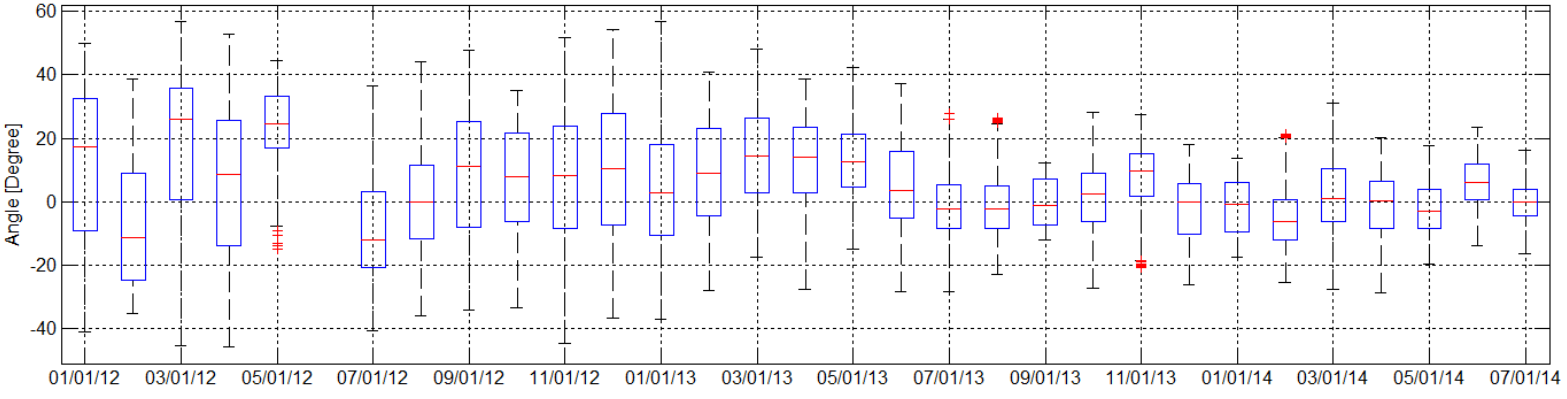
FarWest 7-North 7



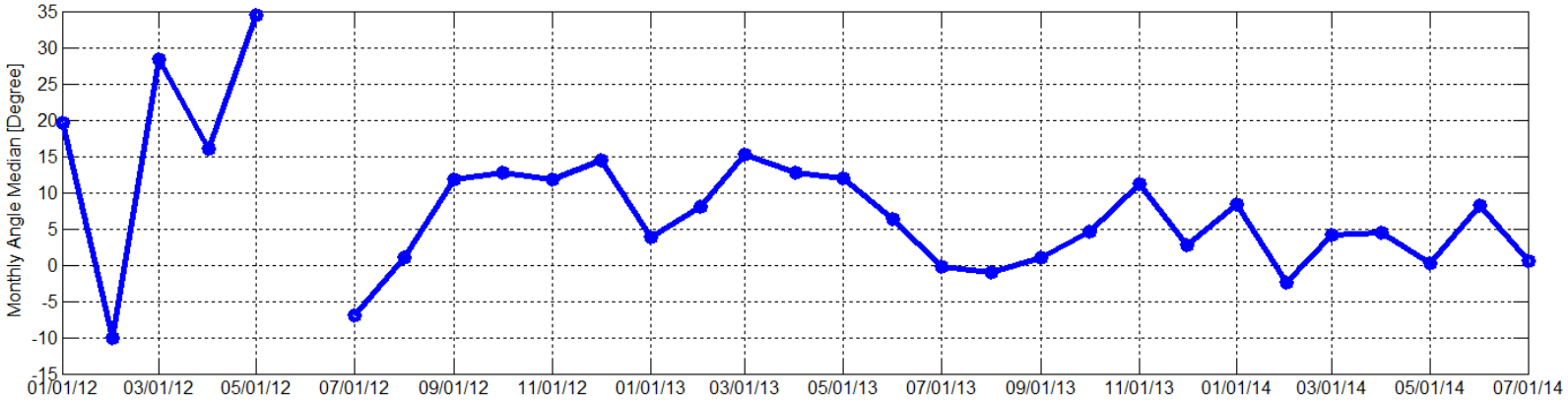


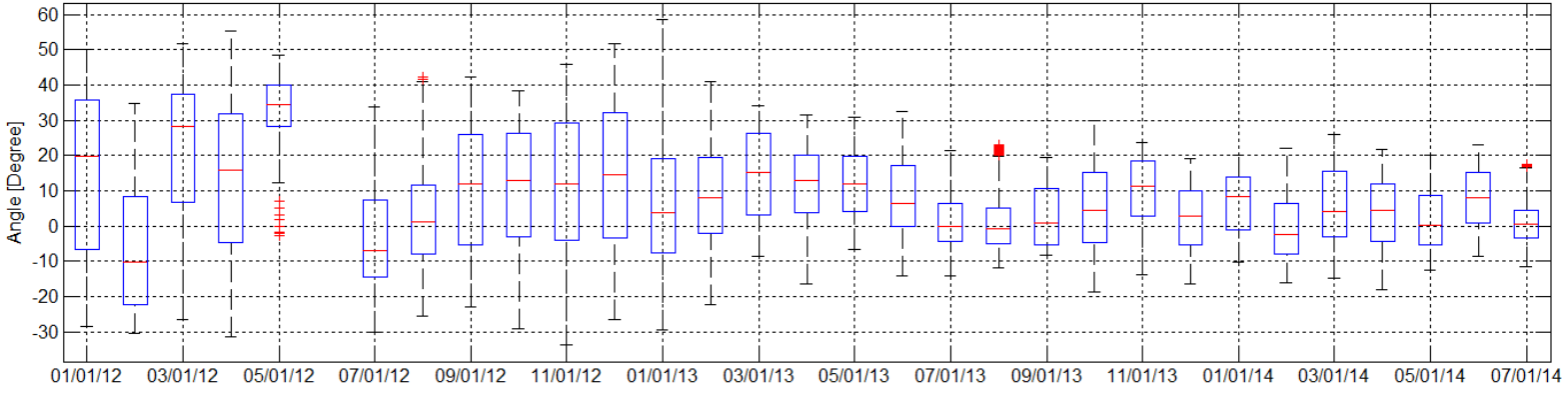
FarWest 7-South 9*



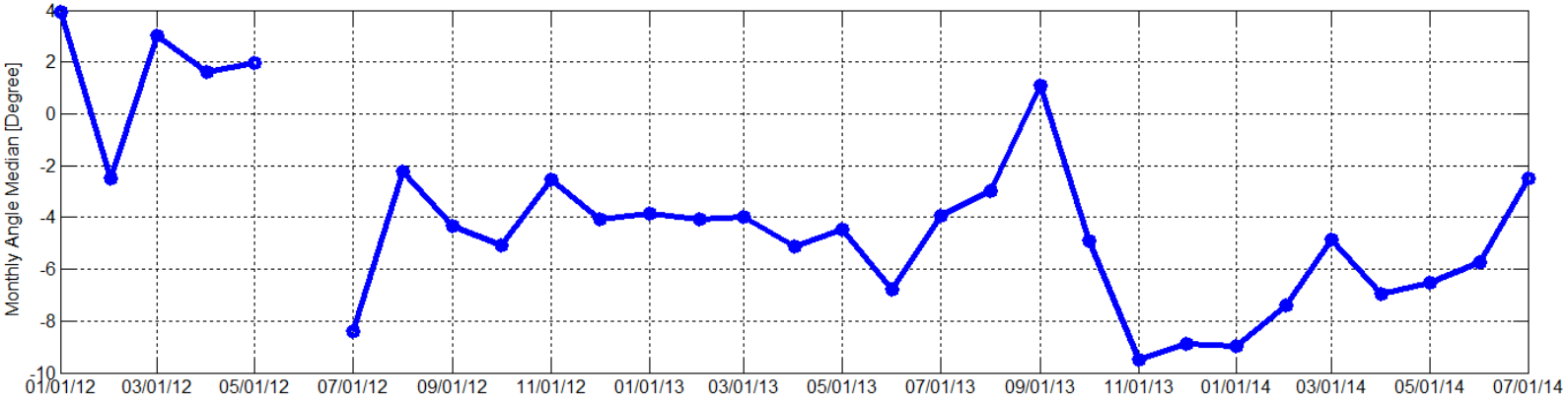


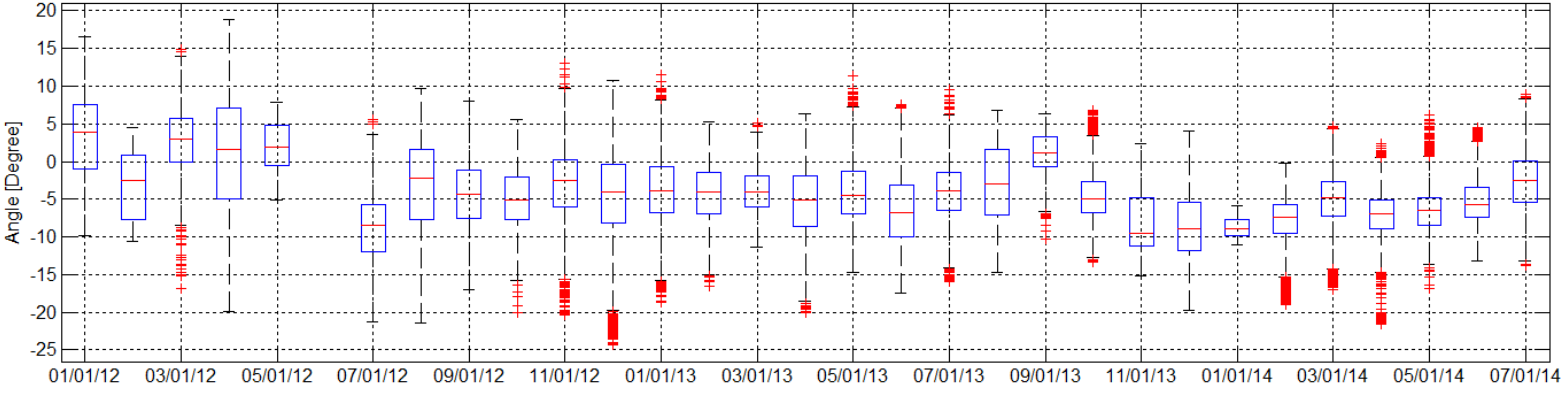
West 11-North 7



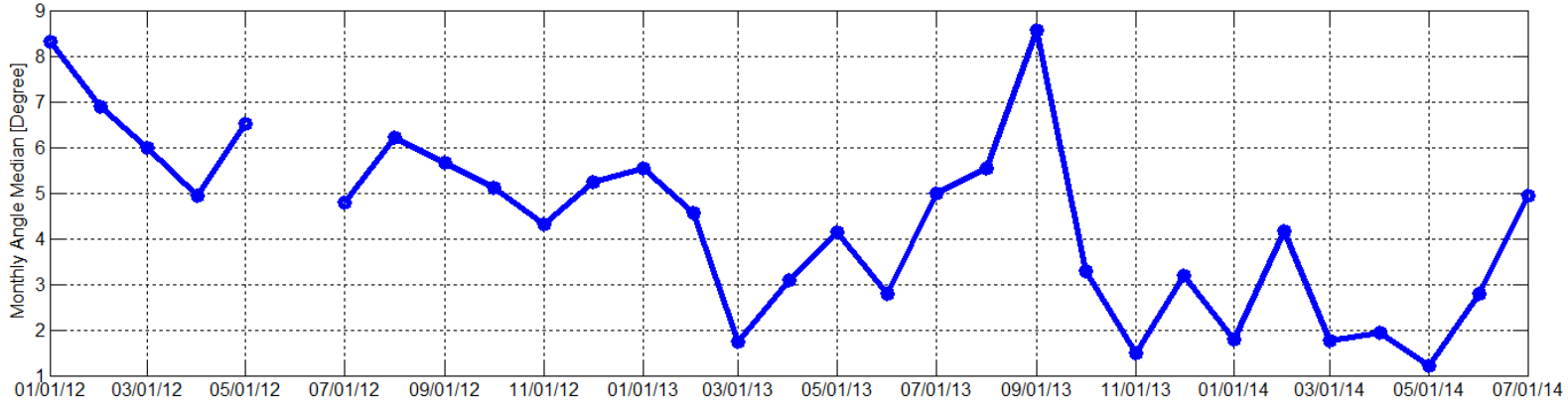


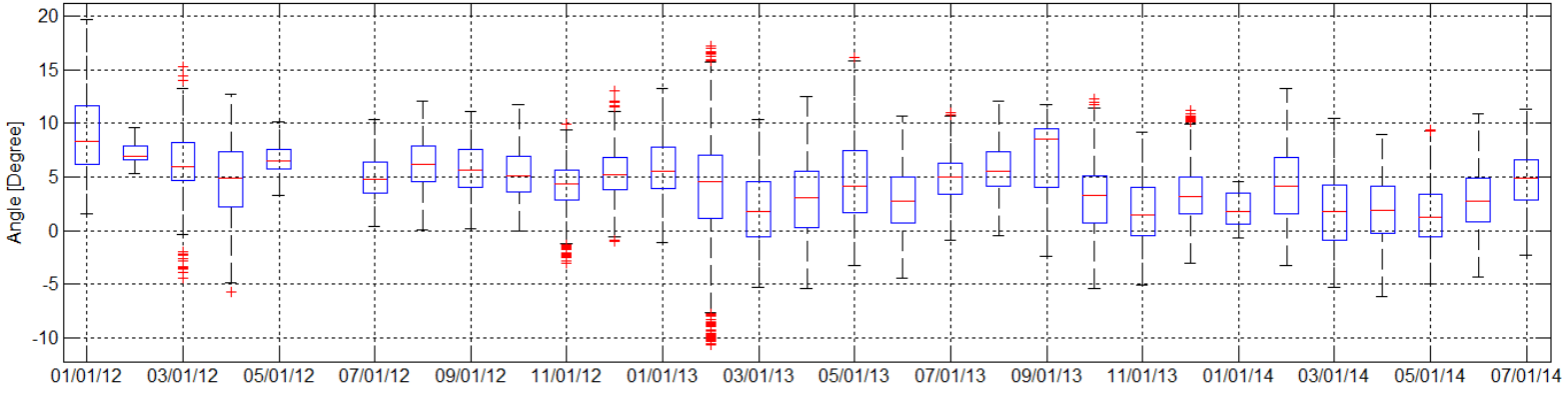
North 5-North 7



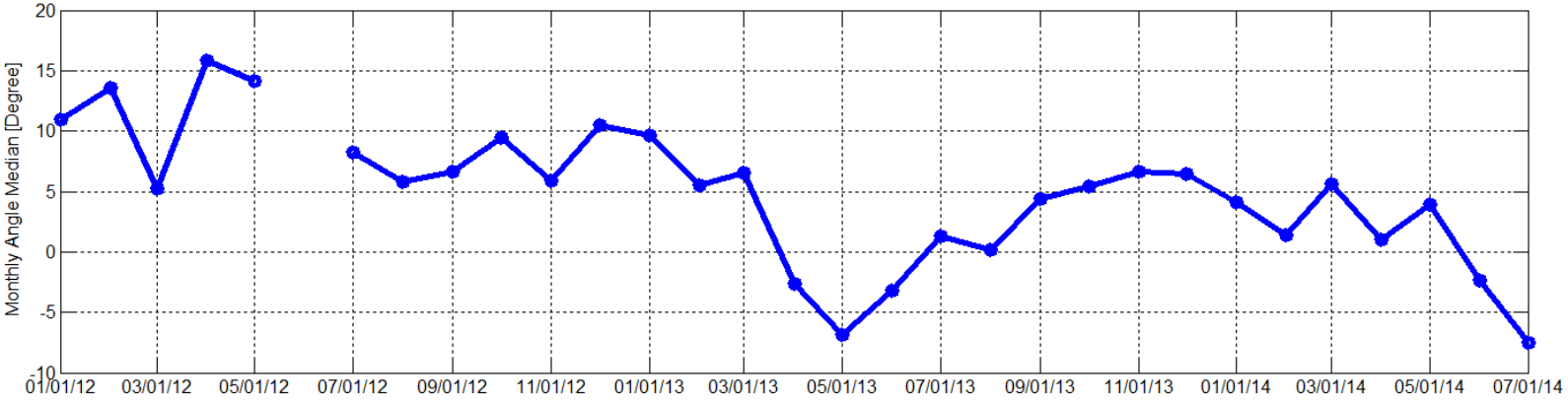


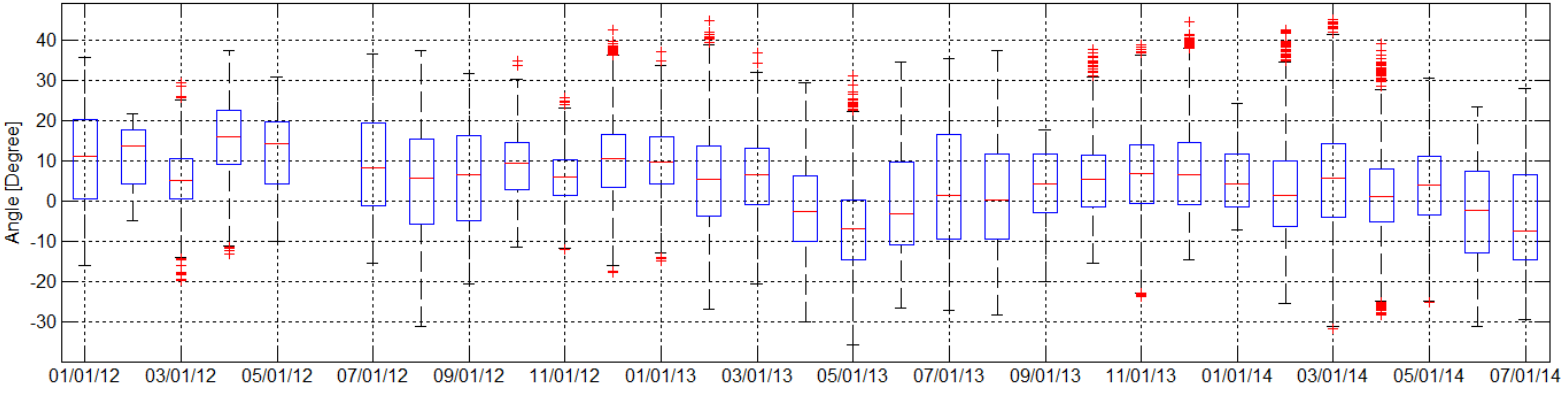
North 6-North 7



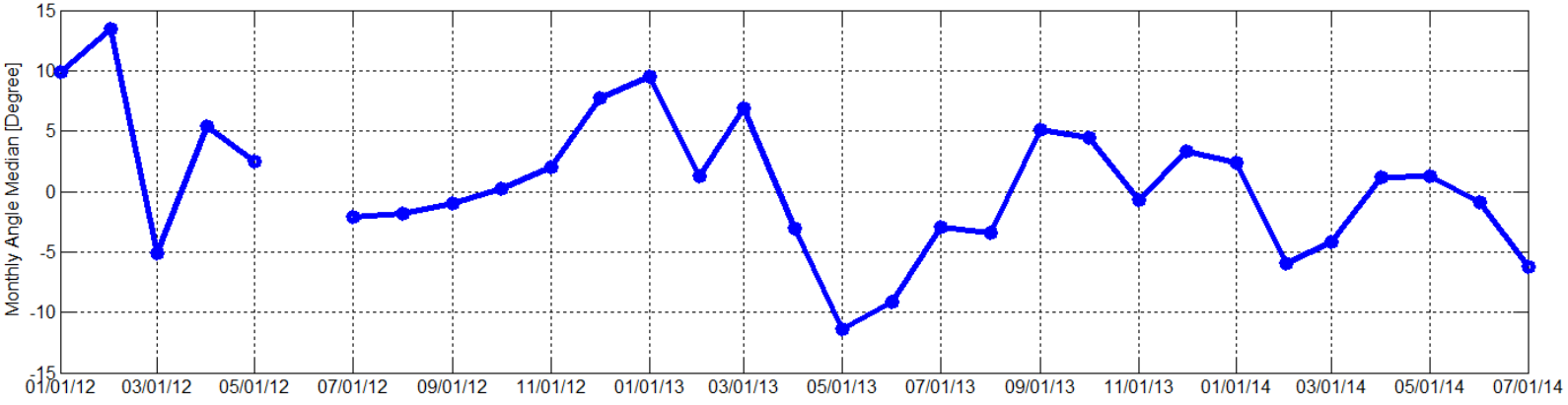


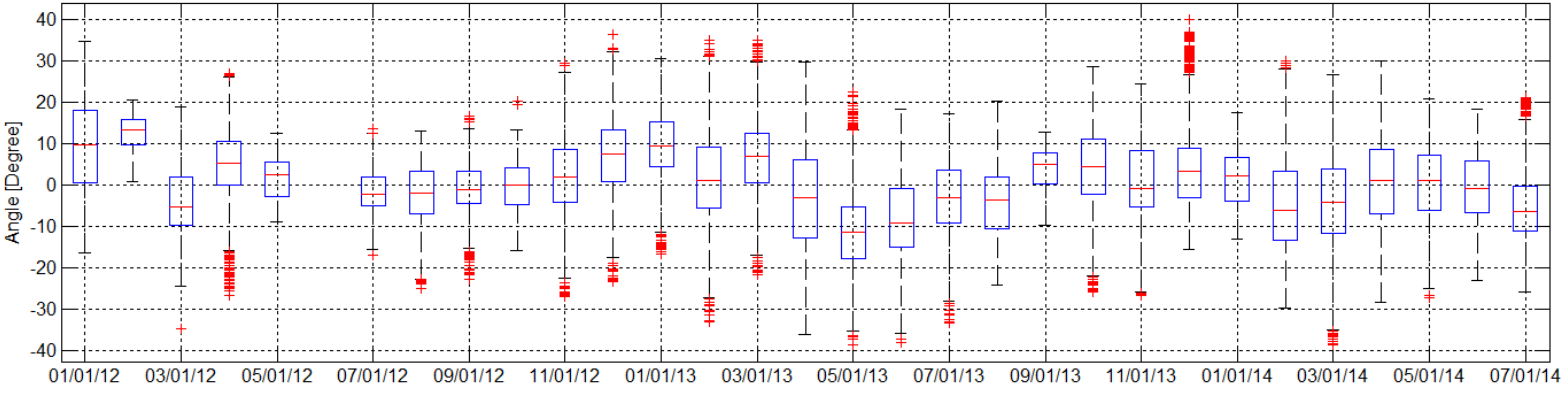
Coast 1-North 7



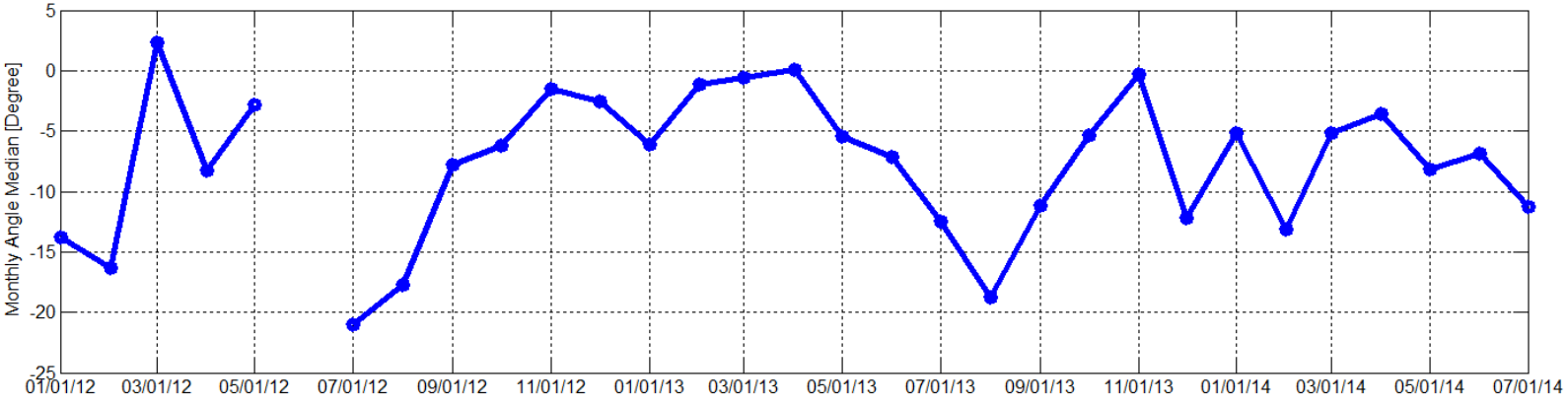


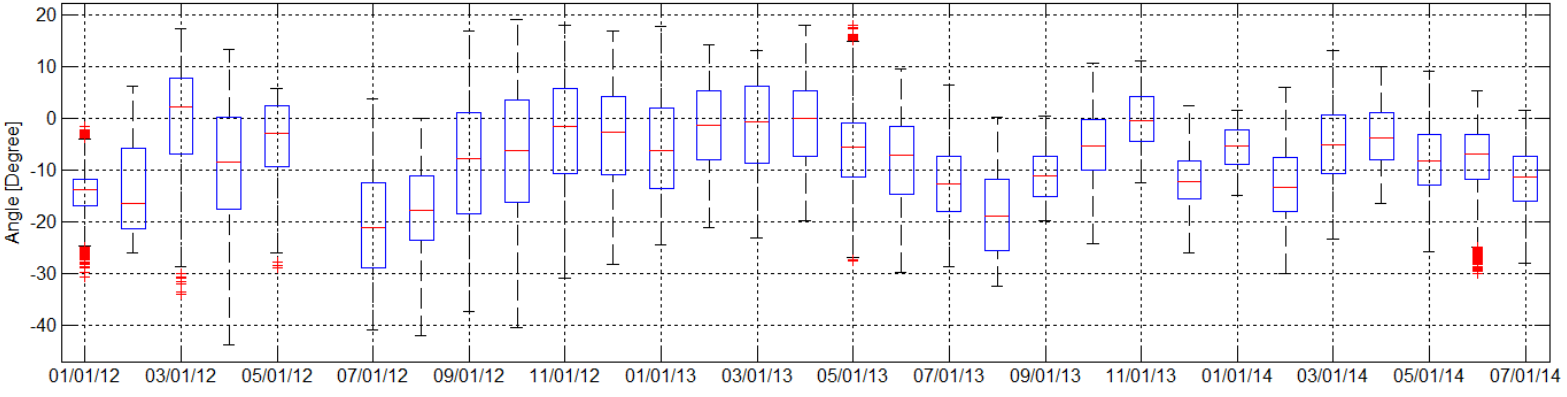
South 13-South 11*



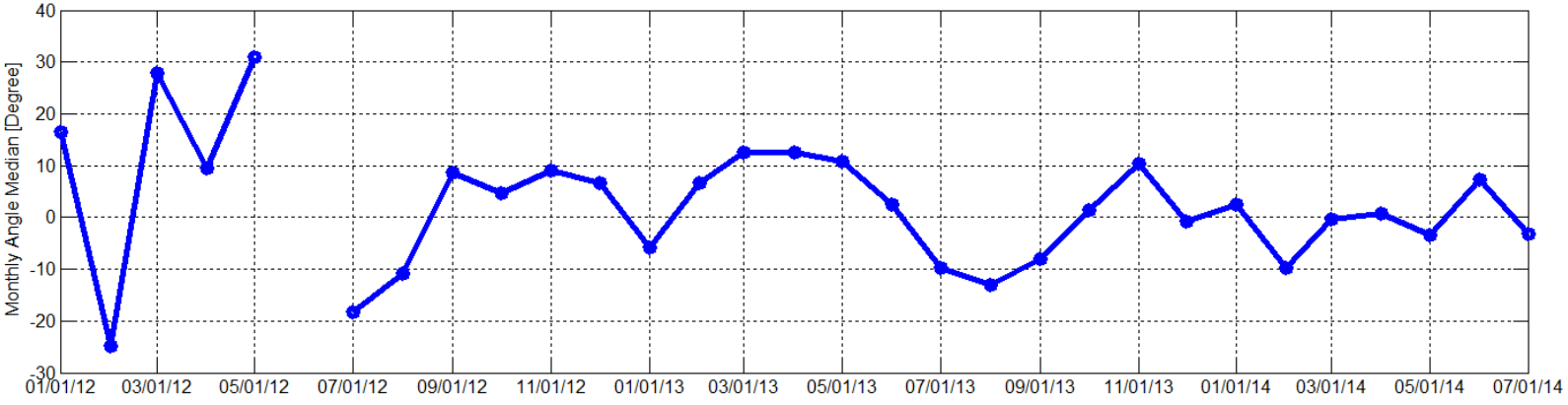


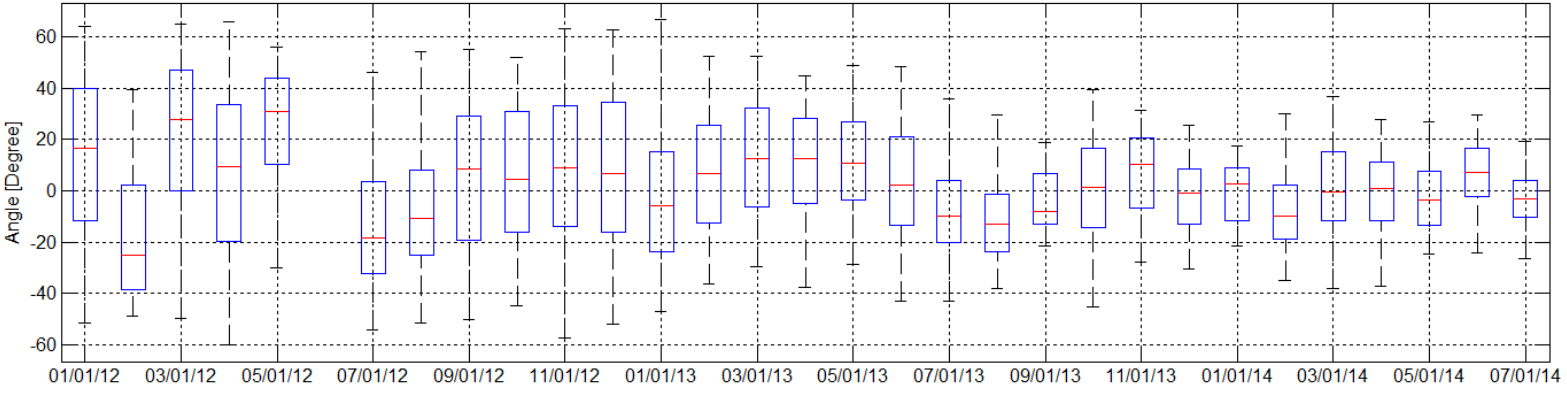
West 4-South 11*



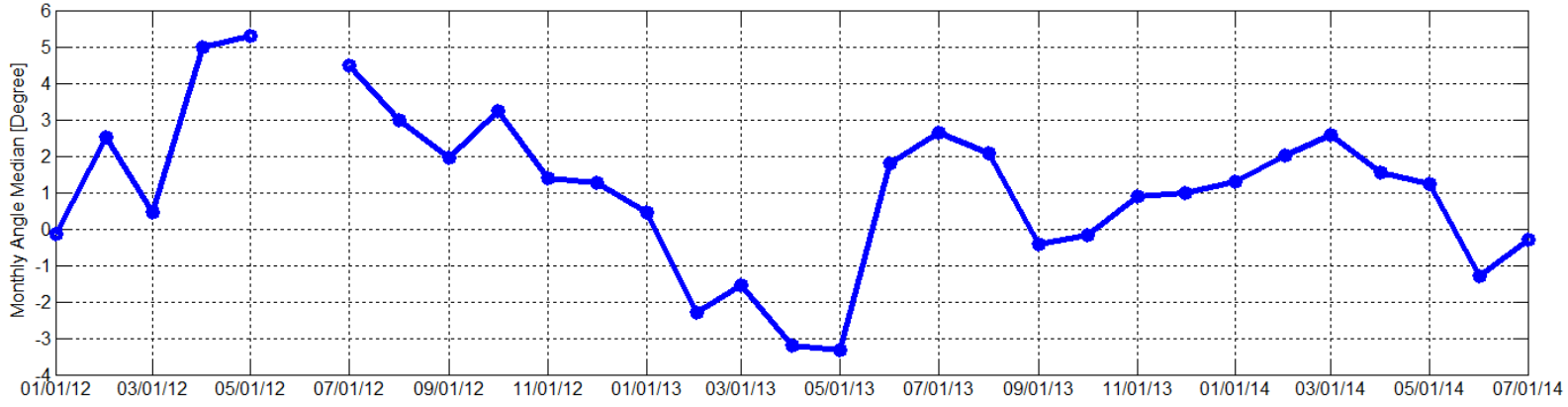


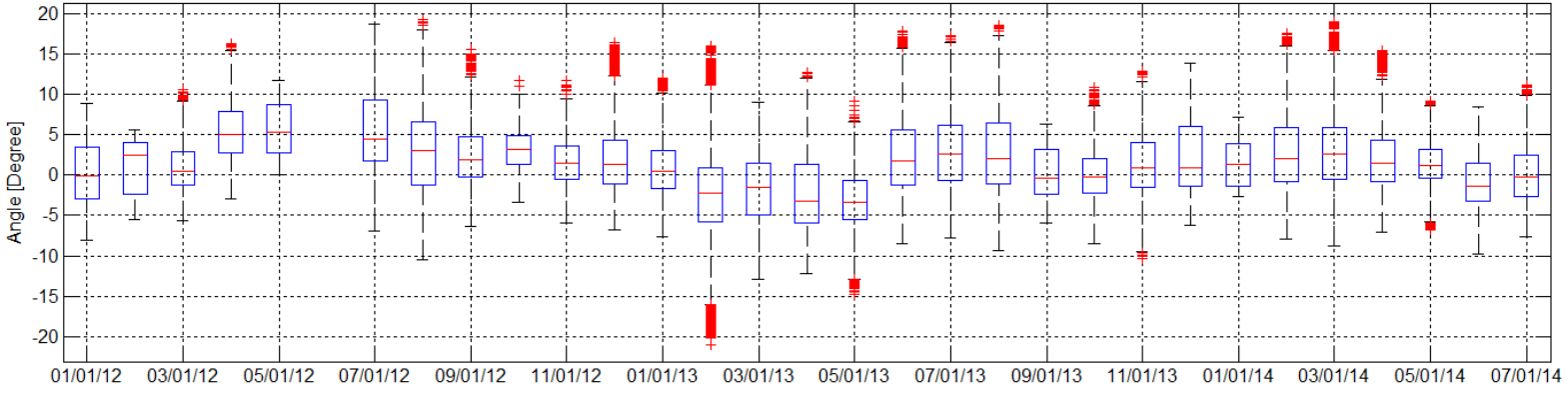
FarWest 9-South 11*





South 11*-North 7





Attachment 6. Data Quality Study

Center for Commercialization Of Electric Technologies Discovery Across Texas Project

ERCOT Synchrophasor Network Data Quality Analysis

Final Report

Submitted to:
Milton L. Holloway, Ph.D.
MHolloway@ElectricTechnologyCenter.com

Submitted by:

John Ballance
Prashant Palayam

Electric Power Group

October 27, 2014

TABLE OF CONTENTS

1. INTRODUCTION

The Center for Commercialization of Electric Technologies (CCET) was awarded contract DE-OE0000194 by the Department of Energy to perform the Discovery Across Texas demonstration project. Electric Power Group, LLC (EPG) received a sub-award from CCET to provide professional services to perform, among other things, an analysis of the accuracy and continuity of synchrophasor data delivery from the Transmission Owners' phasor data concentrators, through the various communications systems and computer networks, and into the Real Time Dynamics Monitoring System[1] (RTDMS®)server and database. The goal of this particular analysis was to validate that data was flowing continuously through the communications and computer systems, and was being accurately recorded and archived in the ERCOT enhanced Phasor Data Concentrator (ePDC) and RTDMS® database systems.

This Data Quality Study analyzed the data streams from the three participating Transmission Owners: American Electric Power (AEP), Oncor Electric Delivery (Oncor), and Sharyland Utilities. This analysis was initially performed using the AEP data stream. Following completion of the initial analysis, examinations of the Oncor and Sharyland data streams were completed.

2. PROJECT SCOPE

In order for the Electric Reliability Council of Texas (ERCOT) to achieve production-quality phasor monitoring that can be relied upon in real-time operations, three conditions must be met:

1. The data must be flowing reliably from the phasor measurement unit (PMU) to the operator's console (data availability).
2. The data must be valid.
3. The data must be monitoring the critical locations (right places).

This report reflects the study being done on the first portion of this Data Quality assessment, data availability, and is focused on identifying any portion of the synchrophasor data network where data is being lost. The approaches include:

1. Identify nodes in the phasor network affecting data availability (i.e., data dropouts).
2. Classify identified dropout issues by severity and frequency.
3. Determine likely causes of data dropouts at identified locations.
4. Propose solutions to help eliminate the identified data availability problems.

The 2012 and 2013 Baselining Studies have addressed the validity of the synchrophasor data compared to state estimator data for the ERCOT system, satisfying condition number 2.

The third condition, monitoring at the critical locations, is being addressed by working groups within ERCOT, as expansion of the synchrophasor monitoring system is being planned.

[1] ®Electric Power Group. Built upon GRID-3P platform, US Patent 7,233,843, US Patent 8,060,259, and US Patent 8,401,710.

3. PHASOR DATA NETWORK

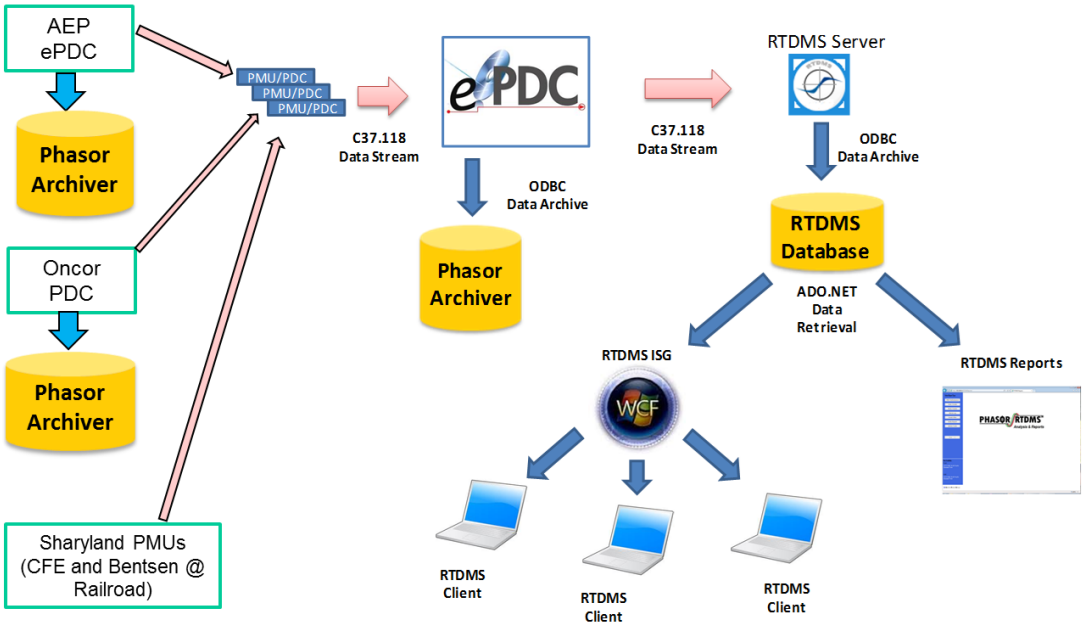
The ERCOT Synchrophasor Network was originally implemented beginning in 2006. With the development of the CCET Discovery Across Texas Regional Demonstration Project, the three participating Transmission Owners, AEP, Oncor, and Sharyland, committed to install PMUs in their respective transmission networks, and to provide their synchrophasor data signals to ERCOT, as a means of improving the overall operation of the ERCOT grid, while accommodating a large increase in remote wind generation.

In 2012 and 2013, dozens of new PMUs were activated and connected to the data collection system. With the inherent complexity of the data collection and communications systems, it quickly became apparent that there were many opportunities for data to be lost or compromised. Available monitoring systems indicated that the network was not successfully delivering all the data that was expected.

3.1 Observable Dropouts

- RTDMS daily reports showed significant dropout data on some signals (60-99%).
- Observation of the *e*PDC Management Tool showed major dropouts (60-99%) in real-time data streams.
- Observation of the *e*PDC and RTDMS performance logs showed the presence of missing samples as dropouts for past streams.
- Data availability checks performed on the RTDMS® and *e*PDC database confirmed the presence of data dropouts.
- Examination of one-second and one-minute tables in the RTDMS® database confirmed down-sampled data was missing on signals as well.

3.2 Phasor Data Network



3.3 Possible Locations of Data Dropout

- RTDMS® reports (and/or RTDMS® Intelligent Synchrophasor Gateway) to RTDMS® database interface.
- RTDMS® server to RTDMS® database interface.
- *e*PDC to RTDMS® server interface problems.
- *e*PDC input and/or output configuration problems.
- Problems on the outbound *e*PDC stream to *e*PDC database.
- Problems on the inbound *e*PDC stream (e.g., T.O. PDC/PMU problems, PMU installation problems, etc.).

4. DATA PROCESSING

Data extracts from the respective PDCs were provided in .csv file formats in full resolution (30 samples per second) for pre-determined time periods. For the AEP analysis, 26 hours of data for two different days were analyzed. For the Oncor analysis, three hours of data were analyzed, and for the Sharyland analysis, one hour of data was analyzed. These data extracts were loaded into MATLAB to conduct a performance test on all the available status signals for the identified dates. A MATLAB script was written to scan through the database and populate performance metrics, such as data dropouts, data invalid, GPS sync errors, time errors, received samples, good samples, and missing samples using the status flag information embedded in the PMU status signals. These performance metrics provided hourly statistics of the database for all the available signals.

The performance metrics, such as data dropouts, data invalid, GPS sync errors, and time errors, were derived, and data availability statistics, such as received samples, good samples, and missing samples, were calculated on periodic intervals (hourly).

The performance metrics and data availability were calculated to:

- Identify the data dropouts
  - Recurring and non-recurring missing samples
- Compare with the *e*PDC and RTDMS® performance log
  - Identify differences in missing samples

A comparative check on the signal headers was also performed between the ERCOT *e*PDC and RTDMS® databases to validate that all data was being properly forwarded.

A comparative check on the data values (accuracy and time alignment) was also performed between the *e*PDC and RTDMS® databases at ERCOT, and between the *e*PDC databases at AEP, Oncor, Sharyland, and ERCOT.

Analysis was conducted separately on each of the three companies' data delivery into the ERCOT databases (ePDC & RTDMS):

1. Phase 1 – AEP.
2. Phase 2 – Oncor.
3. Phase 3 – Sharyland.

5. DATA AVAILABILITY FOR STUDY

The study approach for this “data availability” phase was to compare the phasor data being sent from the (AEP, Oncor ,and Sharyland) PDCs to ERCOT with the data reported as received by the ERCOT PDC, and also with the data reported as received by the ERCOT RTDMS® database. The study initially (for the AEP data) focused on two recent days (26-hours of data over two different days was used to avoid any time synchronization issues).

The two identified study dates were:

1. Friday, January 25, 2013 – The day with the highest number of PMU dropouts.
2. Sunday, January 28, 2013 – The day with the lowest total data availability in the RTDMS® database.

Extracts from the following sources for a 26-hour period were used to analyze data quality:

1. ERCOT RTDMS® Database (Central Time).
2. ERCOT *e*PDC Phasor Archiver Database (Central Time).

3. AEP *e*PDC Phasor Archiver Database (Eastern Time) – the stream is currently sent to ERCOT.

Oncor‘s database was unavailable for the sample dates selected above, so it was decided to complete the analysis using the AEP data, and to follow up with an analysis of Oncor’s data stream using a different set of study dates/hours:

1. January 9, 2014 (10-11 a.m. UTC).
2. January 17, 2014 (midnight-1 a.m. UTC), (1-2 a.m. UTC).

Extracts from the following sources were used to analyze data quality:

1. ERCOT ePDC Phasor Archiver Database (UTC) – Collected at EPG.
2. Oncor PDC Database (UTC) – the stream is currently sent to ERCOT.

The identified study date for Sharyland was:

1. June 19, 2014 (5-6 p.m. UTC)

The data provided includes PMU2 & PMU3 from the South13 substation without status flag information.

Extracts from the following sources for a 1-hour period were used to analyze data quality:

1. ERCOT ePDC Phasor Archiver Database (UTC) – Collected at EPG.
2. Sharyland PDC Database (UTC) – the stream is currently sent to ERCOT.

6. OBSERVATIONS

6.1 Phase 1 – Investigation of ERCOT and AEP Data

6.1.1 AEP ePDC Database Recurring and Non-Recurring Missing Samples

During the study, it was found that there were missing samples in the local AEP *e*PDC database, both recurring and non-recurring, which are shown in the table below.

Missing samples - Frequency Type	Jan 25, 2013 - AEP Stream	ERCOT ePDC Performance Log	Jan 28, 2013 – AEP Stream	ERCOT ePDC Performance Log
Recurring – 1800 per hour	Second 59 of every minute is missing entire 30 samples	Received most of the samples.	Second 59 of every minute is missing entire 30 samples	Received most of the samples.
Non-recurring – 1,800 plus additional	14th hour missing additional 336 samples at 5th minute	Received most of the samples.	3rd hour missing additional 412 samples at 54th minute	**Log shows missing 469 samples at same hour.**
Non-recurring – 1,800 plus additional	15th hour missing additional 332 samples at 30th minute	Received most of the samples.	16th hour missing additional 307 samples at 32nd and 33rd minute combined	Received most of the samples.

A confirmation was performed by scanning through another day - Jan 24 , 2013. The likely cause for samples being received by the ERCOT performance log, but not found in the local AEP database, could be a problem on the outbound side of the AEP *e*PDC stream to its local database. And the likely cause for samples missing in both the ERCOT performance log and AEP database could be a problem on the inbound stream of the AEP *e*PDC receiving the data from the PMUs.

Resolution:

The AEP *e*PDC was upgraded to *e*PDC v3.0.3 from v2.3.2 ,which corrected the recurring data loss of missing the entire 30 samples at the 59th second of every minute, plus the additional non-recurring samples. A confirmation was done by scanning through another day - May 20, 2013. The problem was identified on the outbound stream of the *e*PDC to the local *e*PDC database. The *e*PDC was corrected to send data to its database without missing samples.

The table below shows the results. All AEP data is being received successfully in the local database. No further dropouts were observed in the AEP Database.

From	Date/Time 2013-05-20	PMU Signal	Data Dropout	Data Invalid	GPS Usync	Time Error	Good Samples	Received Samples	Missing Samples
AEP ePDC database extract	Hour 11	Line_1@FarWest_9.Status	0	0	0	0	108000	108000	**0**
	Hour 11	Line_1@West14.Status	0	0	0	0	108000	108000	**0**
	Hour 11	Line_2@West14.Status	0	0	0	0	108000	108000	**0**
	Hour 11	Line_3@West_4.Status	70	0	0	0	107930	108000	**0**
	Hour 12	Line_1@FarWest_9.Status	0	0	0	0	108000	108000	**0**
	Hour 12	Line_1@West14.Status	0	0	0	0	108000	108000	**0**
	Hour 12	Line_2@West14.Status	0	0	0	0	108000	108000	**0**
	Hour 12	Line_3@West_4.Status	61	0	0	0	107939	108000	**0**
	Hour 13	Line_1@FarWest_9.Status	0	0	0	0	108000	108000	**0**
	Hour 13	Line_1@West14.Status	0	0	811	0	107189	108000	**0**
	Hour 13	Line_2@West14.Status	0	0	1197	0	106803	108000	**0**
	Hour 13	Line_3@West_4.Status	1002	0	0	0	106998	108000	**0**

6.1.2 RTDMS Database Missing Samples

6.1.2.1 ERCOT RTDMS Database Missing Samples at Specific Hour on January 25, 2013

Missing samples - Frequency Type	Jan 25, 2013 - RTDMS Database	ERCOT RTDMS Performance Log	ERCOT RTDMS Operations Log	*e*PDC Database Tool
Non-recurring	9th hour missing 93,600 samples after 8th minute	Reported 37 missing samples for that hour	Watch dog message - heart beat message sent out successfully for application for that hour	Error message while retrieving data from database

The RTDMS® database for Jan 25, 2013 had data available only for the first 8 minutes of hour 9. The database extractor reported an error message by the *e*PDC database tool while retrieving data for that hour. The error could not be reproduced, because the data archive causing the problem was no longer available. The RTDMS® database storage capacity is approximately 30 days.

The likely cause for samples not found in the ERCOT database could be:

- Time-out problem to query data from the database by the *e*PDC database client tool.
- Batch size duration issue in the *e*PDC database tool specific for that hour.
- Database *.ini configuration problem like table_cache (default values are limited to few rows).

6.1.2.2 ERCOT RTDMS Database Missing Samples at Specific Hour on January 28, 2013

For Jan 28, 2013, hour 10, the entire 30 samples started dropping from the 10th second of the 6th minute until the 10th second of 15th minute, equivalent to 16,230 missing samples. The likely cause for samples not found in the ERCOT database can be a problem on:

- RTDMS® server to RTDMS database interface (the RTDMS server log reported a connection problem with the database).

Another observation during the investigation was that the missing samples reported in the RTDMS® daily report and the missing samples in the RTDMS® database did not match.

- RTDMS® 2012 daily report shows that the RTDMS® database was filled with 23.83 hours of data availability. (24 – 23.83 = 0.17 missing hours) or (0.17 * 60 = 10.2 missing minutes) or (10.2 * 60 = 612 missing seconds) or samples (612 * 30 = 18,360 samples).
- The daily report shows loss of about 72 seconds more than the RTDMS® database.

Missing samples - Frequency Type	Jan 28, 2013 - RTDMS Database	ERCOT RTDMS Performance Log	ERCOT RTDMS Operations Log	RTDMS Daily Report 2012
Non-recurring	10th Hour missing 16,230 samples.	Reported missing 1 sample for that hour	Watch dog message – database error during batch table insertion and connection failed for that period of time.	23.83 hours of data availability. (Missing 0.17 hours)

Resolution:

On Monday, July 08, 2013 – the ERCOT system was upgraded to:

System Component	Version
*e*PDC	3.1.1
*e*PDC Phasor Archiver (MySQL)	3.1.1
*e*PDC Database Tool	3.1.1
RTDMS® server	2.4.0
RTDMS® database	2.1.6
Intelligent Synchrophasor Gateway (ISG)	3.3.1
RTDMS® clients (on the server and single user laptop)	2.0.0.350

Starting July 9, 2013, until present, the data availability is 24 hours. No dropouts in the ERCOT RTDMS® database. The data dropout problem was identified on the outbound stream of the RTDMS® server to the RTDMS® database, which was resulting in a database insertion error. RTDMS® server was corrected to send raw data, second average, and minute average data without any database insertion errors, leaving no room for dropouts in RTDMS® database.

6.1.2.3 Mismatch in Signal Headers between ERCOT ePDC and RTDMS Database

The RTDMS® server calculates the pseudo signals such as Real Power (*.PP) and Reactive Power (*.PQ), together with virtual signals such as system frequency and angle difference pairs. The pseudo signal names account for some of the mismatch of signals available in the RTDMS® database, but not found in the *e*PDC database. Additionally, there were 56 additional RTDMS® non-pseudo signal headers which were not found in the *e*PDC database.

#	Possible Reason	RTDMS Signal Header Example	ePDC Signal Header Example	Additional Examples
1	Signal Name Change	WEST10.V1LPM.VM WEST10.I1WPM.IM	WEST10.AEP_WEST10 +SV.VM WEST10.AEP_WEST10 +SI.IM	
2	Signal Name Duplicates (Good data vs Bad data)	WEST10.V1LPM.VM (Good data) WEST10.V1LPM.VM (Bad data – zeros) WEST10.V1LPM.VA (Good data) WEST10.V1LPM.VA (Bad data – zeros)		FARWEST_7, WEST11, NORTH_1, FARWEST_8, NORTH_4, NORTH_5, WEST_6, NORTH_6, NORTH_7, FARWEST_4
3	Bad Data Dropouts	Line_3@South13.VALPM.IA Line_3@South13.VALPM.IA Line_3@South13.VALPM.IM Line_3@South13.VALPM.IM		SOUTH13
4	Signal Name Change – Current Magnitude Phase Name	FARWEST7HV11425/11420.VALPM.IM FARWEST7HV11425/11420.VALPM.IA	FARWEST7HV11425/11420.I1SPM.IM FARWEST7HV11425/11420.I1SPM.IA	WEST11, NORTH_1, FARWEST_8, NORTH_4, NORTH_5, WEST_6, NORTH_6, NORTH_7, FARWEST_4

Conclusion: The RTDMS® database had both old and new signal headers in the database.

On the other hand, there were 58 *e*PDC signal headers not found in the RTDMS® database.

#	Possible Reason	RTDMS Signal Header Example	ePDC Signal Header Example	Additional Examples
1	Missing Phase A Signals – Voltage Magnitude	Missing	NORTH_1 8070.VAPM.VA NORTH_1 8070.VAPM.VM	WEST11, FARWEST_7, FARWEST_8

2	Complete Missing PMU stream	Missing	Coast2_11/1690/8530.Frequency.DF Coast2_11/1690/8530.Frequency.FR Coast2_11/1690/8530.I1XPM.IA Coast2_11/1690/8530.I1XPM.IM Coast2_11/1690/8530.Status Coast2_11/1690/8530.V1LPM.VA Coast2_11/1690/8530.V1LPM.VM	Coast_4, West_4, Coast_2
3	Others - Digitals		North_2 138KV.PSV49,PSV50,PSV51,PSV52,PSV53,PSV54,PSV55,PSV56,PSV57,PSV58,PSV59,PSV60,PSV61,PSV62,PSV63,PSV64	
4	PMU Name Change	Line_2@West14.Frequency.FR	Line_3@West14.Frequency.FR	DF, IM, IA, Status
5	Bad Data Dropouts		Line_1@South13.VALPM.VM Line_1@South13.VALPM.VA	South13

Conclusion: the *e*PDC database also had both old and new headers.

Resolution:

The signal name changes and duplicate names between the *e*PDC and RTDMS® database can be corrected.

- *e*PDC can be corrected to set the output configuration for the phasor identification method to be same as the input name for a input stream.
- For each PMU under an input stream, the PMU output system configuration can be set the same as the input system configuration.
- *e*PDC sends data to the RTDMS® server and *e*PDC database. The above two steps can be corrected to both output streams from the *e*PDC.

The missing signals, legacy signal names, and incorrect channel names in the RTDMS® database can be corrected.

- RTDMS® server output to the RTDMS® database can be configured to output the same as the *e*PDC output to the *e*PDC database.
- After *e*PDC gets corrected, the RTDMS® server output and input channel name can be mapped to the correct signal type.

6.1.2.4 Difference in Missing Samples between ERCOT ePDC Performance Log and Database

6.1.2.4.1 January 25, 2013

Until mid-2014, two PMUs from Sharyland stream their data directly to the ERCOT *e*PDC, and were logged as separate streams in the ERCOT *e*PDC performance log. In the table below,

for Line_3@South13 PMU, the “Difference” column shows the number of samples that were not reported in the log, but were available in the ERCOT *e*PDC database. The possible reason behind the positive difference in missing samples is progressive forward padding.

The current version of *e*PDC padding feature does not flag the associated padded data sample timestamp as “data dropout,” which causes the difference between the missing samples in the performance log and the data dropout in the ERCOT *e*PDC database. The occurrence of progressive forward padding, and the count of occurrence, are not logged, but the difference could give the plausible number of padded samples. A similar difference was also found in the Line_1@South13 PMU stream.

Input Name	Hour	Checkword Error	Format Error	Time Error	GPS UnSync	Good	Received	Missing	Data Dropout - ERCOT ePDC Database	Difference
SHARYLAND2	1/25/2013 3:00	0	0	0	0	105481	105481	2519	2507	12
SHARYLAND2	1/25/2013 1:00	0	0	0	0	107172	107172	828	822	6
SHARYLAND2	1/25/2013 2:00	0	0	0	0	105479	105479	2521	2515	6
SHARYLAND2	1/25/2013 4:00	0	0	0	0	105456	105456	2544	2538	6
SHARYLAND2	1/25/2013 5:00	0	0	0	391	107164	107164	836	830	6
SHARYLAND2	1/25/2013 6:00	0	0	0	0	105465	105465	2535	2529	6
SHARYLAND2	1/25/2013 13:00	0	0	0	0	107192	107192	808	802	6
SHARYLAND2	1/25/2013 19:00	0	0	0	0	105480	105480	2520	2514	6
SHARYLAND2	1/25/2013 21:00	0	0	0	0	107204	107204	796	790	6
SHARYLAND2	1/25/2013 23:00	0	0	0	0	105372	105372	2628	2622	6

6.1.2.4.2 January 28, 2013

In the table below, for Line_1@South13, the “Difference” column shows the number of samples that were considered available in the ERCOT *e*PDC database. The possible reason behind the positive difference in missing samples is progressive forward padding. The occurrence of progressive forward padding and the count of occurrence is not logged. A similar, but not identical, difference was also found in Line_3@South13 PMU stream. There was a noticeable huge negative difference in missing samples between the ERCOT *e*PDC performance log and the database.

It was likely that the *e*PDC marked them as data dropouts due to:

- Errors in the timestamps.
- Duplicate timestamps.

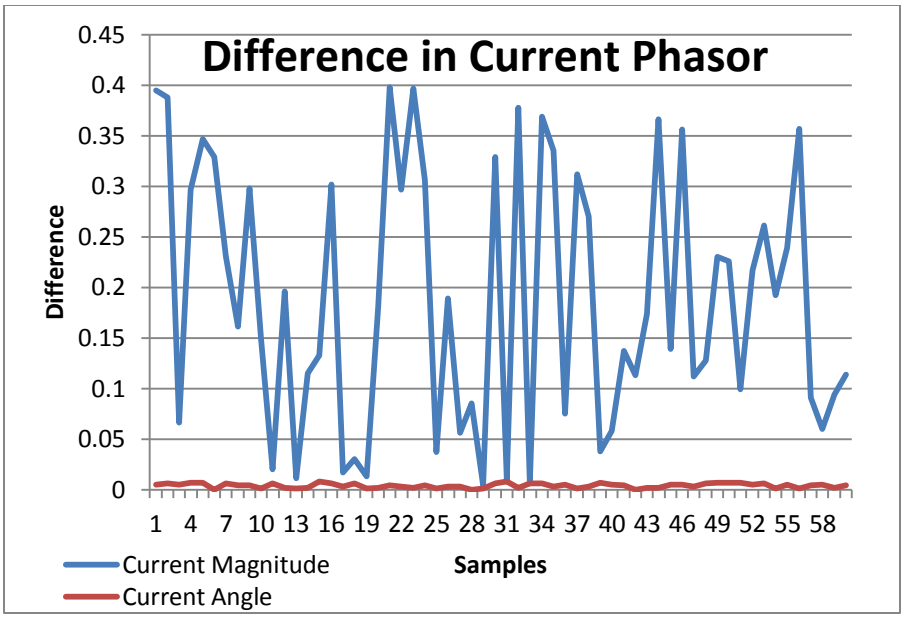
Input Name	Hour	Checkword Error	Format Error	Time Error	GPS UnSync	Good	Received	Missing	Data Dropout - ERCOT ePDC Databa	Difference
SHARYLAND1	1/28/2013 7:00	0	0	0	0	107375	107375	625	0	625
SHARYLAND1	1/28/2013 16:00	0	0	0	0	105447	105447	2553	2547	6
SHARYLAND1	1/28/2013 19:00	0	0	0	0	107154	107154	846	840	6
SHARYLAND1	1/28/2013 20:00	0	0	0	0	107203	107203	797	791	6
SHARYLAND1	1/28/2013 8:00	0	0	0	0	107901	107901	99	2548	-2449

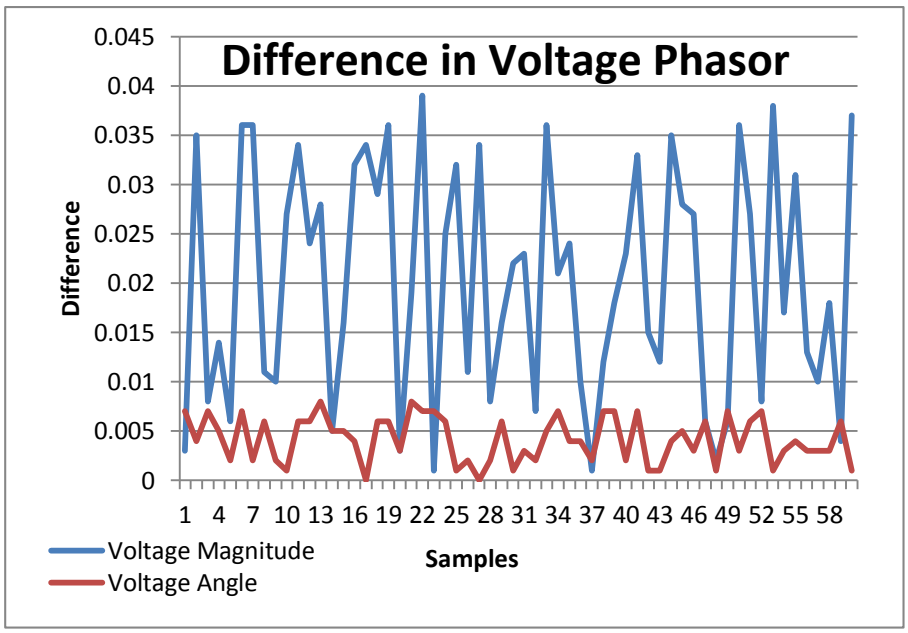
No difference in missing samples between the ERCOT *e*PDC performance log and database.

The possible reason behind the positive difference in missing samples is progressive forward padding. The occurrence of progressive forward padding, and count of occurrence, are not logged, but the latest version of *e*PDC v3.1.1 is enhanced to flag the associated data sample padded timestamp as data dropout. The data dropout is indicated when all the four STAT bits from bit 15 – bit 12 are set to 1. The padded sample will have PMU STAT word set as 0xF200.

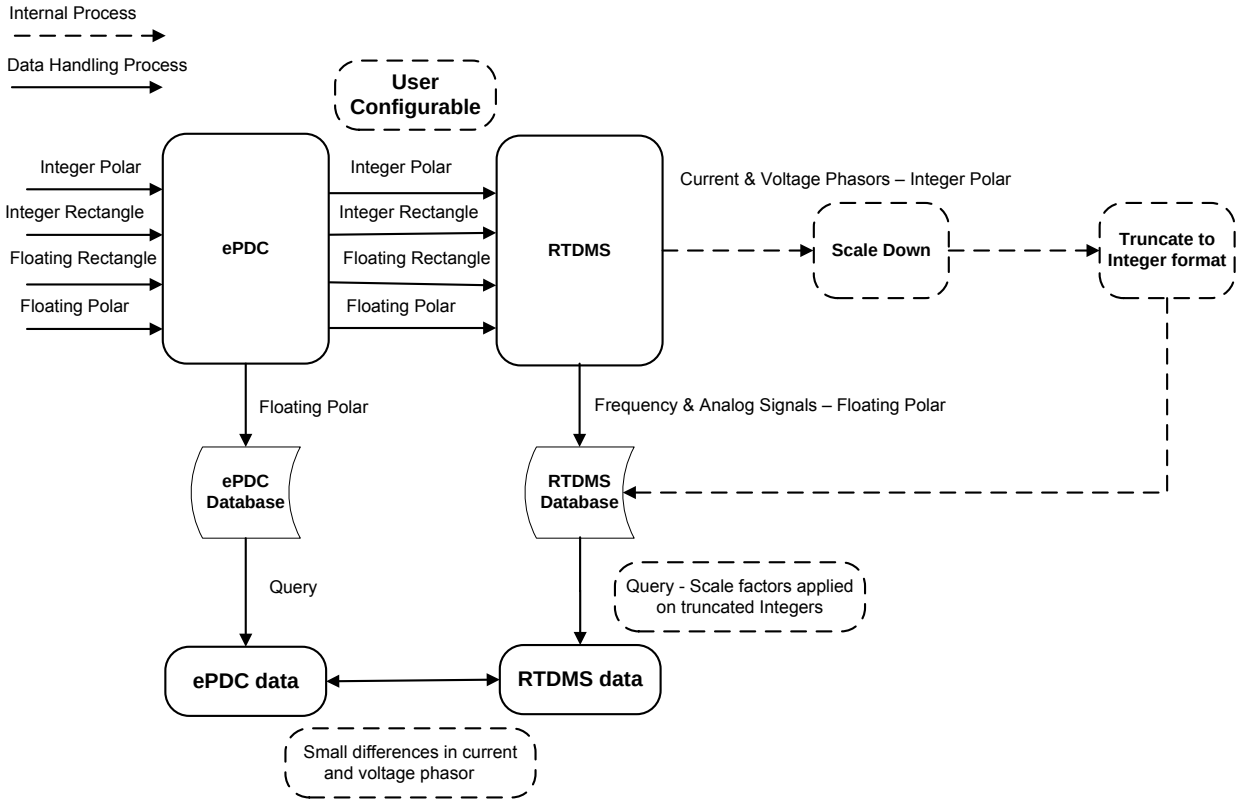
6.1.3 Accuracy of Decimal Digits between ERCOT ePDC and RTDMS® Database – Jan 24, 2013, 23rd Hour

RTDMS® data was observed to be stored and extracted at a slightly lower accuracy than the *e*PDC. It was observed that the accuracy of decimal digits is more noticeable in the voltage magnitude phasor than in the current magnitude phasor, in terms of significant digits after the decimal. The voltage and current angle phasors show matching decimal digits up to the second significant digit after the decimal (the hundredths digit). In contrast, the frequency phasor matches identically between the ePDC and the RTDMS® database. The graphs below show differences in current phasor and voltage phasor. (Difference = *e*PDC data – RTDMS® data).





These small differences in accuracy between *e*PDC and RTDMS ®database can be explained.



The diagram above illustrates the data handling process. The *e*PDC database always stores the received phasor data in floating point polar format in the database, and outputs the received phasor data, in whatever format the user chooses (often with the same format as was received), to other applications such as RTDMS®. The RTDMS® converts phasor data to a scaled integer format for database storage, in order to save storage space in the database (floating point data storage requires approximately twice as much space as does scaled integer format).

RTDMS® stores the phasor data (voltage and current) in scaled integer polar format, while frequency and analog signals are stored in floating point format. Since integers are whole numbers, preservation of the accuracy requires scaling the value so an integer representation will retain most of the accuracy. For example, if 15.4 amperes is converted to an integer 15, the resolution has been reduced from .65% to 7%. If the value is first scaled (divided) by 0.1, the stored value is 154. When retrieved and rescaled, it has its full pre-storage accuracy. However, if we have a current of 8,477.34 amperes and scale by 0.1, the integer representation will be 84,773 which will overflow the integer storage range (-32,767 to 32,767) and will corrupt the value.

The following fixed scale factors are used currently in RTDMS® to handle the trade-off between reducing storage space and limiting the 2-byte 2's compliment range (-32,767 to 32, 767).

Phasor	Current Magnitude	Voltage Magnitude	Angle
Scale Factor	0.4	0.04	0.008
Resolution limit	0.4 amps	0.04 kV (40 volts)	0.008 degrees
Maximum range	± 13,106 amps	± 1311 kV	262 degrees

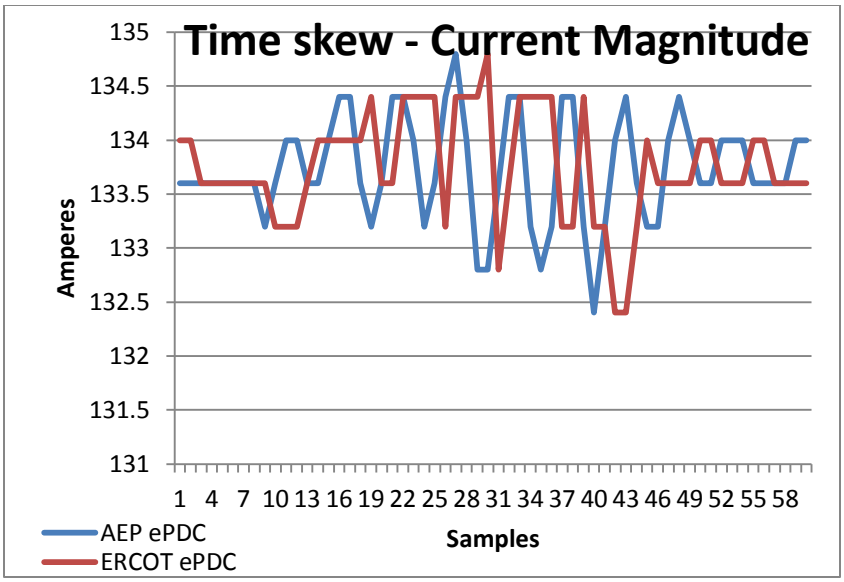
The following describes how the data is scaled down and stored in the RTDMS® database:

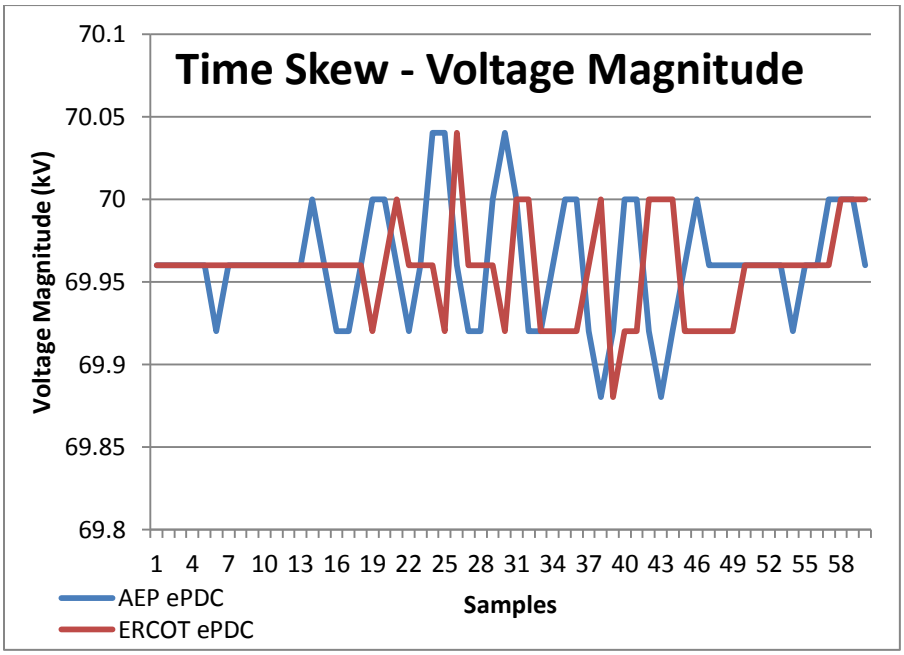
- Scale Up - For those metrics that require a conversion, and need to be stored as integer/polar data format, the value of each part of the phasor (magnitude and angle) with the entire resolution (all fractional part of the mantissa) is divided by its corresponding scale factor.
- The scaled up value of each part of the phasor is truncated to an integer and stored in the database.
- When the data is queried directly from the database, scale factors are used (to multiply) to rescale the received phasor data from the *e*PDC.
- Hence the following was be observed
  - The accuracy of the mantissa was more noticeable in voltage magnitude compared to current magnitude.
  - The frequency phasor had a very good match between the *e*PDC and RTDMS® database as the values are stored in floating point.
  - The order of resolution is current magnitude < voltage magnitude < vngle < frequency.
- Resolution: RTDMS® enhancement: The option to store data as floating point will be made available in RTDMS® server v2.7 for voltage and current phasors.

6.1.4 Time Skew Between AEP and ERCOT ePDC Database – Jan 24, 2013, 23rd Hour (Central Time)

ERCOT *e*PDC data extracted appears to be time skewed from the AEP *e*PDC data. When the ERCOT *e*PDC data is shifted forward by 2 time samples (2/30 of a second), then the voltage and current angles nearly coincide. Voltage and current magnitude are close enough, but not as close as angles.

It appears that ERCOT data is time shifted (delayed) by 0.067 seconds compared to the AEP *e*PDC data. The plots below show comparison between AEP *e*PDC data and ERCOT *e*PDC data for current magnitude and voltage magnitude.



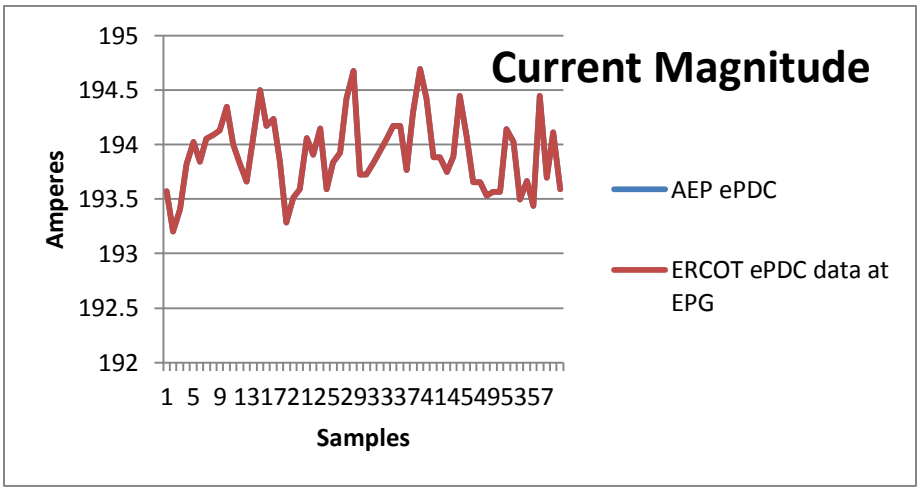


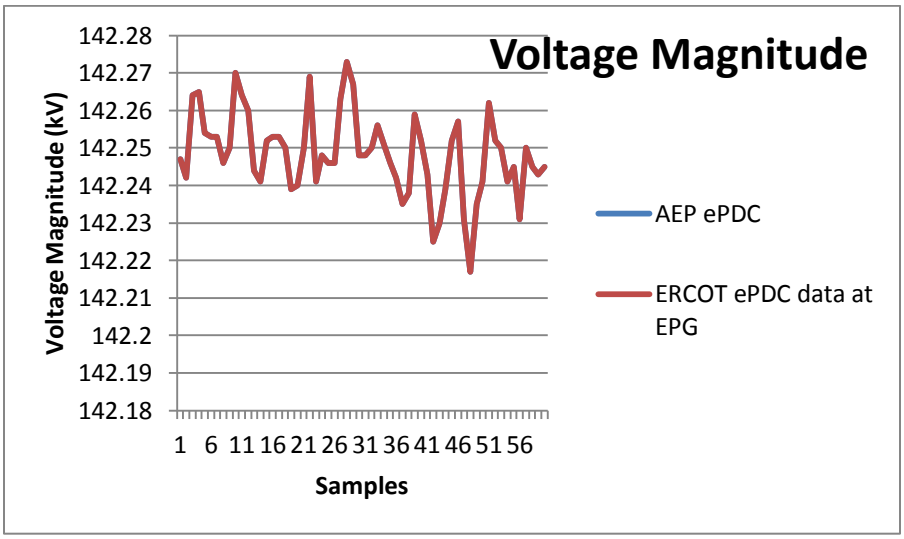
Resolution:

The time skew issue was related to user-defined *e*PDC minimum output latency, and the use of progressive forward padding. To resolve this issue, the *e*PDC at AEP was corrected to wait longer (increase the minimum output latency to 100 ms), or to disable the progressive forward padding. Currently AEP is running *e*PDC v3.1.1 with missing data padding disabled.

Following a configuration change to the AEP *e*PDC, an extract was obtained for 30 minutes, starting 27 August ,2013 11 a.m. UTC, and compared with ERCOT data for the same time collected at the EPG database. An investigation was performed on the voltage phasor, current

phasor, and frequency for two PMUs, namely West 10 and Coast 1. It was found that there were no longer any differences between the two databases, and that they now overlay on top of each other, as shown below.





6.2 Analysis of ERCOT and Oncor Data Streams

To analyze the Oncor-ERCOT data stream, three hours of data was extracted from the Oncor PDC local database:

1. January 9, 2014 (10-11 a.m. UTC).
2. January 17, 2014 (midnight-1 a.m. UTC), (1-2 a.m. UTC).

A matching set of data was extracted from the ERCOT *e*PDC Phasor Archiver Database (which is replicated at EPG for this project).

6.2.1 Dropouts in Oncor Database Extracts

Missing Samples - Frequency Type	Jan 9, 2014 (10-11AM UTC) – Oncor DB	ERCOT DB	Observation
Non-recurring – 1,716	59th Minute Start to miss from 3rd second until last second	Received most of the samples.	Local archiving between Oncor PDC & DB

Missing samples means no record of the data was found in the Oncor dataset. However, there were no missing samples for any other dates. It is recommended that Oncor check their PDC logs for possible data insertion errors in case the dropout was due to maintenance or network issues. It is also recommended to verify querying the database directly in case it was data extraction issue.

6.2.2 ERCOT Receiving a Higher Count of Flagged Data

PMU Name	Oncor - Number of Flagged Data	ERCOT - Number of Flagged Data	Observation
WEST1_10840/10835	0	197	Flagged bad as '0xe' (0xe meaning data invalid, PMU Error and GPS Sync Error)
WEST2_11130/11135	0	234	
WEST2_11140/11135	0	234	
WEST1_10845/10850	0	197	

The study of the data from January 17, 2014 (midnight-1 a.m. UTC) reveals that there is a higher count of bad data flags in the ERCOT *e*PDC database than in the Oncor database. There are only four PMUs in the Oncor single stream to ERCOT that are flagged bad. As a rule of thumb, dropouts from a single stream, such as Oncor to ERCOT, will be flagged '0xF'. It is more likely a communication issue between Oncor and ERCOT, not at the Oncor PDC. On the other hand, the above table shows only four PMUs flagged bad (not likely a communication issue since they belong to the same stream) as '0xe'. '0xe' seems to be marked by the PDC at Oncor while sending to ERCOT.

Possible Explanation: The Oncor PDC flagged the data bad when it was sent to ERCOT, but waited longer to archive the data samples locally in the database, at which time the data was valid (perhaps there is more latency in these four signals than the PDC would accept).

6.2.3 Missing Signals in ERCOT Database

Oncor confirmed that these signals are being archived in their local database, and not being sent to ERCOT (at ERCOT's request):

- NORTH_5 025
- WEST2_11125/11120
- WEST2_11145/11150
- WEST1_11540/11545
- WEST1_11550/11545
- WEST1_10855/10850
- WEST1_10860/10865
- WEST1_10885/10880

6.3 Analysis of ERCOT and Sharyland Data Streams

For the analysis of the Sharyland-ERCOT data stream, one-hour of data was extracted from the Sharyland PDC local storage:

1. June 19, 2014 (5-6 p.m. UTC).

The data provided includes PMU2 & PMU3 from the South13 substation without status flag information.

A matching set of data was extracted from the ERCOT *e*PDC Phasor Archiver Database (which is replicated at EPG for this project).

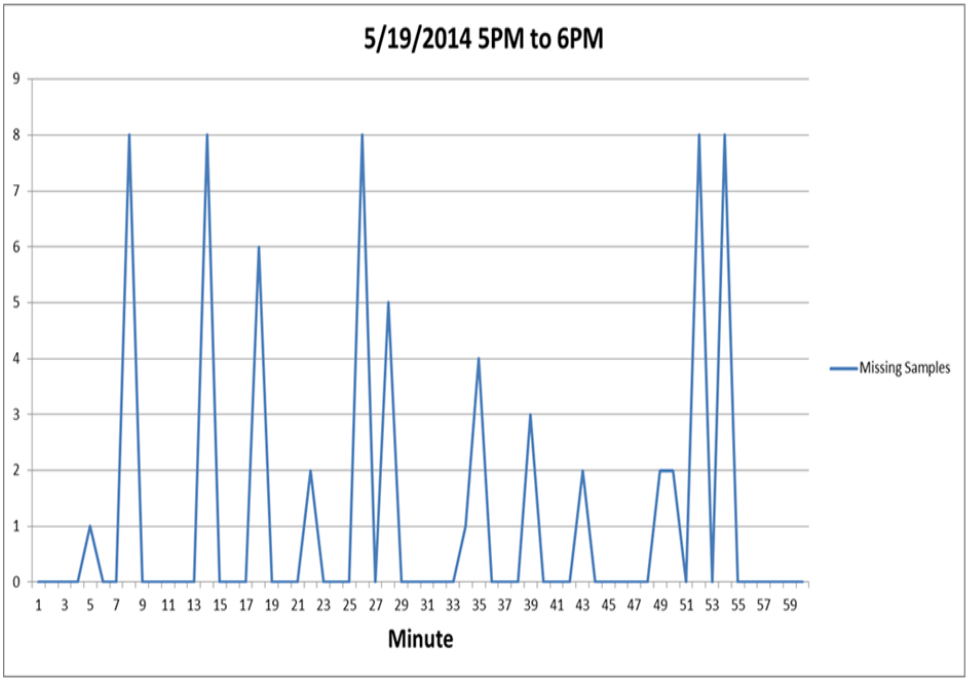
6.3.1 Dropouts in Sharyland Database Extracts

Missing Samples - Frequency Type	June 19, 2014 (5-6 P.M. UTC) Sharyland	ERCOT DB	Observation
Non-recurring – 68	Scattered	Received most of the samples.	Local archiving between Sharyland PDC & database

Missing samples means no record of data found in the Sharyland dataset. It is recommended that Sharyland check their PDC logs for data insertion error in case the missing data was due to maintenance or a network issue. It is also recommended to verify querying the database directly in case it was data extraction issue. The missing samples did not have evident pattern, and they were scattered over different minutes in that hour.

The plot and table below shows that:

- Maximum number of missing samples – 8 per minute.
- Missing either at beginning of a second or towards end of factors of 10 second.



Minute ?	Second?	Missing Samples
7	9th & 10th	8
13	49th & 50th	8
25	19th & 20th	8
51	10th	8
53	9th & 10th	8
4	10th	1
21	0th	2
42	0th	2
48	40th	2
49	20th	2
34	10th	4

6.3.2 ERCOT Receiving More Count of Flagged Data

PMU Name	Sharyland - Number of Flagged Data	ERCOT - Number of Flagged Data	Observation
PMU2-South13	Cannot Determine	2406	Flagged bad as '0xe'
PMU3-South13	Cannot Determine	0	

Date/Time	PMU Signal	Data Dropout	Data Invalid	GPS Usync	Time Error	Data Invalid + GPS Unsyn + PMU Error (0xe)	GPS Unsyn + Time Error (0x3)	Flagged Good Samples (0x0)	Good Samples	Received Samples	Missing Samples
_2014-05-19T170000_60m.csv	"PMU2-South13.Status.ST"	6759	0	0	0	2406	0	98835	98835	108000	0
_2014-05-19T170000_60m.csv	"PMU3-South13.Status.ST"	108000	0	0	0	0	0	0	0	108000	0

This issue appears to be similar to the Oncor PDC. There were higher counts of bad data in the ERCOT database than in the Sharyland database. ‘0xe’ seems to be marked by the Sharyland PDC while sending the data to ERCOT, and not while archiving. The signal values looks good in the Sharyland database, even without knowing status flag information.

7. SUGGESTIONS AND RECOMMENDATIONS

Any Utility/ISO with a phasor network should:

- Validate the data quality and data flow – don't assume it is good.
- Validate data storage on received data samples.
- Check for missing samples – received versus reported.
- Verify data time alignment between databases.
- Verify data accuracy and sufficient resolution between databases.
- Verify signal name consistency between databases.
- Fix data quality issues in a timely manner.
- Conduct periodic validation of data quality.
- Also plan to validate the data measurements.
- Continuously monitor data being received.

Attachment 7. Data Quality Inputs to ERCOT Communications Handbook

Excerpt from Draft

ERCOT Synchrophasor Communication Handbook

V1.0

August 11, 2014

5 SYNCHROPHASOR NETWORK DATA QUALITY

In order for ERCOT and their Market Participants to achieve a production quality phasor network system that can be relied upon in real-time operations, it is important to check whether the data link that is established between a market participant and ERCOT carries data flow reliably to ERCOT. The Data Quality Test will address the prior condition and will certify whether data sent from Market Participants is received and archived same at ERCOT.

Once a reliable synchrophasor network is established, it is also important to check the performance of each PMU on a continuous basis. The reliable synchrophasor network ensures high data availability but may not have high PMU performance. A highly reliable synchrophasor network may still have PMUs reporting with flagged data which cannot be used in real time operations. The occurrence of flagged data from the PMUs (or PDC) can be recurring or non-recurring (repeating or non-periodic respectively). It is important to check and correct the occurrence of flagged data in order to establish a reliable synchrophasor network with high PMU performance.

The good practices on the two phasor data test on the synchrophasor network are briefly explained below. The Data quality test ensures reliable synchrophasor network between the Market Participant and ERCOT. The PMU Performance Test will improve the occurrence of good data and reporting from PMU & PDCs itself.

The testing method listed here is specific for EPG RTDMS product.

5.1 RTDMS Data Quality Test

The Data Quality Test is an end-to-end analysis between the Market Participant (or any data sender) and ERCOT. This end-to-end analysis is a direct comparison between the data sent by Market Participant and the data received and archived at ERCOT. In order to conduct the study, it is most important that Market Participant (MP) and ERCOT archive data at both ends.

It is recommended to capture one hour of data (minimum) or more from both ends for two different days (minimum) or more. The data collected at both ends for the same time duration will help to conduct the data quality test. Some of the common findings on data quality issues between data collected at both ends are as follows:

1. Missing Samples
2. Missing PMUs & Signals
3. Mismatch in PMU & Signal Headers/Names
4. Data Shift in time (Time Skewed)
5. Difference in Data Resolution
6. Difference in Count of Flagged Data

Missing Samples

1. Verify the count of samples reported matches the received rate

   For example – If the phasor data reporting rate is 30 samples per second, then the count of samples expected for duration of 1 hour is equal to 108000 samples.

2. Compare the results at both ends to verify
   a. There are no local archiving issues
   b. There are no communication issues between MPs and ERCOT

Missing PMUs

1. Verify the count of PMUs sent matches the received PMUs

   For example – If the MP is sending 10 PMUs to ERCOT, then ERCOT should be receiving data for all the 10 PMUs.
2. Verify the count of signals sent under each PMU matches the reported received signals under that PMU
3. Compare the results at both ends to verify

   There are no lost PMUs/Signals during the communication

Mismatch in PMU & Signal Headers/Names

1. Verify whether PMU headers/names sent matches the received PMU headers/names
2. Verify whether Signal headers/names sent matches the received Signal headers/names under each PMU
3. Compare the results at both ends to verify
   a. There is no mismatch due to configuration changes
   b. There is consistent PMU naming convention
   c. There is consistent name for a PMU and its signal for common displays and analysis

Data Shift in time (Time Skewed)

1. Verify whether PMU signal data reported for a timestamp matches exactly at both ends

   For Example: Plot and Compare same PMU signal data from both ends for a duration of time
2. Compare the results at both ends to verify
   a. There is Time alignment – PMU Signal data at both ends should be identical (they will lie on top of each other when plotted)
   b. There is no Time Skew – PMU Signal data from one end will be time shifted from other and will not lie on top of each other when plotted
   c. If there is time skew, it could possibly be latency issue related to the PDC

Difference in Data Resolution

1. Verify whether the PMU signal data value matches (magnitude and phase angle) at both ends for a duration of time

   For Example: Calculate the Difference between PMU signal data from both ends for a duration of time (Assuming there is no time skew)

2. Compare the results to verify
   a. There is no difference in resolution at both ends
   b. There are no data conversion issues at the PDC
   c. There is no mismatch in scaling factors used at the PDC

Difference in Count of Flagged Data

1. Verify the count of flagged data matches at both ends

   For Example: If the count of data samples, flagged good, sent by MP were 108000 in an hour, then ERCOT should receive the same count of good data samples during the same hour

3. Compare the results to verify
   a. There are no communication issues causing data dropouts
   b. The count of flagged data at the receiving end matches the count at the sending end
   c. There is consistency of flagged data samples at both ends (data is flagged identically for the same time interval)
   d. There is no communication delay between both ends

Flagged Data Samples

The C37.118 data stream includes quality information for all the signals for each PMU in a Status flag. The Status flag is represented by hexadecimal integer 0x0000. The left most hexadecimal integer carries the quality information for the PMU data (0x0). Below table shows the findings on different types of observed flags on data samples.

#	Types of Flags	Description – The data is flagged bad due to
1	‘0x0’	Good Quality data
2	‘0xF’	Dropouts (set by the ePDC)
3	‘0x8’	Data Invalid
4	‘0x1’	Time Alignment Error (Sorted by Arrival and not by Timestamp)
5	‘0x2’	GPS Sync Error
6	‘0x3’	GPS Sync Error + Time Error
7	‘0xE’	Data Invalid + GPS Sync Error + PMU Error

The data quality test is needed to be expanded to the following

1. Within ERCOT Synchrophasor Network – Between ePDC and RTDMS
2. Between PMU and MP, if there are local archives at PMU level

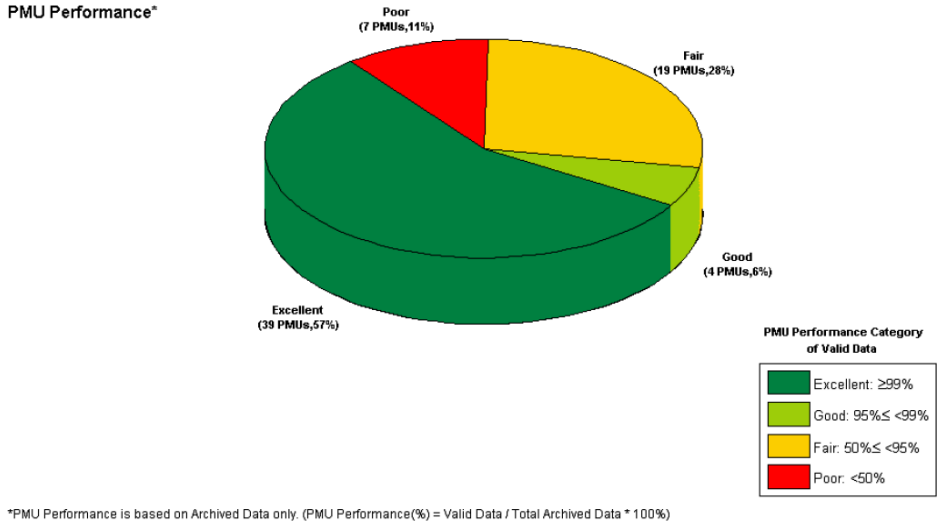
5.2 RTDMS PMU Performance Test

A highly reliable synchrophasor network may still have PMUs reporting with flagged data which cannot be used in real time operations. The occurrence of flagged data from the PMUs or PDC can be recurring or non-recurring (repeating or non-periodic respectively). It is important to check and prevent the occurrence of flagged data to establish a reliable synchrophasor network with high PMU performance.

PMU Performance Chart shown below is a pie chat from the RTDMS Daily Report showing the performance of PMUs under different performance categories. The objective of the PMU Performance analysis is to

1. Make all PMUs perform excellently
2. Identify plausible reasons for those PMUs that don't have excellent data quality
3. Find consistent patterns that affect PMU Performance
4. Identify any other inconsistent data quality issues affecting PMU Performance on a continuous basis

This study may identify issues with PMU devices and their supporting instruments, network issues transporting data within the synchrophasor network and many more.



PMU Performance Chart – RTDMS Daily Report

The PMU Performance analysis is done at the ERCOT level to identify the PMUs that are not performing well (as reported in the data delivered to ERCOT) and report to MPs on consistent data quality issues for improved performance. It is recommended to

1. Use one month of data collected at ERCOT
2. Count occurrence of flagged data (see above list of flagged data types), good samples, received samples and missing samples on a daily basis for all PMUs
3. Find patterns of data quality issues over the month

Some of the common findings on data quality issues affecting PMU Performance are as follows:

1. Daily Dropouts between MPs and ERCOT
2. Daily Dropouts between Specific PMUs and MPs
3. Specific PMUs showing GPS Sync Error
4. Specific PMUs reporting more count of flagged data

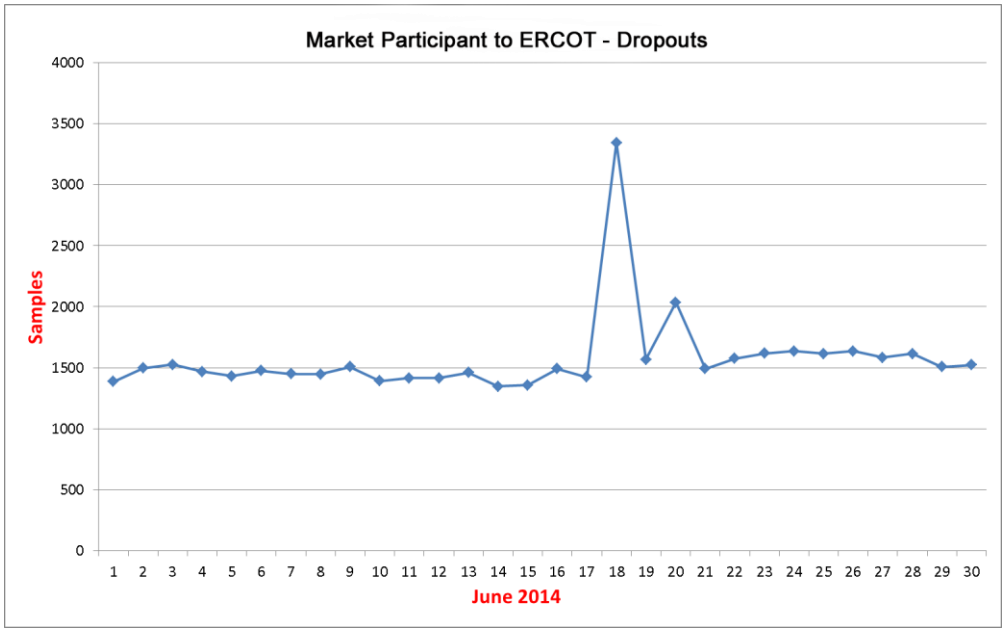
Daily Dropouts between MPs and ERCOT

The data samples are flagged bad as dropouts when they don't reach the destination due to communication issues. It is likely that the PDC sets the flag. Some of the common patterns of dropouts are

1. Daily Consistent Dropouts for entire stream from MP
2. Daily Irregular Dropouts for entire stream from MP

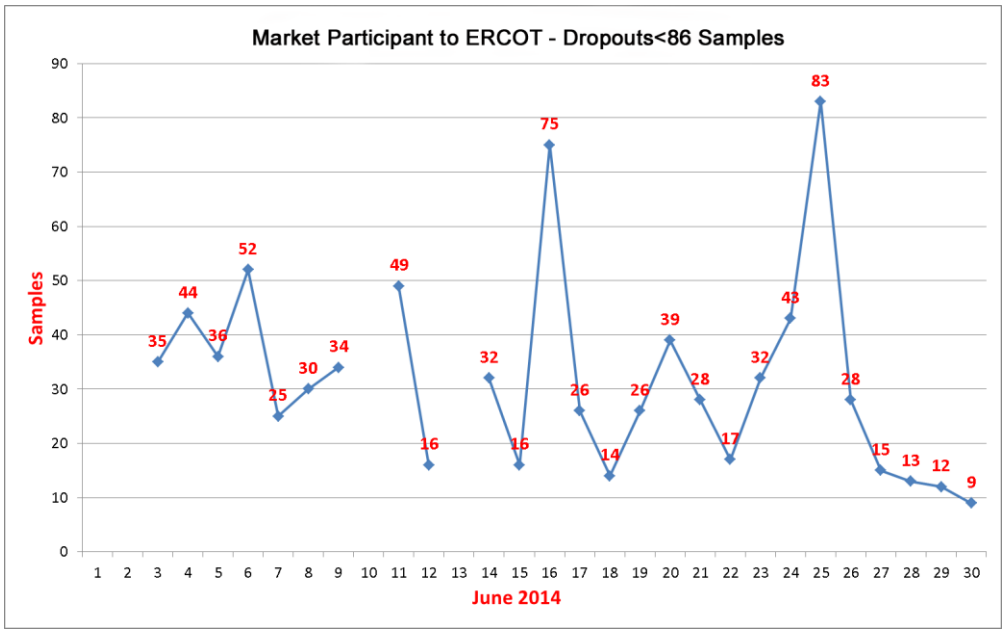
Daily Consistent Dropouts for entire stream from MP

1. If all the PMUs in the stream from MP shows same dropouts, it is more likely that there is communication issues between the MP and ERCOT
2. If the dropouts are consistent over the entire month, then there is most likely there are communication issues between MP and ERCOT on a daily basis.
3. For Example: Below figure illustrates the scenario that a certain Market Participant is having consistent daily dropouts for their entire data stream to ERCOT.



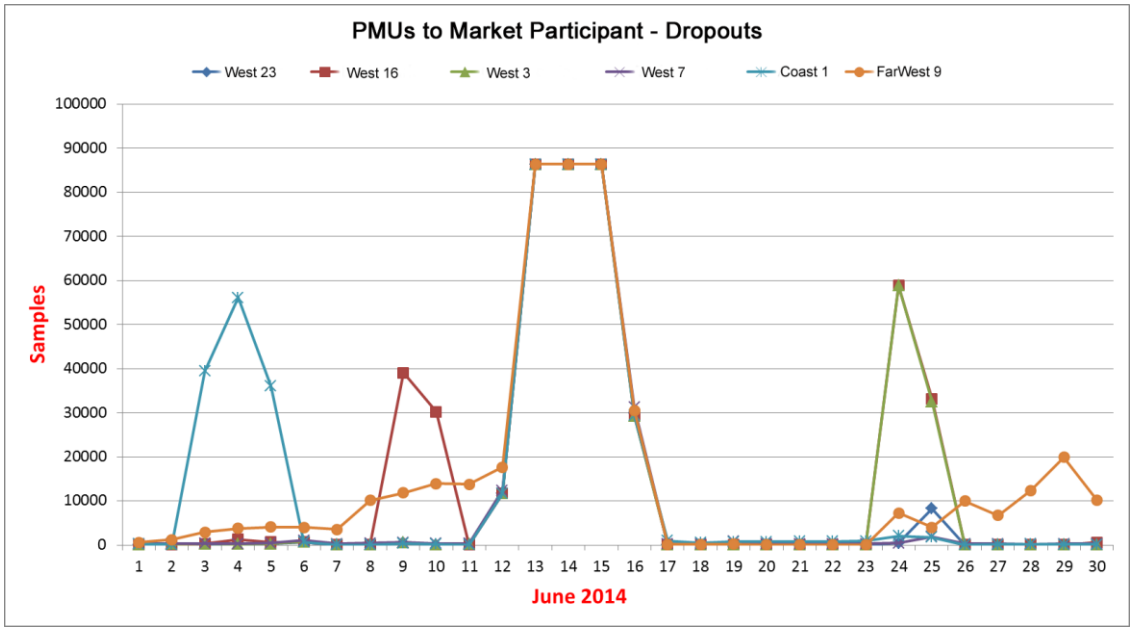
Daily Irregular Dropouts for entire stream from MP

1. If all the PMUs in the stream from MP shows same dropouts, it is more likely that there is communication issues between the MP and ERCOT
2. Sometimes the dropouts are not consistent over the entire month and are found to be irregular over the entire month
3. For Example: Below figure illustrates the scenario where a certain Market Participant is having inconsistent daily dropouts for entire stream to ERCOT



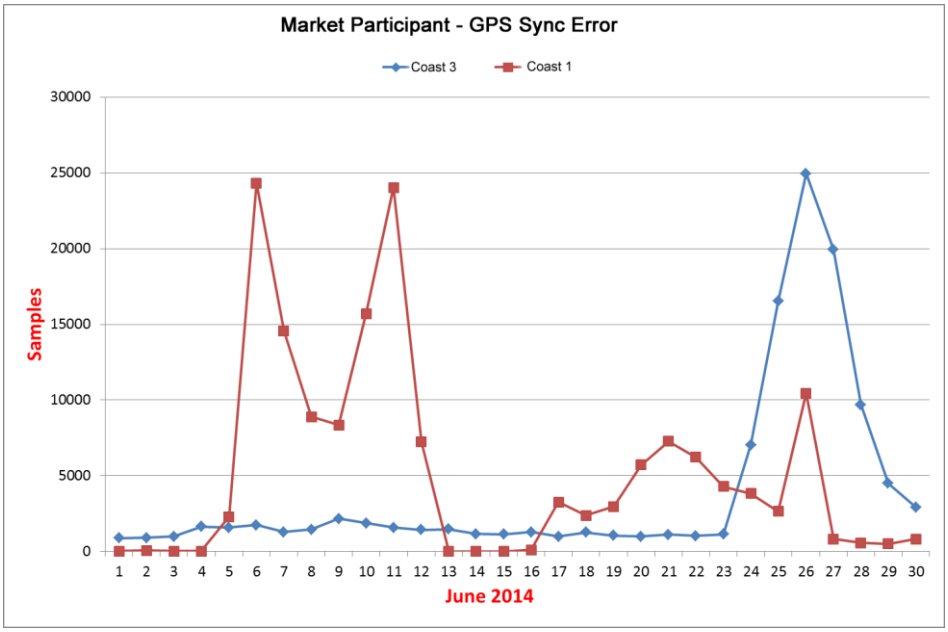
Daily Dropouts between Specific PMUs and MPs

1. MP sent PMU data stream as a single stream to ERCOT. So when there is a communication link failure, then all the PMUs are subject to be flagged as dropouts.
2. If specific PMUs in the stream from MP show dropouts, it is more likely that there are communication issues between the specific PMUs and MP PDC
3. It is most likely the dropouts are not the same for all PMUs as they represent dropouts from specific PMUs and are found to be irregular over the entire month.
4. Sometimes dropouts are the same for specific group of PMUs, if they are sent from a substation PDC or on a common communications path
5. For Example: Below figure illustrates the scenario where a certain Market Participant is having inconsistent daily dropouts for specific PMUs to their PDC



Specific PMUs showing GPS Sync Error

1. PMU data samples are flagged bad as GPS Sync Error if the PMU loses synchronization with its GPS clock.
2. The occurrence of flagged data samples under this category may be consistent or non-periodic over the entire month for each PMU.
3. Identifying the PMUs which frequently lose synchronization with the GPS clock can enable the MP to correct the GPS clock in order to improve the PMU performance.
4. For Example: Below figure illustrates the scenario where two PMUs from a Market Participant were showing frequent counts of flagged data samples. The plot below illustrates that Coast 3 (in blue) had a consistent count of samples flagged bad every day of the month and Coast 1 (in red) was irregular over the month.



Specific PMUs reporting higher count of flagged data

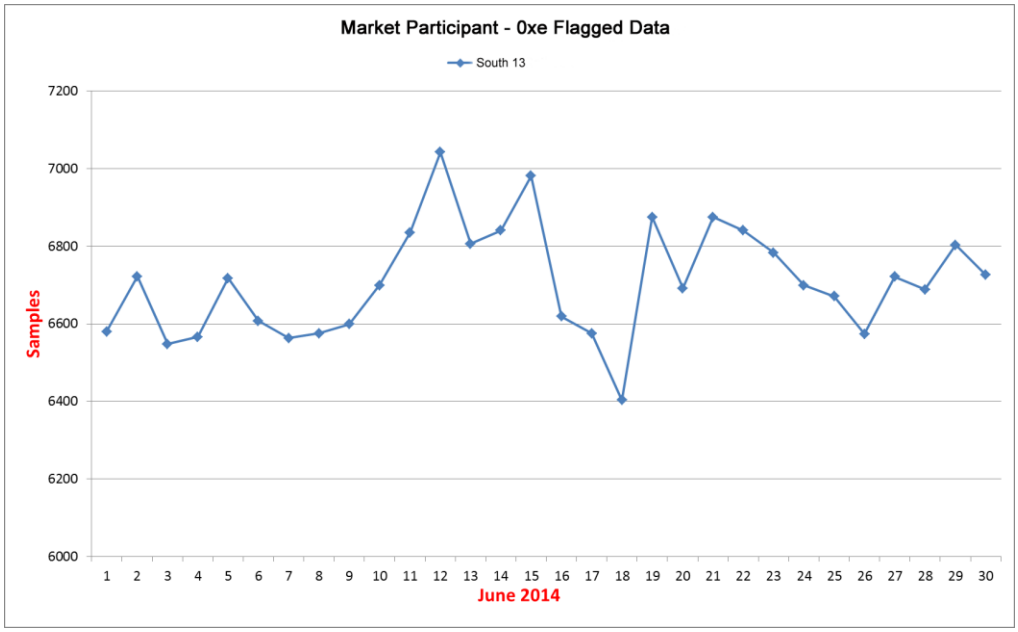
ERCOT might notice data samples from specific PMUs that are flagged bad as '0xE', most likely set by the MP's PDC and sent to ERCOT. It was found that those flagged data samples were flagged and archived as good at the MP database. It was observed that ERCOT was receiving a greater count of flagged data samples under this category, and this condition needs to be monitored.

It is likely that the PDC sets the flag. Some of the common patterns of '0xE' are

1. Daily Consistent Pattern from specific group of PMUs
2. Daily Irregular Pattern from specific group of PMUs

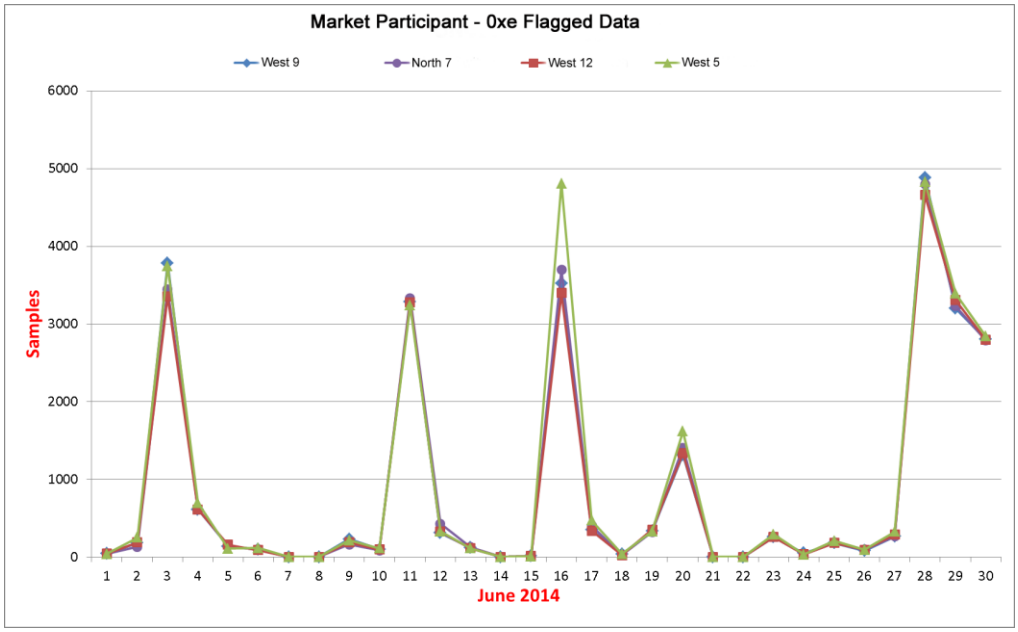
Daily Consistent Pattern from specific group of PMUs

1. Identifying the PMUs which frequently have flagged data samples can be notified and corrected to improve the PMU performance.
2. For Example: Below figure illustrates the scenario where a PMU from a Transmission Owner was showing a consistently high count of flagged data samples over the entire month.



Daily Irregular Pattern from specific group of PMUs

1. Identifying the PMUs which frequently have flagged data samples can be notified and corrected to improve the PMU performance.
2. For Example: Below figure illustrates the scenario where a specific group of PMUs from a Transmission Owner were showing irregular counts of flagged data samples over the entire month, but the irregular patterns were very similar for the entire group over the entire month.



The PMU Performance analysis can be expanded to other types of flagged data samples as tabulated in the previous section. This analysis can pinpoint which PMUs are the "bad actors" sinking the overall PMU performance. The data quality test and PMU performance test on a continuing basis can drive to a reliable and high performance synchrophasor network. It is also a good practice to include other non-duplicative findings that are of concern based on future observations.

Attachment 8. PMU Event Analysis Report for 10 January 2014

EVENT DETAILS

On January 10, 2014, at about 8:30 a.m., after logging on into RTDMS system, ERCOT Operations Engineers noticed oscillations on the RTDMS displays. Since the oscillations were showing up only at the Wind Farm PMU as shown in Figure 1, ERCOT looked at the generation at the Wind Farm unit close to Wind Farm PMU. It was generating about 56 MW (Figure 2). These oscillations were showing up even though there was no line outage at the substation. (In October 2013, ERCOT had observed oscillations due to a line outage at the Wind Farm substation).

In order to reduce the oscillations, ERCOT advised the Wind Farm unit to turn OFF their AVR. This did not help to reduce the oscillations. In order to reduce oscillations, they were curtailed to 45 MW output. This reduced the oscillations to some extent. Since the oscillations did not go away completely, they were further constrained to 40 MW and the oscillations finally went away as shown in Figure 3 and Figure 4. It was found that oscillations were present in the system since 6:15 p.m. of January 9, 2014. Analysis of these oscillations using Phasor Grid Dynamics Analyzer (PGDA) tool indicated that the dominant mode that was present was 3.3 Hz, as shown in Figures 5 and 6. The voltage oscillations were having magnitude of about 1kV, as shown in Figure 7. The oscillations were present till the next morning. Figures 7 and 8 show the oscillations present in the morning of January 10, 2014 until the unit had been curtailed to less than 40 MWs. ERCOT Operations contacted the plant operator at the Wind Farm to determine the cause of oscillations. It was discovered that some updates were made to the settings for the system controller on January 9, which matched the time of initial observation of the oscillations. After ERCOT informed the Wind Farm Operators about the oscillations, they pulled back the updates which finally stopped the oscillations. After that, no oscillations were observed even when the plant was generating at greater than 50 MWs.

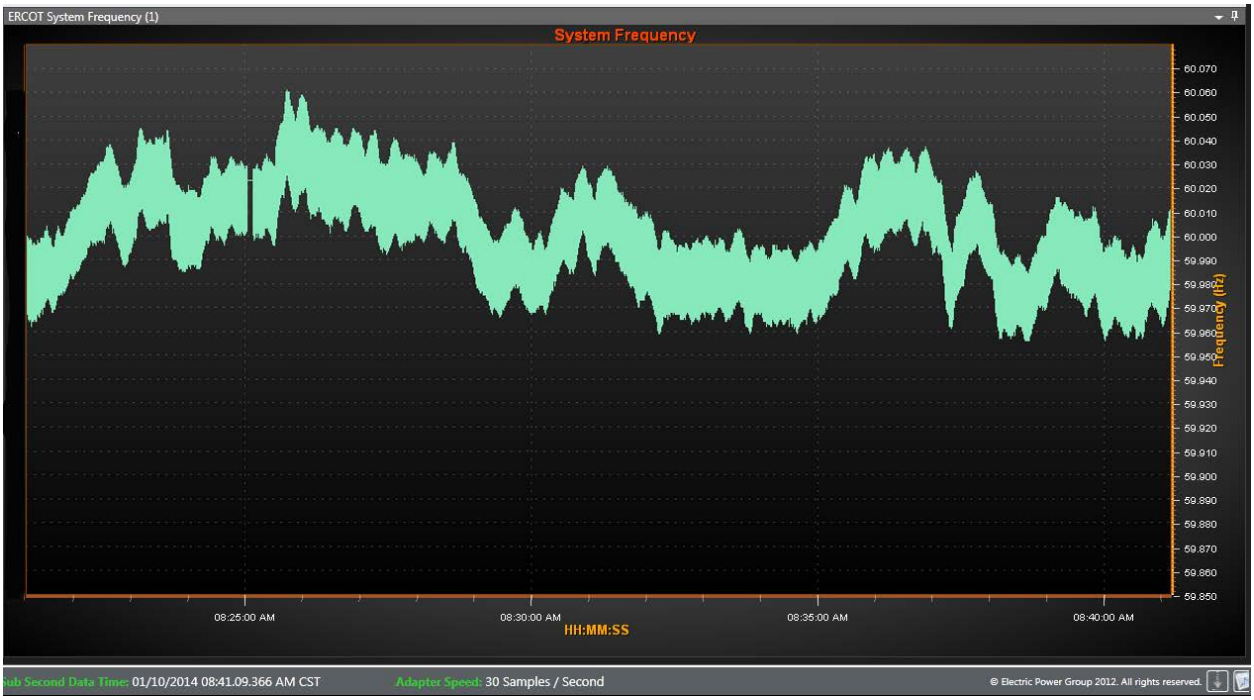


Figure 1. Frequency at Wind Farm PMU on RTDMS System on 10 January 2014.

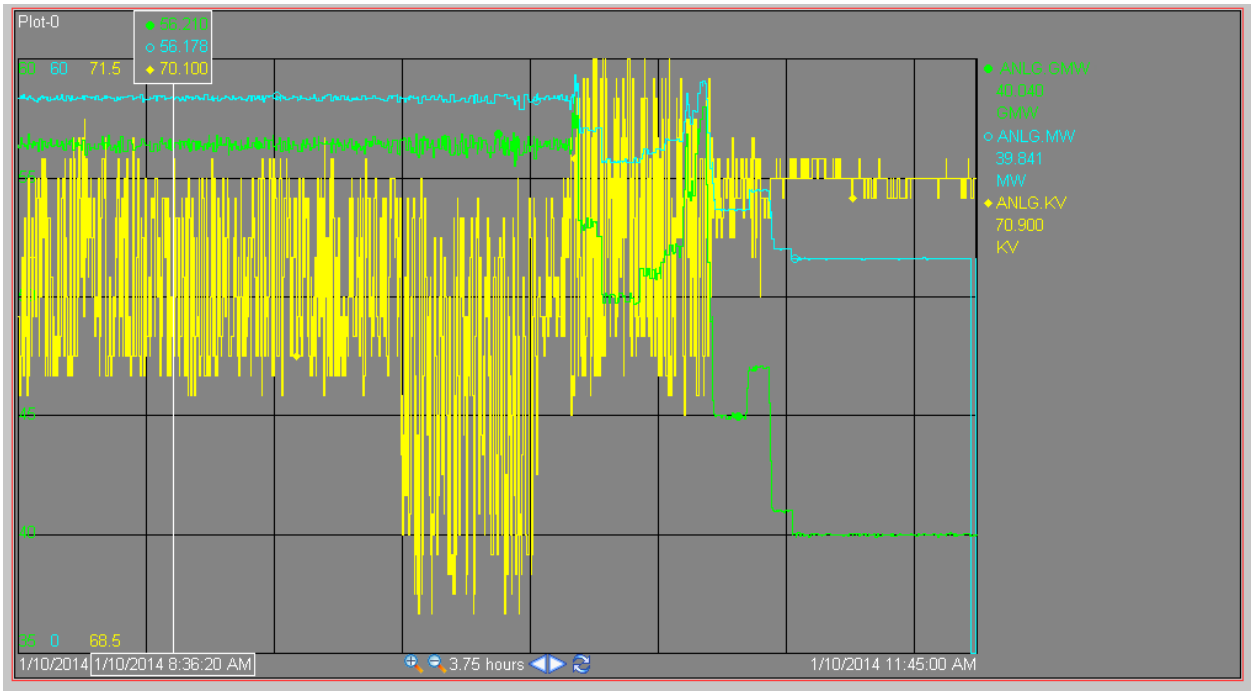


Figure 2: EMS Trend for Generation at the Wind Farm on 10 January 2014.

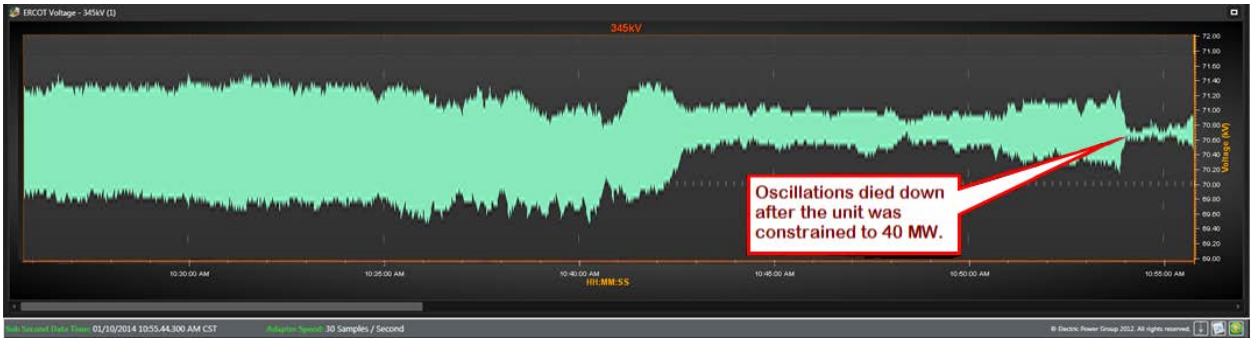


Figure 3: Reduction of Oscillations after Constraining the Plant to 40 MW on 10 January 2014.

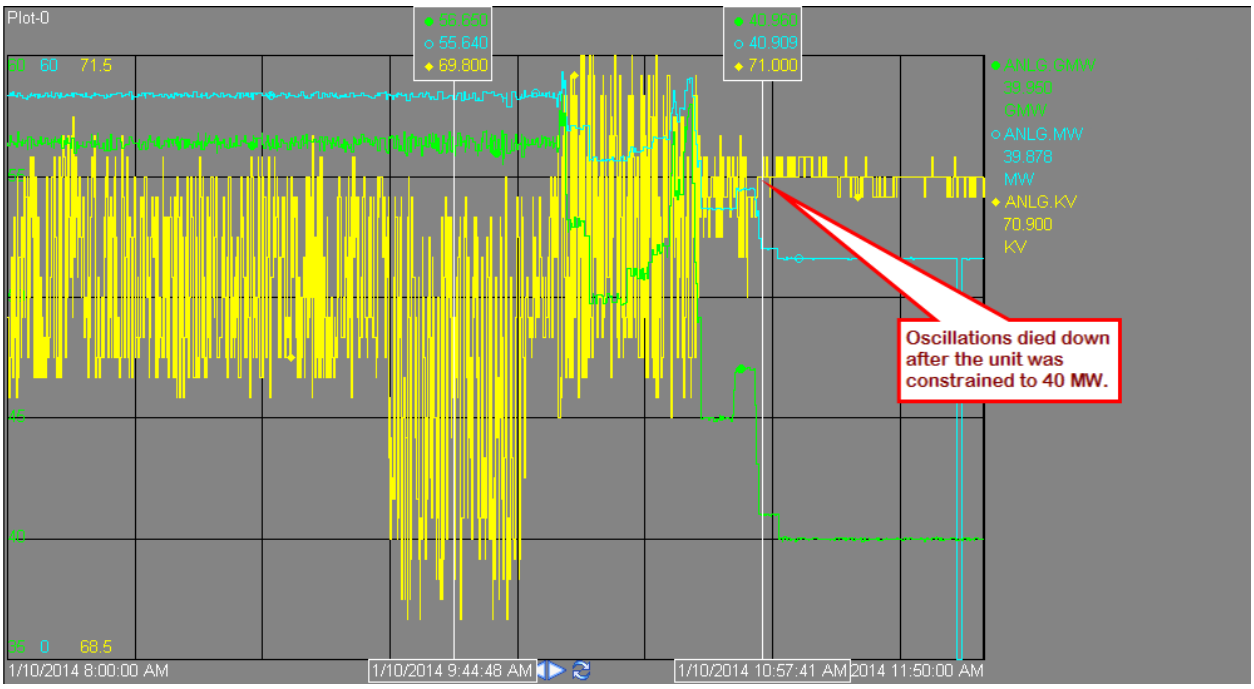


Figure 4: EMS Trend for Generation at the Wind Farm on 10 January 2014.

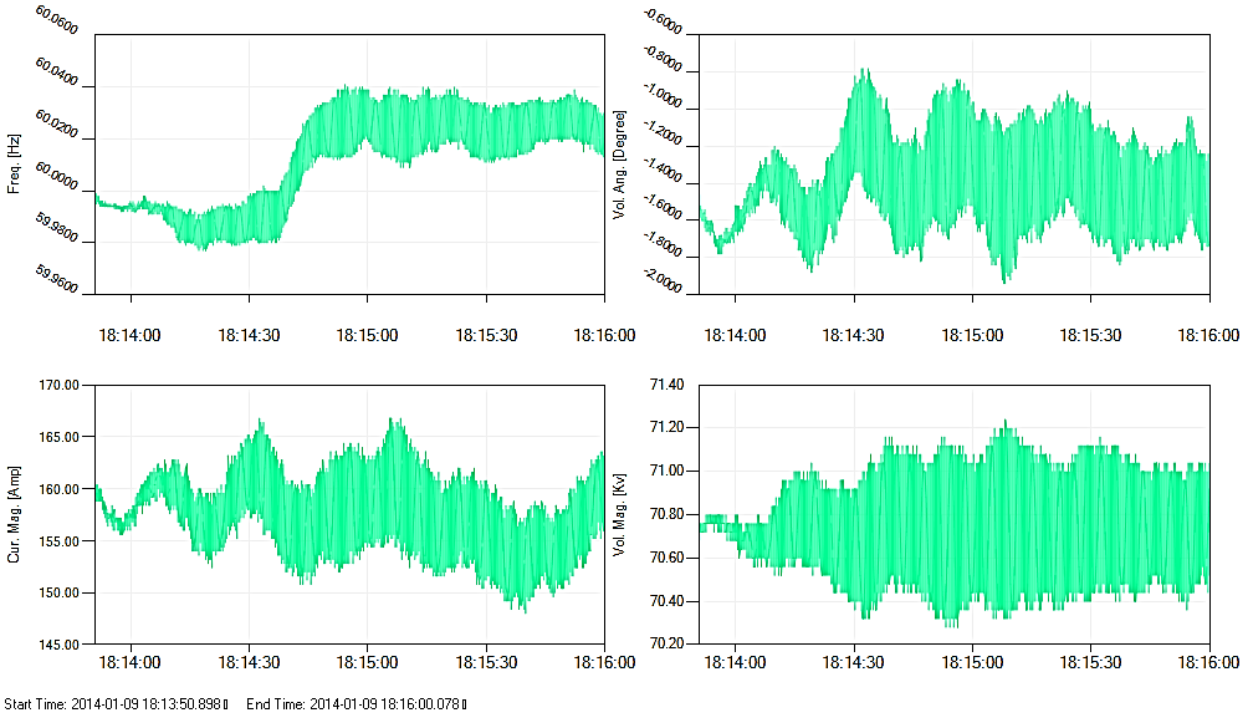


Figure 5: The Frequency, Voltage and Current Captured by the Wind Farm PMU on 9 January 2014

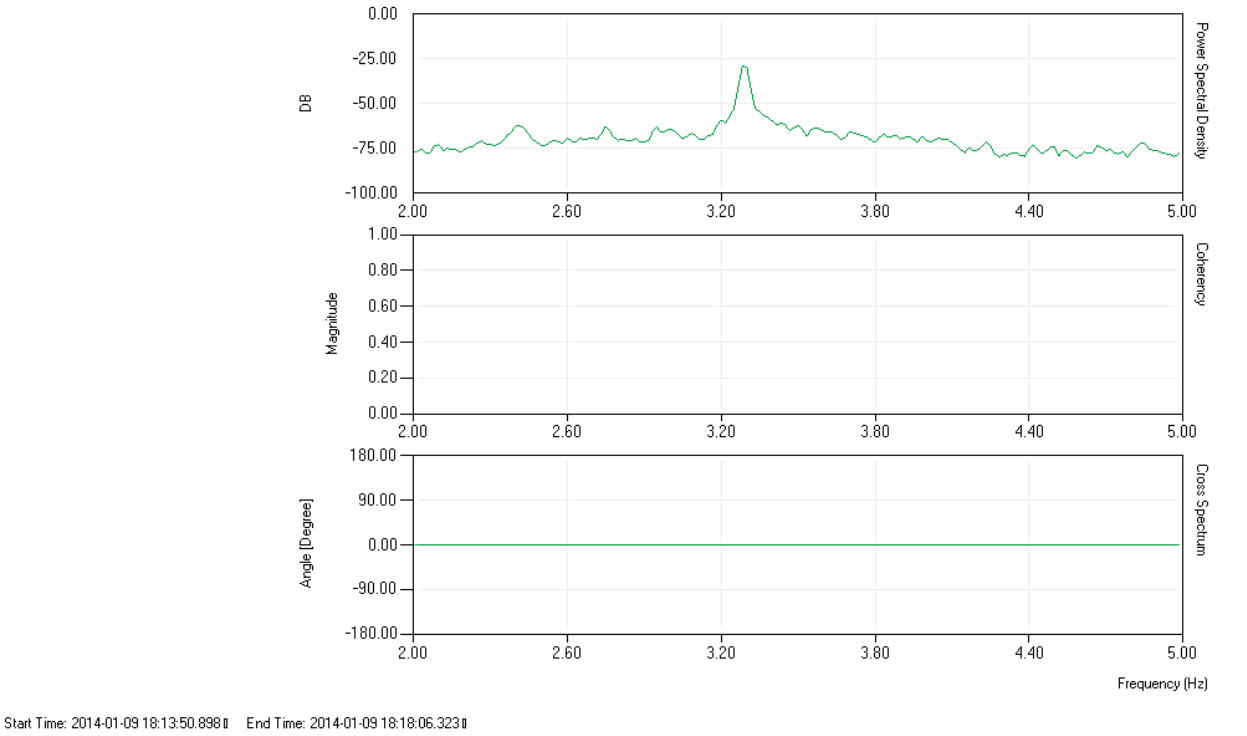


Figure 6a: Modal Analysis of the Frequency Data using PGDA on 9 January 2014.

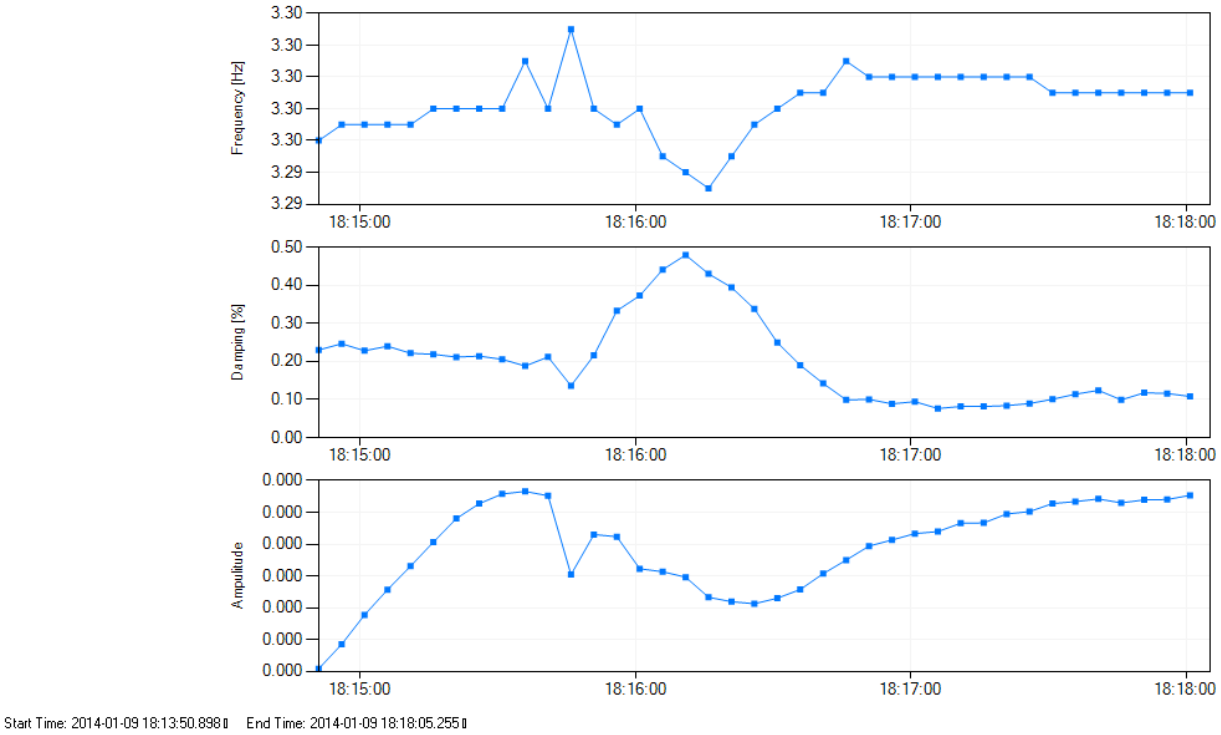


Figure 6b: Modal Analysis of the Frequency Data using PGDA on 9 January 2014.

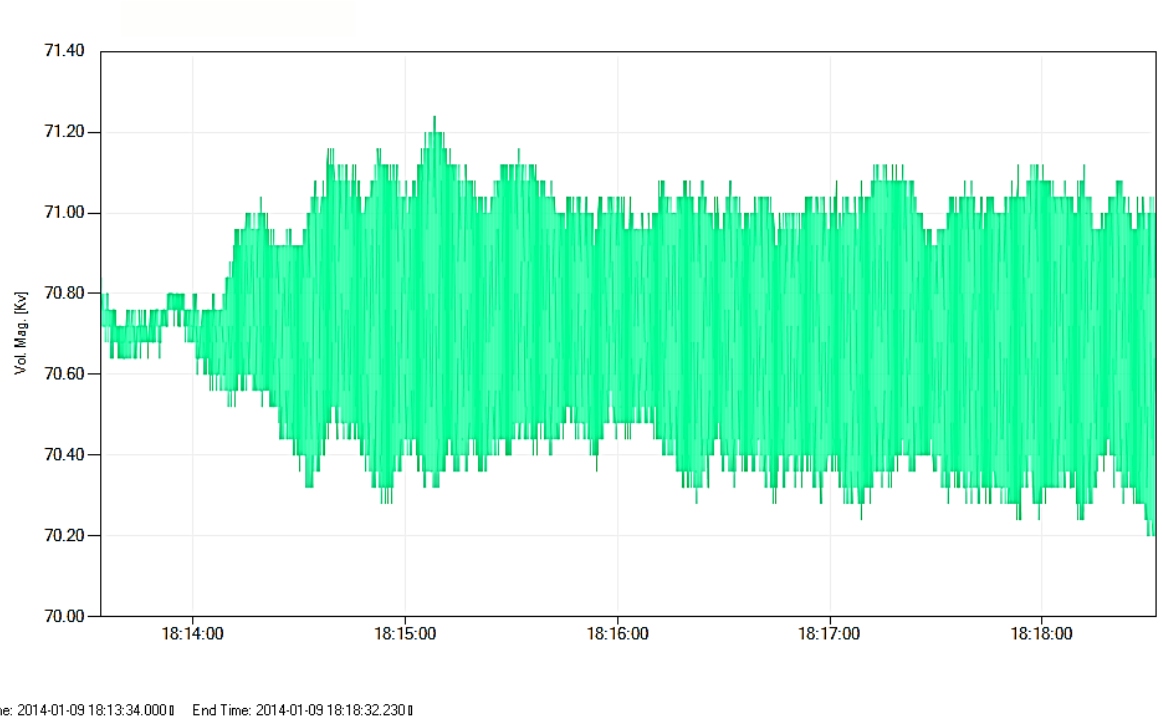


Figure 7: Voltage Oscillations at Wind Farm

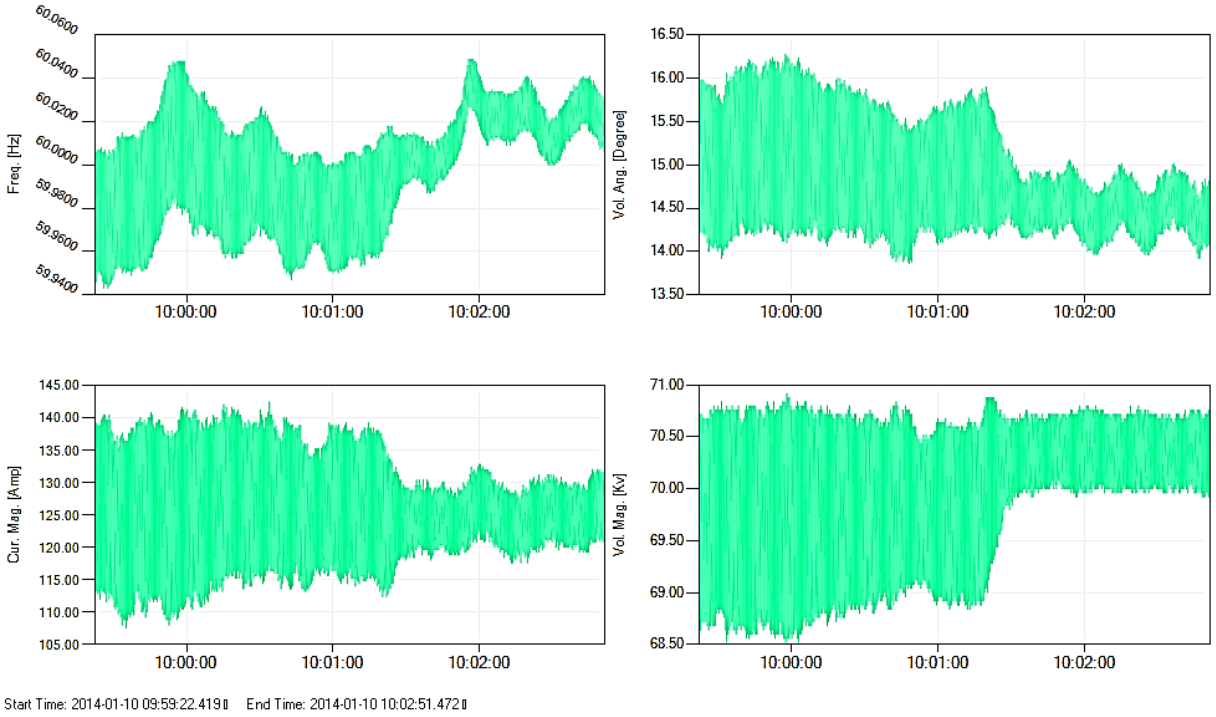


Figure.8: The Frequency, Voltage and Current Captured by the Wind Farm PMU on 10 January 2014

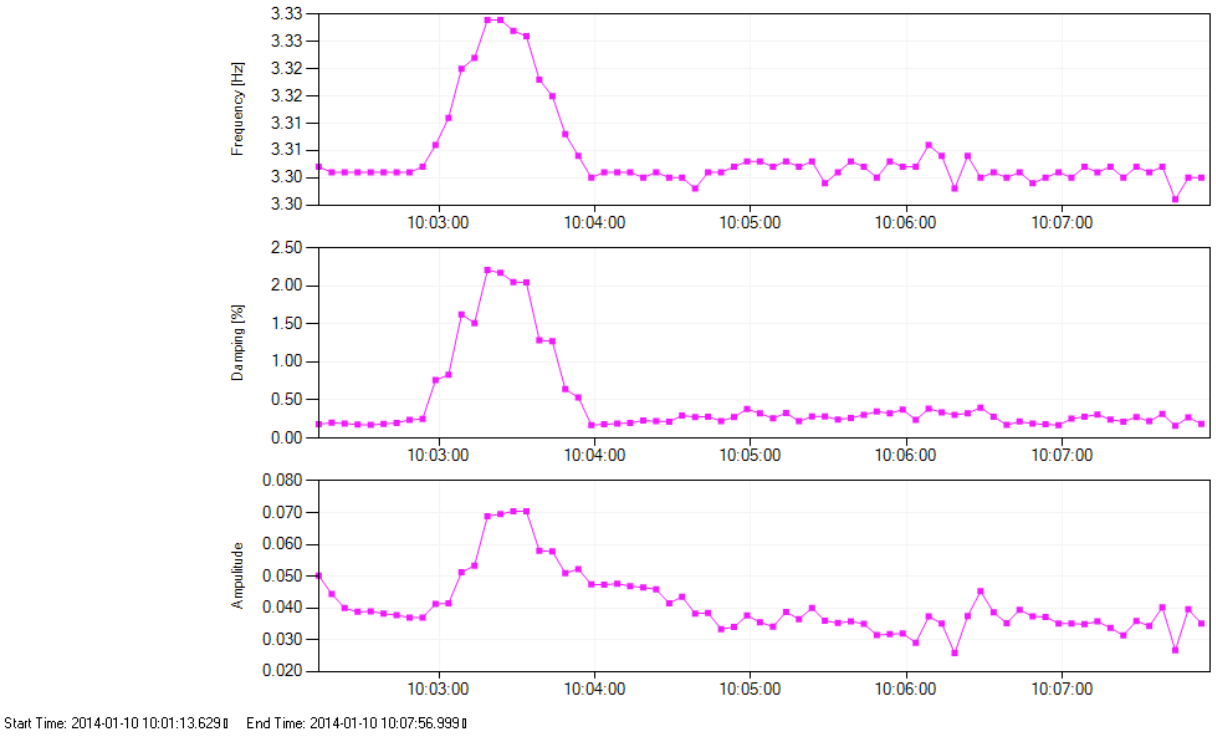


Figure 9: Modal Analysis of the Frequency Data using PGDA on 10 January 2014.

Attachment 9. PMU Event Analysis Report for 18 & 27 February 2014

EVENT DETAILS

On February 18th, 2014, at about 8:30 am, after logging on into RTDMS system, ERCOT Operations Engineers noticed oscillations on the RTDMS displays as shown in Figure 1. On analysis, it was found that the oscillations were showing up only at Line 1@West 4 PMU as shown in Figure 2a and Figure 2b. ERCOT looked at the generation at the Hydro Unit close to West 4 PMU. It was generating about 25 MW (Figure 3). It was found that when the unit went offline at about 10:00 am, the oscillations died down as shown in Figure 4. It was noticed that, when the second unit at the same plant was running there were no oscillations observed. Oscillations showed up again on February 27th, 2014 when Unit 1 came online, as shown in Figure 5a and Figure 5b. Analysis of these oscillations using Phasor Grid Dynamics Analyzer (PGDA) tool indicated that the dominant mode that was present was 1.8 Hz as shown in Figures 6a and 6b. ERCOT discussed with the power plant operators to find the root cause of these oscillations with one of the units of the plant. It was confirmed that they could also see the oscillations for that unit. It was then decided that the plant operators would change some of the control cards for the problematic unit and test to see if it would solve the problem. Usually they operate the units alternatively. Since ERCOT was going through some severe weather conditions, the plant operators decided to operate only the good unit until ERCOT passed through this severe weather conditions. On March 5th, when weather conditions were good, Unit 1 (for which some of the control cards had been replaced) was brought online at about 4:00 pm (Figure 7). It was found that the oscillations were significantly reduced, as shown in Figure 7a, Figure 7b, and Figure 7c, after the control cards were replaced.

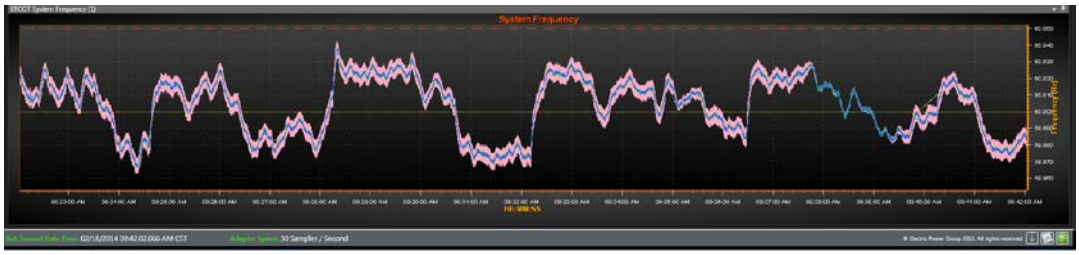


Figure 1: Frequency Oscillations on RTDMS System on February 18th, 2014.

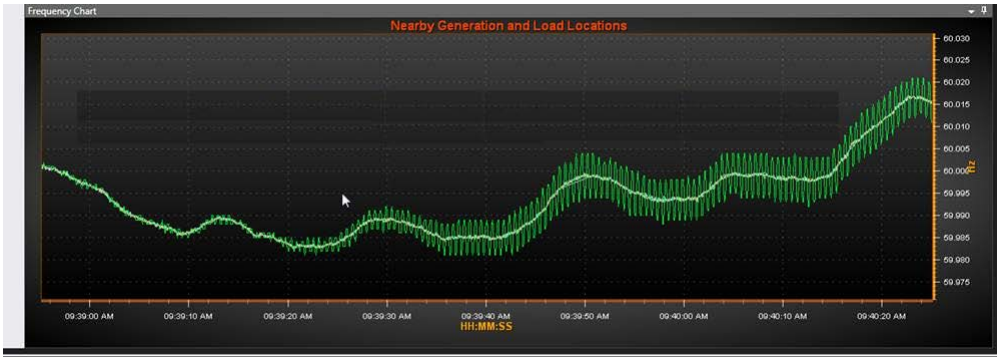


Figure 2a: Frequency Oscillations in West 4 PMU on February 18th, 2014.

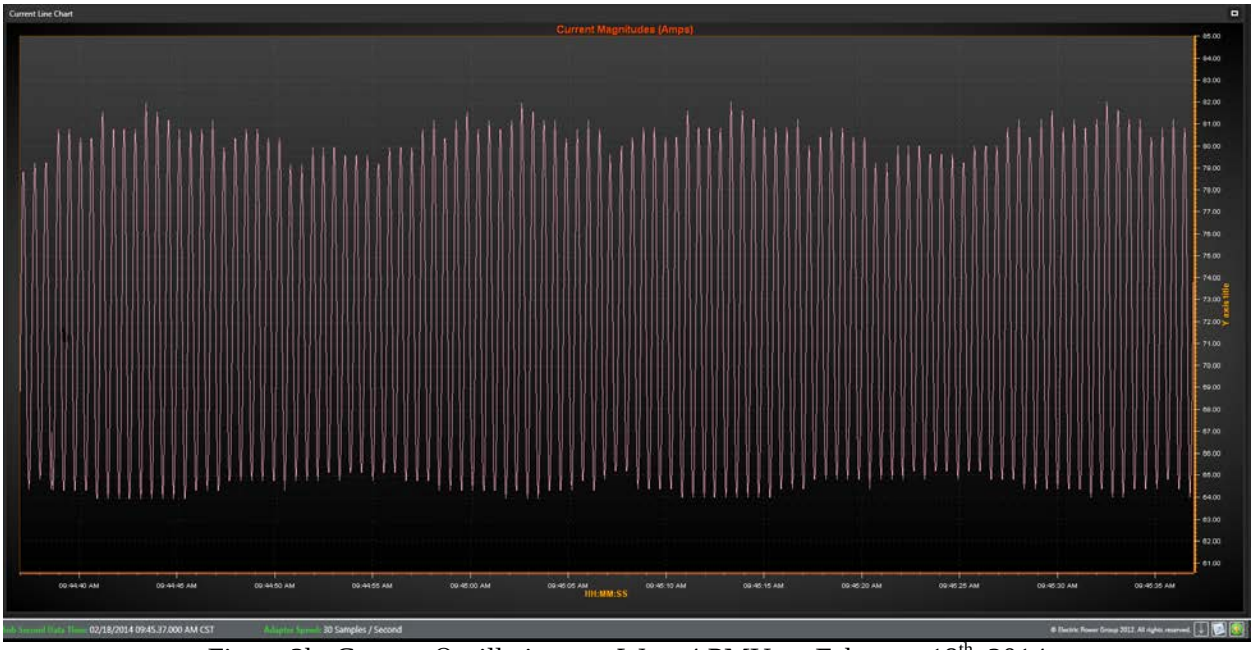


Figure 2b: Current Oscillations on West 4 PMU on February 18th, 2014.

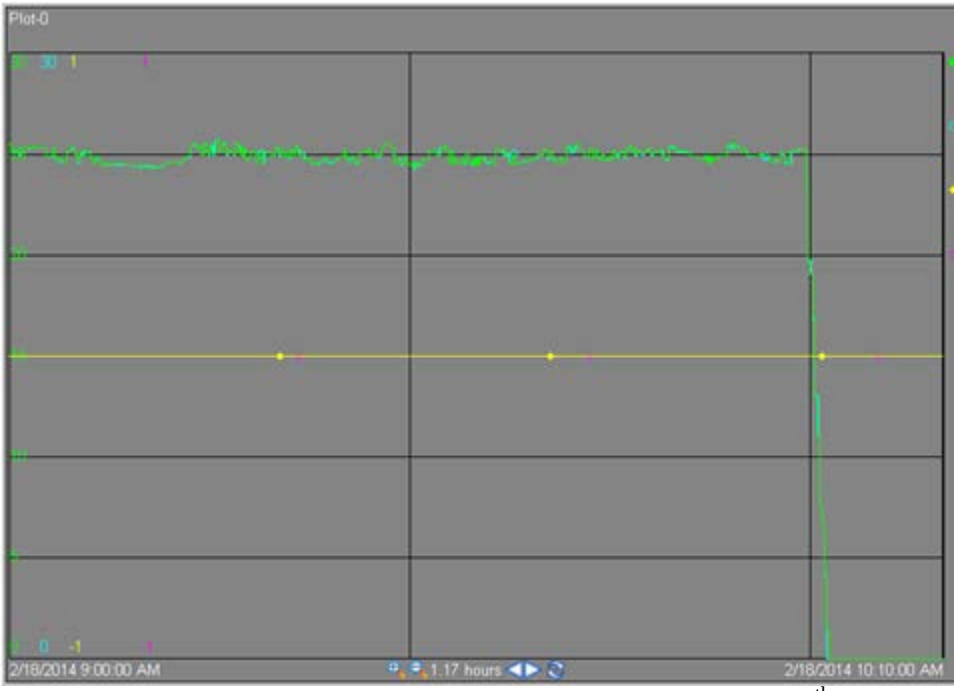


Figure 3: EMS Trend for Generation at the Power Plant on February 18th, 2014 at 10:00 a.m.

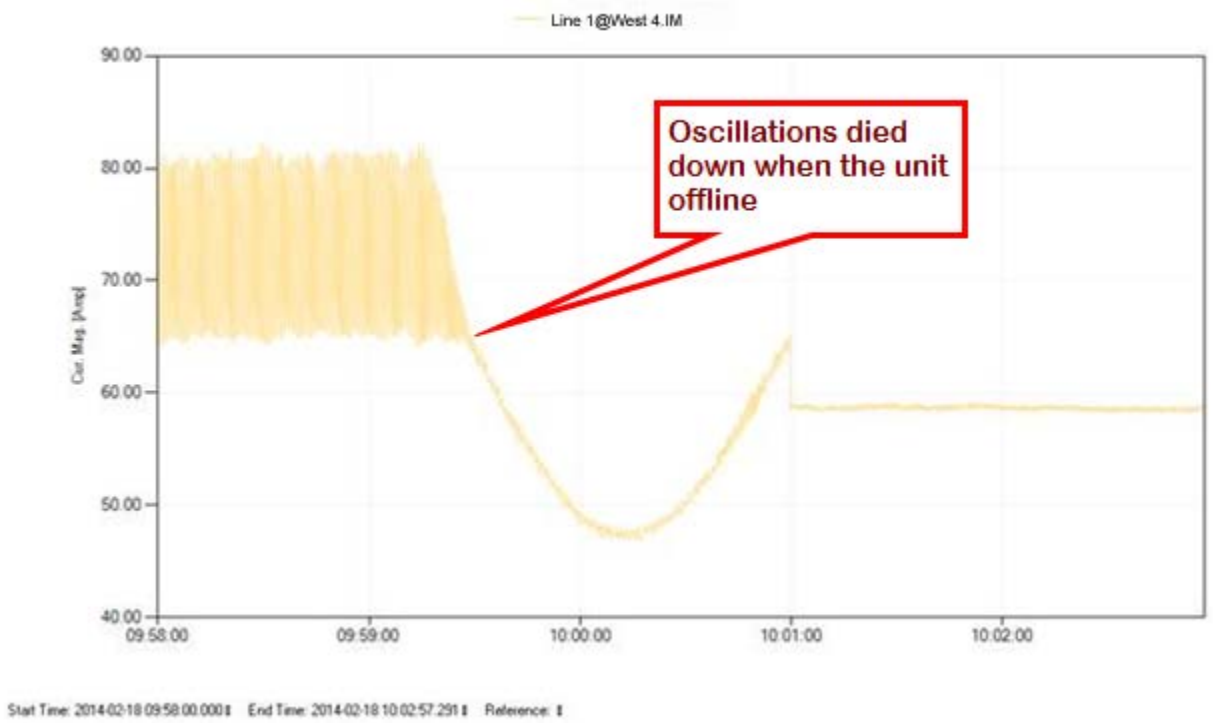


Figure 4: Current Oscillations when the Unit Went Offline on February 18th, 2014 at 10:00 a.m.

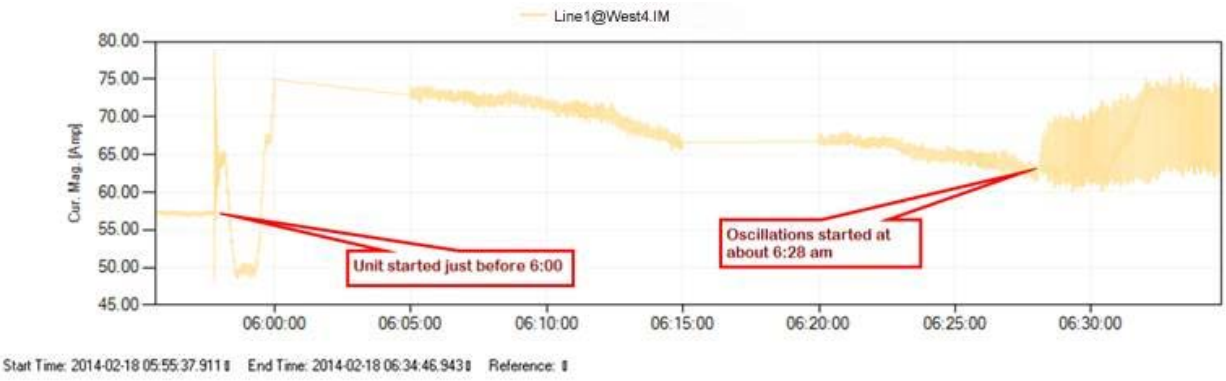


Figure 5a: Oscillations on February 27th, 2014

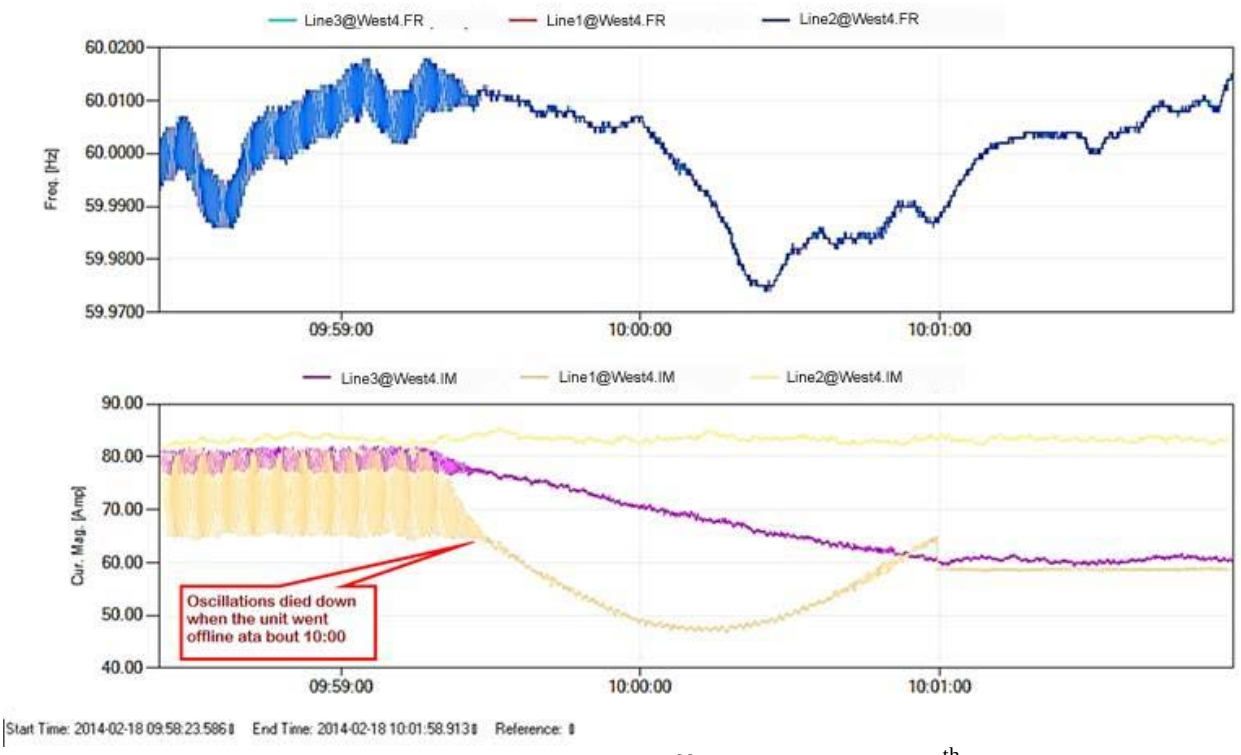


Figure 5b: Oscillations when the Unit Went Offline on February 27th, 2014 at 9:59 a.m.

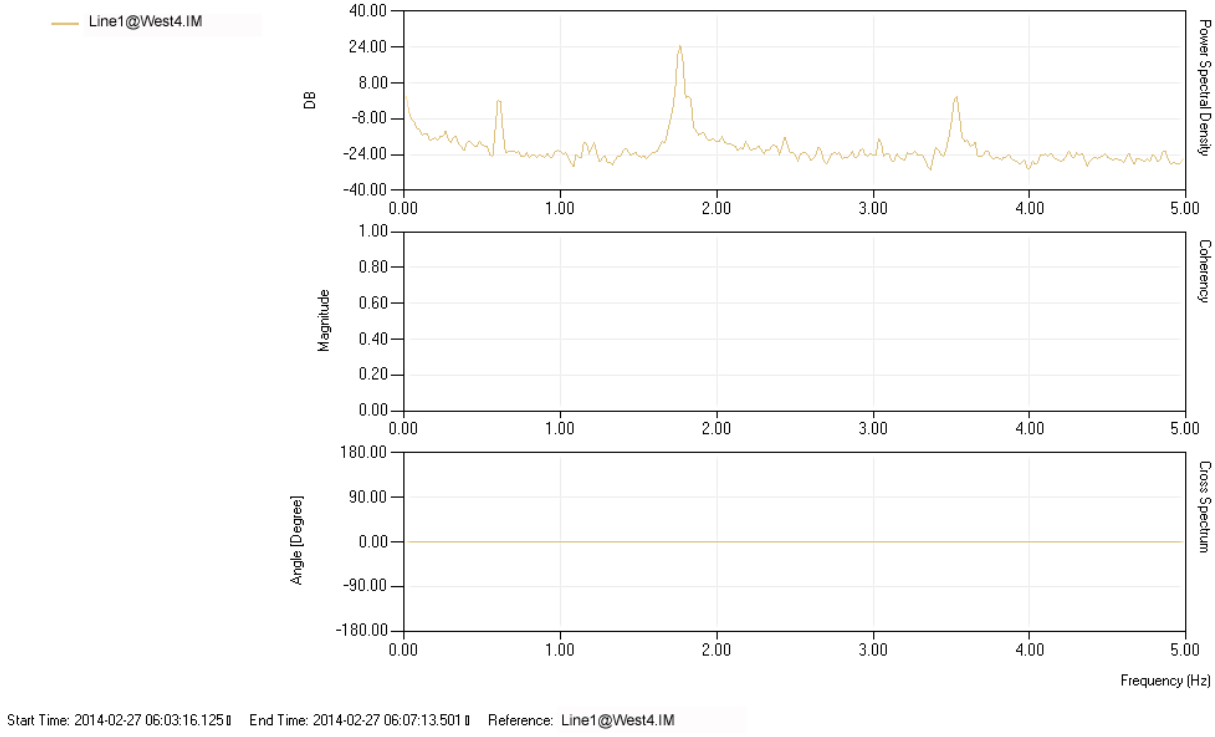


Figure 6a: Modal Analysis of the Current Data using PGDA on February 27th, 2014.

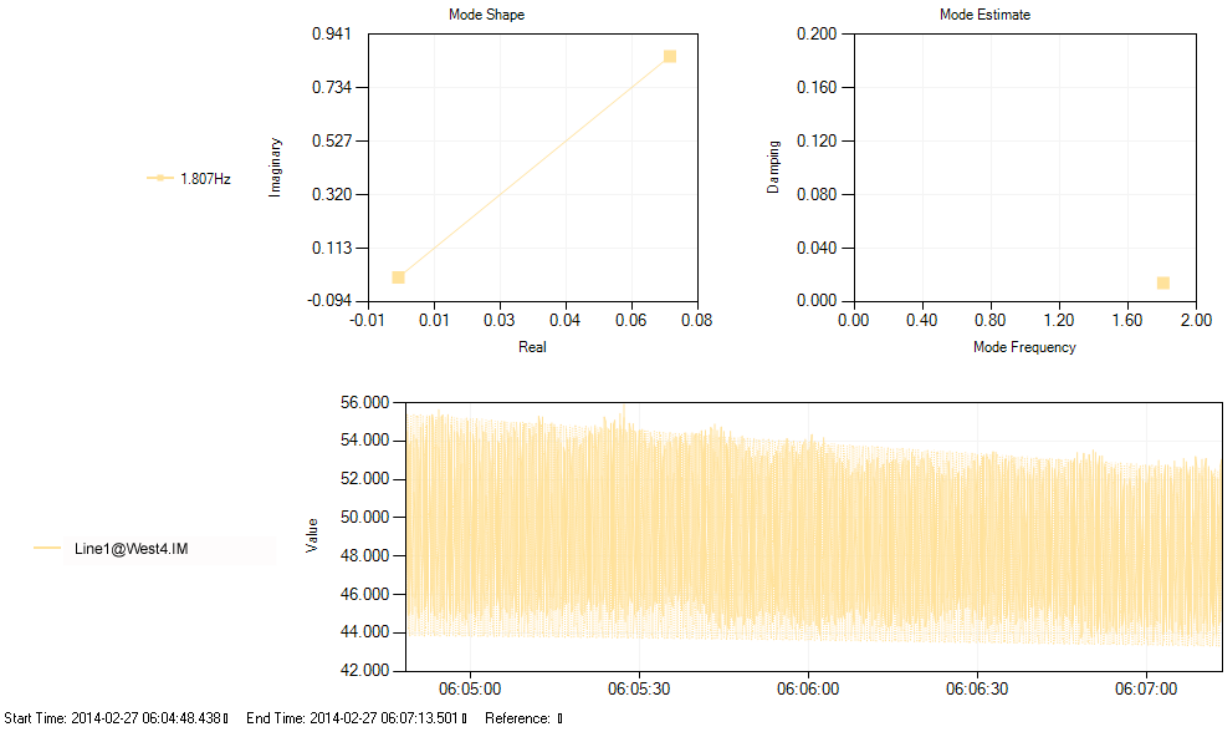


Figure 6b: Modal Analysis of the Current Data using PGDA on February 27th, 2014.

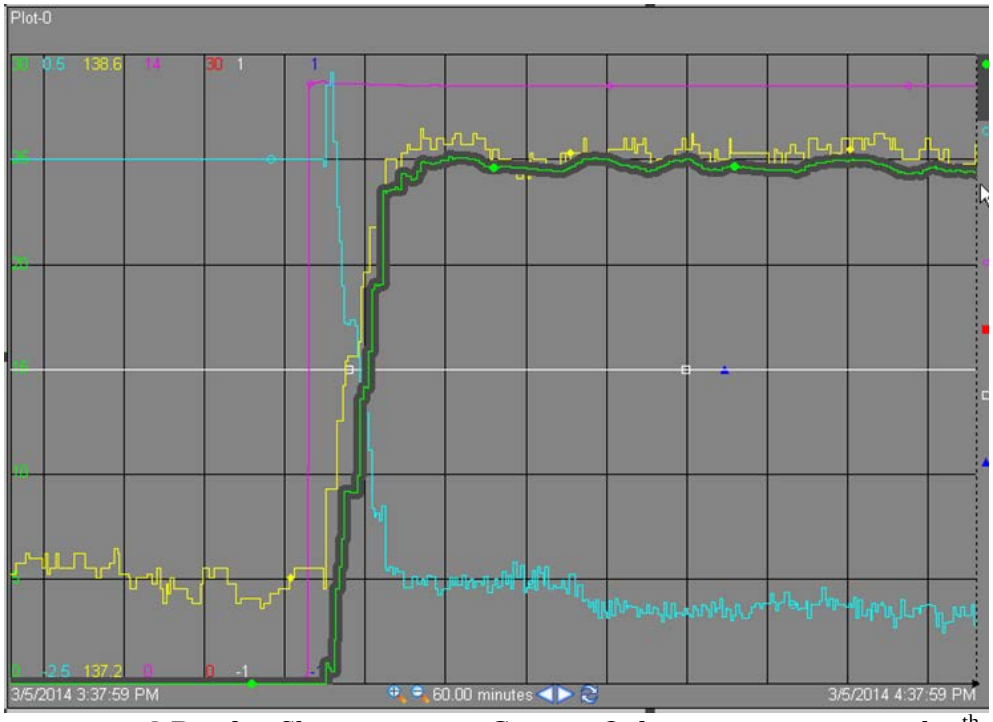


Figure 7: EMS Display Showing Unit 1 Coming Online at 4 p.m. on March 5th, 2014

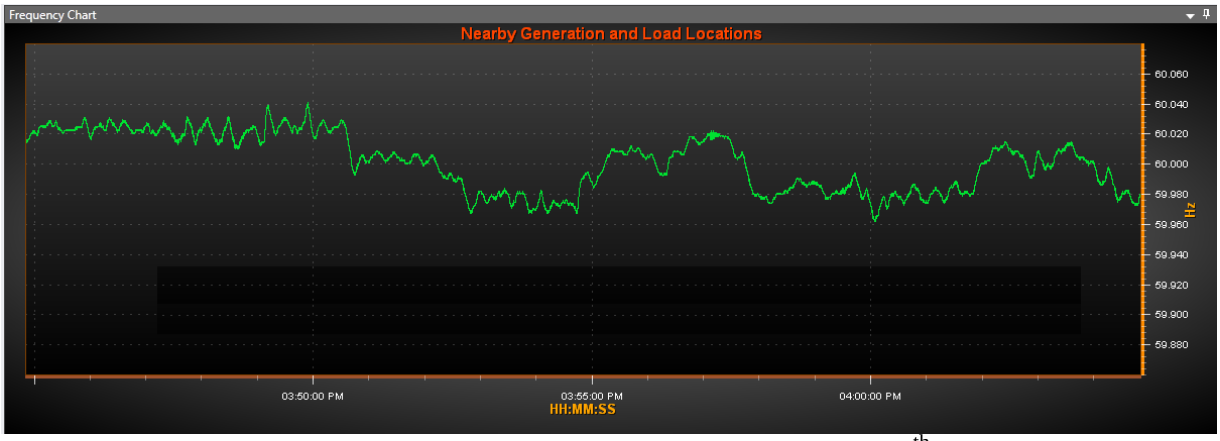


Figure 8a : Frequency Display on RTDMS on March 5th, 2014

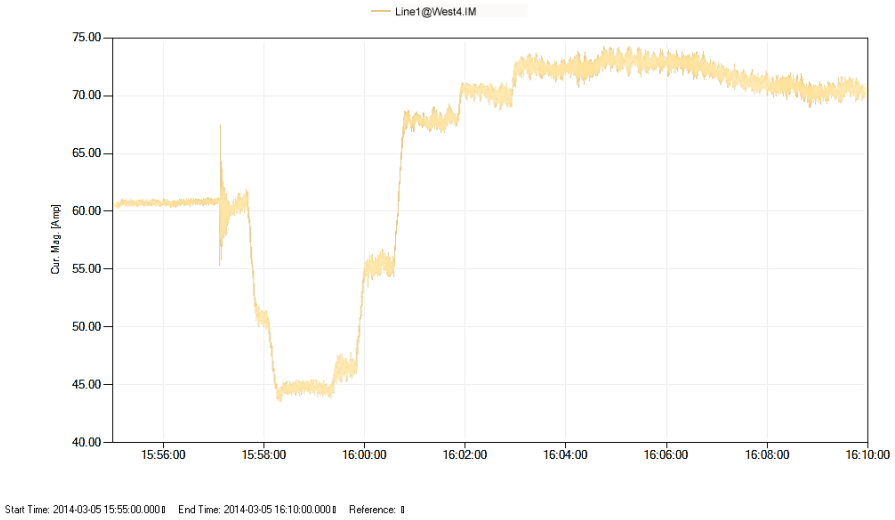


Figure 7b: Current Display on PGDA on March 5th, 2014

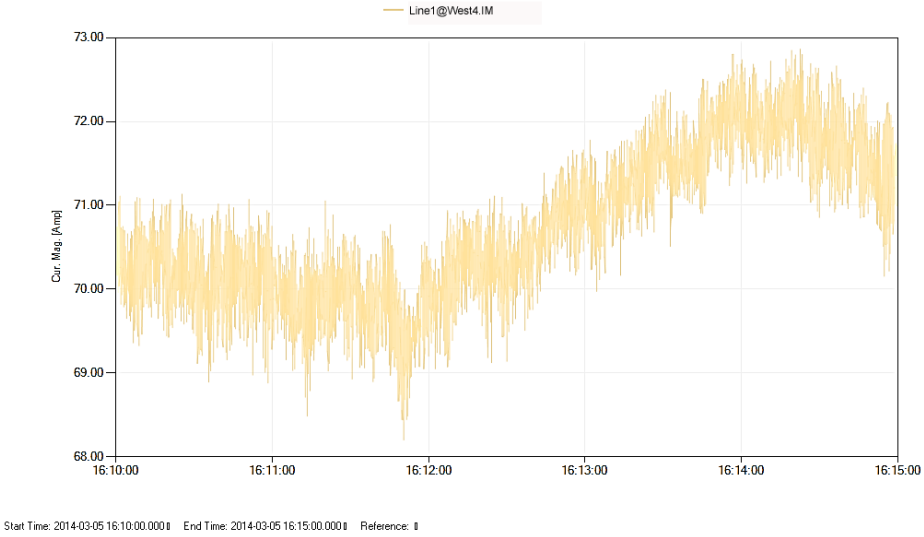


Figure 7c: Current Display on PGDA on March 5th, 2014

Attachment 10. Inertial Frequency Response Study

Center for Commercialization of Electric Technologies (CCET)

Discovery Across Texas Project

Final Report on

Wind Characteristics

Inertial Frequency Response Study

Submitted to
Milton Holloway, Ph.D.
mholloway@electrictechnologycenter.com

Prepared by:

Electric Power Group

John W. Ballance
Prashant C. Palayam

October 30, 2014

Table of Contents

List of Figures

CCET Discovery Across Texas

Wind Characteristics – Inertial Frequency Response Study

CCET 3.1.3, Task c

1. Introduction

The Center for Commercialization of Electric Technologies (CCET) was awarded contract DE-OE0000194 by the Department of Energy to perform the Discovery Across Texas demonstration project. Electric Power Group, LLC (EPG) received a sub-award from CCET to provide professional services to perform, among other things, an analysis of the impact of increasing levels of wind generation on the inertial frequency response of the Electric Reliability Council of Texas (ERCOT) grid. Texas has the greatest amount of wind generation online in the nation, and attains a new wind production record every year. Increasing wind production and penetration (percentage of total energy production) into the grid under different operating conditions poses operating challenges for ERCOT. One of the challenges with high wind penetration is to maintain an adequate level of inertial frequency response that is crucial to ensure reliable operation of the grid. Inertial frequency response represents the inherent resistance of the grid to frequency decline following a sudden loss of generation. It is measured by the amount of generation loss (in MW) required to cause a first swing frequency decline of 0.1 Hz, and a larger value corresponds to increased grid resilience. This study was initiated to investigate the contribution of wind generation to the ERCOT grid inertial frequency response based on a starting hypothesis that a decline in inertial frequency response, with respect to increasing levels of wind generation, was being observed in the ERCOT Interconnection.

This analysis summarizes four illustrative scenarios that collectively conclude that wind generation provides no significant contribution to inertial frequency response. Rather, inertial frequency response appears to be primarily dependent upon the total amount of non-wind generation available online, including non-wind generation that is unloaded but online to provide spinning reserve. This report provides insights on the minimum amount of non-wind generation needed to maintain adequate levels of inertial frequency response under all conditions for the ERCOT Interconnection.

2. Executive Summary

Texas has the greatest amount of wind generation online in the nation, and attains a new wind production level every year. With increasing amounts of wind production and penetration into the grid under different operating conditions, there are challenges and observations faced by ERCOT. One of the challenges with high wind penetration is to maintain an adequate level of inertial frequency response that is crucial to ensure reliable operation of grid.

A generator unit trip or sudden loss of generation will result in a frequency drop due to the imbalance between generation and load. The frequency drop gets arrested by the inertial frequency response. Inertial frequency response represents the inherent resistance of the grid to frequency decline following a sudden loss of generation. It is measured by the amount of generation loss (in MW) required to cause a first swing frequency decline of 0.1 Hz, and a larger index corresponds to increased grid security. Inertial frequency fesponse is illustrated in Figure 2.

Inertial frequency response is a measure of how far the frequency will drop following loss of a generator. Primary and secondary frequency response (including automatic governor and load response actions together with operator-dispatched generating reserves) will eventually restore the frequency back to a nominal system frequency value. This study was proposed to investigate the contribution of wind generation on inertial frequency response based on a starting hypothesis that a decline in inertial frequency response with respect to increasing wind generation was being observed in ERCOT Interconnection. The performance of inertial frequency response was investigated at different levels of wind generation as part of this analysis.

This analysis was based on 183 generator trip frequency events, collected over three years (2012-2014), to investigate the contribution of wind generation on the inertial frequency response of the ERCOT grid. Inertial frequency response was calculated for each individual event using Electric Power Group's Phasor Grid Dynamics Analyzer (PDGA) and correlated with different operating conditions using an assumed linear relationship between the amount of generation loss and the corresponding frequency drop. For the analysis, ERCOT load, ERCOT generation, ERCOT wind generation, ERCOT spinning reserves, and phasor measurement unit (PMU) data collected from substations located nearby wind units were collected and analyzed to quantify the variation and trend in inertial frequency response. There was empirical evidence from operating performance of a general decline in inertia with increasing levels of wind generation. This analysis identified four different illustrative scenarios which collectively lead to a conclusion that wind generation does not contribute to inertial frequency response.

The key findings that suggest there is no contribution from wind generation to inertial frequency response are:

1. The seasonal trend of inertial frequency response remained the same even at different levels of wind penetration, indicating no relationship between response and penetration.
2. Inertial frequency response and the total level of non-wind generation online had a strong positive correlation, suggesting inertia is proportional to non-wind generation.

3. The generation trip events, which showed a decline in inertial frequency response with higher wind generation, were found to have lower non-wind generation online.
4. There was no significant increase in the power output from the wind plants (as measured by the nearby PMUs) coincident with frequency drop for each of the frequency events, indicating no inertia contribution from the wind plants. In contrast, the power flows from locations near non-wind generation showed coincident power flow changes.

This study concludes that inertial frequency response of the ERCOT Interconnection is directly correlated to the amount of non-wind generation available online, and finds that the level of wind generation has no impact on the inertial frequency response. The report also provides insights on the minimum amount of non-wind generation that would need to be maintained online in order to maintain minimum levels of inertial frequency response under all operating conditions.

3. Goals & Methodology

The objective of this analysis was to identify if wind generation contributed to inertial frequency response. Utilizing 183 different generator trip events, during the period of 2012-2014, the study set four goals:

1. Calculate the inertial frequency response for each event.
2. Estimate the typical inertial frequency response under different operating conditions (e.g., high wind/low load, high wind /high load, low wind/high load, etc.).
3. Find any identifiable trends in inertial frequency response with respect to increasing levels of wind generation under different conditions of ERCOT:
    a. Load
    b. Total generation
    c. Wind generation
    d. Spinning reserves
4. Identify the causes of different levels of inertia.

Figure 1 shows the flowchart that describes the workflow of the analysis study. The different steps in the analysis study were:

Step 1 Identify and collect PMU data containing frequency events (generator trips) for three years.
Step 2 Gather ERCOT EMS data associated with each event.
Step 3 Gather amount of generation loss in MW from the EMS logs associated with each event.
Step 4 Using PGDA, calculate the inertial frequency response associated with each event.
Step 5 Tabulate each event and its associated EMS data & calculated inertial frequency response.
Step 6 Calculate variables and derive metrics needed for the study.

Step 7 Conduct analysis to achieve the goals for this study.

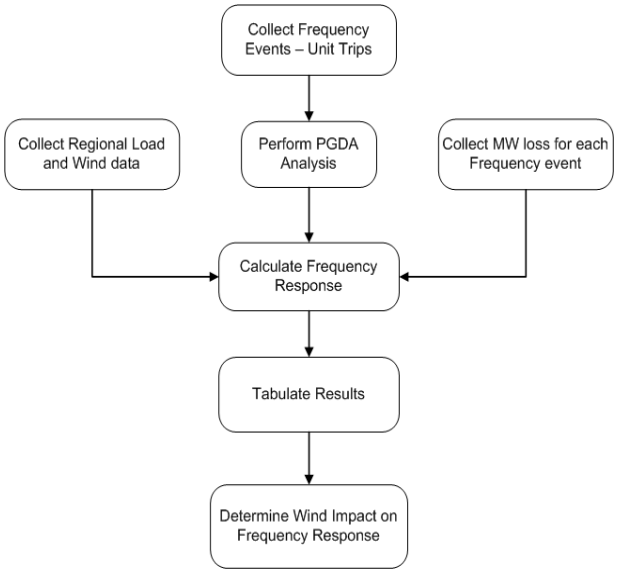


Figure 1. Analysis Workflow

4. Derived Metrics & Calculated Variables

The following data associated with each event was collected from the ERCOT EMS:

1. Regional wind data.
2. Regional load data.
3. Total generation.
4. Spinning reserve data.
5. Total amount of generation loss.

The variables calculated for this study are:

1. Total Online Generation = Total Generation + Spinning Reserves (MW).
2. Wind Generation = Summation of Regional Wind Data (3 Regions)
    a. ERCOT Wind = West + North + South (MW)
3. Non-Wind Generation = Total Online Generation – Wind Generation (MW).
4. ERCOT Load = Summation of Regional Load Data (8 Regions)
   ERCOT Load = Coast + East + Far West + North + North Central + Southern + Southern Central + West (MW)

The metrics derived for this study are:

1. Percentage of wind generation (%) = (wind generation / total online generation) * 100.
2. Inertial frequency response (MW/0.1Hz)= (amount of generation loss) / (F_A - F_C)*0.1
    a. F_A – represents value of frequency in Hz immediately before the disturbance.
    b. F_C – represents the lowest value of frequency in Hz, which occurred within 12 seconds of initial disturbance.
    c. (F_A - F_C) – represents the frequency drop (Hz).

5. Inertial Frequency Response Calculation – Using PGDA

The inertial frequency response calculation for each event is calculated based on the amount of generation loss and change in frequency during the frequency event. The unit for inertial frequency response is MW/0.1 Hz.

Inertial Frequency Response = (Amount of Generation Loss) / (F_A - F_C)*0.1 (MW/0.1Hz).

a. F_A – represents value of frequency in Hz immediately before the disturbance.
b. F_C – represents the lowest value of frequency in Hz.
c. (F_A - F_C) – represents the frequency change (Hz).

The frequency change calculation is automated in PGDA by identifying the start of disturbance, and lowest value of frequency, during the disturbance using the North American Electric Reliability Corporation (NERC) methodology. For a given period of time containing frequency event data, the event start time T(0) is determined and then F_A and F_C are calculated. The algorithm used to calculate the:

F_A – average frequency value between T(-16) and T(-1)

F_C – lowest frequency value within 12 seconds after T(0)

The inertial frequency response is calculated for each event to study its seasonal trend over three years, and its correlation with the amount of wind generation online during each event.

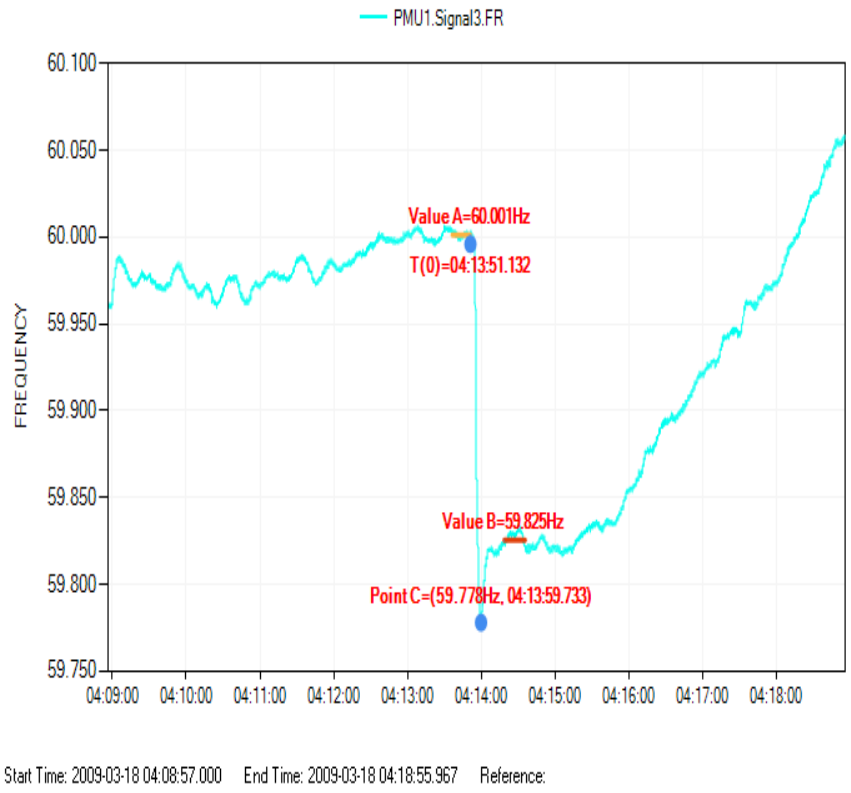


Figure 2. PGDA Event Analysis Plot

6. Inertial Frequency Response Estimation – Using Linear Relationship

The inertial frequency response estimation for a group of events is done based on an assumed linear relationship between the amount of generation loss (MW) and the associated frequency change (Hz). The inertial frequency response is estimated from the slope of the linear regression model, between the generation loss and frequency change. The linear regression model is intercepted at zero, based on the assumption that there will be no change in frequency change (0 Hz) for no loss of generation (0 MW). Figure 3 shows the estimation of inertial frequency response for 2014, by grouping all 27 events. The inertial frequency response for 2014 is estimated at approximately 444 MW/0.1Hz. Figures A-1 and A-2 in the Appendix show the estimation of inertial frequency response for 2012 and 2013, respectively.

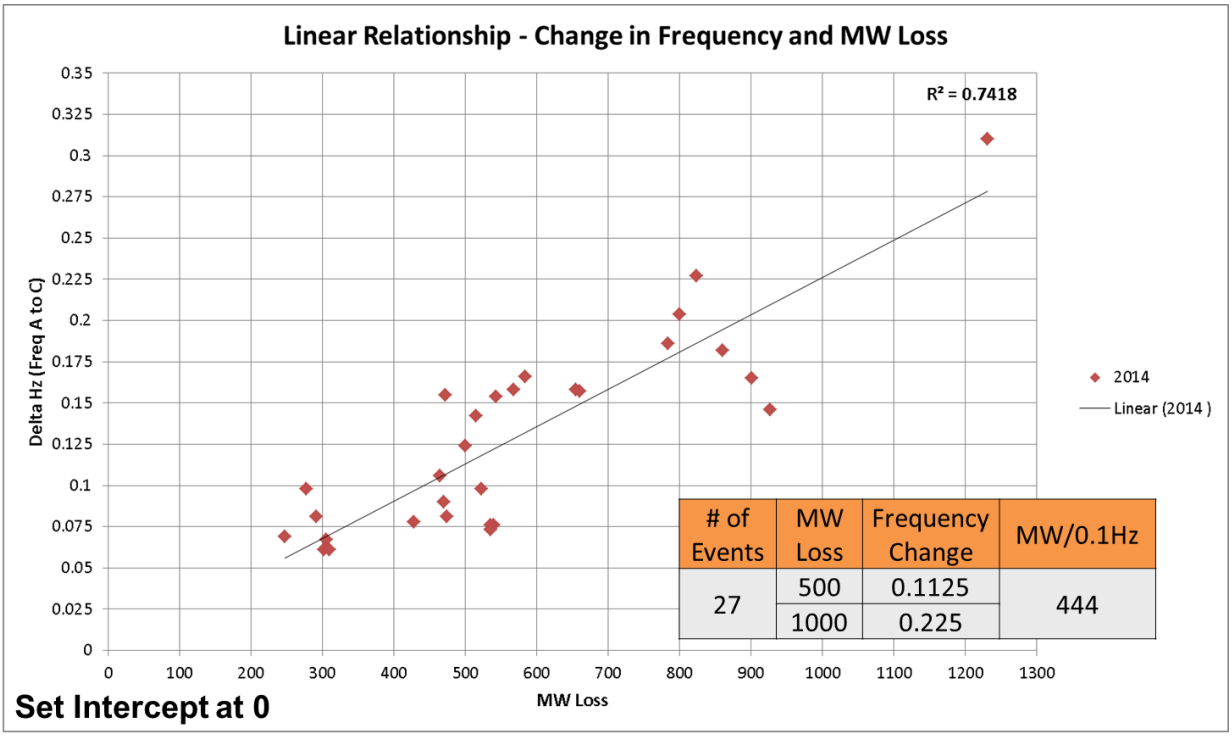


Figure 3. Estimation of Inertial Frequency Response – 2014

The above technique was used to estimate the inertial frequency response at:

1. Different levels of wind generation.
2. Different levels of load.

And to assess:

1. If there is any decline in inertial frequency response with increasing levels of wind.
2. If the above statement is true, is the decline the same or different at high load and low load conditions.

7. Decline in Inertial Frequency Response During High Wind Generation

The estimation of inertial frequency response, using a linear relationship, was applied to different levels of wind generation. Figure 4 shows the estimation of inertial frequency response for 2014, under two levels of wind penetration (percentage of wind generation to total online generation) without filtering on different load conditions. The two levels of wind penetration chosen were:

1. <= 10%
2. > 10%

There appears to be clear evidence of a decline in inertial frequency response by 40 MW/0.1Hz, as the wind penetration increases. But there can be other variables in the grid reducing the inertial frequency response such as load conditions, or the amount of non-wind generation. Hence, the hypothesis that there is a decline in inertial frequency response when wind penetration increases needs to be validated against different loading conditions in the grid.

The next section identifies different loading conditions, and examines the relationship between inertial frequency response and various levels of wind generation.

Figures A-3 and A-4 in the Appendix show the estimation of inertial frequency response for 2012 and 2013.

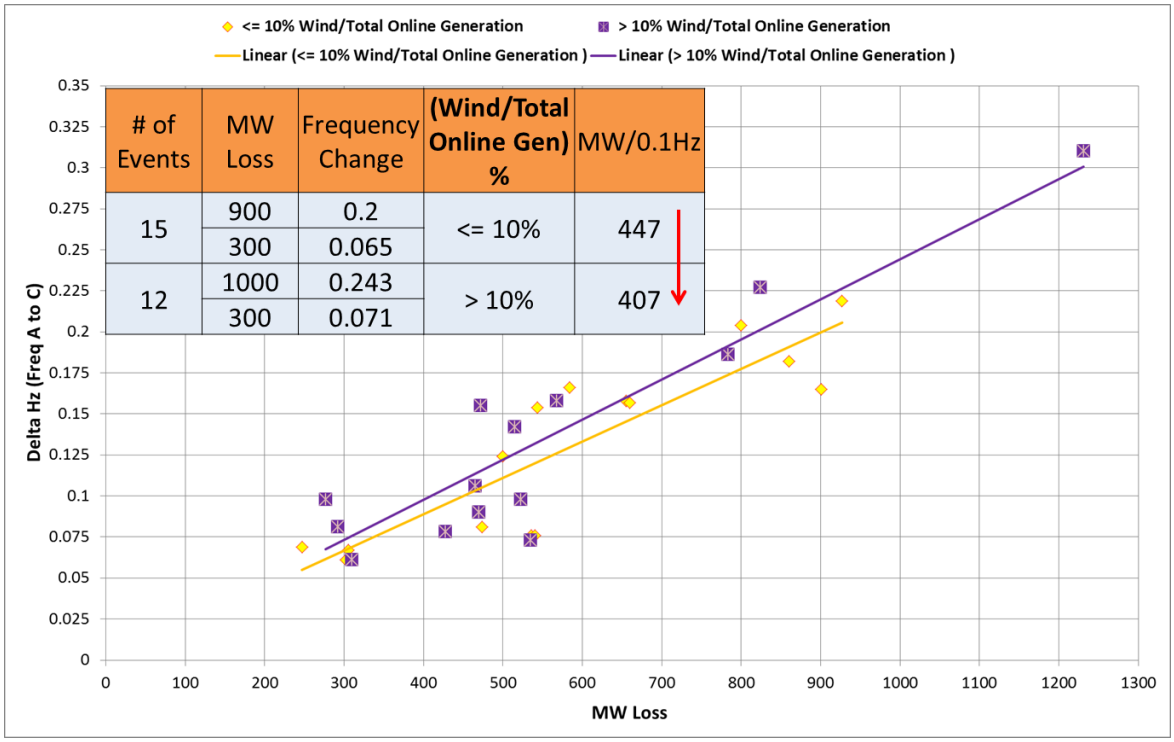


Figure 4. Estimation of Inertial Frequency Response (Two Wind Levels & No Load Levels) – 2014

8. Inertial Frequency Response Estimation – Under Operating Conditions

The load duration curve for 2012 was used to identify the loading conditions which would reasonably divide high versus low load. Figure 5a shows the ERCOT load duration curve for 2012, and identifies the median load at 50% of the year to be approximately 35,000 MW. The load duration curve was leveraged to identify other loading conditions such as:

1. Load < 30,000 MW.

2. Load > 35,000 MW.
3. Load > 40,000 MW.

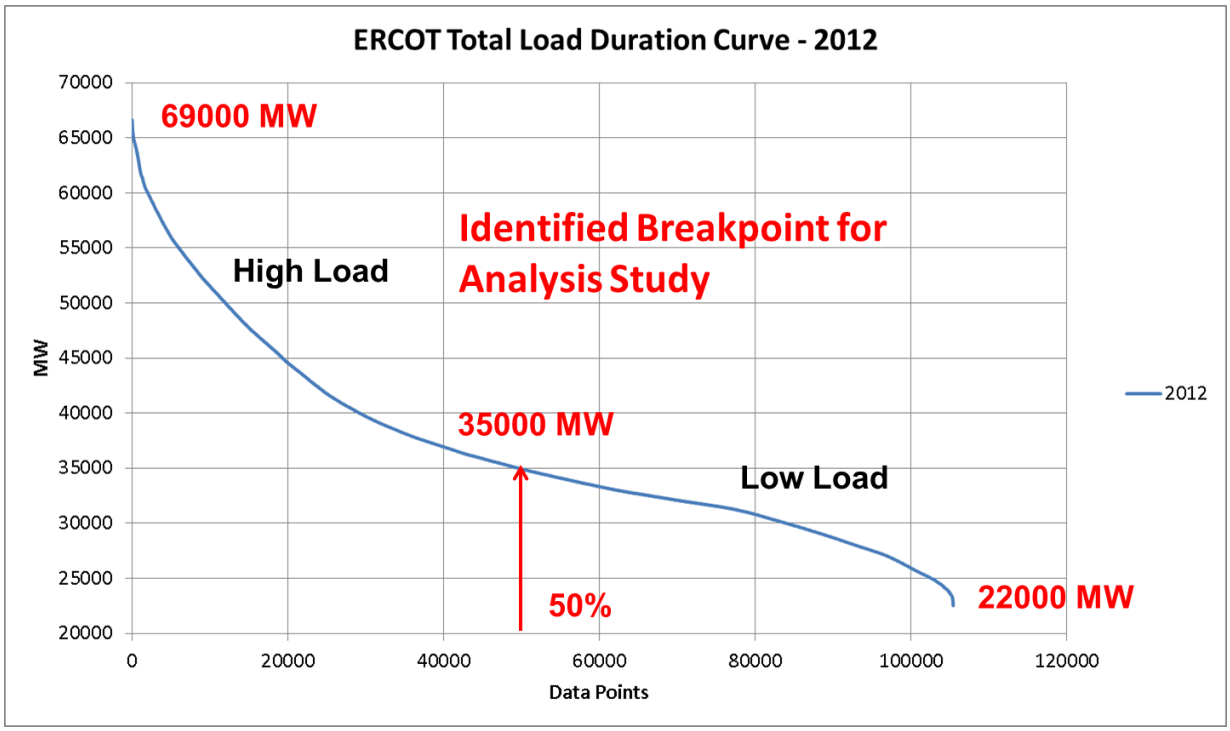


Figure 5a. Load Duration Curve – 2012

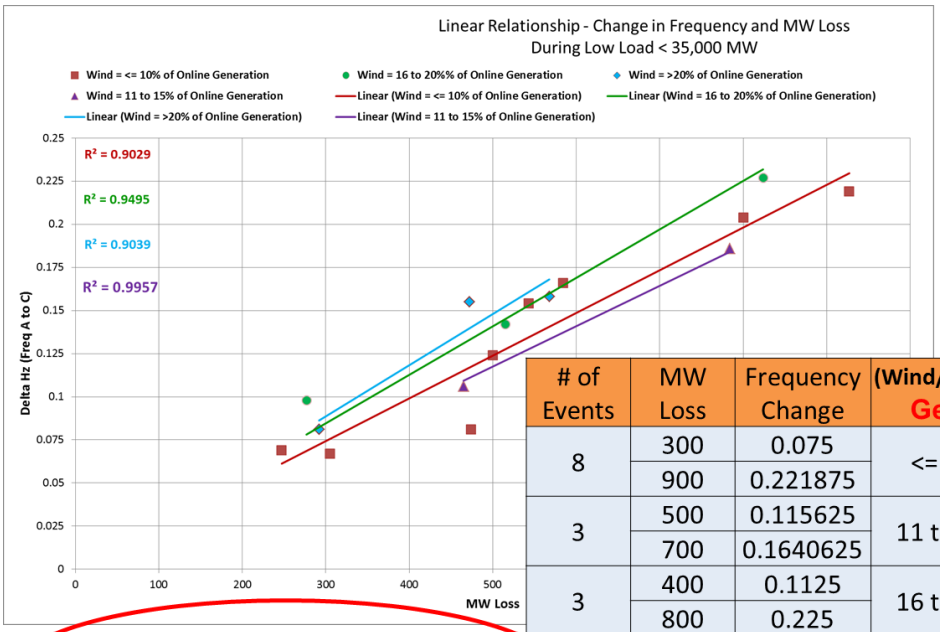
Figure 5b shows an example of estimating inertial frequency response for 2014, with load less than 35 GW using four different levels of wind generation. The events for this case were divided into four different levels of wind generation, and using the linear relationship between generation and frequency change, inertial frequency response was estimated under each level of wind. It is interesting to note that, even though inertial frequency response showed an overall decline with increasing wind generation, it was relatively insensitive to changes in wind generation below 15%, and to changes in wind generation greater than 15% (the inertial response dropped above 15%, but remained constant as generation exceeded 20%). This suggests that the percentage of wind generation, without consideration of different loading conditions, may not be the most useful metric.

Similarly, inertial frequency response was estimated for several loading conditions with different levels of wind generation, as shown in Figure 6. It suggests that at high levels of load (e.g., above 40 GW), increasing wind generation above 10% has little impact on inertial frequency response, while the same increase in wind generation seems to reduce inertial response at lower load levels. The inertial frequency response remained unchanged under:

1. Different levels of wind generation when load > 40 GW.

2. When Load > 35 GW and wind penetration is less than 10%.
3. When load < 35GW and wind penetration is less than 16%.

Figures A-5 to A-17 in the Appendix contain estimations of inertial frequency response under different loading conditions, and different levels of wind generation, for 2012, 2013 & 2014.



Decline in Inertia with increasing levels of wind resources

Increase in Inertia with increasing levels of wind resources

# of Events	MW Loss	Frequency Change	(Wind/Online Gen) %	MW/0.1Hz
8	300	0.075	<= 10%	408.5
	900	0.221875		
3	500	0.115625	11 to 15%	412.9
	700	0.1640625		
3	400	0.1125	16 to 20%	355.5
	800	0.225		
2	400	0.11875	> 20%	355.5
	500	0.146875		

Same Inertia, at Different Levels of Wind Impact

Figure 5b. Estimation of Inertial Frequency Response (Four Wind Levels & Load < 35GW) – 2014

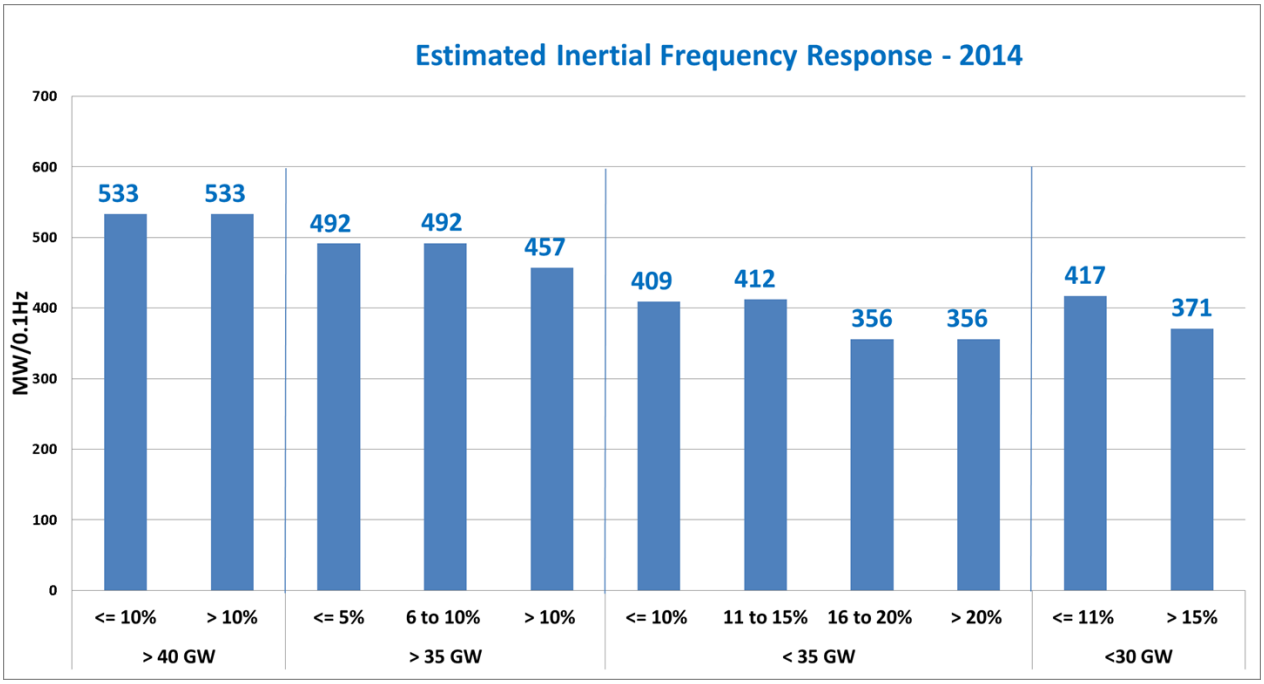


Figure 6. Estimation of Inertial Frequency Response (Different Wind Levels & Load Levels) – 2014

9. Wind Generation – No Contribution to Inertial Frequency Response

This section of the report provides four illustrative scenarios to support a conclusion that wind generation does not contribute to inertial frequency response. The four scenarios are:

1. Inertial Frequency Response vs. Wind Pattern.
2. Inertial Frequency Response vs. Non-Wind Generation Online.
3. Inertial Frequency Response vs. Different Operating Conditions.
4. Wind Output vs. Frequency Change (PMU Data).

1. Inertial Frequency Response vs. Wind Pattern

The calculated inertial frequency response for each event and the percentage of wind generation were compared to examine the relationship between them. Figures 7, 8, and 9 show the seasonal trends of inertial frequency response and percentage of wind generation for each generator loss event in all three years. The seasonal trend of inertial frequency response remained the same in all three years. The pattern of inertial frequency response was high in summer, low in winter, rising and falling during spring and fall, respectively in all three years. The pattern of inertial frequency response remained the same, even at different levels of wind penetration in all seasons, illustrating no relationship between them. The relationship between

inertial frequency response and wind generation was inverse in 2012, linear in 2013, and close to inverse in 2014 (first six months of 2014). The generation loss events occurred at different times during the day, and that had different levels of wind generation from year to year. Collectively, this illustrates that there is no simple relationship between inertial frequency response and the level of wind generation.

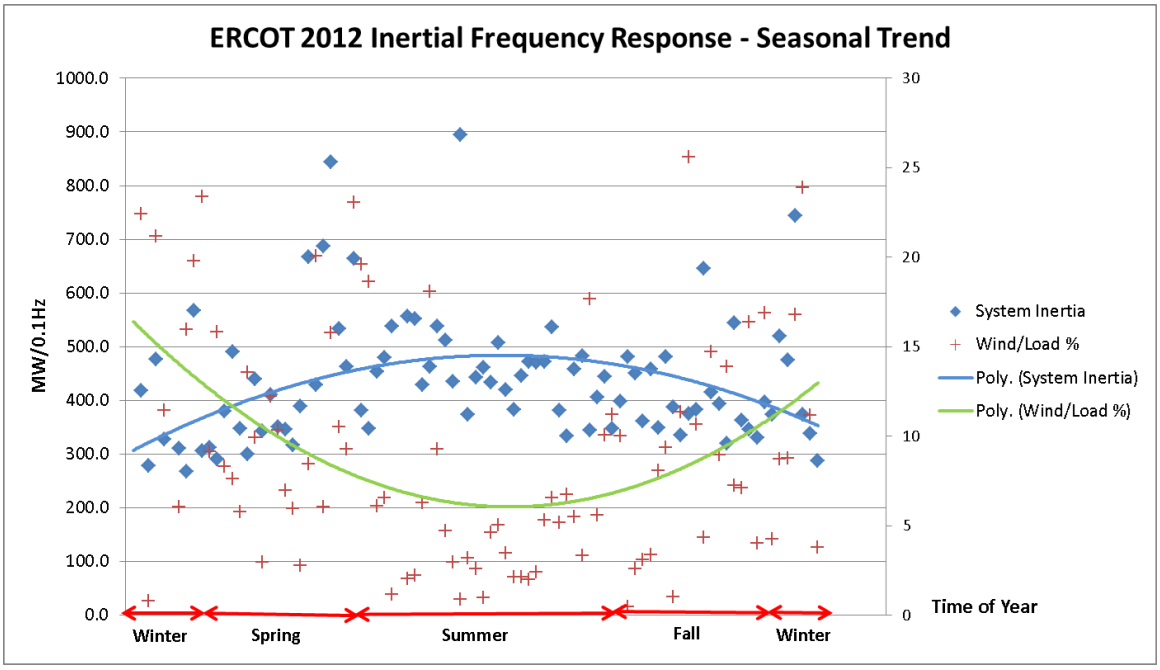


Figure 7. Seasonal Trend of ERCOT Inertial Frequency Response & Percentage of Wind Generation – 2012

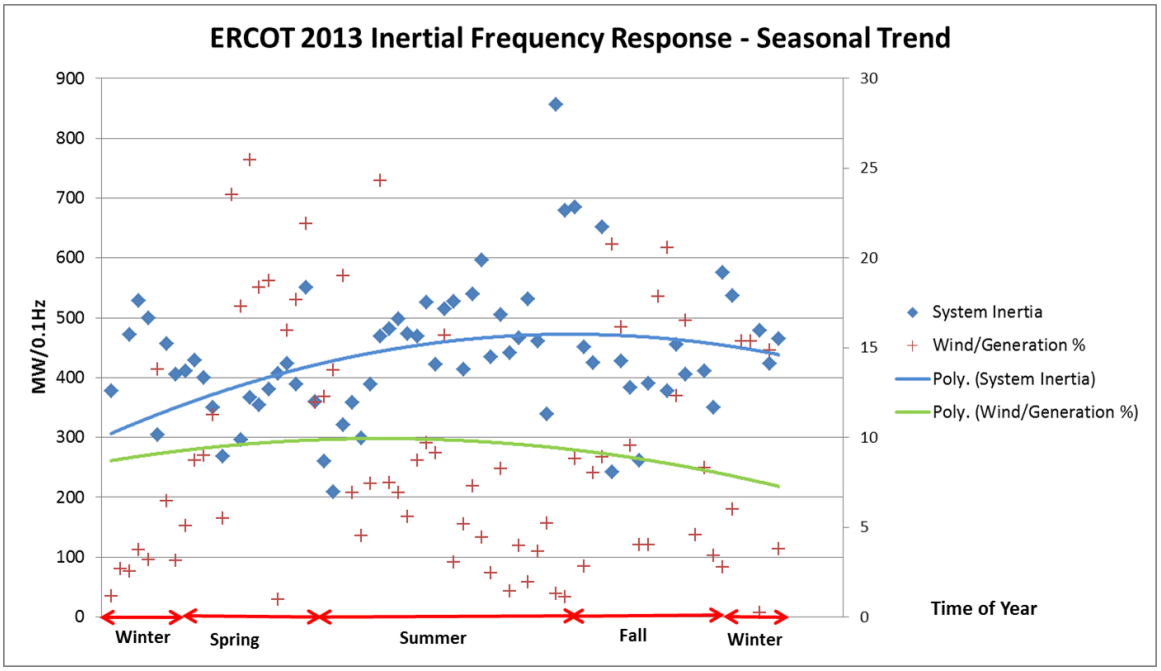


Figure 8. Seasonal Trend of ERCOT Inertial Frequency Response & Percentage of Wind Generation – 2013

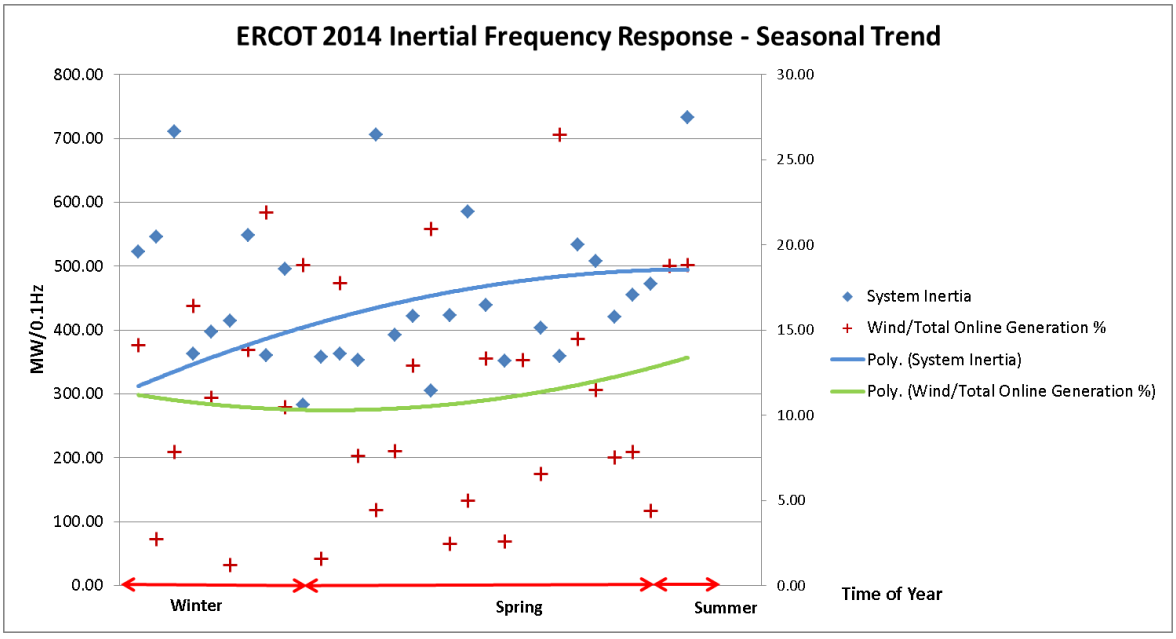


Figure 9. Seasonal Trend of ERCOT Inertial Frequency Response & Percentage of Wind Generation – 2014

2. Inertial Frequency Response vs. Non-Wind Generation Online

The relationship between the calculated inertial frequency response for each event and the non-wind generation was then examined. Figure 10 shows that the relationship between inertial frequency response and non-wind generation online is both linear and positively correlated, suggesting a strong relationship. The non-wind generation online is the sum of total ERCOT generation plus spinning reserves minus wind gseneration. Because the recorded level of spinning reserve was only available for 2014, this analysis could not be completed on 2012 and 2013 data.

The relationship between inertial frequency response and wind generation, as shown in Figure 11, is relatively flat, illustrating no significant contribution from wind generation and no impact with different levels of wind penetration.

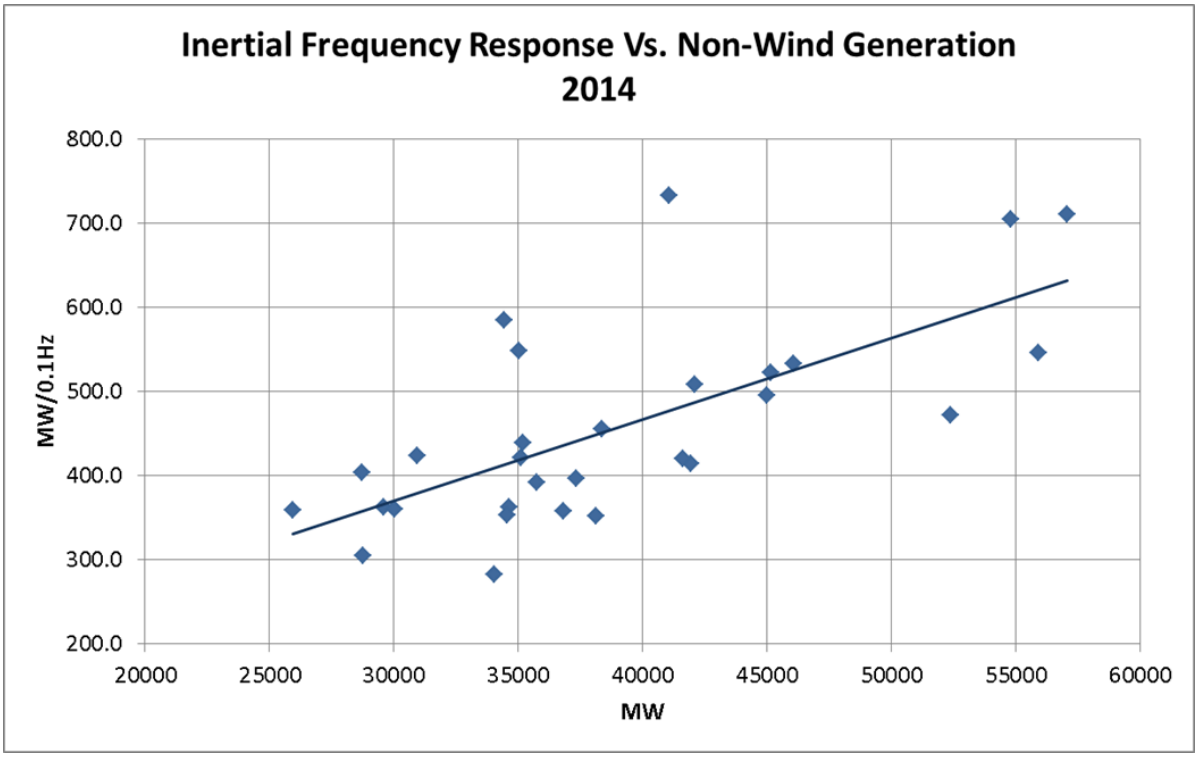


Figure 10. Linear Relationship (Inertia Proportional to Non-Wind Generation) – 2014

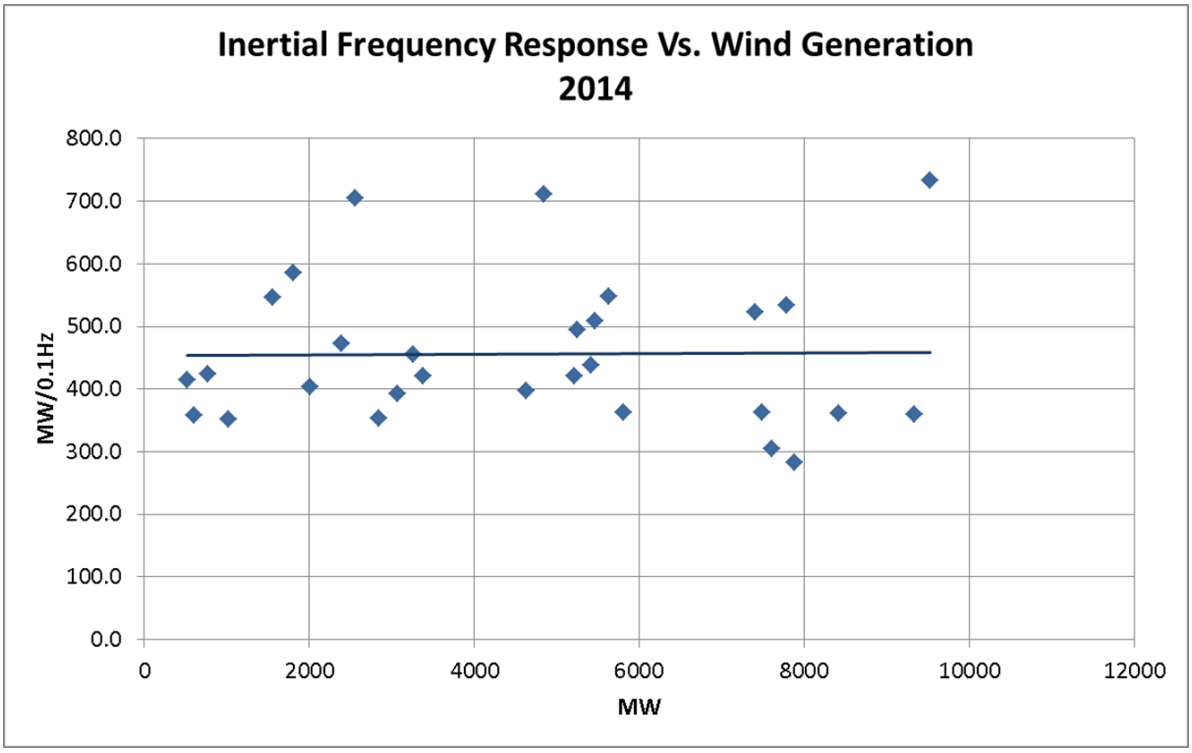


Figure 11. Wind Generation Showing No Contribution to Inertial Frequency Response – 2014

3. Inertial Frequency Response vs. Different Operating Conditions

The inertial frequency response for a group of events was estimated based on a linear regression between the amount of generation loss and the associated frequency drop. The inertial frequency response was estimated for different conditions of ERCOT load and levels of wind generation for 2014, as shown previously in Figure 6. The different levels of wind generation were determined based on the availability and occurrence of actual generator loss events.

There is partially clear evidence of no change in inertial frequency response with increasing levels of wind generation, as explained in the previous section. There is also evidence of a decline in inertia with increasing wind generation, which is likely due to wind generation displacing non-wind generation.

The inertial frequency response declined with increasing levels of wind generation under the following conditions:

1. When load < 30 GW and wind penetration is greater than 15%.
2. When load < 35GW and wind penetration is greater than 15%.
3. When load > 35GW and wind penetration is greater than 10%.

Figure 12 illustrates the first two cases, showing the minimum, maximum and average non-wind generation for different levels of wind generation, for both low and high load conditions. The average non-wind generation is the mean for the grouped events. As there is a decline in inertial frequency response with increasing wind generation, there is also a decline or decrease in average non-wind generation, reducing the rotating mass available to sustain the level of inertial response.

This suggests that, as the penetration (percent of total energy production) of wind generation increases, non-wind generation is displaced off-line, thus reducing the rotating inertia available to support the grid during frequency events (such as loss of a generator). When the non-wind generation is retained online (e.g., as spinning reserve), the inertial frequency response remains higher.

The decline in inertial frequency response may not be exactly proportional to the level of non-wind generation because different types of generation have different levels of inertia contribution. Steam and gas turbines have much higher inertia constants (MW-seconds per MW) than do hydro units. The mix of non-wind generation online during an event will have an impact on the inertial frequency response and affect the linearity of the relationship between the level of non-wind generation and inertial response. Unfortunately, the data needed to estimate the connected inertia was not available to test the linearity of the relationship.

# of Events	MW Loss	Frequency Change	(Wind/Online Gen) %	MW/0.1Hz	Min Non-Wind Gen (MW)	Max Non-Wind Gen (MW)	Average Non-Wind Gen (MW)
8	300	0.075	<= 10%	408.5	28708	38364	34712
	900	0.221875					
3	500	0.115625	11 to 15%	412.9	35062	35173	35116
	700	0.1640625					
3	400	0.1125	16 to 20%	355.5	29585	34648	32752
	800	0.225					
2	400	0.11875	> 20%	355.5	25924	30018	28232
	500	0.146875					

# of Events	MW Loss	Frequency Change	(Wind/Online Gen) %	MW/0.1Hz	Min Non-Wind Gen (MW)	Max Non-Wind Gen (MW)	Average Non-Wind Gen (MW)
2	600	0.14375	<= 10%	417.3	28708	30936	29822
	900	0.215625					
2	568	0.158	> 20 %	371	25924	29585	27754
	824	0.227					

Figure 12. Decline in Inertia at Low Load & High Wind (For the Reason that Non-Wind Generation is Lower) – 2014

4. Wind Output vs. Frequency Change (PMU Data)

The existing PMUs located nearby wind and non-wind generators were used to check if there was any observable inertial contribution during the frequency events. Inertial contribution from generators would be indicated by an increase in power output coincident with the frequency drop caused by a generator trip event. An analysis of the synchrophasor data from selected PMUs was performed to study if there is any **change in power output** from different types of generators **coincidental with drop in frequency** following a generation trip.

The analysis was completed for several events under different scenarios as shown in Figure 13. Twenty-seven (27) events spanning two years (2012-2013) were selected to examine different event scenarios and different system conditions to identify whether wind generation was observed to contribute to inertial frequency response. Events were categorized into four different scenarios:

1. Generation loss of more than 1000 MW.
2. Generation loss when load was low and wind production was high.
3. Generation loss when load was high and wind was high.
4. Generation loss during the months of October-December.

Examining the 27 different events, it was observed that there was **"no significant"** increase in power change coincidental with the frequency drop for each of the events from the **wind plants**, indicating no inertia contribution to the grid. However, an **"increase in power change"** was observed, coincidental during the frequency drop, from **non-wind units,** indicating inertial response from rotating mass. The changing levels of inertial frequency response appear to be driven primarily by the amount of non-wind generation online.

Year	Event Scenarios	Conditions	Count of Events
2012	Generation Loss	> 1000 MW	4
	Low Load & High Wind	<35 GW & > 16%	4
2013	Generation Loss	> 1000 MW	3
	Low Load & High Wind	<35 GW & > 10%	11
	High Load & High Wind	>35 GW & > 16%	2
	October – December	> 35GW & > 6%	3
2	4	5	27

Figure 13. Event Scenarios & Count of Events – Wind Output vs. Frequency Range (PMU data)

Figure 14 shows an example of data from PMUs located close to wind units and non-wind units during a frequency event. Using the PGDA tool, the real power was calculated from voltage and current phasors from each of the selected PMUs, and de-trended by first value to more clearly illustrate the change in power output during the frequency drop. The lower plot illustrates the grid frequency drop following the loss of generation. The upper plot illustrates:

1. A change in power flow (increase) is very clear in non-wind units at **West 11**, **FarWest 7**, and **North 1**.
2. No significant change in power flow in the transmission lines near wind generation at **FarWest 4**, West 10, and West 6.

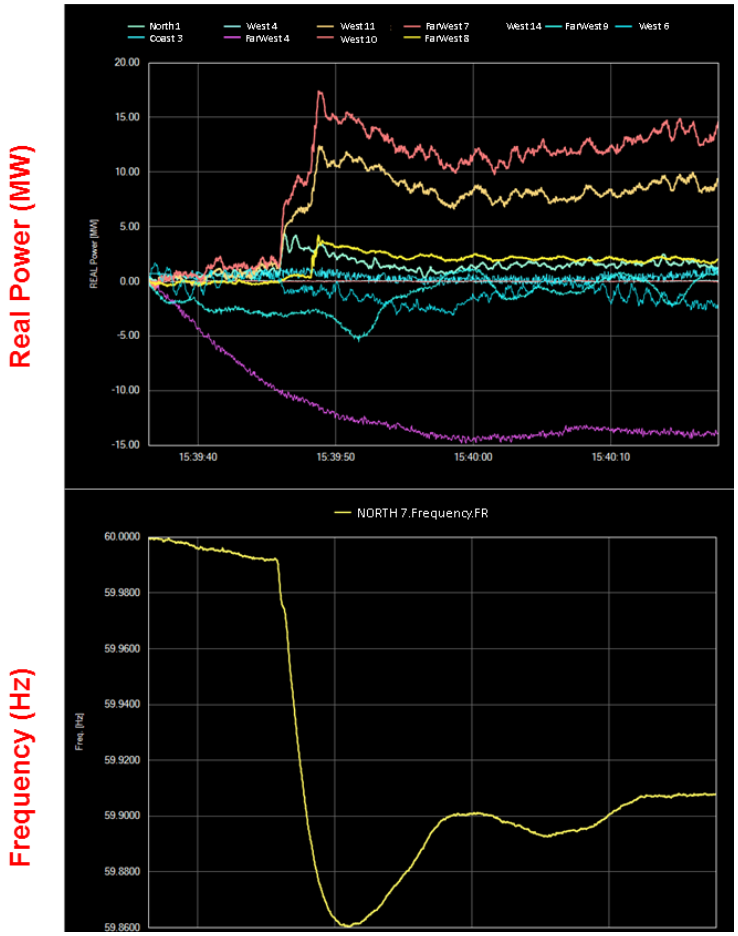


Figure 14. Example of No Inertia from Wind Plants Using PGDA – Wind Output vs. Frequency Range (PMU data)

Taken together, the four different analysis scenarios presented above provide sufficient evidence to conclude that wind generation does not contribute to inertial frequency response.

10. Conclusion

The analysis study used 183 generator trip frequency events, collected from the ERCOT grid over three years (2012-2014), to investigate the impact of wind generation on inertial frequency response. Inertial frequency response was calculated for each individual event using PGDA, and estimated for different operating conditions using a linear relationship between the amount of generation loss and the corresponding first swing frequency drop. For this analysis study, ERCOT load, ERCOT generation, ERCOT wind generation, ERCOT spinning reserves, and data from PMUs located near wind units were collected and analyzed to understand the variation and trends in inertial frequency response. The analysis examined four different illustrative scenarios to evaluate whether wind generation contributes to inertial frequency response.

Some of the key highlights of the findings from the illustrative scenarios that reflect no contribution of wind generation to inertial frequency response are:

1. **Inertial Frequency Response vs. Wind Pattern** - The seasonal trend of inertial frequency response remained the same, even at different levels of wind penetration, indicating no relationship between inertial response and wind penetration.
2. **Inertial Frequency Response vs. Non-Wind Generation** - Inertial frequency response and non-wind generation had a strong positive correlation, suggesting inertia is proportional to non-wind generation.
3. **Inertial Frequency Response vs. Different Operating Conditions** - The instances of decline in inertial frequency response with higher wind generation were found to have lower non-wind generation.
4. **Wind Output vs. Frequency Change (PMU Data)** - There was no significant increase in power output coincidental with frequency drop for each of the frequency events from the wind plants under different conditions, indicating no inertia contribution from the wind plants.

The four different analyses provided evidence that wind generation provides no contribution to inertial frequency response. The inertial frequency response is driven (primarily) by the amount of non-wind generation available online.

To maintain a minimum level of inertial frequency response on the grid, ERCOT operations will need to commit a minimum level of non-wind generation online under all conditions.

Example: Maintaining an adequate level of inertial frequency response (450MW/0.1Hz) for reliable operation of the grid would require ERCOT to commit minimum non-wind generation (35,000 MW) under all conditions (e.g., under frequency load shedding coordination).

11. Appendix

Inertial Frequency Response Estimation – Using Linear Relationship

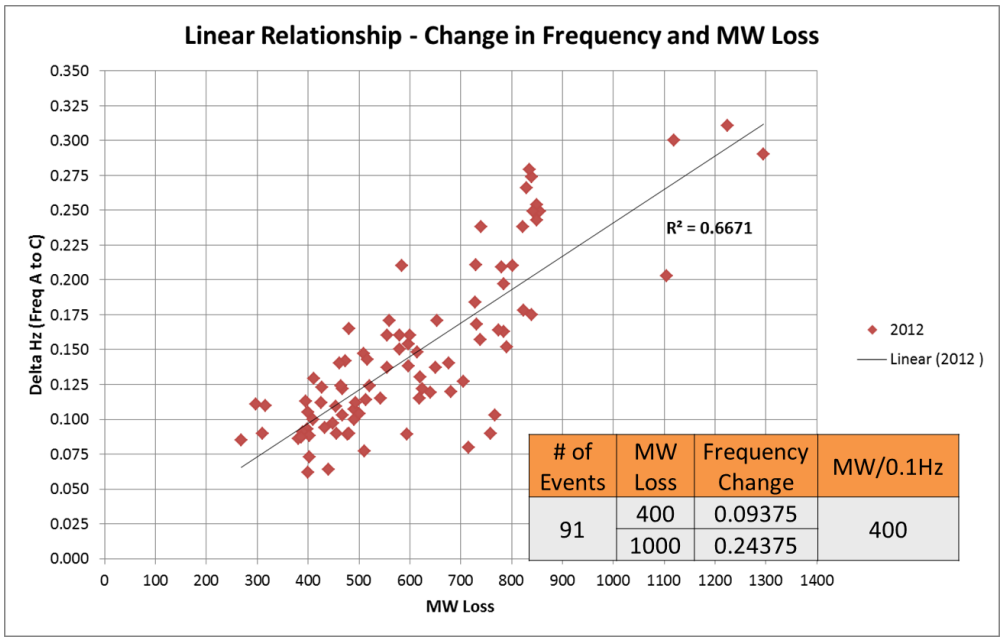


Figure A-1. Estimation of Inertial Frequency Response – 2012

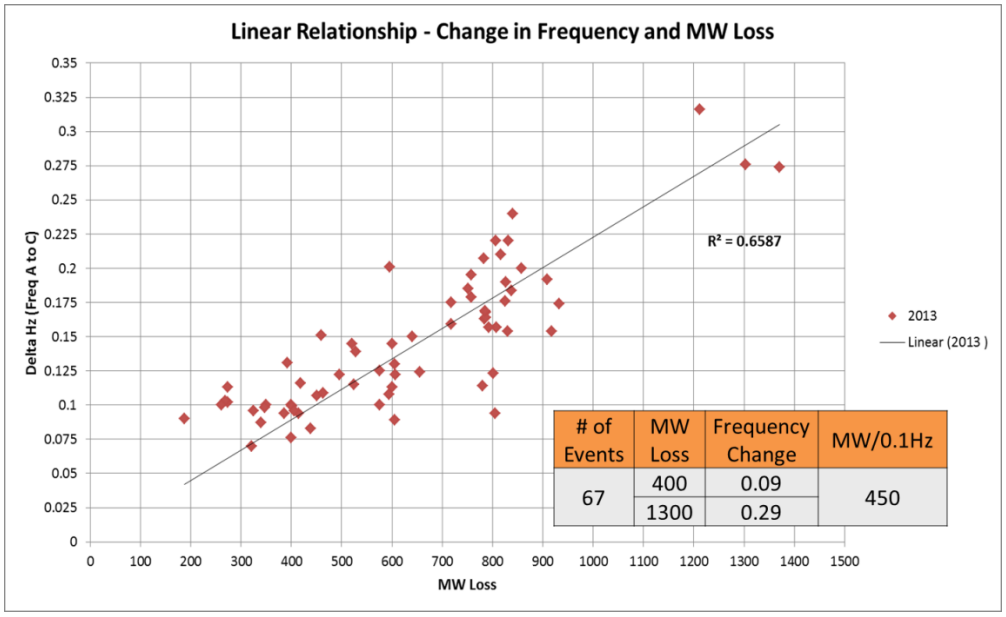


Figure A-2. Estimation of Inertial Frequency Response – 2013

Hypothesis – Decline in Inertial Frequency Response

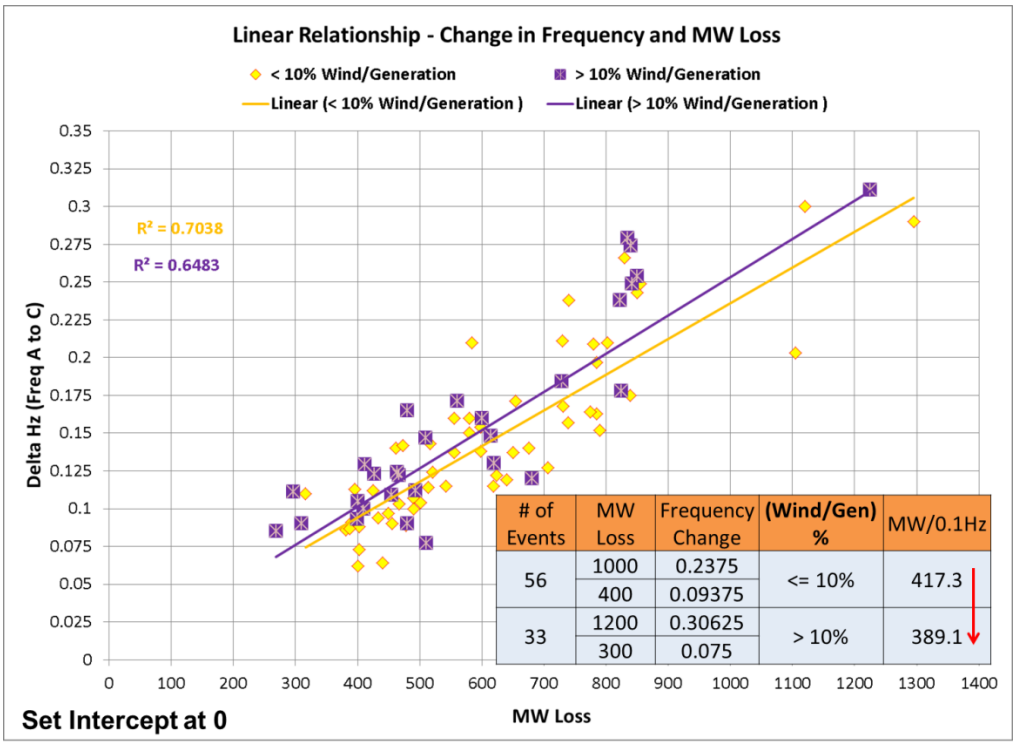


Figure A-3. Estimation of Inertial Frequency Response (Two Wind Levels & No Load Levels) – 2012

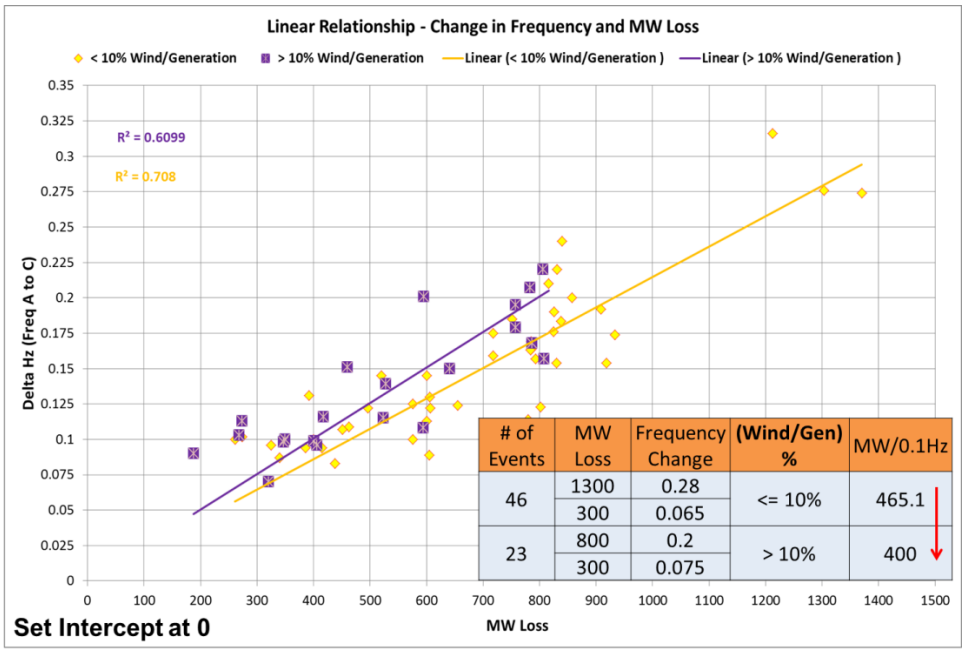
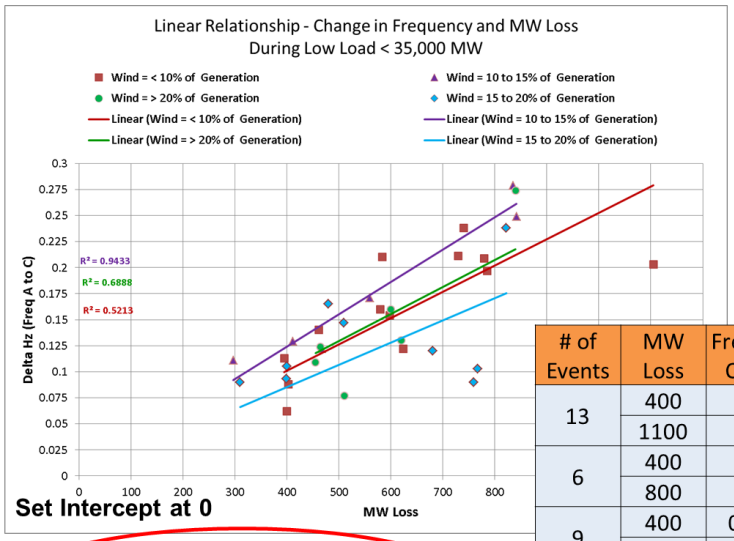


Figure A-4. Estimation of Inertial Frequency Response (Two Wind Levels & No Load Levels) – 2013



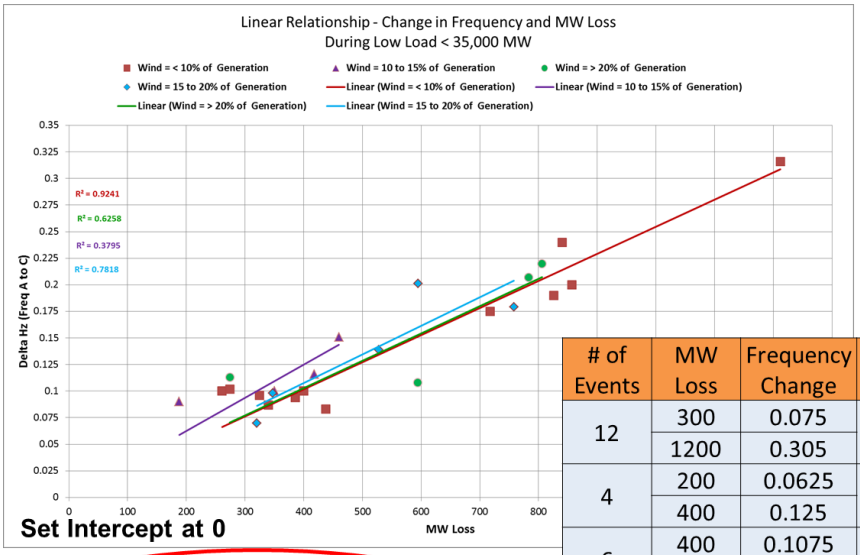
Decline in Inertia with increasing levels of wind resources

Increase in Inertia with increasing levels of wind resources

# of Events	MW Loss	Frequency Change	(Wind/Gen) %	MW/0.1Hz
13	400	0.1	<= 10%	400
	1100	0.275		
6	400	0.125	11 to 15%	320
	800	0.25		
9	400	0.0875	16 to 20%	492.3
	800	0.16875		
6	500	0.13125	> 20%	400
	800	0.20625		

Same Inertia, at Different Levels of Wind Impact

Figure A-5. Estimation of Inertial Frequency Response (Four Wind Levels & Load <35 GW) – 2012



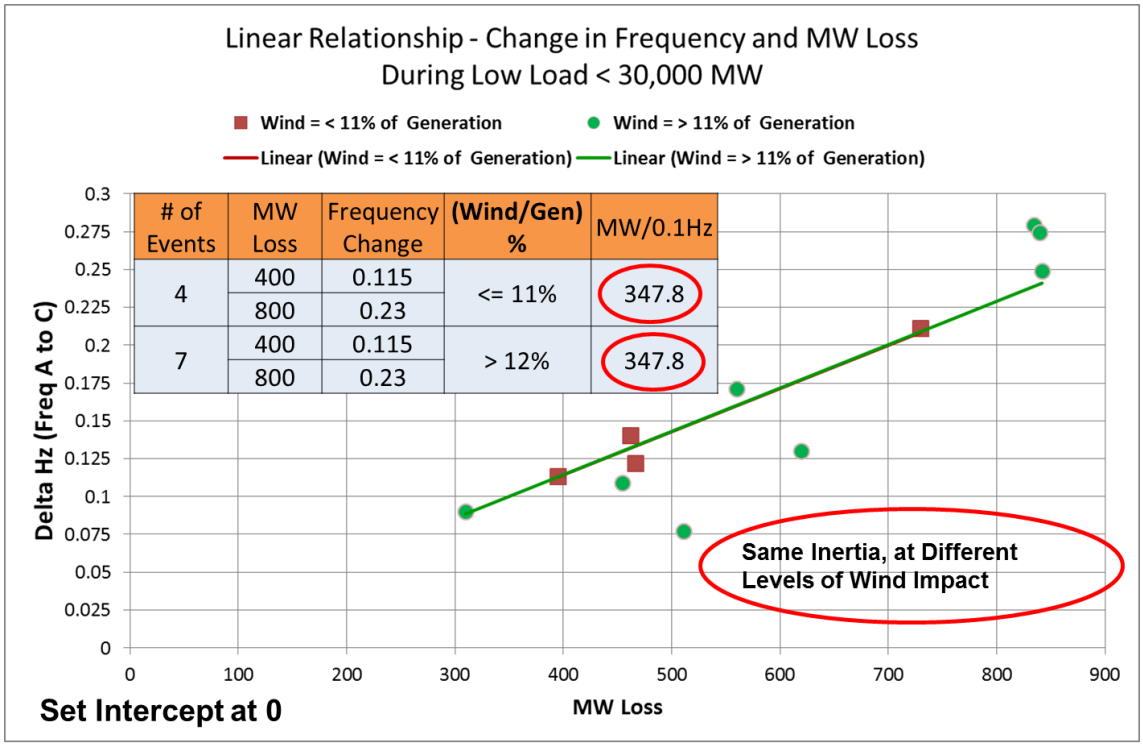
Decline in Inertia with increasing levels of wind resources

Increase in Inertia with increasing levels of wind resources

# of Events	MW Loss	Frequency Change	(Wind/Gen) %	MW/0.1Hz
12	300	0.075	<= 10%	391.3
	1200	0.305		
4	200	0.0625	11 to 15%	320
	400	0.125		
6	400	0.1075	16 to 20%	375
	700	0.1875		
3	300	0.0775	> 20%	392.1
	800	0.205		

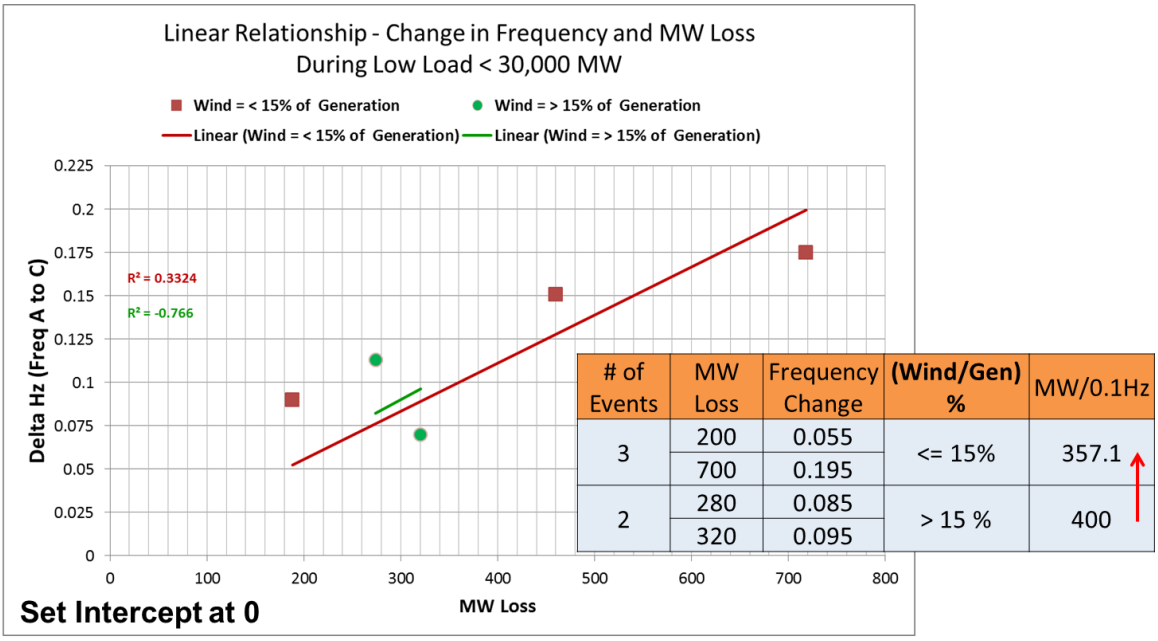
Same Inertia, at Different Levels of Wind Impact

Figure A-6. Estimation of Inertial Frequency Response (Four Wind Levels & Load <35 GW) – 2013



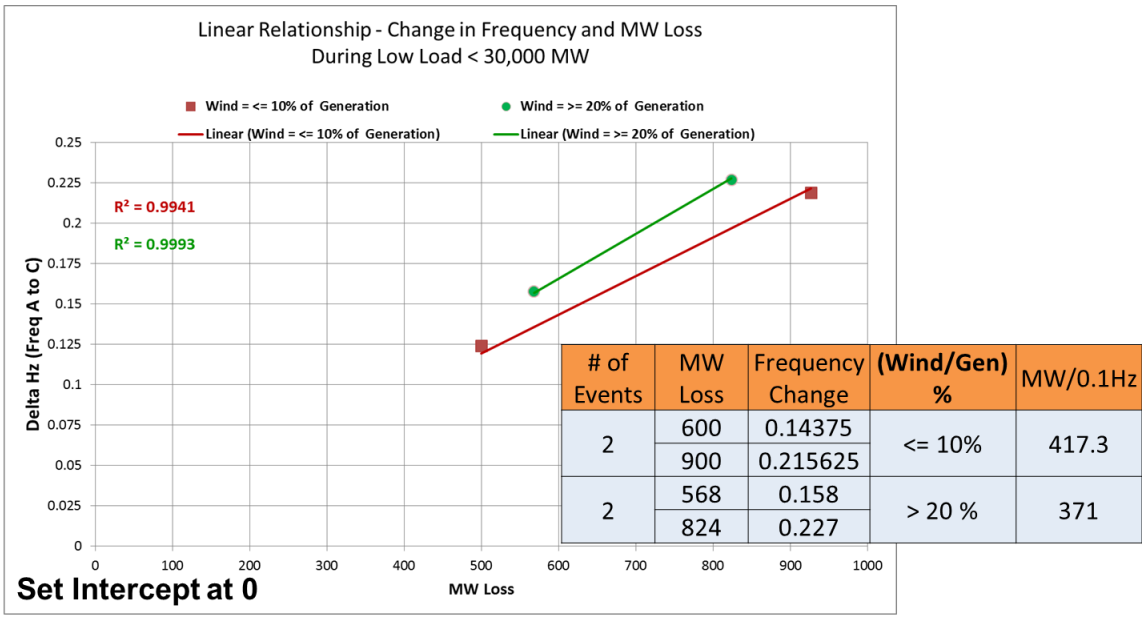
# of Events	MW Loss	Frequency Change	(Wind/Gen) %	MW/0.1Hz
4	400	0.115	<= 11%	347.8
	800	0.23		
7	400	0.115	> 12%	347.8
	800	0.23		

Figure A-7. Estimation of Inertial Frequency Response (Two Wind Levels & Load <30 GW) – 2012



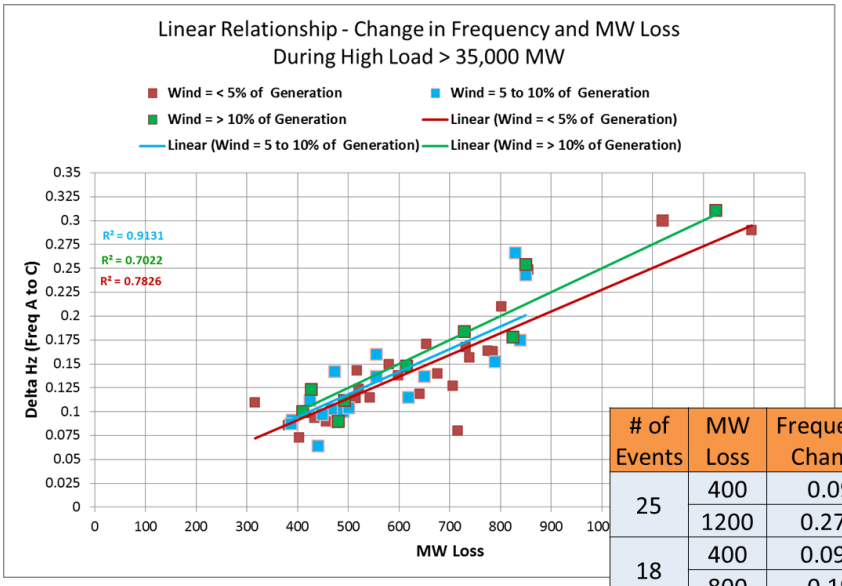
# of Events	MW Loss	Frequency Change	(Wind/Gen) %	MW/0.1Hz
3	200	0.055	<= 15%	357.1
	700	0.195		
2	280	0.085	> 15 %	400
	320	0.095		

Figure A-8. Estimation of Inertial Frequency Response (Two Wind Levels & Load <30 GW) – 2013



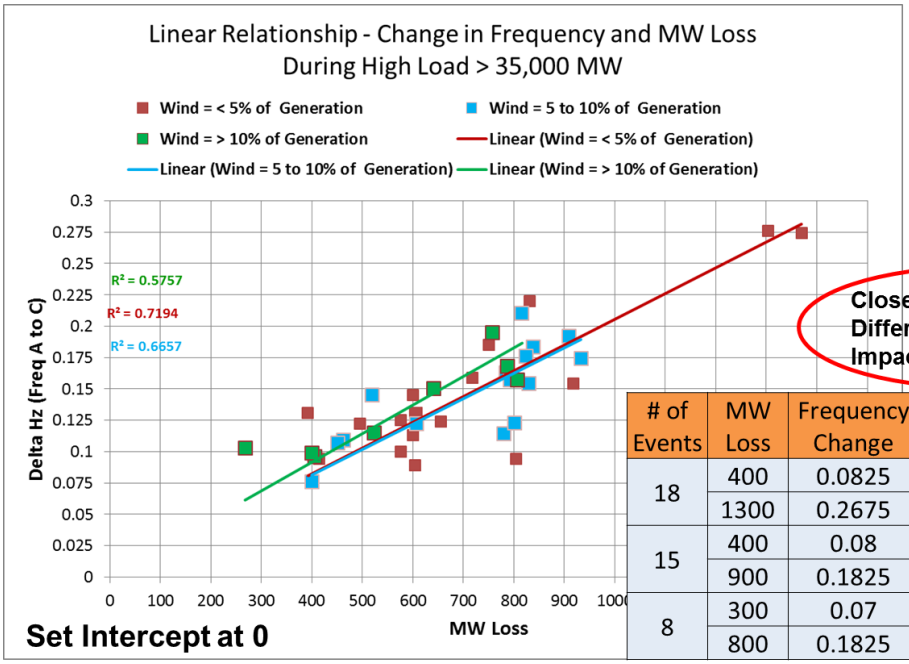
# of Events	MW Loss	Frequency Change	(Wind/Gen) %	MW/0.1Hz
2	600	0.14375	<= 10%	417.3
	900	0.215625		
2	568	0.158	> 20 %	371
	824	0.227		

Figure A-9. Estimation of Inertial Frequency Response (Two Wind Levels & Load <30 GW) – 2014



# of Events	MW Loss	Frequency Change	(Wind/Gen) %	MW/0.1Hz
25	400	0.09	<= 5%	432.4
	1200	0.275		
18	400	0.095	6 to 10%	421
	800	0.19		
9	500	0.125	> 10%	400
	1200	0.3		

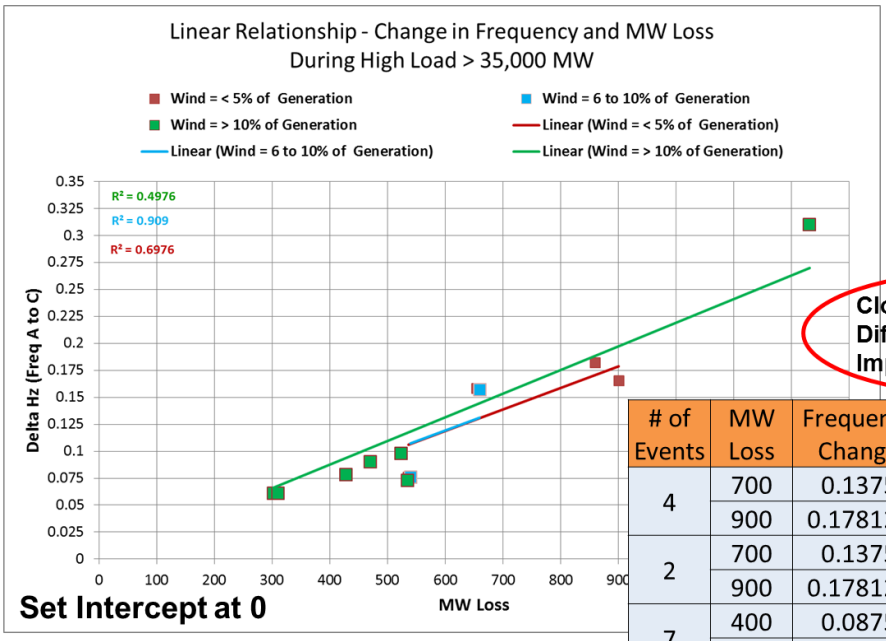
Figure A-10. Estimation of Inertial Frequency Response (Three Wind Levels & Load >35 GW) – 2012



Close to same Inertia, at Different Levels of Wind Impact

# of Events	MW Loss	Frequency Change	(Wind/Gen) %	MW/0.1Hz
18	400	0.0825	<= 5%	486.4
	1300	0.2675		
15	400	0.08	6 to 10%	487.8
	900	0.1825		
8	300	0.07	> 10%	444.4
	800	0.1825		

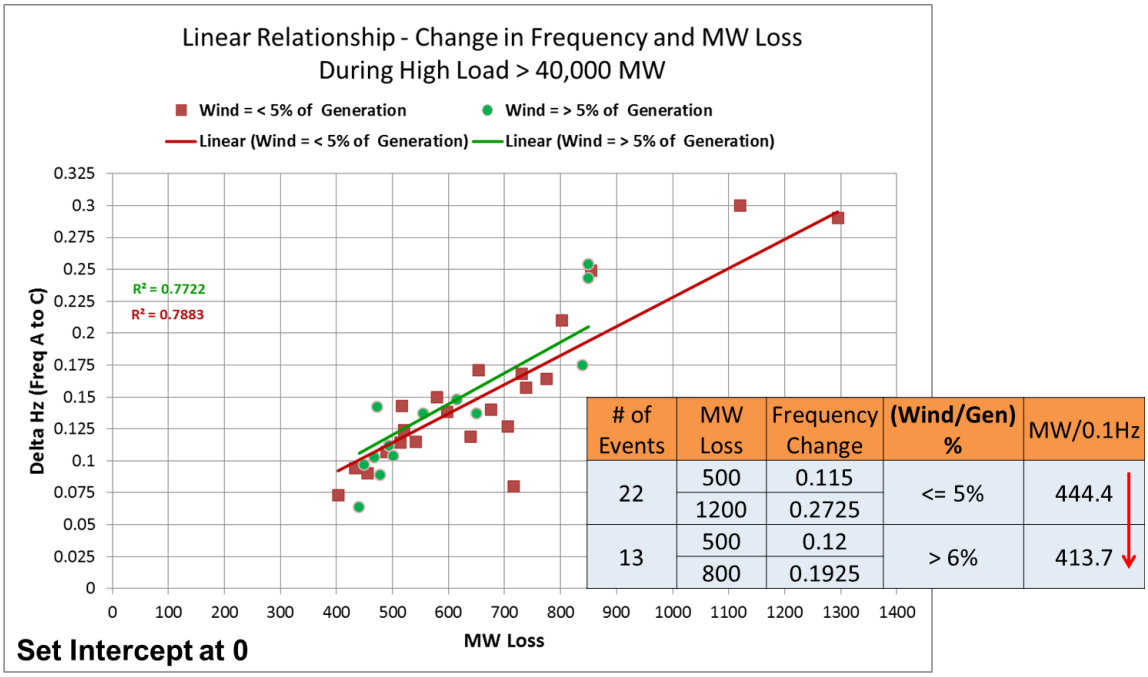
Figure A-11. Estimation of Inertial Frequency Response (Three Wind Levels & Load >35 GW) – 2013



Close to same Inertia, at Different Levels of Wind Impact

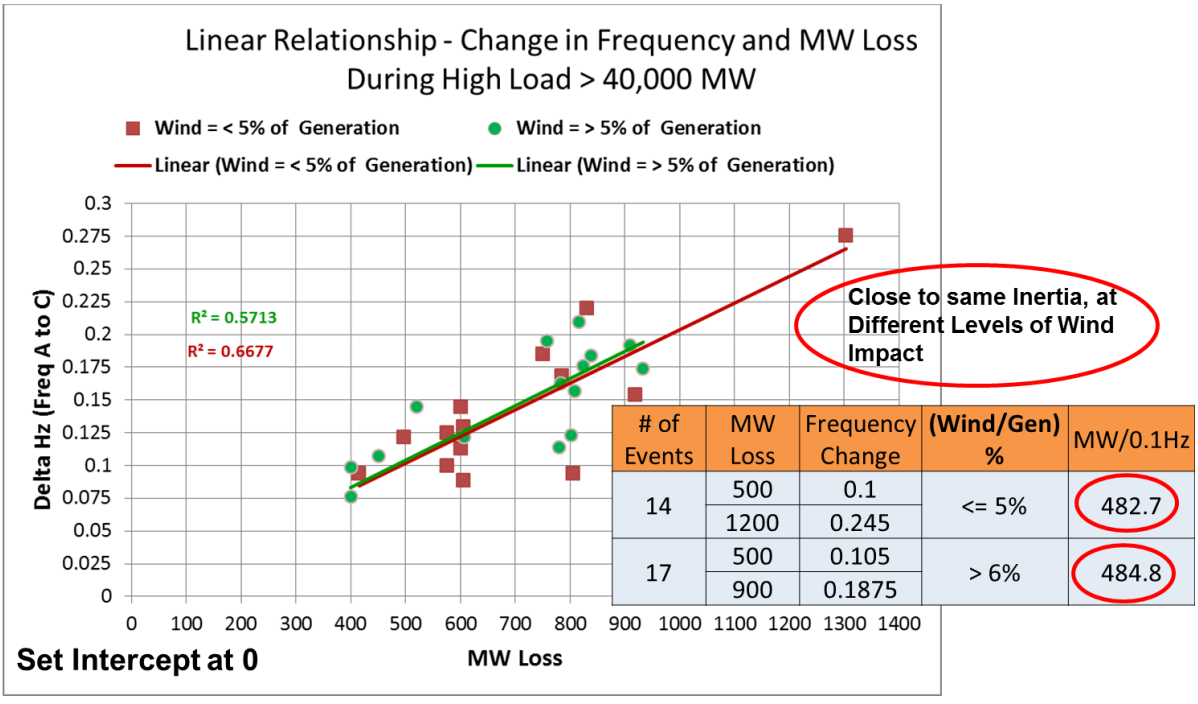
# of Events	MW Loss	Frequency Change	(Wind/Gen) %	MW/0.1Hz
4	700	0.1375	<= 5%	492.3
	900	0.178125		
2	700	0.1375	6 to 10%	492.3
	900	0.178125		
7	400	0.0875	> 10%	457.1
	1200	0.2625		

Figure A-12. Estimation of Inertial Frequency Response (Three Wind Levels & Load >35 GW) – 2014



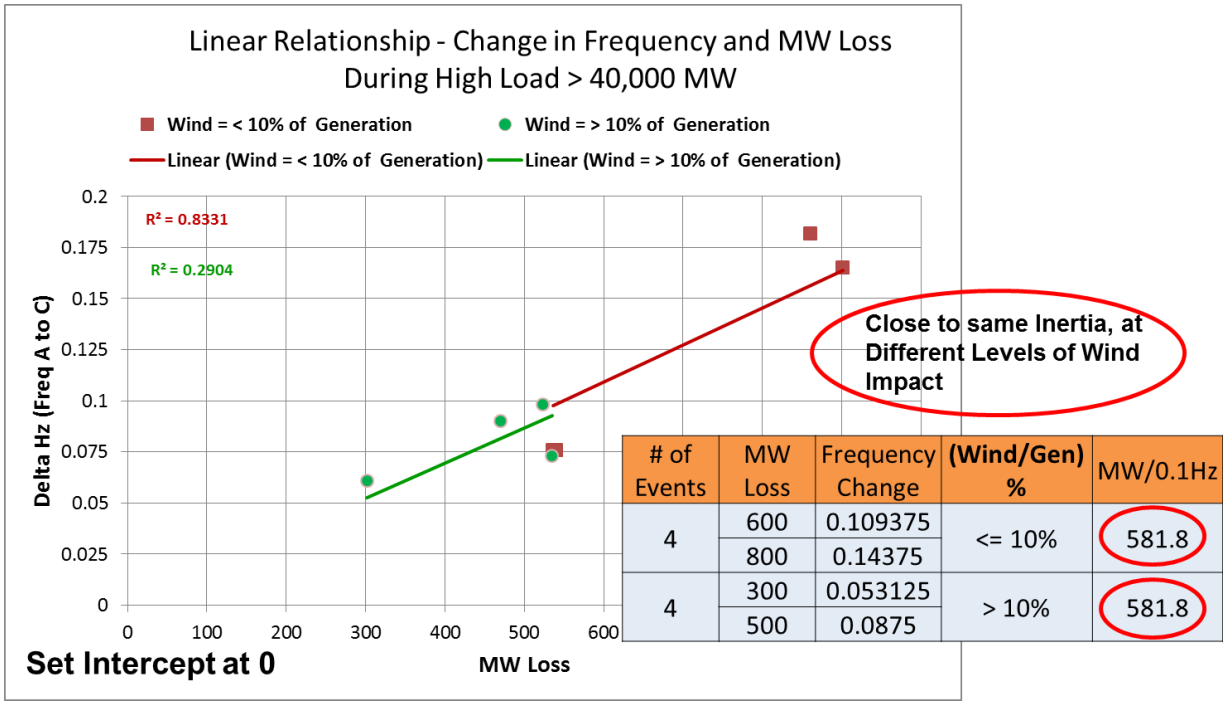
# of Events	MW Loss	Frequency Change	(Wind/Gen) %	MW/0.1Hz
22	500	0.115	<= 5%	444.4
	1200	0.2725		
13	500	0.12	> 6%	413.7
	800	0.1925		

Figure A-13. Estimation of Inertial Frequency Response (Two Wind Levels & Load >40 GW) – 2012



# of Events	MW Loss	Frequency Change	(Wind/Gen) %	MW/0.1Hz
14	500	0.1	<= 5%	482.7
	1200	0.245		
17	500	0.105	> 6%	484.8
	900	0.1875		

Figure A-14. Estimation of Inertial Frequency Response (Two Wind Levels & Load >40 GW) – 2013



# of Events	MW Loss	Frequency Change	(Wind/Gen) %	MW/0.1Hz
4	600	0.109375	<= 10%	581.8
	800	0.14375		
4	300	0.053125	> 10%	581.8
	500	0.0875		

Figure A-15. Estimation of Inertial Frequency Response (Two Wind Levels & Load >40 GW) – 2014

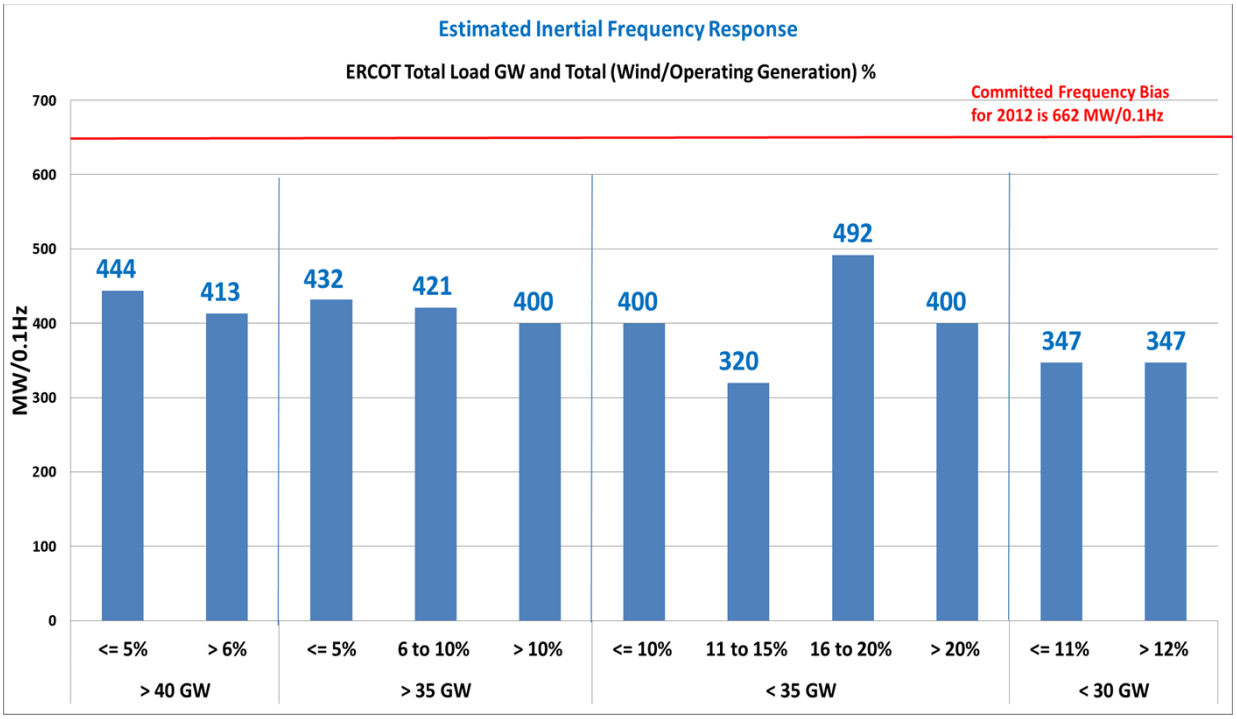


Figure A-16. Estimation of Inertial Frequency Response (Different Wind Levels & Load Levels) – 2012

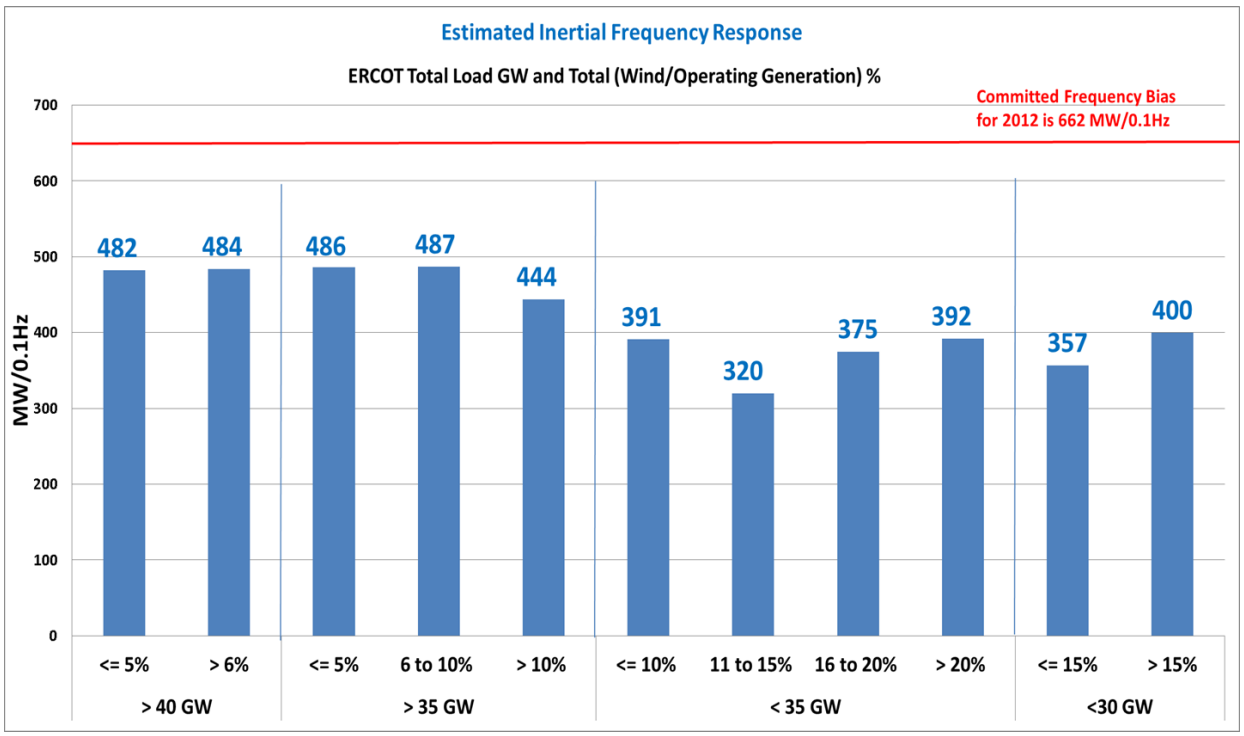


Figure A-17. Estimation of Inertial Frequency Response (Different Wind Levels & Load Levels) – 2013

12. References

1. Sandip Sharma, Shun-Hsien Huang and NDR Sarma, "System Inertial Frequency Response Estimation and Impact of Renewable Resources in ERCOT Interconnection".

Attachment 11. Oscillation Data Mining Study

Center for Commercialization of Electric Technologies (CCET)

Discovery Across Texas Project

Final Report on

Wind Characteristics

Oscillation Data Mining Study

Submitted to:
Milton Holloway, Ph.D.
mholloway@electrictechnologycenter.com

Prepared by:

Electric Power Group

John W. Ballance
Prashant C. Palayam

November 17, 2014

Table of Contents

List of Figures

CCET Discovery Across Texas

Wind Characteristics – Oscillation Data Mining Study

CCET 3.1.3, Task C

1. Introduction

The Center for Commercialization of Electric Technologies (CCET) was awarded contract DE-OE0000194 by the Department of Energy to perform the Discovery Across Texas demonstration project. Electric Power Group, LLC (EPG) received a sub-award from CCET to provide professional services to perform, among other things, an analysis to identify unknown oscillations from existing connected wind generators in the Electric Reliability Council of Texas (ERCOT) grid to prevent system vulnerability and customer complaints. Texas has the greatest amount of wind generation online in the nation, and attains a new wind production record every year. Increasing wind production with installation of wind controllers poses operating challenges for ERCOT. One of the challenges faced by ERCOT is presence of high/low frequency oscillations from wind generators driven by control systems with a bad setting. The wind farms are embedded with electronic controllers to monitor wind output and manage voltage. These fast responding wind controllers with a bad setting or bad design introduce high/low frequency control system oscillations, either intermittently with high energy or consistently with low energy, which can plausibly cause the following:

1. Voltage fluctuations at the distribution level power systems.
2. Damage to motor and pumps at homes and residential circuits.
3. Drive nearby wind farms to oscillate at the same frequency, and damage nearby wind farm turbine blades and shafts.
4. Interact with other conventional generation units, such as coal, natural gas, etc., in the grid to oscillate at the same frequency and cause significant forced damage to mechanical parts, such as generator shafts.

This analysis summarizes the investigation on examining the phasor data from nearby wind generators for three years, and identification of unknown oscillations. The nearby location with the highest occurrence of those oscillations are identified and labeled as critical locations to monitor in real-time for early detection and mitigation. Based on the occurrence of each mode pattern, and its associated energy level spanning over three years, the report groups the

oscillations and provides guidelines for ERCOT to help prevent grid vulnerability and customer complaints.

2. Executive Summary

Texas has the greatest amount of wind generation online in the nation and attains a new wind production record every year. Increasing wind production with installation of wind controllers poses operating challenges for ERCOT. One of the challenges faced by ERCOT is presence of high/low frequency oscillations from wind generators driven by control systems with a bad setting. The wind farms are embedded with electronic controllers to monitor wind output and manage voltage. These fast responding wind controllers with a bad setting or bad design introduce high/low frequency control system oscillations, either intermittently with high energy or consistently with low energy. The early detection and mitigation of emerging oscillations in real-time is crucial to ensuring reliable operation of grid. This sets the stage for baselining the oscillations from nearby wind generators, leveraging the existing and installed PMU locations measuring grid metric samples at 30 frames per second.

Hence, this study was proposed to investigate:

1. Other unknown oscillations from wind generators.
2. The locations with highest occurrence of those oscillatory modes.
3. Precursors (if any) for such occurrences and the associated energy output.
4. Frequency band and minimum energy for additional monitoring.

The detection of unknown oscillations from phasor data, spanning three years, was done using EPG's Phasor Data Mining Tool. The tool enabled automatic scanning of the data in periodic intervals, and it records the incidents of detected oscillations with damping and energy levels time-stamped for each PMU location.

This analysis was based on six PMUs located near wind farms in the ERCOT Interconnection. The Phasor Data Mining Tool was configured with needed algorithm settings to scan through six PMU locations for different frequency bands, ranging from 0.1 Hz to 15 Hz. The measurements, including frequency, voltage phasor and current magnitude, under each PMU were examined to record detected modes every minute, and calculated damping and energy associated with each mode. The results were time-stamped and tagged to the PMU locations to identify the source of the oscillations. The tool was set to discard modes with damping greater than 8%, regardless of the detected energy level. The tool leveraged the PMU status information to clean bad data and avoid false detections. The detection results from the tool were parsed and post-processed through MATLAB scripts to rank the oscillatory modes with the highest occurrence and highest energy. These results were then examined to identify any relationship between each mode occurrence and the corresponding regional wind data. The highest energy of a mode was extracted and compared with the mode occurrence to baseline the minimum energy required to monitor in real-time, and also to differentiate modes related to wind production versus modes driven by control systems, or setting changes in control systems.

Some of the key findings are as follows:

1. The study identified 10 different ERCOT oscillatory modes.
2. The occurrence of 2 modes appears to be related to wind production – 0.9 Hz (West 6) & 2.7 Hz (FarWest 4).
3. The occurrence of 4 modes appear to be related to control system settings changes – 1.5 Hz (Coast 3), 1.7 Hz (FarWest 7), 2 Hz (Coast 3), and 3.2 Hz (West 10).
4. The occurrence of 3 modes appear to be related to the presence of wind generation and control systems - 5.0 Hz (Coast 3),5.4 Hz (West 10 & FarWest 4), and 6.0 Hz (West 10).
5. The occurrence of 1 mode appears to be a local oscillation caused by topology change or mis-tuning of the wind generator control system – 0.6 Hz (West 10).

This study concludes that four modes appeared consistently for three years, and are still present. There are four other modes that appeared intermittently with high energy. There are another two modes that appeared consistently for the first two years, but were not detected in 2014. The report provides insights on the Real Time Dynamics Monitoring System[1] (RTDMS®) configuration for monitoring certain modes in real time to detect and mitigate the oscillations. The modes which appear only sporadically may need additional review by ERCOT with the plant owners to determine the root cause and evaluate the need for additional monitoring.

3. Goals & Methodology

The objective of this analysis was to identify unknown oscillations from existing connected wind generators in the Electric Reliability Council of Texas (ERCOT) grid to prevent system vulnerability and customer complaints. Utilizing six different PMUs, located near wind generators during the period of 2012-2014, the study set five goals:

1. Build a Phasor Data Mining Tool that can scan through the phasor data, detect low damped oscillatory modes, and record the associated damping and energy values.
2. Using the results from the mining tool, calculate following monthly statistics for each mode
    a. Mode occurrence (in percent of time)
    b. Highest energy value
    c. Timestamp and PMU measurement with the highest energy value
3. Identify the nearby PMU location that had the highest mode occurrence.
4. Correlate mode occurrences with regional wind data to determine the type of oscillation – related to wind production, or driven by control Systems.

[1] Built upon GRID-3P® platform. US Patent 7,233,843, US Patent 8,060,259, and US Patent 8,401,710.

5. Baseline oscillation characteristics – minimum energy level and frequency band for additional monitoring in real time.

Figure 1 shows the flowchart that describes the workflow of the analysis study. The different steps in the analysis study were:

Step 1 Gather phasor data from six different PMU locations for three years in a database.
Step 2 Set up jobs in the Phasor Data Mining Tool to connect to the database and scan through the data with user-defined configuration.
Step 3 Export the mining tool results from the results database into a CSV file.
Step 4 Parse the CSV file containing results for all PMU measurements for post processing in MATLAB.
Step 5 Write MATLAB script to calculate monthly statistics on mode occurrence and filter oscillatory modes with low occurrence and low energy.
Step 6 Export post-processed results for each PMU measurement.
1. Mode occurrence of each mode
2. Highest energy for each mode
3. Timestamp of the mode with highest energy

Step 7 Conduct analysis to achieve the goals for this study.

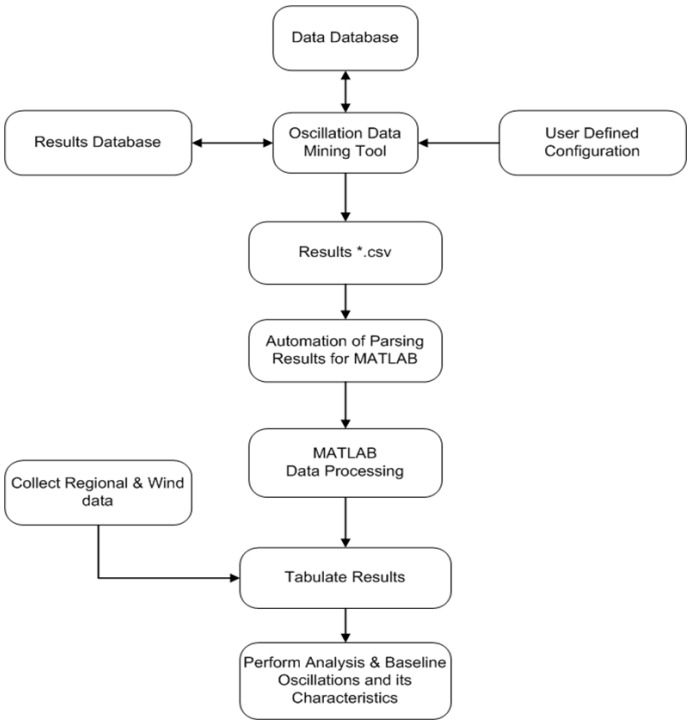


Figure 1. Analysis Workflow

4. Derived Metrics & Calculated Variables

The following results associated with oscillations were collected from the Phasor Data Mining Tool after scanning through the phasor data:

1. Oscillatory mode (frequency value in Hz).
2. Damping associated with oscillatory mode (percentage).
3. Energy level associated with oscillatory mode (no unit, magnitude).

The above sets of results were time-stamped and tagged with the associated PMU measurement. The tool was configured to output results every minute (sampling of successive 60-second intervals of phasor data).

The variables calculated for this study were:

1. Monthly average regional wind generation (3 regions)
    a. Wind North = aggregation (north)
    b. Wind West = aggregation (far west, west)
    c. Wind South = aggregation (south, coastal wind)

The metrics derived for this study were:

1. Monthly mode occurrence (%) = (count of minutes having mode/total number of reported minutes) * 100 (e.g. 0.9 Hz appeared 42% of the time in April 2012)
2. Monthly highest energy = maximum energy of an oscillatory mode each month

Other information extracted along with monthly statistics was:

1. Timestamp associated with the highest energy
2. PMU measurement associated with mode

5. Phasor Data Mining Tool – Oscillation Candidates

The six different PMU locations that were used in the study were located near wind generators, but do not directly monitor the output of individual wind farms. They include the following:

1. FarWest 7
2. West 10
3. FarWest 4
4. West 6
5. Coast 4
6. Coast 3

The PMU at substation North 7 was used in the study as a reference for PMU voltage angle measurements. The signal types from PMU measurements used in the study were as follows:

1. Frequency.
2. Voltage phasor (voltage magnitude and voltage angle).
3. Current magnitude.

The mining tool was configured to look for oscillatory modes within one frequency band, from 0.1 Hz to 15 Hz. Bad data in the phasor measurements were removed before scanning for oscillations using the flags set in the status signal embedded with PMU measurements in C37.118 format. The algorithm settings to scan for oscillations were set in such a way that the output results were reported:

1. Every minute – The output result for each (study) minute is the algorithm output for the phasor data available in that minute.
2. Modes are discarded with damping greater than 8%.
3. Energy for each mode is computed.
4. Minimum frequency – 0.1 Hz.
5. Maximum frequency – 15 Hz.

6. Oscillation Data Mining Tool Performance & Processing

The Phasor Data Mining Tool performs several functions, such as data extraction, data cleaning, data calculation, and data storage into the results database. The approximate time taken to completely process one minute of phasor data (for multiple PMUs) is approximately 4 seconds. Using this average processing timing, the processing of a full month of phasor data would take approximately 2 days. Figure 2 shows the tool performance for an processing 1 hour, 1 day, and 1 month.

Task	Time
Data Loading (1 minute of data, All PMU signals)	3 sec
Data Filtering Mode Solving Result Exporting	1 sec
Total **(All Frequency Bands)**	**4 sec**
Ideal Example	
1 Hour	4 Min
1 Day	1.6 Hours
1 Week	11.2 Hours
1 Month (31 days)	**2.06 Days**

Figure 2. Phasor Data Mining Tool Performance

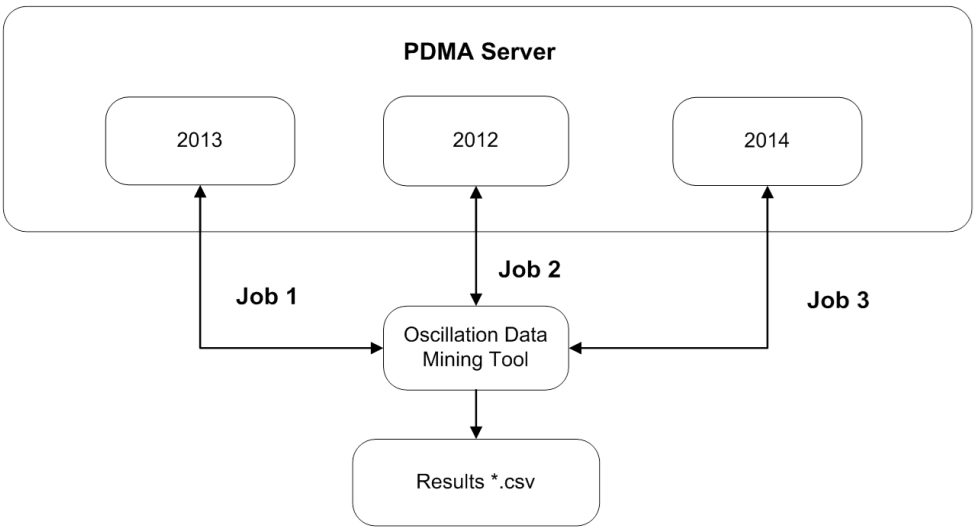


Figure 3. Analysis Work flow

In order to expedite the scanning process to successfully scan a full 3-years worth of data, three simultaneous processing jobs were established to scan each of the three different years in parallel. This reduced the overall processing time to that of one year instead of three years. This parallel processing helped expedite the completion of oscillation scanning process in a more effective way instead of scanning one year after another.

7. Oscillation Data Mining Results – Post Processing

The Phasor Data Mining Tool reports results for each study minute which has a detectable oscillatory mode, including its associated damping and energy value, time-stamped with PMU measurements. The MATLAB script was written to read the output results of the Phasor Data Mining Tool and scan through to populate monthly statistics for each detected mode in each of the PMU measurements. The statistics and metrics are explained briefly in Section 4. It is important for planners and operators to focus on those oscillatory modes that occur most of the time, and those modes that occur with high energy. Hence, those oscillatory modes with a monthly occurrence which was less than 20% of the highest occurrence among all the modes observed in all PMU measurements were discarded. Similarly, oscillatory modes were discarded where the highest mode energy was less than 20% of the highest energy among all the modes observed in all PMU measurements. The output results from MATLAB post processing include PMU metric identification (name and signal type), oscillatory modes detected, mode occurrence, and highest energy and associated timestamps for further analysis studies in order to accomplish the goals of the project.

The output results for three years from MATLAB post processing are attached to this report as an Excel workbook, “Wind Oscillation Study – Monthly Statistics.” The Excel workbook

consists of two sheets. The first sheet, "Modes_Aval", contains the modes filtered by highest occurrence, and the second sheet, "Modes_Ene", contains the modes filtered by highest energy. Both sheets include the following information in the following order: year-month, PMU name, signal name, signal type, frequency range, monthly occurrence, highest energy, mode (associated oscillatory frequency value in Hz), and timestamp (associated time in UTC). The highest energy, mode and timestamp fields are associated with each other.

8. Summary of Identified ERCOT Oscillatory Modes

Figure 4 shows a quick summary of the 10 identified oscillatory modes in the ERCOT Interconnection, as measured by PMUs located at nearby wind generators. All the modes appeared due to the presence of wind generators, but differed in terms of energy levels and mode occurrence. The mode occurrence and energy levels provided clues to differentiate between those modes related to wind production and those which appear to be driven by control systems. There appear to be four modes (0.9 Hz, 5.0 Hz, 5.4 Hz, and 6.0 Hz) that are consistent in occurrence during the three years, and continue to be present. The rest of the modes appear to fall into two categories of intermittency. The 0.6 Hz and 2.7 Hz modes appeared constantly for a period of time (four months and twenty-four months, respectively), but then they disappeared, and have not reoccurred. Their disappearance may indicate a relationship between the oscillation and a topology change, or a change in the tuning of the generator controls. These modes need further investigation to review their disappearance for additional monitoring. The second category of intermittent oscillations showed high energy when they occurred. These modes need additional monitoring to identify their nature and initiating factors. The 1.7 Hz, 1.5 Hz, 3.2 Hz, and 2Hz belong to this second category, and appear to be driven by temporary changes in the control systems settings of the nearby generators.

Figure 5 shows the list of 10 oscillatory modes with the nearby location of wind generators that saw the highest occurrence of each mode. The 0.9 Hz and 2.7 Hz mode occurrences followed the regional wind pattern and appeared to be related to wind production. The monthly highest energy levels, gathered across three years, tracked the level of occurrence, providing further indication that the respective modes were related to wind production. The monthly highest energy levels of the 5.0 Hz, 5.4 Hz and 6.0 Hz modes remained flat, and didn't appear to vary in relationship with changing levels of regional wind production, except for the 6.0 Hz mode, which had relatively high energy during certain periods of time. This mode deserves additional monitoring. The highest energy levels of these modes appear to be driven by settings changes in control systems, and the baseline energy levels can be used as a reference for the minimum energy to set for additional monitoring (alarming) in real time. It is also evident that there are several modes observed from another PMU location nearby to wind generators.

#	Mode (Hz)	2012	2013	2014	Oscillation Type
1	**0.6**	Till March	Absent	Absent	Local
2	**0.9**	Present	Present	Present	Wind Production Related
3	**1.5**	Only in April	Absent	Absent	Control Systems
4	**1.7**	4 Months	Absent	Absent	Control Systems
5	**2.0**	Absent	April	Absent	Control Systems
6	**2.7**	Present	Present	Absent	Wind Production Related
7	**3.2**	4 Months	Absent	Only in Jan	Control Systems
8	**5.0**	Present	Present	Present	Control Systems
9	**5.4**	Present	Present	Present	Control Systems
10	**6.0**	Present	Present	Present	Control Systems

Figure 4. Presence/Absence of 10 Oscillatory Modes over 3 Years

#	Mode (Hz)	Nearest PMU	Related to Wind Production	Highest Energy Level
1	**0.6**	West 10	No	Low Energy & Flat
2	**0.9**	West 6	Yes	High Energy & Tracking Occurrence
3	**1.5**	Coast 3	No	Low Energy
4	**1.7**	FarWest 7	No	High Energy
5	**2.0**	Coast 3	No	Low Energy
6	**2.7**	FarWest 4	Yes	High Energy & Tracking Occurrence
7	**3.2**	West 10	No	High Energy
8	**5.0**	Coast 3	No	Low Energy & Remained Flat
9	**5.4**	West 10, FarWest 4	No	Low Energy & Remained Flat
10	**6.0**	West 10	No	Intermittent High Energy

Figure 5. Ten Oscillatory Modes – Location, Type, and Energy Level Pattern

9. Detailed Description of 10 Identified Modes

This section of the report describes the four types of oscillatory modes identified in the ERCOT Interconnection associated with nearby wind generators. The four types of oscillatory modes are:

1. The occurrence of 2 modes appears to be related to wind production – 0.9 Hz (West 6) and 2.7 Hz (FarWest 4).
2. The occurrence of 4 modes appears to be related to control system settings changes – 1.5 Hz (Coast 3), 1.7 Hz (FarWest 7), 2 Hz (Coast 3), and 3.2 Hz (West 10).
3. The occurrence of 3 modes appears to be related to the presence of wind generation and related to wind generation control systems - 5.0 Hz (Coast 3), 5.4 Hz (West 10 & FarWest 4), and 6.0 Hz (West 10).
4. The occurrence of 1 mode appears to be a local oscillation due to a topology change or tuning of wind generators – 0.6 Hz (West 10).

Mode 2: 0.9 Hz

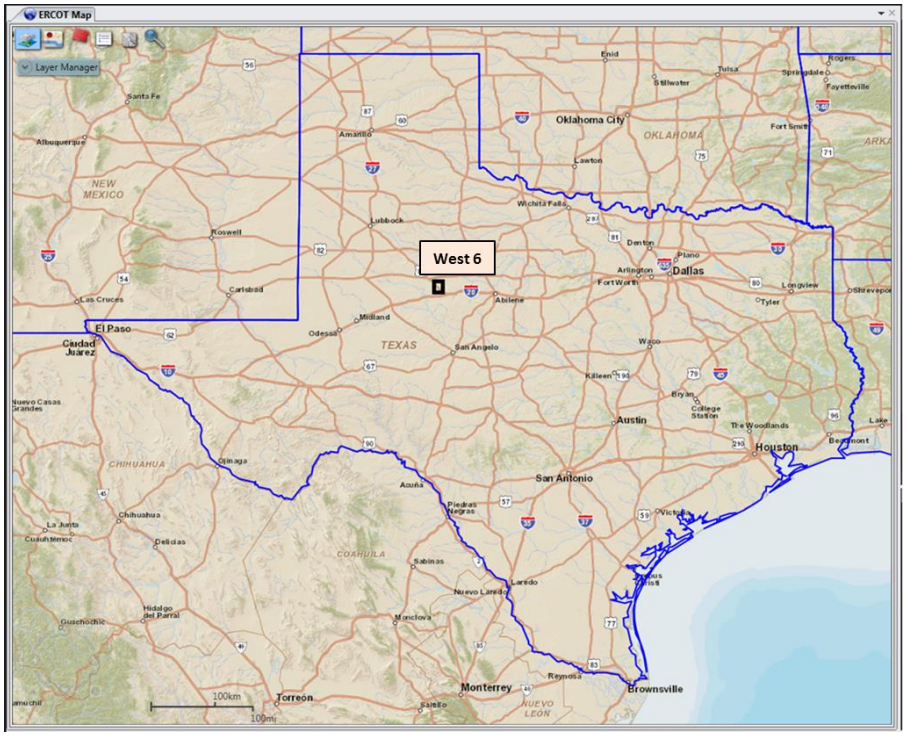


Figure 6. Mode 2 – PMU Location

Figure 6 shows the PMU location in ERCOT that had consistent occurrence of the 0.9 Hz mode spanning 3-years, and which continues to be present. The mode showed up in the current magnitude signal measurement for the West 6 substation which is located near wind generators

including WestGen1, WestGen2, WestGen3, and WestGen4. Figure 8 shows the trend of the 0.9 Hz mode occurrence in the West 6 current magnitude signal over the 3 years. The maximum occurrence of the 0.9 Hz mode appeared 53% of the time in June 2014, and the minimum occurrence of the same mode appeared 22% of the time in December 2013. The average occurrence over all 3 years is about 42% of the time each month. Figure 7 shows the comparison between the mode occurrence of 0.9 Hz and the monthly average west wind production in MW from January 2012 to April 2013. The trend of mode occurrence and average west wind has similar patterns and provides a first indication that 0.9 Hz is likely related to wind production. The mode occurrence reduced from 40% to 30% when the average wind production showed reduction from 3,000 MW to 1,600 MW in August 2012, suggesting that mode 0.9 Hz is related to wind production. This relationship is based on west wind generation (an aggregation of wind production), since wind production solely at West 6 was not available for comparison. Similarly, the mode occurrence increased to 48% in April 2013, when the average wind production increased to 3,500 MW in the same month.

This mode appears to be related to wind production, and occurs consistently every month. It is noted that the energy level of the mode closely tracks wind production (e.g., increases with increasing levels of wind production). Figure 8 shows the comparison of the mode occurrence to the highest energy of the mode during each month spanning the three years. The mode obtained its maximum highest monthly energy of approximately 12 in February 2013, and the minimum highest monthly energy in September 2013 of approximately 0.5. It is recommended that ERCOT monitor this mode in real time, with the following mode meter configuration, to detect increasing energy levels during high wind production.

- PMU signal: West 6 current magnitude.
- Minimum frequency = 0.85 Hz.
- Maximum frequency = 1.2 Hz.
- Minimum energy = 2.
- Damping = 8%.

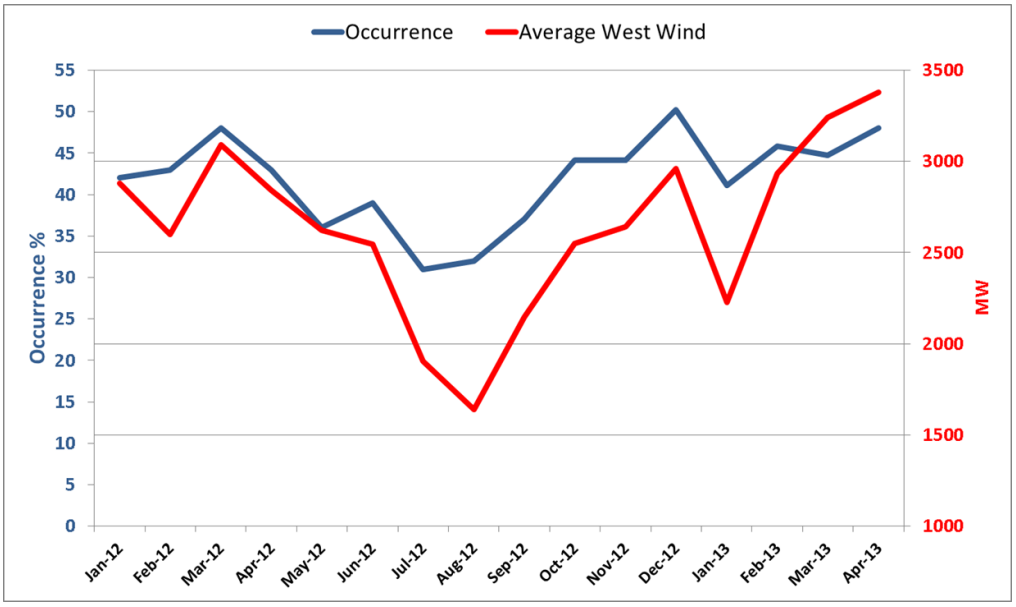


Figure 7. Mode 2 – Mode Occurrence vs. Regional West Wind

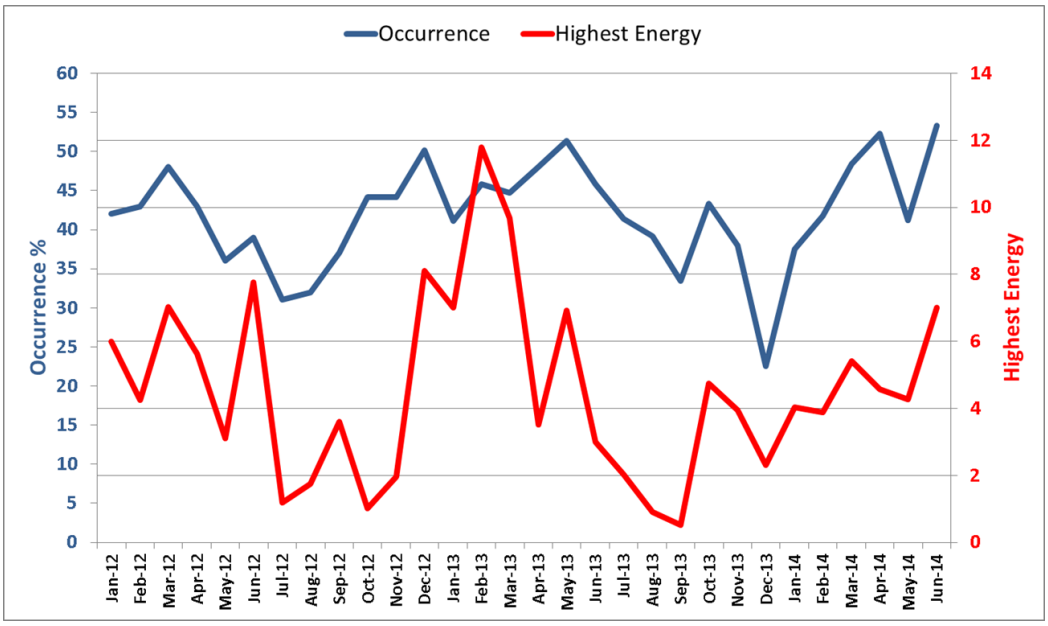


Figure 8. Mode 2 – Mode Occurrence vs. Highest Energy

Mode 6: 2.7Hz

Similar to 0.9 Hz, the study discovered another mode at 2.7 Hz related to wind production. Figure 9 shows the PMU location in the ERCOT Interconnection that had the most consistent occurrence of the 2.7 Hz mode. The mode showed up in the current magnitude signal measurement in the FarWest 4 substation, located near generators, including FarWestGen4.

Figure 11 shows the trend of this 2.7 Hz mode occurrence in the FarWest 4 current magnitude signal over 2 years, and then suddenly disappearing starting January of 2014. The maximum occurrence of the 2.7 Hz mode appeared for 34% of the time in May 2013, and the minimum occurrence of the same mode appeared 9% of the time in July 2013. The average occurrence in the first 2 years is approximately 20% of the time each month. Figure 10 shows the comparison between mode occurrence of 2.7 Hz and the monthly average west wind production in MW from January 2012 to April 2013. The trends of mode occurrence and average west wind have similar patterns, and provide a first indication that the 2.7 Hz mode is likely related to wind production.

This mode is no longer present and its disappearance may be related to the addition of new CREZ transmission lines near FarWest 4, or the re-tuning of machines at FarWestGen4. Figure 11 shows the comparison of the mode occurrence to the highest energy of the mode during each month spanning the first 2 years. During the mode occurrence, the highest energy was not relatively high, as compared to 0.9 Hz. It is recommended that ERCOT review the disappearance of the mode with wind owners and determine the root cause to evaluate the need for additional monitoring.

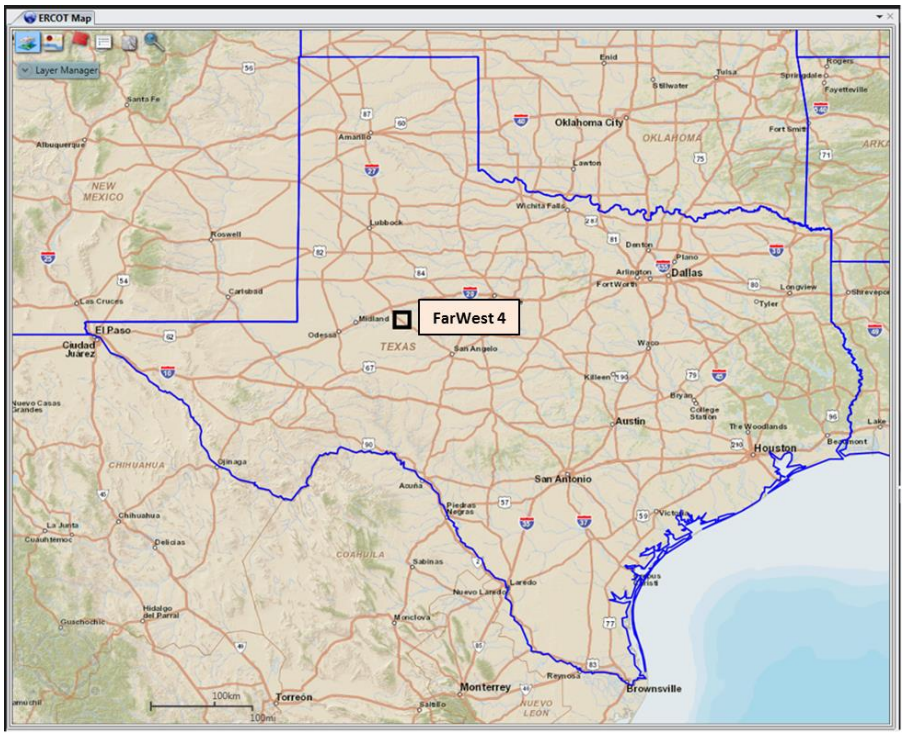


Figure 9. Mode 6 – PMU Location

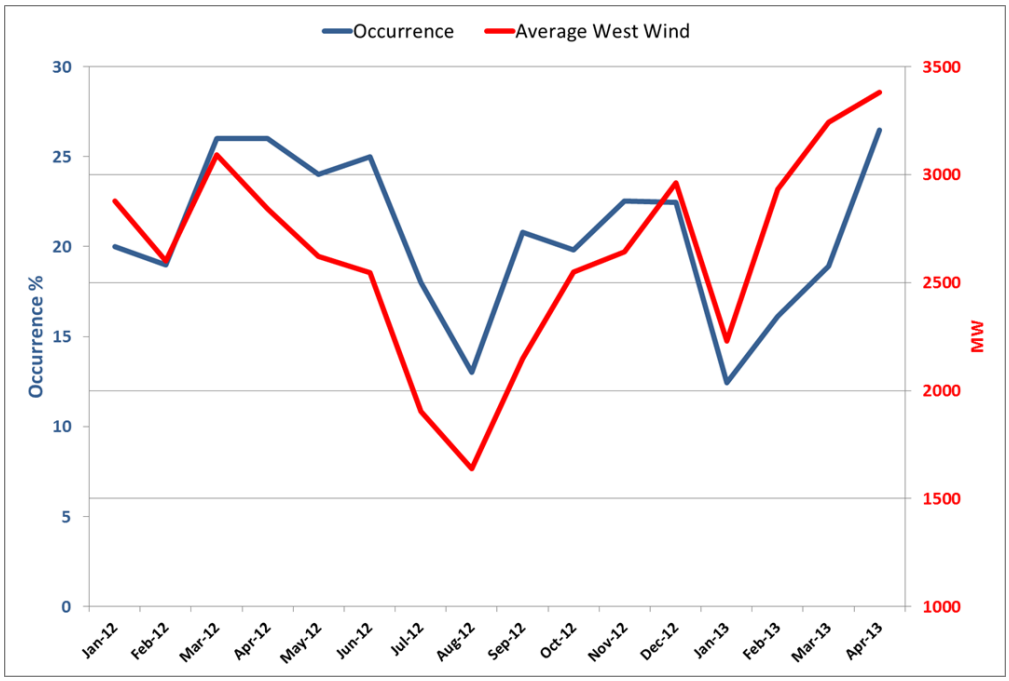


Figure 10. Mode 6 – Mode Occurrence vs. Regional West Wind

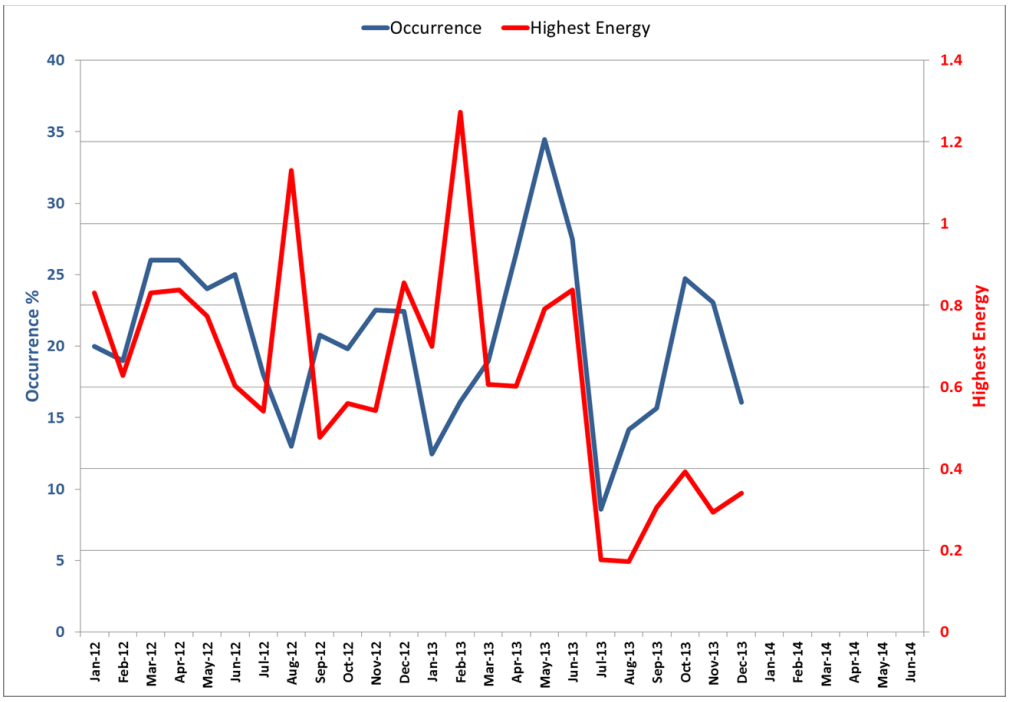


Figure 11. Mode 6 – Mode Occurrence vs. Highest Energy

Mode 8: 5.0 Hz

Figure 12 shows the six different PMU locations in ERCOT that showed the occurrence of the 5.0 Hz mode. Of these six locations, Coast 3 and Coast 4 in the Valley saw the highest, and most consistent, occurrence of this mode. This mode showed up in the voltage magnitude, voltage angle and frequency signal measurements in the Coast 3 and Coast 4 substations, both of which are located near wind generators. Figure 14 shows the trend of the 5.0 Hz mode occurrence in the Coast 3 voltage magnitude signal over 3 years. The mode appeared every month in all three years, except the first three months of 2012 and the month of March 2013. The maximum occurrence of the 5.0 Hz mode was 57% of the month in May 2014, and the minimum occurrence was 0.1% of the month in December 2012.

Figure 13 shows the comparison between the mode occurrence of 5.0 Hz from all signal measurements of Coast 3 and the monthly average south wind production in MW from January 2012 to April 2013. The trend of mode occurrence from all signal measurements does not have patterns similar to the average south wind MW, and thus it appears that this mode is likely not related to wind production. Figure 14 shows the comparison between mode occurrence and monthly highest energy of the 5.0 Hz mode. The highest energy level remained flat and low; not changing with different levels of south wind production, suggesting that the mode is likely driven by the control systems of the nearby wind generators. The mode appears to be related to the operation (simply being online) of the wind generation, and not to the level wind production. During the span of 3 years, the energy level of this mode remains consistently low. The mode obtained its maximum highest monthly energy of approximately 0.09 in May 2013, and its minimum highest monthly energy, in December 2012, was approximately 0.00015.
It is recommended that ERCOT review this 5.0 Hz oscillation with wind owners to determine the root cause, and to evaluate the need for additional monitoring and possible mitigation.

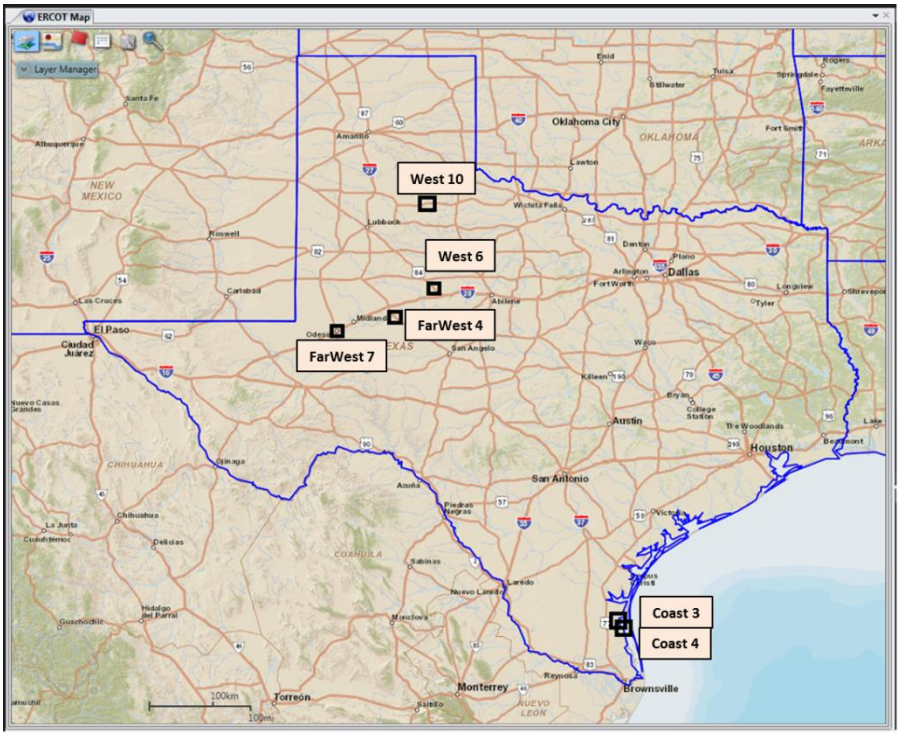


Figure 12. Mode 8 – PMU locations

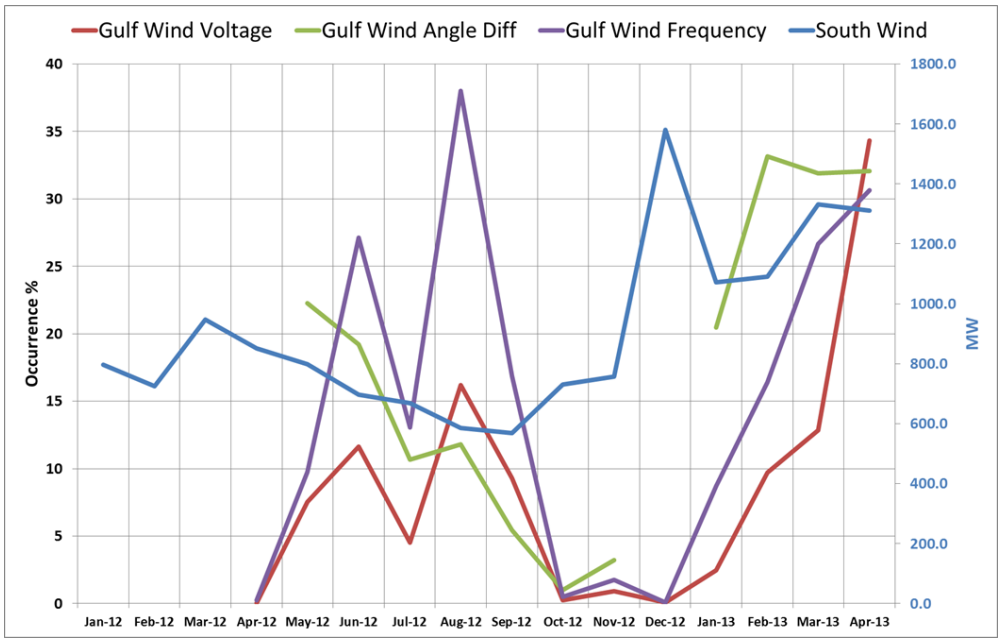


Figure 13. Mode 8 – Mode Occurrence vs. Regional South Wind

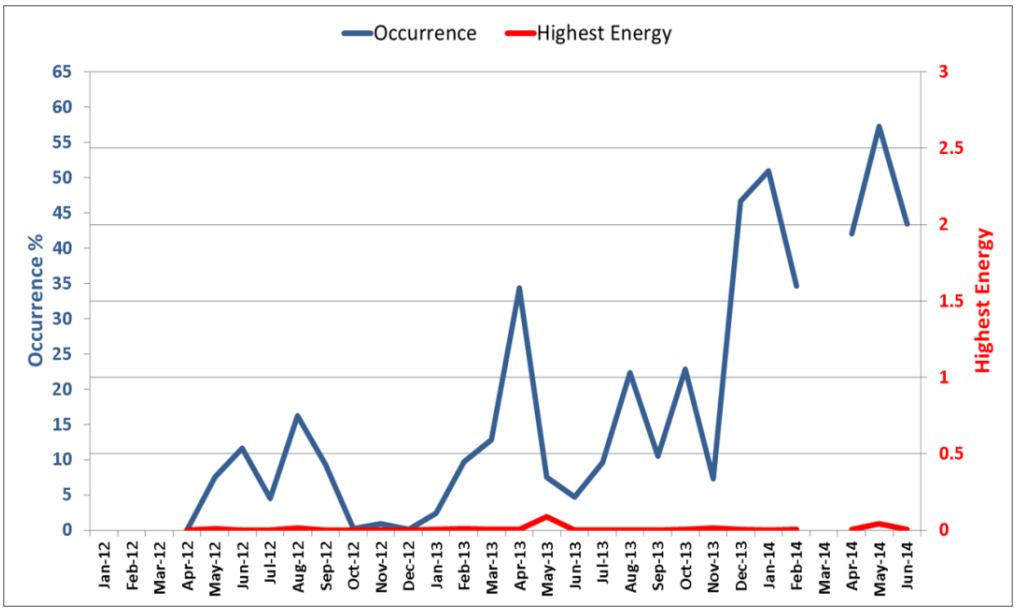


Figure 14. Mode 8 – Mode Occurrence vs. Highest Energy

Mode 9: 5.4 Hz

Similar to the 5.0 Hz mode, the study discovered another mode at 5.4 Hz, at six different locations, as shown in Figure 15. The highest occurrence of the mode showed up in both west Texas and the Panhandle regions of the ERCOT Interconnection. This mode exhibits patterns similar to the 5.4 Hz mode occurrence. The voltage magnitude signal measurement at FarWest 4 substation showed the highest occurrence of the mode in west Texas (FarWest 7 and West 6 also showed the mode, but at lower energy levels). Figure 20 shows the mode occurrence of 5.4 Hz at West 10 and FarWest 4, indicating that the 5.4 Hz mode has different drivers in the two regions. Hence, FarWest 4 in west Texas and West 10 in the Panhandle were identified as critical locations to monitor the 5.4 Hz mode.

Similar to the 5.0 Hz mode at Coast 3 and Coast 4, the 5.4 Hz mode at West 10 appears to be driven by the control systems of the nearby wind generators, and not by the level of wind production. The same forensics for mode 5.0 Hz were obtained using figures 16 and 17. Figure 16 shows the comparison between the mode occurrence of 5.4 Hz and the monthly average north wind production in MW from January 2012 to April 2013. Figure 17 shows the comparison between the mode occurrence and the monthly highest energy of the 5.4 Hz mode. The same relationship appears to be true for this 5.4 Hz mode at FarWest 4, as shown in figures 18 and 19. The highest energy level trend of the 5.4 Hz mode at FarWest 4 remained flat and low; not changing with different levels of wind production, even though the mode occurrence interestingly tracked the west wind production. It is recommended that ERCOT review the 5.4 Hz

oscillation with wind owners to determine the root cause, and to evaluate the need for additional monitoring and possible mitigation.

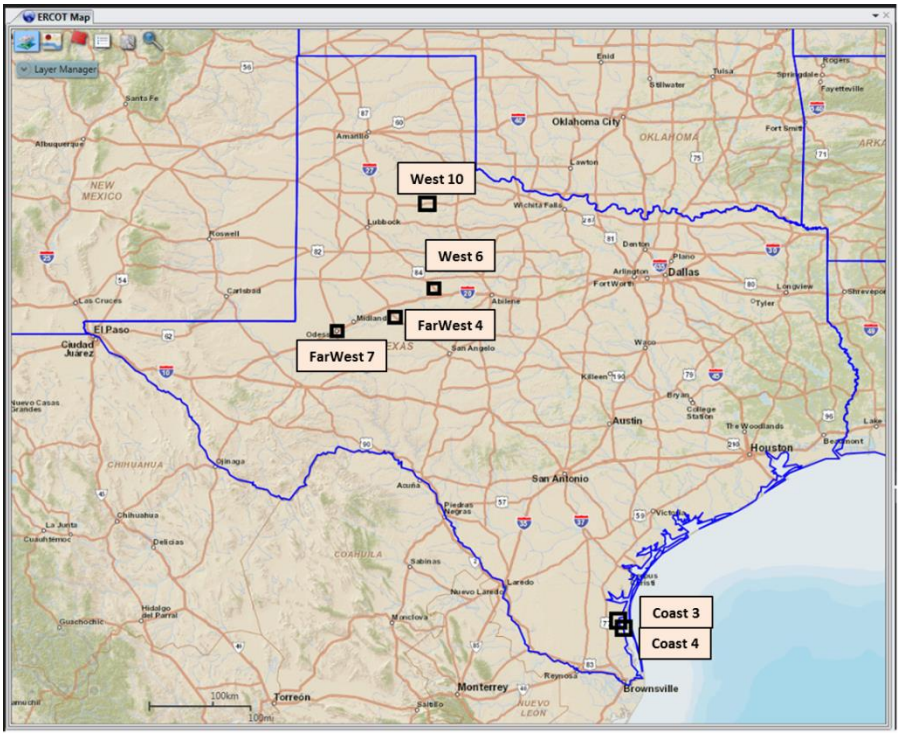


Figure 15. Mode 9 – PMU Locations

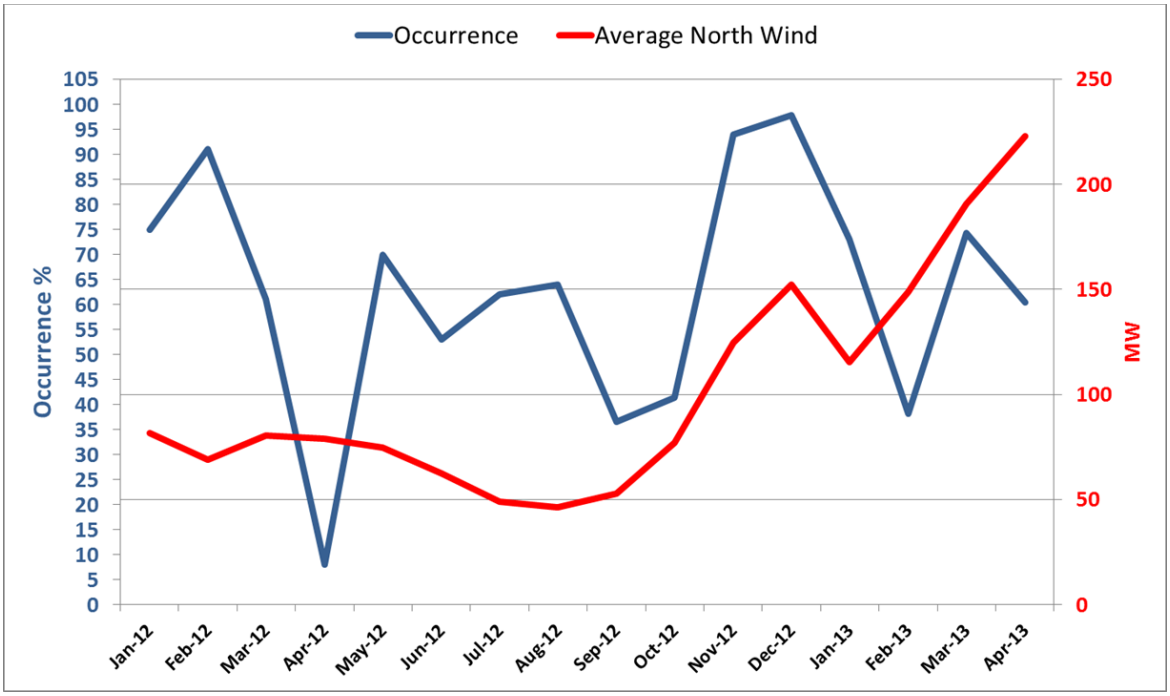


Figure 16. Mode 9 at West 10 – Mode Occurrence vs. Regional North Wind

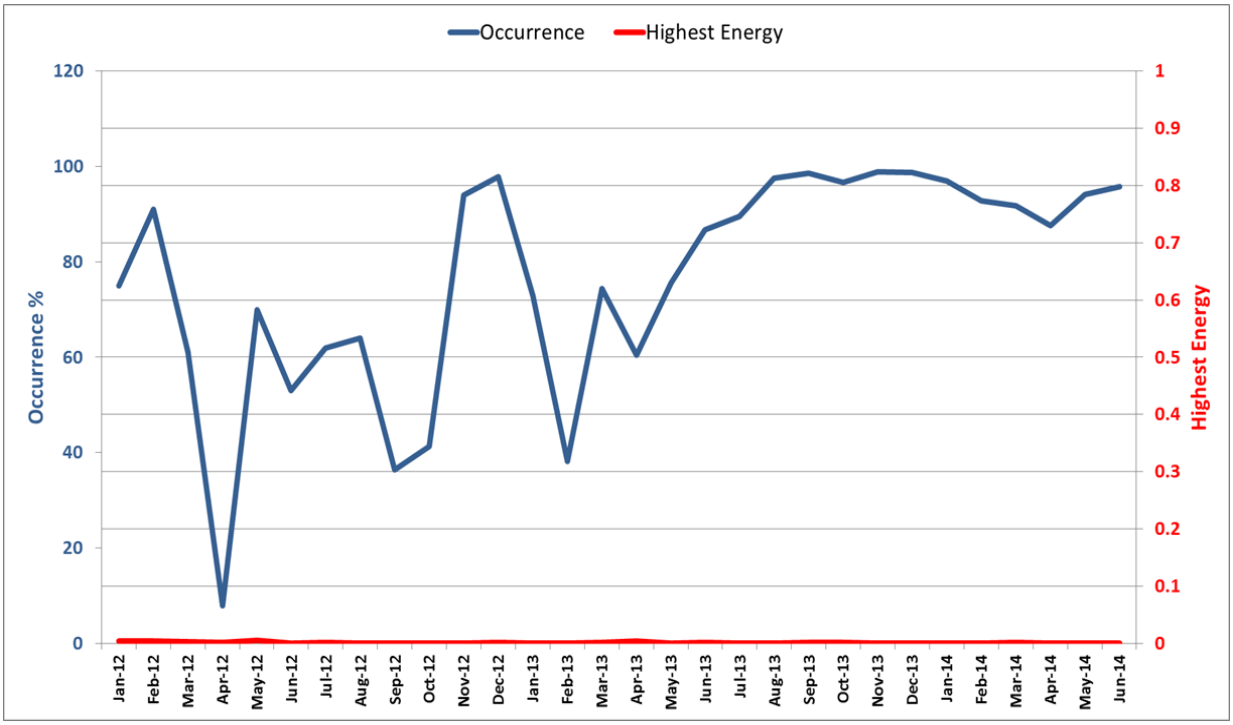


Figure 17. Mode 9 at West 10 – Mode Occurrence vs. Highest Energy

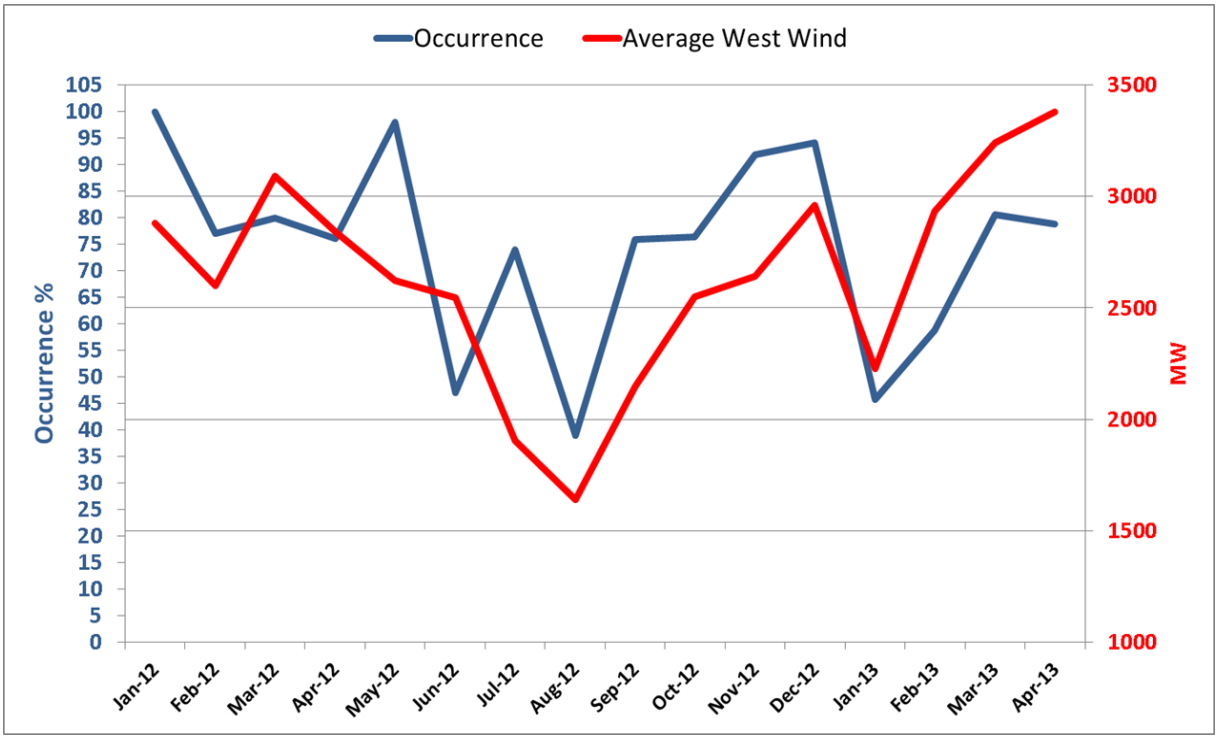


Figure 18. Mode 9 at FarWest 4 – Mode Occurrence vs. Regional West Wind

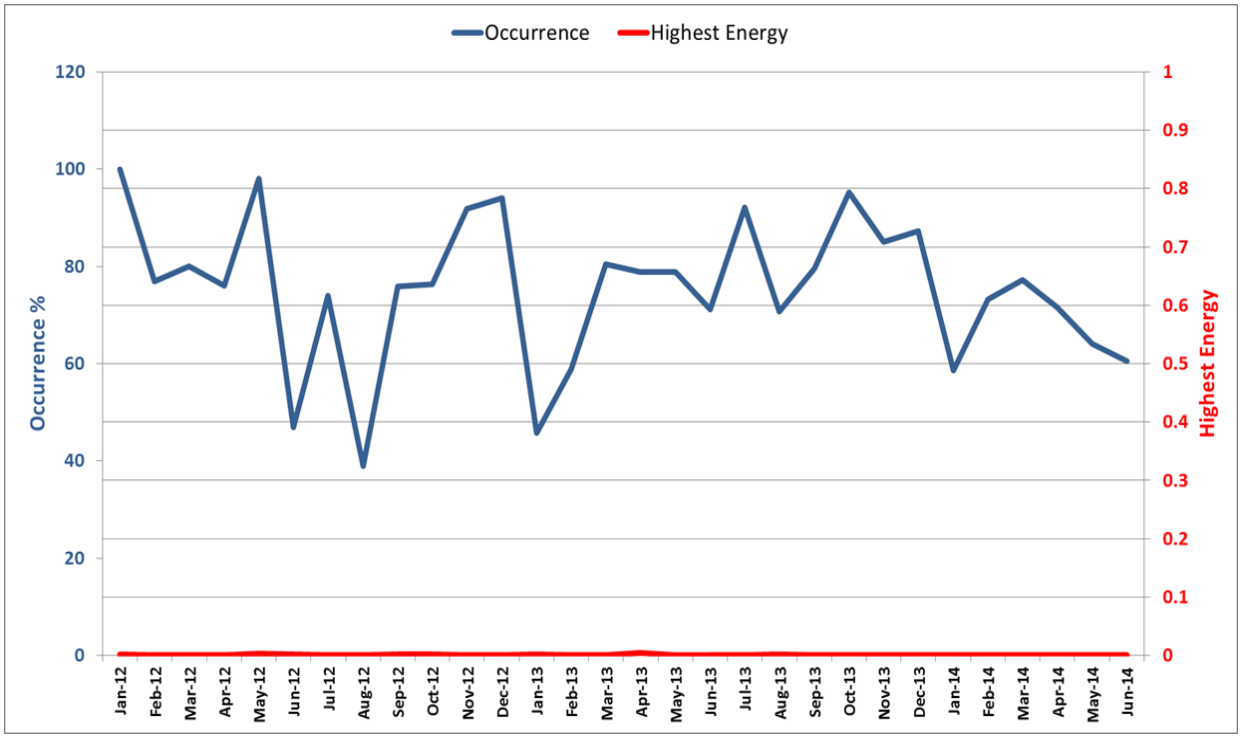


Figure 19. Mode 9 at FarWest 4 – Mode Occurrence vs. Highest Energy

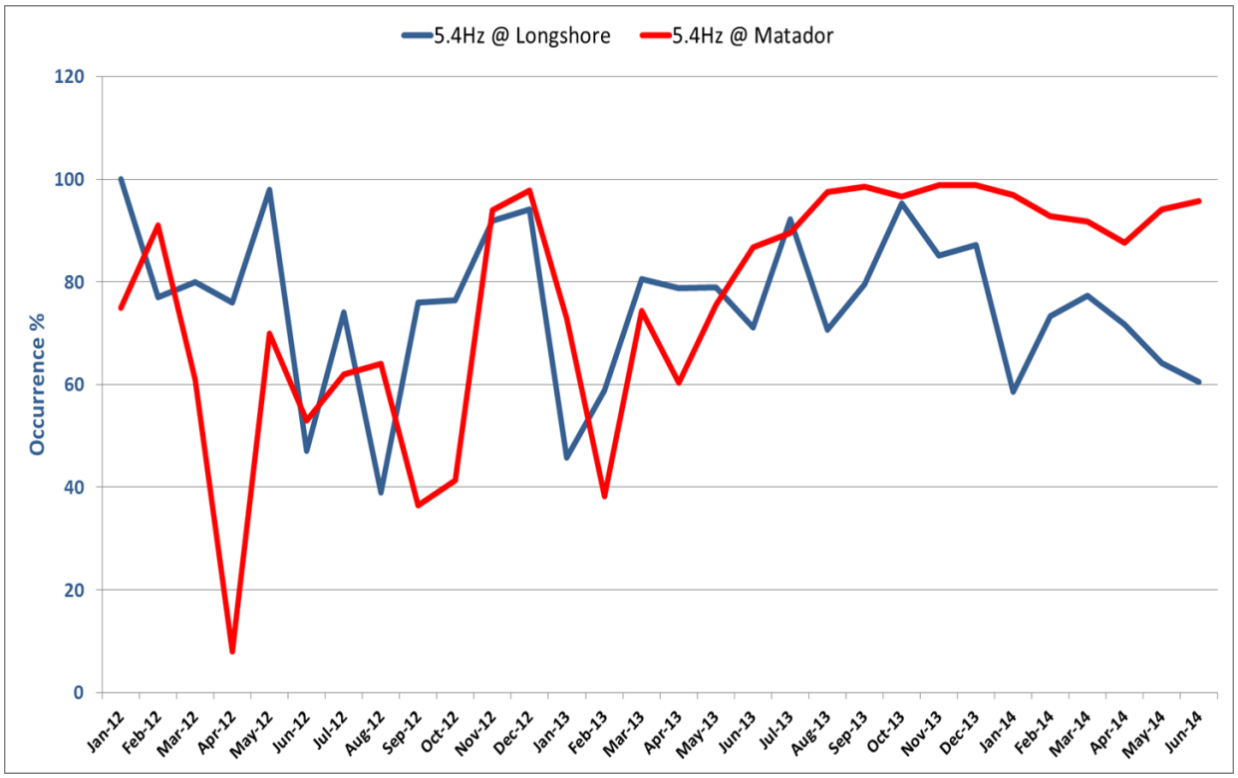


Figure 20. Mode 9 – West 10 vs. FarWest 4

Mode 10: 6.0 Hz

Similar to the 5.0 Hz and 5.4 Hz modes, the study discovered another mode at 6.0 Hz, which was present at six locations, as shown in Figure 21. The mode was strongest at West 10. Figure 22 shows the first indication that the mode at 6.0 Hz appears not to be related to average monthly north wind production, but these oscillations are detected more strongly near wind generators. Figure 23 shows the comparison of the mode occurrence with the highest energy level of the current magnitude signal measurement at West 10. The monthly highest energy trend remained fairly flat at low levels (< 0.01) except in January to March and in August 2012, suggesting that these oscillations are driven by control systems at the local wind generators and can reach high energy levels. This also suggests the need for additional monitoring. The West 10 current magnitude signal was selected as the critical location to monitor in real time.

It is recommended that ERCOT review the 6.0 Hz oscillation with wind owners for possible mitigation, and also monitor this mode in real time with the following configuration to detect increasing energy levels during high wind production.

- PMU signal: West 10 current magnitude.
- Minimum frequency = 5.5 Hz.
- Maximum frequency = 6.5 Hz.
- Minimum energy = 5.
- Damping = 8%.

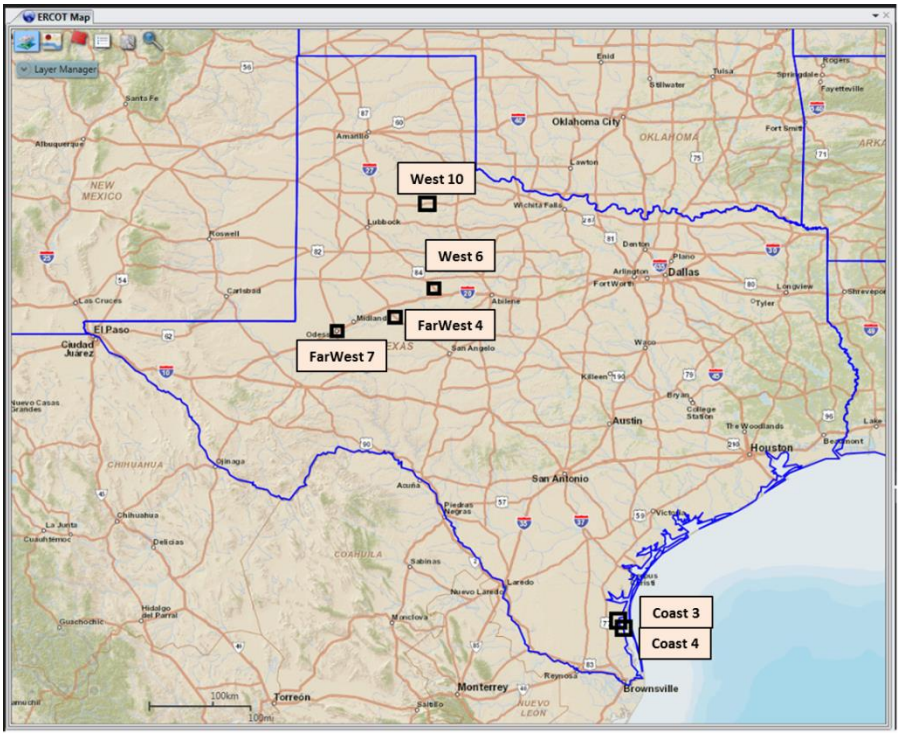


Figure 21. Mode 10 – PMU Location

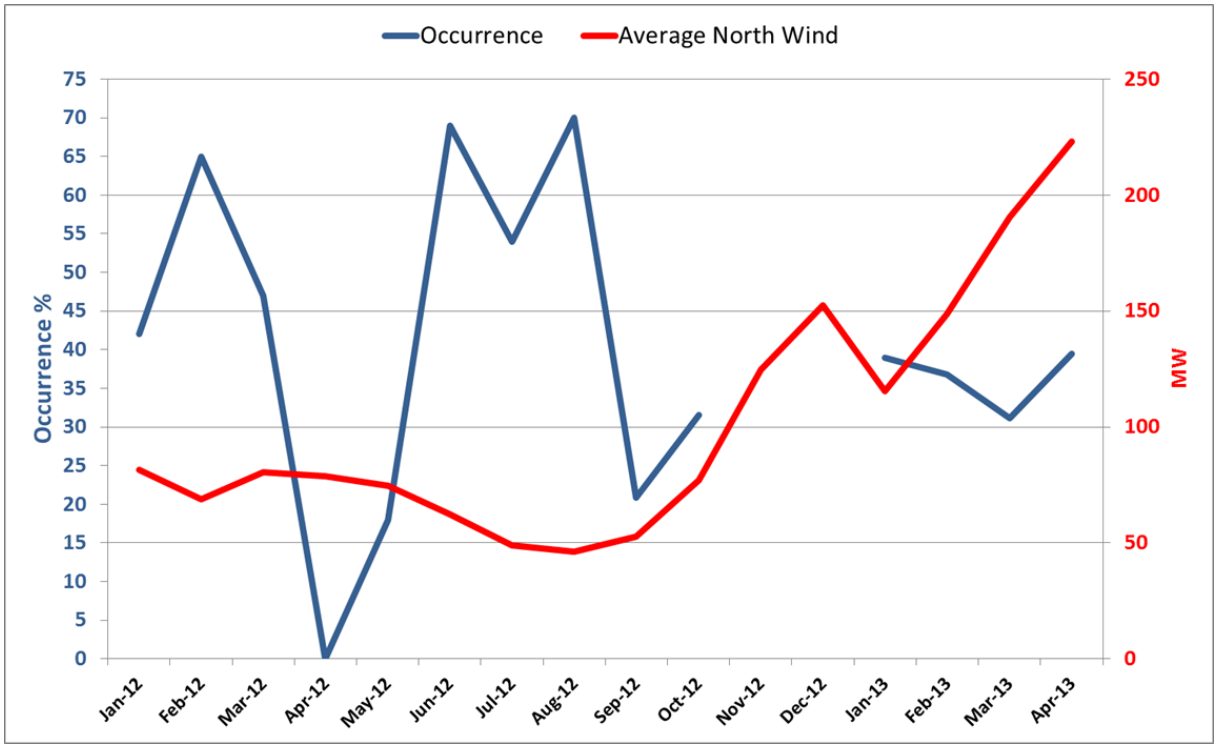


Figure 22. Mode 10 – Mode Occurrence vs. Regional North Wind

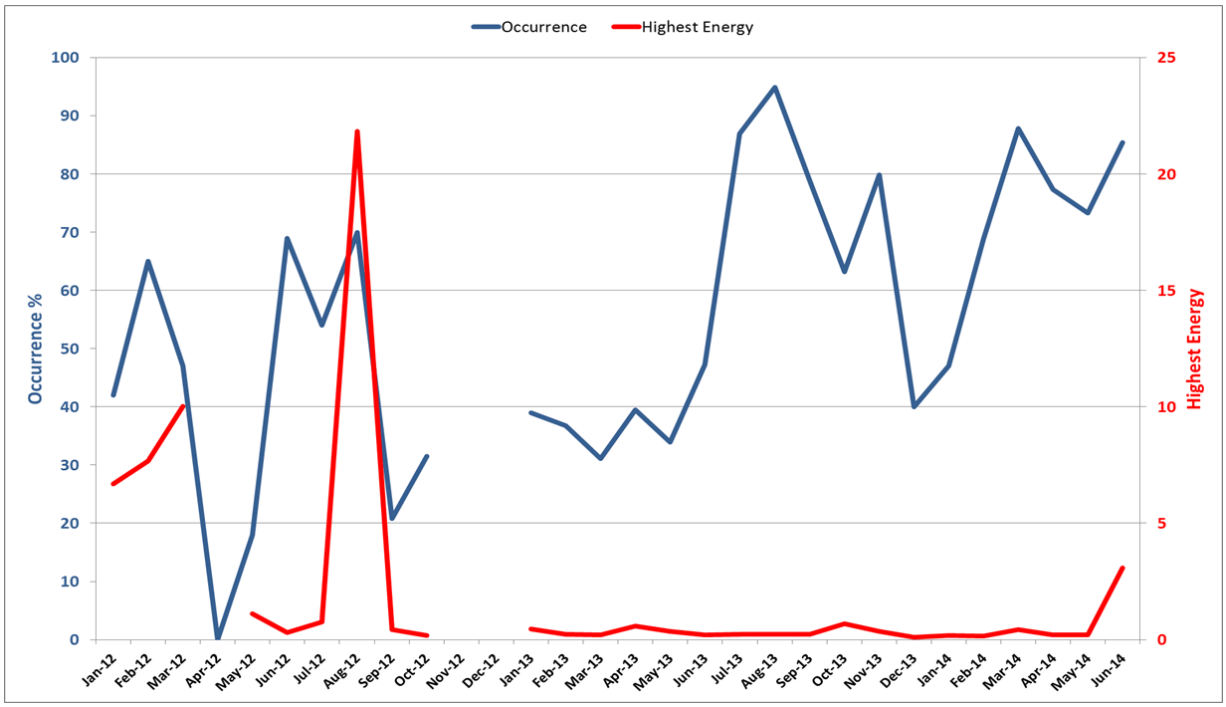


Figure 23. Mode 10 – Mode Occurrence vs. Highest Energy

West 10 appears to have two strong modes at 6.0 Hz and 5.4 Hz, both driven by the control systems of the nearby wind generators. Figure 24 shows the mode occurrence of 5.4 Hz at West 10 measured from current magnitude signal spanning 3 years. The mode occurrence at 5.4 Hz shows consistently higher persistence than the 6.0 Hz trend, but never showed the high energy levels which were recorded for the 6.0 Hz mode.

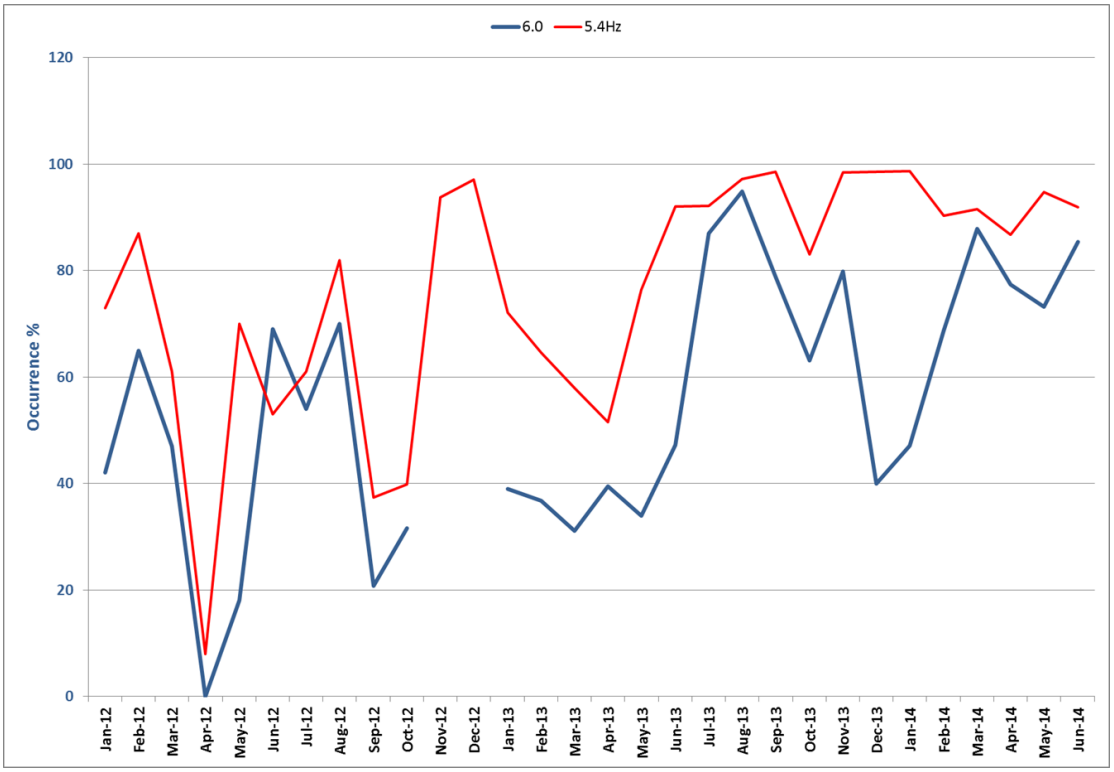


Figure 24. Mode 10 at West 10 – 5.4 Hz vs. 6.0 Hz

Mode 7: 3.2 Hz

Figure 25 shows the PMU location in the ERCOT Interconnection that had observed a 3.2 Hz mode. This mode showed up in the current magnitude signal measurement in the West 10 substation. Figure 27 shows the trend of the 3.2 Hz mode occurrence in the West 10 current magnitude signal over 3 years. The mode does not appear to be consistent ,such as 5.0 Hz, 5.4 Hz and 6.0 Hz, but rather intermittent. The mode appeared in January, February, March, and June of 2012, then disappeared until January 2014, when it reappeared. The maximum occurrence of the 3.2 Hz mode appeared for 20% of the time in January 2014, and the minimum occurrence of the same mode appeared 10% of the time in March 2013. Figure 26 shows the comparison between the mode occurrence of 3.2 Hz and the monthly average north wind production in MW from January 2012 to April 2013, suggesting no causal relationship.

Figure 27 also shows the comparison of the monthly mode occurrence and the highest energy levels, suggesting that the energy of the mode is relatively high when it occurs. This mode appears to be driven by control system setting changes, and not by the level of wind production. This mode does not appear all the time with low energy, but rather occurs sporadically with high energy, which requires additional monitoring to detect and mitigate oscillations.

It is recommended that ERCOT do additional monitoring in real time with the following configuration to detect increasing energy levels during high wind production.

- PMU signal: West 10 current magnitude.
- Minimum frequency = 2.6 Hz.
- Maximum frequency = 3.8 Hz.
- Minimum energy = 50.
- Damping = 8%.

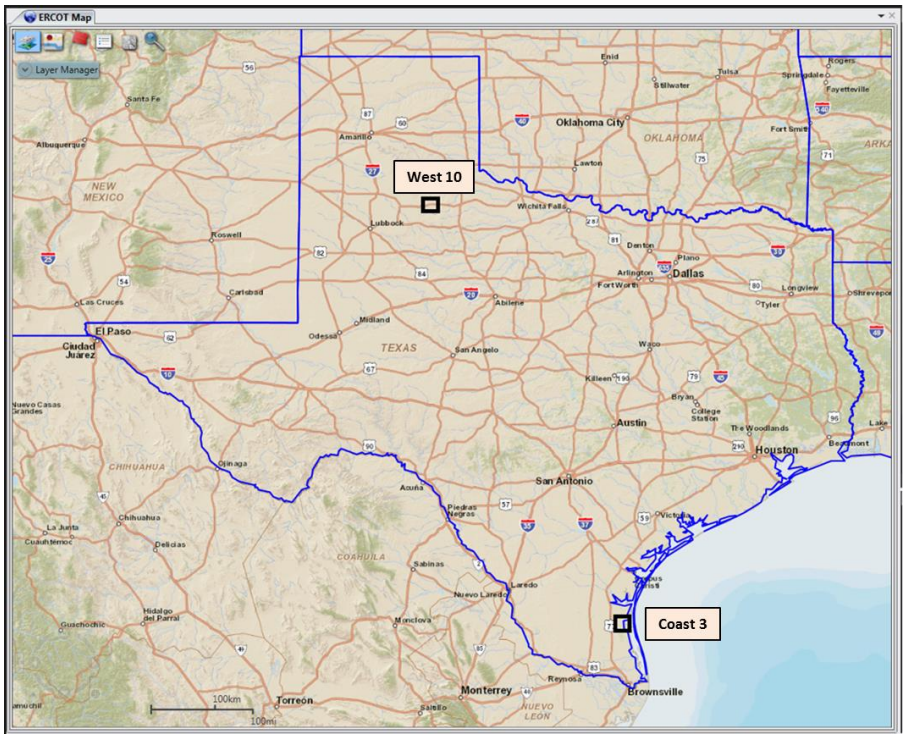


Figure 25. Mode 7 – PMU Locations

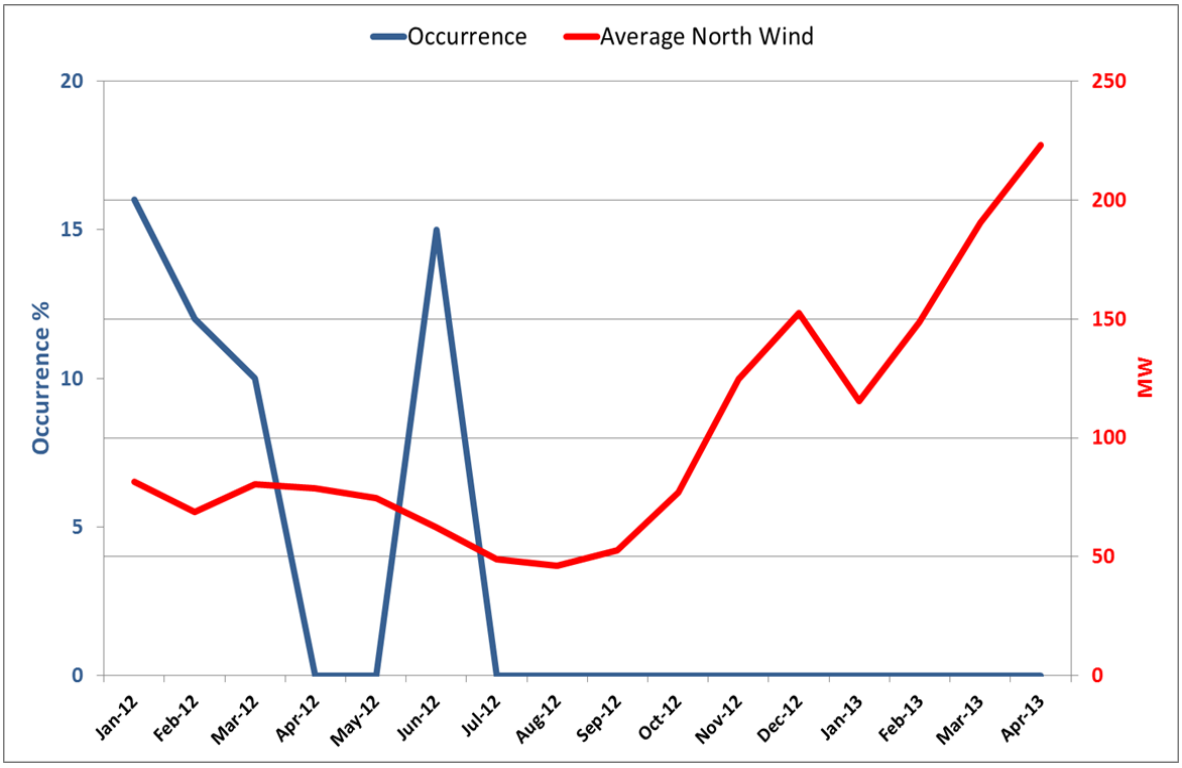


Figure 26. Mode 7 – Mode Occurrence vs. Regional North Wind

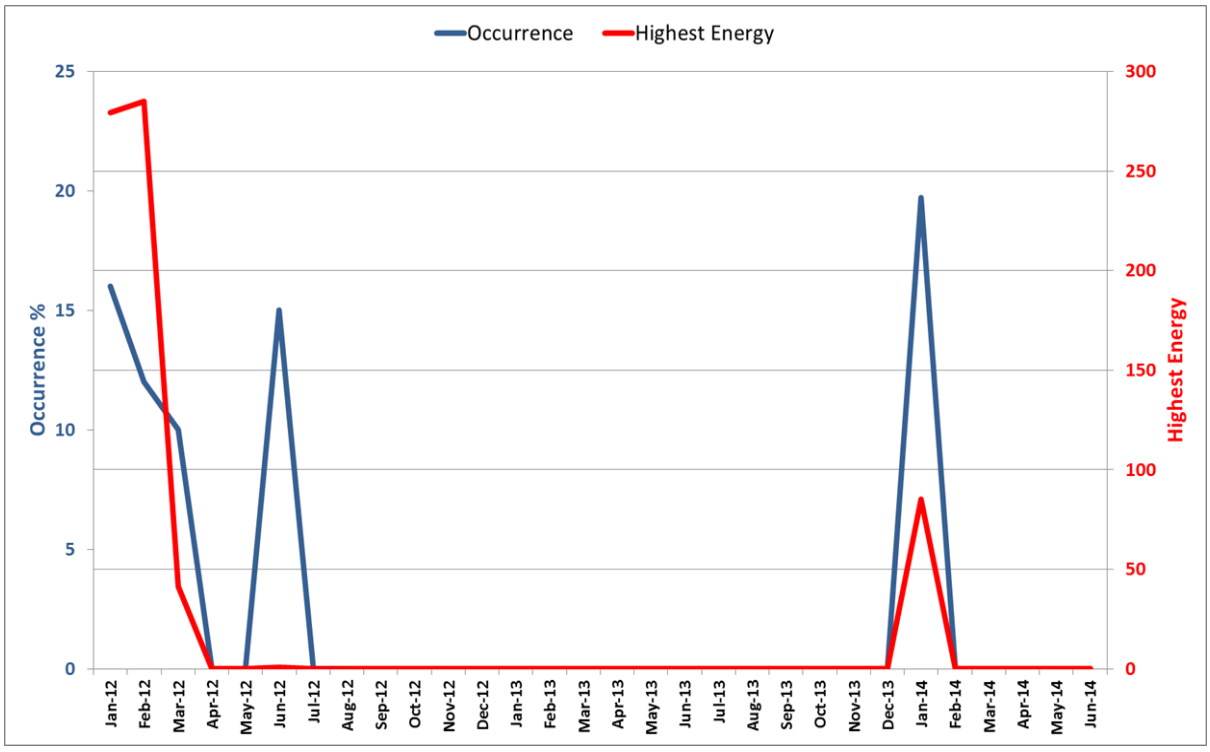


Figure 27. Mode 7 – Mode Occurrence vs. Highest Energy Level

The study also discovered other modes (1.5 Hz, 1.7 Hz, and 2 Hz) similar to 3.2 Hz which are apparently driven by setting changes in the control systems of the nearby wind generators. The sources and energy levels of those modes are explained below.

Mode 3: 1.5 Hz

The study discovered a mode at 1.5 Hz, at Coast 3 in the Valley region, as shown in Figure 28. This mode occurred only in April 2012, for 0.04% of the time, and with a small energy of approximately 0.02. Figure 29 shows the comparison of the mode occurrence at Coast 3 current magnitude signal with the average south wind production, suggesting that this mode occurs intermittently, and is driven by settings change in the wind generation control systems. It is recommended that ERCOT do additional monitoring of this mode with the following configuration.

- Minimum frequency = 1.0 Hz.
- Maximum frequency = 2.0 Hz.
- Minimum energy = 0.1.

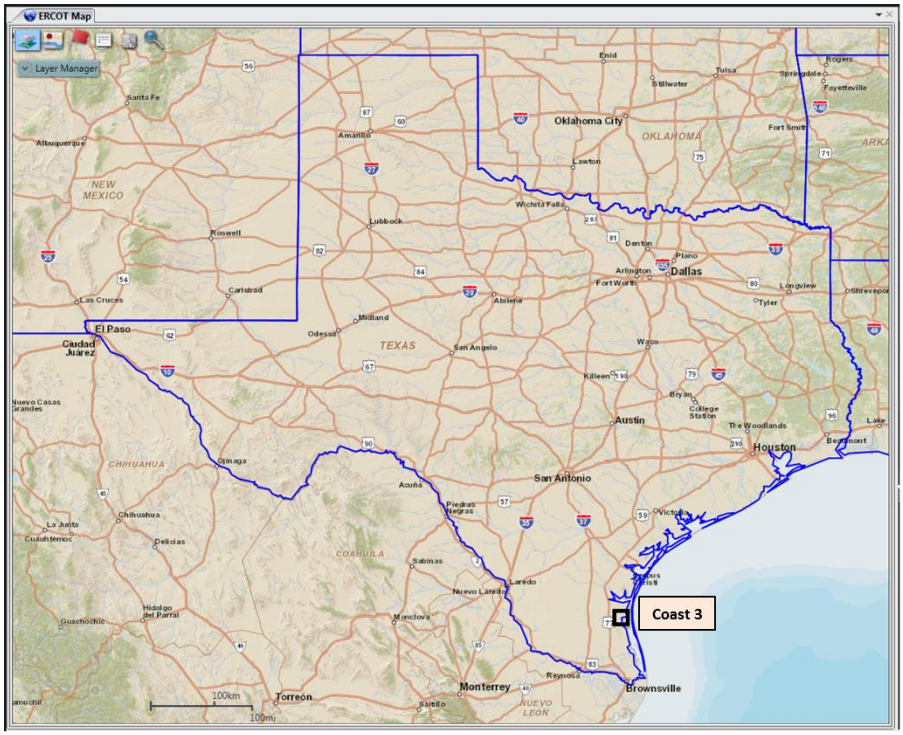


Figure 28. Mode 3 – PMU Location

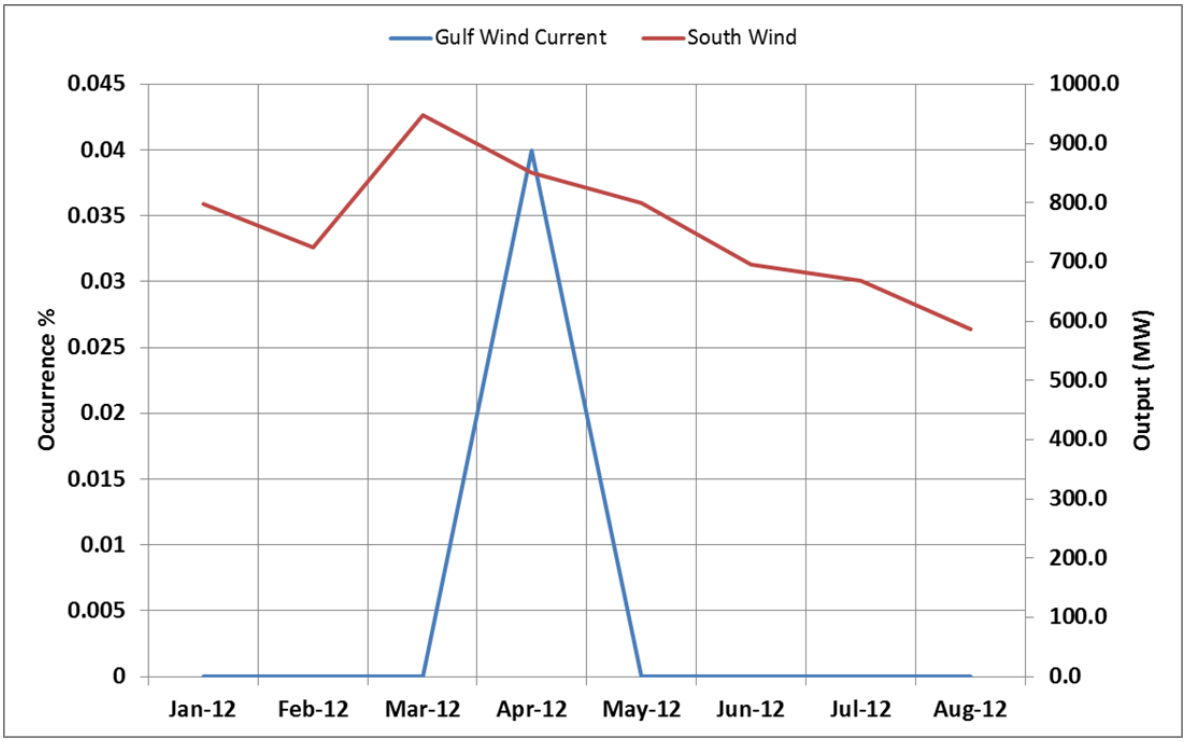


Figure 29. Mode 3 – Mode Occurrence vs. Regional South Wind

Mode 4: 1.7 Hz

The study also discovered a mode at 1.7 Hz, at FarWest 7 in the west Texas region, as shown in Figure 30. This mode occurred only in January 2012, for 4% of time, with high energy of approximately 36. Figure 31 shows the comparison of the mode occurrence at FarWest 7 in the current magnitude signal with the average west wind production, suggesting this is an intermittent occurrence. The oscillation was observed more strongly near FarWest 7, which has nearby combined cycle units. This appears to be a local issue and ERCOT needs to review the appearance of this mode with the local generation plant owners to determine the root cause, and to evaluate the need for additional monitoring.

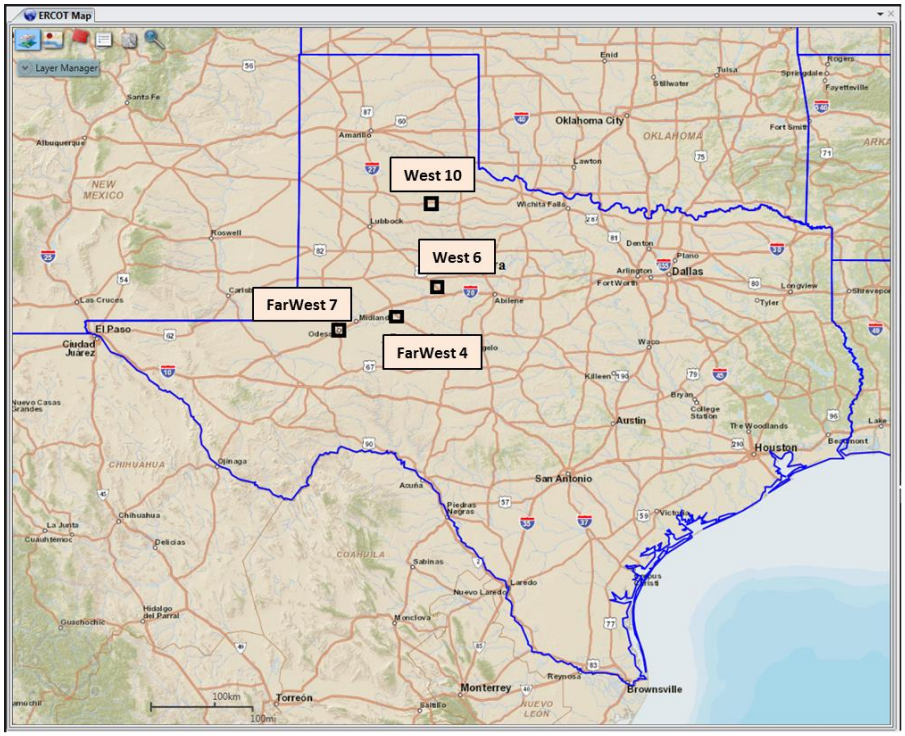


Figure 30. Mode 4 – PMU Location

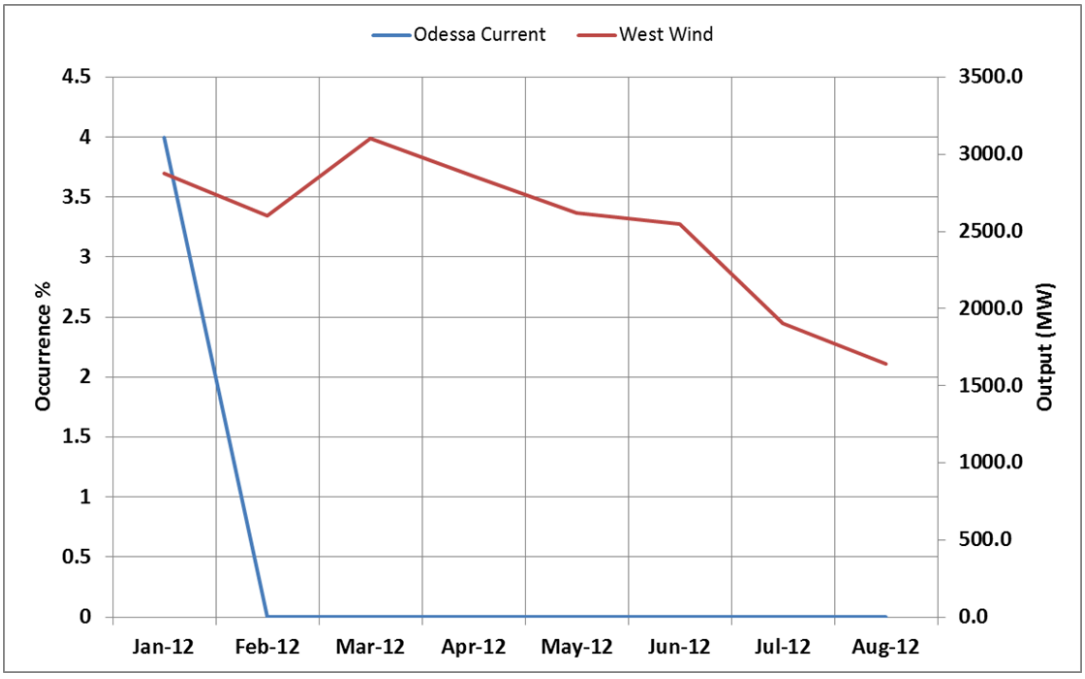


Figure 31. Mode 4 – Mode Occurrence vs. Regional West Wind

Mode 5: 2.0 Hz

The study also discovered another mode at 2.0 Hz at Coast 3 (voltage magnitude signal measurement) in the Valley region, as shown in Figure 32. This mode occurred only in April 2013, for 0.8% of time, with high energy approximately 0.5. The oscillation was observed more strongly near Coast 3, which has nearby wind generators such as CoastGen3, CoastGen4, and CoastGen5. It is recommended that ERCOT do additional monitoring of the mode with the following configuration.

- Minimum frequency = 1.5 Hz.
- Maximum frequency = 2.5 Hz.
- Minimum energy = 0.1.

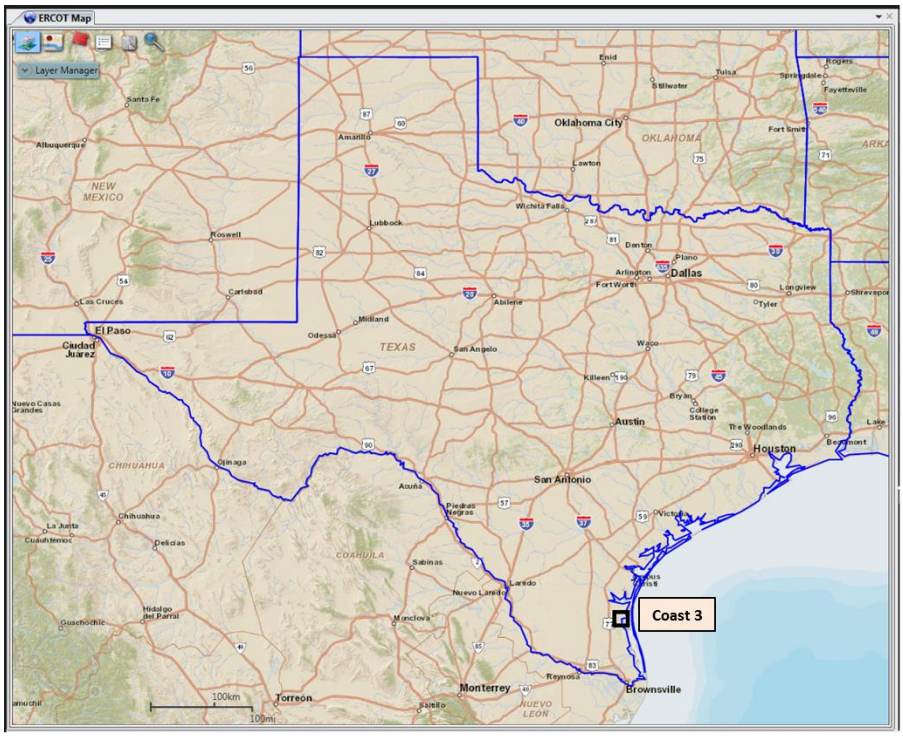


Figure 32. Mode 5 – PMU Location

Mode 1: 0.6 Hz

The study uncovered a mode at 0.6 Hz, showing most strongly in the West 10 current magnitude signal, and which appeared for the first three months of 2012, and was never detected again. This mode occurrence at West 10 did not follow the average north wind production, but was observed at nearby wind generators, including WestGen10 at West 10. This appears to be a local issue and may be related to a local oscillation triggered by a transmission network topology change. The maximum highest energy of the mode was approximately 2, and the minimum highest energy was about 1.6. It is recommended that ERCOT review the appearance of this mode with plant owners in order to determine the root cause, and to evaluate the need for additional monitoring.

Figure 33 shows the PMU locations that observed the 0.6 Hz mode, but more strongly at West 10. Figure 34 shows the comparison of the mode occurrence with the average monthly north wind production, and indicates that it is likely not related to the level of wind production.

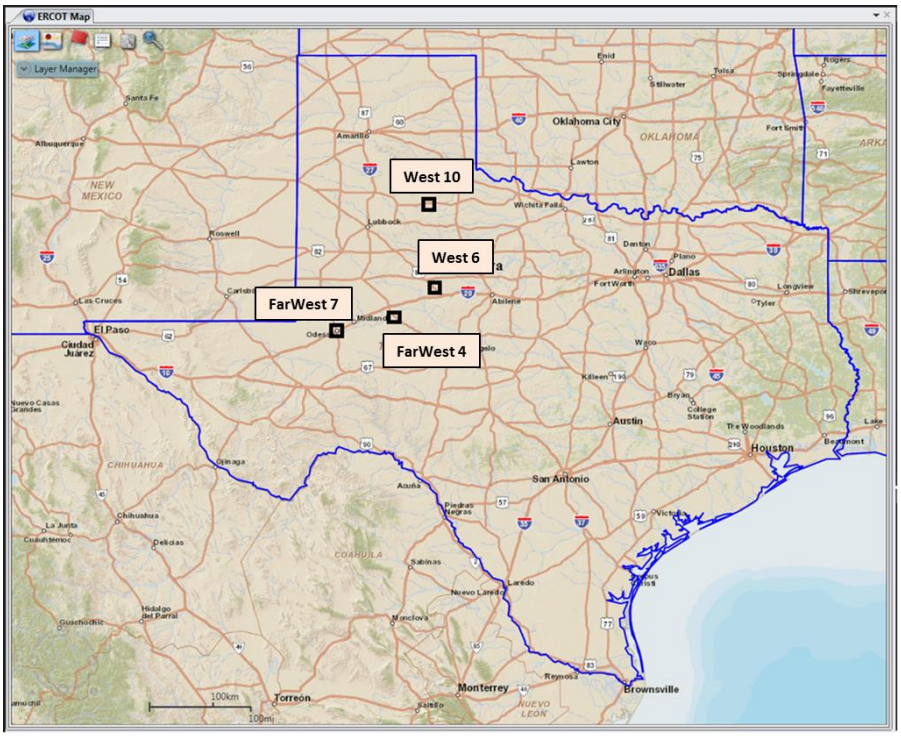


Figure 33. Mode 1 – PMU Location

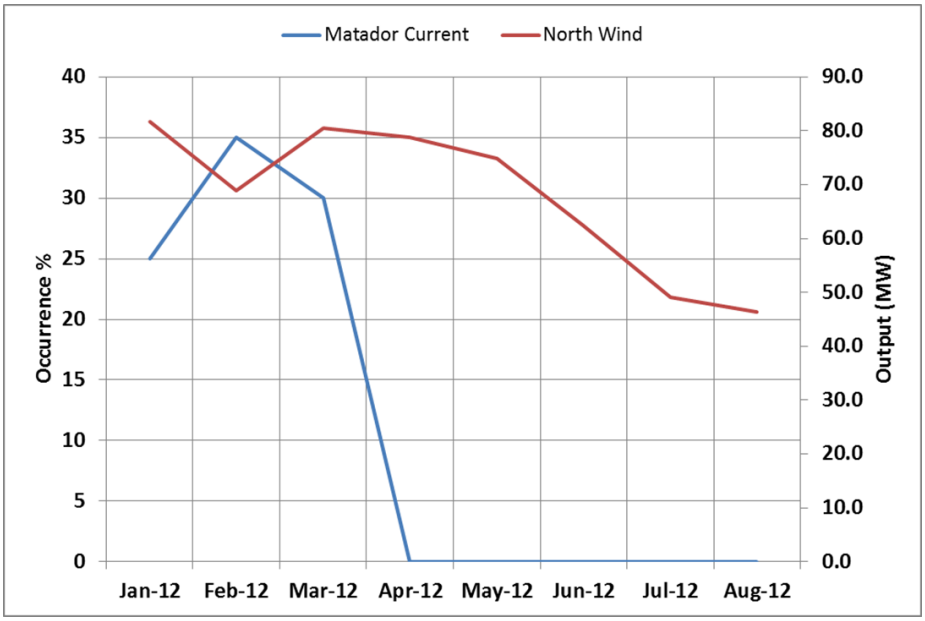


Figure 34. Mode 1 – Mode Occurrence vs. Regional North Wind

10. Conclusion

The detection of unknown oscillations from phasor data spanned 3 years of ERCOT synchrophasor data, and was performed using the Phasor Data Mining Tool. The tool enabled the automatic scanning of the data in periodic intervals, and produced a results summary, including detected oscillations, percentage of occurrence (time), and energy level, time-stamped with the PMU location.

This analysis was based on six PMUs located near wind farms in the ERCOT Interconnection. The Phasor Data Mining Tool was configured with the needed algorithm settings to scan for oscillations within the frequency band from 0.1 Hz to 15 Hz. The measurements, including frequency, voltage phasor and current magnitude for each PMU, were used to scan through the input data for oscillation modes using 60-second blocks of data, and, when oscillations were detected, the calculated damping and energy of each mode was recorded.
The results were time-stamped and tagged to the PMU measurements to identify the source of the oscillations. The tool was used to discard modes with damping greater than 8%. The tool leveraged the PMU status information to clean bad data in order to avoid false detections. The output results from the tool were parsed and post processed through MATLAB scripts to rank the oscillatory modes according to high occurrence and high energy. Then the results were studied to identify any relationships between mode occurrence and regional wind data. The highest energy of each mode was extracted and compared with the mode occurrence to baseline the minimum energy required to monitor the mode in real time, and also to differentiate modes related to wind production versus modes driven by control systems, or setting changes in control systems.

Some of the key findings are as follows:

1. The study identified 10 different ERCOT oscillatory modes.
2. The occurrence of 2 modes appear to be related to wind production – 0.9 Hz (West 6) and 2.7 Hz (FarWest 4).
3. The occurrence of 4 modes appear to be related to control system settings changes – 1.5 Hz (Coast 3), 1.7 Hz (FarWest 7), 2 Hz (Coast 3), and 3.2 Hz (West 10).
4. Three modes appear to be related to the presence of wind generation and control systems - 5.0 Hz (Coast 3), 5.4 Hz (West 10 & FarWest 4), and 6.0 Hz (West 10).
5. The occurrence of 1 mode appears to be a local oscillation due to a topology change or tuning of wind generators – 0.6 Hz (West 10).

This study concludes that four modes appear consistently for 3 years and are still present. There are four other modes that appear intermittently with high energy. There are two other modes that appeared consistently at the beginning of the study, and then were never detected again. The report provides insights on the configuration for monitoring certain modes in real time to detect these oscillations. The modes which disappeared after some duration of time may need additional

review by ERCOT with plant owners to determine the root cause and to evaluate the need for additional monitoring.

11. Appendix

1. Final Report Presentation Material - "CCET_Data_Mining_Oscillation_Study_313b_110414_ppt_external.pdf".

CCET Discovery Across Texas
Wind Characteristics – Oscillations Data Mining

Presented to CCET
November 5, 2014

John W. Ballance

Prashant C. Palayam

Electric Power Group

PUBLIC VERSION

CCET

Oscillations Data Mining - Outline

- Background & Purpose
- Goals
- Methodology
- Oscillations Data Mining Candidates
- MATLAB – Post Processing
- Oscillations Data Mining Performance
- Oscillations Mining Results – 3 years, 10 Modes
- Conclusion

Background & Purpose

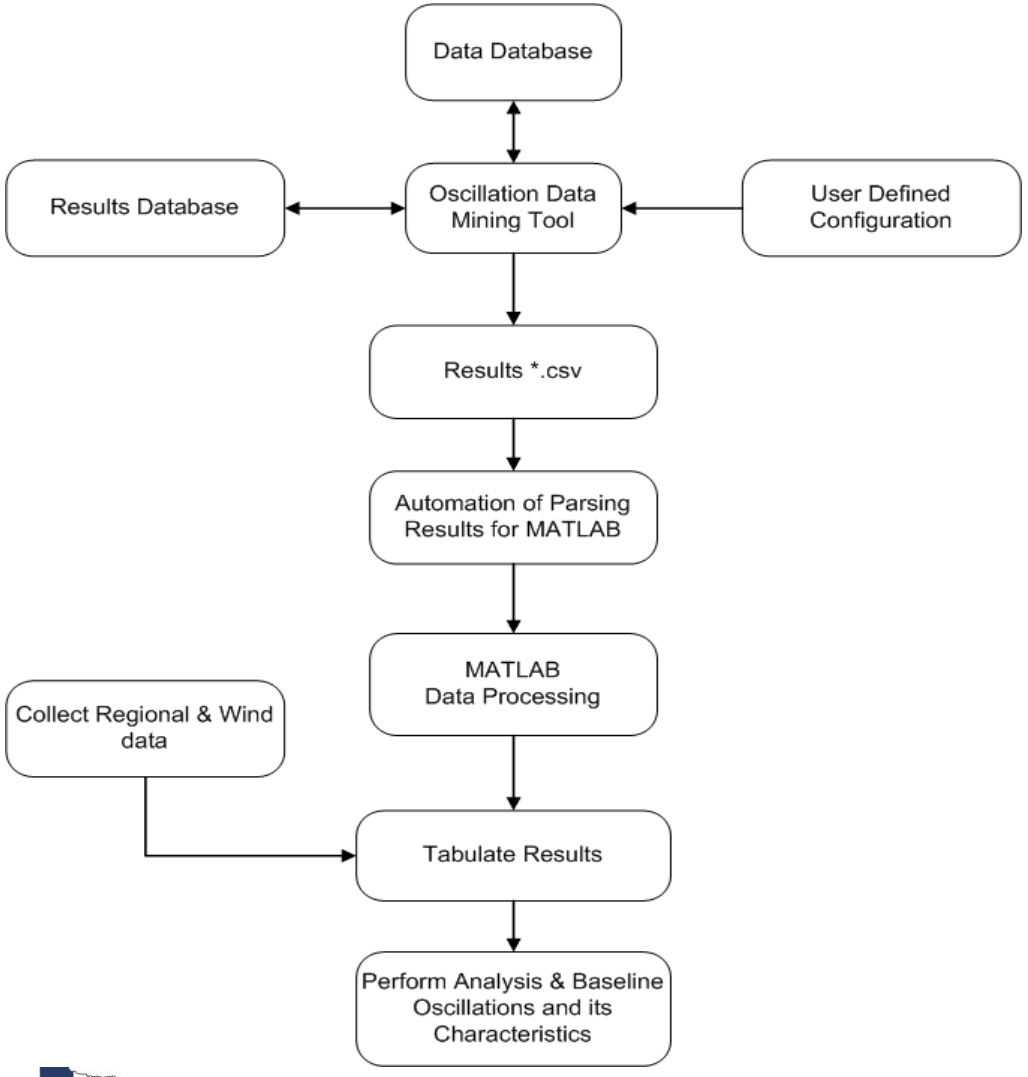
- Texas has the greatest amount of wind generation online in the nation, and set a new wind production record each year
- Early detection and mitigation of oscillations prevents system vulnerability and customer complaints
- These oscillations can possibly grow at high energy with increasing levels of wind generation
- Baselining the grid oscillations and monitoring in real time is crucial to ensuring reliable operation of grid
- Purpose – Perform phasor data mining analytics to investigate oscillations in the ERCOT Interconnection and study its impact with increasing levels of wind generation

Goals

- Determine other unknown oscillations
- Determine source of unknown oscillations
- Determine the type of identified oscillations –wind related or driven by control system
- Baseline oscillations characteristics – mode damping and energy for real-time monitoring

Methodology

- Phasor data (2012-2014)
- Regional load/wind – EMS data
- User configuration –*.xml file
- Identify significant oscillations using MATLAB
- Map different sources of data
- Perform study



Oscillations Data Mining Candidates

- **PMUs near wind farms** – FarWest 7, West 10, FarWest 4, West 6, Coast 4, Coast 3, and North 7 (voltage angle reference)
- **Signal types** – frequency, voltage phasor, current
- **1 frequency band -** captures all modes
- **Use C37.118 status bits–** clean data
- **Mining tool – reports**
- Every minute
- Modes with damping < 8%
- Minimum energy = 0

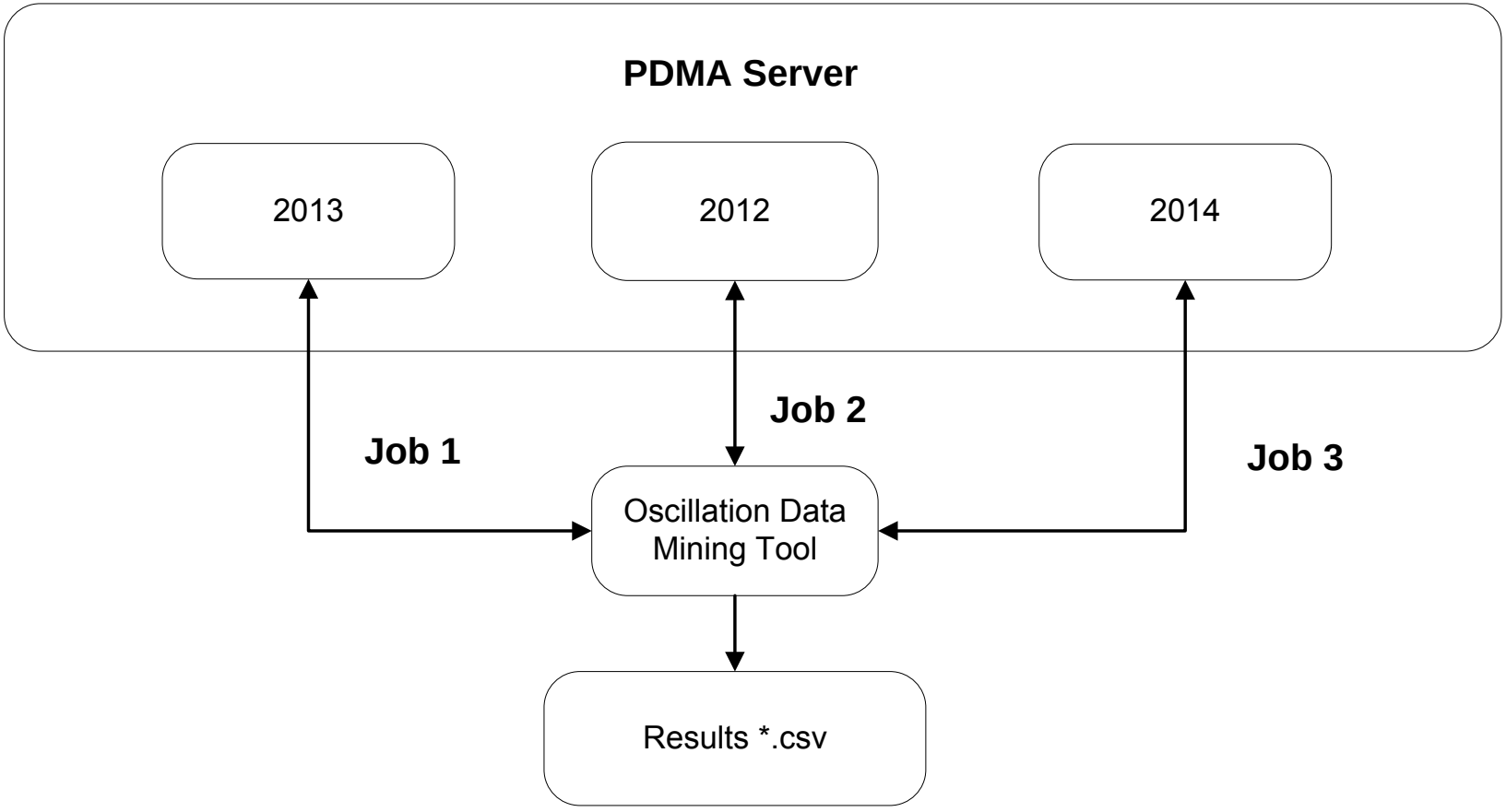
Identification of Significant Oscillations – MATLAB Post Processing

- Oscillation Data Mining Tool outputs **all calculated modes** every minute for all configured signals
- Planners and Operators need to focus on “modes” that:
  - Occur most of the time (high occurrence)
  - Occur with high energy (high magnitude)
- MATLAB code was written to identify such critical “modes” whose:
  - Existence is “>=“ 20% of highest occurrence
  - Magnitude is “>=“ 20% of highest energy
- Intelligence is included in code to count only distinct modes

Oscillations Data Mining Performance

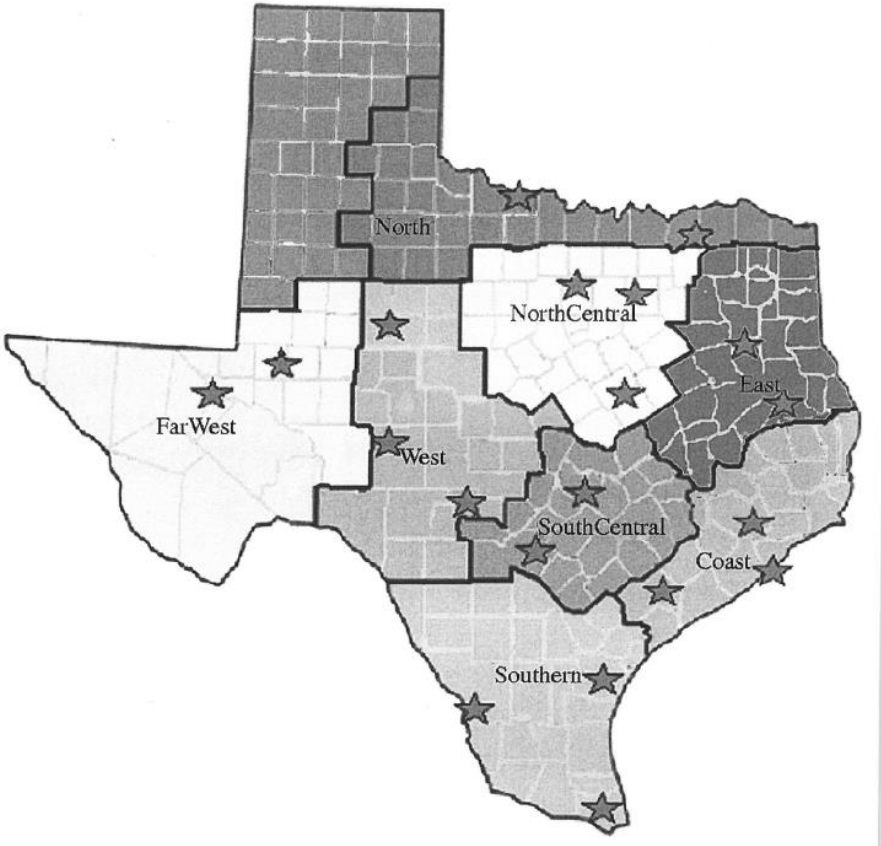
Task	Time
Data Loading (1 minute of data, All PMU signals)	3 sec
Data Filtering Mode Solving Result Exporting	1 sec
Total **(All Frequency Bands)**	**4 sec**
Ideal Example	
1 Hour	4 Min
1 Day	1.6 Hours
1 Week	11.2 Hours
1 Month (31 days)	**2.06 Days**

Oscillation Data Mining - Parallel Job Processing



Regional Wind Data

- **Wind Variables**
  - Wind north = aggregation (north)
  - Wind west = aggregation (far west, west)
  - Wind south = aggregation (south, coastal wind)



Source: ERCOT

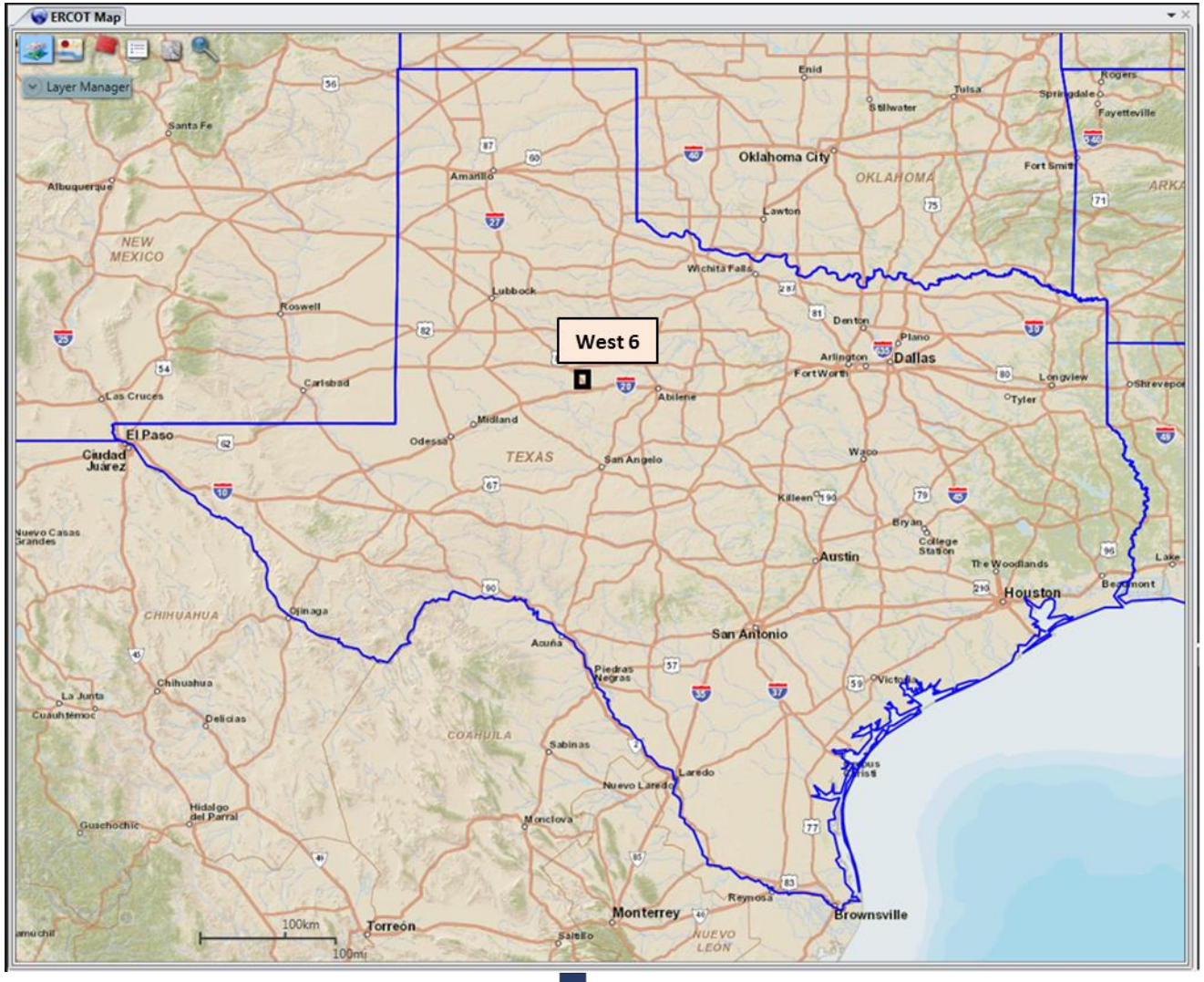
Identified 10 ERCOT Oscillatory Modes

#	Mode (Hz)	2012	2013	2014	Oscillation Type
1	**0.6**	Till March	Absent	Absent	Local
2	**0.9**	Present	Present	Present	Wind Production Related
3	**1.5**	Only in April	Absent	Absent	Control Systems
4	**1.7**	4 Months	Absent	Absent	Control Systems
5	**2.0**	Absent	April	Absent	Control Systems
6	**2.7**	Present	Present	Absent	Wind Production Related
7	**3.2**	4 Months	Absent	Only in Jan	Control Systems
8	**5.0**	Present	Present	Present	Control Systems
9	**5.4**	Present	Present	Present	Control Systems
10	**6.0**	Present	Present	Present	Control Systems

Identified 10 ERCOT Oscillatory Modes

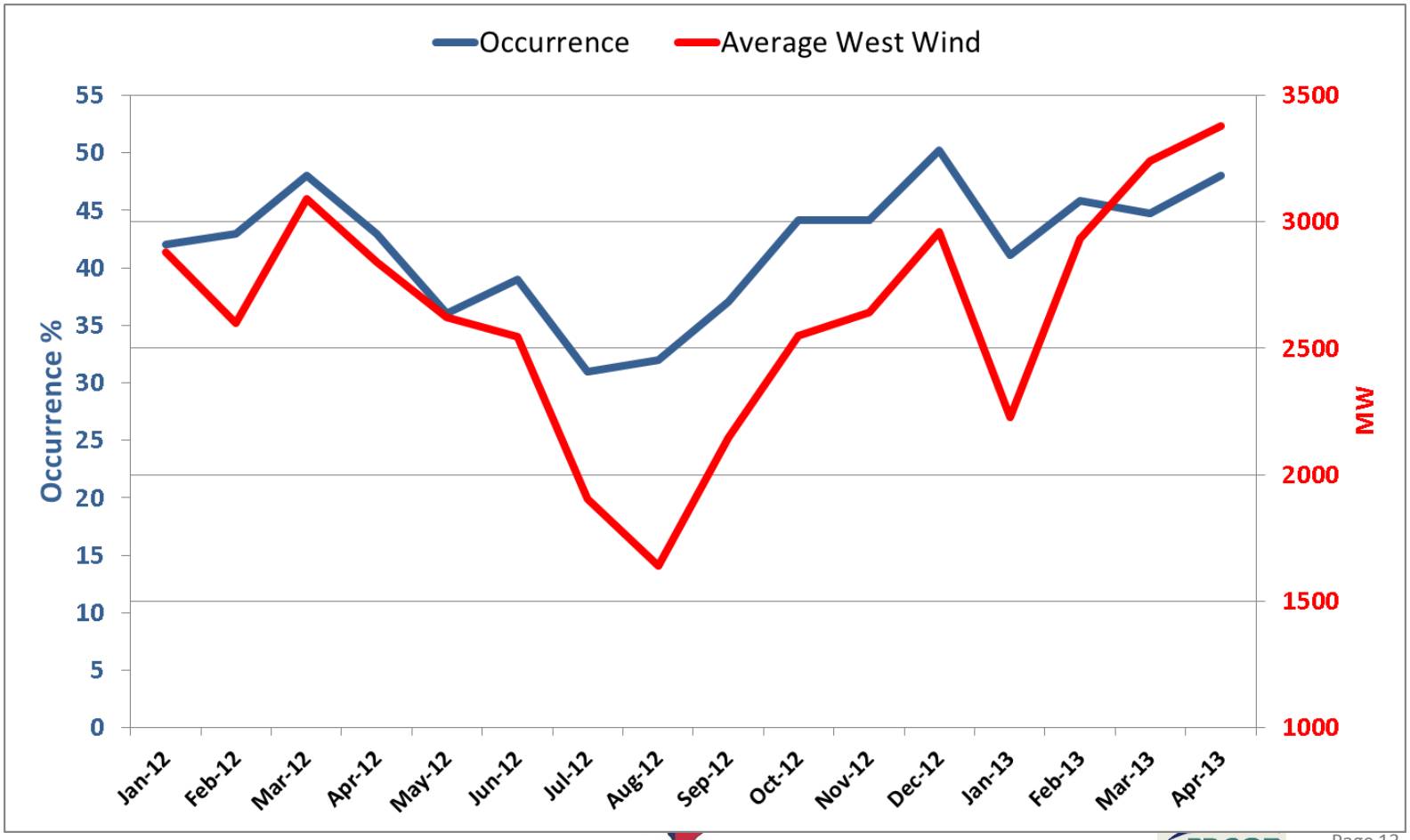
#	Mode (Hz)	Nearest PMU	Related to Wind Production	Highest Energy Level
1	**0.6**	West 10	No	Low Energy & Flat
2	**0.9**	West 6	Yes	High Energy & Tracking Occurrence
3	**1.5**	Coast 3	No	Low Energy
4	**1.7**	FarWest 7	No	High Energy
5	**2.0**	Coast 3	No	Low Energy
6	**2.7**	FarWest 4	Yes	High Energy & Tracking Occurrence
7	**3.2**	West 10	No	High Energy
8	**5.0**	Coast 3	No	Low Energy & Remained Flat
9	**5.4**	West 10, FarWest 4	No	Low Energy & Remained Flat
10	**6.0**	West 10	No	Intermittent High Energy

Mode #2 – 0.9Hz @ West 6



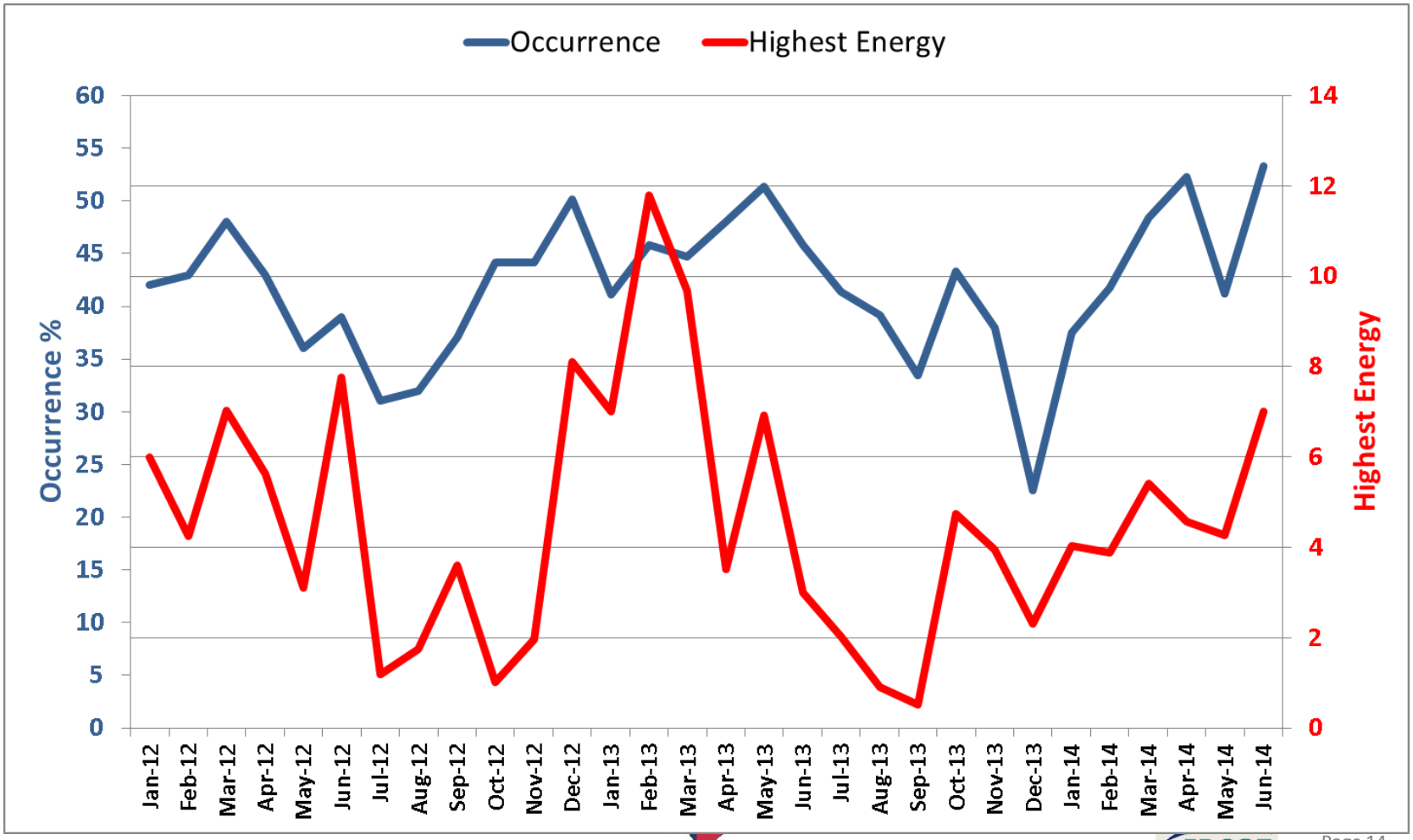
Mode #2 – 0.9 Hz @ West 6

The trend of mode occurrence & average west wind have similar pattern and provides first indication that 0.9 Hz is more likely related to wind production



Mode #2 – 0.9 Hz @ West 6

The peaks & valleys of mode occurrence & highest energy matched very well to provide second indication that 0.9 Hz is more likely related to wind production near West 6



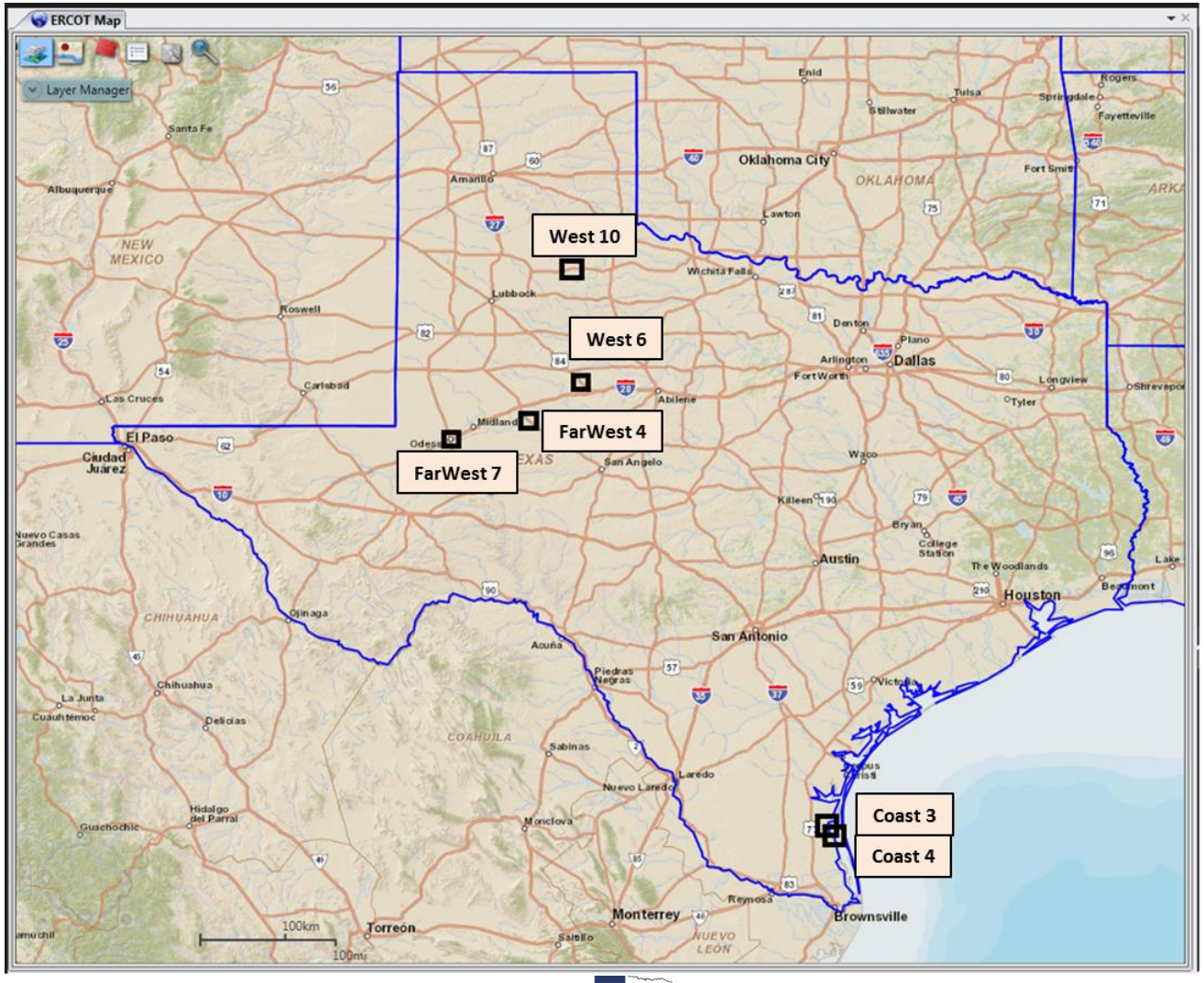
Mode #2 – 0.9 Hz @ West 6

- Source: West 6
- Signal type: current magnitude
- Oscillation type: wind related
- Wind generators nearby: WestGen1, WestGen2, WestGen3, WestGen4
- Occurrence: appeared every month in all three years
  - Minimum occurrence in Dec 2013 and appeared for 22% of time
  - Maximum occurrence in June 2014 and appeared for 53% of time
  - Average occurrence in all three years is about 42% of time during the month

Mode #2 – 0.9 Hz @ West 6

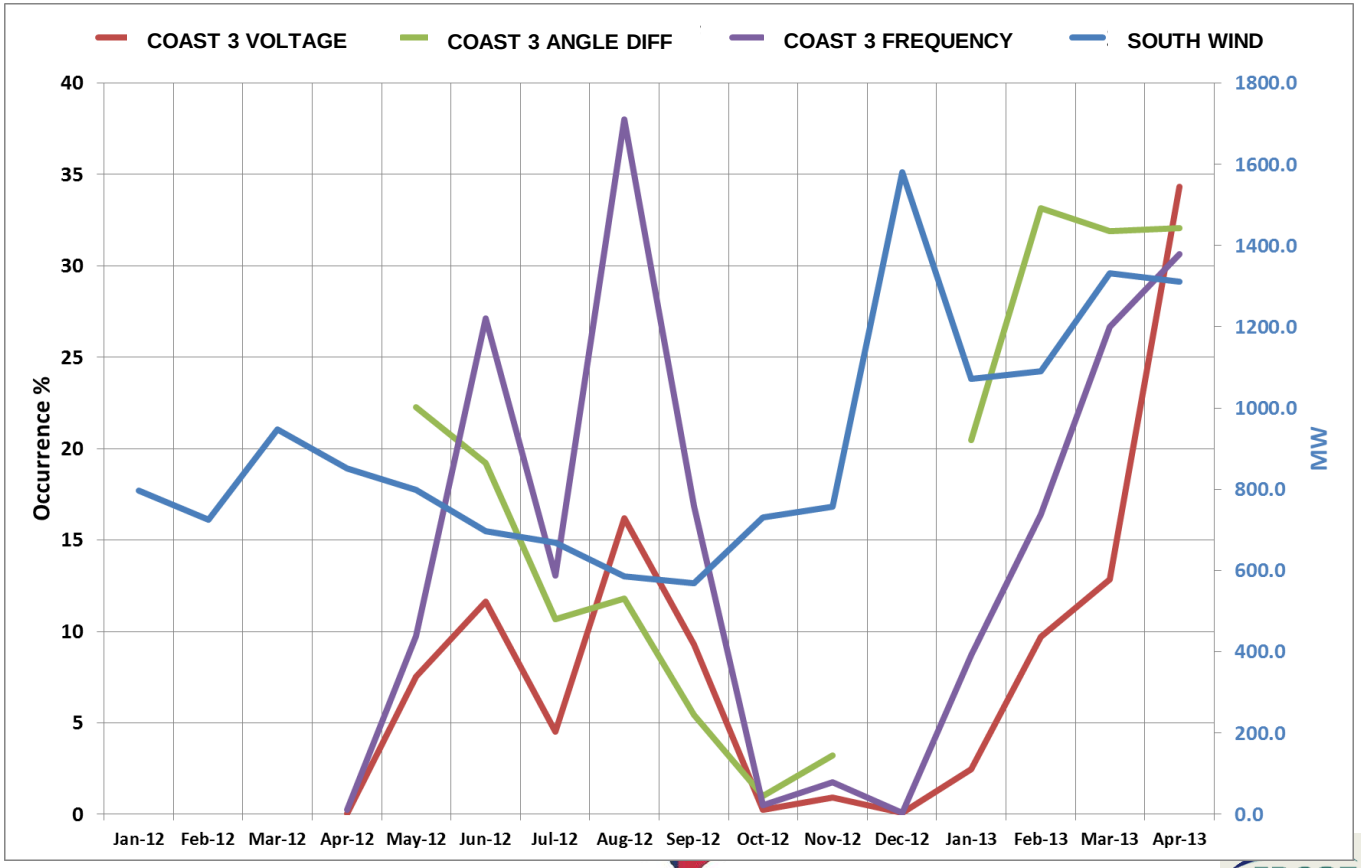
- Highest energy: Represents the highest energy of the mode during each month
  - Maximum highest energy in Feb 2013 and energy was 12
  - Minimum highest energy in Sep 2013 and energy was 0.5
- **ERCOT should monitor in real time with the following configuration**
  - West 6 current magnitude
  - Minimum frequency = 0.85 Hz
  - Maximum frequency = 1.2 Hz
  - Minimum energy = 2
  - Damping = 8%

Mode #8 – 5.0 Hz @ 6 Locations



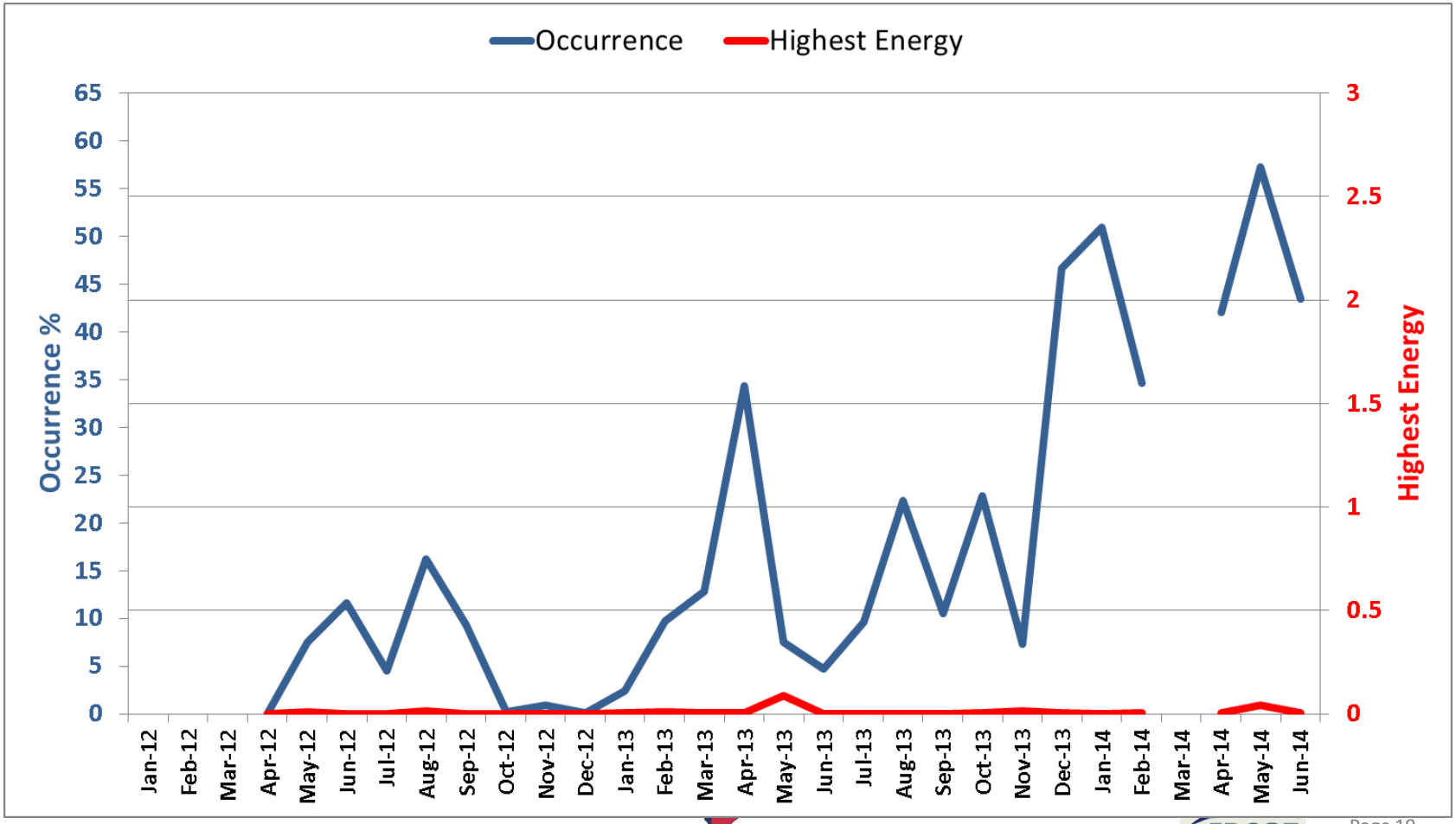
Mode #8 – 5.0 Hz (May Not be Wind Related)

- Mode occurrence @ Coast 3 does not follow south wind pattern & may need local wind production data to confirm any relationship
- But these oscillations are observed more strongly near wind generators



Mode #8 – 5.0 Hz (Local Control Systems)

- The energy of the mode remained fairly flat at low levels (< 0.01) indicating no relationship with changing wind production
- These oscillations are more likely driven by control systems at the local wind generators



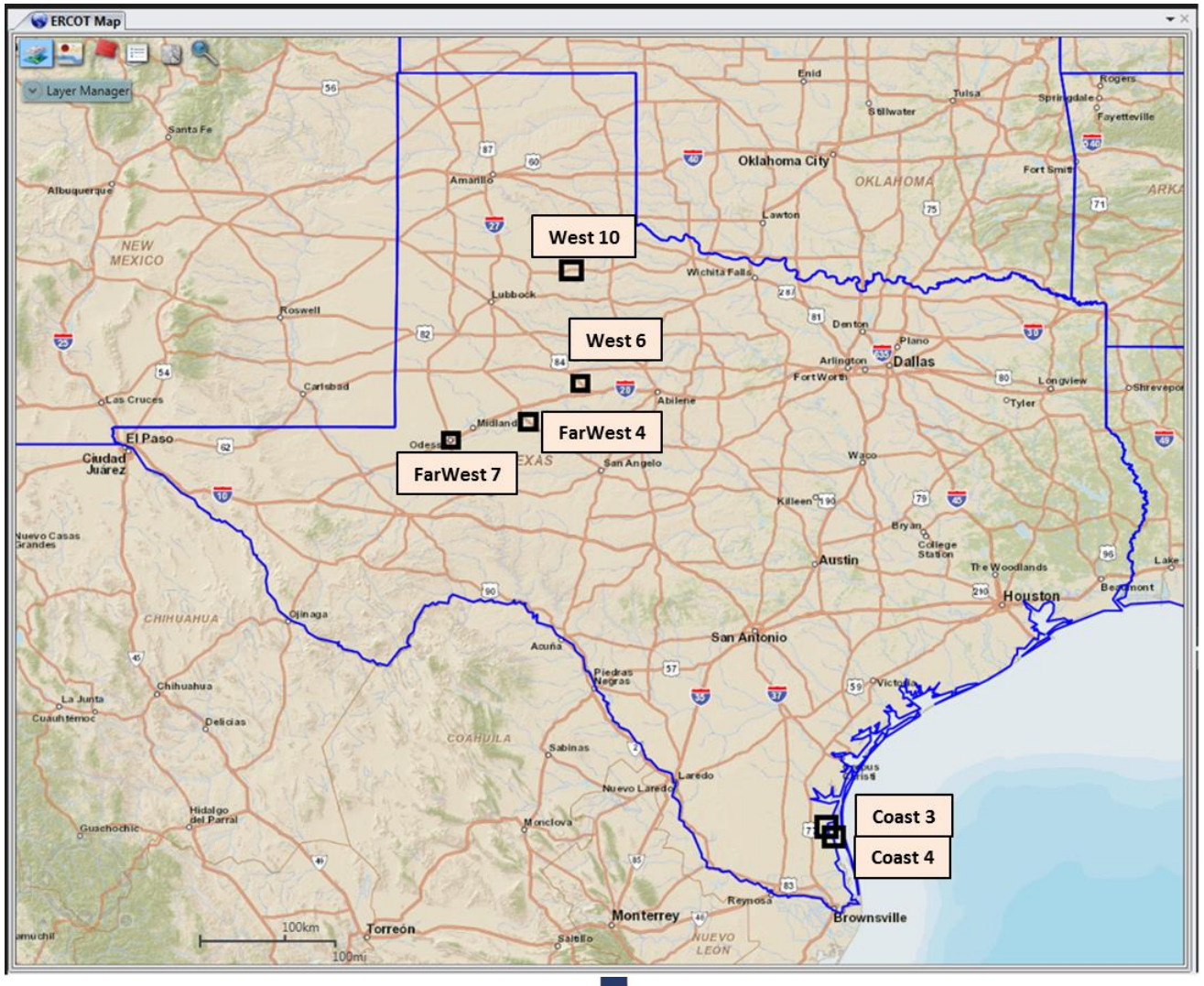
Mode #8 – 5.0 Hz @ Coast 3

- Source: Valley (Coast 3 & Coast 4 – most occurrence)
- Signal type: voltage magnitude
- Oscillation type: wind generator control system
- Generators nearby: CoastGen3 & CoastGen4
- Occurrence: appeared every month in all three years, except first 3 months of 2012 and in March 2013
  - Minimum occurrence in Dec 2012 and appeared for 0.1% of time
  - Maximum occurrence in May 2014 and appeared for 57% of time

Mode #8 – 5.0 Hz @ Coast 3

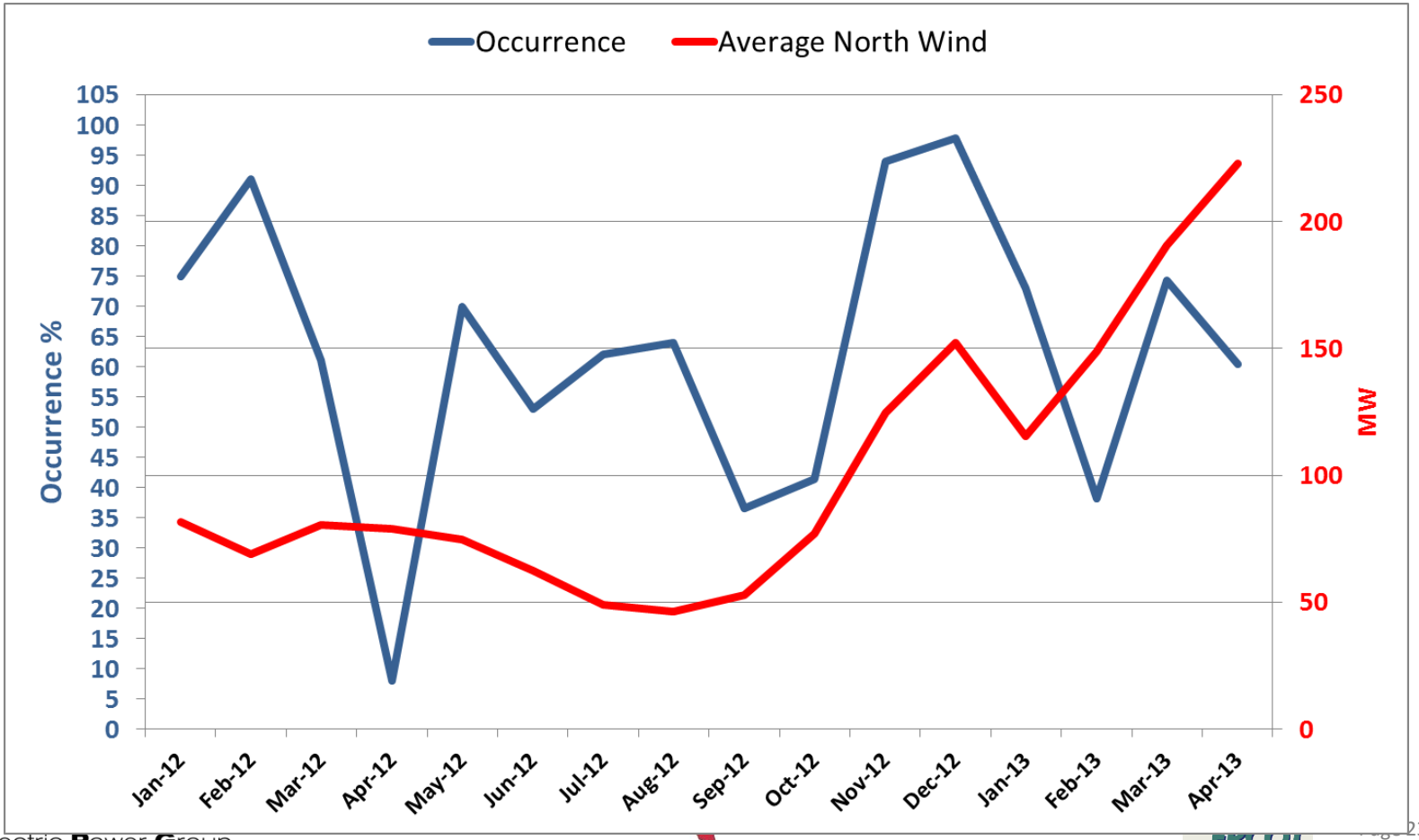
- Highest energy: represents the highest energy of the mode during each month (no significant event with high energy)
  - Maximum highest energy in May 2013 and energy was 0.09 (low)
  - Minimum highest energy in Dec 2012 and energy was 0.00015 (very low)
- **ERCOT should review 5.0 Hz oscillation with wind owners for possible mitigation, and determine root cause to evaluate need for additional monitoring**

Mode #9 – 5.4 Hz @ 6 Locations



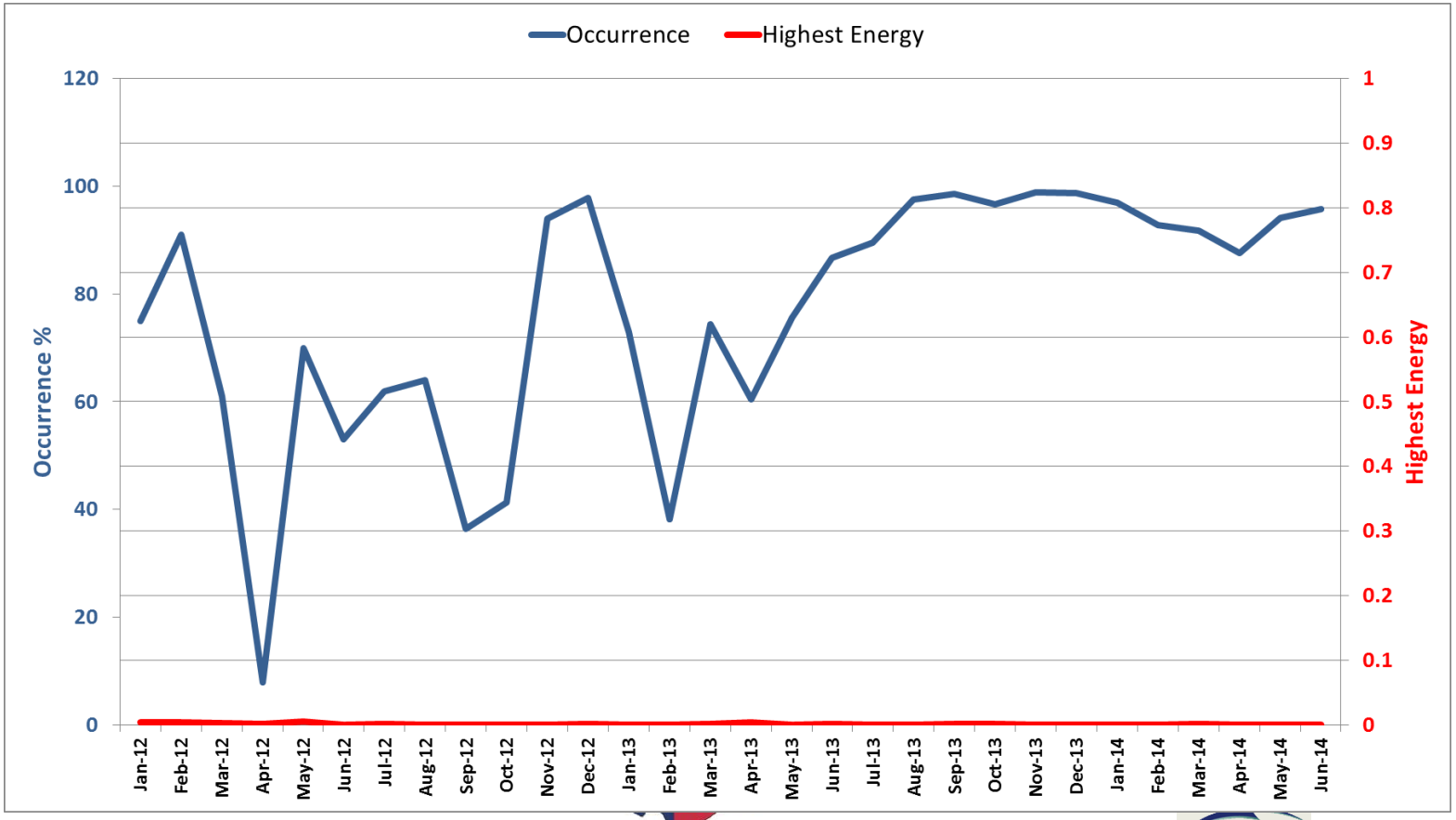
Mode #9 – 5.4 Hz @ West 10

- Mode occurrence @ West 10 does not follow north wind pattern & may need local wind production data to confirm any relationship
- But these oscillations are observed more strongly near wind generators



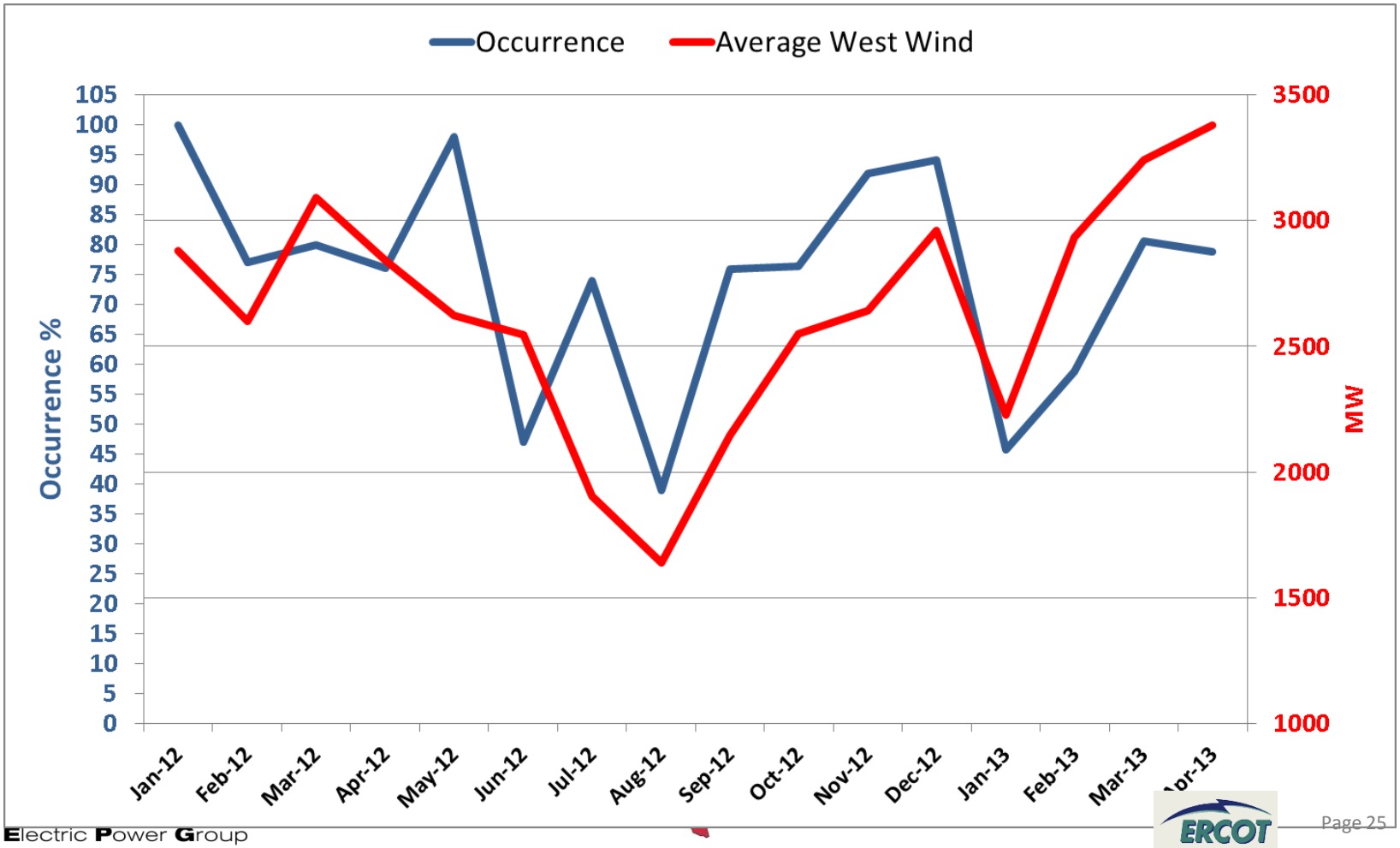
Mode #9 – 5.4 Hz @ West 10 (Local Control Systems)

- The energy of the mode remained fairly flat at low levels (< 0.01) indicating no relationship with changing wind production
- But these oscillations are more likely driven by control systems at the local wind generators



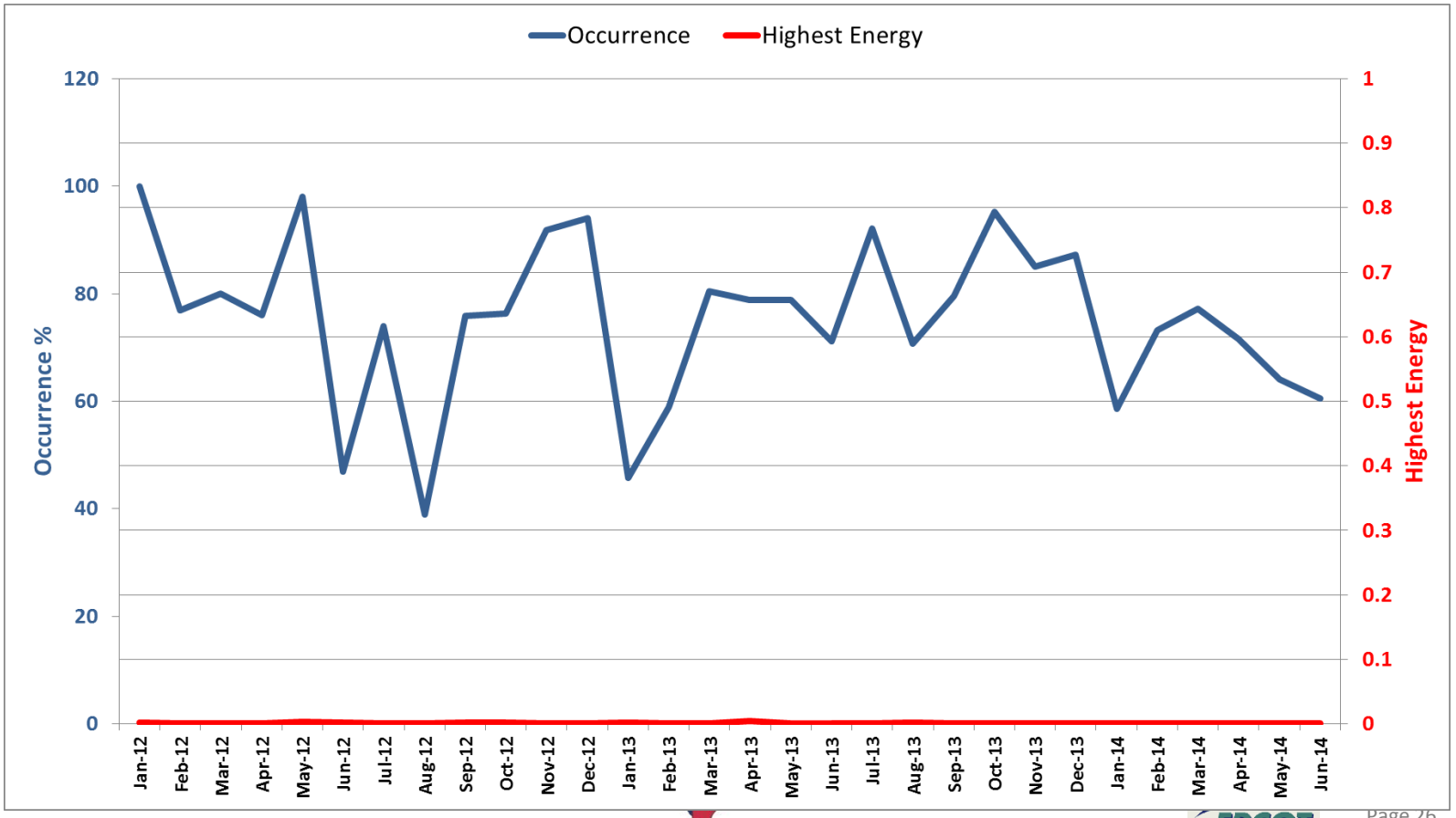
Mode #9 – 5.4 Hz @ FarWest 4

The trend of mode occurrence and average west wind have similar pattern, and provides first indication that 5.4 Hz may be related to wind production

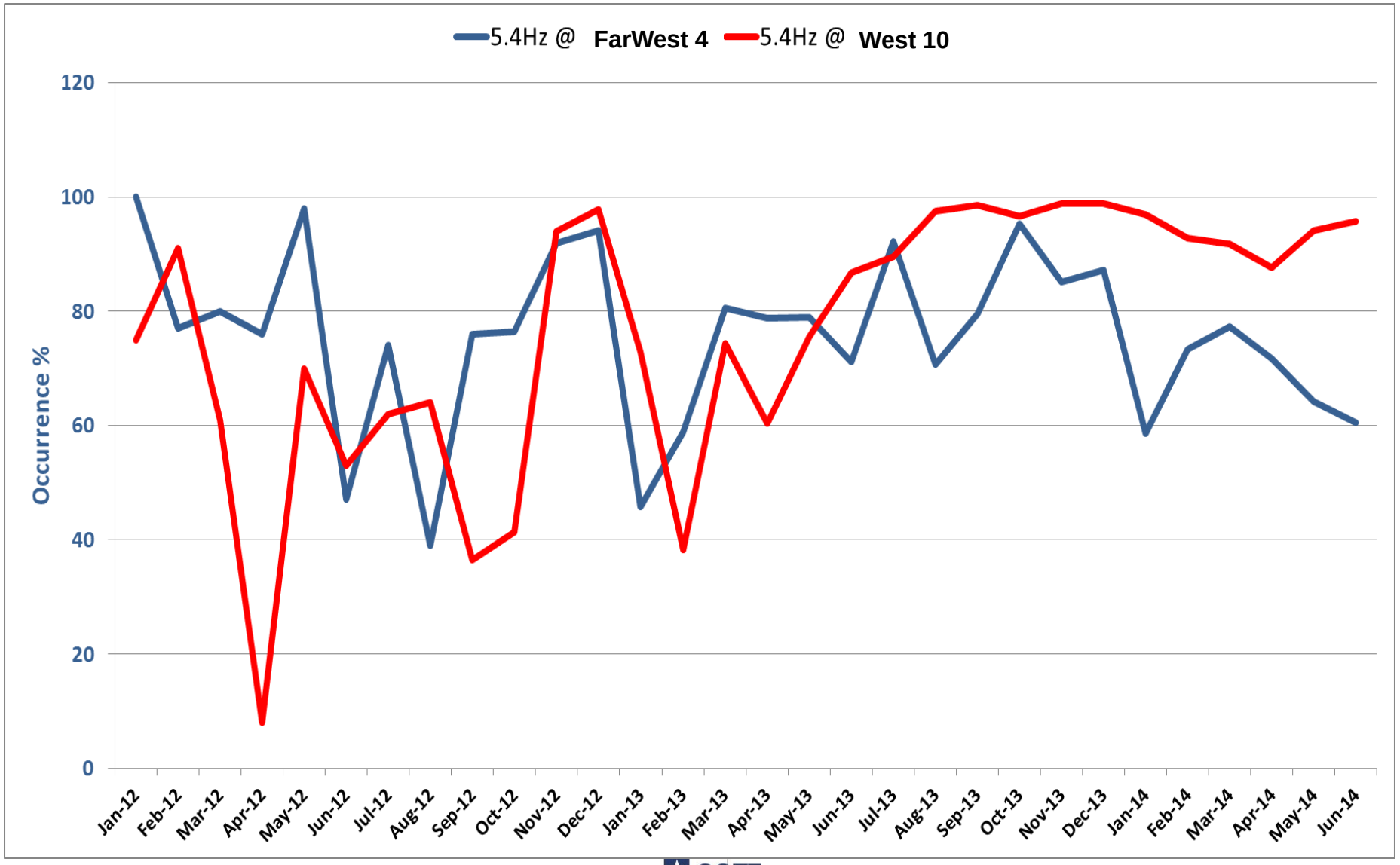


Mode #9 – 5.4 Hz @ FarWest 4 (Local Control Systems)

- The energy of the mode remained fairly flat at low levels (< 0.01) indicating no relationship with changing wind production
- But these oscillations are more likely driven by control systems at the local wind generators



5.4 Hz Mode Pattern – FarWest 4 Vs. West 10



Mode #9 – 5.4 Hz @ West Texas & Panhandle

- Source: Panhandle (West 10), West (FarWest 4, FarWest 7, West 6) – most occurrence
- PMU: West 10 and FarWest 4
  - West 10 was selected to monitor mode in the Panhandle region
  - FarWest 4 was selected since it had the highest mode occurrence among FarWest 7 and West 6 in west Texas
- Signal type: voltage magnitude
  - Voltage magnitude was selected since it had the highest occurrence in each PMU
- Oscillation type: wind generator control system
- Wind generators nearby: WestGen10 and FarWestGen4

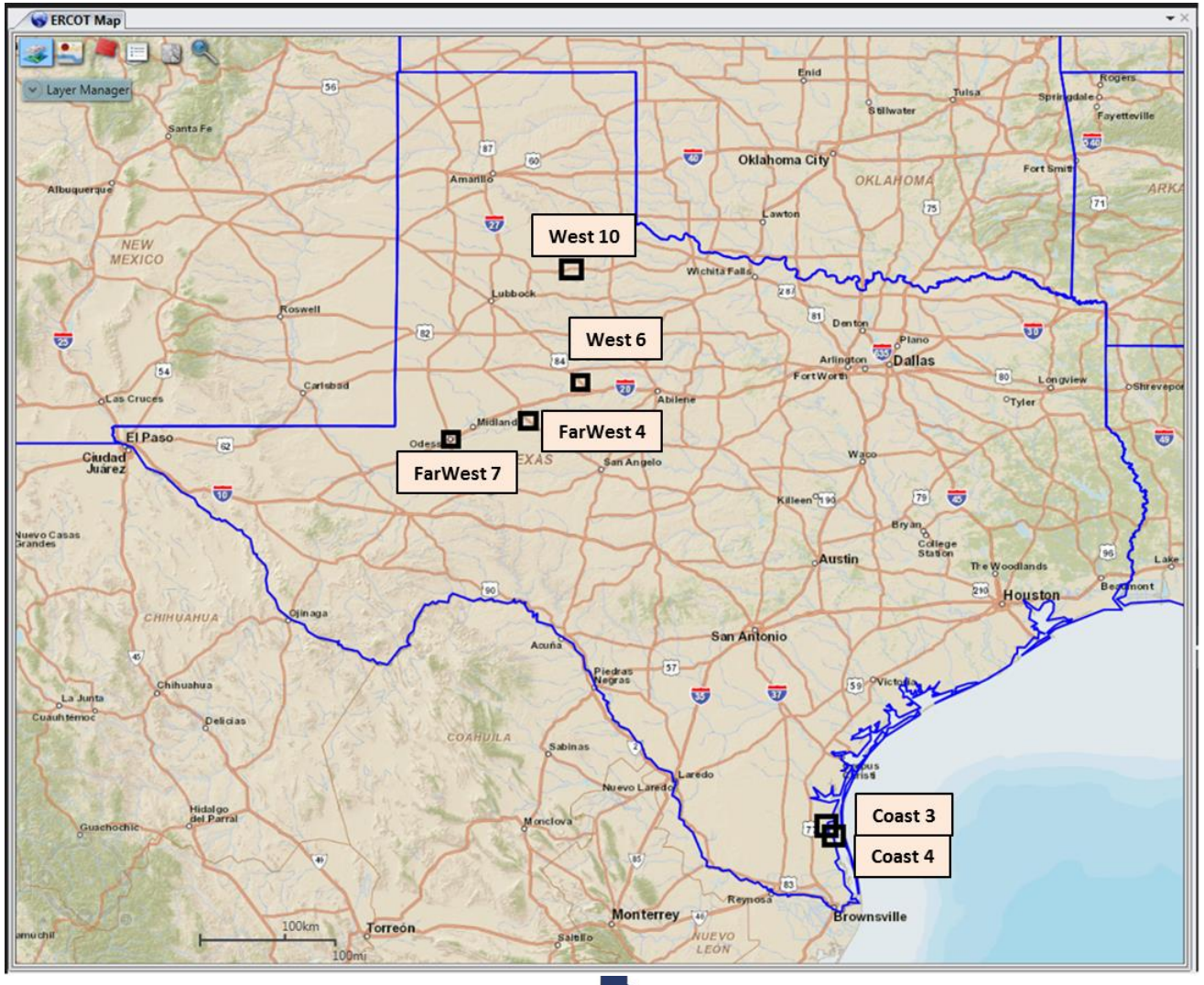
Mode #9 – 5.4 Hz @ West 10

- Occurrence: appeared every month in all three years
  - Minimum occurrence in April 2012, and appeared for 8% of time (2.5 Days)
  - Maximum occurrence in Sep, Nov, and Dec 2013, and appeared for 99% of time (all the time)
- **ERCOT should review 5.4 Hz oscillation with wind owners for possible mitigation, and determine the root cause to evaluate need for additional monitoring**

Mode #9 – 5.4 Hz @ FarWest 4

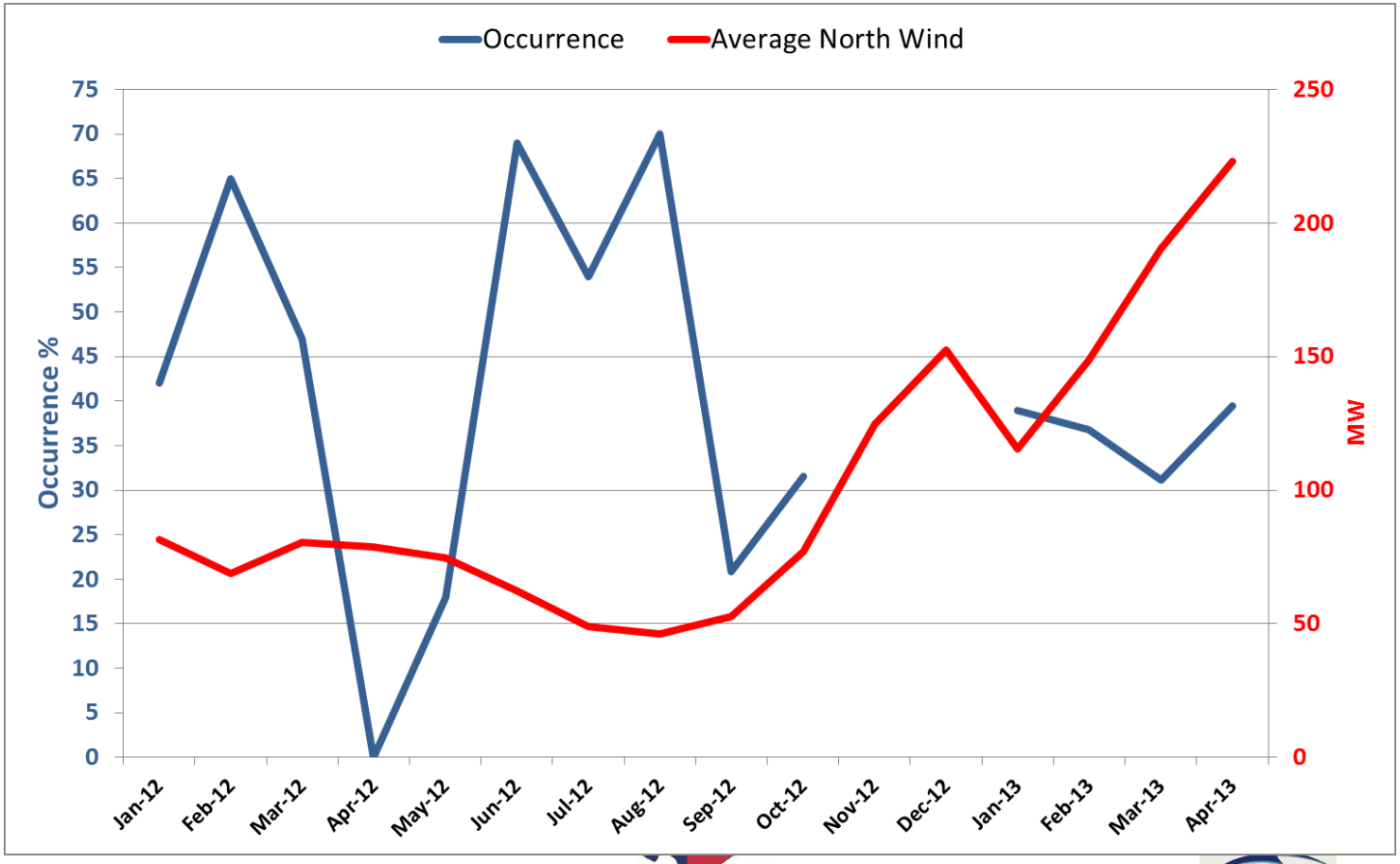
- Occurrence: appeared every month in all three years
  - Minimum occurrence in August 2012, and appeared for 39% of time (12 Days)
  - Maximum occurrence in Jan 2012, and appeared all the time
- **ERCOT should review 5.4 Hz oscillation with wind owners for possible mitigation, and determine the root cause to evaluate need for additional monitoring**

Mode #10 – 6.0 Hz @ 6 Locations



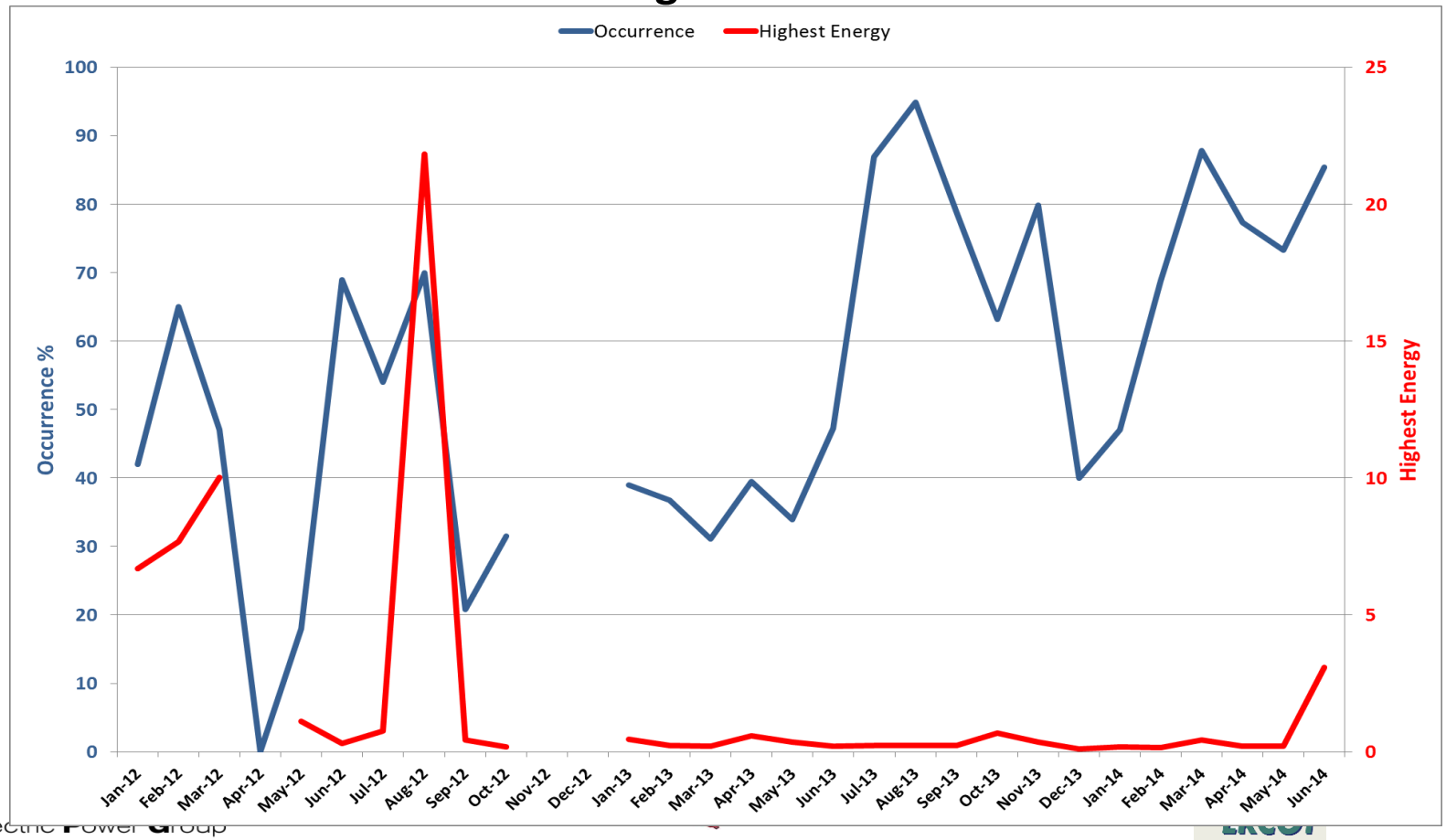
Mode #10 – 6.0 Hz @ West 10

- Mode occurrence @ West 10 does not follow north wind pattern & may need local wind production data to confirm any relationship
- But these oscillations are observed more strongly near wind generators



Mode #10 – 6.0 Hz @ West 10 (Local Control Systems)

- The energy of the mode remained fairly flat at low levels (< 0.01) except in January-March & August 2012, indicating oscillations driven by control systems at the local wind generators can also reach high energy levels and needs additional monitoring



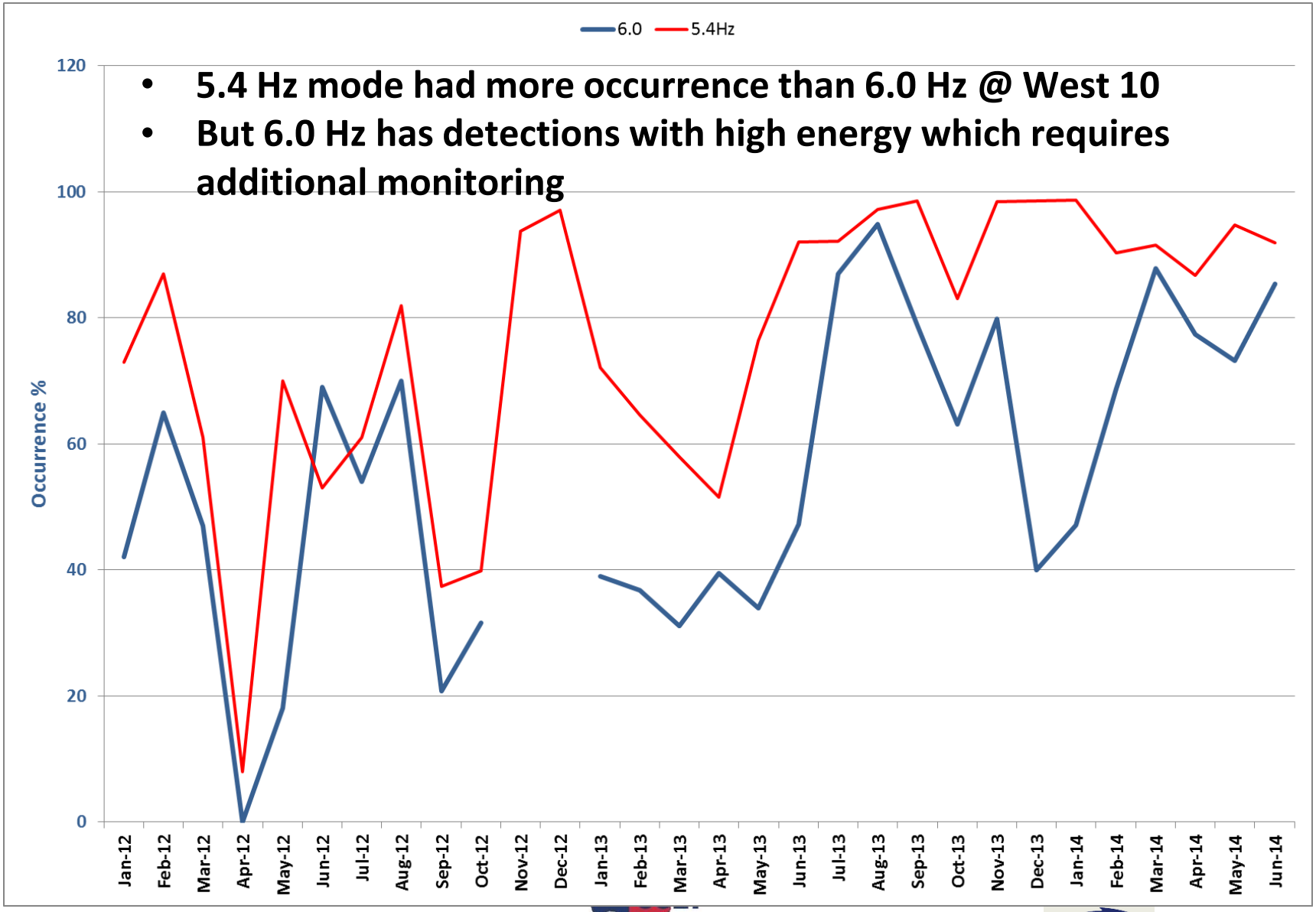
Mode #10 – 6.0 Hz @ West Texas & Panhandle

- Source: Panhandle (West 10) – most occurrence
- PMU: West 10
  - West 10 was selected to monitor mode in the Panhandle region since it had the most & consistent mode occurrence
- Signal type: current magnitude
  - Current magnitude was selected since it had the highest occurrence among other signal types
- Oscillation type: wind generator control systems
- Generators nearby: WestGen10

Mode #10 – 6.0 Hz @ West 10

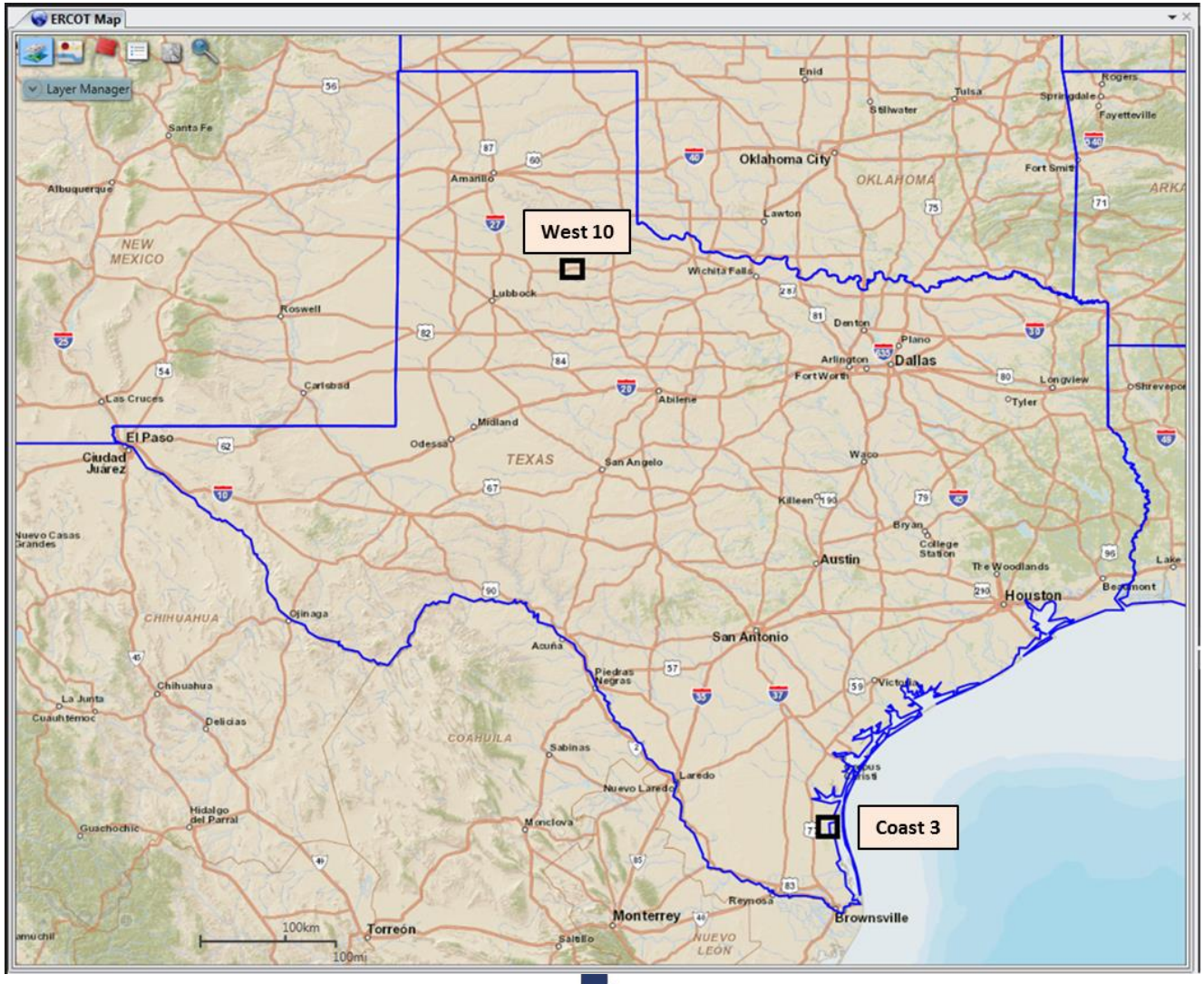
- Occurrence: appeared every month in all three years except April 2012
  - Minimum occurrence in May 2012, and appeared for 18% of time
  - Maximum occurrence in Aug 2013, and appeared 95% of time
- **ERCOT should review 6.0 Hz oscillation with wind owners for possible mitigation and also monitor with following configuration**
  - West 10 current magnitude
  - Minimum frequency = 5.5 Hz
  - Maximum frequency = 6.5 Hz
  - Minimum energy = 5
  - Damping = 8%

West 10 – 5.4 Hz vs. 6.0 Hz



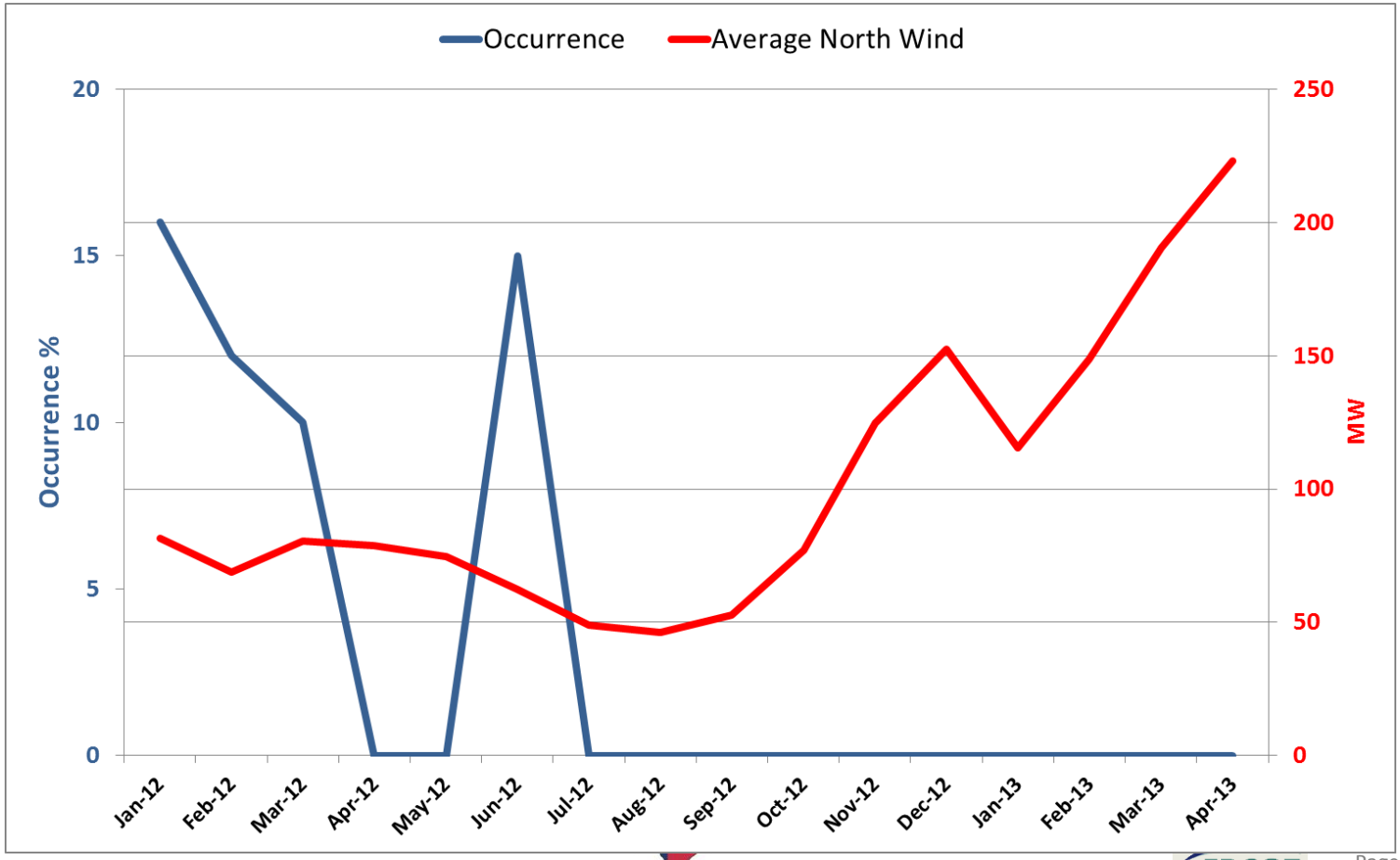
- 5.4 Hz mode had more occurrence than 6.0 Hz @ West 10
- But 6.0 Hz has detections with high energy which requires additional monitoring

Mode #7 – 3.2 Hz @ West 10



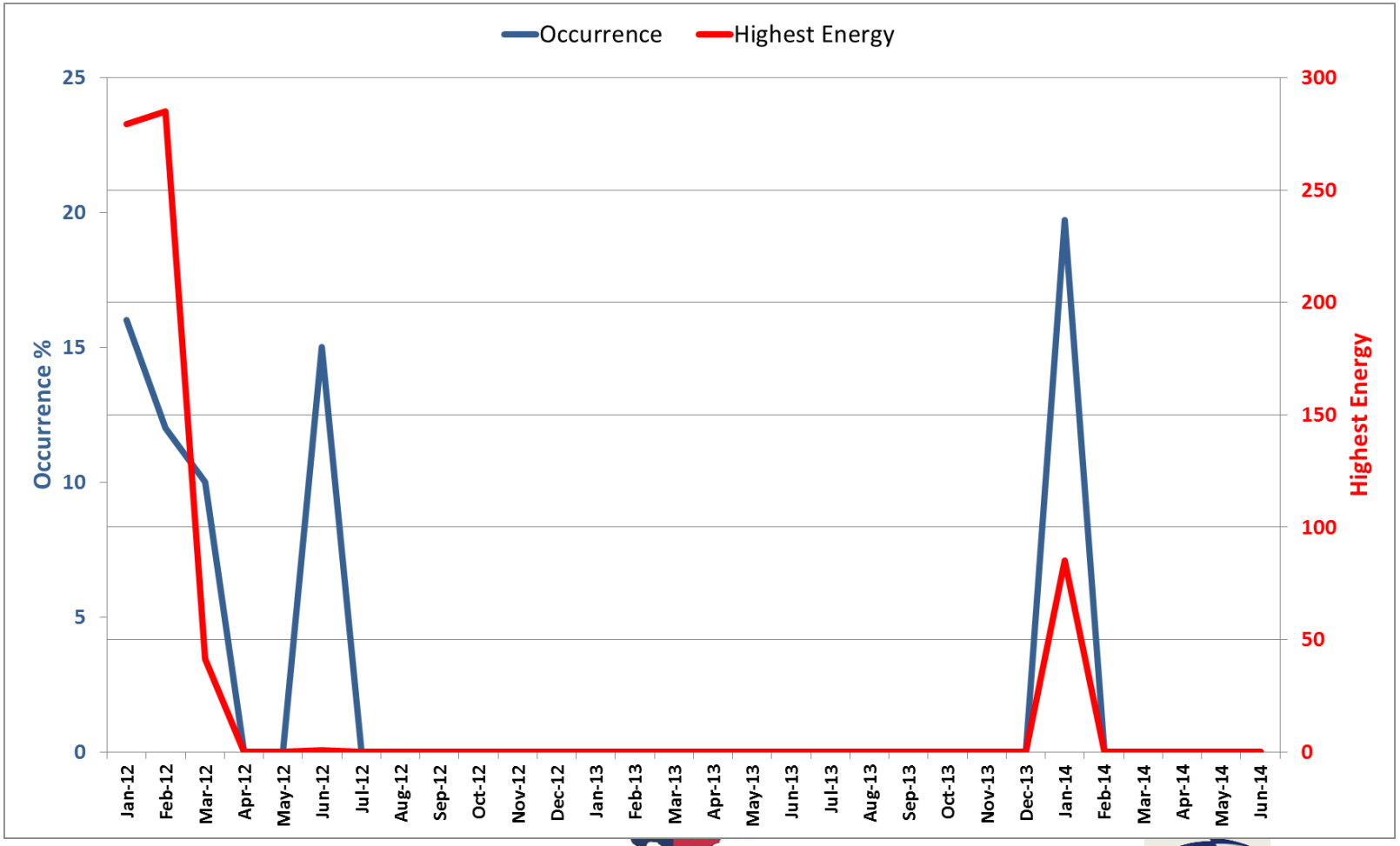
Mode #7 – 3.2 Hz @ West 10

- Mode occurrence @ West 10 does not follow north wind pattern & does not appear to be consistent as 5.4 Hz or 6.0Hz, rather intermittent
- But these oscillations are observed more strongly near wind generators and appear to be driven by "settings change in the control systems"



Mode #7 – 3.2 Hz @ West 10

- **The occurrence of 3.2 Hz mode appears to be intermittent, and energy is high during the occurrence. Would require additional monitoring to detect occurrence of same mode at West 10**



Mode #7 – 3.2 Hz @ West 10

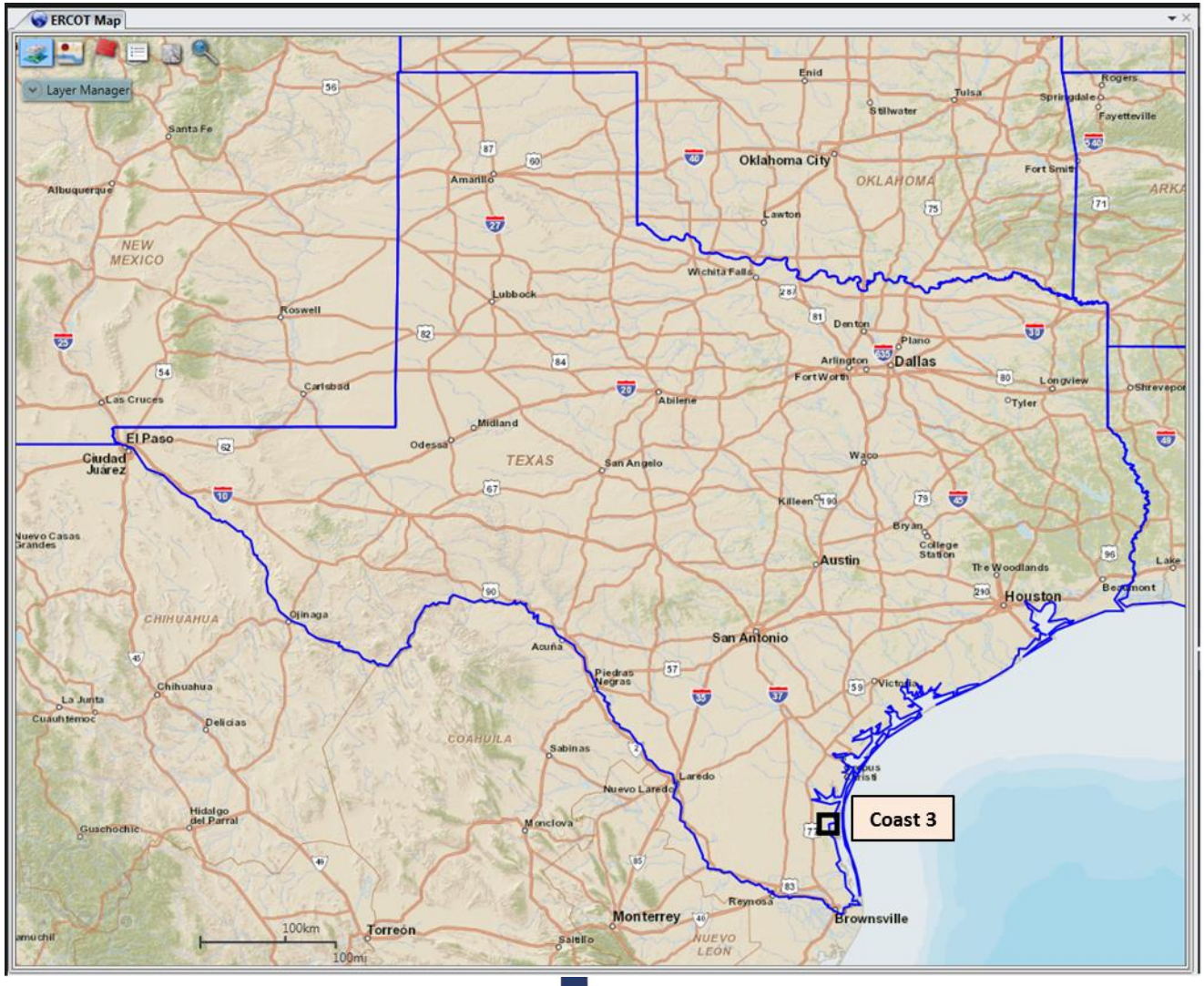
- Source: West 10
- Signal type: current magnitude
- Oscillation type: wind generator control systems setting change
- Generators nearby: WestGen10
- Occurrence:
  - Appeared in first 3 months & June of 2012, Jan of 2014
  - Minimum occurrence in Mar 2013, and appeared for 10% of time
  - Maximum occurrence in Jan 2014, and appeared for 20% of time

Mode #7 – 3.2 Hz @ West 10

- The mode 3.2 Hz is driven by control systems settings change and needs additional monitoring at West 10

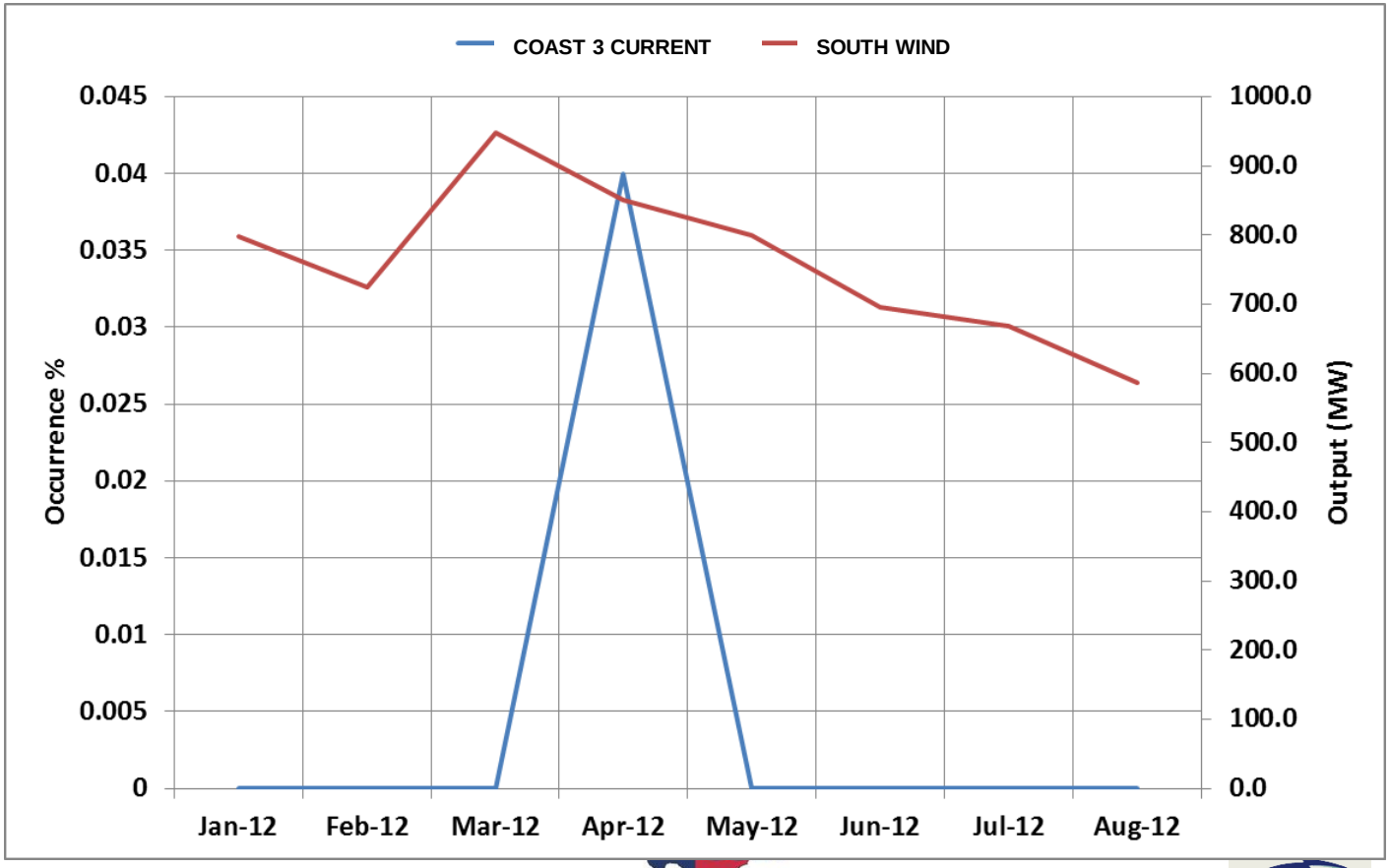
- **ERCOT should do additional monitoring of the mode with the following configuration**
  - Signal: West 10 current magnitude
  - Minimum frequency = 2.6 Hz
  - Maximum frequency = 3.8 Hz
  - Minimum energy = 50
  - Damping = 8%

Mode #3 – 1.5 Hz @ Coast 3



Mode #3 – 1.5 Hz @ Coast 3

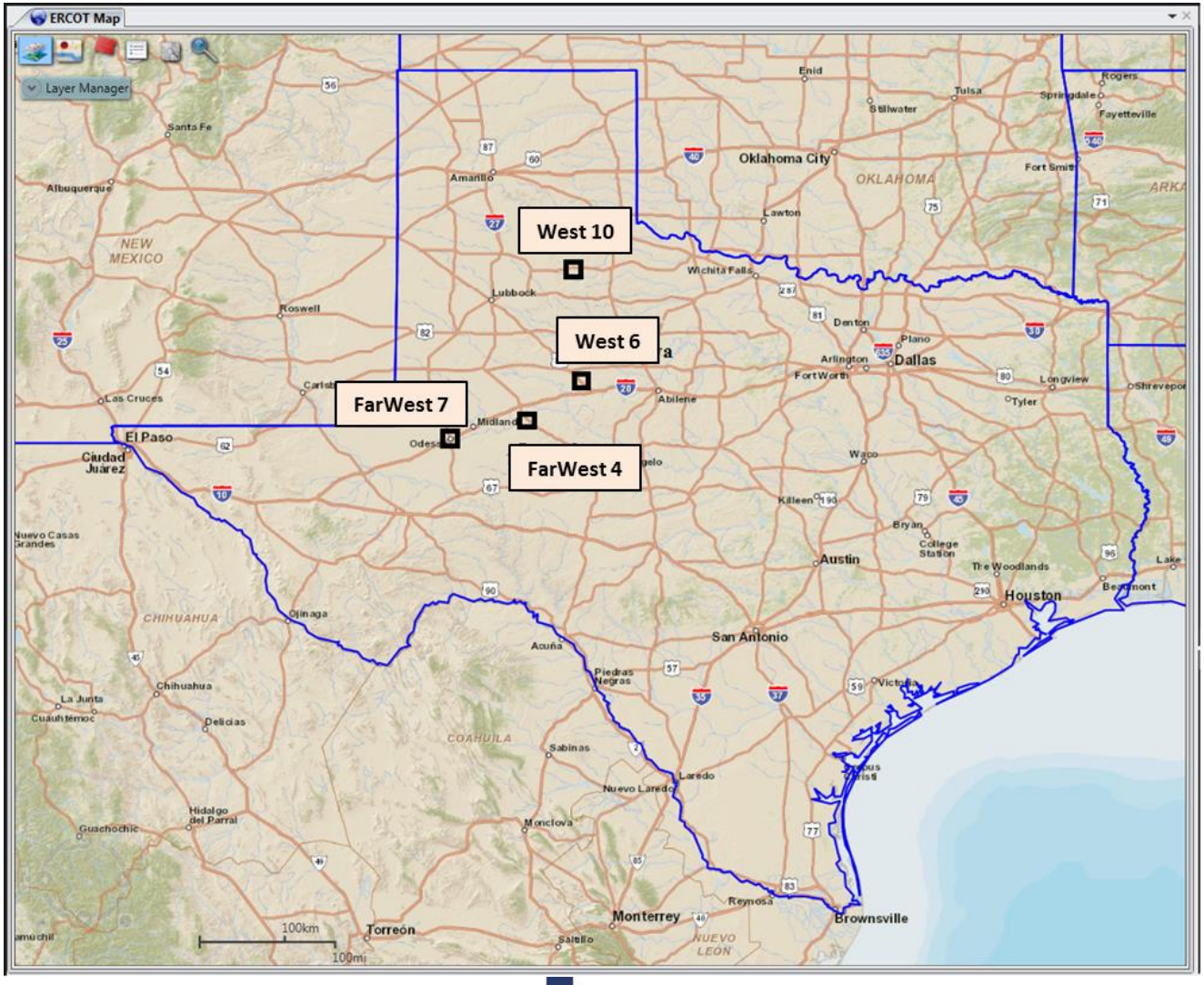
- Mode occurrence @ Coast 3 does not follow south wind pattern & does not appear to be consistent as 5.4 Hz or 6.0 Hz, rather occurred once
- But these oscillations are observed more strongly near wind generators, and appear to be driven by “settings change in the control systems”



Mode #3 – 1.5 Hz @ Coast 3

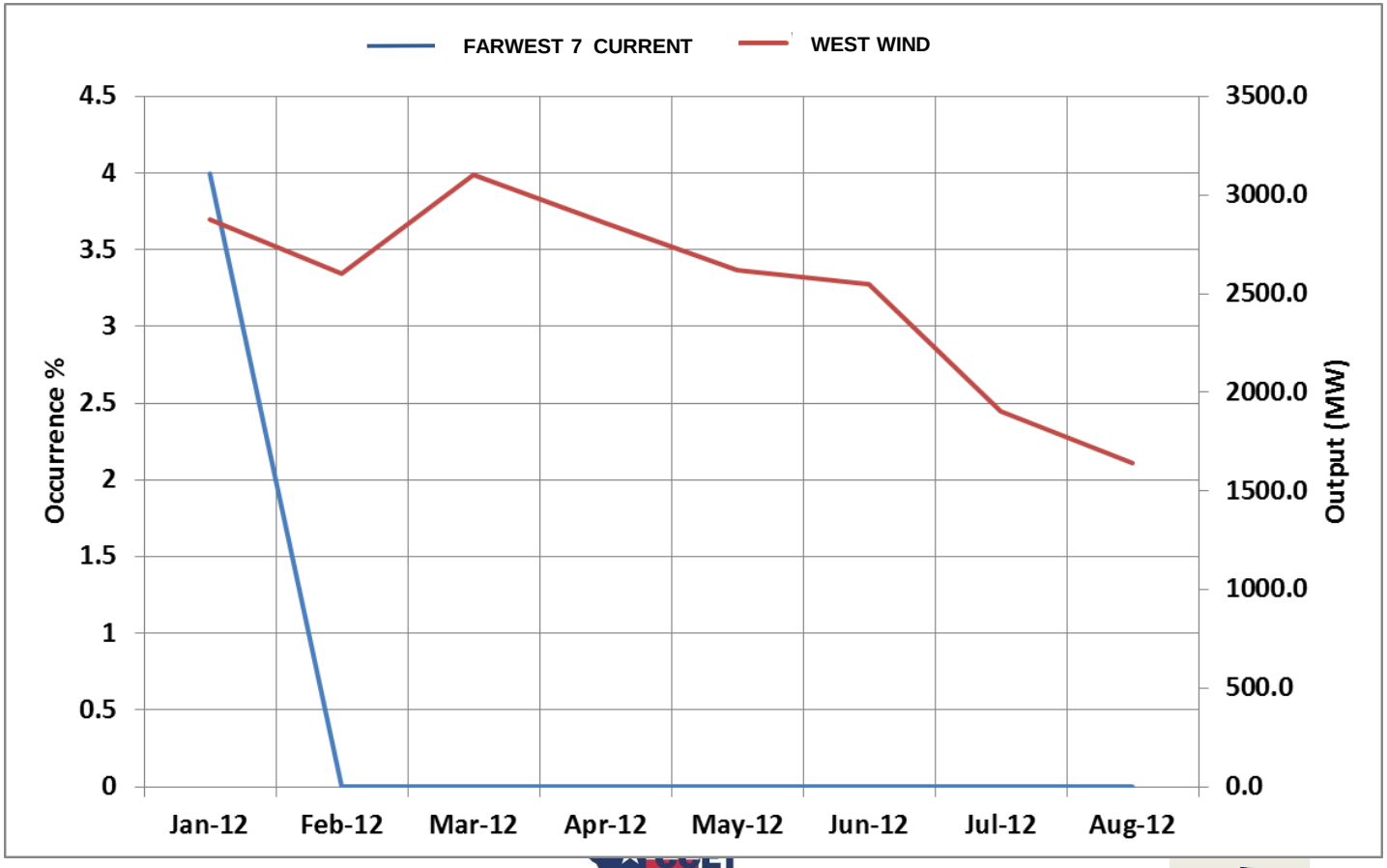
- Source: Valley (Coast 3)
- Oscillation type: wind generator control systems setting change
- Wind generators nearby: CoastGen3 & CoastGen4
- Occurrence:
  - Appeared only in April 2012 for 0.04% of time
- Energy – within the period of occurrence
  - Highest energy was about 0.02
- Occurred for a short period of time with low energy

Mode #4 – 1.7 Hz @ 4 Locations



Mode #4 – 1.7 Hz Mode Occurrence

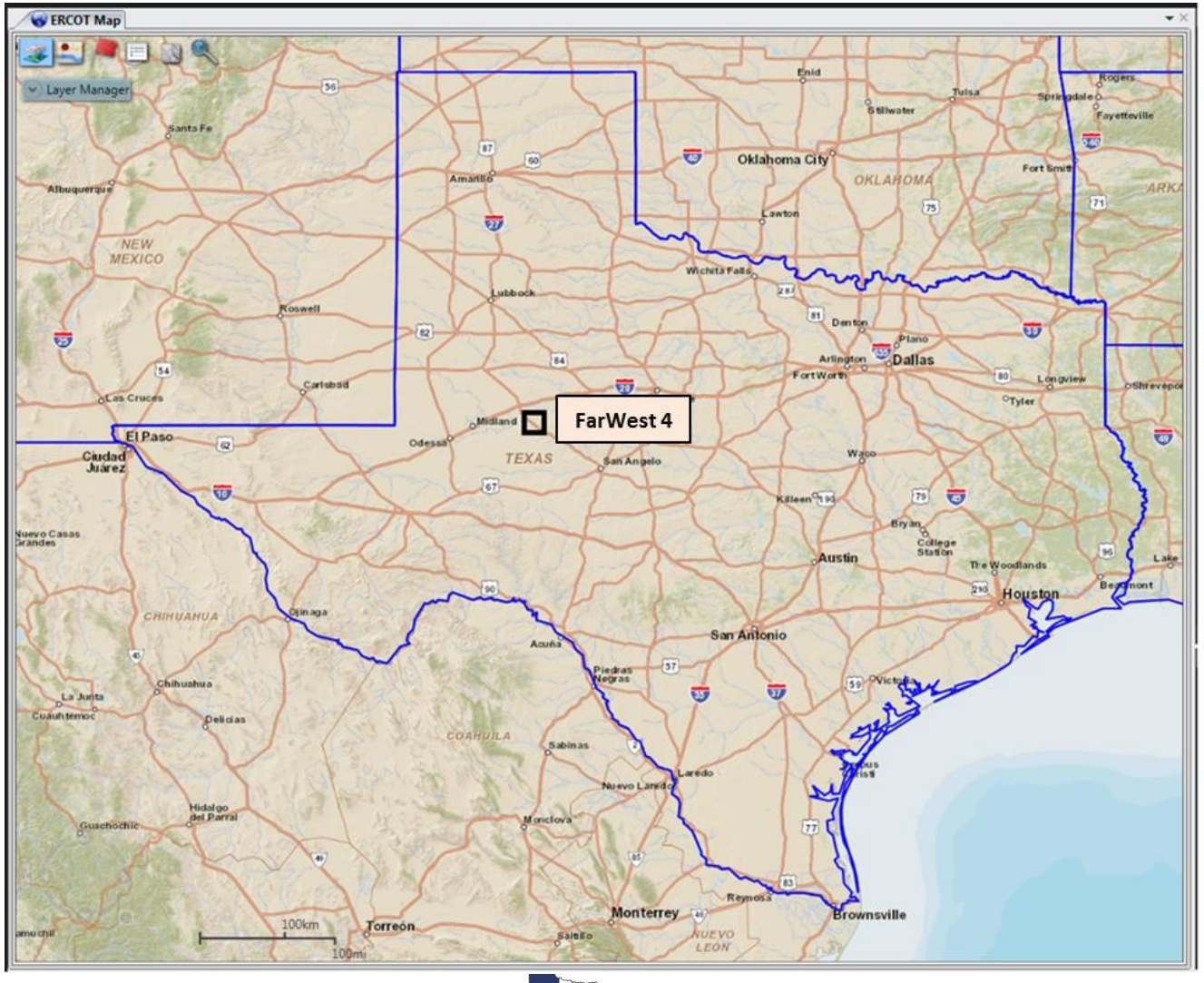
- Mode occurrence @ FarWest 7 does not follow west wind pattern & does not appear to be consistent as 5.4 Hz or 6.0 Hz, rather occurred once
- But these oscillations were observed more strongly near combined cycle unit with total capacity of 1,135 MW (6 Units)



Mode #4 – 1.7 Hz @ FarWest 7

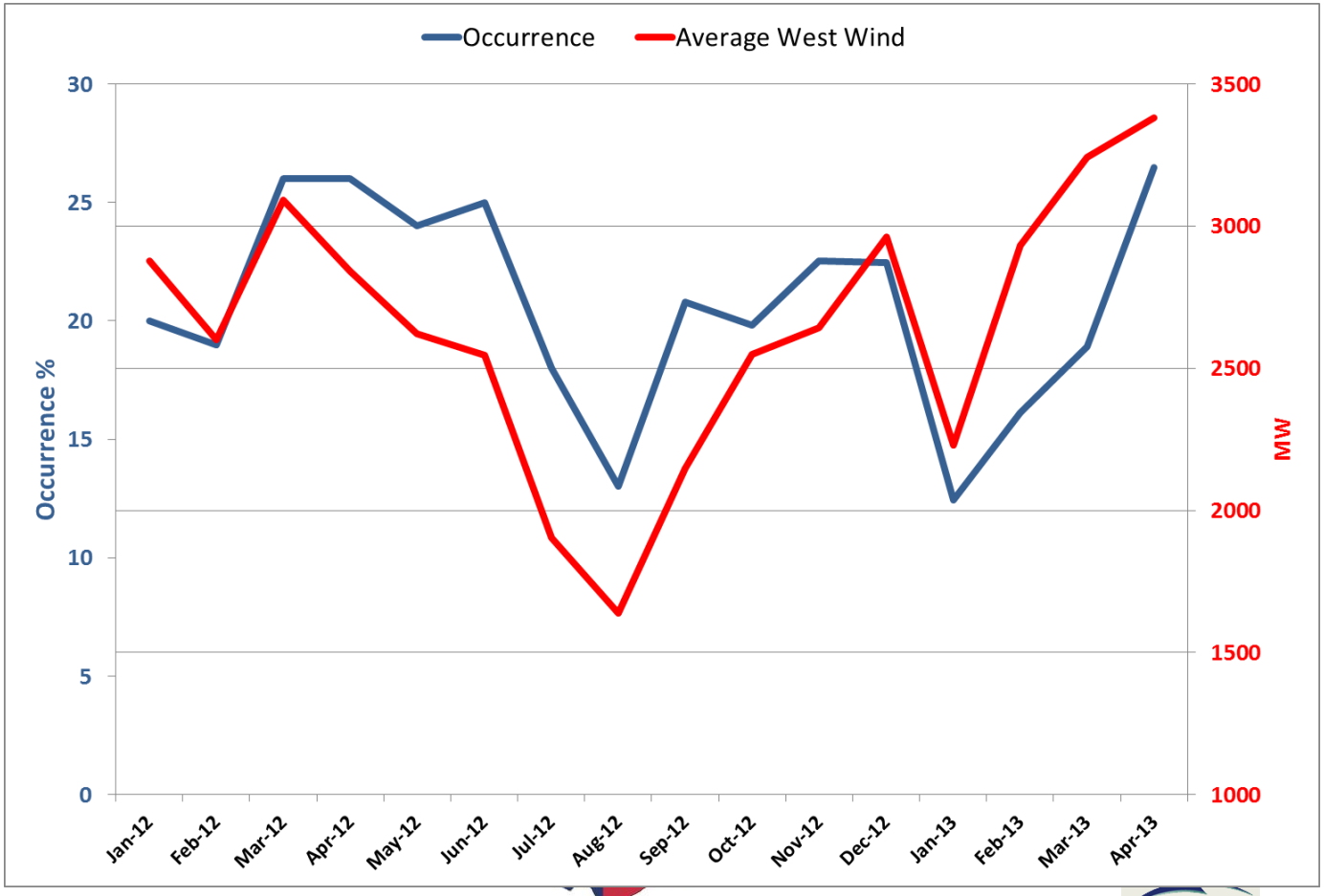
- Source: west Texas (FarWest 7)
- Oscillation type: local
- Other generators nearby: FarWestGen7 & FarWestGen8
- Occurrence:
  - Appeared only in Jan of 2012
- Highest energy – within the period of occurrence
  - Highest value was about 36
- **Appears to be a local issue & ERCOT needs to review the appearance of the mode with plant owners and determine the root cause to evaluate the need for additional monitoring**

Mode #6 – 2.7 Hz @ FarWest 4

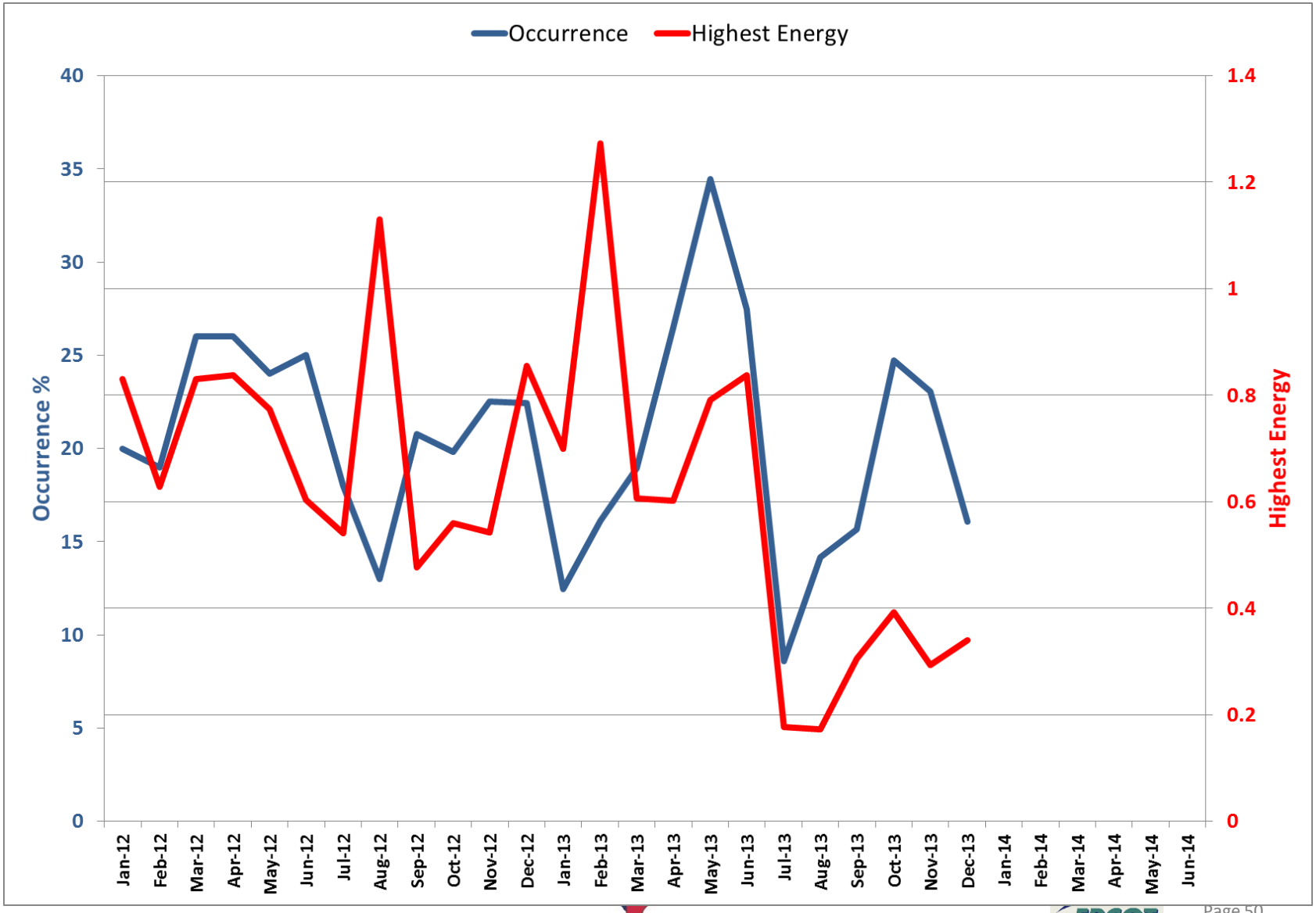


Mode #6 – 2.7 Hz @ FarWest 4

The trend of mode occurrence & average west wind have similar pattern, and provides first indication that 2.7 Hz is more likely related to wind production



Mode #6 – 2.7 Hz @ FarWest 4



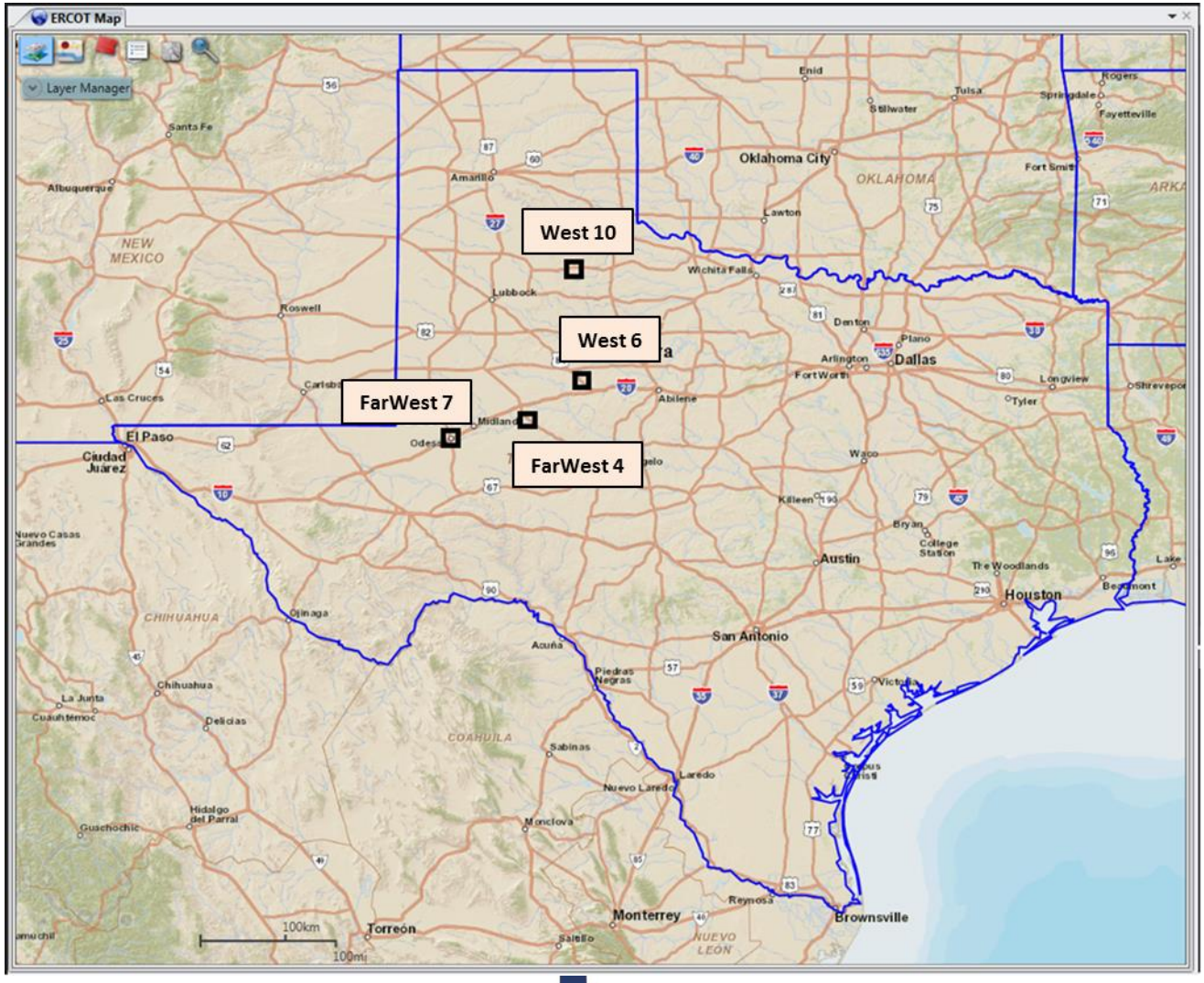
Mode #6 – 2.7 Hz @ FarWest 4

- Source: FarWest 4
- Signal type: current magnitude
- Oscillation type: wind generation related
- Wind generators nearby: FarWestGen4
- Occurrence:
  - Appeared every month in all three years
  - Minimum occurrence in July 2013, and appeared for 9% of time
  - Maximum occurrence in May 2013, and appeared for 34% of time
  - Average occurrence in all three years is about 20% of time during the month

Mode #6 – 2.7 Hz @ FarWest 4

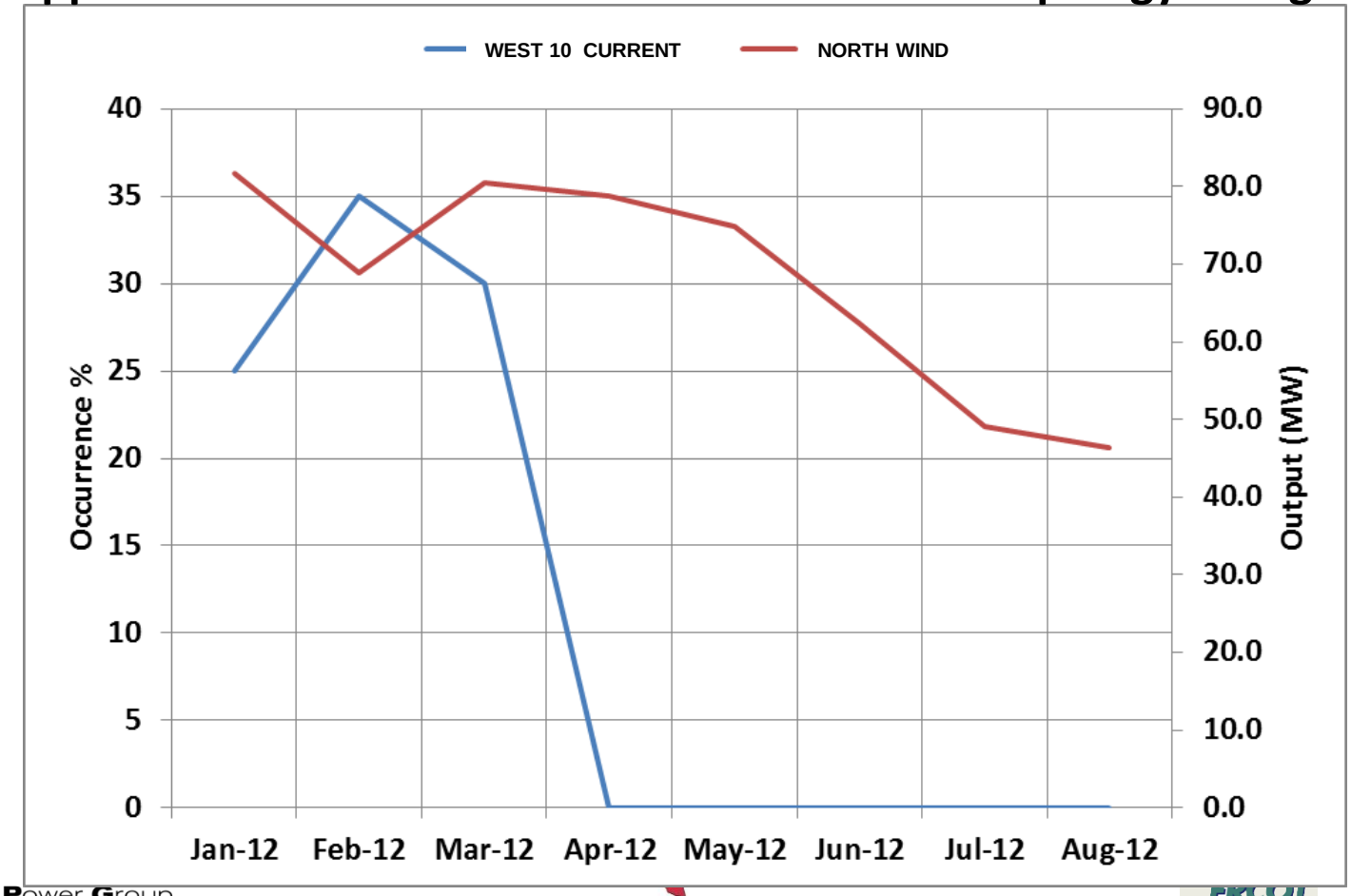
- Occurrence:
  - Mode disappears at beginning of 2014
- Disappearance of 2.7 Hz mode may be related to addition of new CREZ transmission lines near FarWest 7, running down to West 29 and West 8 on Jan 3, 2014, or any tuning of control systems @ FarWestGen4
- **ERCOT should review the disappearance of the mode with wind owners and determine the root cause to evaluate the need for additional monitoring**

Mode #1 – 0.6 Hz @ 4 Locations



Mode #1 – 0.6 Hz @ West 10

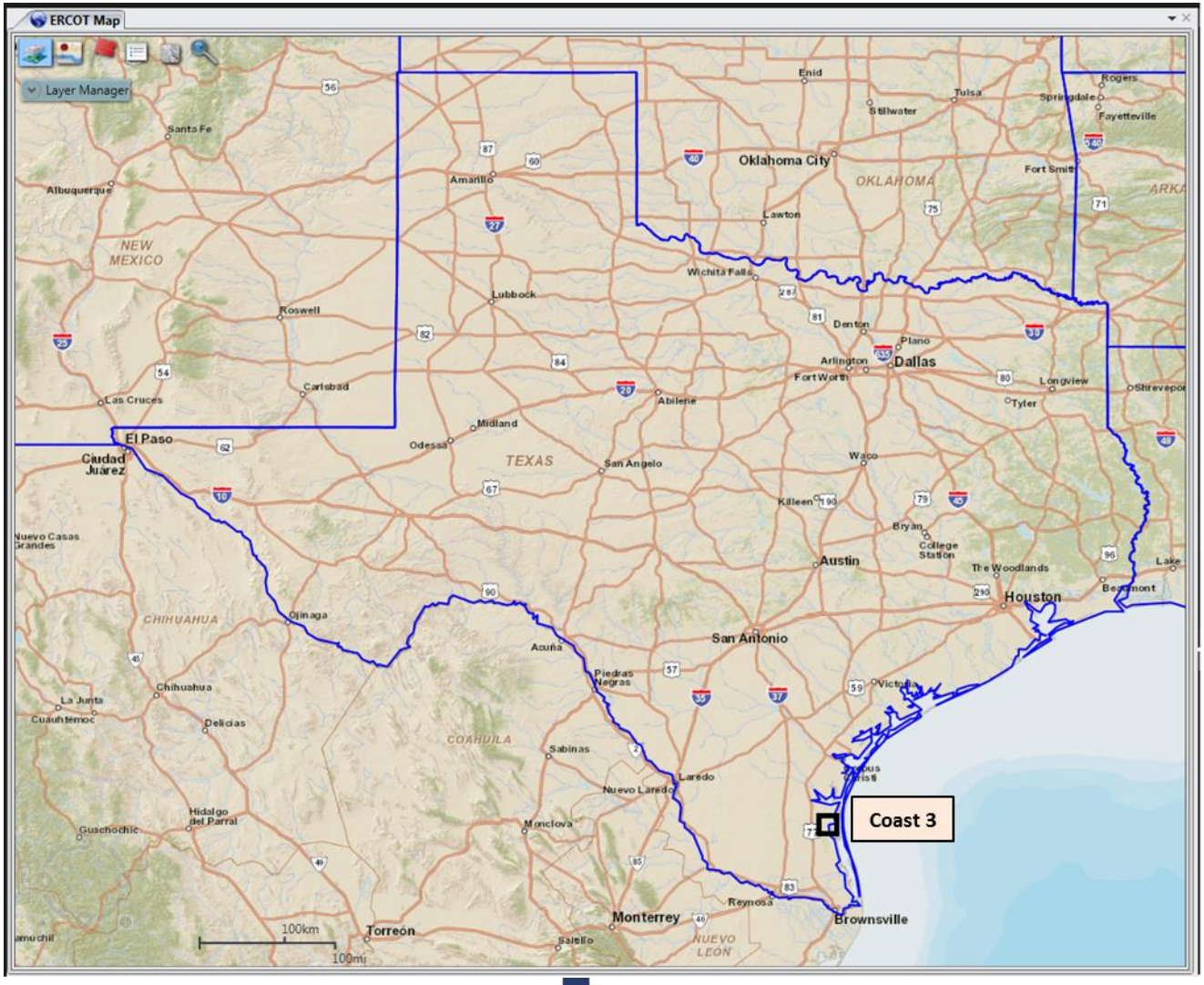
- Mode occurrence @ West 10 does not follow north wind pattern & does not appear to be consistent as 3.2 Hz, rather disappeared after March 2012
- But these oscillations were observed more strongly near wind generators, and appear to be related to local oscillation due to topology change



Mode #1 – 0.6 Hz @ West 10

- Source: Panhandle (West 10)
- Oscillation type: local
- Generators nearby: WestGen10
- Occurrence:
  - Appeared only in first three months in 2012
- Energy – within the period of occurrence
  - Maximum highest energy was about 2
  - Minimum highest energy was about 1.6
- **Appears to be a local issue & ERCOT needs to review the appearance of the mode with plant owners & determine the root cause to evaluate the need for additional monitoring**

Mode #5 – 2 Hz @ Coast 3



Mode # – 2 Hz @ Coast 3

- Source: Valley (Coast 3)
- Signal type: voltage magnitude
- Oscillation type: local control systems from nearby wind generators
- Wind generators nearby: CoastGen3, CoastGen4, CoastGen5
- Occurrence:
  - Appeared only in April 2013, for 0.8% of time
- Energy – within the period of occurrence
  - Highest energy value was about 0.5
- Occurred for a short period of time with low energy

Conclusion – Identified 9 Oscillatory Modes

- Occurrence of some modes appear to be related to wind production – 0.9 Hz (ongoing) & 2.7 Hz (no longer present)
- Occurrence of some modes appear to be related to control system changes –1.5 Hz (Coast 3), 1.7 Hz (FarWest 7), 2 Hz (Coast 3), 3.2 Hz (West 10)
  - Appear with significant energy for a short period of time and disappear
- Occurrence of some modes (5.0 Hz, 5.4 Hz, and 6.0Hz) appear to be related to the presence of wind generation, but not to production
- 0.6 Hz from West 10 – local oscillation (no longer present)
- 0.9 Hz from West 6 (ongoing)
- 5.0 Hz from Coast 3 (ongoing)
- 5.4 Hz from west wind & Panhandle (ongoing)
- 6.0 Hz from Panhandle (ongoing)

Thank You.

Any questions ?

www.electricpowergroup.com

626.685.2015

Electric Power Group

Attachment 12. 2014 RTDMS and PGDA Training Comments

ERCOT RTDMS User Training Evaluation Form/Responses

September 16, 2014

44 responses received

1. Did the training meet your expectations?

- 39 - Yes
- 2 - Yes and more than expected
- Yes, but 2 days not enough to go through a lot of new information
- First exposure to material, but provided good introduction to analysis tool

2. What was the most effective part of this training?

- 13 - Case study
- 13 - Hands on use
- 2 - Tools and slides
- 2 - Understanding navigation tools, GUI features, and what types of raw data is available
- Understanding voltage phase angle and stress on transmission system; case studies interesting and improved understanding
- Reviewing the various tabs in order to analyze trends
- Learning how to use the dashboard and responding to alarms
- Display interaction
- Monitoring grid stability in real time
- Event recognition and diagnosis
- How much data is analyzed
- Phasor grid dynamics
- Interaction of personal with question and answer sessions
- Synchrophasors is a very new topic for me and I think every part of this training was very effective in terms of giving me a good overview of it and the tools
- Lots of computers

3. What was the least effective part of this training?

- 16 - NA
- 6 - Too much information in a short period of time
- 3 - Slides
- 4 - Laptop/Server was slow and could not be used most of the time
- 2 - Need written material to follow presentation as part of presentation may be missed while trying to follow on computer and slides presentation
- 2 - How to customize displays
- 2 - Basic navigation and settings
- Navigating through screen too quick
- At times it got too technical, to the engineer level, so we will never use
- Sharing laptop limited hands on, so gained less experience
- Using just the RTDMS to analyze an event

- Nothing on setting alarm thresholds
- Real-time dynamics monitoring presenter
- Need more hands on
- Hard to understand
- Understanding dialects. It's rude to tear down while the last 2 are presenting. Shorten other talks, give them their time, then tear down your laptops after we leave

4. What suggestions do you have to improve the training?

- 14 - NA
- 5 - More hands on and use cases training on ERCOT examples
- 4 - More training days with less time per each day, with more hands on
- 3 - Break down in smaller groups
- 3 - More breaks
- 2 - Have screenshots of step-by-step for the solutions, sort of a visual manual of how past analysis was done to determine what happened
- 2 - Speakers need more improvement on crowd involvement
- Make it longer and more technical (not for operators). For operators, cover more on damping. Cover algorithms for location of unit trip and first responders
- Add some more power system dynamics analysis knowledge. Help students review some concepts first
- Develop web-based training modules that can be used later to reinforce the presented material
- Try to have people hold questions about specifics until after the "big picture" presentations are over
- Show examples of how the RTDMS will be integrated using SCADA, SE, and RTCA
- Make more displays/profiles
- Follow an observation to learn how to analyze a system problem
- Follow-up once it is available to the user
- Power points

5. Are you comfortable with your level of proficiency to use the RTDMS application?

- 25 – Yes
- 13 - Need more practice
- 3 - Somewhat
- Limited to moderate. We do not have this application at my company
- No, but not just because of presenter, but because the software is new to me
- No

ERCOT PGDA User Training Evaluation Form/Responses

September 17, 2014

42 responses received

1. Did the training meet your expectations?

- 37 - Yes
- 2 - Yes, and beyond
- Training was short and fast, but fairly straight-forward system
- Not quite, information was presented very rapidly
- For the most part. I was more looking for analytics behind the scene stuff, not how to change colors, names, and titles. It has been touched upon over the course of training but wasn't the main focus.

2. What was the most effective part of this training?

- 11 - Use case studies
- 8 - Hands on
- 3 - Demos
- 3 - Navigation views, displays and tools
- 2 - Walking through step-by-step
- 2 - Using the computer to figure out the scenario
- 2 – Analysis/Frequency response analysis
- The baselining. How different events in the system change the system response, how frequency phase angle changes, how to learn and categorize typical system events
- Phasor grid dynamics analyzer
- Knowledge of the instructors
- User interaction
- Data collected
- Lots of computers
- 5 - Not answered

3. What was the least effective part of this training?

- 21 - NA
- 4 - Too much information in a short period of time
- 3 - Slides
- 2 - Some are hard to understand
- 2 - Need more hands on

- A lot of options/settings that weren't explained, perhaps due to highlighting most useful/important features
- How and when to start taking actions? You have all the data streaming through, lots of data, lots of information, alarms. For the operator having to take action within minutes, it is not helpful to initiate the proper action process
- The last case, more in-depth analysis
- Introduction to user interface, but necessary
- Overall intuitiveness of locating information in the GUI
- Multiple view and analysis was confusing
- Zoom-in function didn't always work properly
- How to customize displays
- Server could not keep up

4. What suggestions do you have to improve the training?

- 17 - NA
- 7- More event cases
- 2 - More hands on
- 2 - More training days with less time per each day, with more hands on
- 2 - Break down in smaller groups based on audience needs
- 2 - More breaks
- Develop web-based training modules that can be used later to reinforce the presented material
- Need more time to explain how to get access and when it will be available
- More time spent on frequency response and more in-depth on modal analysis
- Discuss NERC A,B,C points
- Get through exercise for New-Load-Save-Open process
- Good to have written outline that's easy to follow
- Less days
- Better server
- Speaker
- More snacks

5. Are you comfortable with your level of proficiency to use the RTDMS application?

- 30 - Yes
- 8 - Need more practice
- 4 - Somewhat

Attachment 13. Generator Model Validation Tool

Center for Commercialization of Electric Technologies (CCET)

Discovery Across Texas Project

Generator Parameter Validation

Submitted to

Milton Holloway, Ph.D.
mholloway@electrictechnologycenter.com

Prepared by:

Electric Power Group

John W. Ballance
Prashant C. Palayam
Neeraj Nayak

November 20, 2014

Table of Contents

List of Figures

CCET Discovery Across Texas

Generator Parameter Validation

CCET 3.1.1

1. Introduction

The Center for Commercialization of Electric Technologies (CCET) was awarded contract DE-OE0000194 by the Department of Energy to perform the Discovery Across Texas demonstration project. Electric Power Group, LLC (EPG) received a sub-award from CCET to provide professional services to perform, among other things, development of the Generator Parameter Validation (GPV) tool for Electric Reliability Council of Texas (ERCOT) use. The Generator Parameter Validation (GPV) tool is based on the research work done by Dr. Wei-Jen Lee et al from the University of Texas at Arlington [1][2]. EPG appreciates their contribution to the generator parameter validation process and for providing the program code which was used for the development of the GPV tool.

Power systems are complex networks with thousands of components. Computer simulations are used as the basis to simulate and study the power system's response to a variety of contingencies. Generators, loads, transmission lines and other power system components are represented as mathematical models in the computer simulation programs to predict network responses. Simulations, based on models of the network components, are used widely in both power system planning and operation, and play an important role in predicting the grid response and preparing for contingencies. Hence, having correct models is very essential. Checking and validating models is a must for maintaining grid reliability. Also, periodic validation of the models would be required to comply with North American Electric Reliability Corporation (NERC) reliability standards [3].

Generators are one of the most important components of the power systems. Having correct generator models is highly important. The traditional testing method of performing staged tests on generators, taking detailed recordings of the generator's response, and then comparing the measured and predicted responses, is very expensive, time-consuming and may risk damage to the equipment. Also, the units typically have to be taken out of service for testing.

GPV is the process of validating generator model parameters using Phasor Measurement Units (PMU) measured data. GPV uses recorded disturbance data measured at the output of a generator to validate and calibrate generator model parameters. Disturbances occur frequently on the network, and afford the opportunity to measure the response of the generator, if appropriate data

recording capability is in place and operational. PMU data collected at the output of the generator provides the continuous high-speed monitoring capability needed to perform model validation. The GPV tool provides a means of validating the simulated results with the measured generator response from these occasional grid disturbances. If the model simulation results don't match the recorded data, the model parameters are likely to be incorrect and the model needs to be corrected. The correct model parameters are identified by the optimization process using advanced algorithms. The types of models that can be validated are generators, governors, exciters and stabilizers. This validation process can be done frequently, using data from normally occurring grid disturbances, without taking the generators offline. The GPV tool allows the user to perform the validation process with a user interface.

2. Executive Summary

Power systems are complex networks with thousands of components. Models are required to understand system behavior and are used widely in power system studies, planning and operation. They play an important role in predicting the grid response and planning for contingencies. Hence, having correct models is very essential. Checking and validating models is a must for maintaining grid reliability. Also, periodic validation of the models would be required to comply with North American Electric Reliability Corporation (NERC) reliability standards.

Generators are one of the most important components of the power system. Having correct generator models is highly important. The traditional testing method of performing staged tests on generators is very expensive, time-consuming and may damage the equipment. The units have to be taken out of service for testing. GPV is a process of validating the generator model parameters using synchrophasor data. Using synchrophasor data, the models can be periodically validated without taking the generators offline. The GPV tool uses measured disturbance data captured by Phasor Measurement Units (PMUs) to validate the generator models. The types of models that can be validated are generator models, exciter models, governor models and stabilizer models.

The generator parameter validation consists of three processes: validation, sensitivity analysis and optimization. In the validation process, the model simulation output waveform is compared to the PMU measured waveform. If the validation results indicate a poor match between the simulated and measured waveforms, sensitivity analysis should be performed. Sensitivity analysis identifies the model parameters which have the greatest effect on the output of the simulation. Thus, sensitivity analysis helps to identity the key parameters that need to be selected for the final step, which is the optimization process. Sensitivity analysis also enables plotting of trajectories of the change in active and reactive power for every parameter. Optimization is the process of finding the set of parameter values for which the simulation output best matches the PMU recorded measurements. Advanced algorithms are used for the optimization process. Also,

the variation of parameters can be restricted by specifying a maximum and minimum value for individual parameters. This enables fine-tuning of the identified parameters and helps to converge on the most representative parameter values. The newly identified parameter values can then be used for calibrating the models. The GPV tool provides a user interface for all three steps in the generator parameter validation process.

This report includes a brief description of the generator parameter validation process. It includes the work done towards the development of the GPV tool and also includes some results obtained by using the tool.

3. Process and Methodology

The steps involved in the generator parameter validation process are shown in Figure 1 below:

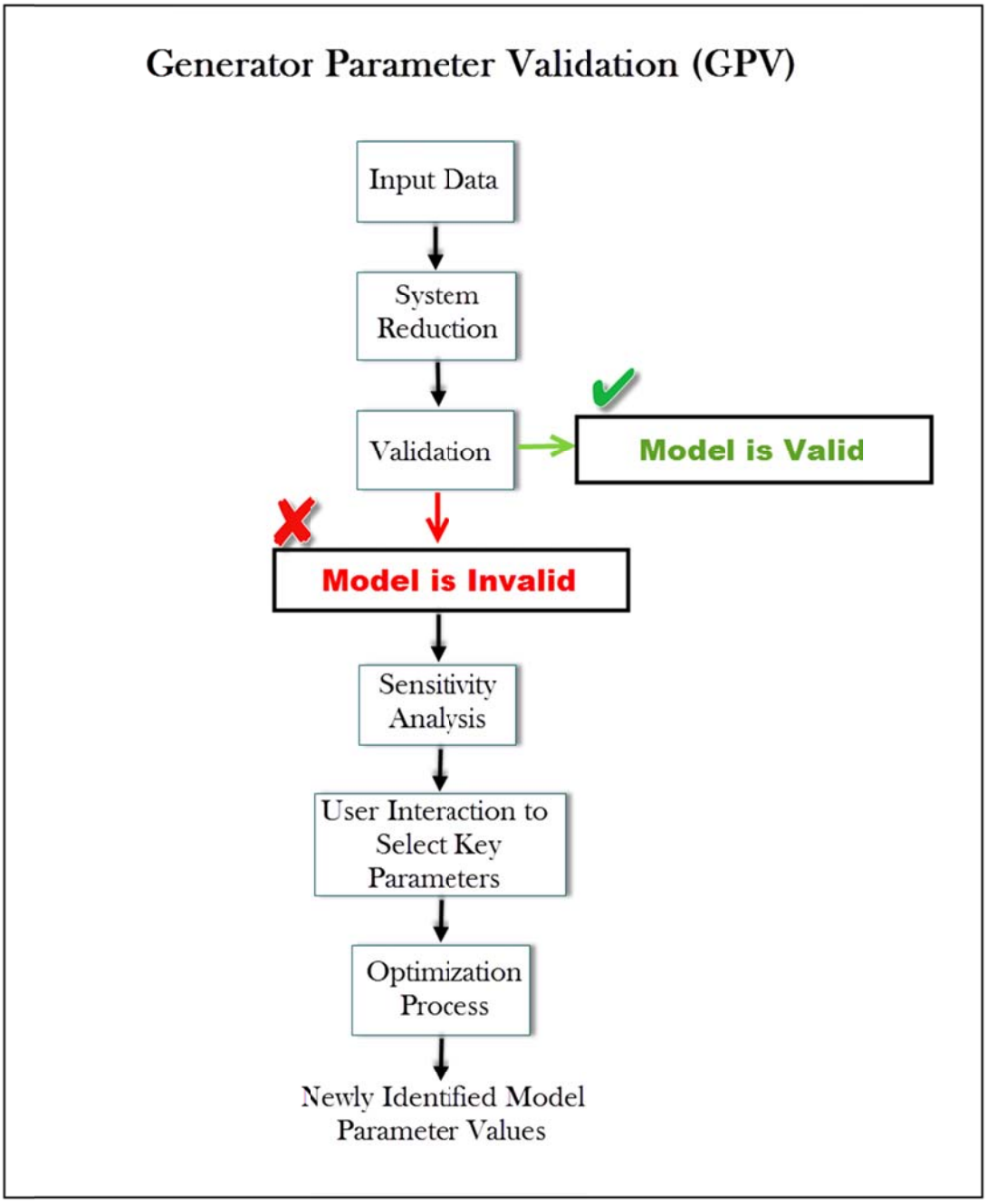


Figure 1. Generator Parameter Validation Process Workflow

Step 1 Obtain PMU measured data (Voltage, Voltage angle, Active Power and Reactive power) at the output of the individual generator unit as input data in the format required by the tool.

Step 2 Using a system reduction approach, reduce the entire system to a smaller system at the output of the generator.

Step 3 Perform the validation process by comparing model simulation results with the measured data and evaluate the need for calibration.
Step 4 Run sensitivity analysis to display sensitivity of power flows to each parameter.
Step 5 Select key parameters for the optimization process based on the sensitivity analysis results. Optionally specify range (minimum, maximum) limits for parameter variation.
Step 6 Run the optimization process to identify correct parameter values.

The generator parameter validation process requires three input data files: an Excel file with PMU measured data in the required format; a PSS\E saved case file, and PSS\E dynamics file corresponding to the electrical network at the time of the recorded disturbance. A system reduction approach is used whereby the entire power system is reduced to a smaller system at the output of the generator, and the simulations are then performed using a concept called as hybrid dynamic simulation [1][2]. Hybrid dynamic simulation uses measured data as well as the simulation model to perform dynamic simulations. The GPV tool runs the PSS\E simulation engine in the background using the python programming language.

The system reduction process is followed by three processes: validation, sensitivity analysis, and optimization. In the validation process, the model simulation output waveform is compared to the PMU measured waveform. If the validation results indicate a poor match between the simulated and measured waveforms, sensitivity analysis should be performed. Sensitivity analysis identifies those model parameters which have the greatest effect on the output of the simulation. Thus, sensitivity analysis helps to identity the key parameters that need to be selected for the next step, which is the optimization process. Sensitivity analysis also enables plotting of trajectories of the change in active and reactive power for every parameter. These trajectory plots provide an additional visualization of the sensitivities of the power flows to each parameter change.

When there is a mismatch in the simulation results and measured results, it is important to identify the parameters that caused the mismatch. Optimization is the process of finding the set of parameter values for which the simulation output best matches the PMU recorded measurements. Two advanced algorithms, namely Particle Swarm Optimization (PSO) and Simultaneous Perturbation Stochastic Approximation - Particle Swarm Optimization (SPSA-PSO) Cooperative Method may be used for the optimization process [1][2]. For the optimization process, the variation of parameters can be restricted by specifying maximum and minimum values for individual parameters. This enables fine-tuning of the identified parameters and helps to narrow down on the correct parameter values. The newly identified parameter values will be useful for calibrating the models.

4. User Interface

A user interface was built for the GPV process.

The interface allows users to:

1. Select input data files.
2. Specify case and model information.
3. Run the validation process and view results and plots.
4. Perform sensitivity analysis and view results.
5. Select key parameters.
6. Select algorithm for optimization process.
7. Run the optimization process and view results and plots.

The GPV tool interface is shown in Figure 2 below.

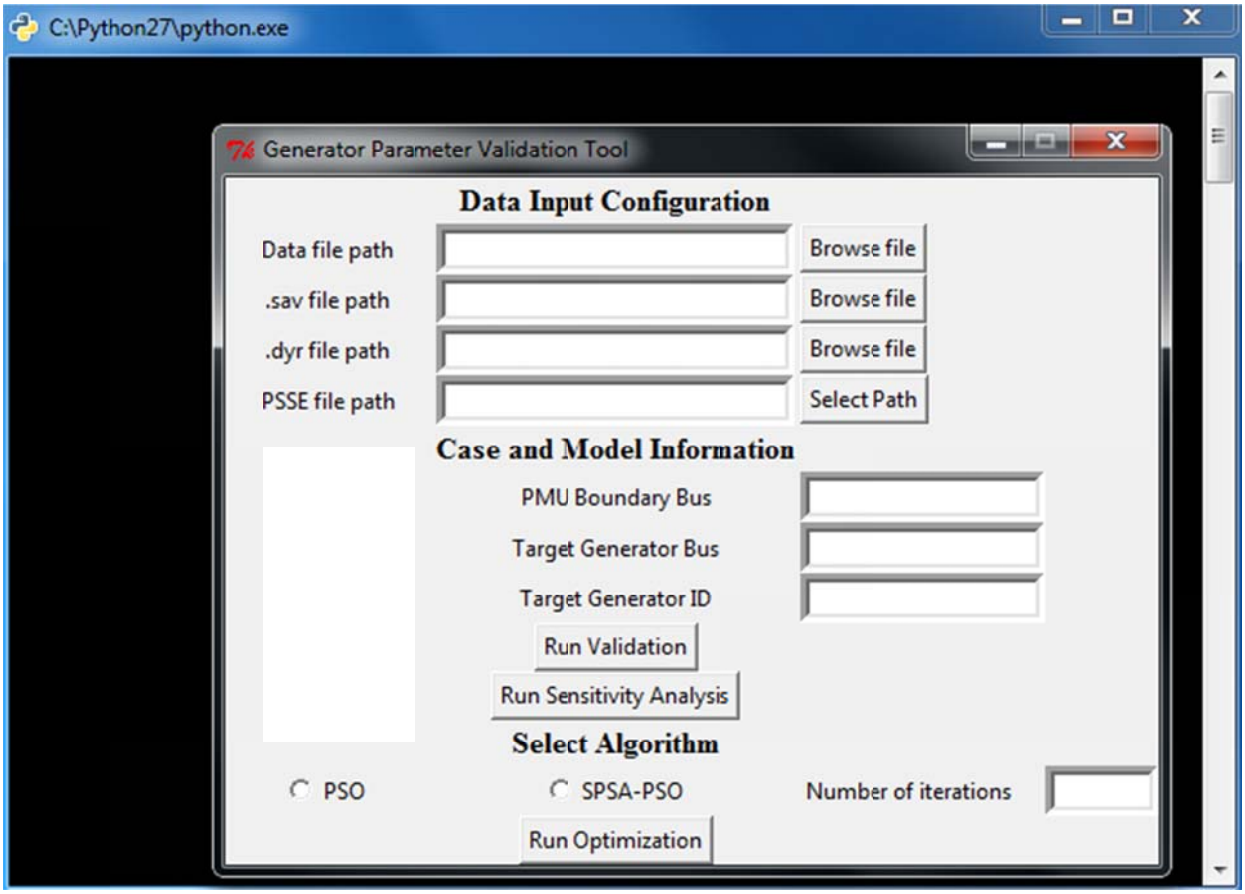


Figure 2. GPV tool user interface

5. Tool Features

Some of the key features of the GPV tool are listed below:

1. Automation of the system reduction process.
2. Sensitivity analysis results with ranked and color coded parameter values.
3. Comparison plots for validation – simulation output vs. measured data.
4. User interaction to select key parameters and optionally specify range for each parameter.
5. Plot trajectories for sensitivity of active and reactive power flows to each parameter.
6. Optimization process with two advanced algorithms.
7. Plots comparing measured data, actual model simulation output and new identified model simulation output .

6. Test Case Results

The GPV tool was tested on PSS\E example case files using simulated data as input measured data. Input data for 10 seconds was obtained by simulating a bus fault event and obtaining P, Q, V, and Angle measurements at the PMU boundary bus (201) in order to validate a hydro generator at bus number 211. The one-line diagram view of the generator is shown in Figure 3 below. This generator is a part of a 23 bus example system provided by PSS/E. The models associated with this generator are generator model - GENSAL, governor model – HYGOV and exciter model - SCRX. One of the dynamic model parameters was manually changed to create a mismatch between the simulated and measured results. Parameter number 3 (H-Inertia) from the GENSAL model was changed from 5 to 4 per unit on machine MVA base. In other words, simulation data that was used as measured data input to the tool was obtained with the parameter value of 5 but the input dynamic data for running simulations with the tool had parameter value set to 4.

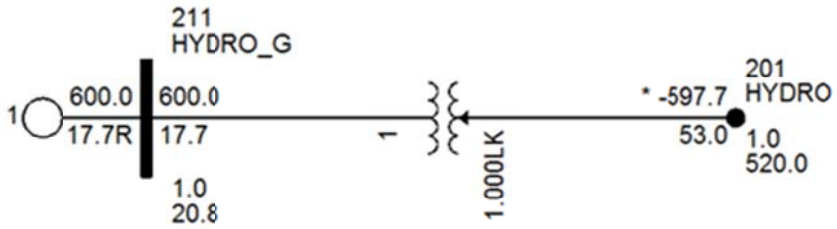


Figure 3. One-line diagram view of the target generator

The results from the validation process are shown in figures 4 and 5 below.

Active Power (P)

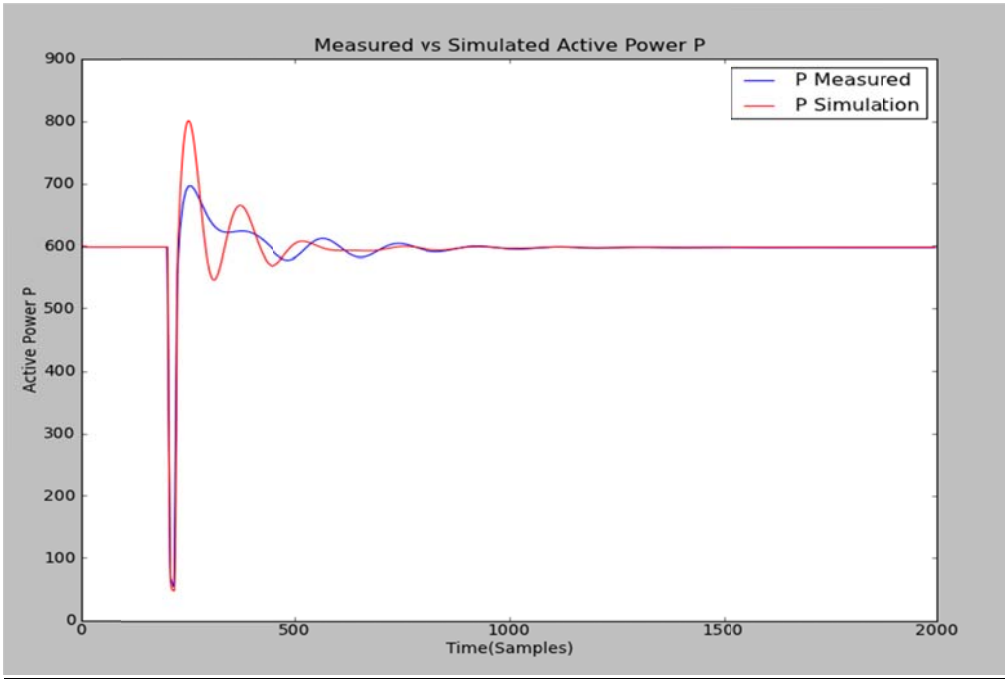


Figure 4. Validation Plots for active power (P)

Reactive Power (Q)

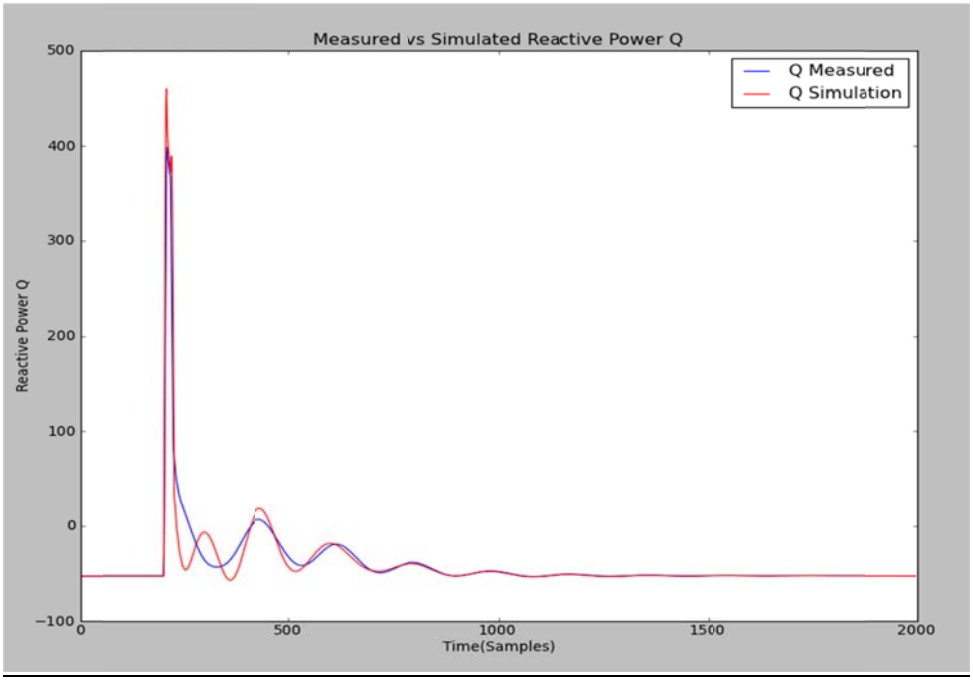
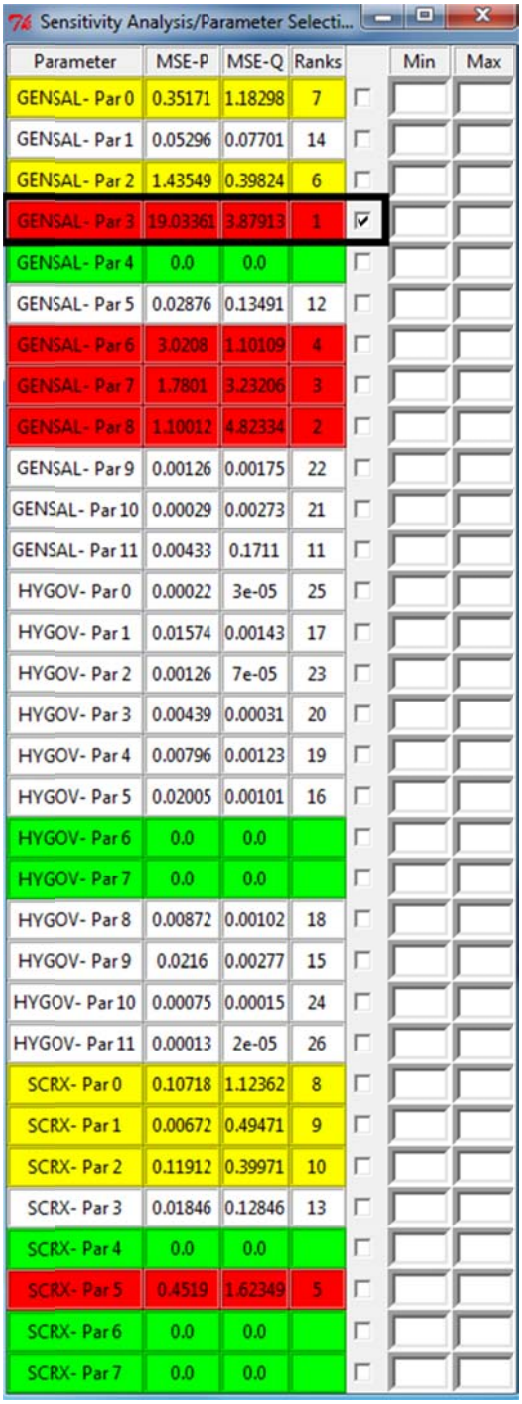


Figure 5. Validation plots for reactive power (Q)

A mismatch in the measured and simulation results is observed in the validation plots. Sensitivity analysis was then performed to identify the key parameters that have highest impact on the simulation response. The sensitivity analysis results are shown in figure 6 below.



Parameter	MSE-P	MSE-Q	Ranks		Min	Max
GENSAL- Par 0	0.35171	1.18298	7	☐		
GENSAL- Par 1	0.05296	0.07701	14	☐		
GENSAL- Par 2	1.43549	0.39824	6	☐		
GENSAL- Par 3	19.03361	3.87913	1	☑		
GENSAL- Par 4	0.0	0.0		☐		
GENSAL- Par 5	0.02876	0.13491	12	☐		
GENSAL- Par 6	3.0208	1.10109	4	☐		
GENSAL- Par 7	1.7801	3.23206	3	☐		
GENSAL- Par 8	1.10012	4.82334	2	☐		
GENSAL- Par 9	0.00126	0.00175	22	☐		
GENSAL- Par 10	0.00029	0.00273	21	☐		
GENSAL- Par 11	0.00433	0.1711	11	☐		
HYGOV- Par 0	0.00022	3e-05	25	☐		
HYGOV- Par 1	0.01574	0.00143	17	☐		
HYGOV- Par 2	0.00126	7e-05	23	☐		
HYGOV- Par 3	0.00439	0.00031	20	☐		
HYGOV- Par 4	0.00796	0.00123	19	☐		
HYGOV- Par 5	0.02005	0.00101	16	☐		
HYGOV- Par 6	0.0	0.0		☐		
HYGOV- Par 7	0.0	0.0		☐		
HYGOV- Par 8	0.00872	0.00102	18	☐		
HYGOV- Par 9	0.0216	0.00277	15	☐		
HYGOV- Par 10	0.00075	0.00015	24	☐		
HYGOV- Par 11	0.00013	2e-05	26	☐		
SCRX- Par 0	0.10718	1.12362	8	☐		
SCRX- Par 1	0.00672	0.49471	9	☐		
SCRX- Par 2	0.11912	0.39971	10	☐		
SCRX- Par 3	0.01846	0.12846	13	☐		
SCRX- Par 4	0.0	0.0		☐		
SCRX- Par 5	0.4519	1.62349	5	☐		
SCRX- Par 6	0.0	0.0		☐		
SCRX- Par 7	0.0	0.0		☐		

Figure 6. Sensitivity Analysis Results

Note that the top five highest sensitivity parameters are color-coded in red. Parameter 3 (Inertia-H) from the GENSAL model was ranked 1 in the sensitivity analysis results. This parameter was selected for the optimization process.

Results from the optimization process for one iteration using the SPSA-PSO [1][2] algorithm are shown below.

Active Power (P)

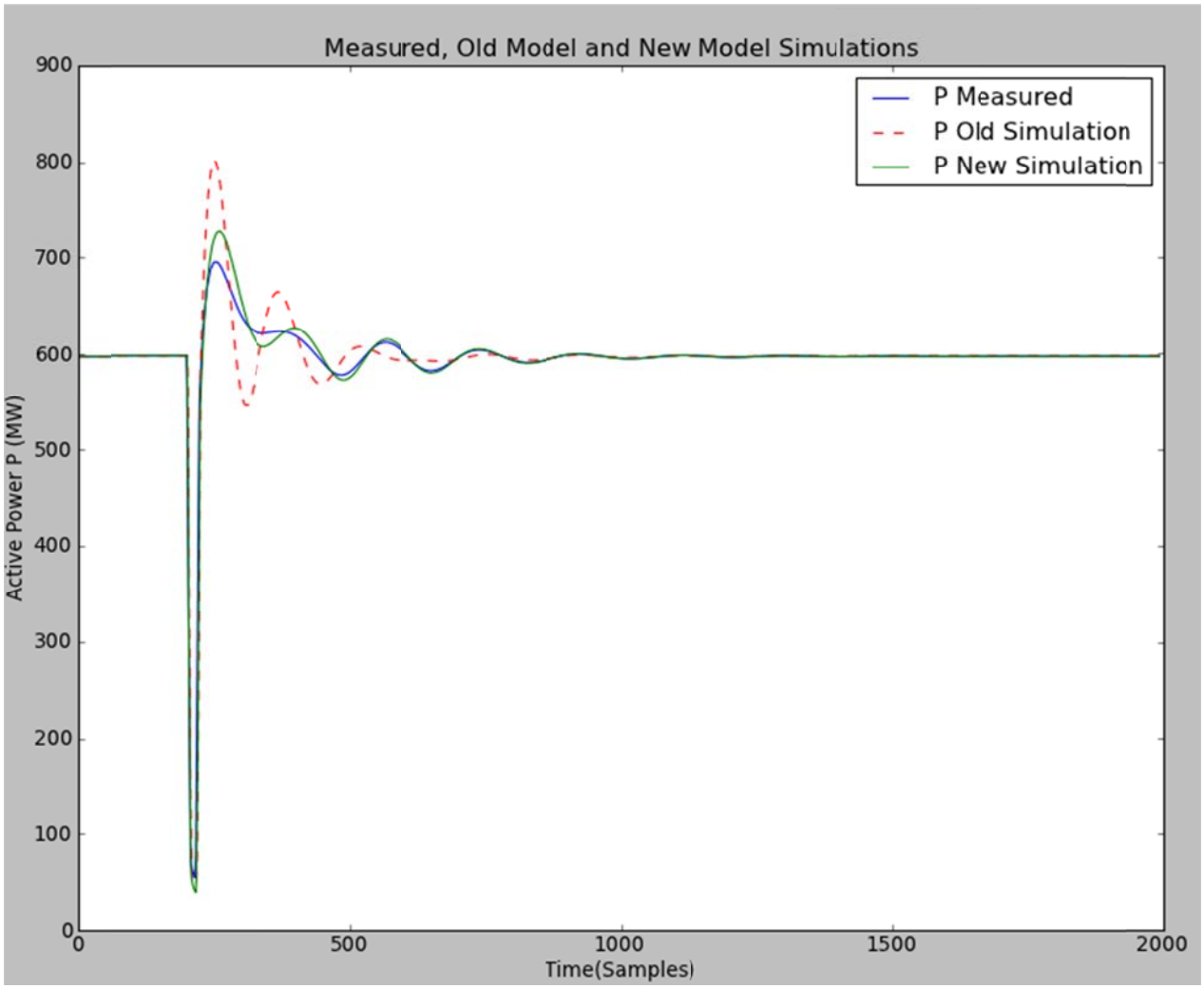


Figure 7. Active power plots after the optimization process

Reactive Power (Q)

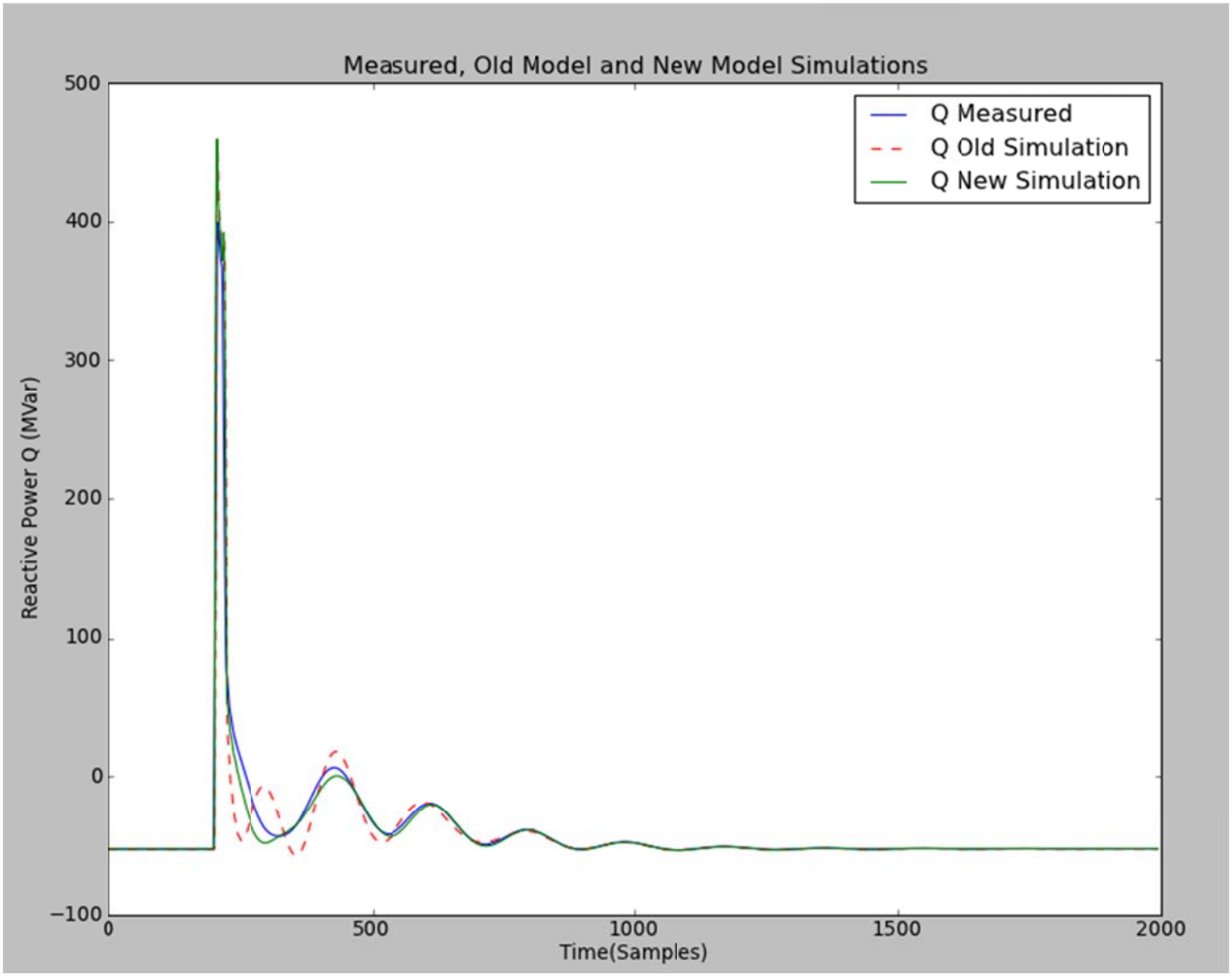


Figure 8. Reactive power plots after the optimization process

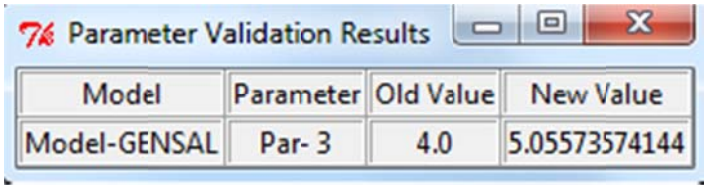


Figure 9. Parameter validation results – new identified parameter values

It can be seen from the figures 7 and 8 that the P and Q response with the new identified parameter value (green line) is much closer to the measured input value (blue line) than the original model simulation (red line). Note that some error due to the use of a reduced system is inevitable. The newly identified parameter value for GENSAL parameter 3 is 5.056 as shown in figure 9 above. This value is very close to the actual value (5) of the parameter in the model.

Some information with regards to the tool run time is provided below:

For the input data corresponding to 10 second duration:

1. Validation Process took about 15 seconds.
2. Sensitivity Analysis took about 7 minutes.
3. Optimization process with one iteration took about 8 minutes.

It was observed that with simulation data as input, one or two iterations were sufficient to identify the parameter change and reduce the mismatch. However, the optimization process for two iterations and five iterations takes approximately 11 minutes and 23 minutes, respectively on the test machine.

7. Testing with Real Data

The GPV tool was recently tested with real data obtained from an electric utility. The following data was obtained for the testing purpose.

1. PMU recorded Voltage and Current Phasors at the output of a generator corresponding to an event – Excel file (.xlsx).
2. PSS\E Model data – Case file (.sav) and Dynamic file (.dyr).

Validation was performed on generator, exciter, governor and stabilizer models. The results are shown in figures 10 and 11 below.

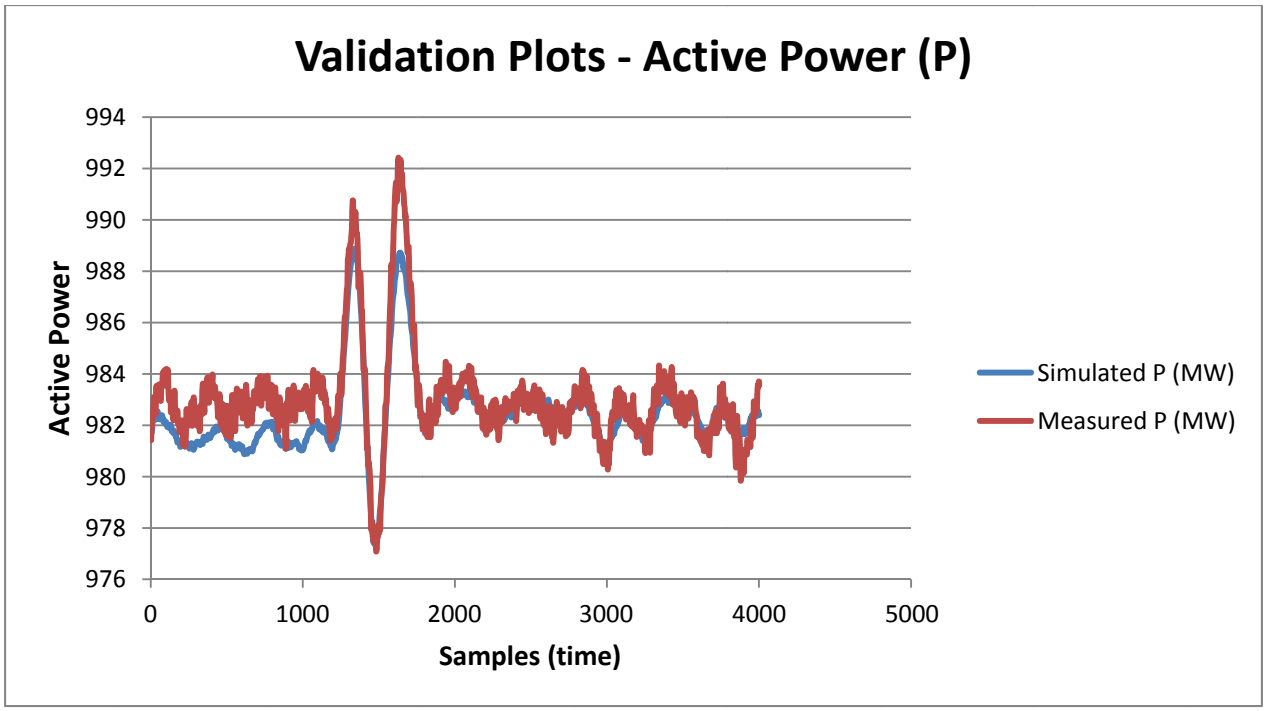


Figure 10. Validation plots for active power (P)

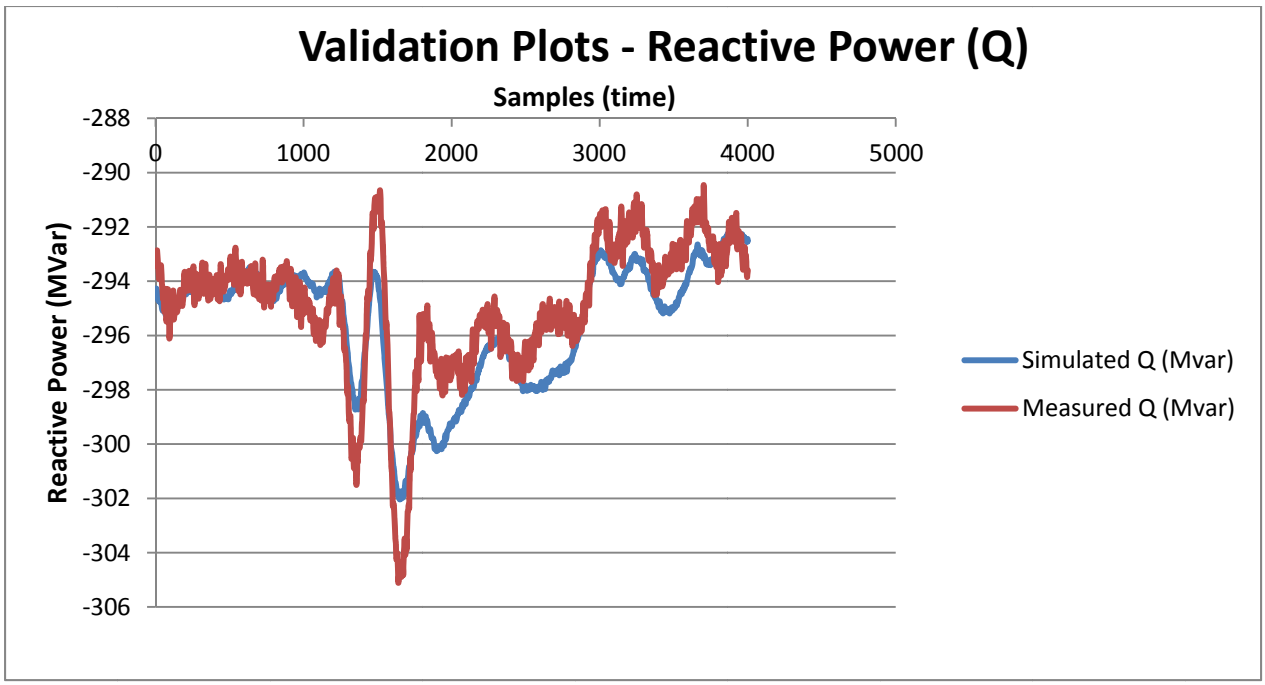


Figure 11. Validation plots for reactive power (Q)

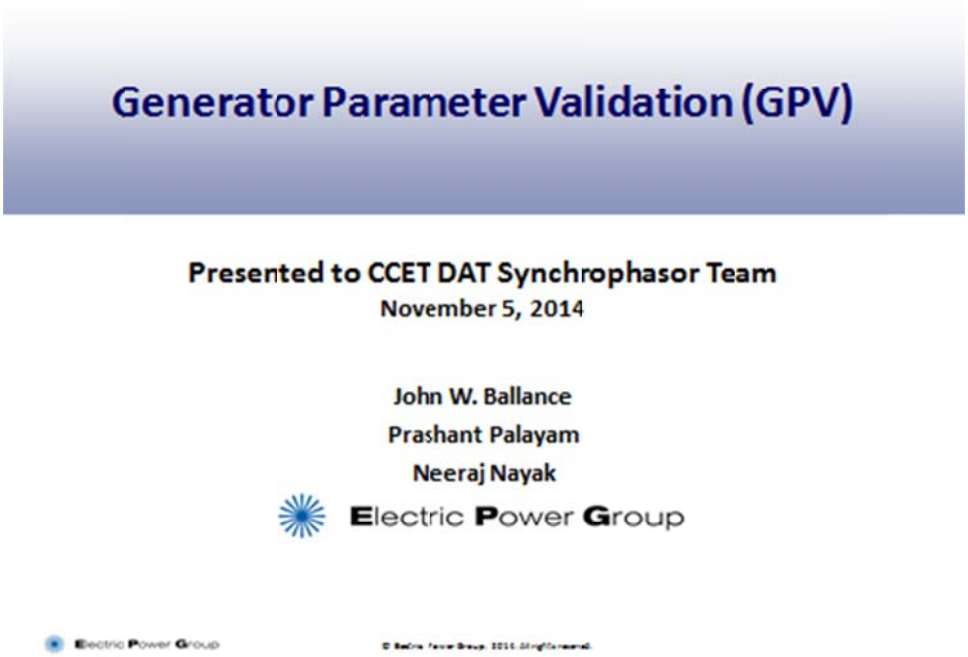
We can see from the plots above that the model simulation results reasonably match that of the measured data. It is important to remember that models are an approximation of the real system and some error due to the use of a reduced system is inevitable.

8. Conclusion

A tool was built for use by Electric Reliability Council of Texas (ERCOT) to perform the generator parameter validation process. The tool, Generator Parameter Validation, uses synchrophasor data from Phasor Measurement Units. The PMUs must be located at the output of the individual generator unit and measure the individual generator branch for validating the generator. The system reduction approach used for this methodology has been automated and is –built-in to the tool. The entire process is split into three steps in sequence - Validation, Sensitivity Analysis, and Optimization. Validation results show comparison plots between simulation and measured data. Sensitivity analysis shows sensitivity of the power flows to each parameter and identifies the key parameters. User interaction is enabled for key parameter selection and for fine-tuning parameter values by specifying a range for the parameters. The optimization process identifies new parameter values for which the model simulation results best match the measured data. The results from the optimization process produces plots comparing the measured, actual model and new model parameter simulation results. The entire validation process for a 10-second input data record takes approximately 20-minutes with one iteration of the optimization algorithm.

9. Appendix

Generator Parameter Validation Presentation



10. References

[1] Chin-Chu Tsai; Wei-Jen Lee; Nashawati, E.; Chin-Chung Wu; Hong-Wei Lan, "PMU based generator parameter identification to improve the system planning and operation.

[2] Chin-Chu Tsai, “PMU based parameter identification for the synchronous generator dynamic model”, December 2011

[3] http://www.nerc.net/standardsreports/standardssummary.aspx

Generator Parameter Validation (GPV)

John W Ballance

Prashant Palayam

Neeraj Nayak

Electric Power Group

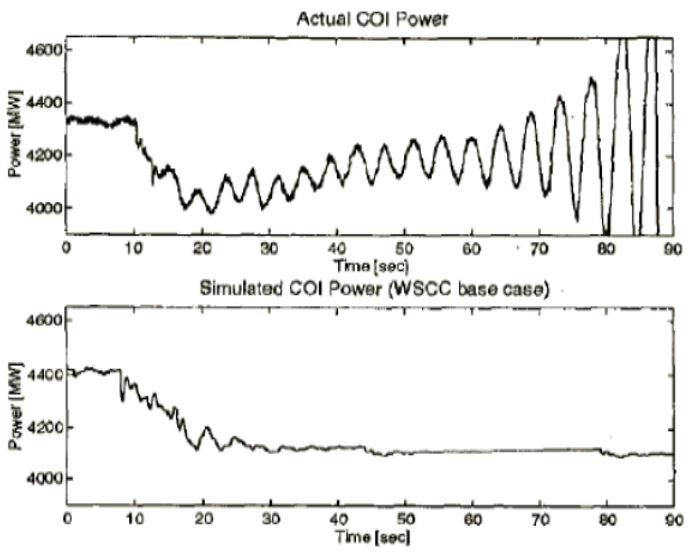
November 5, 2014

Presented to CCET DAT Synchrophasor Team

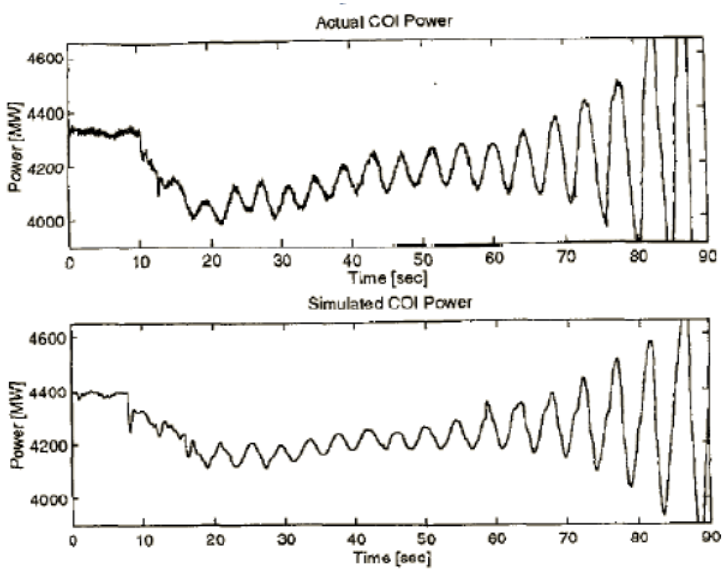
Outline

- Background and purpose
- Introduction
- Generator parameter validation process
- Example
- Testing on real data
- Best practices
- Limitations and areas of smprovement
- Summary

Background and Purpose



After Tuning Models



August, 1996 WSCC

Importance of Correct Models

- Match dynamic grid response
- Establish operation limits and guidelines
- Study contingencies and analyze events
- System planning

Background and Purpose

- Staged Tests
  - Online testing is expensive , time consuming and can damage the equipment
  - Unit has to be taken out of service.
  - Periodic validation is needed - Parameters may change over time with aging of equipment
- NERC recommended a process for validating power system models and data including generator dynamic models to address the shortcomings that contributed to August 14th 2003 blackout
- NERC Standards
  - MOD-012 requires power plant owners to provide power plant data for dynamic simulations
  - MOD-026 requires power plant owners to verify that the provided dynamic models of excitation controls are accurate and up to date
  - MOD-027 requires power plant owners to verify that the provided dynamic models of governors and turbine controls are accurate and up to date

Background and Purpose

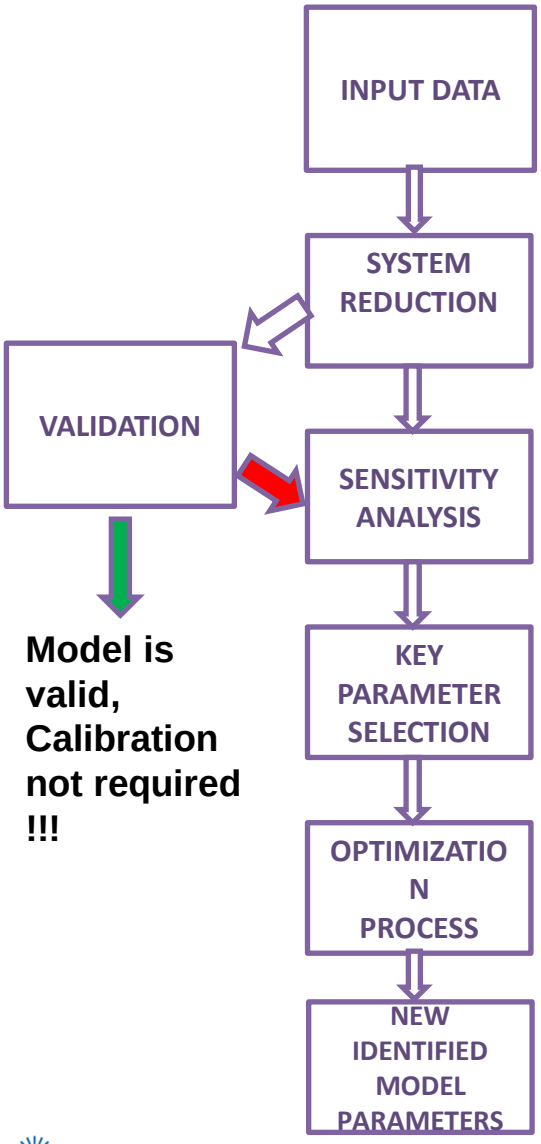
- Dr. Wei-Jen Lee (UT Arlington) et. al proposed and developed a PMU-based parameter identification method
- The purpose of the GPV tool is to validate generator models and calibrate the models to identify correct parameter values
- An initial first phase development of GPV method as a tool that was planned is completed
- The algorithm was implemented and tested using 8 different case studies via simulation data that mimics the phasor data
- Lately, the tool was also tested with PMU data

Introduction

Methodology:

- Use PMU measured event data to validate the generator model parameters
- Develop a model parameter validation process based on the following constraints:
  - PMU measured event data (P, Q, V, Angle) is available
  - System operation conditions corresponding to the disturbance are available
  - PSS/E case file (.sav) and dynamics file (.dyr) are available (Only applicable to PSSE models)
- Types of Models that can be validated:
  - Generators
  - Governors
  - Exciters
  - Stabilizers
- Software Used : PSS/E Version 33.4.0, Python 2.7

Generator Parameter Validation Process

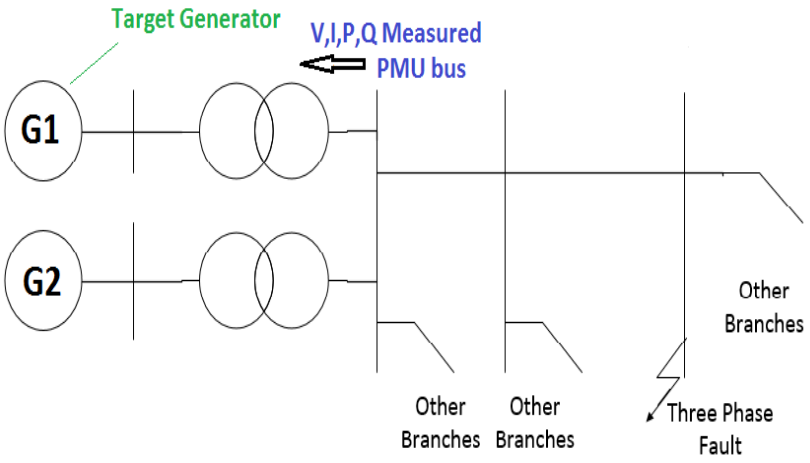


Steps :

1. Input Data – Obtain PMU event data and convert it into Excel file format (P,Q,V,Angle). Obtain the PSSE case file(.sav) and dynamics file(.dyr)
2. System Reduction- Reduce the system beyond the boundary bus (PMU bus) keeping the target generator bus and the boundary bus in the reduced system
3. Validate the measured response with model simulation
4. Trajectory Sensitivity Analysis – Compute sensitivities of P and Q flows to parameter change
   - Tabulate results
   - Plot results
5. Key Parameter Selection
   - User interaction to select key parameters from the sensitivity analysis for the optimization Pprocess
6. Optimization Process – Run the optimization process with the selected key parameters to identify the new model parameters
   - Tabulate results
   - Plot results

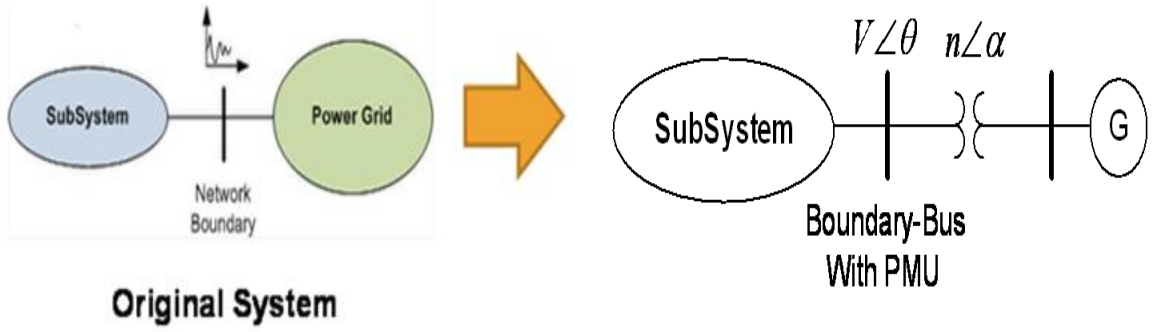
Input Data

- Obtain PMU data (V, I, P, Q) at the generator point of interconnection for an **event** as shown below
- Individual generator data is required. For example: for validating G1, data for the branch PMU bus – G1 should be obtained
- Extract the PMU data into the Excel file format as shown



T	V	Angle	P	Q
0	1.026683	24.728	-149.704	-109.731
0.026666	1.026683	24.728	-149.704	-109.731
0.059999	1.026683	24.728	-149.704	-109.731
0.093332	1.026682	24.72764	-149.708	-109.731
0.126665	1.02668	24.72699	-149.714	-109.731
0.159998	1.026678	24.72595	-149.722	-109.731
0.193331	1.026675	24.72445	-149.732	-109.732
0.226664	1.026671	24.72244	-149.741	-109.732
0.259997	1.026667	24.71987	-149.75	-109.733
0.29333	1.026662	24.71669	-149.757	-109.735
0.326663	1.026657	24.71289	-149.762	-109.738
0.359996	1.026652	24.70847	-149.763	-109.74
0.393329	1.026646	24.70344	-149.762	-109.743
0.426662	1.026644	24.69784	-149.758	-109.744
0.459995	1.026638	24.69175	-149.751	-109.749
0.493328	1.026637	24.6852	-149.743	-109.749
0.526661	1.026632	24.67833	-149.732	-109.753
0.559994	1.02663	24.67121	-149.721	-109.755
0.593327	1.02663	24.66394	-149.71	-109.756
0.626659	1.02663	24.65664	-149.7	-109.757
0.659992	1.026631	24.64941	-149.69	-109.757
0.693325	1.026632	24.64234	-149.682	-109.757
0.726657	1.026635	24.63551	-149.675	-109.756
0.75999	1.026637	24.62899	-149.671	-109.755
0.793323	1.026641	24.62283	-149.668	-109.754
0.826656	1.026647	24.61705	-149.667	-109.75

System Reduction



- An artificial generator and an ideal transformer are added at the boundary bus
- The turns ratio and the phase shift of the added transformer are adjusted to inject the measured voltage and angle signals at the boundary.
- The model of the generator is a classical generator model with zero internal reactance, very high inertia constant, and zero damping ratio.
- The transformer is a near zero impedance ideal transformer.
- This method allows for the dynamic simulation of a subsystem with measured signals injected at its boundary, without introducing errors caused by the external system model.

Validation

- Use the reduced system for event playback by injecting voltage and angle
- Compare measured P and Q with the simulated P and Q
- No calibration required if the models match
- Mismatch indicates calibration is required

Sensitivity Analysis

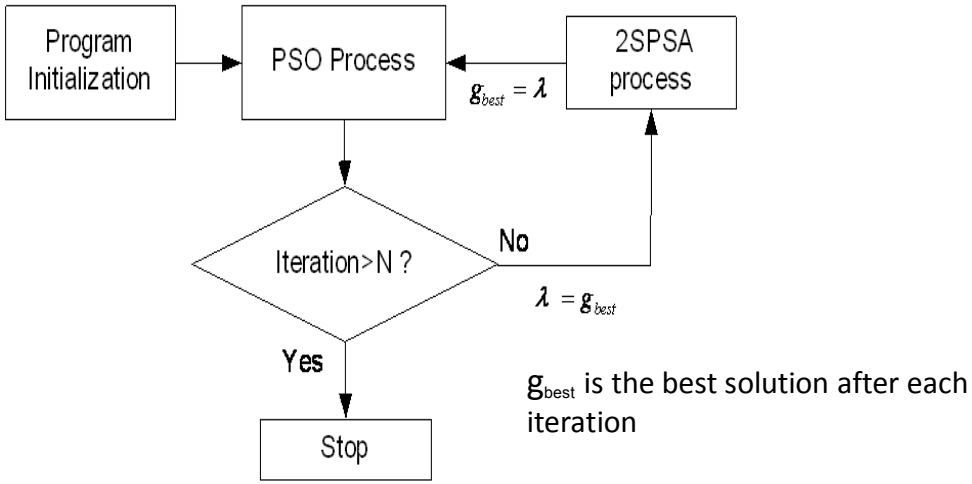
- The objective of sensitivity analysis is to identify the key parameters to be chosen for the validation process
- There are several parameters in generator unit's models, each parameter has a different influence on system response.
- The trajectory sensitivity analysis is carried out to understand the effect of each parameter on the simulation results.
- Sensitivity Analysis computes the sensitivity of P (active power) and Q (reactive power) flows by changing each parameter by a certain value(5%)
- Mean square error (MSE) of P and Q is used as an index for the sensitivities, and the analysis identifies parameters having sensitivity above a threshold value

$$\Delta P(t) = \frac{\partial P(t)}{\partial X_0}\Delta X_0 = P_{X_0}(t)\Delta X_0$$

$$\Delta Q(t) = \frac{\partial Q(t)}{\partial X_0}\Delta X_0 = Q_{X_0}(t)\Delta X_0$$

Optimization Process

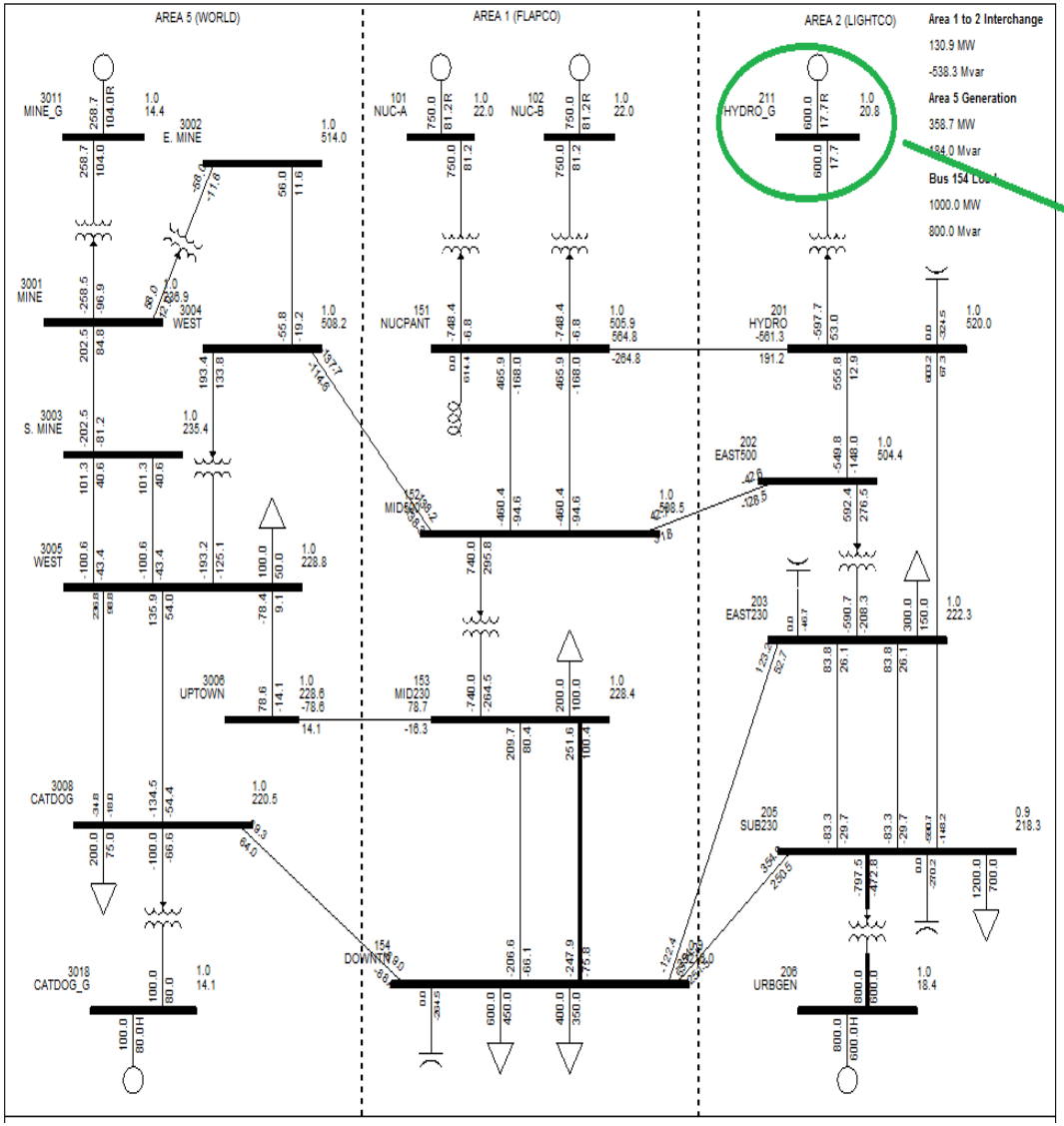
- Optimization objective is to fit the simulation curves with the measured curves by adjusting the model parameters and identify the new model parameter values
- Two algorithms are used for the optimization process:
  - Particle Swarm Optimization (PSO)
  - Simultaneous Perturbation Stochastic Approximation (SPSA)–PSO
- PSO is not affected by initial guess and has global search ability but the convergence rate is slow
- SPSA is a gradient based algorithm which steers the particle to the right direction and has better convergence
- A new intelligent optimization method SPSA-PSO cooperative method is used to obtain a combination of global search ability and better convergence. SPSA drives the results of PSO for faster convergence.



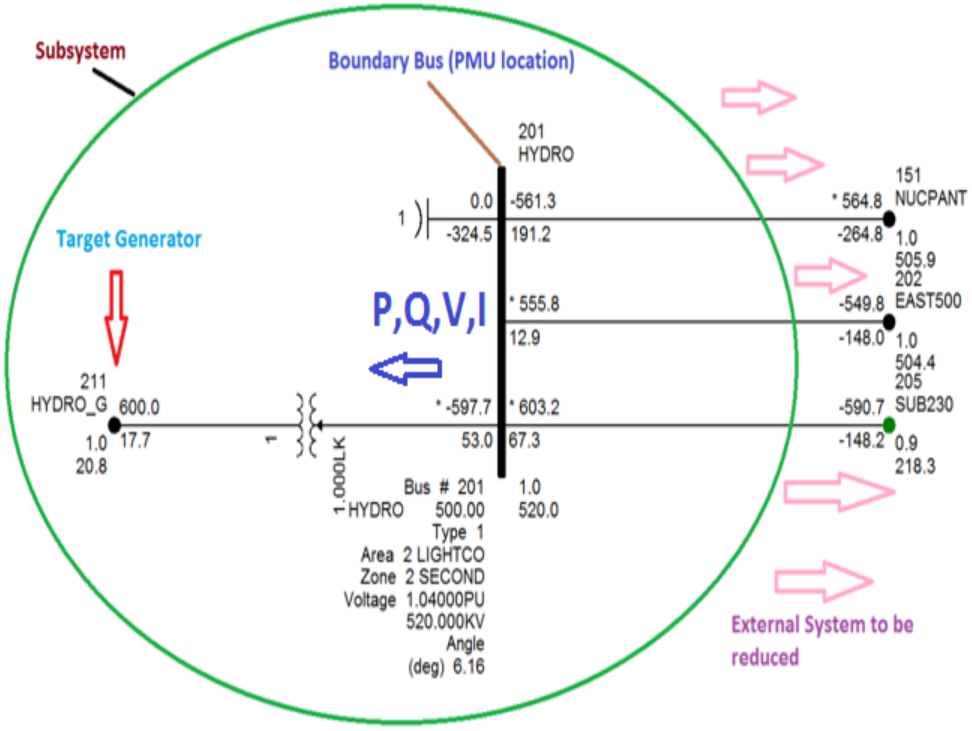
g_{best} is the best solution after each iteration

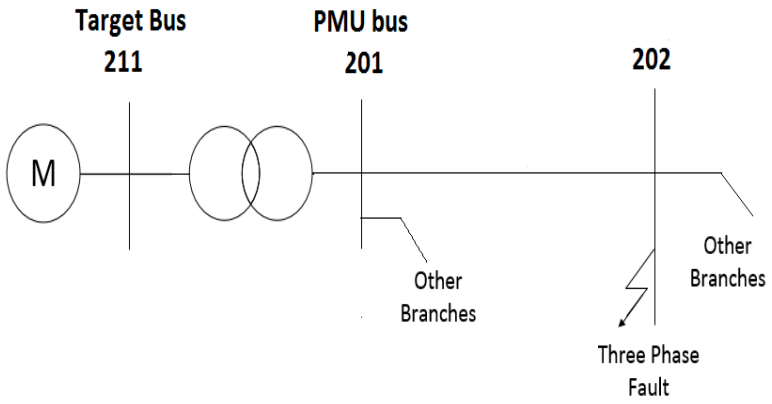
EXAMPLE

PSSE Example Case savnw.sav



Bus Display View





Event description : 3 phase bus fault at bus no: 202 at t=1 sec , fault cleared at t =1.08 sec and system is run to 5 sec

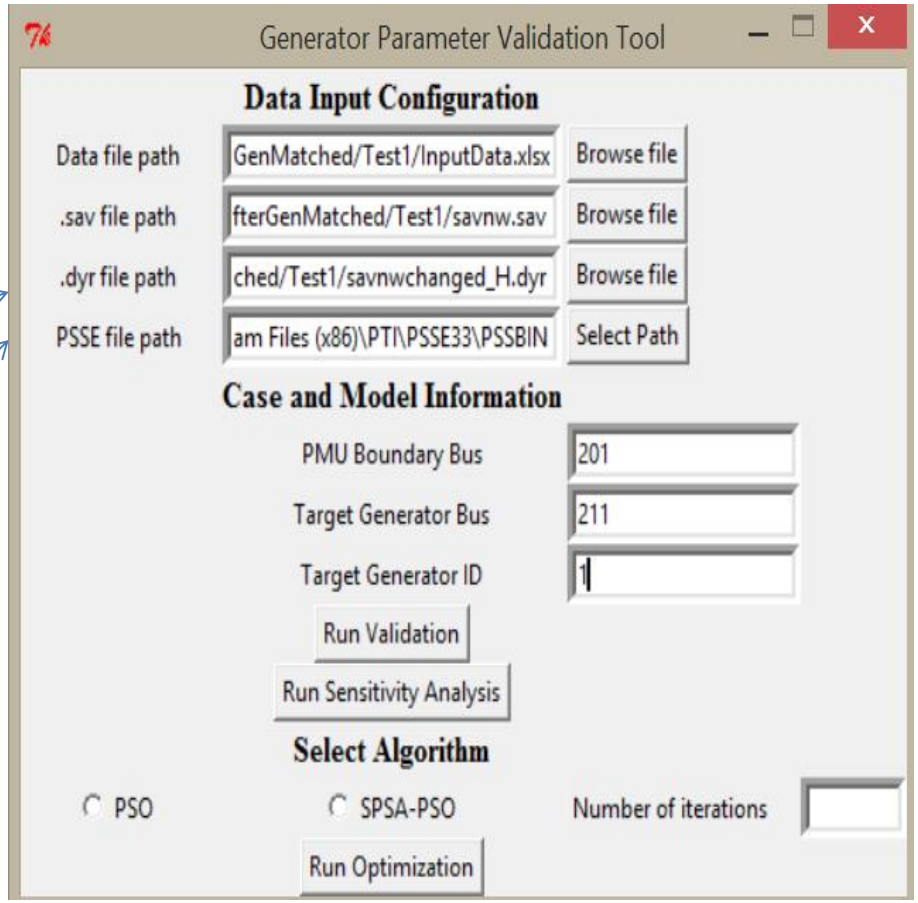
Run GPV Tool

Input data file (.xlsx)

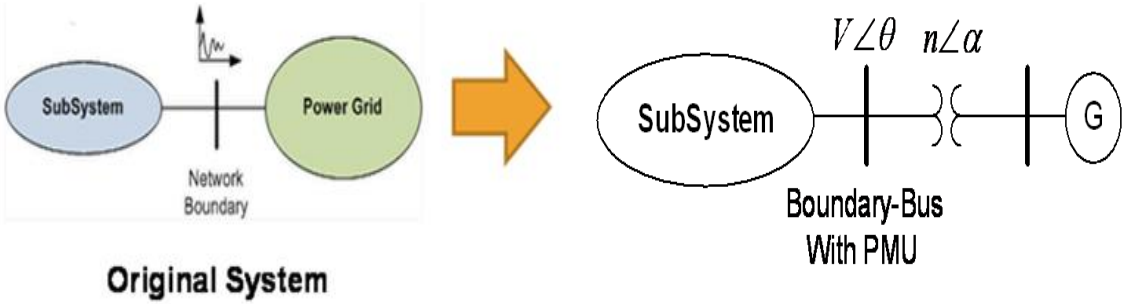
PSSE case file (.sav)

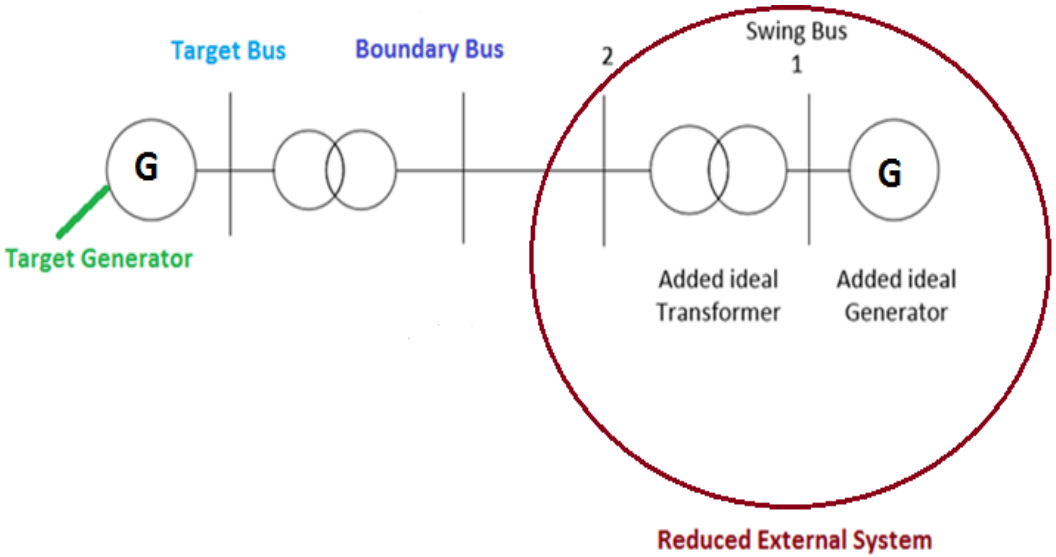
PSSE dynamics file(.dyr)

Path to PSSE PSSBIN folder containing python modules

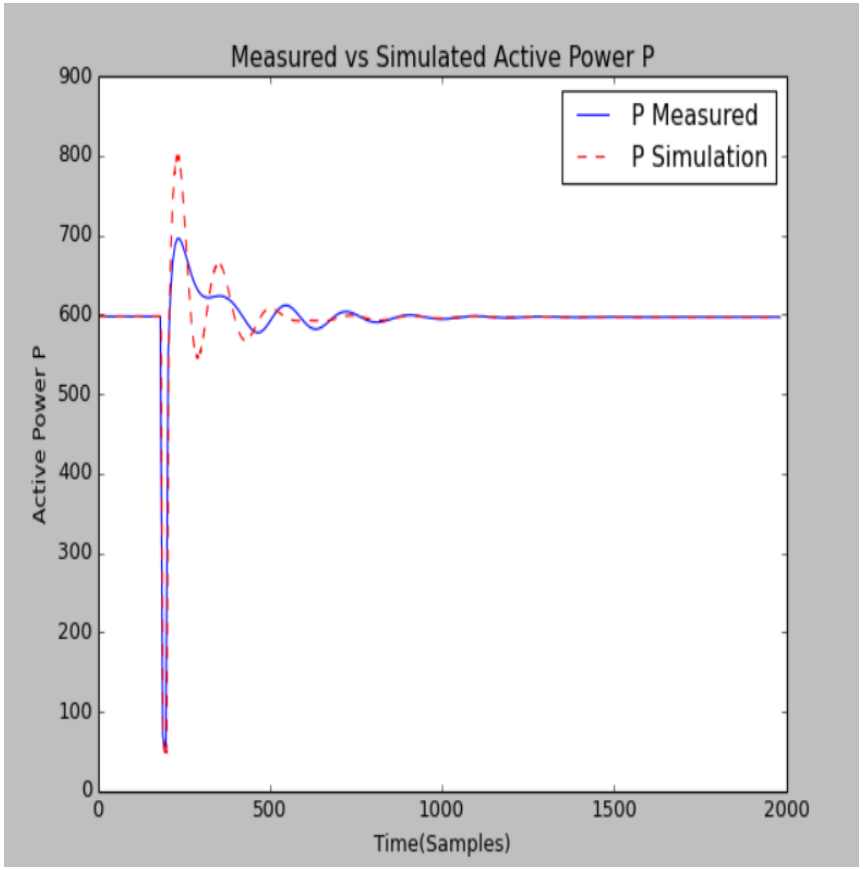


Automated System Reduction

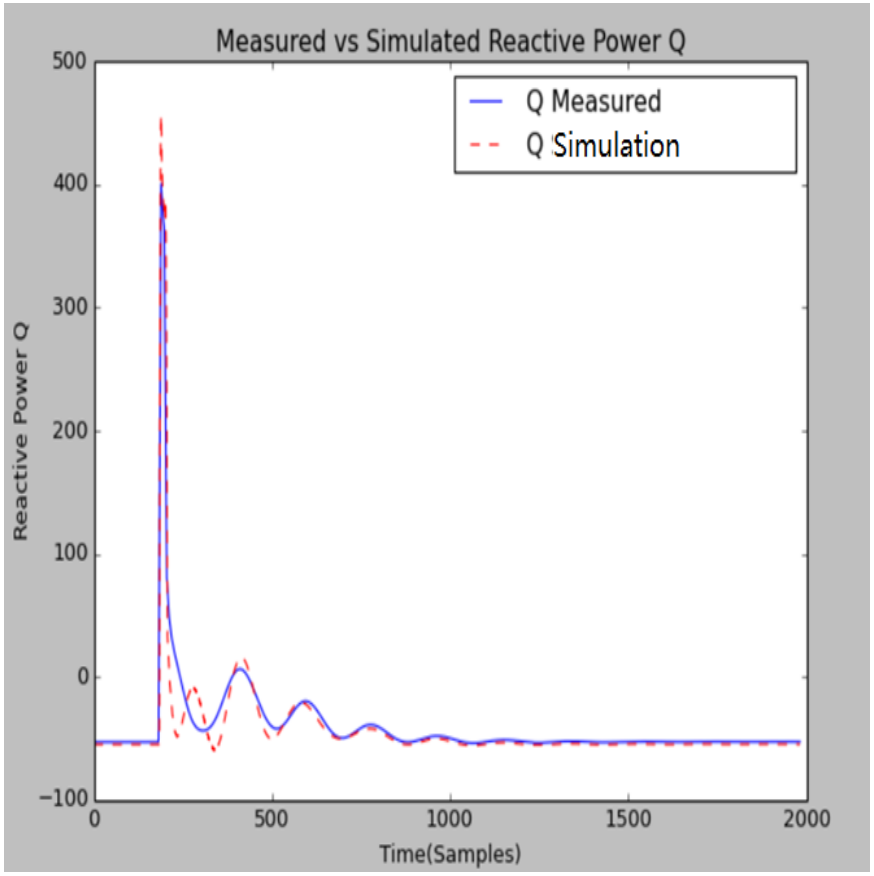




Validation Plots



Active Power (P)

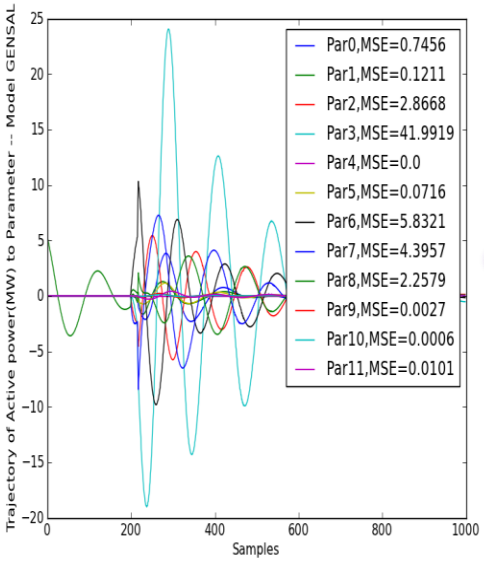


Reactive Power (Q)

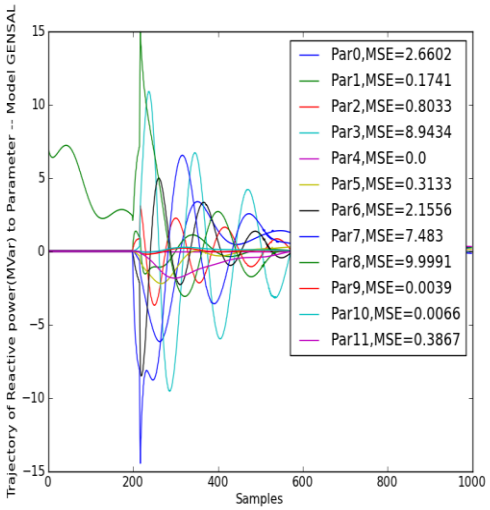
Sensitivity Analysis- Identify Key Parameters

Sensitivity Analysis/Parameter Selecti...

Parameter	MSE-P	MSE-Q	Ranks		Min	Max
GENSAL- Par 0	0.3562	1.19294	7	☐		
GENSAL- Par 1	0.05373	0.07745	14	☐		
GENSAL- Par 2	1.4388	0.39999	6	☐		
GENSAL- Par 3	19.1313	3.89948	1	☑		
GENSAL- Par 4	0.0	0.0		☐		
GENSAL- Par 5	0.02824	0.13205	12	☐		
GENSAL- Par 6	3.02644	1.10927	4	☐		
GENSAL- Par 7	1.79128	3.23443	3	☐		
GENSAL- Par 8	0.95289	4.44052	2	☐		
GENSAL- Par 9	0.00129	0.00177	22	☐		
GENSAL- Par 10	0.00028	0.00267	21	☐		
GENSAL- Par 11	0.00419	0.16833	11	☐		
HYGOV- Par 0	0.00021	3e-05	25	☐		
HYGOV- Par 1	0.01525	0.00142	17	☐		
HYGOV- Par 2	0.0012	6e-05	23	☐		
HYGOV- Par 3	0.00402	0.00028	20	☐		
HYGOV- Par 4	0.00805	0.00125	19	☐		
HYGOV- Par 5	0.01905	0.00096	16	☐		
HYGOV- Par 6	0.0	0.0		☐		
HYGOV- Par 7	0.0	0.0		☐		
HYGOV- Par 8	0.0088	0.00104	18	☐		
HYGOV- Par 9	0.02207	0.00282	15	☐		
HYGOV- Par 10	0.00074	0.00016	24	☐		
HYGOV- Par 11	0.00012	2e-05	26	☐		
SCRX- Par 0	0.11311	1.13153	8	☐		
SCRX- Par 1	0.00683	0.49723	9	☐		
SCRX- Par 2	0.12592	0.42198	10	☐		
SCRX- Par 3	0.01961	0.12695	13	☐		
SCRX- Par 4	0.0	0.0		☐		
SCRX- Par 5	0.44422	1.58719	5	☐		
SCRX- Par 6	0.0	0.0		☐		
SCRX- Par 7	0.0	0.0		☐		



Trajectory of Pnew-Pold for GENSAL model parameters



Trajectory of Qnew-Qold for GENSAL model parameters

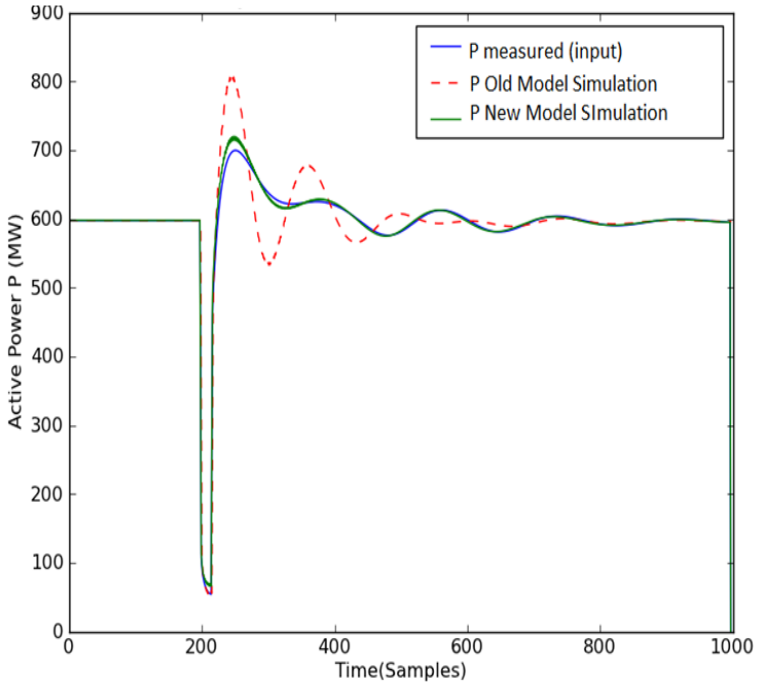
Note:
Pnew = Active Power flow for original model parameter value
Qnew = Reactive Power flow for original model parameter value
Pold/Qold = Active Power/Reactive Power flow for a 5% increase in the corresponding parameter value
*Key Parameter column based on a sensitivity threshold of 0.01

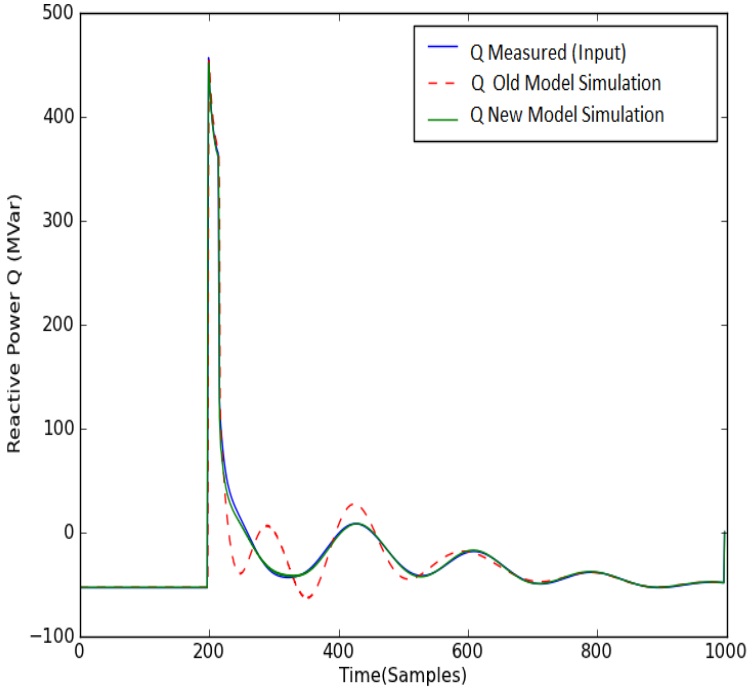
Optimization Results - Identified Parameter Values

Parameter Validation Results

Model	Parameter	Old Value	New Value
Model-GENSAL	Par- 2	0.239999994636	0.168001055427
Model-GENSAL	Par- 3	4.0	4.6727793482

Parameter	Constant Description
GENSAL Parameter 2	T''qo (sec)
GENSAL Parameter 3	H, Inertia

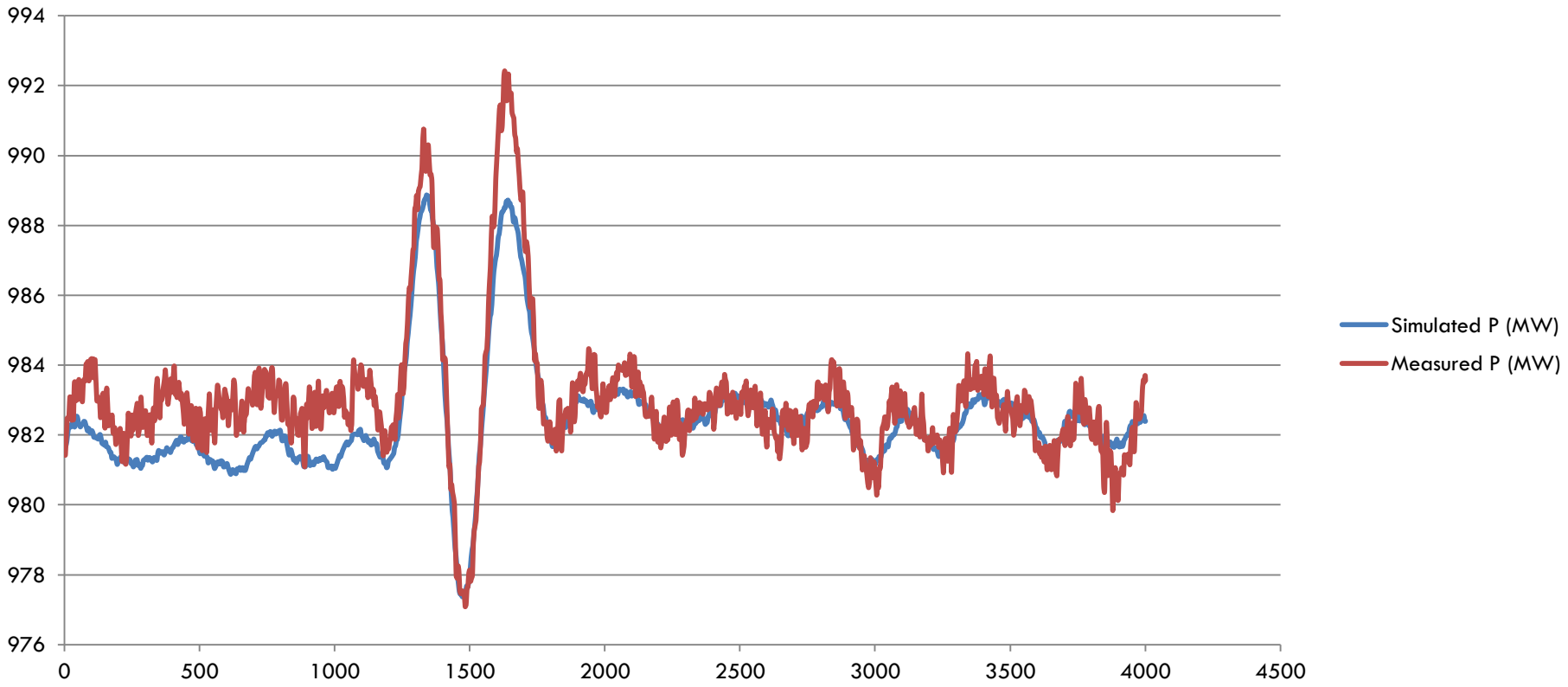




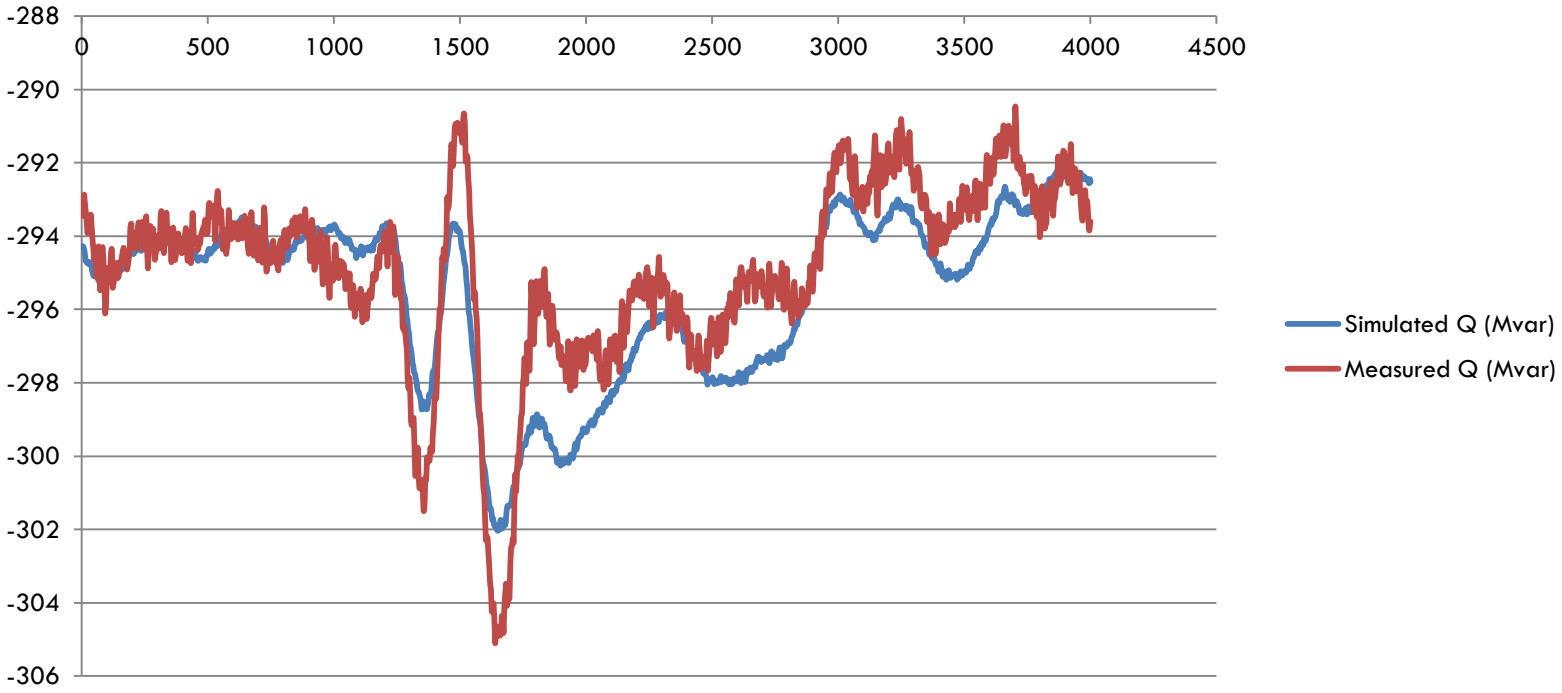
Testing on Real Data

- The tool was tested on data sets obtained from an electric utility
- Data obtained:
  - PMU recorded voltage and current phasors at the output of a generator corresponding to an event
  - PSS\E Model data – case file and dynamic file
- Performed validation on generator, exciter, governor, and stabilizer models

Validation - Real Power (P)



Validation – Reactive Power (Q)



Best Practices

- Use individual branch data to validate and calibrate individual generators
- Obtain input data covering the dynamics during the event
- Select key parameters that have highest P,Q sensitivity (Example:top 5)→ Check the results→ Change key parameters selection→ Check Results→ Narrow down on key parameters and fine tune parameter values
- Specify maximum and minimum range for the parameters to restrict their variation (based on knowledge about the parameters)
- Use multiple runs for the same generator-event case and multiple events for the same generator to tune results

Limitation and Area of Improvement

- Limitation:
  - Applicable for PSS\E models
  - Processing time increases with length of input data and number of iterations
- Area of Improvement:
  - Update code to correct for offset due to system reduction
  - Update code to correct for any initial transient
  - Update code to unwrap angles before interpolation to avoid periodic transients

Summary

- Built the user interface to
  - Accept input data
  - Automate system reduction process
  - Perform validation to evaluate the need for calibration
  - Perform sensitivity snalysis to identify key parameters
  - Restrict parameter variation by adding upper and lower bounds on the parameter values
  - Calibrate the models using an optimization process and display identified parameter values
- Next Steps
  - Obtain recorded event data at the output of individual generators
  - Obtain model data for the generators
  - Test the tool to validate and calibrate on additional data sets

Thank You.

Any questions ?

Neeraj Nayak

nayak@electricpowergroup.com

Electric Power Group

Attachment 14. Use Cases with Sample Events

Synchrophasor Technology – PMU Use Case Examples

John W Ballance - EPG

Prashant C Palayam – EPG

Sarma (NDR) Nuthapalati - ERCOT

November 5, 2014

Prepared for CCET DAT Synchrophasor Team

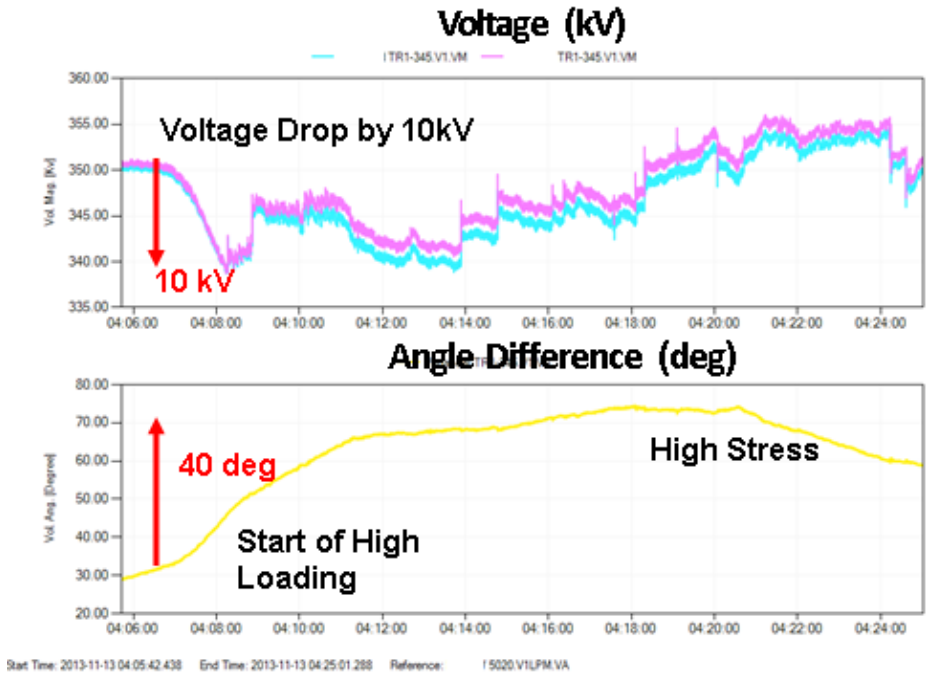
Use Case Overview

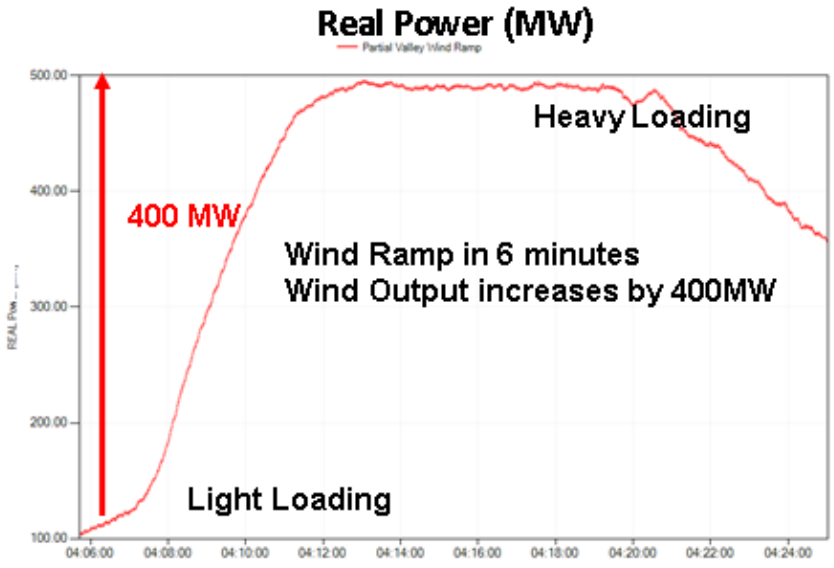
Use Case	Grid Scope	Streaming 30 samples/sec	Slow Speed 3 samples/min	Local Event Capture	Example of Application on ERCOT Grid
High Stress Across System (High Phase Angle) Observed	Wide Area	Yes	Yes		High Phase Angle from Valley - November 13, 2013
Small Signal Stability – Damping is Low	Wide Area	Yes			Control system oscillations from wind plant - January 9, 2014
Small Signal Stability – Emerging Oscillation Observed	Wide Area and Local	Yes			Slow System Oscillation Detected October 12,2014
Voltage Oscillation Observed	Regional	Yes			Wind Control System Oscillations in Valley - April 12-13, 2013
Voltage Instability Monitoring (real-time P-V or Q-V curve)	Regional	Yes			High Phase Angle in Valley - November 13, 2013
Detection of Subsynchronous Interactions (Not necessarily resonance, just below 60 Hz)	Local Regional	Yes			
Integrate PMU Data Into State Estimator	Wide Area	Yes	Yes		Baselining Study confirmed correlation between PMU and State Estimator data
System Disturbance – Capture and Interpretation	Regional	Yes	Yes, not high resolution	Yes	Enhanced Event Analysis Capabilities - including control system performance diagnostics
Generator Parameter Determination	Local	Yes		Yes	Wind plant oscillation and trip following line outage - September 2011, reported in 2012 IEEE PES paper
Major Load Parameter Determination	Local	Yes		Yes	
PMU-Based Fault Location	Local Regional	Yes		Yes	
Phase Angle Across Breaker for Reclosing Action		Yes	Yes		ERCOT operating studies identify need for monitoring phase angles
Subsynchronous Resonance Identification and Mitigation (PGRR027)	Regional	Yes			
Transmission Characteristics Determination	Regional	Yes		Yes	
Dynamic Transmission Line Ratings using PMU monitoring	Regional	Yes			
Validation of Control Devices (e.g. SVC) performance	Regional	Yes		Yes	

Use Case - High Stress Across System (High Phase Angle) Observed

- **Need:** PMU phase angle data can advise the Shift Engineer about the measured angle across wide area to provide early warnings on high power flow (high grid stress)
- **EXAMPLE: HIGH PHASE ANGLE AT COAST 3 (VALLEY) – NOV 13, 2013**
- **Possible Action:**
- Shift Engineer reviews high phase angle, and examines possible consequences if an event aggravates this.
  - Online TSAT Study
  - Online VSAT study
  - Online Power flow study
- Shift Engineer may recommend action to shift supervisor
  - Impose transfer limit
  - Adjust generation pattern

Event Analysis – Impact of High Wind on System Performance Following Wind Ramp



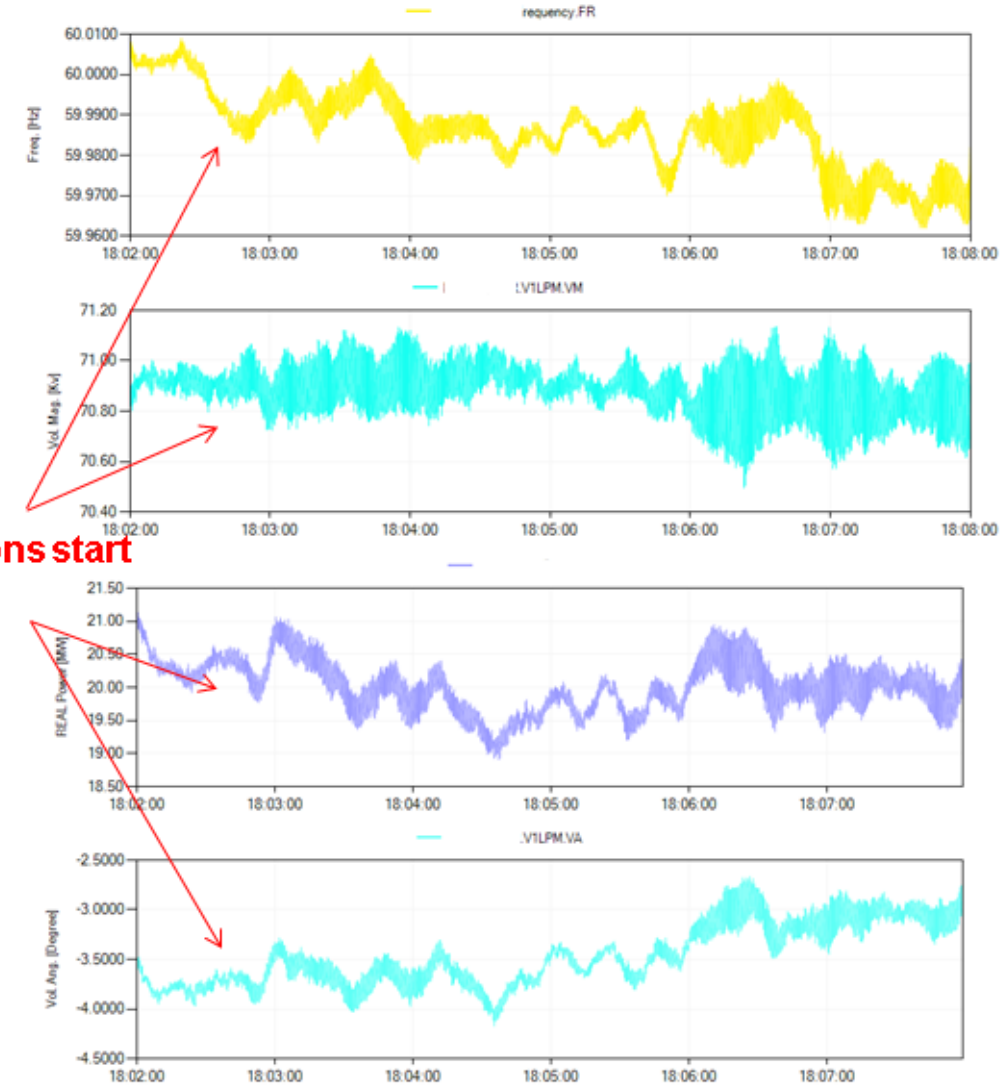


Reference Angle: North 7

Use Case - Small Signal Stability – Low Damping

- **Need:** PMU data can advise the Shift Engineer about both known and unknown oscillations at location/s
- **EXAMPLE: CONTROL SYSTEM OSCILLATIONS FROM WIND PLANT – JANUARY 9, 2014**
- **Possible Action:**
- Shift engineer should review
  - Oscillatory frequency & damping
  - Determine type of oscillation (inter-area such as 0.6Hz North-South mode, local control system such as 3.2Hz at West 10)
- Shift Engineer may recommend action to shift supervisor
  - Reduce transfer out of area
  - Reduce generation output
  - Revert control system settings to original value and restore output

PMU Data Illustrates Oscillation With Low Damping



Oscillations start sharply

Frequency (Hz)

Voltage (kV)

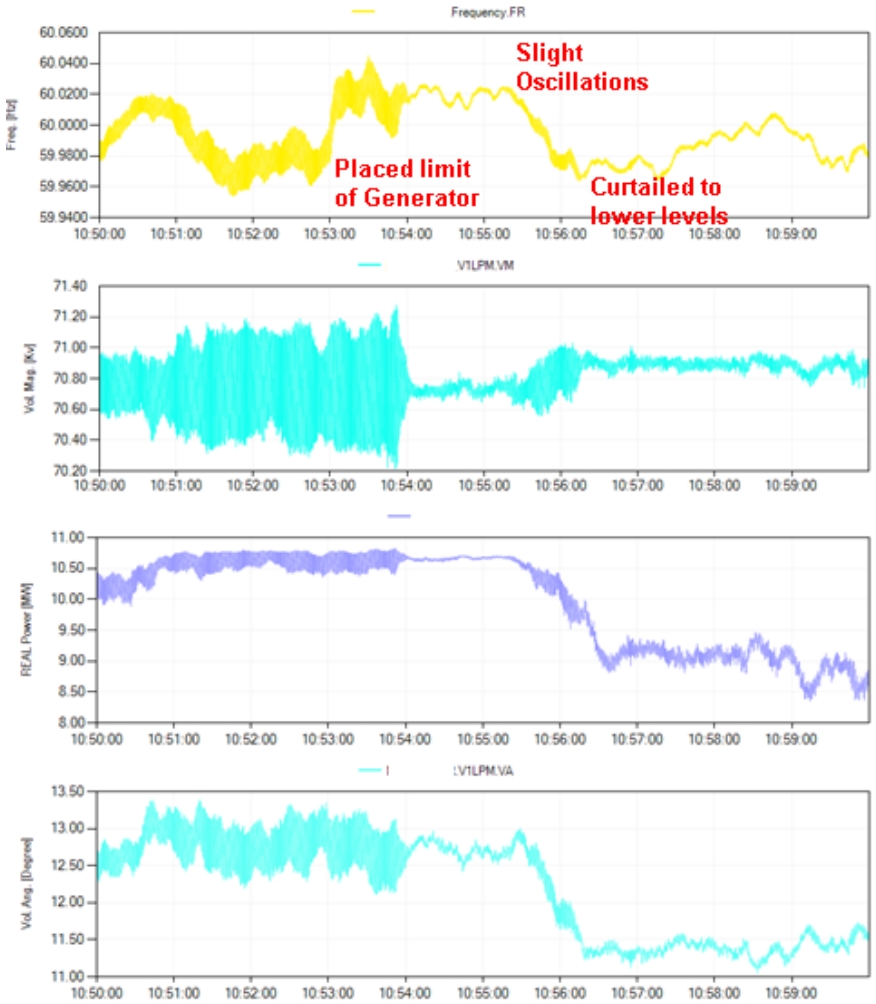
Real Power MW)

Angle Difference (deg)

Reference Angle: North 7

Phasor Grid Dynamic Analyzer (PGDA) plots

PMU Data Illustrates Oscillation With Low Damping



Frequency (Hz)

Voltage (kV)

Real Power MW)

Angle Difference (deg)

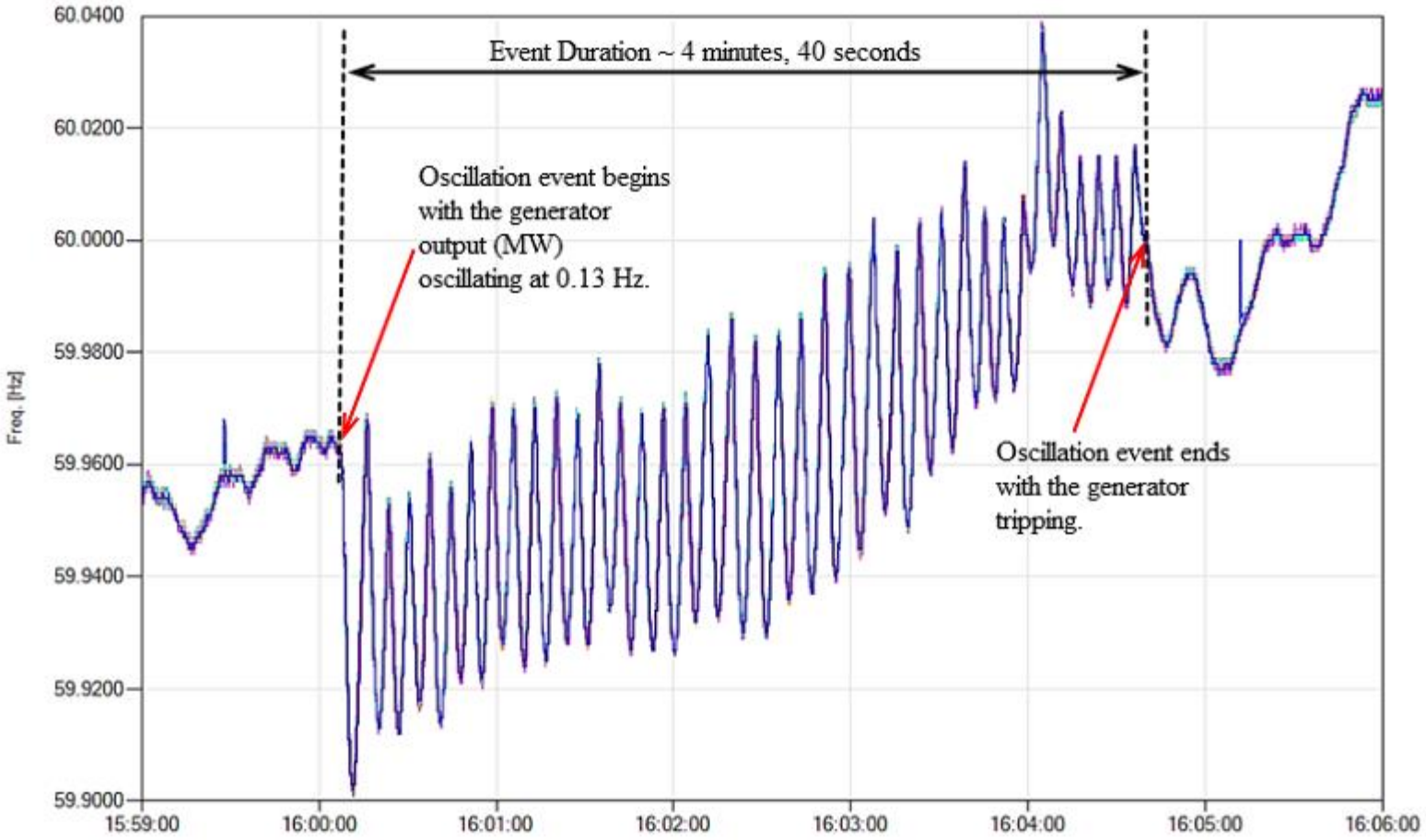
Reference Angle: North 7

Phasor Grid Dynamic Analyzer (PGDA) plots

Use Case - Small Signal Stability – Emerging Oscillation Observed

- **Need:** PMU data can advise the Shift Engineer about both known and unknown oscillations at location/s
- **EXAMPLE: SYSTEM-WIDE OSCILLATIONS FOLLOWING LOSS OF GENERATION – OCTOBER 12, 2014**
- **Possible Action:**
- Shift engineer should review
  - Oscillatory frequency & damping
  - Determine type of oscillation (e.g. inter-area such as 0.6Hz North-South Mode or Local Control system such as 3.2Hz at West 10)
- Shift Engineer may recommend action to shift supervisor
  - Reduce transfer out of area
  - Reduce generation output
  - Block control system (to eliminate control system-driven oscillations)

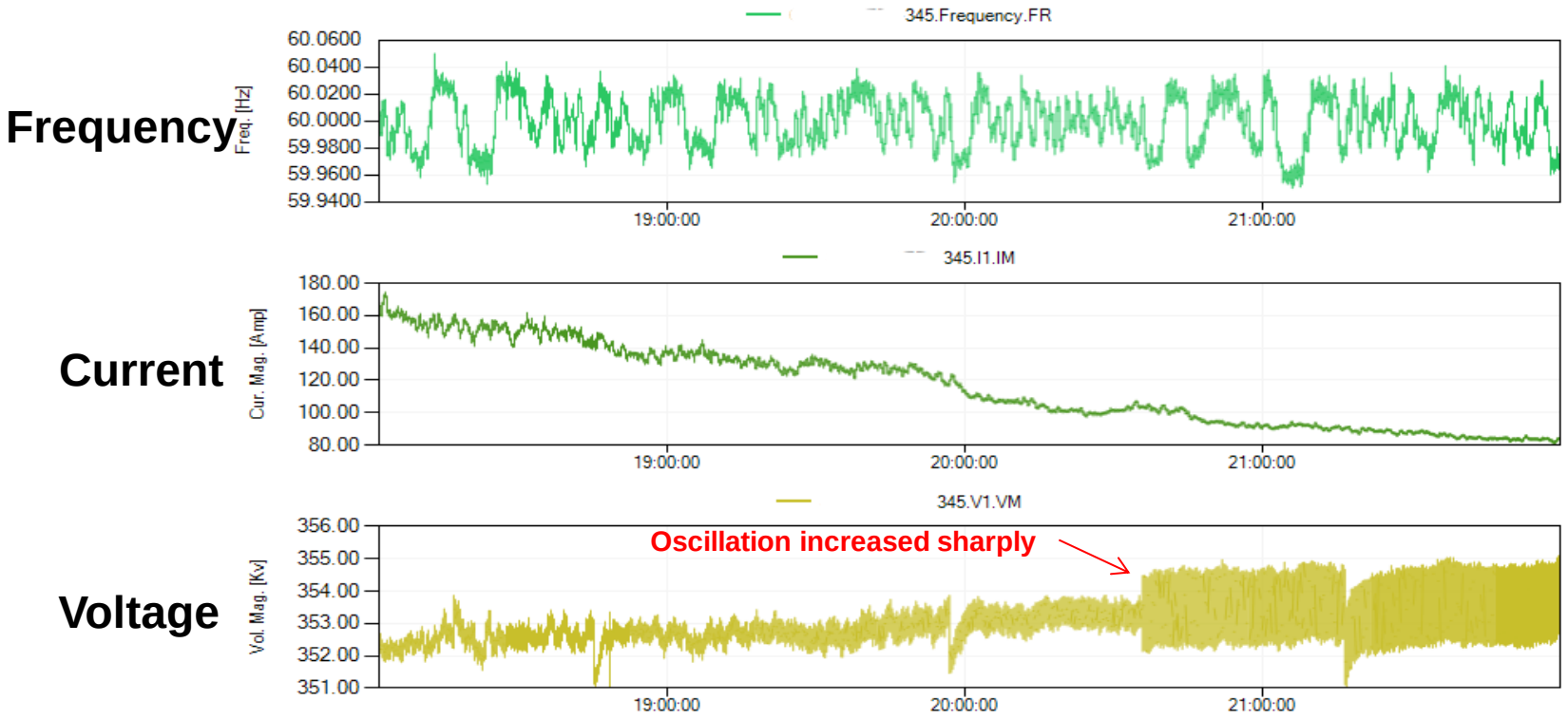
PMU Data Illustrates Emerging Oscillation



Use Case - Voltage Oscillation Observed

- **Need:** PMU voltage phasor can advise the Shift Engineer about the voltage oscillations at location/s due to fast voltage controllers at wind generators and other control devices in the grid
- **EXAMPLE: VOLTAGE CONTROL OSCILLATIONS FROM NEARBY WIND PLANT – APRIL 12-13, 2013**
- **Possible Action:**
- Shift engineer should review location for possible causes
  - Low strength area (weak grid or low circuit ratio)
  - Incorrect settings on voltage controllers/voltage regulators
- Shift Engineer may recommend action to shift supervisor
  - Reduce transfer out of area
  - Reduce generation output
  - Restore outages

Nearby PMU Detects Voltage Oscillation

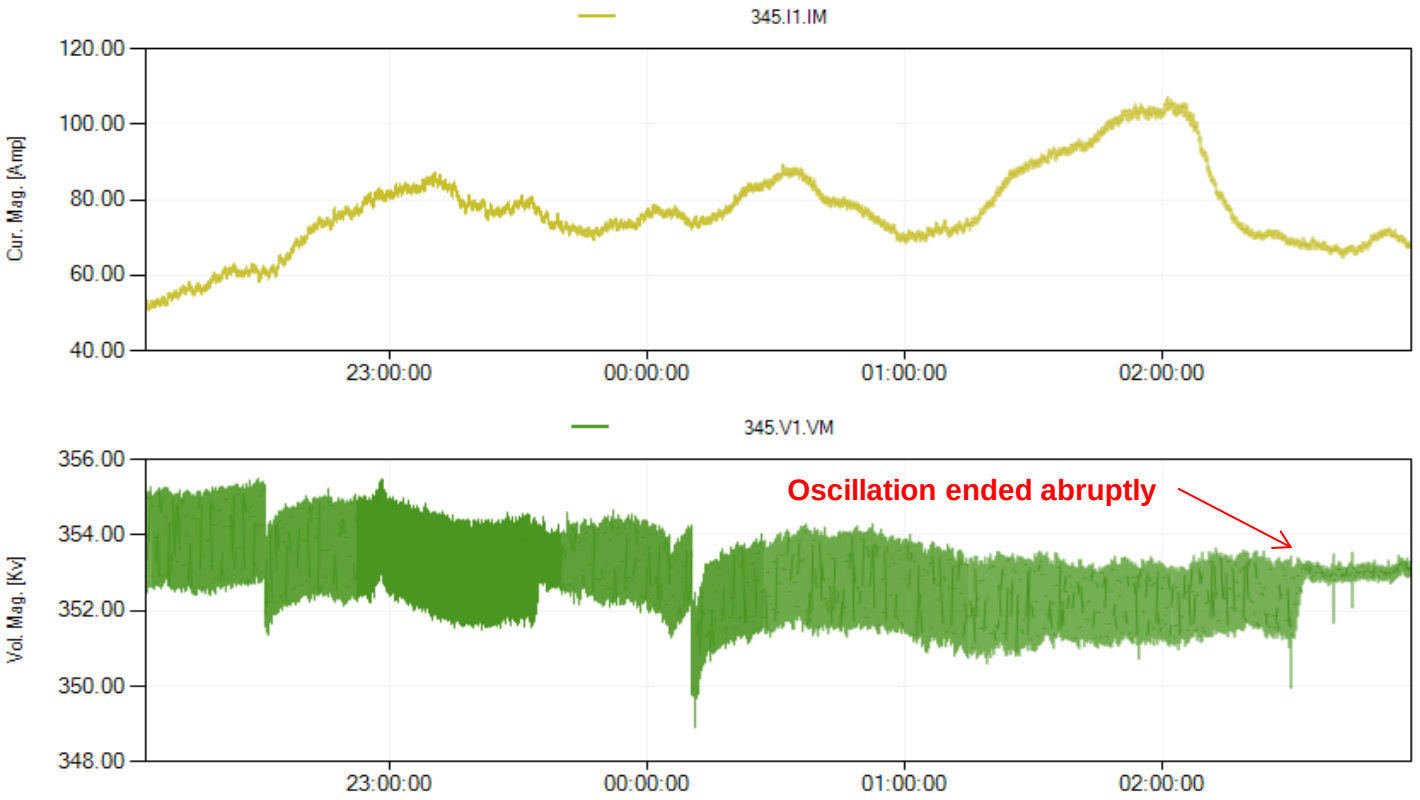


Screenshot of PGDA (Phasor Grid Dynamics Analyzer)

Nearby PMU Detects Voltage Oscillation

Current

Voltage



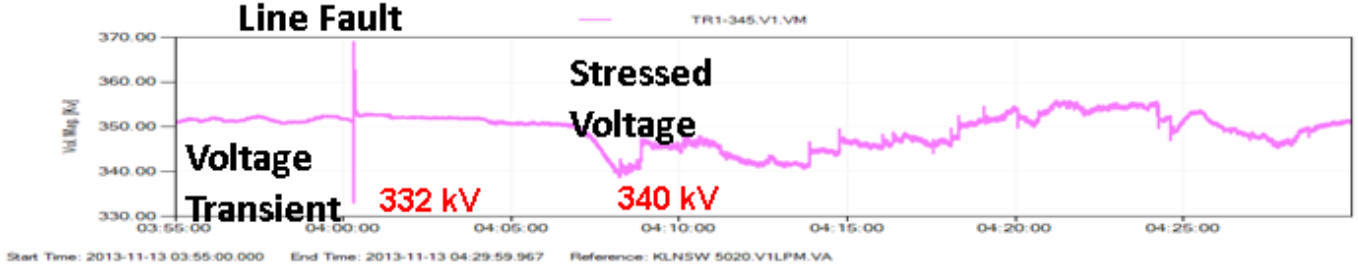
Screenshot of PGDA (Phasor Grid Dynamics Analyzer)

Use Case - Voltage Instability Monitoring (P-V, Q-V)

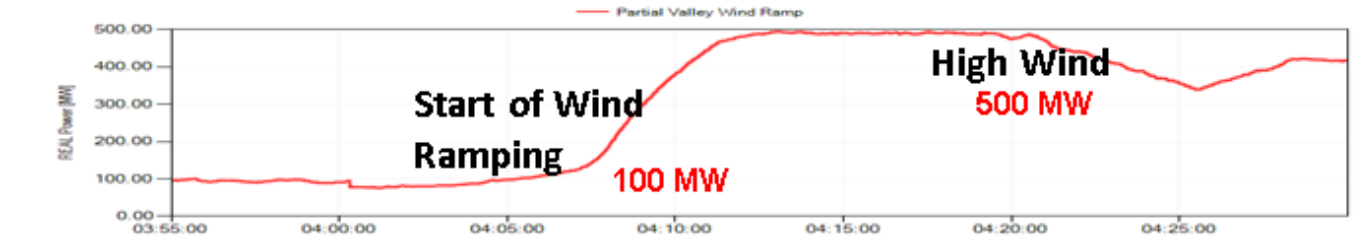
- **Need:** PMU data (real, reactive power and voltage) can advise the Shift Engineer indirectly on high grid stress under low voltage deteriorating conditions
- **EXAMPLE: HIGH PHASE ANGLE AT COAST 3 (VALLEY) – NOV 13, 2013**
- **Possible Action:**
- Shift Engineer reviews P-V performance, compares to online VSAT study
- Shift Engineer may recommend action to shift supervisor
  - Impose transfer limit
  - Adjust generation pattern
- Operations planning studies and benchmarking will be required to identify critical substations for voltage instability monitoring

PMU Data Illustrates Voltage Stress During Power Ramp

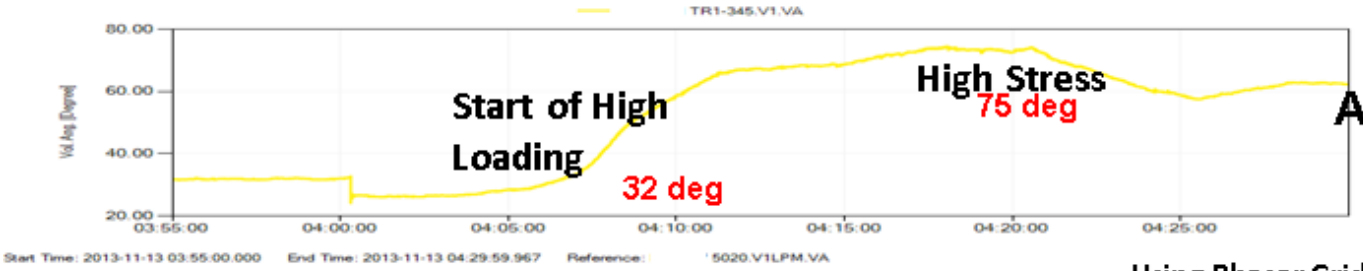
Frequency (Hz)



Voltage (kV)



Real Power MW)



Angle Difference (deg)

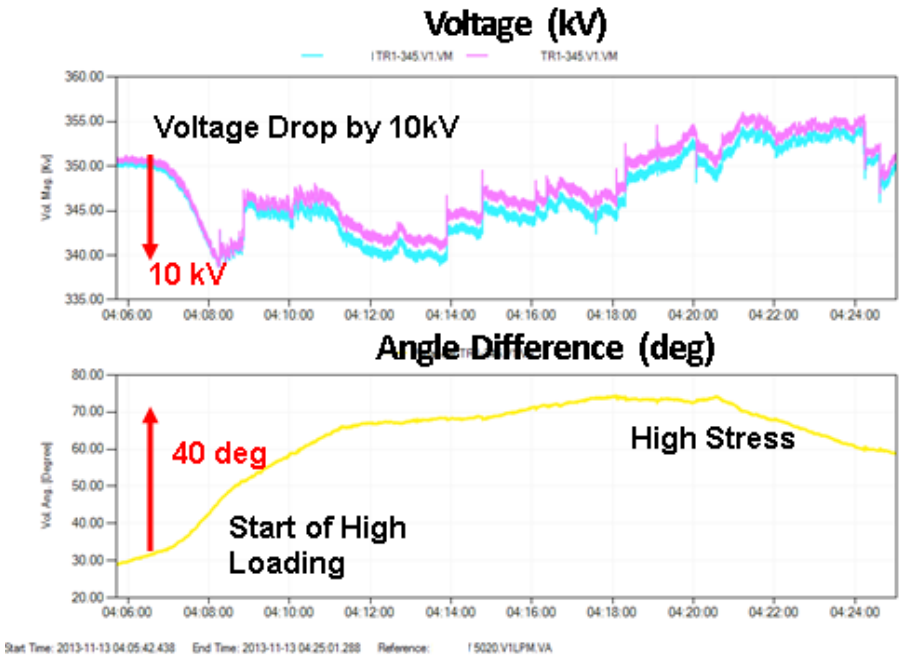
Start Time: 2013-11-13 03:55:00.000 End Time: 2013-11-13 04:29:59.967 Reference: KLNSW 5020.V1LPM.VA

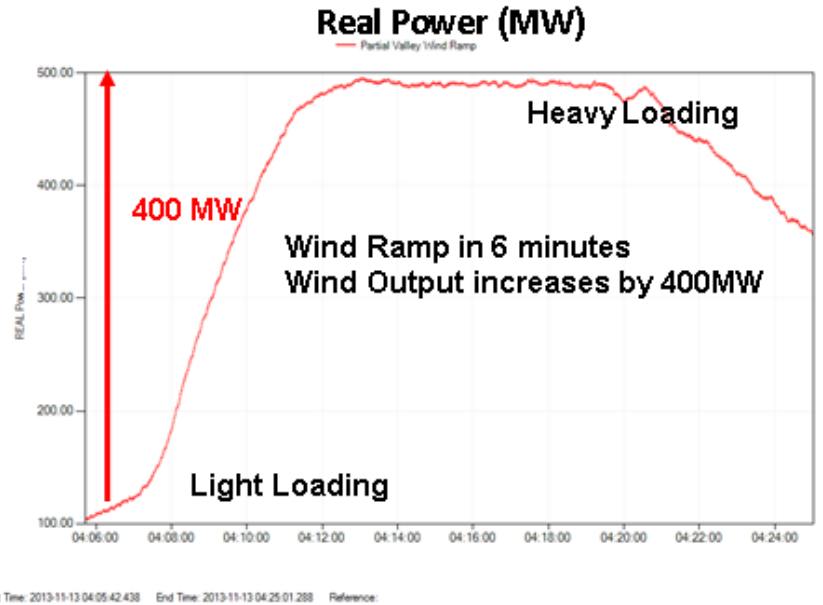
Start Time: 2013-11-13 03:55:00.000 End Time: 2013-11-13 04:29:59.967 Reference: 5020.V1LPM.VA

Reference Angle: North 7

Using Phasor Grid Dynamic Analyzer (PGDA) plots

PMU Data Illustrates Voltage Stress During Power Ramp





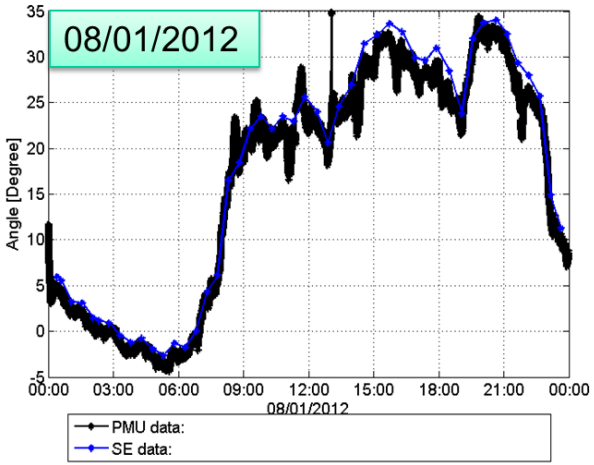
Reference Angle: North 7

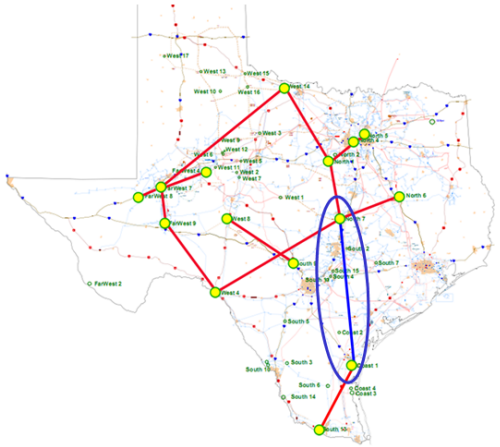
Use Case - Validate State Estimator Results Used in Control Rooms

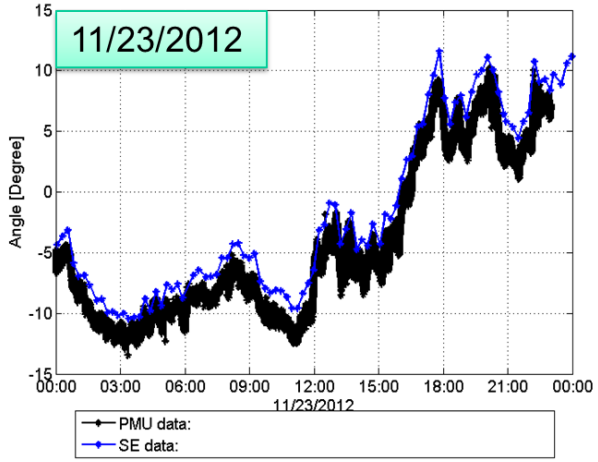
- **Need:** PMU phase angles can be used to validate the state estimator results used in control rooms (locate differences which reflect anomalies in models used for state estimation)
- **EXAMPLE: BASELINING STUDIES**
- Possible Action:
  - Identify the root cause for the mismatch and update models

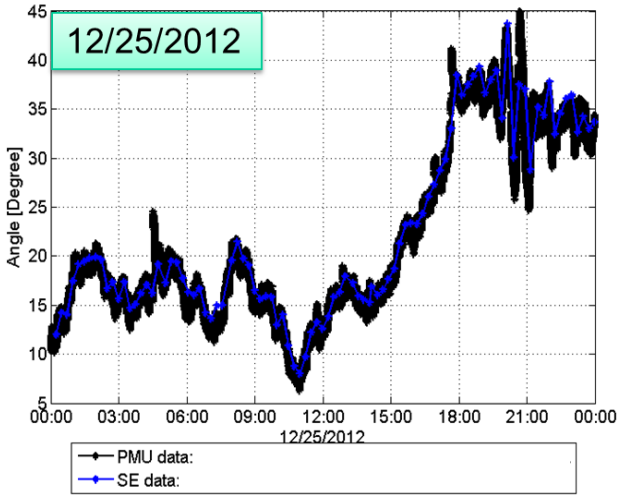
PMU Data vs SE Data Comparison

Coast 1-North 7









Use Case - System Disturbance – Cause & Interpretation

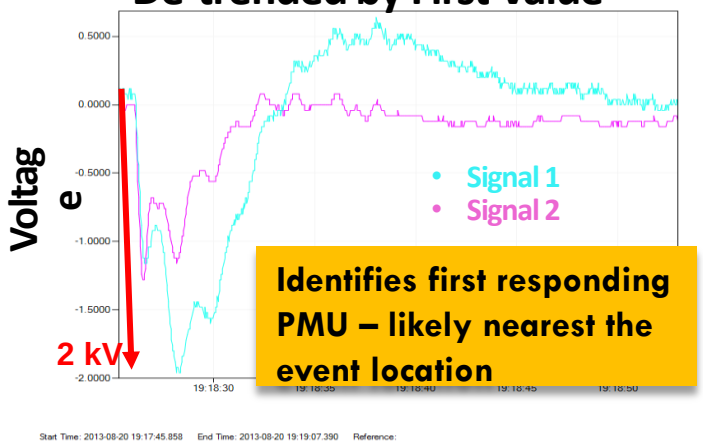
- **Need:** PMU data is useful for event analysis and determine root cause of the event and its location.
- **EXAMPLE: EVENT SIGNATURES OF GENERATION TRIP, LINE TRIP & OSCILLATIONS**
- **Possible Action:**
  - Shift Engineer reviews network performance, including frequency dip and recovery, voltage dip and recovery, power dip (and phase angle) and recovery, and any transient oscillations and the associated ring-down characteristics
  - If recovery looks slow, refers to Advanced Network Applications expert or System Planning dynamics expert to determine if some action is recommended, or for further review
  - If frequency, voltage, or power (and phase angle) dip looks too large or too small, or does not return to expected levels, refer to Advanced Network Applications expert or System Planning dynamics expert to investigate the reasons for abnormal grid responsiveness
  - Frequency response and/or transient voltage response of generation (including wind, solar, and conventional generation) should be monitored for compliance with standards
  - Should include an automatic reporting capability, providing a high-level review of the network performance

PMU Data Enables Effective Post-Event Analysis

Event Analysis

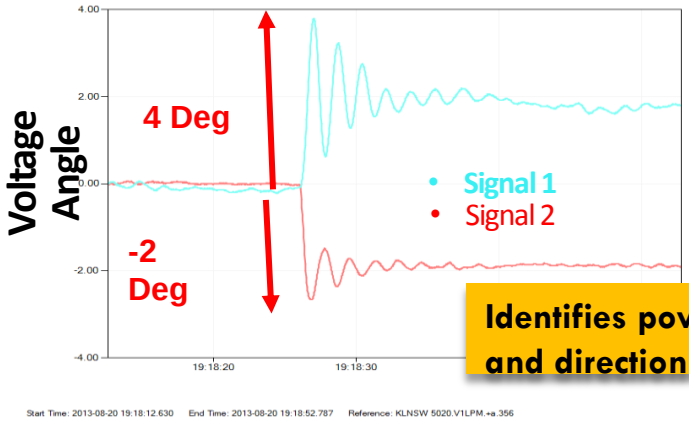
NERC-defined A, B and C Frequency
A – 60.004 Hz
B – 59.924 Hz
C – 59.893 Hz

De-trended by First Value



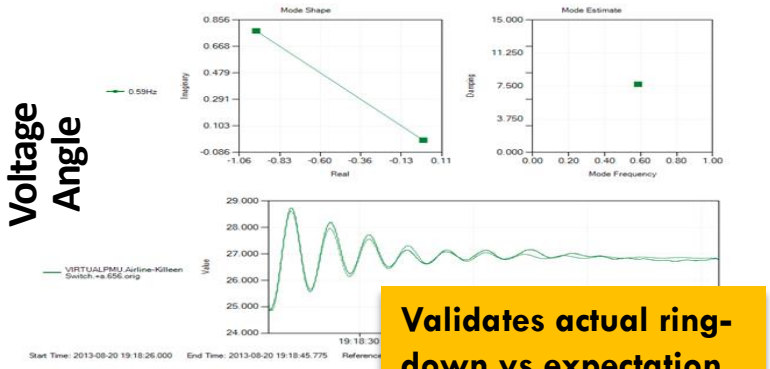
Identifies first responding PMU – likely nearest the event location

De-trended by First Value



Identifies power transfer and direction

Ringdown Analysis



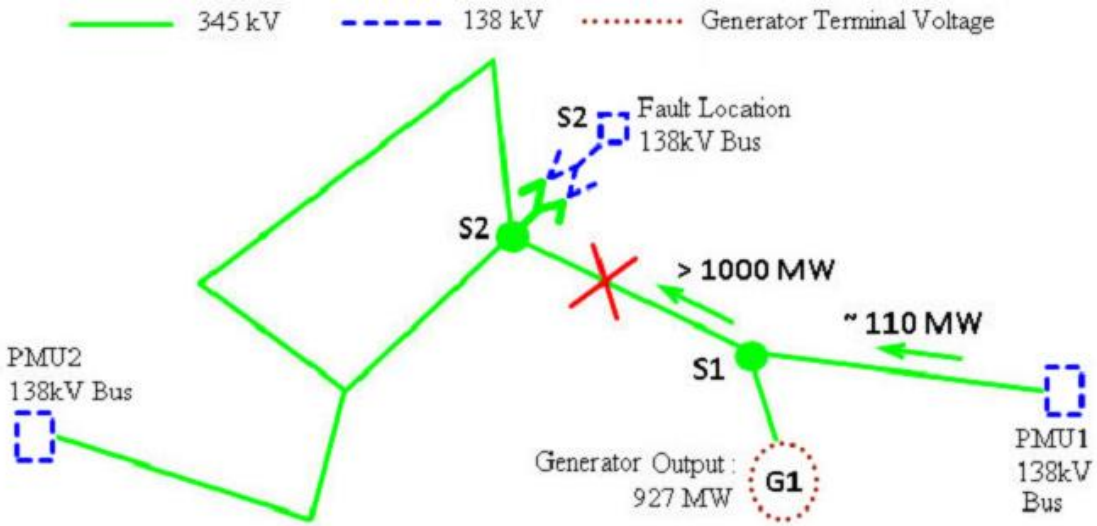
Validates actual ring-down vs expectation

PGDA used for analysis

PMU Data Enables Effective Post-Event Analysis – Power Load Unbalance Circuit Example

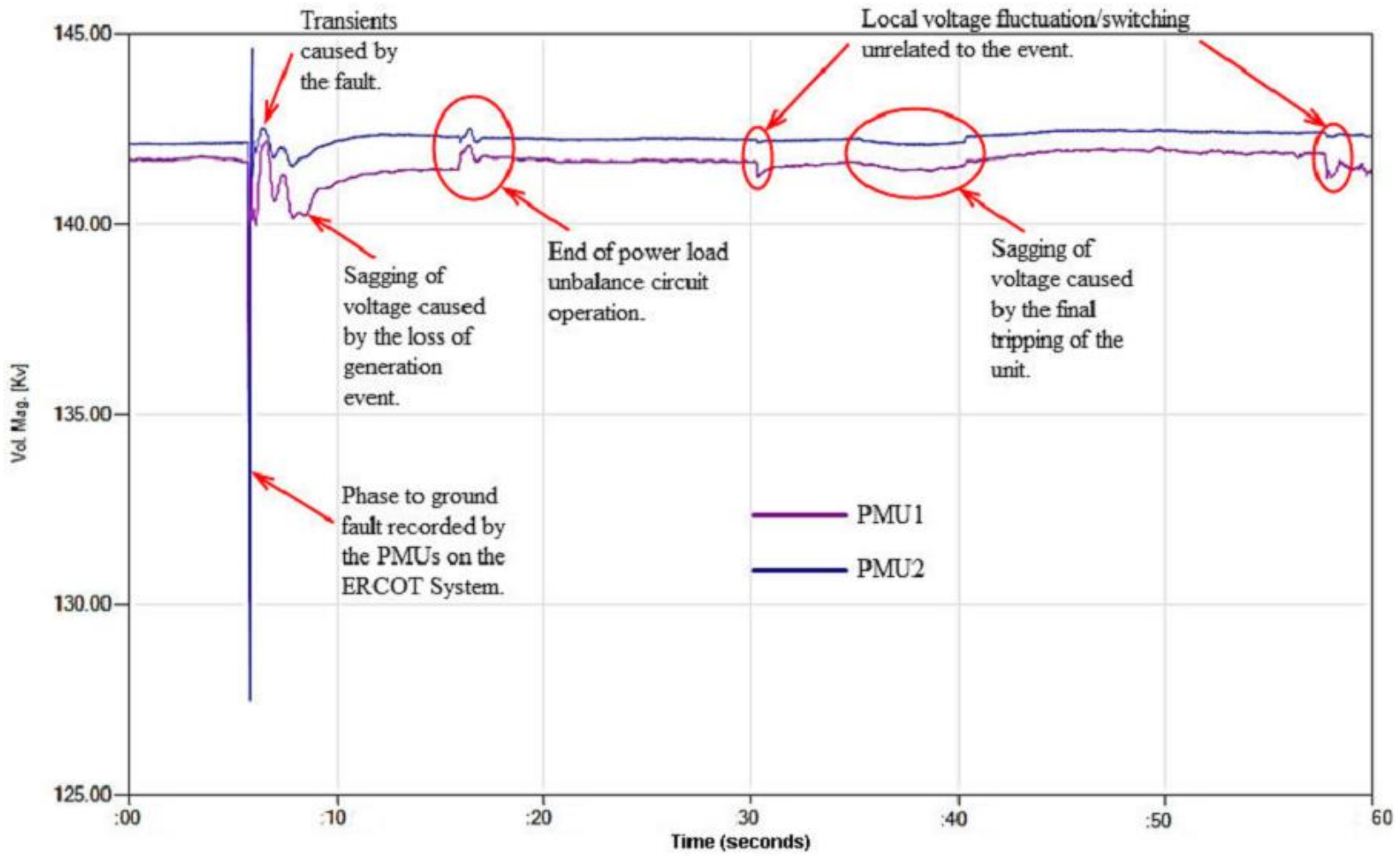
- **Predictive relaying**
  - Protection against possible over-speed of generator/turbine
- **Designed to rapidly close control/intercept valves under load imbalance conditions**
- **Relay checks for two conditions –**
  - Difference in mechanical and electrical loading
    - operates if the difference is greater than 40% (typically)
  - Rate of decrease of electrical load
- **After clearing of unbalanced condition –**
  - Wait for pre-set time delay
  - Reset PLU relay
  - Allow intercept valves to open again

Event Analysis - System Condition



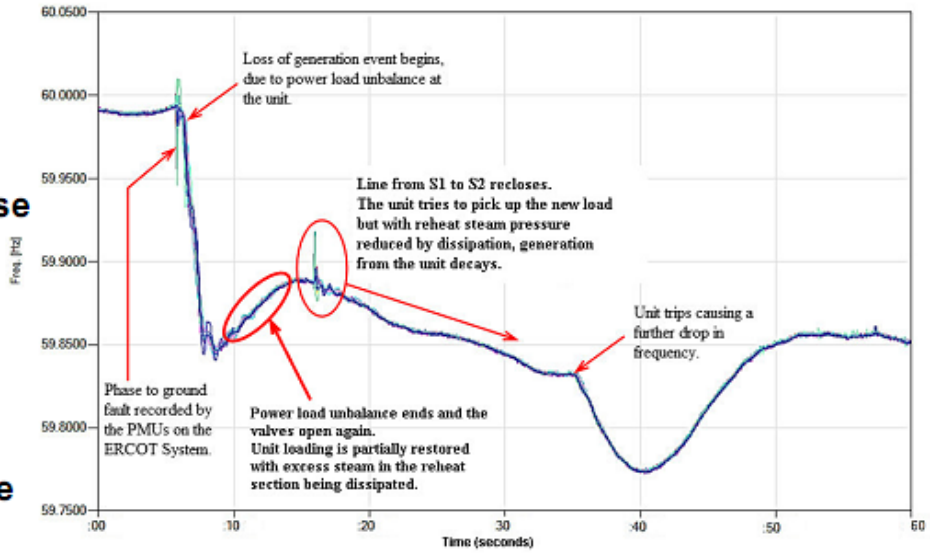
- **Generator 'G1' close to full output.**
- **Fault on 138kV bus section at sub-station 'S2'**
  - Fault cleared in ~5 cycles
  - Three 138kV circuits tripped as part of the fault clearing.
- **Fault detection and mis-operation of relay at substation 'S1'**
  - Line from 'S1' to 'S2' tripped due to mis-operation

Event Analysis - Fault



Event Analysis - Description

- **Following the fault and clearing –**
  - Due to loss of the 'S1' – 'S2' circuit, PLU initiated at unit 'G1'
  - Closing of control/intercept valves leading to ~575 MW loss
  - Frequency drop from 59.99 Hz to 59.846 Hz
- **Frequency decline arrested by inertial response**
  - PLU condition cleared
  - Intercept valves allowed to open again
  - Loading restored partially to ~500 MW
  - Excess steam in reheat dissipated
- **'S1' – 'S2' circuit reclosed 10 seconds after the fault**
  - Unit 'G1' loading increased after reclosing
  - Lack of sufficient pressure in reheat to sustain increased load
  - Generation decay – run back
- **Trip of Unit 'G1'**



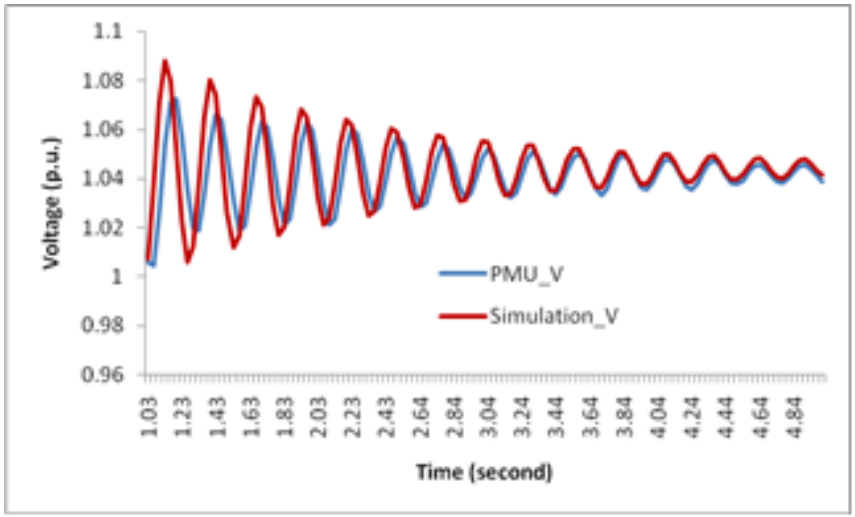
Event Analysis - Lessons Learned

- **New use-case for synchrophasor technology from ISO viewpoint**
  - Correction of incorrect design/operation of protection systems
- **Sequence of Events established by collaboration with Transmission Owner and Plant Operator**
  - Mis-operation of transmission relay leading to line trip
  - No mis-operation in PLU circuit, relay operated as designed
- **Unit tripping not the objective of PLU circuit**
- **Plant Operator in discussion with vendor to determine –**
  - whether unit trip was necessary
  - whether PLU circuit parameters need to be changed
- **Accurate representation of PLU relaying effects in modeling of contingencies in planning studies**
  - Investigate the possibility of other generators on the system having similar characteristics
  - Possible detailed dynamic studies to investigate improved modeling of this type of event.
  - Consider when these type studies would be appropriate.
    - Possibly as part of interconnection process.

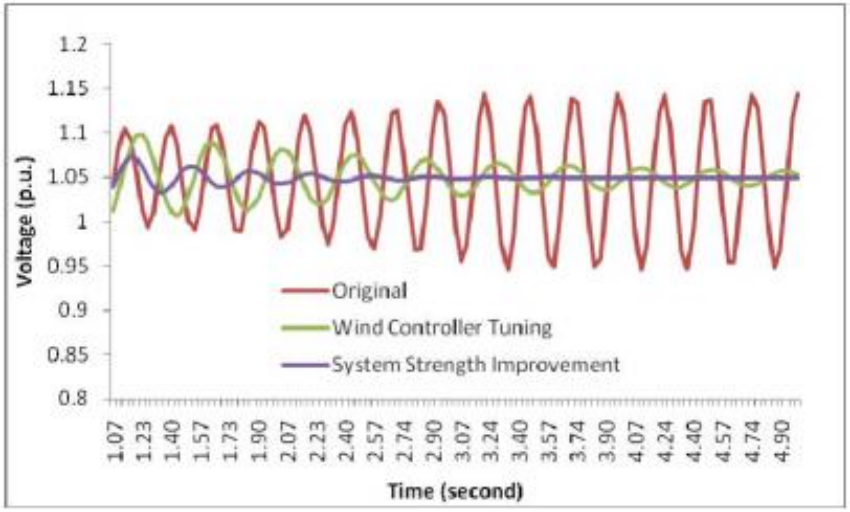
Use Case - Generator Parameter Determination

- **Need:** PMU data (voltage phasor, P & Q) can advise generator dynamic response following a nearby transient, compares results to simulated response (based on system planning models), and alerts if differences are significant (meaning that the generator response to the transient event was different from what was expected)
- **EXAMPLE: PMU DATA USED TO VALIDATE AND CALIBRATE GENERATOR MODELS**
- **Possible Action:**
- Advanced Network Applications expert or System Planning dynamics expert reviews the event and the generator response differences, and, if necessary, triggers the capture of the current grid state for further study
- System Planning dynamics expert coordinates with generator owner to investigate the reasons for unexpected generator response
- System Planning – Dynamics Working Group utilizes the apparent unit parameters and system response data to tune/benchmark the dynamic model associated with the unit in the ERCOT DWG dynamic dataset

Generator Parameter Validation



Recorded vs Simulated Voltage Response at Wind Power Plant – Low Power Output



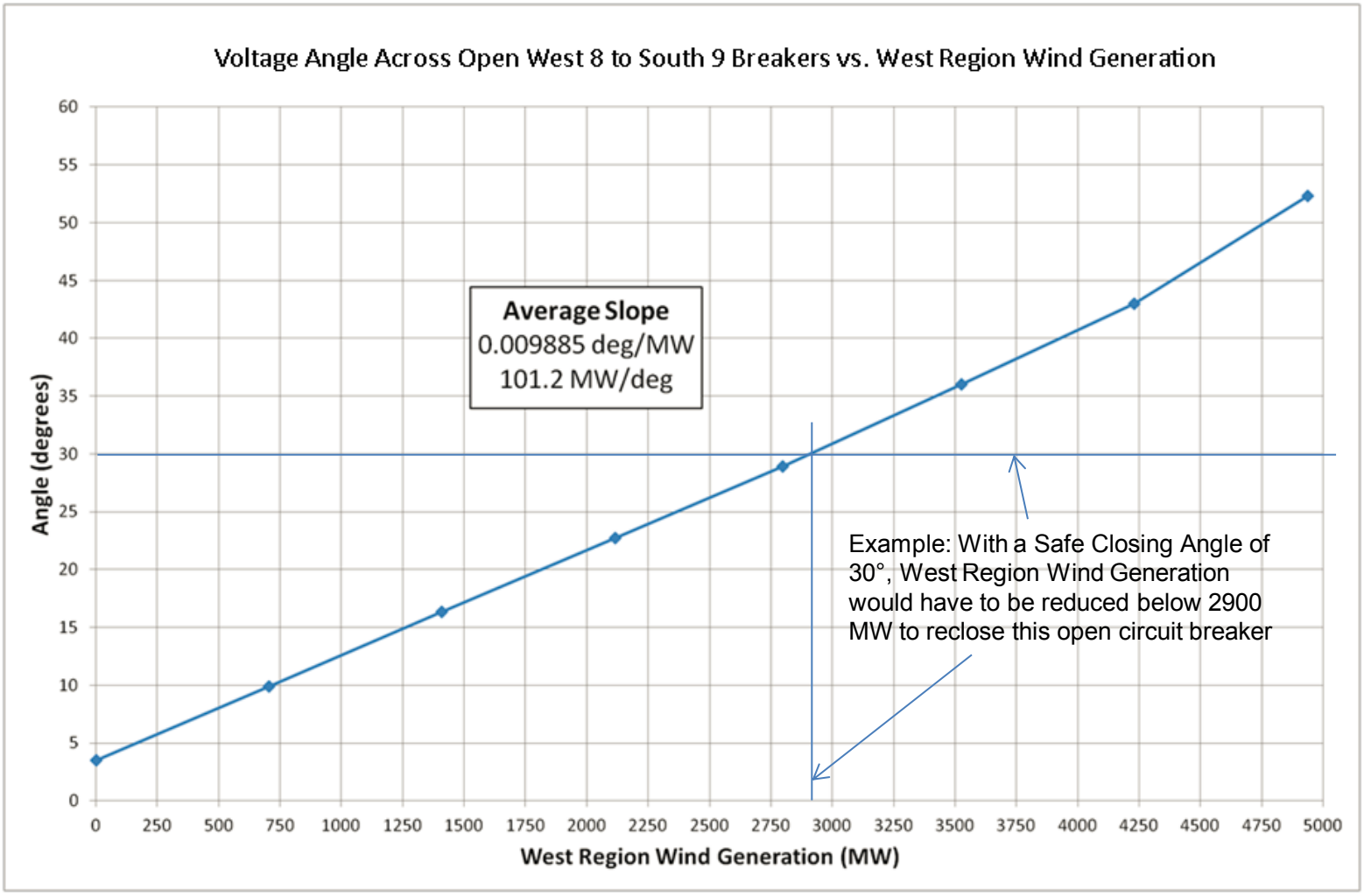
Recorded vs Simulated Voltage Response at Wind Power Plant – High Power Output – Improved performance after tuning wind controller settings

Source: Jian Chen, Prakash Shrestha, Shun-Hsien Huang, N.D.R. Sarma, John Adams, Diran Obadina, John Balance, “Use of Synchronized Phasor Measurements for Dynamic Stability Monitoring and Model Validation in ERCOT”, Proceedings of the 2012 IEEE PES General Meeting, San Diego, July 2012.

Use Case - Phase Angle Across Breaker for Reclosing Action

- **Need:** PMU data is useful during an event to identify stress across system, and validate safe restoration actions
- **EXAMPLE: HIGH PHASE ANGLE ACROSS BREAKER**
- **Possible Action:**
  - Shift Engineer reviews PMU voltage phase angle differences between substations (with breaker open between them)
  - If voltage phase angle difference is within safe breaker reclosing limits, proceed with planned restoration of lines
  - If voltage phase angle difference looks too large, refer to Advanced Network Applications expert or System Planning dynamics expert to identify mitigation actions needed to reduce phase angle to within limits for restoration

Phase Angle Across Open Breaker - Example



Thank You.

Any questions ?

John W Ballance

ballance@electricpowergroup.com

Prashant C Palayam

palayam@electricpowergroup.com

Sarma NDR Nuthalapati

sarma.nuthalapati@ercot.com

Attachment 15. TTU Network Forensics Report

Texas Tech University Network Forensics Report

Security Connected for Critical Infrastructure (SC4CI) Demonstration for Cyber Security Protection of Synchrophasor Network

Executive Overview

A cooperative effort between the Center for Commercialization of Energy Technologies (CCET), Electric Power Group (EPG), and Intel Corp. (including Intel subsidiaries McAfee and Wind River) has resulted in the demonstration installation of a set of security controls for the Synchrophasor *enhanced* Phasor Data Concentrator *e*PDC devices deployed in the Texas Tech University (TTU) campus Electric Smart Grid and Real Time Dynamics Monitoring Platform (RTDMS) for analytics and visualization. The Intel solution, known as Security Connected for Critical Infrastructure (SC4CI), is comprised of an embedded security system that provides network and endpoint hardening technologies for each EPG synchrophasor application/device – ePDC, RTDMS, and RTDMS Client. In addition, the solution includes Security Management and Monitoring capabilities to understand and react to the threats and security status of the devices in the environment.

Upon installing the SC4CI devices on the TTU network in December, 2013, significant traffic originating from China and Eastern Europe was identified as attempting to access the resources of the SC4CI protected devices. The nature of this traffic was mainly relegated to attempts to access the exposed SSH port (Secure Shell port 22) on the Management Instance protecting the EPG applications on the device. Additional controls are being put into place to increase the sensitivity of the security awareness to provide new data points to help understand the quantity, quality, and nature of the threats.

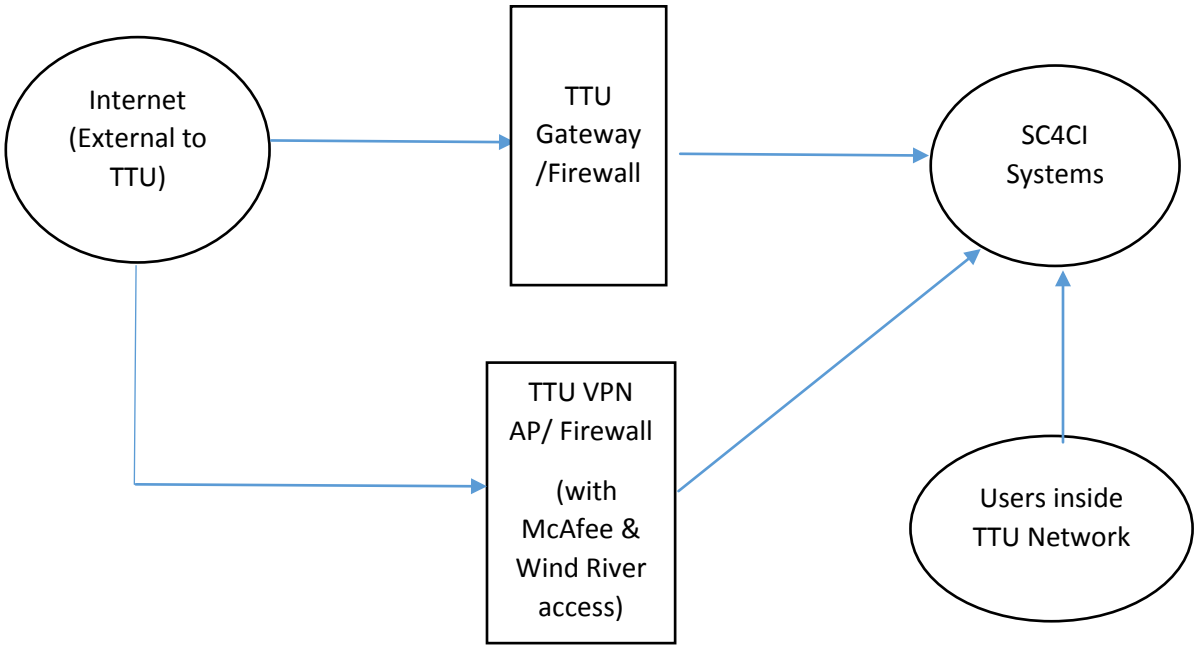
This forensics report describes the analysis of unauthorized attempts to access the SC4CI devices installed at TTU during the time period December 2013 through February 2014. The variety of intrusion attempts demonstrates the need to provide active protection and monitoring of critical infrastructure computer systems. It is expected that additional forensics analyses will be performed over the next several months of this demonstration, to document the performance of the SC4CI systems.

Conclusions

Almost immediately upon connecting the SC4SI systems to the TTU network in December, 2013, significant traffic originating from China and Eastern Europe was identified as attempting to access the resources of the SC4CI protected devices. In general, the attacks observed consisted of generic SSH Brute Force exploit attempts. These are common on the Internet and are generally automated. Sifting through the logs indicated that all the brute force attempts failed to authenticate and only whitelist IP addresses have been successful thus far in accessing the systems. There has been evidence in the logs that something is trying to access one of the protected services, but again, the systems have been successful (so far) in rejecting those attempts. Continued monitoring and analysis of intrusion attempts will be needed to validate the security performance of the systems.

Technical Background

The setup at TTU is deployed roughly as shown in the network topology diagram below,



The above network connectivity layout represents the network environment at the TTU campus within which the devices protected by the SC4CI have been deployed. The majority of the other network topology details are not specified as they are out of scope for this document. The above representation depicts three network connection sources found to be accessing the SC4CI systems and are explained in more detail below.

It is important to note that there exists an SSH listener on the SC4CI device(s) that accepts network connections from any network source with correct credentials, and is a potential vulnerability to the system. This SSH listener service is a desirable feature in order to allow ease of management when unexpected modifications are required to the system from support personnel accessing the device from arbitrary network source locations (within the TTU network, over the VPN, etc.). The SSH listener is not expected to be a feature available in future versions of the platform, but it is being leveraged as a good proof point for the security capabilities of the platform to demonstrate the security response capabilities when new vulnerabilities are discovered. At the conclusion of this investigation on the malicious traffic coming from China and Eastern Europe, passive countermeasures shall be implemented, using the tools provided by the SC4CI platform, to mitigate the threat to the SSH listener. The countermeasure will leverage the SC4CI Console to remotely configure the embedded firewall to block all traffic originating outside of the TTU network from reaching the SSH listener service. This creates Tailored Trustworthy Space within the TTU network consisting of a select set of nodes, both endpoint device and security server, that comprise the SC4CI protection platform.

Internet Connection Source

Connections from the open Internet, external to the TTU network, apparently have network connectivity to the SC4CI systems directly. Currently the firewall rules on the perimeter TTU Gateway do not appear to restrict, or at least not to successfully prevent, this traffic. There is presently no influence to be exerted over the TTU Gateway from the members of this project, so the network connectivity issue must be dealt with using the SC4CI controls we have at our disposal. Again, these connections will be blocked in the future to prevent access to the system by non-legitimate sources of network traffic.

TTU Connection Sources

Connections originating from the internal TTU network address space also have the ability to access the SC4CI device(s). It is not desirable to block these connections as they include the support and operations personnel that leverage the EPG applications, and therefore are assumed to be legitimate sources of traffic. However, there is concern related to the threat from insider attacks as well as compromised devices within the TTU perimeter, so additional controls may need to be put into place to restrict access down to a known set of hosts within the network.

The connections traversing the TTU VPN network address space have the ability to access the SC4CI device(s). It is not desirable to block these connections as they have been authenticated and authorized by the TTU VPN, and therefore are assumed to be legitimate sources of traffic. However, there is concern related to the threat from insider attacks as well as from compromised devices within the TTU perimeter, so additional controls may need to be put into place to restrict access down to a known set of hosts within the network.

There is currently no known differentiation scheme to segregate the TTU VPN traffic originating from outside of the TTU network from the TTU internal (local) TTU network traffic.

Threat Observations

Assumptions

- There is no management control over the TTU Gateway or VPN access point by project personnel.
- There are no allowable changes to firewall rules for any of the TTU Gateways and Firewalls.

The appropriate process to manage the access to the SC4CI devices is by implementing the embedded security controls on each of them. This is managed from the SC4CI console, the McAfee ePO product (ePolicy Orchestrator), by modifying the embedded Firewall policy configuration and the Secure Tunnel VPN policy definitions for the endpoint Nodes protecting the EPG software. There are additional policies that define the monitoring of log files on the endpoint Nodes to collect data points to be evaluated on the McAfee ePolicy Orchestrator (ePO) product, as well as the McAfee Enterprise Security Manager (ESM) product.

Any violations of the policies triggers an alarm to be generated and an update to the security visualization dashboards within the ePO product. The ePO product defines the policies and automates the provisioning of the policies to the endpoint Nodes. The ESM product doesn't exert operational

control on these systems but is merely an observer. The ESP performs security audit operations such as data aggregation, data correlation, analysis (risk algorithm for each node and the network communication between the nodes), and generates alarms in response to rule violations, which are forwarded to the ePO system for automated response (for example, notifying appropriate response personnel, or updating policy on devices which are under attack).

Since all data points pass through the ESM analytics, it is the logical point to perform both audit operations and any needed forensics duties. Therefore, the ESM product is the best source of evidence relating to the security posture of the endpoint node devices. The security metrics presented in this document are derived from the raw data collected by the ESM.

Within the ESM, we are expecting to see two categories of network addresses,

- External connection sources attempting to directly access the SSH listener on the SC4CI system via the port 22. These users must have proper credentials to gain access.
- Connection sources with TTU internal network address space attempting to access the SSH listener on the SC4CI system via the port 22. These sources could be either from users that have authenticated to the TTU VPN or users already authenticated on one of the systems within TTU network. At present, these two classifications of users and network locations cannot be differentiated within the ESM.

Network Forensics

The network forensics process model followed in this document has a phased approach wherein each stage feeds data to the following. The phases are described below in detail.

Detection

All events from all devices are logged remotely in the ESM. The ESM leverages the consolidated view of the logs collected to uncover behavioral anomalies. The logs currently available in the ESM date back to the time when the platform went live in mid-December, 2013.

Forensics performed using the ESM data illustrates that unwanted network traffic has been occurring since the SC4CI devices have been connected to the TTU network. Examples of this activity are listed below.

Direct Internet Connections to SSH Listener Trace Data

```
12/13/2013 02:26:06, ,Local ESM
(144115188075855872),Informational,Authentication,User Device Failed
Login. Dec 13 08:26:05 McAfee sshd[4422]: input_userauth_request:
invalid user app [preauth]

12/13/2013 02:26:06, ,Local ESM
(144115188075855872),Informational,Authentication,User Device Failed
Login. Dec 13 08:26:06 McAfee sshd[4422]: Failed password for invalid
user app from 112.91.240.230 port 33701 ssh2

12/13/2013 02:26:06, ,Local ESM
(144115188075855872),Informational,Authentication,User Device Logout.
```

```
Dec 13 08:26:06 McAfee sshd[4422]: Received disconnect from
112.91.240.230: 11: Bye Bye [preauth]

12/13/2013 02:26:08, ,Local ESM
(144115188075855872),Informational,Authentication,User Device Failed
Login. Dec 13 08:26:08 McAfee sshd[4458]: input_userauth_request:
invalid user bin [preauth]

12/13/2013 02:26:08, ,Local ESM
(144115188075855872),Informational,Authentication,User Device Failed
Login. Dec 13 08:26:08 McAfee sshd[4458]: Failed password for invalid
user bin from 112.91.240.230 port 35242 ssh2

12/13/2013 02:27:40, ,Local ESM
(144115188075855872),Informational,Authentication,User Device Logout.
Dec 13 08:27:40 McAfee sshd[5063]: Received disconnect from
112.91.240.230: 11: Bye Bye [preauth]
```

…<snip>….. The brute force search for username continues until the attacker finds “root” ……<snip>…

```
12/13/2013 02:27:42, ,Local ESM
(144115188075855872),Informational,Authentication,User Device Failed
Login. Dec 13 08:27:42 McAfee sshd[5077]: Failed password for root
from 112.91.240.230 port 60346 ssh2

12/13/2013 02:27:43, ,Local ESM
(144115188075855872),Informational,Authentication,User Device Logout.
Dec 13 08:27:43 McAfee sshd[5077]: Received disconnect from
112.91.240.230: 11: Bye Bye [preauth]
```

Internal Connections to SSH Listener Trace Data

```
12/02/2013 17:11:14, ,Local ESM
(144115188075855872),Informational,Authentication,User Device Failed
Login. Dec  2 23:11:14 McAfee sshd[6997]: Failed password for root
from 129.118.26.37 port 62563 ssh2

12/02/2013 17:11:23, ,Local ESM
(144115188075855872),Informational,Authentication,User Device Login.
Dec  2 23:11:23 McAfee sshd[6997]: Accepted password for root from
129.118.26.37 port 62563 ssh2
```

Examination

A methodical search has been performed on the collected logs to identify data sets which contain least information and highest possible evidence. Python scripts matched the attack patterns (data sets) seen in the logs to malicious activities. After running the python scripts on the copy of logs, it segregates the below data sets into separate text files.

Data Sets:

Example of Failed Login Attempts:

```
12/02/2013 17:11:14, ,Local ESM
(144115188075855872),Informational,Authentication,User Device Failed
Login. Dec  2 23:11:14 McAfee sshd[6997]: Failed password for root
from 129.118.26.37 port 62563 ssh2
```

Example of Accepted Password Messages:

```
12/02/2013 17:11:23, ,Local ESM
(144115188075855872),Informational,Authentication,User Device Login.
Dec  2 23:11:23 McAfee sshd[6997]: Accepted password for root from
129.118.26.37 port 62563 ssh2
```

Example of Username Brute Force

```
12/13/2013 02:26:08, ,Local ESM
(144115188075855872),Informational,Authentication,User Device Failed
Login. Dec 13 08:26:08 McAfee sshd[4458]: input_userauth_request:
invalid user bin [preauth]
```

```
12/13/2013 02:26:08, ,Local ESM
(144115188075855872),Informational,Authentication,User Device Failed
Login. Dec 13 08:26:08 McAfee sshd[4458]: Failed password for invalid
user bin from 112.91.240.230 port 35242 ssh2
```

Other Example Traces

```
12/15/2013 05:13:51, ,Local ESM (144115188075855872),,,yqj6j9gjlyo_8v
log-in failed - incorrect username or password
```

```
12/15/2013 05:13:52, ,Local ESM (144115188075855872),,,v13oi8o3zyi
log-in failed - incorrect username or password
```

Analysis

The attacks are replayed in a controlled Lab environment to understand the nature of the attacks, to ensure that the logs in the replay generate identical output, and also to validate the methodology of the attacker.

Failed Login Attempt Logs

In general, the attacks observed consisted of generic SSH Brute Force exploit attempts. These are common on the Internet and are generally automated such that they are set to run on a regular basis looking for new target systems with open SSH port (22). The brute force attack initially attempts to determine a legitimate username and once that has been accomplished, a brute force attack on the password is attempted. This type of automated attack is designed to identify systems on the network that have either default passwords, or weak passwords, and if any are found, to notify the Threat Source of the compromise and the availability of a new beachhead device on that particular network.

All evidence indicates that these Internet crawlers repeatedly tried brute force tactics to guess the username even though they had already found a username in the past. Therefore, it is reasonable to assume that the level of sophistication of the attacker is not high.

Sifting through the names list used for brute forcing the usernames indicates that they were commonly used usernames on the Internet. It appears that the password guessing was random in nature. It is interesting to observe that the automated attacks perform a limited number of brute force attempts at any one time in order to avoid detection and limit the amount of evidence in the local logs. But every set of attempts being made definitely tried a different set of passwords. A medium to strong password would require an average of millions of years to compromise with a daily attack schedule such as is being observed in this situation. However, with billions of devices on the Internet, these attacks are likely to be both statistically successful, and also potentially lucrative as a foundation for generating more automated attacks, thereby increasing the odds of finding more victims to exploit.

Accepted Logins

One objective of the forensics work is to ensure that none of the malicious connections were able to successfully authenticate to the SSH listener. An implicit whitelist of acceptable, and therefore currently not considered hostile, network addresses has been compiled, consisting of the internal and VPN TTU network address space. Sifting through these logs indicated that all the brute force attempts failed to authenticate and only whitelist IP addresses have been successful thus far. Therefore, it can be assumed that the automated threats have not yet compromised any of the SC4CI devices.

Other Login Attempts

It should be noted that there have been evidence in the logs of other activity that appears suspicious, for example:

```
12/15/2013 05:13:51, ,Local ESM (1441151880758558 72),,,yqj6j9gjlyo_8v
log-in failed - incorrect username or password
```

```
12/15/2013 05:13:52, ,Local ESM (1441151880758558 72),,,v13oi8o3zyi
log-in failed - incorrect username or password
```

These two traces indicate that something is trying to access one of the protected services. The two logs appear to show random passwords used in brute forcing the credentials. Following good secure programming techniques, the generic web service error message consisting of “incorrect username and password” message makes it difficult for the attackers to guess the credentials because it is not clear whether it is the password or the username that is incorrect.

NOTE: upon discovery of potentially nefarious network activity, all passwords in all systems are reviewed for their strength, and where necessary, the password strength is increased. Also, a password rotation policy has been put into place to regularly change the passwords.

Investigation

In general, the Investigation phase of forensics involves tracing the attackers back to their source. The data for this phase is iterative provided by the analysis and examination phases. In this report, we do not try to trace back to the attacker for prosecution and hence this phase is limited to identifying either the source country or that the source was within the TTU environment or on the TTU VPN.

Reporting

In order to understand the nature of the attacks and to match the log entries with the actual attack operations, one must replay the attack and confirm that the forensics match what was seen during the actual attack. This is an iterative process. Once the attacks have been replayed and the log patterns have been reverse engineered, the patterns are correlated in the database and the attacks can be quickly identified and collated. Below are the initial attacks that were found soon after installation of the secured platform.

Please note that the data points are correlated based on information from the network packets themselves. Therefore, the data could be "spoofed" or "faked". In addition, the simplistic nature of the attack and the fact that there seemed to be little variability between the attacks from day to day indicates that the attacks are automated, therefore, it is entirely possible that the source of the attacks has no knowledge of the activity, and therefore is not itself the active threat actor.

IP Address	Type of Network	Failure Attempts	Successful Attempts	Number of Attempts	Region	Type of Attempt
113.240.248.18	External	7824	0	7824	China Telecom	Brute Force
121.96.56.11	External	1425	0	1425	Bayan Telecommunications, Inc.	Brute Force
222.186.15.153	External	1825	0	1825	China Telecom	Brute Force
222.211.85.150	External	436	0	436	China Telecom	Brute Force
58.215.173.114	External	410	0	410	China Telecom	Brute Force
61.147.113.93	External	768	0	768	China Telecom	Brute Force
114.80.202.30	External	275	0	275	China Telecom	Brute Force
114.80.226.94	External	408	0	408	China Telecom	Brute Force
61.147.116.20	External	400	0	400	China Telecom	Brute Force
61.147.116.24	External	276	0	276	China Telecom	Brute Force
61.147.119.106	External	264	0	264	China Telecom	Brute Force
60.191.45.248	External	228	0	228	China	Brute Force
112.91.240.230	External	109	0	109	China Unicom Jieyang Branch	Brute Force
195.93.180.125	External	105	0	105	Russia	Brute Force
112.216.82.130	External	99	0	99	Korea	Brute Force
222.88.154.79	External	87	0	87	Russia	Brute Force
92.63.96.106	External	86	0	86	Russia	Brute Force
85.232.244.50	External	84	0	84	Poland	Brute Force
61.235.70.231	External	68	0	68	China	Brute Force
222.186.59.42	External	95	0	95	China	Brute Force
222.189.239.10	External	126	0	126	China	Brute Force
208.115.201.251	External	61	0	61	Limestone Networks, Brazil	Brute Force
103.23.244.22	External	48	0	48	Indonesia	Brute Force
106.186.116.117	External	45	0	45	Tokyo	Brute Force
221.234.231.190	External	37	0	37	China	Brute Force
198.172.23.11	External	36	0	36	Orem, Utah, US	Brute Force
116.213.79.220	External	35	0	35	China	Brute Force
212.116.159.146	External	34	0	34	Bulgaria	Brute Force
61.160.251.141	External	48	0	48	China	Brute Force
114.80.246.146	External	24	0	24	China	Brute Force
61.147.116.5	External	44	0	44	China	Brute Force

2.139.155.90	External	18	0	18	Madrid	Brute Force
32.65.252.65	External	15	0	15	AT&T Global Network Services	Brute Force
77.81.50.113	External	15	0	15	Romania	Brute Force
61.136.208.23	External	21	0	21	China	Brute Force
222.186.57.67	External	24	0	24	China	Brute Force
221.230.54.115	External	10	0	10	China	Brute Force
183.86.221.244	External	7	0	7	South Korea	Brute Force
183.61.164.202	External	9	0	9	China	Brute Force
61.147.103.157	External	10	0	10	China	Brute Force
61.182.227.182	External	5	0	5	China	Brute Force
211.202.2.135	External	3	0	3	South Korea	Unknown /Brute Force
207.210.192.36	External	3	0	3	Unknown	Unknown /Brute Force
37.247.103.107	External	2	0	2	Turkey	Unknown
113.108.211.131	External	2	0	2	China	Unknown
115.236.79.98	External	2	0	2	China	Unknown
123.232.122.162	External	1	0	1	China	Unknown
183.224.249.22	External	1	0	1	China	Unknown
209.255.116.35	External	1	0	1	New York	Unknown
183.247.177.35	External	1	0	1	China	Unknown
67.207.180.163	External	1	0	1	Las Vegas, NV	Unknown
128.226.31.97	External	1	0	1	Binghamton University, NY	Unknown

Attachment 16. Security Fabric Compliance and Penetration Testing

Appendix A: TTU Security Testing Part 1

Verification of Security Fabric Requirement Specifications

This appendix provides details of testing against given security requirement specifications summarized in Section 4.5.1.1 of the Final Technical Report. Each section groups a set of test specifications by the NIST's requirement category. Each subsection gives details of a specific test including the description of NIST requirement along with its corresponding specification developed by Intel/McAfee, and verification results. If the specification is satisfactorily verified, evidence will be provided when appropriate. Otherwise, the explanation to why the specification is not satisfied will be described. In the latter case, the explanation should clarify how the issue can be resolved. It is noted that all of the issues identified can be fixed to meet the requirements by defining the specifications more thoroughly, eliminating some inappropriate requirements, providing additional information for testing, or by incorporating additional existing Intel/McAfee tools or applications.

A.1 Access Control (SG.AC)

The focus of access control is ensuring that resources are accessed only by the appropriate personnel, and that personnel are correctly identified. Mechanisms need to be in place to monitor access activities for inappropriate activity.

A.1.1 Remote Access Policy and Procedures (SG.AC-2)

Requirement

The organization—

1. Documents allowed methods of remote access to the Smart Grid information system;
2. Establishes usage restrictions and implementation guidance for each allowed remote access method;
3. Authorizes remote access to the Smart Grid information system prior to connection; and
4. Enforces requirements for remote connections to the Smart Grid information system.

Supplemental Guidance

Remote access is any access to an organizational Smart Grid information system by a user (or process acting on behalf of a user) communicating through an external, non-organization-controlled network (e.g., the Internet).

Category

Common Governance, Risk, and Compliance (GRC) Requirement

Specification

The development of the machine policy, based on the corporate or regulatory Policy, defining how the machines communicate is managed by the platform. So, instead of managing policy via Word Document, PDF, etc. (in prose), the platform provides the ability to digitally define policy, distribute to appropriate endpoints, enforce the policy, and monitor for policy violations.

1) Manage policy on ePO to define allowed system behavior: describe server components and endpoint components, defining how the system can communicate to other (remote) systems.
2) Define policy specifically to restrict access to platform services which have not been explicitly allowed.
3) Authorizes that each communication is allowed based on policy.
4) Non-allowed communications are blocked.

Verification Results

Satisfactory. The proposed system provides remote access policy via ePO policy management system to control communication among the components (including outside of SF system). The following gives an example of Security Fabric IPTFW configuration from the ePO policy management system:

```
# S2-Layer2 Note this comment is used by the script to detect the policy type is L2

in tcp 129.118.26.8 1113

out tcp 129.118.26.8 1113

in tcp 129.118.105.50 1113

out tcp 129.118.105.50 1113

in tcp 0.0.0.0 3389

out tcp 0.0.0.0 3389

out udp 129.118.26.8 123

out udp 129.118.105.50 123

in tcp 129.118.26.8 1433

out tcp 129.118.19.210 1433

in tcp 129.118.105.44 6688

out tcp 129.118.105.44 6688
```

A.1.2 Account Management (SG.AC-3)

Requirement

The organization manages Smart Grid information system accounts, including:

1. Authorizing, establishing, activating, modifying, disabling, and removing accounts;
2. Specifying account types, access rights, and privileges (e.g., individual, group, system, guest, anonymous and temporary);
3. Reviewing accounts on an organization-defined frequency; and
4. Notifying account managers when Smart Grid information system users are terminated, transferred, or Smart Grid information system usage changes.

Management approval is required prior to establishing accounts.

Additional Considerations

1. The organization reviews currently active Smart Grid information system accounts on an organization-defined frequency to verify that temporary accounts and accounts of terminated or transferred users have been deactivated in accordance with organizational policy.
2. The organization authorizes and monitors the use of guest/anonymous accounts.
3. The organization employs automated mechanisms to support the management of Smart Grid information system accounts.
4. The Smart Grid information system automatically terminates temporary and emergency accounts after an organization-defined time period for each type of account.
5. The Smart Grid information system automatically disables inactive accounts after an organization-defined time period.
6. The Smart Grid information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.

Category

Common Governance, Risk, and Compliance (GRC) Requirement

Specification

Inherit from Org Policy. ePO is dependent upon HR & other systems for the user information. The Active Directory server is configured to authorize the target systems to use defined system resources in Security Fabric. Active directory acts as Authentication system as it uses Kerberos as the authentication mechanism. The provisioning of the AD system with Machine principals is automated. The import of User Principals from AD into ePO is automated.

1. We leverage the Org Policy. We do not introduce new User Principals, but use Machine Principals. All Kerberos principals are Machine Principals, therefore, there are no user principals required. By default, there are no other accounts (guest, anonymous or individual user account)

to be monitored or managed by the Security Fabric devices. This simplifies the management activities. Any existing User Principals in AD can be imported into ePO to simplify the management of the users, and therefore keep the system more secure.

2. Accounts/principals should be reviewed on an organization-defined frequency in ePO. Scheduled Tasks may be created to remind personnel to review the User accounts.
3. Since User Accounts are not leveraged in the Security Fabric, there is less impact from termination of employees and such. In ePO and ESM, the accounts may need to be manually synchronized.

A heightened level of access is required to establish Machine Principals in Active Directory.

Verification Results

Issue Identified – specification needs more information. The specification does not describe account type, access rights, and privileges (e.g., the users of the proposed system and their individual responsibility). Based on system account information, the specification should state how to authorize, establish, activate, modify, disable, and remove accounts (i.e., functions of account management system) in the proposed system.

A.1.3 Access Enforcement (SG.AC-4)

Requirement

The Smart Grid information system enforces assigned authorizations for controlling access to the Smart Grid information system in accordance with organization-defined policy.

Additional Considerations

1. The organization considers the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies.

Category

Common Governance, Risk, and Compliance (GRC) Requirement

Specification

The control/monitor systems (AD, ePO and ESM) are part of the back-end systems that manage the security fabric. Password authentication is necessary to access these devices/instances.

Verification Results

Satisfactory. The control/monitor systems are protected by secured authentication (authentication with encrypted channel) as shown below.

System	Protocol	Location	Password	Encrypted
ePO	HTTPS	https://129.118.19.210:8443/core/orionSplashScreen.do	Yes	Yes
ePO	RDP	129.118.19.210:3389	Yes	Yes
ESM	SSH	129.118.26.40:22	Yes	Yes
ESM	SSH	129.118.26.40:23	Yes	Yes
ESM	HTTPS	http://129.118.26.40/Application.html	Yes	Yes
AD	RDP	129.118.26.37:3389	Yes	Yes

Table 1. Verification results from checking authentication with secured channel in SF Components.

A.1.4 Information Flow Enforcement (SG.AC-5)

Requirement

The Smart Grid information system enforces assigned authorizations for controlling the flow of information within the Smart Grid information system and between interconnected Smart Grid information systems in accordance with applicable policy.

Supplemental Guidance

Information flow control regulates where information is allowed to travel within a Smart Grid information system and between Smart Grid information systems. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict Smart Grid information system services or provide a packet-filtering capability.

Additional Considerations

1. The Smart Grid information system enforces information flow control using explicit labels on information, source, and destination objects as a basis for flow control decisions.
2. The Smart Grid information system enforces dynamic information flow control allowing or disallowing information flows based on changing conditions or operational considerations.
3. The Smart Grid information system enforces information flow control using organization-defined security policy filters as a basis for flow control decisions.
4. The Smart Grid information system enforces the use of human review for organization-defined security policy filters when the Smart Grid information system is not capable of making an information flow control decision.
5. The Smart Grid information system provides the capability for a privileged administrator to configure, enable, and disable the organization-defined security policy filters.

Category

Unique

Specification

The flow of information is enforced in the Management Instance. There are no connections allowed to the internal Operational Instance that have not been explicitly pre-allowed. This is configured via policy in the remote console (ePO server instance) which inherits from the Org Policy.

The device has multiple layers of security:

a) external firewall to reject incoming (and outgoing) connections to non-allowed systems
b) mutual authentication of connections to ensure the identity of the remote endpoint
c) secure tunnel implementation upon successful mutual authentication to ensure the data cannot be intercepted or disclosed enroute

Therefore, all flow control decisions are made "below the Operational OS" in the Management instance. In addition, the flow control rules are defined by policy provided by ePO so that it is quite dynamic in nature and can be modified as required based on situation.

Violations of the flow-control policy are remotely logged and can be reviewed by a human if the automated controls prove to be insufficient.

A privileged user on the remote ePO console can change the organization-defined security policy filters if needed. During an emergency, increased access can be assigned to one or more users on the ePO system.

The information flow regulation policies are created in firewall on Windows, iptables on WR Linux and also the secure communications EPO policy where the create string defines the flow of the data between the WRL boxes.

Verification Results

Satisfactory. The proposed system regulates the flow of information using ePO policy. The following example is the proxy configuration from policy titled “Security Fabric CORE Configuration” from ePO policy configuration:

```
   delete
lport=tcp:192.168.250.3:8712;tport=ssl:129.118.26.8:129.118.105.50:1113;rport=tcp:192.
168.250.3:8712;tlskey=kerberos;servicehost=Reese-SF;maxdatarate=1;mdreventperiod=10

   create
lport=tcp:192.168.250.3:8712;tport=ssl:129.118.26.8:129.118.105.50:1113;rport=tcp:192.
168.250.3:8712;tlskey=kerberos;servicehost=Reese-SF;maxdatarate=1000;mdreventperiod=10

   create lport=tcp:192.168.250.3:1433;tport=tcp:129.118.26.8:129.118.19.210:1433

   create lport=tcp:192.168.250.3:8443;tport=tcp:129.118.26.8:eposerver:8443

   create lport=tcp:192.168.250.3:6688;tport=tcp:129.118.105.50:129.118.105.44:6688

   create tport=tcp:0.0.0.0:129.118.105.50:3389;rport=tcp:192.168.250.3:3389
```

```
create tport=tcp:0.0.0.0:129.118.26.8:3389;rport=tcp:192.168.250.3:3389

create lport=udp:192.168.250.3:123;tport=udp:129.118.26.8:129.118.26.37:123

create lport=udp:192.168.250.3:123;tport=udp:129.118.105.50:129.118.26.37:123
```

A.1.5 Separation of Duties (SG.AC-6)

Requirement

The organization—

1. Establishes and documents divisions of responsibility and separates functions as needed to eliminate conflicts of interest and to ensure independence in the responsibilities and functions of individuals/roles;
2. Enforces separation of Smart Grid information system functions through assigned access authorizations; and
3. Restricts security functions to the least amount of users necessary to ensure the security of the Smart Grid information system.

Category

Integrity

Specification

1) the organization partitions the responsibilities into buckets as needed to eliminate any conflicts of interest and to ensure independence in the responsibilities of users and roles
2) the ePO system (as well as AD and ESM) enforce the separation of system functions based on the roles and permission defined.
3) The users assigned to the roles that have permission to specific resources are kept to a minimum.

ePO facilitates separation of duties on the server side. Different accounts can be setup in ePO to perform different administrative tasks. ePO user accounts may be disabled. Also no console access will be enabled on the end point (WRL) for any user. Any administrative task to be performed on the end-point will be performed from EPO.

Verification Results

Issue Identified – specification needs more information. The specification does not describe roles and responsibilities in the proposed system. Without the defined roles and responsibilities, it is not possible to test whether the Separation of Duties constraints are enforced in the proposed system. The separation of duties constraint is commonly used to solve the problem of conflict of interest. The specification should also address where conflicts of interest occur and show how the separation of duties can be enforced in the system.

A.1.6 Least Privilege (SG.AC-7)

Requirement

1. The organization assigns the most restrictive set of rights and privileges or access needed by users for the performance of specified tasks; and
2. The organization configures the Smart Grid information system to enforce the most restrictive set of rights and privileges or access needed by users.

Additional Considerations

1. The organization authorizes network access to organization-defined privileged commands only for compelling operational needs and documents the rationale for such access in the security plan for the Smart Grid information system.
2. The organization authorizes access to organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information.

Category

Integrity

Specification

ePO provides users, roles, permissions, and groups to allow the administrator to define the least permission possible for each user to do his/her job.

1. The organization assigns the most restrictive set of rights and privileges as need to for users to perform the needed tasks.
2. The organization configures the policy to enforce the most restrictive controls that still enable the users to perform their tasks.

User accounts must be created on the EPO (server-side) with different levels of privileges for performing different tasks so that the users can perform only those tasks as are allowed by their role. On the client-side, there would be no user account and not even root access for a remote user.

Verification Results

Issue Identified – specification needs more information. Without the descriptions of roles and responsibilities, it is not possible to test if the least privilege constraints are enforced in the proposed system. The least privilege refers to the fact that every user must be able to access only the resources that are necessary for completing their assigned tasks. Verifying the least privilege property requires: (1) role and its associated responsibilities, (2) list of user privileges (i.e., access authorization), and (3) system configuration settings and corresponding documents.

A.1.7 Unsuccessful Login Attempts (SG.AC-8)

Requirement

The Smart Grid information system enforces a limit of organization-defined number of consecutive invalid login attempts by a user during an organization-defined time period.

Supplemental Guidance

Because of the potential for denial of service, automatic lockouts initiated by the Smart Grid information system are usually temporary and automatically released after a predetermined time period established by the organization. Permanent automatic lockouts initiated by a Smart Grid information system must be carefully considered before being used because of safety considerations and the potential for denial of service.

Additional Considerations

1. The Smart Grid information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded; and
2. If a Smart Grid information system cannot perform account/node locking or delayed logins because of significant adverse impact on performance, safety, or reliability, the system employs alternative requirements or countermeasures that include the following:
    a. Real-time logging and recording of unsuccessful login attempts; and
    b. Real-time alerting of a management authority for the Smart Grid information system when the number of defined consecutive invalid access attempts is exceeded.

Category

Integrity

Specification

ePO has a configurable number of user login attempts before the account is locked for a period of time.

The remote access login into the WRL instances via ssh is protected by username/password mechanism, but may be set to Certificate auth. All Endpoint login attempts are monitored by ESM.

ESM monitors login attempts whether it fails or succeeds. So, alarms will be raised if there are a suspicious number of failed login attempts for actions to be taken. Also, ESM can be configured to monitor for a certain number of failed logins followed by a successful login.

Verification Results

Satisfactory. The proposed system has real-time logging and recording of login attempts (both successful and unsuccessful), which can be configured to alert the system administrator when the number of defined consecutive invalid access attempts exceeds the organization-defined number.

A.1.8 Smart Grid Information System Use Notification (SG.AC-9)

Requirement

The Smart Grid information system displays an approved system use notification message or banner before granting access to the Smart Grid information system that provides privacy and security notices consistent with applicable laws, directives, policies, regulations, standards, and guidance.

Supplemental Guidance

1. Smart Grid information system use notification messages can be implemented in the form of warning banners displayed when individuals log in to the Smart Grid information system.
2. Smart Grid information system use notification is intended only for Smart Grid information system access that includes an interactive interface with a human user and is not intended to call for such an interface when the interface does not currently exist.

Category

Integrity

Specification

ePO has a configurable message on the login screen. ESM has a warning message on the login screen.

Verification Results

Satisfactory. The two parts of the proposed system, namely ePO and ESM can display the system use notification message before system access.

A.1.9 Previous Logon Notification (SG.AC-10) – Wait for ePO verification

Requirement

The Smart Grid information system notifies the user, upon successful logon, of the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.

Category

Unique

Specification

The last login notification made on any system will be recorded in ESM. User can query this information in ESM, and it is displayed after login.

ePO tracks the user logins and a query can be built that displays this information in a dashboard and the dashboard can be configured as the default screen, therefore the user sees the last login date/time when he logs in.

Verification

Issue Identified – additional information required for testing. Only the verification of ESM is satisfied, but information related to the ePO is necessary to fully satisfy this requirement. The figure below shows the last login notification on the ESM system and the number of unsuccessful logon attempts since the last successful login.

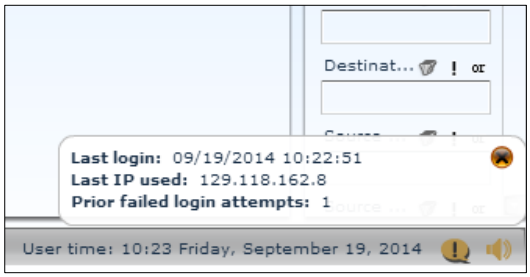


Figure 1. Message notification after successful logon from ESM.

However, at the time of finalizing this report, the evidence of last login notification on the ePO system is not available.

A.1.10 Session Lock (SG.AC-12)

Requirement

The Smart Grid information system—

1. Prevents further access to the Smart Grid information system by initiating a session lock after an organization-defined time period of inactivity or upon receiving a request from a user; and
2. Retains the session lock until the user reestablishes access using appropriate identification and authentication procedures.

Supplemental Guidance

A session lock is not a substitute for logging out of the Smart Grid information system.

Additional Considerations

The Smart Grid information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.

Category

Unique

Specification

EPO and ESM time out after a certain time period of inactivity and the user is logged out. User must authenticate again to reestablish the session.

Verification Results

Satisfactory. ESM Web component has a feature to "set console timeout value" for the current session on the ESM console to remain open as long as there is activity. We can define the amount of time with no activity before the session closes. To set this value, (1) On the ESM console, select *System Properties* followed by *Login Security* (2) In *UI Timeout Value,* select number of minutes that must pass with no activity, then click *OK* to update the configuration. The figure below shows the current setting in the system which is still disabled.

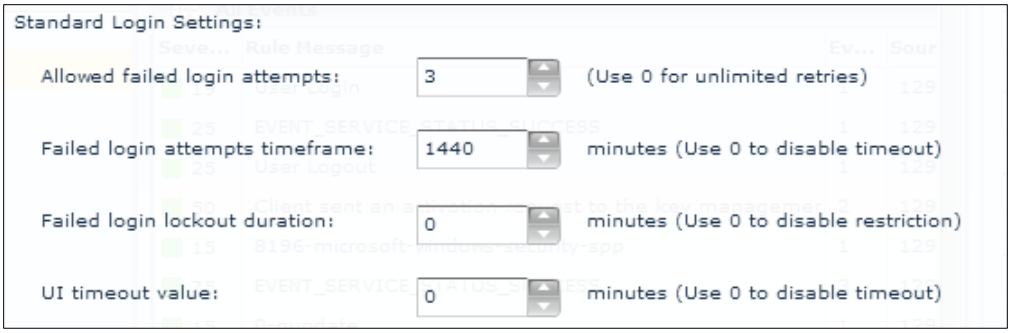


Figure 2. Part of Login Security property from ESM component.

The ePO web component also has a feature to set "session timeout interval" for the current session on ePO. We can define this value by select *Menu* and followed by *Server Settings* from *Configuration*. Then, we select the last item, which is *User Session*. Shows the current setting of session timeout interval from the ePO component.

Figure 3. Current Setting of session timeout interval from ePO web component.

A.1.11 Remote Session Termination (SG.AC-13)

Requirement

The Smart Grid information system terminates a remote session at the end of the session or after an organization-defined time period of inactivity.

Additional Considerations

Automatic session termination applies to local and remote sessions.

Category

Unique

Specification

Remote login to ESM terminates after configurable time limit has been exceeded. The remote access to the windows are disabled. Removing the ESM remote login is potentially viable as well (only local login allowed)

Verification Results

Satisfactory. ESM Web component has a feature to “set console timeout value” for the current session on the ESM console to remain open as long as there is an activity. We can define the inactive time duration before the session closes. To set this duration value, execute the following steps: (1) On the ESM console, select *System Properties* followed by *Login Security* (2) In *UI Timeout Value*, select the number of minutes that must pass with no activity, then click *OK* to update the configuration. The figure below shows current settings in the system which is still disabled.

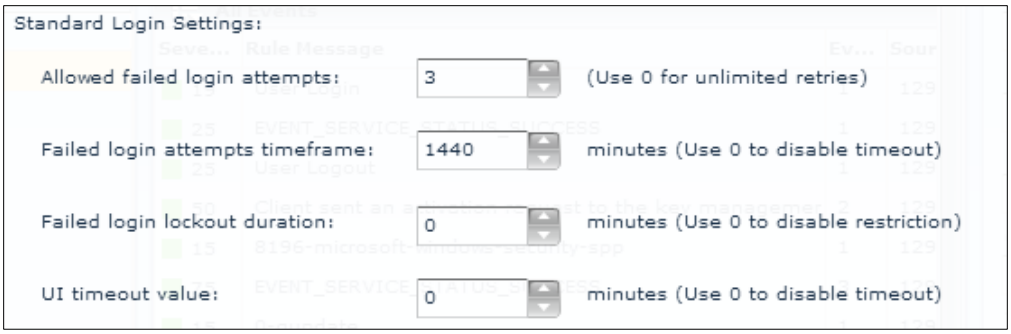


Figure 4. Part of Login Security property from ESM component.

The ePO web component also has a feature to set "session timeout interval" for the current session on the ePO. We can define this value by selecting *Menu* followed by *Server Settings* from *Configuration*. Then the last item, *User Session* is selected. The figure below shows the current setting of session timeout interval from the ePO component.

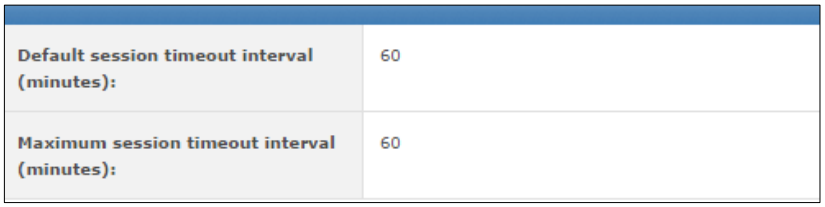


Figure 5. Current Setting of session timeout interval from ePO web component.

A.1.12 Remote Access (SG.AC-15)

Requirement

The organization authorizes, monitors, and manages all methods of remote access to the Smart Grid information system.

Supplemental Guidance

Remote access is any access to a Smart Grid information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).

Requirement Enhancement

1. The organization authenticates remote access, and uses cryptography to protect the confidentiality and integrity of remote access sessions;
2. The Smart Grid information system routes all remote accesses through a limited number of managed access control points;

3. The Smart Grid information system protects wireless access to the Smart Grid information system using authentication and encryption. Note: Authentication applies to user, device, or both as necessary; and
4. The organization monitors for unauthorized remote connections to the Smart Grid information system, including scanning for unauthorized wireless access points on an organization-defined frequency and takes appropriate action if an unauthorized connection is discovered.

Additional Considerations

1. Remote access to Smart Grid information system component locations (e.g., control center, field locations) is enabled only when necessary, approved, authenticated, and for the duration necessary;
2. The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods;
3. The organization authorizes remote access for privileged commands and security-relevant information only for compelling operational needs and documents the rationale for such access in the security plan for the Smart Grid information system; and

The organization disables, when not intended for use, wireless networking capabilities internally embedded within Smart Grid information system components.

Category Unique

Specification

1) Security Fabric leverages authentication on all accesses to endpoints (SSH) and back-end servers (user credentials). It also enforces encryption on all connections unless specifically configured not to encrypt.
2) The Security Fabric enforces access to services from a specific set of source and destination systems as part of its policy. Therefore it is possible to define a limited number of managed access points.
3) NA - wireless currently not managed by Security Fabric
4) The remote access to the end-point systems is monitored and recorded in ESM, and alarms on detection. Responses to these actions can be defined in ePO.

The remote access to the Server side systems (EPO, AD, ESM) are monitored

a. NA - Organizational Policy
b. Monitoring via ESM is automatable
c. NA - Operational Policy
d. NA - wireless currently not managed by Security Fabric

Verification Results

Satisfactory. All access to endpoints and back-end servers requires authentication with encryption to protect the credential of the user as shown below. The ESM system can be configured to monitor and record all remote access attempts.

Host	Port	Service	Description
WRL (TTU)	22	ssh	OpenSSH 6.0 (protocol 2.0)
WRL (TTU)	3389	ms-wbt-server	Microsoft Terminal Service
WRL (Reese)	22	Ssh	OpenSSH 6.0 (protocol 2.0)
WRL (Reese)	3389	ms-wbt-server	Microsoft Terminal Service
ePO	3389	ms-wbt-server	Microsoft Terminal Service
ESM	22	Ssh	protocol 2.0 with 2048 (RSA)
ESM	23	Ssh	libssh 0.5.2 (protocol 2.0) with 2048 (RSA)

Table 2. Remote Access to Security Fabric Enabled System.

A.1.13 Use of External Information Control Systems (SG.AC-18)

Requirement

The organization establishes terms and conditions for authorized individuals to—

1. Access the Smart Grid information system from an external information system; and
2. Process, store, and transmit organization-controlled information using an external information system.

Supplemental Guidance

External information systems are information systems or components of information systems that are outside the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of security requirements or the assessment of security requirement effectiveness.

Requirement Enhancements

1. The organization imposes restrictions on authorized individuals with regard to the use of organization-controlled removable media on external information systems.

Additional Considerations

1. The organization prohibits authorized individuals from using an external information system to access the Smart Grid information system or to process, store, or transmit organization-controlled information except in situations where the organization (a) can verify the implementation of required security controls on the external information system as specified in the organization's security policy and security plan, or (b) has approved Smart Grid information system connection or processing agreements with the organizational entity hosting the external information system.

Category

Common Governance, Risk, and Compliance (GRC) Requirement

Specification

1) Configure management instance firewall such that incoming connections may only be initiated from specific sources external to the network. Ensure that the firewall only allows specific protocols from those sources. Finally, ensure that the user access is strictly enforced from the Operational Instance. NOTE: Full control is not yet implemented, but monitoring of the operations on the system can be accomplished via the SIEM.
2) Managing the actions of processing, storing, and transmitting information on external system requires a Data Loss Prevention (DLP) product on the external system. NOTE: NOT IN DEMONSTRATION INSTANCE).

In order to fully implement this requirement, the external instance must be fitted with DLP software, and the operational instant must be configured to allow only the external instance to connect on specific ports with services listening that are configured with proper user access restrictions.

Verification Results

Satisfactory. The specification provides the condition to access 1) the smart grid information system from an external information system and 2) the process and store and to transmit the smart grid information using an external information system. For example, the condition may be operated via firewall configure management and Data Loss Presentation (DLP) system. However, the DLP system has not been implemented in the current SF-enabled system yet.

A.1.14 Control System Access Restrictions (SG.AC-19)

Requirement

The organization employs mechanisms in the design and implementation of a Smart Grid information system to restrict access to the Smart Grid information system from the organization's enterprise network.

Supplemental Guidance

Access to the Smart Grid information system to satisfy business requirements needs to be limited to read-only access.

Category

Common Governance, Risk, and Compliance (GRC) Requirements

Specification

The endpoint is able to control the network traffic into and out of the Management instance. Therefore, it is possible to restrict network access to the endpoint even from the organization's enterprise network (or from any other location).

Verification Results

Satisfactory. The endpoints (i.e., the agent of security fabric components, which are WRLs on both RTDMS and ePDC) control the communication between entities in the network by using the security policy from ePO. Partial policies from ePO web interface are shown below.

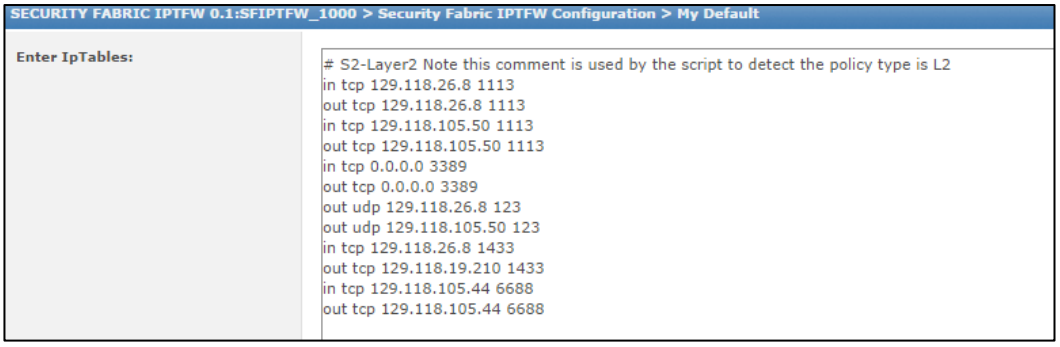


Figure 6. IP Table Firewall rule in ePO policy.

A.1.15 Password (SG.AC-20)

Requirement

The organization—

1. Designates individuals authorized to post information onto an organizational information system that is publicly accessible;
2. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
3. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system;
4. Reviews the content on the publicly accessible organizational information system for nonpublic information on an organization-defined frequency; and
5. Removes nonpublic information from the publicly accessible organizational information system, if discovered.

Supplemental Guidance

Information protected under the Privacy Act and vendor proprietary information are examples of nonpublic information. This requirement addresses posting information on an organizational

information system that is accessible to the general public, typically without identification or authentication.

Category

Common Governance, Risk, and Compliance (GRC) Requirement

Specification

1.1. Password policies can be configured in ePO (for user login to the ePO console)
1.2. Password strength can be defined in ePO.
1.3. ESM may have specific password strength requirement policy.
1.4. Credential rotation is not tracked by ePO, nor is extended non-use.

Verification Results

Satisfactory. The ESM has the password policy as follows: (1) at least eight characters long (2) at least one number (3) at least one punctuation or symbol (4) at least one uppercase, and (5) different from previous password by four characters.

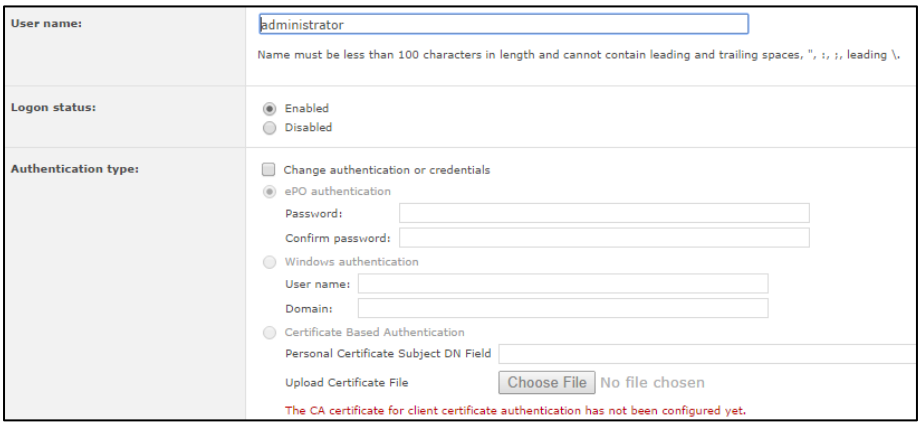


Figure 7. Password Policy for each user in ePO system.

There are three levels of policy (applied to each user) to choose from ePO system, which are (1) *low criticality*: any password strength (2) *Medium criticality*: apply the environment's password policy via Active Directory (3) *High criticality*: no password, leverage certificate authentication only. The figure above shows the password policy for ePO system.

A.2 Audit and Accountability (SG.AU)

Periodic audits and logging of the Smart Grid information system need to be implemented to validate that the security mechanisms present during Smart Grid information system validation testing are still installed and operating correctly. These security audits review and examine a Smart Grid information system's records and activities to determine the adequacy of Smart Grid information system security

requirements and to ensure compliance with established security policy and procedures. Audits also are used to detect breaches in security services through examination of Smart Grid information system logs. Logging is necessary for anomaly detection as well as forensic analysis.

A.2.1 Auditable Events (SG.AU-2)

Requirement

The organization—

1. Develops, based on a risk assessment, the Smart Grid information system list of auditable events on an organization-defined frequency;
2. Includes execution of privileged functions in the list of events to be audited by the Smart Grid information system; and
3. Revises the list of auditable events based on current threat data, assessment of risk, and post-incident analysis.

Supplemental Guidance

The purpose of this requirement is for the organization to identify events that need to be auditable as significant and relevant to the security of the Smart Grid information system.

Requirement Enhancements

1. The organization should audit activities associated with configuration changes to the Smart Grid information system.

Category

Common Technical Requirements, Integrity

Specification

1. Define list of events that must be stored for future security analysis by the McAfee ePO and McAfee ESM systems.
2. Ensure that all events are monitored, logged, and reported up to the ePO and ESM systems.

Verification Results

Satisfactory. List of auditable events can be selected in both McAfee ePO system (as shown below) and McAfee ESM system (as shown in the second figure). Moreover, users at ePO can also define their own events as shown in the third figure. All defined events are monitored and can be reported to user of both ESM and ePO systems as shown in the fourth and fifth figures, respectively.

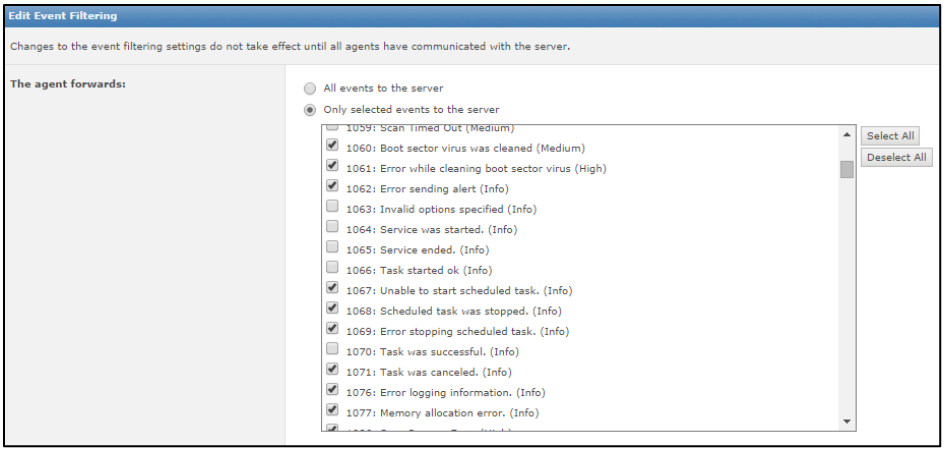


Figure 8. Event Filtering in ePO system.

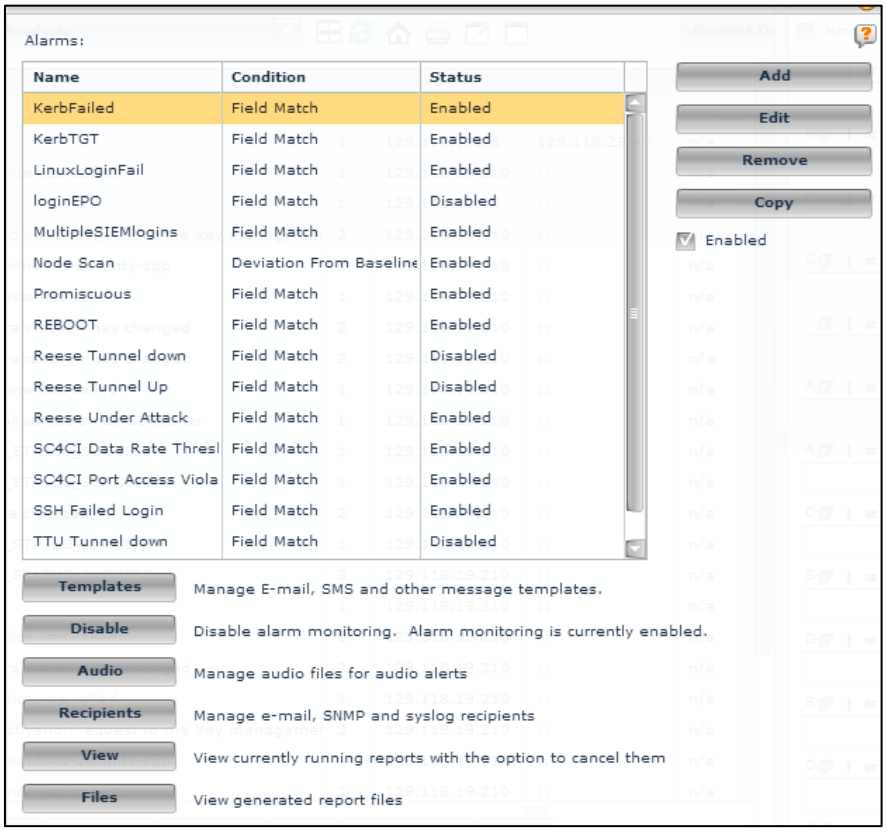


Figure 9. Event Editor and Filtering in ESM system.

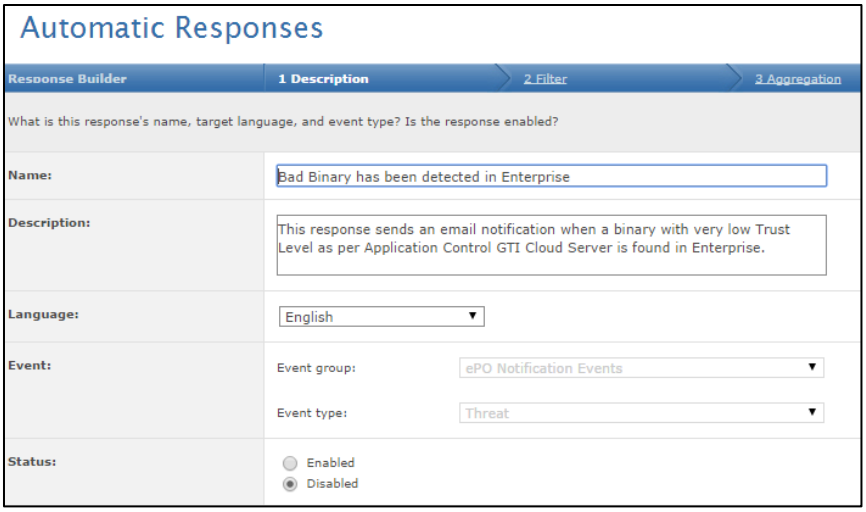
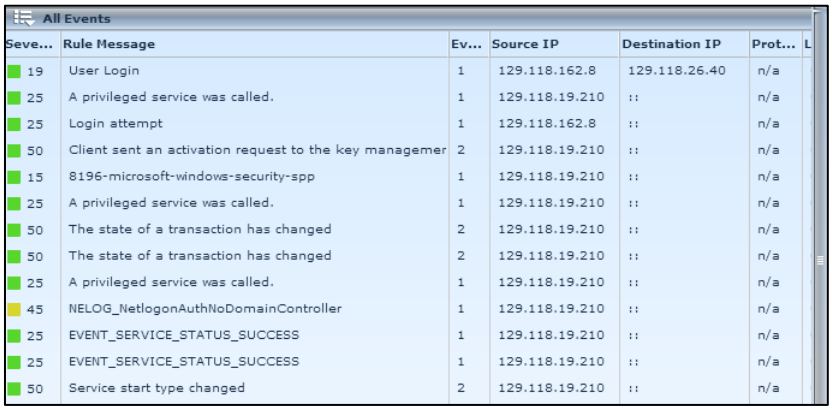


Figure 10. Automatic Responses for specific events in ePO system.



Seve...	Rule Message	Ev...	Source IP	Destination IP	Prot...
19	User Login	1	129.118.162.8	129.118.26.40	n/a
25	A privileged service was called.	1	129.118.19.210	::	n/a
25	Login attempt	1	129.118.162.8	::	n/a
50	Client sent an activation request to the key managemer	2	129.118.19.210	::	n/a
15	8196-microsoft-windows-security-spp	1	129.118.19.210	::	n/a
25	A privileged service was called.	1	129.118.19.210	::	n/a
50	The state of a transaction has changed	2	129.118.19.210	::	n/a
50	The state of a transaction has changed	2	129.118.19.210	::	n/a
25	A privileged service was called.	1	129.118.19.210	::	n/a
45	NELOG_NetlogonAuthNoDomainController	1	129.118.19.210	::	n/a
25	EVENT_SERVICE_STATUS_SUCCESS	1	129.118.19.210	::	n/a
25	EVENT_SERVICE_STATUS_SUCCESS	1	129.118.19.210	::	n/a
50	Service start type changed	2	129.118.19.210	::	n/a

Figure 11. Event log for ESM system.

Event Received Time	Threat Type	Event ID	Threat Target IPv4 Add	Reporter PayLoad	Reporter Type	Event Description	Threat Target IP Addres
11/22/13 4:54:34 PM	Reported Event-Nov:21	35400	129.118.26.8	IPT/FIREWALL VIOLATI	Firewall	IPTFW DOS Attack	0:0:0:0:1111:2222:33
11/22/13 4:54:34 PM	Reported Event-Nov:21	35400	129.118.26.8	IPT/FIREWALL VIOLATI	Firewall	IPTFW DOS Attack	0:0:0:0:1111:2222:33
11/22/13 5:00:26 PM	Reported Event-Nov:21	35400	129.118.105.50	IPT/FIREWALL VIOLATI	Firewall	IPTFW DOS Attack	0:0:0:0:1111:2222:33
11/22/13 5:00:26 PM	Reported Event-Nov:21	35400	129.118.105.50	IPT/FIREWALL VIOLATI	Firewall	IPTFW DOS Attack	0:0:0:0:1111:2222:33
11/22/13 5:00:26 PM	Reported Event-Nov:21	35400	129.118.105.50	IPT/FIREWALL VIOLATI	Firewall	IPTFW DOS Attack	0:0:0:0:1111:2222:33
11/22/13 5:00:25 PM	Reported Event-Nov:22	35403	129.118.105.50	IPTABLES LEVEL 3 WEF	Firewall	IPTFWUpdated	0:0:0:0:1111:2222:33
11/22/13 5:00:26 PM	Reported Event-Nov:22	35403	129.118.105.50	IPTABLES LEVEL 3 WEF	Firewall	IPTFWUpdated	0:0:0:0:1111:2222:33
11/22/13 4:54:34 PM	Reported Event-Nov:22	35403	129.118.26.8	IPTABLES LEVEL 3 WEF	Firewall	IPTFWUpdated	0:0:0:0:1111:2222:33
11/22/13 4:54:34 PM	Reported Event-Nov:22	35403	129.118.26.8	IPTABLES LEVEL 3 WEF	Firewall	IPTFWUpdated	0:0:0:0:1111:2222:33
11/22/13 4:54:34 PM	Reported Event-Nov:22	35403	129.118.26.8	IPTABLES LEVEL 3 WEF	Firewall	IPTFWUpdated	0:0:0:0:1111:2222:33
11/22/13 4:54:33 PM	Reported Event-Nov:22	35403	129.118.26.8	IPTABLES LEVEL 3 WEF	Firewall	IPTFWUpdated	0:0:0:0:1111:2222:33

Figure 12. Event log in ePO system.

A.2.2 Content of Audit Records (SG.AU-3)

Requirement

The Smart Grid information system produces audit records for each event. The record contains the following information:

- Data and time of the event,
- The component of the Smart Grid information system where the event occurred,
- Type of event,
- User/subject identity, and
- The outcome of the events.

Additional Considerations

1. The Smart Grid information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject; and
2. The Smart Grid information system provides the capability to centrally manage the content of audit records generated by individual components throughout the Smart Grid information system.

Category

Common Technical Requirements, Integrity

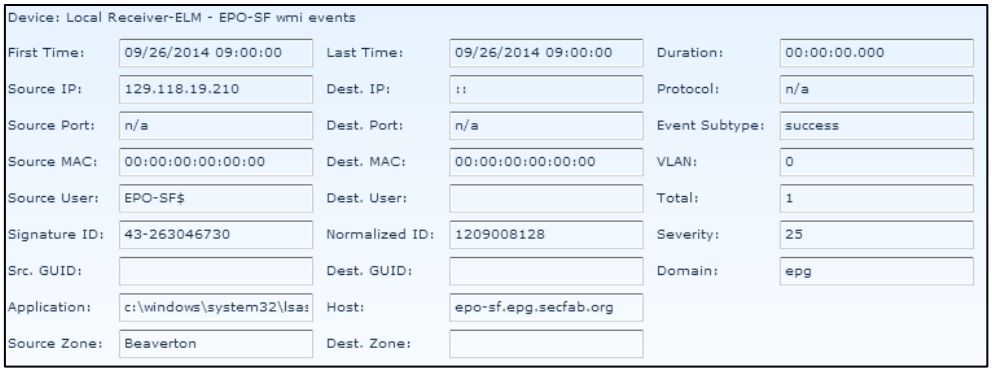
Specification

1. Define list of events that must be stored for future security analysis by the McAfee ePO and McAfee ESM systems.
2. Include the following fields in each audit record:
   - Date and time
   - Asset ID
   - Type of event
   - User/subject identity (if applicable, else the machine principal)
   - Outcome of event

Include additional information as needed on location, subject, type, etc. Audit records are centrally managed in the ESM.

Verification Results

Satisfactory. McAfee ESM system can be configured to include additional information to the defined auditable event. An example of audited event that meet the criteria of the requirement is shown below.



Device: Local Receiver-ELM - EPO-SF wmi events

First Time:	09/26/2014 09:00:00	Last Time:	09/26/2014 09:00:00	Duration:	00:00:00.000
Source IP:	129.118.19.210	Dest. IP:	::	Protocol:	n/a
Source Port:	n/a	Dest. Port:	n/a	Event Subtype:	success
Source MAC:	00:00:00:00:00:00	Dest. MAC:	00:00:00:00:00:00	VLAN:	0
Source User:	EPO-SF$	Dest. User:		Total:	1
Signature ID:	43-263046730	Normalized ID:	1209008128	Severity:	25
Src. GUID:		Dest. GUID:		Domain:	epg
Application:	c:\windows\system32\lsa:	Host:	epo-sf.epg.secfab.org		
Source Zone:	Beaverton	Dest. Zone:			

Figure 13. Content of audit event from ESM.

A.2.3 Audit Storage Capacity (SG.AU-4)

Requirement

The organization allocates organization-defined audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

Supplemental Guidance

The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity.

Category

Common Technical Requirements, Integrity

Specification

1. NA/Organizational
2. Ensure that all file systems and historian databases have sufficient space allocated to store the appropriate quantity of events. Event storage includes device file system as well as back-end situational awareness systems such as ePO/ESM databases.
3. On device: enable log rotation. For remote logging, define only those events and logs on the endpoint that are appropriate for determining security metrics on the back-end. Do not simply include all logs.

Verification Results

Satisfactory. While the specification does not describe the capacity of audit record storage for the proposed system, there is a policy (log rotation) for reducing the likelihood of exceeding capacity on device in WRL (Wind River Linux) on both TTU and Reese sites.

A.2.4 Response to Audit Processing Failures (SG.AU-5)

Requirement

The Smart Grid information system—

1. Alerts designated organizational officials in the event of an audit processing failure; and
2. Executes an organization-defined set of actions to be taken (e.g., shutdown Smart Grid information system, overwrite oldest audit records, and stop generating audit records).

Supplemental Guidance

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

Requirement Enhancements

1. The Smart Grid information system provides a warning when allocated audit record storage volume reaches an organization-defined percentage of maximum audit record storage capacity; and
2. The Smart Grid information system provides a real-time alert for organization defined audit failure events.

Category

Common Governance, Risk, and Compliance (GRC)

Specification

1. in ePO, define personnel that may be notified. Enter them into the "Contacts" section.
2. define ePO Automated Responses to notify one or more "Contacts" via email that an event of interest has occurred on an endpoint.
3. NA/Organizational (organization documents these actions for personnel to enact)
4. Organizationally defined actions will be taken upon audit processing failures. For example: person X is notified via email when a processing error occurs.
5. NA/Organizational (organization defines the percentage of capacity usage to alert on)
6. Endpoint: NA/Organizational (logs on endpoint are remotely monitored, so log file overflow does not concern Security Fabric) [see SG.AU-4.1]
7. NA/Organizational (organization defines alerts that should be near-real-time in nature, e.g. network whitelisting violation, or firewall violation)
8. Events are being monitored in near-real-time by both ePO and ESM.

When events are captured by ePO, the system state can be immediately altered and automated responses triggered. When events are captured by ESM, a notification is sent to ePO, triggering a state change, and an automated response can be triggered.

Verification Results

Satisfactory. The proposed system has the mechanism to alert security administrator by sending an email to the specified contact person when specific event occurs. This mechanism can be used when there is a failure in processing of audit records. The figure below shows an example of email message to contact a person when there is a new update for software component.

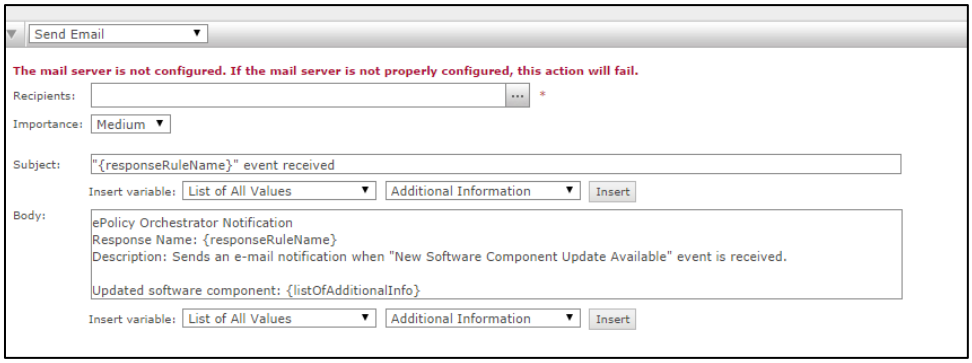


Figure 14. Alerting mechanism in ePO system.

A.2.5 Audit Monitoring, Analysis, and Reporting (SG.AU-6)

Requirement

The organization—

1. Reviews and analyzes Smart Grid information system audit records on an organization-defined frequency for indications of inappropriate or unusual activity and reports findings to management authority; and
2. Adjusts the level of audit review, analysis, and reporting within the Smart Grid information system when a change in risk occurs to organizational operations, organizational assets, or individuals.

Supplemental Guidance

Organizations increase the level of audit monitoring and analysis activity within the Smart Grid information system based on, for example, law enforcement information, intelligence information, or other credible sources of information.

Additional Considerations

1. The Smart Grid information system employs automated mechanisms to integrate audit review, analysis, and reporting into organizational processes for investigation and response to suspicious activities;

2. The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness;
3. The Smart Grid information system employs automated mechanisms to centralize audit review and analysis of audit records from multiple components within the Smart Grid information system; and
4. The organization integrates analysis of audit records with analysis of performance and network monitoring information to further enhance the ability to identify inappropriate or unusual activity.

Category

Common Governance, Risk, and Compliance (GRC)

Specification

1. NA/Organizational: organization defines the frequency
2. The platform assists in the gathering of data and identifies inappropriate or unusual activity.
3. NA/Organizational: notification to the appropriate management authority is left to the discretion of the organization
4. NA/Organizational: depends upon the organization's response to specific triggers by changing the level of audit, review, analysis, and reporting.

Verification Results

Satisfactory. ESM and ePO provide a mechanism for monitoring the audit records, analysis using the defined condition, and reporting the content from audit records. These evidences were captured in Figures 8, 10-12, and the two below.

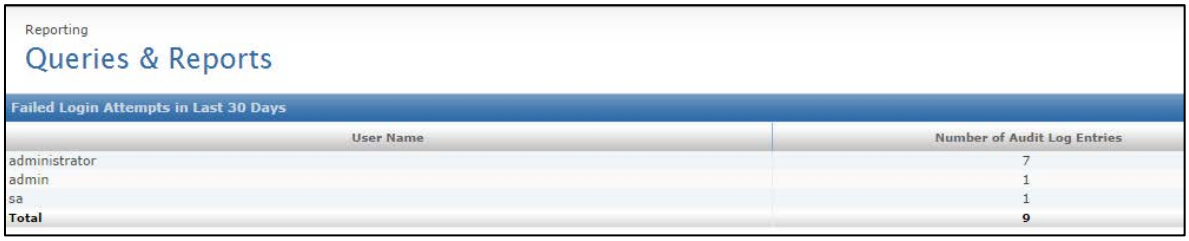


Figure 15. Report generation from ePO system.

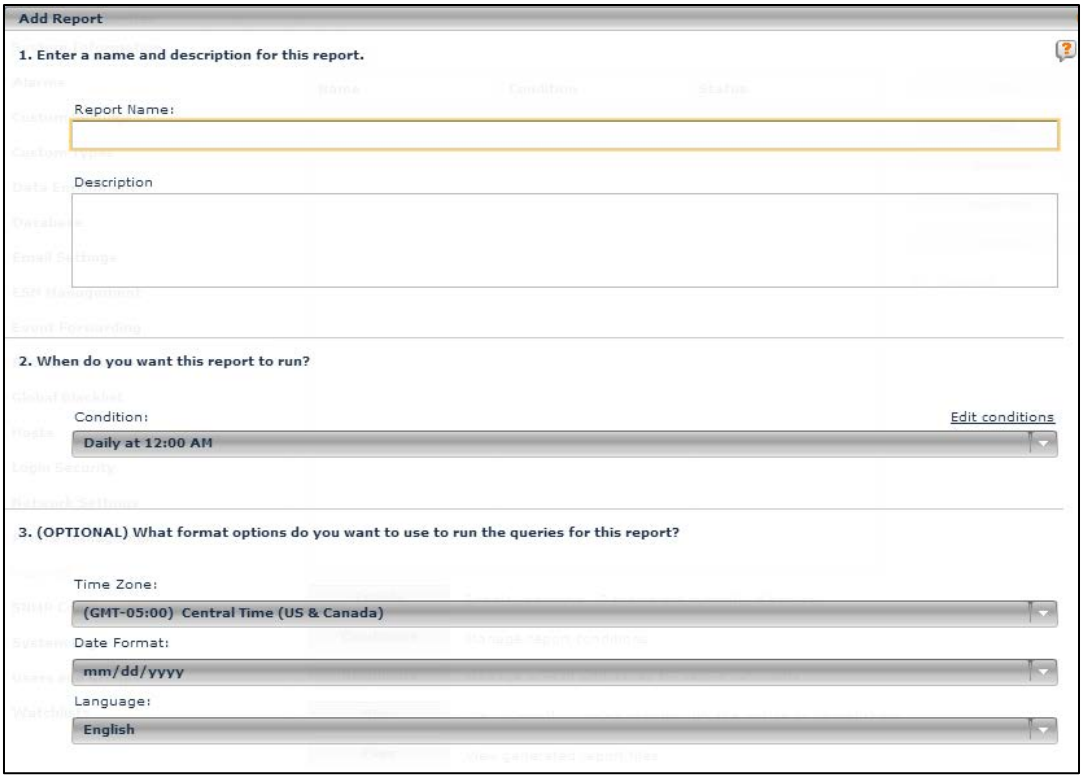


Figure 16. Report generation in ESM.

A.2.6 Audit Reduction, and Report Generation (SG.AU-7)

Requirement

The Smart Grid information system provides an audit reduction and report generation capability.

Supplemental Guidance

Audit reduction and reporting may support near real-time analysis and after-the-fact investigations of security incidents.

Additional Considerations

1. The Smart Grid information system provides the capability to automatically process audit records for events of interest based on selectable event criteria

Category

Common Governance, Risk, and Compliance (GRC)

Specification

A mechanism exists on the ESM and ePO to allow generation of reports and will support near real-time analysis. Search functionality in the ESM enables audit reduction. Reporting, Dashboards, and Queries in ePO also enable the conversion from raw data into information for human consumption by reducing, sorting, filtering, and leveraging visualization techniques.

Verification Results

Satisfactory. ESM and ePO have the mechanism for report generation as shown in Figures 15-16. In term of audit reduction, both components provide event filtering and the condition for report generation as shown in the next two figures, respectively.

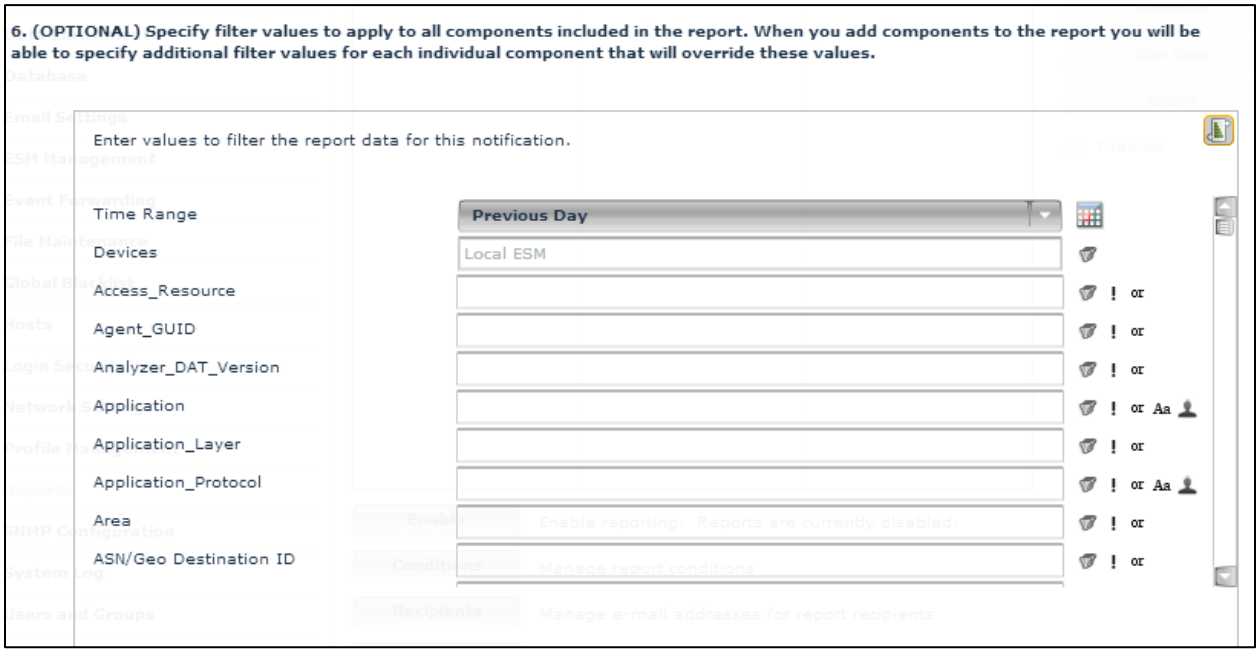


Figure 17. Event filtering in report generation from ESM.

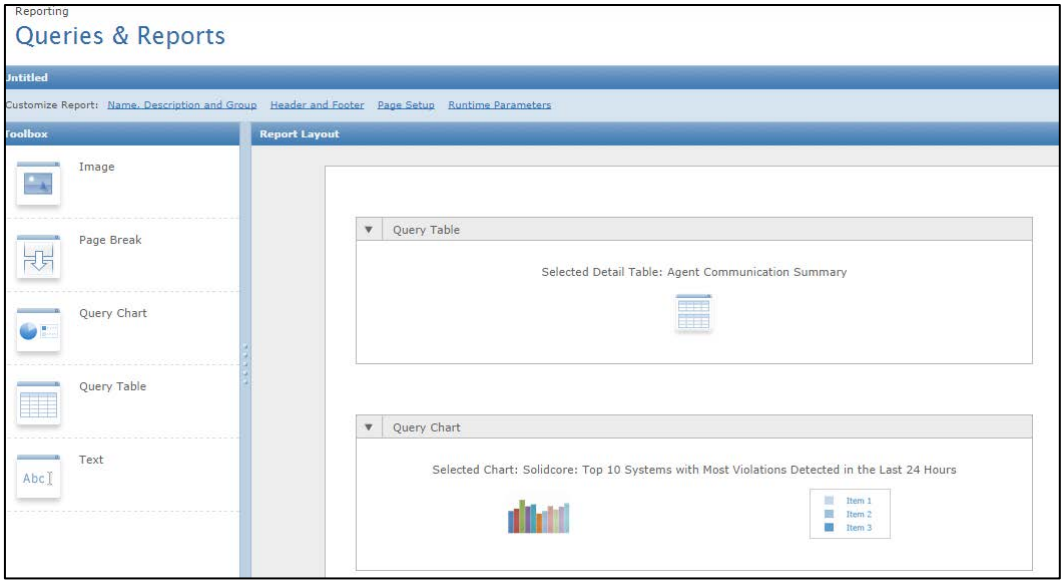


Figure 18. Event filtering in report generation from ePO.

A.2.7 Time Stamps (SG.AU-8)

Requirement

The Smart Grid information system uses internal system clocks to generate time stamps for audit records.

Supplemental Guidance

Time stamps generated by the information system include both date and time, as defined by the organization.

Requirement Enhancements

1. The Smart Grid information system synchronizes internal Smart Grid information system clocks on an organization-defined frequency using an organization-defined time source.

Category

Common Governance, Risk, and Compliance (GRC)

Specification

Regardless of whether the information system uses internal system clocks, the Security Fabric platform leverages internal clocks to generate accurate time stamps for audit records.

- clock synchronization using NTP is supported, and a time source is required
- frequency of synchronization is configurable in the platform

- The platform ensures that the platform synchronizes its internal clocks at the configured frequency using the configured time source(s).

Verification Results

Satisfactory. The content of audit record in both ePO and ESM uses the internal system clocks (which can acquire the time from NTP by specifying the server as shown below) to generate time stamps for the record as shown in the audit content records from Figures 12-13.

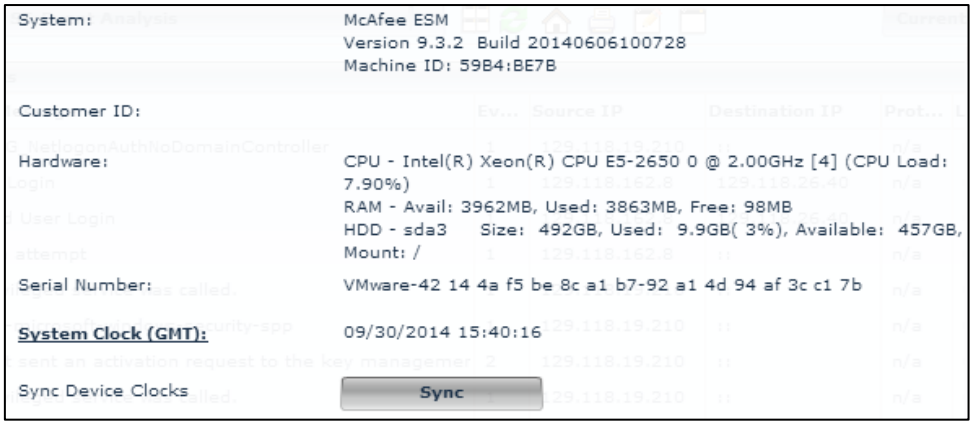


Figure 19. ESM system clock configuration.

A.2.8 Protection of Audit Information (SG.AU-9)

Requirement

The Smart Grid information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Supplemental Guidance

Audit information includes, for example, audit records, audit settings, and audit reports.

Additional Considerations

1. The Smart Grid information system produces audit records on hardware-enforced, write-once media.

Category

Common Governance, Risk, and Compliance (GRC)

Specification

The platform protects audit information and audit tools from unauthorized access, modification, and deletion via authentication and authorization controls (access control).

Access to specific functional components is managed by the permissions assigned to the roles on each resource.

Verification Results

Satisfactory. Both ESM and ePO have the authentication and authorization controls to protect the system from unauthorized access as shown in Table 1.

A.2.9 Audit Record Retention (SG.AU-10)

Requirement

The organization retains audit logs for an organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Category

Common Governance, Risk, and Compliance (GRC)

Specification

1. NA/Organizational
2. Audit records, including logs, are retained for a configurable amount of time as required to support investigations and regulatory requirements.

Verification Results

Satisfactory. The proposed system does not define the time period to provide support for after-the-fact investigations of security incidents. However, the provider of the system (McAfee) claims to use the available space as the measure of how long the message can retain in the system. The following is what provider's claim:

- The proposed system provided space for 500GB
- 1061.8MB is used for the base (available space for keeping record is around 400GB)
- The **estimate** for daily event is around 2.35MB
- 400GB/2.35MB is around 466.33 years

If the daily event does not exceed the estimated value, all events can be stored in the proposed system.

A.2.10 Conduct and Frequency of Audits (SG.AU-11)

Requirement

The organization conducts audits on an organization-defined frequency to assess conformance to specified security requirements and applicable laws and regulations.

Supplemental Guidance

Audits can be either in the form of internal self-assessment (sometimes called first-party audits) or independent, third-party audits.

Category

Common Governance, Risk, and Compliance (GRC)

Specification

1. NA/Organizational (defined frequency)
2. NA/Organizational (audits relative to defined frequency)
3. Regular audits are measured for compliance with the security requirements, processes and regulations. A combination of Technical controls + Policy compliance tools are required.

Verification Results

Satisfactory. ESM and ePO can automatically generate the report according to the organization defined time. This mechanism helps the organizations to conducts the audition based on their defined frequency to access conformance to their own specified security requirement.

A.2.11 Security Policy Compliance (SG.AU-14)

Requirement

The organization demonstrates compliance to the organization's security policy through audits in accordance with the organization's audit program.

Supplemental Guidance

Periodic audits of the Smart Grid information system are implemented to demonstrate compliance to the organization's security policy. These audits—

1. Assess whether the defined cyber security policies and procedures, including those to identify security incidents, are being implemented and followed;
2. Document and ensure compliance to organization policies and procedures;

3. Identify security concerns, validate that the Smart Grid information system is free from security compromises, and provide information on the nature and extent of compromises should they occur;
4. Validate change management procedures and ensure that they produce an audit trail of reviews and approvals of all changes;
5. Verify that security mechanisms and management practices present during Smart Grid information system validation are still in place and functioning;
6. Ensure reliability and availability of the Smart Grid information system to support safe operation; and
7. Continuously improve performance.

Category

Common Governance, Risk, and Compliance (GRC)

Specification

Compliance to the security policy is tracked through event collection and correlation, assessments/analytics, and identification of potential security concerns. It is left to the organization to demonstrate compliance to the security policy.

Verification Results

Satisfactory. The security policy in Smart Grid system is described electronically in policy management of ePO system. To demonstrate the compliance of the policy, the organization needs to specify events to be monitored in the organization defined security policy in both ePO and ESM. This requires experiential knowledge of ePO and ESM systems (e.g., see SG.AC-2 as an example of security policy specification and SG.AU-2, SG.AU-5, SG.AU-7 for audit and report generation).

A.2.12 Audit Generation (SG.AU-15)

Requirement

The Smart Grid information system—

1. Provides audit record generation capability and generates audit records for the selected list of auditable events; and
2. Provides audit record generation capability and allows authorized users to select auditable events at the organization-defined Smart Grid information system components.

Supplemental Guidance

Audit records can be generated from various components within the Smart Grid information system.

Additional Considerations

1. The Smart Grid information system provides the capability to compile audit records from multiple components within the Smart Grid information system into a Smart Grid information system-wide audit trail that is time-correlated to within an organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail.

Category

Common Technical Requirements, Integrity

Specification

Ensure the audit records are generated for specific auditable events as defined by authorized users.

Verification Results

Satisfactory if the specification explicitly states what or how the audit generation can be done in the proposed system. In other words, ESM and ePO, as the centralization of security management in proposed system, allow user to specify event to be monitored (as shown in SG.AU-6 and SG.AU-2). Moreover, both ESM and ePO have the ability to automatically generate the report (as shown in SG.AU-7).

A.2.13 Non-Repudiation (SG.AU-16)

Requirement

The Smart Grid information system protects against an individual falsely denying having performed a particular action.

Supplemental Guidance

Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Non-repudiation services are implemented using various techniques (e.g., digital signatures, digital message receipts, and logging).

Category

Unique Technical Requirements

Specification

ESM event monitoring coupled with log files will prevent individuals from falsely denying specific actions.

Verification Results

Satisfactory. Non-repudiation services are implemented using logging techniques (i.e., event monitoring and audit generation) in both ESM and ePO systems as shown in SG.AU-2, SG.AU-6, SG.AU-7, SG.AU-8 and SG.AU-9).

A.3 Security Assessment and Authorization (SG.CA)

Security assessments include monitoring and reviewing the performance of Smart Grid information system. Internal checking methods, such as compliance audits and incident investigations, allow the organization to determine the effectiveness of the security program. Finally, through continuous monitoring, the organization regularly reviews compliance of the Smart Grid information systems. If deviations or nonconformance exist, it may be necessary to revisit the original assumptions and implement appropriate corrective actions.

A.3.1 Smart Grid Information System Connections (SG.CA-4)

Requirement

The organization—

1. Authorizes all connections from the Smart Grid information system to other information systems;
2. Documents the Smart Grid information system connections and associated security requirements for each connection; and
3. Monitors the Smart Grid information system connections on an ongoing basis, verifying enforcement of documented security requirements.

Supplemental Guidance

The organization considers the risk that may be introduced when a Smart Grid information system is connected to other information systems, both internal and external to the organization, with different security requirements. Risk considerations also include Smart Grid information systems sharing the same networks.

Additional Considerations

1. All external Smart Grid information system and communication connections are identified and protected from tampering or damage.

Category

Common Governance, Risk, and Compliance (GRC)

Specification

1. Any the information system on the platform requesting a service from any other information system, it be, server side or end point, is authenticated before establishing connection. Kerberos V5 protocol is used to authenticate end points systems for secure communication services and HTTPS with PKI is used to authenticate web server (EPO) and agent.
    a. Every information system within the platform would need to be authorized to connect to an external system.
    b. same as above
2. ESM is configured to monitor and record the start/stop/reset of the connections.
3. Information is available near real-time.

Verification Results

Satisfactory. Security Policy in ePO has the features to configure the authorization of all connection from the Smart Grid information system to other information systems (see SG.AC-4 and SG.AC-19). All of security policy is appeared in electronic form and can be printed as the document for audition. All allowed connection could be monitored via ESM (see SG.AU-6 and SG.AU-15).

A.3.2 Continuous Monitoring (SG.CA-6)

Requirement

The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:

1. Ongoing security requirements assessments in accordance with the organizational continuous monitoring strategy; and
2. Reporting the security state of the Smart Grid information system to management authority on an organization-defined frequency.

Supplemental Guidance

A continuous monitoring program allows an organization to maintain the security authorization to operate of a Smart Grid information system over time in a dynamic operational environment with changing threats, vulnerabilities, technologies, and missions/business processes.

The selection of an appropriate subset of security requirements for continuous monitoring is based on the impact level of the Smart Grid information system, the specific security requirements selected by the organization, and the level of assurance that the organization requires.

Additional Considerations

1. The organization employs an independent assessor or assessment team to monitor the security requirements in the Smart Grid information system on an ongoing basis;

2. The organization includes as part of security requirements continuous monitoring, periodic, unannounced, in-depth monitoring, penetration testing, and red team exercises; and
3. The organization uses automated support tools for continuous monitoring.

Category

Common Governance, Risk, and Compliance (GRC)

Specification

1. ESM (automated tool) is the continuous monitoring tool on the platform.
2. Reporting the security state of the information system to management authority (in EPO) on a defined frequency.

Verification Results

Satisfactory. Ongoing security requirements assessments in accordance with the organizational continuous monitoring strategy can be defined in ESM, which is a tool for continuous monitoring (see SG.AU-15 and SG.AU-6). The security state of the Smart Grid information system for managing the authority can be reported by using ePO (see SG.AU-6).

A.4 Configuration and Management (SG.CM)

The organization's security program needs to implement policies and procedures that create a process by which the organization manages and documents all configuration changes to the Smart Grid information system. A comprehensive change management process needs to be implemented and used to ensure that only approved and tested changes are made to the Smart Grid information system configuration. Smart Grid information systems need to be configured properly to maintain optimal operation. Therefore, only tested and approved changes should be allowed on a Smart Grid information system. Vendor updates and patches need to be thoroughly tested on a non-production Smart Grid information system setup before being introduced into the production environment to ensure that no adverse effects occur.

A.4.1 Configuration Settings (SG.CM-6)

Requirement

The organization—

1. Establishes configuration settings for components within the Smart Grid information system;
2. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures;
3. Documents changed configuration settings;
4. Identifies, documents, and approves exceptions from the configuration settings; and
5. Enforces the configuration settings in all components of the Smart Grid information system.

Additional Considerations

1. The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings;
2. The organization employs automated mechanisms to respond to unauthorized changes to configuration settings; and
3. The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.

Category

Common Governance, Risk, and Compliance (GRC)

Specification

1. Configuration settings are defined in ePO policy
2. Monitoring of changes is managed via the policy definitions in the policy catalog on ePO.
    a. NA - organizational policy
3. The policy compare functionality can be leveraged to determine what has changed.
    a. NA - organizational policy
    b. NA - organizational policy
    c. NA - organizational policy
4. Enforcement of configuration settings in all components is tracked in ePO.

Verification Results

Satisfactory. The security policy for all components (as shown in the first figure) within the Smart Grid information system can be configured in ePO (see SG.AC-19). The policy changes can be monitored via the policy definitions in the policy catalog on ePO as shown in the second figure.

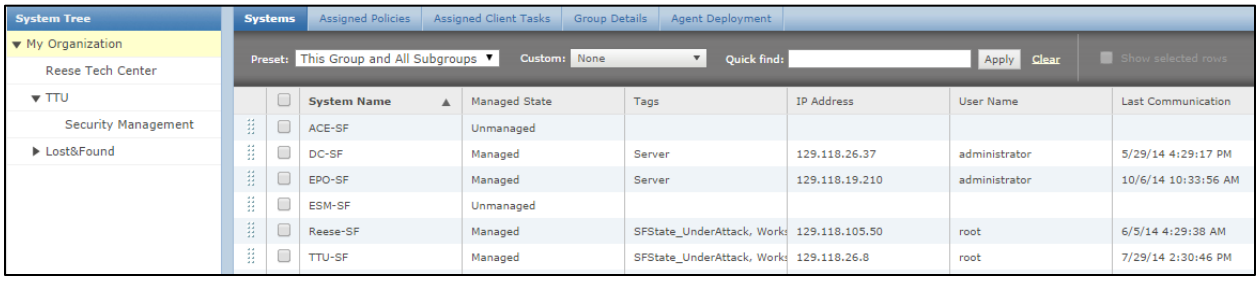
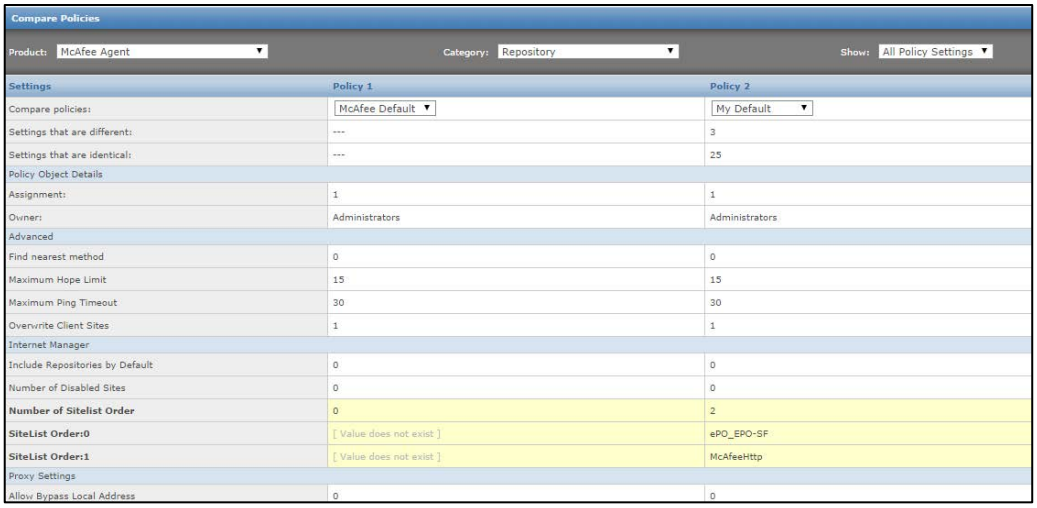


Figure 20. Components controlled by Security Fabric Environment.



Compare Policies

Product: McAfee Agent | Category: Repository | Show: All Policy Settings

Settings	Policy 1	Policy 2
Compare policies:	McAfee Default	My Default
Settings that are different:	---	3
Settings that are identical:	---	25
Policy Object Details		
Assignment:	1	1
Owner:	Administrators	Administrators
Advanced		
Find nearest method	0	0
Maximum Hope Limit	15	15
Maximum Ping Timeout	30	30
Overwrite Client Sites	1	1
Internet Manager		
Include Repositories by Default	0	0
Number of Disabled Sites	0	0
Number of Sitelist Order	0	2
SiteList Order:0	[Value does not exist]	ePO_EPO-SF
SiteList Order:1	[Value does not exist]	McAfeeHttp
Proxy Settings		
Allow Bypass Local Address	0	0

Figure 21. Policy comparison for tracking the changing of policy in ePO.

A.4.2 Configuration for Least Functionality (SG.CM-7)

Requirement

1. The organization configures the Smart Grid information system to provide only essential capabilities and specifically prohibits and/or restricts the use of functions, ports, protocols, and/or services as defined in an organizationally generated “prohibited and/or restricted” list; and
2. The organization reviews the Smart Grid information system on an organization-defined frequency or as deemed necessary to identify and restrict unnecessary functions, ports, protocols, and/or services.

Supplemental Guidance

The organization considers disabling unused or unnecessary physical and logical ports on Smart Grid information system components to prevent unauthorized connection of devices, and considers designing the overall system to enforce a policy of least functionality.

Category

Common Technical Requirements, Integrity

Specification

1. Firewall policy is defined in EPO. Configure policies to apply firewall rules on the systems for exposing only ports or protocols that are needed, and deny all others (therefore creating a default list of prohibited or restricted" resources.
    a. Only capabilities specifically allowed by the firewall are exposed
    b. All functionality not explicitly allowed is denied

Verification Results

Satisfactory. Firewall policy defined in ePO (as shown in Figure 6) can be configured to allow the organization providing only essential capabilities and specifically prohibits and/or restricts the use of functions, ports, protocols, and/or services as defined in an organizationally. All of the firewall policy can be viewed and modified in ePO system (see SG.AU-19).

A.4.3 Component Inventory (SG.CM-8)

Requirement

The organization develops, documents, and maintains an inventory of the components of the Smart Grid information system that—

1. Accurately reflects the current Smart Grid information system configuration;
2. Provides the proper level of granularity deemed necessary for tracking and reporting and for effective property accountability;
3. Identifies the roles responsible for component inventory;
4. Updates the inventory of system components as an integral part of component installations, system updates, and removals; and
5. Ensures that the location (logical and physical) of each component is included within the Smart Grid information system boundary.

Supplemental Guidance

The organization determines the appropriate level of granularity for any Smart Grid information system component included in the inventory that is subject to management control (e.g., tracking, reporting).

Additional Considerations

1. The organization updates the inventory of the information system components as an integral part of component installations and information system updates;
2. The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available inventory of information system components; and
3. The organization employs automated mechanisms to detect the addition of unauthorized components or devise into the environment and disables access by components or devices or notifies designated officials.

Category

Common Technical Requirements, Integrity

Specification

1. The inventory of (security) components/controls is tracked by ePO and regularly refreshed.
2. Installs, updates (and removals) modify the (security) inventory tracked on ePO.

Verification Results

Satisfactory. All agents, security components (i.e., Wind River Linux front-end), in security fabric system are listed, tracked and controlled in ePO system as shown in Figure 20 and Figure 22.

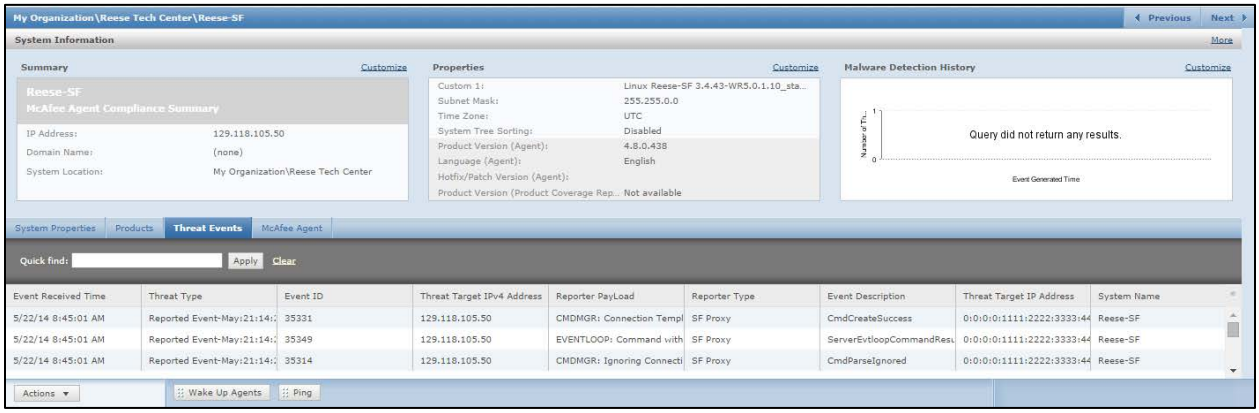


Figure 22. Status of controlled agent in ePO system.

A.5 Continuity of Operations (SG.CP)

Continuity of operations addresses the capability to continue or resume operations of a Smart Grid information system in the event of disruption of normal system operation. The ability for the Smart Grid information system to function after an event is dependent on implementing continuity of operations policies, procedures, training, and resources. The security requirements recommended under the continuity of operations family provide policies and procedures for roles and responsibilities, training, testing, plan updates, alternate storage sites, alternate command and control methods, alternate control centers, recovery and reconstitution and fail-safe response.

A.5.1 Smart Grid Information System Recovery and Reconstitution (SG.CP-10)

Requirement

The organization provides the capability to recover and reconstitute the Smart Grid information system to a known secure state after a disruption, compromise, or failure.

Supplemental Guidance

Smart Grid information system recovery and reconstitution to a known secure state means that—

1. All Smart Grid information system parameters (either default or organization-established) are set to secure values;
2. Security-critical patches are reinstalled;
3. Security-related configuration settings are reestablished;
4. Smart Grid information system documentation and operating procedures are available;
5. Application and Smart Grid information system software is reinstalled and configured with secure settings;
6. Information from the most recent, known secure backups is loaded; and
7. The Smart Grid information system is fully tested.

Requirement Enhancements

1. The organization provides compensating security controls (including procedures or mechanisms) for the organization-defined circumstances that inhibit recovery to a known, secure state; and
2. The organization provides the capability to reimage Smart Grid information system components in accordance with organization-defined restoration time periods from configuration-controlled and integrity-protected media images representing a secure, operational state for the components.

Category

Common Governance, Risk, and Compliance (GRC)

Specification

1. Leveraging the virtualization capabilities, a compromised endpoint VM can simply be replaced to bring the device back to the original "clean" state.
2. The capability to reimage the information system is inherent in the platform's architecture

Verification Results

Satisfactory. The application modules (ePDC and RTDMS) in security fabric framework are deployed as the virtualization operating system on top of ESXi hypervisor component. Any disruption, compromise, or failure in the application modules can be recovered and reconstituted into the secure state (i.e., state that security administrator known that there is no failure in the system).

A.5.2 Fail-Safe Response (SG.CP-11)

Requirement

The Smart Grid information system has the ability to execute an appropriate fail-safe procedure upon the loss of communications with other Smart Grid information systems or the loss of the Smart Grid information system itself.

Supplemental Guidance

In the event of a loss of communication between the Smart Grid information system and the operational facilities, the on-site instrumentation needs to be capable of executing a procedure that provides the maximum protection to the controlled infrastructure. For the electric sector, this may be to alert the operator of the failure and then do nothing (i.e., let the electric grid continue to operate). The organization defines what "loss of communications" means (e.g., 5 seconds or 5 minutes without communications). The organization then defines the appropriate fail-safe process for its industry.

Additional Considerations

1. The Smart Grid information system preserves the organization-defined state information in failure.

Category

Common Governance, Risk, and Compliance (GRC)

Specification

Upon loss of communications with other systems (especially the management system (ePO), monitoring system (ESM), and AAA system (Active Directory)), the endpoint continues to function in its last known good condition.

Loss of an entire endpoint node is remediated by deploying a new node with the same virtual instances

Verification Results

Satisfactory. Since the ePO and ESM, the central management and audition component in security fabric, are loosely coupled with the main communication components (entire endpoints, i.e., McAfee agent in Wind River Linux on ePDC and RTDMS), the loss of communications between control system (ePO and ESM) and communication node will cause less effect to smart grid information system. However, the event auditing in communication nodes might not be able to log in ESM and ePO.

In case of losing an entire endpoint, because of virtualization technique, security administrator can deploy the new node using the image from the previously known working states.

A.6 Identification and Authentication (SG.IA)

Identification and authentication is the process of verifying the identity of a user, process, or device, as a prerequisite for granting access to resources in a Smart Grid information system.

A.6.1 Authenticator Management (SG.IA-3)

Requirement

The organization manages Smart Grid information system authentication credentials for users and devices by—

1. Defining initial authentication credential content, such as defining password length and composition, tokens;
2. Establishing administrative procedures for initial authentication credential distribution; lost, compromised, or damaged authentication credentials; and revoking authentication credentials;
3. Changing/refreshing authentication credentials on an organization-defined frequency; and
4. Specifying measures to safeguard authentication credentials.

Supplemental Guidance

Measures to safeguard user authentication credentials include maintaining possession of individual authentication credentials, not loaning or sharing authentication credentials with others, and reporting lost or compromised authentication credentials immediately.

Additional Considerations

1. The organization employs automated tools to determine if authentication credentials are sufficiently strong to resist attacks intended to discover or otherwise compromise the authentication credentials; and
2. The organization requires unique authentication credentials be provided by vendors and manufacturers of Smart Grid information system components.

Category

Common Governance, Risk, and Compliance (GRC)

Specification

In back-end management system, ePO, the credential (username/password) requirements can be defined to enforce minimum strength requirements.

On front-end systems, the M2M credentials for mutual authentication are implemented via Kerberos. Therefore, the tickets are well defined in KRB standards. In addition, the credentials (keys) for mutual authentication and encryption on the Security Communication Channel are implemented by distributing the public key of the endpoint Mgmt Instance back to ePO, signing the public key (thus a certificate is generated), registering the Machine principal with Kerberos (creating the keytab file), and returning all to the endpoint.

Initial credential distribution is supported in the commissioning/provisioning steps for the platform's endpoints (described in above).

In case of credential compromise, loss, damage, etc. the re-provisioning workflow will generate new credentials for the endpoints to ensure that the communications can continue.

Revoking M2M credentials on the endpoint can be implemented by removing the instance in question in Kerberos, and causing a new kinit to execute. This will force the connection attempt to fail, thus enforcing the credential revocation.

Revoking credentials in Active Directory/KRB, ePO and ESM is implemented by changing the login credentials (password) or locking the account.

However, the system can be leveraged to create scheduled tasks, such as refreshing the credentials on a recurring basis.

The authenticators are available on the server side systems which are locked down for public access. Only authenticated and authorized users can access them. The authenticators are neither shared nor communicated in any form over network, and are encrypted in the database on the server side (ePO). The default credentials are modified for security reasons after initial installation.

On the endpoint, the credentials (keys) are stored in secured folders (leveraging A***c***cess Control mechanisms in Wind River Linux) to secure the credentials.

Verification Results

Satisfactory. The authenticator management for user in ePO and ESM (see SG.AC-20) satisfies this requirement. For device to device, the proposed system uses the Kerberos as the authenticator. In case of lost, compromised, or damaged authentication credentials, the re-provisioning of credentials will generate new credentials for all endpoint to ensure that the communications are secure. The key management for device-to-device authentication in ePO is below.

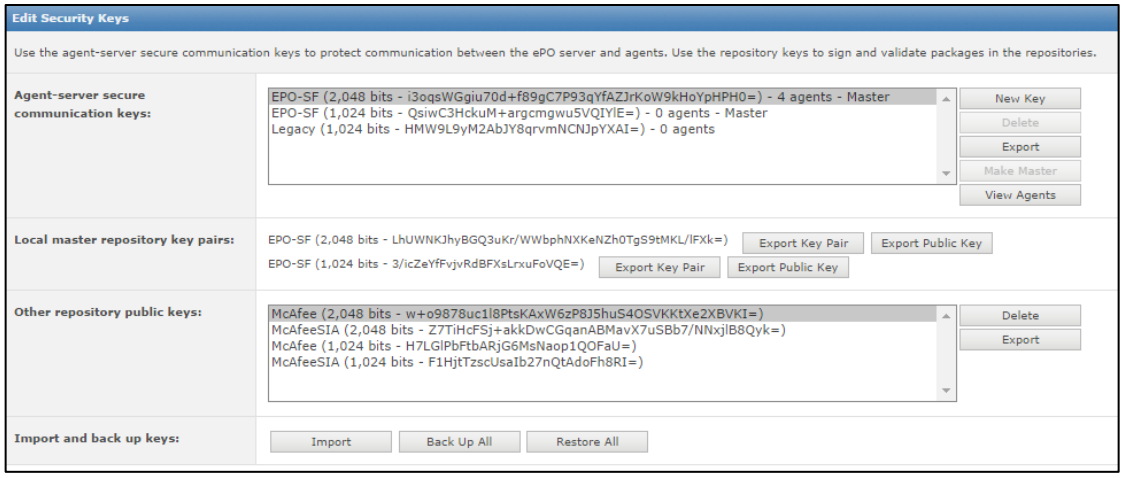


Figure 23. Device-to-Device Key Management in ePO.

A.6.2 User Identification and Authentication (SG.IA-4)

Requirement

The Smart Grid information system uniquely identifies and authenticates users (or processes acting on behalf of users).

Additional Considerations

1. The Smart Grid information system uses multifactor authentication for—
    a. Remote access to non-privileged accounts;
    b. Local access to privileged accounts; and
    c. Remote access to privileged accounts.

Category

Unique Technical Requirements

Specification

1. Users are identified by username/password credential mechanism on the back-end systems. The M2M software stack is identified/authenticated by KRB tickets.
2. Authentication of users is implemented using username/password credentials

The M2M software stack is authenticated using KRB tickets

Verification Results

Satisfactory. The remote access to privileged account on both ESM and ePO uses the username/password authentication (see Table 1 in SG.AC-4) as the identification and authentication. For machine-to-machine communication, the Kerberos technique is used for identifying and authenticating machines to establish the connection among them (see Figure 23 in SG.IA-3).

A.6.3 Device Identification and Authentication (SG.IA-5)

Requirement

The Smart Grid information system uniquely identifies and authenticates an organization-defined list of devices before establishing a connection.

Supplemental Guidance

The devices requiring unique identification and authentication may be defined by type, by specific device, or by a combination of type and device as deemed appropriate by the organization.

Requirement Enhancements

1. The Smart Grid information system authenticates devices before establishing remote network connections using bidirectional authentication between devices that is cryptographically based; and
2. The Smart Grid information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.

Category

Unique Technical Requirements

Specification

1. The organization MUST define the list of devices for which identification and authorization is required before establishing a connection in this platform. Otherwise, the connections will be denied. This applies to all M2M communications as well as any other communications, including, but not limited to the Security Channel, data channels, etc. (e.g. NTP, DB connections, etc)
2. The SF device must uniquely identify an organization-defined device using KRB protocol before establishing a connection.
3. The SF device must authenticate an organization-defined device using KRB protocol before establishing a connection.

The device connections are established only after they are authenticated by Kerberos.

Verification Results

Satisfactory. The identification and authentication of devices in the proposed system are managed in the ePO system (see SG.CM-6 and SG.CM-8). The communication among end-points (device nodes) uses the Kerberos protocol for identification and authentication (see Figure 23 in SG.IA-3).

A.6.4 Authenticator Feedback (SG.IA-6)

Requirement

The authentication mechanisms in the Smart Grid information system obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Supplemental Guidance

The Smart Grid information system obscures feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password). The feedback from the Smart Grid information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism.

Category

Unique Technical Requirements

Specification

Masked passwords - The authentication process does not exchange the secrets that identify a user over the Internet in a clear text format. An encrypted session is established and only then the username/password is exchanged. The password entered by the user on the user interface is always obscure.

On invalid entry of the username or password, the server throws a generic message which doesn't indicate the reason of the access failure.

Verification Results

Satisfactory. Both ESM and ePO components use masked passwords technique (i.e., displaying asterisks when a user types in a password for logging to the system) to obscure feedback of authentication information during the authentication process. The next two figures show the application of masked passwords for both systems. The feedback from the Smart Grid information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism.

Figure 24. Masked password in ePO system.

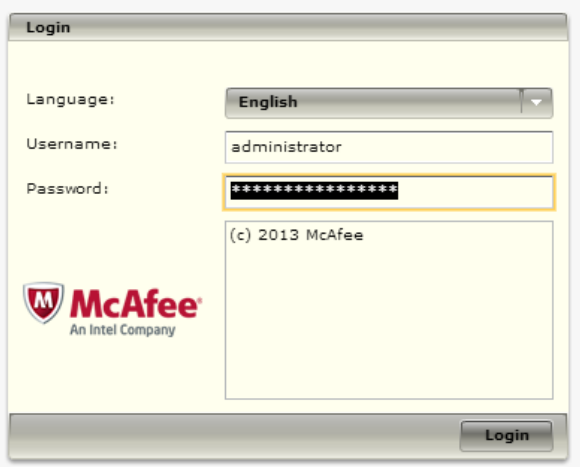


Figure 25. Masked password in ESM system.

A.7 Incident Response (SG.IR)

Incident response addresses the capability to continue or resume operations of a Smart Grid information system in the event of disruption of normal Smart Grid information system operation. Incident response entails the preparation, testing, and maintenance of specific policies and procedures to enable the organization to recover the Smart Grid information system's operational status after the occurrence of a disruption. Disruptions can come from natural disasters, such as earthquakes, tornados, floods, or from manmade events like riots, terrorism, or vandalism. The ability for the Smart Grid information system to function after such an event is directly dependent on implementing policies, procedures, training, and resources in place ahead of time using the organization's planning process. The security requirements recommended under the incident response family provide policies and procedures for incident response monitoring, handling, reporting, testing, training, recovery, and reconstitution of the Smart Grid information systems for an organization.

A.7.1 Incident Monitoring (SG.IR-6)

Requirement

The organization tracks and documents Smart Grid information system and network security incidents.

Additional Considerations

1. The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

Category

Common Governance, Risk, and Compliance (GRC)

Specification

1. Both endpoint and network security incidents are tracked in ESM and/or ePO
2. Records of the incidents can be found in ESM

Verification Results

Satisfactory. The security incidents (described in ePO and ESM event specifications shown in SG.AU-2) can be tracked in the proposed systems (as shown in Figure 11 and Figure 12 in SG.AU-2).

A.8 Smart Grid Information System Development and Maintenance (SG.MA)

Security is most effective when it is designed into the Smart Grid information system and sustained, through effective maintenance, throughout the life cycle of the Smart Grid information system. Maintenance activities encompass appropriate policies and procedures for performing routine and preventive maintenance on the components of a Smart Grid information system. This includes the use of both local and remote maintenance tools and management of maintenance personnel.

A.8.1 Legacy Smart Grid Information System Upgrades (SG.MA-2) – Update Specification

Requirement

The organization develops policies and procedures to upgrade existing legacy Smart Grid information systems to include security mitigating measures commensurate with the organization's risk tolerance and the risk to the Smart Grid information system.

Category

Common Governance, Risk, and Compliance (GRC)

Specification

1. This is the definition of the Security Fabric. The organization develops policies to upgrade legacy systems to the SF platform without affecting the legacy applications.
2. Establish policies for security measures and mitigating controls as per the organization's risk tolerance combined with the risk to the system.

Verification Results

Satisfactory if the specification describes techniques related to virtualization of applications and security manager. The proposed system uses the virtualization technique, which separates security management from the application (i.e., legacy smart grid information system). By applying this technique, the organization can develop (or upgrade) security policy and procedures without affecting the legacy system.

A.8.2 Remote Maintenance (SG.MA-2)

Requirement

The organization policy and procedures for remote maintenance include:

1. Authorization and monitoring the use of remote maintenance and diagnostic activities;
2. Use of remote maintenance and diagnostic tools;
3. Maintenance records for remote maintenance and diagnostic activities;
4. Termination of all remote maintenance sessions; and
5. Management of authorization credentials used during remote maintenance.

Requirement Enhancements

The organization—

1. Requires that remote maintenance or diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the Smart Grid information system being serviced; or
2. Removes the component to be serviced from the Smart Grid information system and prior to remote maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities and after the service is performed, sanitizes the component (with regard to potentially malicious software) before returning the component to the Smart Grid information system.

Additional Considerations

1. The organization requires that remote maintenance sessions are protected through the use of a strong authentication credential; and
2. The organization requires that (a) maintenance personnel notify the Smart Grid information system administrator when remote maintenance is planned (e.g., date/time), and (b) a management authority approves the remote maintenance.

Category

Common Governance, Risk, and Compliance (GRC)

Specification

1. Authorization and monitoring are available for all Security Fabric Nodes/Endpoints being maintained. This is performed via the ePO Security/Management Communication Channel.
2. Remote maintenance and diagnostics are enabled for all Security Fabric Nodes/Endpoints. This is performed via the ePO Security/Management Communication Channel.
3. NA - Organizational Policy

4. Termination of all remote maintenance sessions is automatically performed by the agents that communicate from the endpoint back to the ePO server. This is performed via the ePO Security/Management Communication Channel.
5. The credentials for remote maintenance are automatically managed by ePO and the endpoint agent.
6. The maintenance and diagnostics operations are initiated and controlled by ePO, which has an enhanced level of security, at least equal to the endpoint's.
7. NA - Organizational policy. However, verifying the integrity of the device using a measured boot process as well as remote authentication ensures sanitized devices. Also, application whitelisting ensures that no additional software has been placed on the device, further ensuring the device is sanitized.

Verification Results

Satisfactory. Remote maintenance for the devices deployed the proposed system can be done in the ePO system (see SG.CM-6 and SG.CM-8), which requires authentication for maintainer (see SG.AC-4).

A.9 Risk Assessment (SG.RA)

Risk management planning is a key aspect of ensuring that the processes and technical means of securing Smart Grid information systems have fully addressed the risks and vulnerabilities in the Smart Grid information system.

An organization identifies and classifies risks to develop appropriate security measures. Risk identification and classification involves security assessments of Smart Grid information systems and interconnections to identify critical components and any areas weak in security. The risk identification and classification process is continually performed to monitor the Smart Grid information system's compliance status.

A.9.1 Risk Assessment (SG.RA-4)

Requirement

The organization—

1. Conducts assessments of risk from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and Smart Grid information systems; and
2. Updates risk assessments on an organization-defined frequency or whenever significant changes occur to the Smart Grid information system or environment of operation, or other conditions that may impact the security of the Smart Grid information system.

Supplemental Guidance

Risk assessments take into account vulnerabilities, threat sources, risk tolerance levels, and security mechanisms planned or in place to determine the resulting level of residual risk posed to

organizational operations, organizational assets, or individuals based on the operation of the Smart Grid information system.

Category

Common Governance, Risk, and Compliance (GRC)

Specification

The following capabilities are enabled by leveraging the ESM's security event gathering and log file gathering tools:

- Monitoring the logins to the endpoint management instance and access attempts to protected data sets (e.g. configuration files)
- Monitor outgoing connections from the Application that must be blocked from the Management instance
- Monitor for DOS attacks on management instance network interfaces
- Monitoring the protected data sets (e.g. configuration files)
- Monitoring the protected data sets (e.g. configuration files)

The Security Fabric tracks the risk of endpoints and the connections between them in near real-time using the ESM.

Verification Results

Satisfactory. The risk assessments for this proposed system are described in automatic response feature in both ESM and ePO. However, a security administrator need to know where or what the risk is in the smart grid information system in order to provide the counter-measure to mitigate those risk (see Figure 10 in SG.AU-2). For example, the connection from brute-force attempt logging to the system from attackers can be suspend by using the automatic response provided by security administrator.

A.9.2 Vulnerability Assessment and Awareness (SG.RA-6)

Requirement

The organization—

1. Monitors and evaluates the Smart Grid information system according to the risk management plan on an organization-defined frequency to identify vulnerabilities that might affect the security of a Smart Grid information system;
2. Analyzes vulnerability scan reports and remediates vulnerabilities within an organization-defined time frame based on an assessment of risk;

3. Shares information obtained from the vulnerability scanning process with designated personnel throughout the organization to help eliminate similar vulnerabilities in other Smart Grid information systems;
4. Updates the Smart Grid information system to address any identified vulnerabilities in accordance with organization's Smart Grid information system maintenance policy; and
5. Updates the list of Smart Grid information system vulnerabilities on an organization-defined frequency or when new vulnerabilities are identified and reported.

Supplemental Guidance

Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools to scan for Web-based vulnerabilities, source code reviews, and static analysis of source code). Vulnerability scanning includes scanning for ports, protocols, and services that should not be accessible to users and for improperly configured or incorrectly operating information flow mechanisms.

Requirement Enhancements

1. The organization employs vulnerability scanning tools that include the capability to update the list of Smart Grid information system vulnerabilities scanned; and
2. The organization includes privileged access authorization to organization-defined Smart Grid information system components for selected vulnerability scanning activities to facilitate more thorough scanning.

Additional Considerations

1. The organization employs automated mechanisms on an organization-defined frequency to detect the presence of unauthorized software on organizational Smart Grid information systems and notifies designated organizational officials;
2. The organization performs security testing to determine the level of difficulty in circumventing the security requirements of the Smart Grid information system; and
3. The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in Smart Grid information system vulnerabilities.

Category

Common Governance, Risk, and Compliance (GRC)

Specification

Applies to Security Fabric with presence of automated vulnerability scans (NOTE: requires a vulnerability detection engine that feeds into ESM, such as McAfee Vulnerability Manager Product. This is not currently bundled in security Fabric.)

Applies to Security Fabric with presence of Automated Patch Management systems such as McAfee Remediation Manager. This is not currently bundled in security Fabric.

Leverage ePO update mechanism to update security controls to protect against detected vulnerabilities

Applies to Security Fabric with presence of Automated vulnerability scans where the vulnerability results are stored in centralized systems such as ESM and ePO (NOTE: requires a vulnerability detection engine that feeds into ESM, such as McAfee Vulnerability Manager product. This is not currently bundled in security Fabric.)

Verification Results

Issue Identified – need additional tool. Vulnerability analysis for custom software and applications is currently not included in the SF system. If the Vulnerability Analysis was included, then the specification would have been testable and likely satisfied.

A.10 Smart Grid Information System and Communication Protection (SG.SC)

Smart Grid information system and communication protection consists of steps taken to protect the Smart Grid information system and the communication links between Smart Grid information system components from cyber intrusions. Although Smart Grid information system and communication protection might include both physical and cyber protection, this section addresses only cyber protection. Physical protection is addressed in SG.PE, Physical and Environmental Security.

A.10.1 Communications Partitioning (SG.SC-2)

Requirement

The Smart Grid information system partitions the communications for telemetry/data acquisition services and management functionality.

Supplemental Guidance

The Smart Grid information system management communications path needs to be physically or logically separated from the telemetry/data acquisition services communications path.

Category

Unique Technical Requirements

Specification

The Smart Grid information system management communications path needs to be physically or logically separated from the telemetry/data acquisition services communications path.

Verification Results

Satisfactory if the specification describes how the security management communications are separated from functional communication. The proposed system separates the security management communication (e.g., event logging/monitoring, device-node management) from the functional communication (e.g., smart-grid information exchange between ePDC and RTDMS) by using the security management modules (i.e., Wind River Linux as security patching on Hypervisor component in Security Fabric Framework) to manage the communication channel for both security management and smart-gird communications.

A.10.2 Security Function Isolation (SG.SC-3)

Requirement

The Smart Grid information system isolates security functions from non-security functions.

Additional Considerations

1. The Smart Grid information system employs underlying hardware separation mechanisms to facilitate security function isolation; and
2. The Smart Grid information system isolates security functions (e.g., functions enforcing access and information flow control) from both non-security functions and from other security functions.

Category

Unique Technical Requirements

Specification

EPO provides the framework to define policies independent of each other. A particular policy can also be individually applied to a system or group of systems. This way it allows separation of security and non-security functions.

Leverage virtualization technology to create separation between OT and IT workloads. Also separation of network resources, storage resources, and peripheral resources.

Verification Results

Satisfactory. The proposed system isolates security functions from non-security functions by using the virtualization techniques on the hardware that supports ESXi Hypervisor[1].

[1] http://www.vmware.com/products/vsphere-hypervisor

A.10.3 Information Remnants (SG.SC-4)

Requirement

The Smart Grid information system prevents unauthorized or unintended information transfer via shared Smart Grid information system resources.

Supplemental Guidance

Control of Smart Grid information system remnants, sometimes referred to as object reuse, or data remnants, prevents information from being available to any current user/role/process that obtains access to a shared Smart Grid information system resource after that resource has been released back to the Smart Grid information system.

Category

Unique Technical Requirements

Specification

For inter-process communication or access to shared resources, the hypervisor and separation kernel prevent unauthorized access to the data.

EPO policies allow only communication between its managed nodes. Any unidentified (remnant) node which wouldn't be managed in EPO would never be able to exchange information with any managed node in the platform. Any unauthorized node within managed nodes (remnant) will not be able to interrupt or communicate with active nodes as the policy would not be set for such a node.

Verification Results

Satisfactory. Since the security modules (Wind River Linux) cover managed nodes (i.e., ePDC and RTDMS), any unidentified nodes cannot access the data inside the managed nodes without authentication. The communications among managed nodes are encrypted using public-key infrastructure and specified in ePO. Unauthorized nodes cannot retrieve the information from the secured communication channel.

A.10.4 Denial-of-Service Protection (SG.SC-5)

Requirement

The Smart Grid information system mitigates or limits the effects of denial-of-service attacks based on an organization-defined list of denial-of-service attacks.

Supplemental Guidance

Network perimeter devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial-of-service attacks.

Additional Considerations

1. The Smart Grid information system restricts the ability of users to launch denial-of-service attacks against other Smart Grid information systems or networks; and
2. The Smart Grid information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

Category

Unique Technical Requirements

Specification

Firewall rules have been setup both on the end-point and server side. All the well-known DOS attacks will be filtered by the firewall and would protect the assets. ESM has been built into the security platform which raises alarms on suspicious activities like zero day DOS escaping firewall allowing immediate action to be taken.

Monitor FW protects internal DOS attacks between instances (in VM)

Firewall also prevents any outgoing data from the end-point node which prevents the DOS attack coming from inside the trusted network.

PROVIDE Firewall instance TO LIMIT ACCESS TO SERVER INSTANCES (ePO, ESM, ACE, AND AD)

On the device, the separation kernel prevents one instance from utilizing the resources of another instance, so resource exhaustion cannot occur.

Verification Results

The proposed system can be prevented or mitigated the effected of known (organization defined-list) DoS by using firewall (see SG.AC-5).

A.10.5 Resource Priority (SG.SC-6)

Requirement

The Smart Grid information system prioritizes the use of resources.

Supplemental Guidance

Priority protection helps prevent a lower-priority process from delaying or interfering with the Smart Grid information system servicing any higher-priority process. This requirement does not apply to components in the Smart Grid information system for which only a single user/role exists.

Category

Unique Technical Requirements

Specification

Priority protection helps prevent a lower-priority process from delaying or interfering with the Smart Grid information system servicing any higher-priority process. This requirement does not apply to components in the Smart Grid information system for which only a single user/role exists.

The lower priority security process cannot interfere with the higher priority Grid process due to the separation kernel. All processes between OT (operational/Grid) are separated from the IT (Security) processes. The IT-side is assumed to be running the low priority security processes, leaving the high priority OT processes running in the Application VM.

Availability is ensured for the OT-side.

Verification Results

Satisfactory. Both functional components (ePDC and RTDMS) and security components (McAfee Agent) are deployed in the same hardware using the virtualization technique. The ESXi hypervisor can set priority for each virtualization modules as shown in the document[2] of resource management guideline for ESXi version 5.0.

A.10.6 Boundary Protection (SG.SC-7)

Requirement

1. The organization defines the boundary of the Smart Grid information system;
2. The Smart Grid information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
3. The Smart Grid information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices;

[2] https://pubs.vmware.com/vsphere-50/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-50-resource-management-guide.pdf.

4. The managed interface implements security measures appropriate for the protection of integrity and confidentiality of the transmitted information; and
5. The organization prevents public access into the organization's internal Smart Grid information system networks except as appropriately mediated.

Supplemental Guidance

Managed interfaces employing boundary protection devices include proxies, gateways, routers, firewalls, guards, or encrypted tunnels.

Requirement Enhancements

1. The Smart Grid information system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception);
2. The Smart Grid information system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination; and
3. Communications to/from Smart Grid information system components shall be restricted to specific components in the Smart Grid information system. Communications shall not be permitted to/from any non-Smart Grid system unless separated by a controlled logical/physical interface.

Additional Considerations

1. The organization prevents the unauthorized release of information outside the Smart Grid information system boundary or any unauthorized communication through the Smart Grid information system boundary when an operational failure occurs of the boundary protection mechanisms;
2. The organization prevents the unauthorized exfiltration of information across managed interfaces;
3. The Smart Grid information system routes internal communications traffic to the Internet through authenticated proxy servers within the managed interfaces of boundary protection devices;
4. The organization limits the number of access points to the Smart Grid information system to allow for better monitoring of inbound and outbound network traffic;
5. Smart Grid information system boundary protections at any designated alternate processing/control sites provide the same levels of protection as that of the primary site; and
6. The Smart Grid information system fails securely in the event of an operational failure of a boundary protection device.

Category

Unique Technical Requirements

Specification

1. Boundary is created on each end node by implementing the Separation Kernel. That separates IT/OT and places a security boundary in between the OT and everything outside of the device. There is now a device boundary being enforced.
2. Define the Boundary of the system:
    a. WRL Management instance that separates the OT from the outside of the device between nodes and other external devices
    b. VxWorks Monitor that separates the OT from the WRL instance

   System monitors and controls both boundaries using policy (from ePO). ESM monitors the boundaries by collecting events from WRL and VxWorks instances. EPO manages all the nodes under the security fabric platform configuring the boundary between other nodes and other devices. ESM monitors the events detected on each of these boundaries.
3. Define managed interfaces consisting of boundary protection devices: firewalls in WRL and VxWorks. All traffic going external to the device must pass through the WRL firewall. All traffic moving from instance to instance (inside the device) must pass through the VxWorks monitor firewall. No traffic shall traverse any boundary that is not specifically allowed.
4. The WRL boundary creates an encrypted, mutually authenticated tunnel to pass all data between nodes. All communication between nodes and ePO are encrypted, as is all data passed between nodes and ESM. Kerberos tickets and communication are not encrypted, however, the tickets themselves are already double-encrypted, so the communication channel encryption is not required. The VxWorks boundary in internal to the device, so it cannot be accessed externally, thus no encryption is required between the VM instances.
5. Public access is prevented by the WRL instance blocking unmediated communications from occurring.

Verification Results

Satisfactory. The proposed system defines the boundary of the system by using the functional of operation: (1) *internal-boundary*: domain-specific application (ePDC and RTDMS) and (2) *external-boundary*: security management application (security components). All communications in the proposed system can be monitored and controlled by external boundary components (see SG.AU-2). All communication between internal-boundary parts are encrypted and enforced by the security policy (e.g., firewall rules) from external-boundary parts (see SG.AC-5 and SG.AC-19).

A.10.7 Communication Integrity (SG.SC-8)

Requirement

The Smart Grid information system protects the integrity of electronically communicated information.

Requirement Enhancements

1. The organization employs cryptographic mechanisms to ensure integrity.

Additional Considerations

1. The Smart Grid information system maintains the integrity of information during aggregation, packaging, and transformation in preparation for transmission.

Category

Unique Technical Requirements

Specification

The communication integrity between server-side (EPO/ESM) and end-point systems (WRL) is ensured by HTTPS sessions. The communication integrity between end-point systems is established with Kerberos authenticating the systems themselves and the information being exchanged over TLS (Transport Layer Security).

All the communications happen over TCP which ensures base integrity of package delivery to application.

Communications between McAfee Agent (in WRL) and ePO are signed for integrity.

Verification Results

Satisfactory. The proposed system supports the protocols that guarantee the integrity of information as shown below.

Communication Pair		**Protocol**
User	ESM/ePO	HTTPS
ESM/ePO	WRL	HTTPS
WRL	WRL	TLS

Table 3. Communication Protocol among components in SF.

A.10.8 Communication Confidentiality (SG.SC-9)

Requirement

The Smart Grid information system protects the confidentiality of communicated information.

Requirement Enhancements

1. The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission.

Category

Unique Technical Requirements

Specification

Any sort of information exchange between systems in security platform is over TLS (Transport Layer Security) which ensures the confidentiality.

Verification Results

Satisfactory. The proposed system supports the protocols that guarantee the confidentiality of information as shown in Table 3 in SG.SC-8.

A.10.9 Trusted Path (SG.SC-10)

Requirement

The Smart Grid information system establishes a trusted communications path between the user and the Smart Grid information system.

Supplemental Guidance

A trusted path is the means by which a user and target of evaluation security functionality can communicate with the necessary confidence.

Category

Unique Technical Requirements

Specification

The only means by which the user interacts with end-point systems is via EPO and ESM. This interaction happens over HTTPS sessions and is secured.

Note: SSH port is open on end-point systems which provides another means of interacting but this port will be closed in the future. At this point, the SSH communication is also over the SSL and is secure.

The trusted communications path is tracked in ePO.

Verification Results

Satisfactory. The communication between users and the security functionality of the proposed system (ePO and ESM) uses the secured protocol (i.e., HTTPS) as shown in Table 1 in SG.AC-5.

A.10.10 Cryptographic Key Establishment and Management (SG.SC-11)

Requirement

The organization establishes and manages cryptographic keys for required cryptography employed within the information system.

Supplemental Guidance

Key establishment includes a key generation process in accordance with a specified algorithm and key sizes, and key sizes based on an assigned standard. Key generation must be performed using an appropriate random number generator. The policies for key management need to address such items as periodic key changes, key destruction, and key distribution.

Requirement Enhancements

1. The organization maintains availability of information in the event of the loss of cryptographic keys by users.

Category

Common Technical Requirements, Confidentiality

Specification

- Keys: (1) McAfee Agent Key & Cert (2) Kerberos Key (3) ePO Certificate (4) ESM Certificate (5) AD Certificate
- Provisioning: MA creates X501 Key Pair, sends to ePO for signing (generates certificate), ePO creates Machine principal in AD, generates Kerberos key pair and AD certificate, returns all to the WRL on the node.
- Random number generator leverages Intel hardware.
- Keys are changed regularly on a schedule every year by implementing the expiration on the certificate, and to update the key, simply re-run the provisioning.
- Key Distribution is automated through ePO.
- Key Destruction does not required CRL, rather a node is deprovisioned by removing Kerberos entry.
- Keys will be generated and stored in the TPM in the future.
- Destruction is implemented by generating a new key (in TPM)
- Cryptographic keys are not managed by users

Verification Results

Satisfactory. The proposed system establishes and manages the cryptographic keys that require for cryptography function within the information system. Part of key management in the proposed system is shown as Figure 23 in SG.IA-4.

A.10.11 Use of Validated Cryptography (SG.SC-12)

Requirement

All of the cryptography and other security functions (e.g., hashes, random number generators, etc.) that are required for use in a Smart Grid information system shall be NIST Federal Information Processing Standard (FIPS) approved or allowed for use in FIPS modes.

Supplemental Guidance

For a list of current FIPS-approved or allowed cryptography, see Chapter Four Cryptography and Key Management in NIST IR-7628.

Category

Common Technical Requirements, Confidentiality

Specification

All of the cryptography and other security functions (e.g., hashes, random number generators, etc.) that are required for use in a Smart Grid information system are NIST Federal Information Processing Standard (FIPS) approved or allowed for use in FIPS modes.

Crypto Libs:

- OpenSSL for ePO & ESM
- OpenSSL for TLS connections device-to-device
- OpenSSH for connection to Mgmt VM (will be removed in future)
- Active Directory for Key Generation (Kerberos)
- ePO key generation (in Java) using standard libs (and cert signing)

Verification Results

Satisfactory. From the McAfee Enterprise Security Manager (ESM) version 9.3.0 Product Guide[3], ESM component supports FIPS 140-2 but the user of ESM must select the FIPS mode as the first time log on to the system and the selection is permanent. The current deployed system did not enable FIPS mode.

The table below shows the validation FIPS for both ePO and McAfee Agent. For more detail about FIPS-compliant see https://kc.mcafee.com/corporate/index?page=content&id=KB75739.

Component	Validation Link
ePO	http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2011.htm#1587
McAfee Agent	http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2011.htm#1588

Table 4. FIPS-compliant for ePO and McAfee Agent.

A.10.12 Public Key Infrastructure Certificates (SG.SC-15)

Requirement

For Smart Grid information systems that implement a public key infrastructure, the organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

Supplemental Guidance

Registration to receive a public key certificate needs to include authorization by a supervisor or a responsible official and needs to be accomplished using a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

Category

Common Technical Requirements, Confidentiality

Specification

Security Fabric uses certificates, generates certs, validates the certificates, but also not enforce any rules on the CA so that self-signed certs can be leveraged if needed (depends on the list of "approved" service providers... is the entity itself "approved"?).

---

3 https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/24000/PD24719/en_US/esm_930_product%20guide_en-us.pdf

Verification Results

Satisfactory. McAfee agent creates X509 key pair and sends to public key information to ePO for signing (creating certificate). The ePO component also creates McAfee agent principal in active directory, generates key pair, active directory certificate, and then returns all certificates to McAfee agents. The approved CA in this proposed system is ePO component.

A.10.13 System Connections (SG.SC-18)

Requirement

All external Smart Grid information system and communication connections are identified and protected from tampering or damage.

Supplemental Guidance

External access point connections to the Smart Grid information system need to be secured to protect the Smart Grid information system. Access points include any externally connected communication end point (for example, dial-up modems).

Category

Common Technical Requirements, Confidentiality

Specification

1. All connections much pass through the Management Firewall, and the Monitor Firewall.
2. All tunneled data must pass through the Communication Manager else be blocked.

Verification Results

Satisfactory. The external smart grid information system in this proposed system is the McAfee Agent. All communications among the McAfee Agents are defined in ePO (see SG.AC-5) and secured by using TLS protocol (as shown in Table 3 in SG.SC-8).

A.10.14 Security Roles (SG.SC-19)

Requirement

The Smart Grid information system design and implementation specifies the security roles and responsibilities for the users of the Smart Grid information system.

Supplemental Guidance

Security roles and responsibilities for Smart Grid information system users need to be specified, defined, and implemented based on the sensitivity of the information handled by the user. These roles may be defined for specific job descriptions or for individuals.

Category

Common Technical Requirements, Integrity

Specification

EPO provides the framework to create security roles on the server side providing separation of duties. Different accounts can be setup in EPO to perform different administrative tasks. Also no console access will be enabled on the end point (WRL) for any user. Any administrative task to be performed on the end-point will be performed from EPO.

Currently there is an SSH listener on the endpoint, this will go away in the future, thereby denying any type of login to the Mgmt VM. Therefore, there are no roles, or users on that VM and all operations must be performed in ePO.

The platform ships with one role configured: Administrator. The user at any point can create additional roles on the fly in EPO to limit the duties of different users to various assets and resources. One role is provided out-of-the-box, and the end-user is responsible for defining the actual roles required to correctly, and securely, manage the devices. The actual roles are deployment-dependent.

Verification Results

Satisfactory. The proposed system specifies the security role as “Administrator”, which is responsible for (1) creating different users to manage various assets and resources (delegate administrative task to different users) (2) performing administrative task on ePO component.

A.10.15 Message Authenticity (SG.SC-20)

Requirement

The Smart Grid information system provides mechanisms to protect the authenticity of device-to-device communications.

Supplemental Guidance

Message authentication provides protection from malformed traffic, misconfigured devices, and malicious entities.

Additional Considerations

Message authentication mechanisms should be implemented at the protocol level for both serial and routable protocols.

Category

Common Technical Requirements, Integrity

Specification

On the end point side, Kerberos V5 is used for authenticating device-to-device communication on the security fabric platform. Kerberos ensures strong authentication as it doesn't exchange the secrets over the wire. Once authenticated, the M2M communication is sent via encrypted tunnels, thereby verifying the message authenticity over the wire.

Further, the communications between ePO and the Agent are signed. These cannot be altered in any way without detection.

Server side systems (EPO/ESM) authenticate the user with username/password mechanism and authenticate devices with PKI. EPO/ESM systems communicate over SSL ensuring that the information is encrypted over Internet and sort of provide out of band secure communication.

Device-to-ESM (secure syslog data) is over encrypted tunnels.

Other connections, for example, NTP traffic, are also sent via encrypted tunnels using the M2M communication path (TLS).

Verification Results

Satisfactory. The authenticity of device-to-device communication in the proposed system has the protection as shown below.

Device-To-Device	**Protected By**
McAfee Agent – McAfee Agent	Kerberos V5
ePO – McAfee Agent	HTTPS
ESM – ePO	SSL
ESM – McAfee Agent	TLS

Table 5. Protocol for protecting message authenticity of device-to-device communication.

A.10.16 Secure Name/Address Resolution Service (SG.SC-21)

Requirement

The organization is responsible for—

1. Configuring systems that provide name/address resolution to supply additional data origin and integrity artifacts along with the authoritative data returned in response to resolution queries; and
2. Configuring systems that provide name/address resolution to Smart Grid information systems, when operating as part of a distributed, hierarchical namespace, to provide the means to indicate the security status of child subspaces and, if the child supports secure resolution services, enabled verification of a chain of trust among parent and child domains.

Category

Common Technical Requirements, Integrity

Specification

DNS is not leveraged in the security Fabric

Verification Results

Issue Identified – deemed not applicable. The specification and the proposed system do not appear to support the requirements. It is recommended that this requirement category and the specification be removed.

A.10.17 Fail in Known State (SG.SC-22) – Incomplete information

Requirement

The Smart Grid information system fails to a known state for defined failures.

Supplemental Guidance

Failure in a known state can be interpreted by organizations in the context of safety or security in accordance with the organization's mission/business/operational needs. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the Smart Grid information system or a component of the Smart Grid information system.

Additional Considerations

1. The Smart Grid information system preserves defined system state information in failure.

Category

Common Technical Requirements, Integrity

Specification

In the case of a failure, the system will maintain the current policy definitions.

Verification Results

Issue Identified – specification needs definition. The system specification must define the (known/anticipated) deviations from normal operations (failure states) and describe how the system defines states such as loss of system confidentiality, integrity, or availability.

A.10.18 Thin Nodes (SG.SC-23) – Incomplete information

Requirement

The Smart Grid information system employs processing components that have minimal functionality and data storage.

Supplemental Guidance

The deployment of Smart Grid information system components with minimal functionality (e.g., diskless nodes and thin client technologies) reduces the number of endpoints to be secured and may reduce the exposure of information, Smart Grid information systems, and services to a successful attack.

Category

Unique Technical Requirements

Specification

The deployment of Smart Grid information system components with minimal functionality (e.g., diskless nodes and thin client technologies) reduces the number of endpoints to be secured and may reduce the exposure of information, Smart Grid information systems, and services to a successful attack.

Verification Results

Issue Identified – needs information. The specification needs further information on (1) what the *thin nodes* are and (2) where the *thin nodes* deployed in the proposed system.

A.10.19 Honeypots (SG.SC-24) – Consider to be removed from specification

Requirement

The Smart Grid information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, analyzing, and tracking such attacks.

Additional Considerations

1. The Smart Grid information system includes components that proactively seek to identify Web-based malicious code.

Category

Unique Technical Requirements

Specification

1. Embedded firewall in the Management instance is able to both detect and deflect network attacks. Encrypted TLS tunnels between nodes leverage mutual authentication prior to establishing a connection, thus are able to detect and prevent impersonation attacks, man-in-the-middle attacks, eavesdropping, and data modification enroute.
2. All events are forwarded to the ESM for analysis. The ESM correlates events and generates alarms in order to update the state in ePO
3. All events from all endpoints (and their connections) are forwarded to the ESM. Therefore, it is possible to track attacks as they make their way through the environment, and even apply policy in response to the attacks, or even prior to the attack reaching a particular endpoint.

Verification Results

Issue Identified – requirement is not applicable to the SF system. *Honeypots* are a computer, data or network site that *appears to be part of a network but is actually isolated and monitored*, and which seems to contain information or a resource of value to attackers. There is no description of the elements and functionality of Honeypots in the SF system. Recommend this requirement be removed from the specification.

A.10.20 Operating System Independent Applications (SG.SC-25)

Requirement

The Smart Grid information system includes organization-defined applications that are independent of the operating system.

Supplemental Guidance

Operating system-independent applications are applications that can run on multiple operating systems. Such applications promote portability and reconstitution on different platform architectures, thus increasing the availability for critical functionality while an organization is under an attack exploiting vulnerabilities in a given operating system.

Category

Unique Technical Requirements

Specification

1. The OS independence is built into the design of the platform. There is a separation between the Operational Instance and the Management Instance, so that the security can run NEXT TO, but independent of ANY OS.
2. The organization-defined applications are physically separated from the security applications, services, and capabilities. Therefore, the security does not depend on the environment (OS, etc) of the applications, and the applications are kept separate (different VM) from the security aspects.

Verification Results

Satisfactory. The proposed system uses virtualization technique for separating the domain-specific applications (ePDC and RTDMS) from security applications. Both domain-specific and security application are run on top of ESXi virtualization machine (see SG.SC-3). Because of virtualization, domain-specific application can run on desired operating system without changing anything in order to include the proposed system as the security application. Please note that the proposed system is not an application but it is a security architecture.

A.10.21 Confidentiality of Information at Rest (SG.SC-26)

Requirement

The Smart Grid information system employs cryptographic mechanisms for all critical security parameters (e.g., cryptographic keys, passwords, security configurations) to prevent unauthorized disclosure of information at rest.

Supplemental Guidance

For a list of current FIPS-approved or allowed cryptography, see Chapter Four Cryptography and Key Management in NIST IR-7628.

Category

Unique Technical Requirements

Specification

Access to confidential information, such as Keys, Passwords, and security configurations are protected in a separate OS. Access to these keys from the Operational Instance is strictly blocked. There is no path to these resources from inside of the device or from outside of the device (once SSH listener has been removed). All controls are enacted from within the remote security console, and the Mgmt Instance is a black-box without any login or shell capabilities.

Currently, there is an SSH listener on the Mgmt Instance. This allows login (root only) and shell access. As soon as is feasible this interface shall be removed to prevent all access to the confidential information.

Verification Results

Satisfactory. From the McAfee Enterprise Security Manager (ESM) version 9.3.0 Product Guide[4], ESM component supports FIPS 140-2 when the user of ESM selects the FIPS mode the first time he/she logs on to the system. The setup is permanent. Note: current deployed system did not enable FIPS mode.

For the details of FIPS on ePO components, please see SG.SC-12.

A.10.22 Heterogeneity (SG.SC-27)

Requirement

The organization employs diverse technologies in the implementation of the Smart Grid information system.

Supplemental Guidance

Increasing the diversity of technologies within the Smart Grid information system reduces the impact from the exploitation of a specific technology.

Category

Unique Technical Requirements

Specification

The security platform protects the systems from exploitation irrespective of the technologies used. The security platform design allows integration of security products from different vendors employing

---

4 https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/24000/PD24719/en_US/esm_930_product%20guide_en-us.pdf

different technologies. Therefore, a consistent security API is in place to protect the Operational components with heterogeneous security controls.

By deploying in this manner, the homogeneity of the information systems is preserved to reduce the impact of exploitation, while consistent security APIs protect the systems consistently and allow for automated threat response and remediation across not just those nodes under attack, or victims of compromise, but also those not yet affected by the threat.

Verification Results

Satisfactory. The proposed system allows the integration of security products from different developers (as the core contribution of security fabric systems[5]).

A.10.23 Virtualization Technique (SG.SC-28)

Requirement

The organization employs virtualization techniques to present gateway components into Smart Grid information system environments as other types of components, or components with differing configurations.

Supplemental Guidance

Virtualization techniques provide organizations with the ability to disguise gateway components into Smart Grid information system environments, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms.

Additional Considerations

1. The organization employs virtualization techniques to deploy a diversity of operating systems environments and applications;
2. The organization changes the diversity of operating systems and applications on an organization-defined frequency; and
3. The organization employs randomness in the implementation of the virtualization.

Category

Unique Technical Requirements

[5] http://www.gridwiseac.org/pdfs/forum_papers11/speicher_paper_part3_gi11.pdf

Specification

Virtualization techniques are employed in the platform to deploy different operating systems and their respective applications. A diversity of operating systems are deployable into the platform to ensure homogeneity. The OS and applications can be changed as required by the organization's policy.

Verification Results

Satisfactory. The proposed system uses ESXi hypervisor[6] as a mechanism for virtualization (separating domain-specified applications from security-function applications).

A.10.24 Application Partitioning (SG.SC-29)

Requirement

The Smart Grid information system separates user functionality (including user interface services) from Smart Grid information system management functionality.

Supplemental Guidance

Smart Grid information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from Smart Grid information system management functionality is either physical or logical.

The intent of this additional consideration is to ensure that administration options are not available to general users. For example, administration options are not presented until the user has appropriately established a session with administrator privileges.

Additional Considerations

1. The Smart Grid information system prevents the presentation of Smart Grid information system management-related functionality at an interface for general (i.e., non-privileged) users.

Category

Unique Technical Requirements

[6] http://www.vmware.com/products/vsphere-hypervisor

Specification

The application functionality is completely separated from the Management functionality via the hypervisor and virtualization of the instances Therefore, the Smart Grid management components require a completely different level of access much higher level of access required, depending on application) than the User-level functional components on the device.

The management functionality in the security platform is completely handled by EPO which is physically isolated from the end-point where the application instances would be running. The management functionality (EPO) is only presented to the authenticated users and with privileged access.

Verification Results

Satisfactory. The proposed system separates user functionality (ePDC and RDTMS) from security management functionality by using ESXi hypervisor. The security management functionality is handled by ePO, which allows only authenticated users to access.

A.10.25 Smart Grid Information System Partitioning (SG.SC-30)

Requirement

The organization partitions the Smart Grid information system into components residing in separate physical or logical domains (or environments).

Supplemental Guidance

An organizational assessment of risk guides the partitioning of Smart Grid information system components into separate domains (or environments).

Category

Common Technical Requirements, Integrity

Specification

In a given information system, the partitions (Windows & Linux) are configured to have different network interfaces. The windows network interface is a virtual interface whose gateway is the Linux partition. This way the management interface for Windows is the Linux instance and are logically separated.

The network configuration of the externally facing network adapters, in the Management Partition, are configurable such that they are on any networks or VLANs needed. If there are multiple network interfaces, each can be configured onto a different network or VLAN allowing each of the internal instances (assuming there are multiple that must be partitioned into their own networks) to be routed through different network interfaces.

Verification Results

Satisfactory. The ePO, ESM and the McAfee agent play important roles in the proposed system for monitoring and controlling the security in target system. The following is the main task for each component; (1) ePO provides the overall security policy for McAfee agents (2) ESM monitors the specified event, and (3) McAfee agent enforces the policy from ePO at end-point. The specification should address the components (i.e., ePO, ESM, and McAfee agent) in the proposed system and how they reside in separate physical or logical domains.

A.11 Smart Grid Information System and Information Integrity (SG.SI)

Maintaining a Smart Grid information system, including information integrity, increases assurance that sensitive data have neither been modified nor deleted in an unauthorized or undetected manner. The security requirements described under the Smart Grid information system and information integrity family provide policy and procedure for identifying, reporting, and correcting Smart Grid information system flaws. Requirements exist for malicious code detection. Also provided are requirements for receiving security alerts and advisories and the verification of security functions on the Smart Grid information system. In addition, requirements within this family detect and protect against unauthorized changes to software and data; restrict data input and output; check the accuracy, completeness, and validity of data; and handle error conditions.

A.11.1 Flaw Remediation (SG.SI-2)

Requirement

The organization—

1. Identifies, reports, and corrects Smart Grid information system flaws;
2. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational Smart Grid information systems before installation; and
3. Incorporates flaw remediation into the organizational configuration management process.

Supplemental Guidance

The organization identifies Smart Grid information systems containing software and firmware (including operating system software) affected by recently announced flaws (and potential vulnerabilities resulting from those flaws). Flaws discovered during security assessments, continuous monitoring, or under incident response activities also need to be addressed.

Additional Considerations

1. The organization centrally manages the flaw remediation process. Organizations consider the risk of employing automated flaw remediation processes on a Smart Grid information system;

2. The organization employs automated mechanisms on an organization-defined frequency and on demand to determine the state of Smart Grid information system components with regard to flaw remediation; and
3. The organization employs automated patch management tools to facilitate flaw remediation to organization-defined Smart Grid information system components.

Category

Common Technical Requirements, Integrity

Specification

1. ESM monitors and records the syslogs and events on end-point systems. ESM can help detect flaws with respect to a system on the platform. The remediation would be the action taken by the administrator of ESM.
2. The ESM integration to ePO enables the communication of machine state to ePO. This allows ePO to update specific dashboards to report flaw in the systems.

Verification Results

Issue Identified – need additional tool. If the proposed system included the vulnerability analysis tools (e.g., FoundStone from McAfee), this requirement would have been satisfied. Although ESM can help detect flaws by logging the result of operational failures (e.g., system down based on some specific event), the security administrator still needs to identify the cause of logged failures in order to identify the flaw.

A.11.2 Smart Grid Information System Monitoring Tools and Techniques (SG.SI-4)

Requirement

The organization monitors events on the Smart Grid information system to detect attacks, unauthorized activities or conditions, and non-malicious errors.

Supplemental Guidance

Smart Grid information system monitoring capability can be achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, log monitoring software, network monitoring software, and network forensic analysis tools). The granularity of the information collected can be determined by the organization based on its monitoring objectives and the capability of the Smart Grid information system to support such activities.

Additional Considerations

1. The Smart Grid information system notifies a defined list of incident response personnel;

2. The organization protects information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion;
3. The organization tests/exercises intrusion monitoring tools on a defined time period;
4. The organization interconnects and configures individual intrusion detection tools into a Smart Grid system-wide intrusion detection system using common protocols;
5. The Smart Grid information system provides a real-time alert when indications of compromise or potential compromise occur; and
6. The Smart Grid information system prevents users from circumventing host-based intrusion detection and prevention capabilities.

Category

Common Governance, Risk, and Compliance (GRC) Requirements

Specification

The information systems are monitored via ESM to detect attacks, unauthorized activities, and malicious errors. All logs may be sent to the ESM, so all events may be monitored on the back-end including attacks, unauthorized activities, and malicious errors.

Verification Results

Satisfactory. The proposed system can monitor events to detect attacks, unauthorized activities or conditions, and non-malicious errors by using ESM and ePO event monitoring (see SG.AU-2, SG.AU-3, SG.AU-5, SG.AU-6, SG.AU-10, and SG.AU-16).

A.11.3 Security Functionality Verification (SG.SI-6)

Requirement

1. The organization verifies the correct operation of security functions within the Smart Grid information system upon
    a. Smart Grid information system startup and restart; and
    b. Command by user with appropriate privilege at an organization-defined frequency; and
2. The Smart Grid information system notifies the management authority when anomalies are discovered.

Additional Considerations

1. The organization employs automated mechanisms to provide notification of failed automated security tests; and
2. The organization employs automated mechanisms to support management of distributed security testing.

Category

Common Governance, Risk, and Compliance (GRC) Requirements

Specification

1. At startup, the measured boot data ensures that the endpoint has not been tampered with. In addition, the agent reports in so that communication can be reestablished with ePO.
2. The agent checks in with ePO (via a heartbeat message) at a configurable interval to notify ePO that the security capabilities are still functional.
3. ePO Automated Responses can be configured to respond to events in ePO with predetermined actions or tasks based on which events (anomalies) were detected.
4. ePO policy defines the organization's conditions to the endpoint. Implementing the policy on the endpoint ensures the correct operation of the security functions.
5. ePO Automated Responses define the organizations responses to anomalies, and ensures that the proper responses will follow the appropriate events.

Anomalies that are detected on the endpoint create events that are sent to ePO and/or ESM. These anomalies are then analyzed and if appropriate, reported out. Automated responses can be configured to notify via email of specific events, and dashboards and reports can be leveraged as well.

Verification Results

Satisfactory. The proposed system uses the consistency of *boot string* on the device as the conditions for verifying correct operation of security functions when system starts up or restarts. On the operation time, the proposed system can configure the interval time for checking the security capabilities among devices via *heartbeat message*, which is recorded in ePO component. Any defined anomaly events detected in operation time can be responded by ePO Automated Reponses function (see SG.AU-5).

A.11.4 Error Handling (SG.SI-9)

Requirement

The Smart Grid information system—

1. Identifies error conditions; and
2. Generates error messages that provide information necessary for corrective actions without revealing potentially harmful information that could be exploited by adversaries.

Supplemental Guidance

The extent to which the Smart Grid information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Category

Common Technical Requirements, Integrity

Specification

Error conditions are detected either on the endpoint via events, or on the back-end ePO/ESM systems based on events being sent back.

The error messages generated by the endpoint are sent to ePO. These messages are not visible to anyone outside of the appropriate personnel that is authorized to view them.

Verification Results

Satisfactory. The error conditions are defined as the auditable event in both ePO and ESM (see SG.AU-2). The information in error message can be customized and viewed only by authorized person (see SG.AU-3, SG.AU-7, SG.AU-8, and SG.AU-9).

Appendix B: TTU Security Testing Part 2

Penetration Testing Results

The general process of penetration testing involves identifying vulnerabilities of the system (via scanner and manual) and exploiting the promising vulnerability with the goal to breach the system. This appendix gives details of the vulnerabilities that have been exploited successfully to the TTU synchrophasor network including the security fabric-enabled network as well. For each of the vulnerabilities below, the descriptions, summarized findings, scripts coded to identify vulnerability (e.g., scan network ports or test unsecured software), and detailed results of vulnerability identification and/or penetration testing are given. In many cases, suggestions of how to remove the vulnerability that leads to exploit are also described. This appendix reports seven types of the vulnerability exploits as mentioned in the main report.

B.1 MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution

Descriptions: The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, aka "Remote Desktop Protocol Vulnerability."

Findings: As shown below, there are five remote desktop services in the system. Three (top three rows of the table) are in security fabric environment and two are not.

Component	IP Address	Result

SF-ePDC	129.118.105.50	Fail
SF-RTDMS	129.118.26.8	Fail
SF-AD	129.118.26.37	Pass
ePDC	129.118.105.44	Pass
RTDMS	129.118.19.167	Pass

Table 6. Affected Components and testing result for MS12-020 vulnerability in Security Fabric System

Scripts for testing exploits: Based on the potential vulnerability in testing system, Metasploit script is used for testing the exploitable of vulnerability MS12-020:

```
msf > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids

msf exploit(ms12_020_maxchannelids) > set rhost [IP Address]

msf exploit(ms12_020_maxchannelids) > run
```

Where the parameter `[IP Address]` is IP address for machine to be tested (e.g., 129.118.105.50 for SF-ePDC).

Results:

1. Testing results on SF-ePDC on May 28, 2014:

```
[*] 129.118.105.50:3389 - Sending MS12-020 Microsoft Remote Desktop Use-
After-Free DoS

[*] 129.118.105.50:3389 - 210 bytes sent

[*] 129.118.105.50:3389 - Checking RDP status...

[-] 129.118.105.50:3389 - RDP Service Unreachable

[*] Auxiliary module execution completed
```

After exploiting the vulnerability on SF-ePDC, the connection to Remote Desktop Application service on SF-ePDC cannot be established. Therefore, SF-ePDC is vulnerable for Denial of Service by exploiting MS12-020 vulnerability.

2. Testing results on SF-RTDMS on May 28, 2014:

```
[*] 129.118.26.8:3389 - Sending MS12-020 Microsoft Remote Desktop Use-
After-Free DoS

[*] 129.118.26.8:3389 - 210 bytes sent
```

```
  [*] 129.118.26.8:3389 - Checking RDP status...

  [-] 129.118.26.8:3389 - RDP Service Unreachable

  [*] Auxiliary module execution completed
```

After exploiting the vulnerability on SF-RTDMS, the connection to Remote Desktop Application service on SF-RTDMS cannot be established. Therefore, SF-RTDMS is vulnerable for Denial of Service by exploiting MS12-020 vulnerability.

3. Testing results on Active Directory on May 28, 2014:

```
  [*] 129.118.26.37:3389 - Sending MS12-020 Microsoft Remote Desktop Use-
After-Free DoS

  [*] 129.118.26.37:3389 - 210 bytes sent

  [*] 129.118.26.37:3389 - Checking RDP status...

  [-] 129.118.26.37:3389 - RDP Service Unreachable

  [*] Auxiliary module execution completed
```

After exploiting the vulnerability on Active Directory, the connection to Remote Desktop Application service on Active Directory can be established. Therefore, Active Directory component is not vulnerable for Denial of Service by exploiting MS12-020 vulnerability.

4. Testing results on ePDC machine on May 28, 2014:

```
  [*] 129.118.105.44:3389 - Sending MS12-020 Microsoft Remote Desktop Use-
After-Free DoS

  [*] 129.118.105.44:3389 - 210 bytes sent

  [*] 129.118.105.44:3389 - Checking RDP status...

  [-] 129.118.105.44:3389 - RDP Service Unreachable

  [*] Auxiliary module execution completed
```

After exploiting the vulnerability on ePDC, the connection to Remote Desktop Application service on ePDC can be established. Therefore, ePDC component is not vulnerable for Denial of Service by exploiting MS12-020 vulnerability.

5. Testing results on RTDMS machine on May 28, 2014:

```
  [*] 129.118.19.167:3389 - Sending MS12-020 Microsoft Remote Desktop Use-
After-Free DoS

  [*] 129.118.19.167:3389 - 210 bytes sent

  [*] 129.118.19.167:3389 - Checking RDP status...

  [-] 129.118.19.167:3389 - RDP Service Unreachable

  [*] Auxiliary module execution completed
```

After exploiting the vulnerability on RTDMS, the connection to Remote Desktop Application service on RTDMS can be established. Therefore, RTDMS component is not vulnerable for Denial of Service by exploiting MS12-020 vulnerability.

Suggestion: To remove this vulnerability from the effected components (WRL on both Reese-site and TTU-site), where Microsoft Windows Server 2008 R2 SP1 is used as the back-ends, both machines need to download and apply the patch from http://go.microsoft.com/fwlink/?LinkId=232664.

The following are the list of websites that provide more details about this vulnerability:

- **TA12-073A** http://www.us-cert.gov/ncas/alerts/TA12-073A
- **CVE-2012-0002** http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0002
- **CVE-2012-0152** http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0152
- **MS12-020** https://technet.microsoft.com/library/security/ms12-020
- **MSKB 2671387** http://support.microsoft.com/default.aspx?scid=kb;EN-US;2671387
- http://www.microsoft.com/downloads/details.aspx?familyid=6a07f99c-8ab4-4e44-8d48-6ac787dd2b51

B.2 X.509 Certificate Subject CN Does Not Match the Entity Name

Descriptions: The subject common name (CN) field in the X.509 certificate does not match the name of the entity presenting the certificate.

Before issuing a certificate, a Certification Authority (CA) must check the identity of the entity requesting the certificate, as specified in the CA's Certification Practice Statement (CPS). Thus, standard certificate validation procedures require the subject CN field of a certificate to match the actual name of the entity presenting the certificate. For example, in a certificate presented by "https://www.example.com/", the CN should be "www.example.com".

In order to detect and prevent active eavesdropping attacks, the validity of a certificate must be verified, or else an attacker could then launch a man-in-the-middle attack and gain full control of the data stream. Of particular importance is the validity of the subject's CN that should match the name of the entity (hostname).

A CN mismatch most often occurs due to a configuration error, though it can also indicate that a man-in-the-middle attack is being conducted.

Findings: There are four services provided in testing system where X.509 Certificate Subject CN does not match with the entity name as shown below.

Component	IP Address	Result
SF-ePO	129.118.19.210:443	CN 'AH_EPO-SF' vs. '129.118.19.210'
SF-ePO	129.118.19.210:8443	CN 'EPO-SF' vs. '129.118.19.210'
SF-ePO	129.118.19.210:8444	CN 'Orion_ClientAuth_EPO-SF' vs. '129.118.19.210'
SF-ESM	129.118.26.40:443	CN 'esm.mcafee.local' vs. '129.118.26.40'

Table 7. Affected Components and checking result on mismatch of X.509 certificate

Scripts for testing vulnerabilities: Based on the services with X.509 certificate in testing system, OpenSSL script is used for finding the vulnerability of mismatch CN and *nodename* in X.509:

```
$openssl s_client –connect [IP Address]:[Port] –show certificate
```

Where the parameter `[IP Address]` and `[Port]` are IP address and port of machine to be tested, respectively (e.g., 129.118.19.210:443 for SF-ePO machine on https port).

Result:

1. The partial output results of testing on port 443 of SF-ePO component:

```
CONNECTED(00000003)

depth=0 O = McAfee, OU = ePO, CN = AH_EPO-SF

verify error:num=20:unable to get local issuer certificate

verify return:1

depth=0 O = McAfee, OU = ePO, CN = AH_EPO-SF

verify error:num=27:certificate not trusted

verify return:1

depth=0 O = McAfee, OU = ePO, CN = AH_EPO-SF

verify error:num=21:unable to verify the first certificate

verify return:1
```

```
---

Certificate chain

 0 s:/O=McAfee/OU=ePO/CN=AH_EPO-SF

   i:/O=McAfee/OU=AH/CN=AH_CA_EPO-SF

---
```

As shown in the output the CN appeared (i.e., AH_EPO-SF) in X.509 certificate does not match with the node name of SF-ePO.

2. The partial output results of testing on port 8443 of SF-ePO component:

```
CONNECTED(00000003)

depth=1 O = McAfee, OU = Orion, CN = Orion_CA_EPO-SF

verify error:num=19:self signed certificate in certificate chain

verify return:0

---

Certificate chain

 0 s:/O=McAfee/OU=Orion/CN=EPO-SF

   i:/O=McAfee/OU=Orion/CN=Orion_CA_EPO-SF

 1 s:/O=McAfee/OU=Orion/CN=Orion_CA_EPO-SF

   i:/O=McAfee/OU=Orion/CN=Orion_CA_EPO-SF

---
```

As shown in the output the CN appeared (i.e., Orion_CA_EPO-SF) in X.509 certificate does not match with the node name of ePO.

3. The partial output results of testing on port 8444 of SF-ePO component:

```
CONNECTED(00000003)

depth=1 O = McAfee, OU = Orion, CN = Orion_CA_EPO-SF

verify error:num=19:self signed certificate in certificate chain
```

```
  verify return:0

  ---

  Certificate chain

   0 s:/O=McAfee/OU=Orion/CN=Orion_ClientAuth_EPO-SF

     i:/O=McAfee/OU=Orion/CN=Orion_CA_EPO-SF

   1 s:/O=McAfee/OU=Orion/CN=Orion_CA_EPO-SF

     i:/O=McAfee/OU=Orion/CN=Orion_CA_EPO-SF

  ---
```

As shown in the output the CN appeared (i.e., Orion_ClientAuth_EPO-SF) in X.509 certificate does not match with the node name of ePO.

4. The partial output results of testing on port 443 of SF-ESM component:

```
  CONNECTED(00000003)

  depth=0 C = US, ST = TX, L = Plano, O = McAfee, OU = Enterprise Security
Manager, CN = esm.mcafee.local, emailAddress = support@nitrosecurity.com

  verify error:num=18:self signed certificate

  verify return:1

  depth=0 C = US, ST = TX, L = Plano, O = McAfee, OU = Enterprise Security
Manager, CN = esm.mcafee.local, emailAddress = support@nitrosecurity.com

  verify return:1

  ---

  Certificate chain

   0 s:/C=US/ST=TX/L=Plano/O=McAfee/OU=Enterprise Security
Manager/CN=esm.mcafee.local/emailAddress=support@nitrosecurity.com

     i:/C=US/ST=TX/L=Plano/O=McAfee/OU=Enterprise Security
Manager/CN=esm.mcafee.local/emailAddress=support@nitrosecurity.com

   1 s:/C=US/ST=TX/L=Plano/O=McAfee/OU=Enterprise Security
Manager/CN=esm.mcafee.local/emailAddress=support@nitrosecurity.com
```

```
     i:/C=US/ST=TX/L=Plano/O=McAfee/OU=Enterprise Security
Manager/CN=esm.mcafee.local/emailAddress=support@nitrosecurity.com

   ---
```

As shown in the output the CN appeared (i.e., Orion_ClientAuth_EPO-SF) in X.509 certificate does not match with the node name of ESM.

Suggestion: To remove this mismatch of common name (CN) and node name in X.509 certificate, the subject's CN field in the X.509 certificate should reflect the name of the entity presenting the certificate (e.g., the hostname). We can accomplish this by generating a new certificate that is usually signed by a Certification Authority (CA) and trusted by both client and server.

B.3 SMB signing disabled

Descriptions: This system does not allow SMB signing. SMB signing allows the recipient of SMB packets to confirm their authenticity and helps prevent man in the middle attacks against SMB. SMB signing can be configured in one of three ways: disabled entirely (least secure), enabled, and required (most secure).

Findings: There are seven services provided in testing system where SMB signing is disabled. These are shown below.

Component	IP Address	Result
ePDC	129.118.105.44:139	Message signing disabled (dangerous, but default)
ePDC	129.118.105.44:445	Message signing disabled (dangerous, but default)
RTDMS	129.118.19.167:445	Message signing disabled (dangerous, but default)
SF-ePO	129.118.19.210:139	Message signing disabled (dangerous, but default)
SF-ePO	129.118.19.210:445	Message signing disabled (dangerous, but default)
SF-AD	129.118.19.26.37:139	Message signing required
SF-AD	129.118.19.26.37:445	Message signing required

Table 8. Affected Components and checking result on mismatch of SMB signing disabled

Scripts for testing vulnerabilities: The result from Table 8 is gathered from running the script as follows:

```
  $ nmap --script smb-security-mode.nse [-Pn] –p[port] [host]
```

Results:

1. The output results of testing on port 139 of SF-ePO component:

```
  Starting Nmap 6.00 ( http://nmap.org ) at 2014-06-11 03:40 CDT
```

```
Nmap scan report for p3eepdc.ttu.edu (129.118.105.44)
Host is up (0.00097s latency).
PORT    STATE SERVICE
139/tcp open  netbios-ssn

Host script results:
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
Nmap done: 1 IP address (1 host up) scanned in 1.27 seconds
```

2. The output results of testing on port 445 of SF-ePO component:

```
Nmap scan report for p3eepdc.ttu.edu (129.118.105.44)
Host is up (0.00092s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
```

```
|_  Message signing disabled (dangerous, but default)


Nmap done: 1 IP address (1 host up) scanned in 1.27 seconds
```

3. The output results of testing on port 445 of RTDMS component:

```
Nmap scan report for p3ertdms.ttu.edu (129.118.19.167)
Host is up (0.00040s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds


Host script results:
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)


Nmap done: 1 IP address (1 host up) scanned in 2.27 seconds
```

4. The output results of testing on port 139 of SF-ePO component:

```
Starting Nmap 6.00 ( http://nmap.org ) at 2014-06-11 03:49 CDT
Nmap scan report for epo-sf.epg.secfab.org (129.118.19.210)
Host is up (0.00047s latency).
PORT    STATE SERVICE
139/tcp open  netbios-ssn
```

```
Host script results:
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

5. The output results of testing on port 445 of SF-ePO component:

```
Starting Nmap 6.00 ( http://nmap.org ) at 2014-06-11 03:50 CDT
Nmap scan report for epo-sf.epg.secfab.org (129.118.19.210)
Host is up (0.00050s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

6. The output results of testing on port 139 of SF-AD component:

```
Starting Nmap 6.00 ( http://nmap.org ) at 2014-06-11 03:56 CDT
Nmap scan report for dc-sf.epg.secfab.org (129.118.26.37)
Host is up (0.00053s latency).
PORT    STATE SERVICE
139/tcp open  netbios-ssn

Host script results:
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing required

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

7. The output results of testing on port 445 of SF-AD component:

```
Starting Nmap 6.00 ( http://nmap.org ) at 2014-06-11 03:58 CDT
Nmap scan report for dc-sf.epg.secfab.org (129.118.26.37)
Host is up (0.00043s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-security-mode:
|   Account that was used for smb scripts: guest
```

```
|   User-level authentication

|   SMB Security: Challenge/response passwords supported

|_  Message signing required


Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

Suggestion: To remove this vulnerability, the administrator of the system needs to setup the operating system (e.g., Windows) to enable or require SMB signing appropriately. The method and effect of doing this depend on each system specification (as shown in more details in the following link http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx). Be sure that SMB signing configuration is done for incoming connections (Server).

Moreover, we also need to configure Samba protocol to enable or require SMB signing as appropriate. To enable SMB signing, put the following in the Samba configuration file, typically `smb.conf`, in the global section:

```
server signing = auto
```

To require SMB signing, put the following in the Samba configuration file, typically `smb.conf`, in the global section:

```
server signing = mandatory
```

B.4 Remote Desktop Protocol over SSL supports weak RC4 cipher

Descriptions: Remote Desktop Protocol is a protocol by which Terminal Service provides desktop level access to a remote user. It can be used to remotely login and interact with a Windows machine. Since RDP transfers sensitive information about the user and the system, it can be configured to use encryption to provide privacy and integrity for its sessions. It is possible to configure RDP to use encryption algorithms that are considered insecure, such as RC4 40bit and RC4 56 bit.

Findings: As shown below, there are five services provided in testing system where Remote Desktop Protocol over SSL supports weak cipher can be exploited.

Component	IP Address	Result
RTDMS	129.118.19.167:3389	RC4 40 bit and 50 bit are supported
SF-RTDMS	129.118.26.8:3389	RC4 40 bit and 50 bit are supported
SF-ePDC	129.118.105.50:3389	Cannot connect (wait for service to enable)?

SF-AD	129.118.26.37:3389	RC4 40 bit and 50 bit are supported
ePDC	129.118.105.44:3389	RC4 40 bit and 50 bit are supported

Table 9. Affected Components and checking result on RDP over SSL support weak cipher

Scripts for testing vulnerabilities: The result from Table 9 is generated by running the following script:

```
$ nmap –-script rdp-enum-encryption –p[port] [host]
```

Results:

1. The output results of testing on port 3389 of RTDMS component:

```
Starting Nmap 6.46 ( http://nmap.org ) at 2014-07-07 04:42 CDT

NSE: Loaded 1 scripts for scanning.

NSE: Script Pre-scanning.

Initiating Ping Scan at 04:42

Scanning 129.118.19.167 [2 ports]

Completed Ping Scan at 04:42, 1.20s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 04:42

Completed Parallel DNS resolution of 1 host. at 04:42, 0.00s elapsed

Initiating Connect Scan at 04:42

Scanning p3ertdms.ttu.edu (129.118.19.167) [1 port]

Discovered open port 3389/tcp on 129.118.19.167

Completed Connect Scan at 04:42, 0.00s elapsed (1 total ports)

NSE: Script scanning 129.118.19.167.

Initiating NSE at 04:42

Completed NSE at 04:42, 0.09s elapsed

Nmap scan report for p3ertdms.ttu.edu (129.118.19.167)

Host is up (0.00028s latency).

PORT     STATE SERVICE
```

```
3389/tcp open  ms-wbt-server
| rdp-enum-encryption:
|   Security layer
|     CredSSP: SUCCESS
|     Native RDP: SUCCESS
|     SSL: SUCCESS
|   RDP Encryption level: Client Compatible
|     40-bit RC4: SUCCESS
|     56-bit RC4: SUCCESS
|     128-bit RC4: SUCCESS
|_    FIPS 140-1: SUCCESS
```

2. The output results of testing on port 3389 of SF-RTDMS component:

```
Starting Nmap 6.46 ( http://nmap.org ) at 2014-07-07 04:58 CDT
Nmap scan report for 129.118.26.8
Host is up (0.00048s latency).
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
| rdp-enum-encryption:
|   Security layer
|     CredSSP: SUCCESS
|     Native RDP: SUCCESS
|     SSL: SUCCESS
|   RDP Encryption level: Client Compatible
|     40-bit RC4: SUCCESS
|     56-bit RC4: SUCCESS
```

```
|     128-bit RC4: SUCCESS
|_    FIPS 140-1: SUCCESS


Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

3. The output results of testing on port 3389 of SF-AD component:

```
NSE: Script Post-scanning.
Read data files from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds


Starting Nmap 6.46 ( http://nmap.org ) at 2014-07-07 04:51 CDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Parallel DNS resolution of 1 host. at 04:51
Completed Parallel DNS resolution of 1 host. at 04:51, 0.00s elapsed
Initiating Connect Scan at 04:51
Scanning dc-sf.epg.secfab.org (129.118.26.37) [1 port]
Discovered open port 3389/tcp on 129.118.26.37
Completed Connect Scan at 04:51, 0.00s elapsed (1 total ports)
NSE: Script scanning 129.118.26.37.
Initiating NSE at 04:51
Completed NSE at 04:51, 0.06s elapsed
Nmap scan report for dc-sf.epg.secfab.org (129.118.26.37)
Host is up (0.00051s latency).
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
```

```
| rdp-enum-encryption:
|   Security layer
|     CredSSP: SUCCESS
|     Native RDP: SUCCESS
|     SSL: SUCCESS
|   RDP Encryption level: Client Compatible
|     40-bit RC4: SUCCESS
|     56-bit RC4: SUCCESS
|     128-bit RC4: SUCCESS
|_    FIPS 140-1: SUCCESS


NSE: Script Post-scanning.
Read data files from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

4. The output results of testing on port 3389 of ePDC component:

```
Starting Nmap 6.46 ( http://nmap.org ) at 2014-07-07 04:53 CDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Parallel DNS resolution of 1 host. at 04:53
Completed Parallel DNS resolution of 1 host. at 04:53, 0.00s elapsed
Initiating Connect Scan at 04:53
Scanning p3eepdc.ttu.edu (129.118.105.44) [1 port]
Discovered open port 3389/tcp on 129.118.105.44
Completed Connect Scan at 04:53, 0.00s elapsed (1 total ports)
NSE: Script scanning 129.118.105.44.
```

```
Initiating NSE at 04:53

Completed NSE at 04:53, 0.08s elapsed

Nmap scan report for p3eepdc.ttu.edu (129.118.105.44)

Host is up (0.00089s latency).

PORT     STATE SERVICE

3389/tcp open  ms-wbt-server

| rdp-enum-encryption:

|   Security layer

|     CredSSP: SUCCESS

|     Native RDP: SUCCESS

|     SSL: SUCCESS

|   RDP Encryption level: Client Compatible

|     40-bit RC4: SUCCESS

|     56-bit RC4: SUCCESS

|     128-bit RC4: SUCCESS

|_    FIPS 140-1: SUCCESS


NSE: Script Post-scanning.

Read data files from: /usr/local/bin/../share/nmap

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

Suggestion: Configure the remote desktop application to disallow the connection from weak cipher algorithm (e.g., http://technet.microsoft.com/en-us/library/cc770833.aspx for Windows Server 2008 R2).

B.5 TLS/SSL Server Supports Weak Cipher Algorithms

Descriptions: The TLS/SSL server supports cipher suites based on weak algorithms. This may enable an attacker to launch man-in-the-middle attacks and monitor or tamper with sensitive data. In general, the following ciphers are considered weak:

- So called "null" ciphers, because they do not encrypt data.
- Export ciphers using secret key lengths restricted to 40 bits. This is usually indicated by the word EXP/EXPORT in the name of the cipher suite.
- Obsolete encryption algorithms with secret key lengths considered short by today's standards, e.g. DES or RC4 with 56-bit keys.

Findings: As shown below, there is only one service provided in testing system that provided TLS/SSL Server, which supports weak cipher algorithm.

Component	IP Address	Result
SF-AD	129.118.26.37:636	RC4 128 bit with MD5 should not be used, due to crypto-analytical attacks

Table 10 Affected Components and checking result on TLS/SSL support weak cipher

Scripts for testing vulnerabilities: The result from Table 10 is generated by running the following script:

```
$ nmap --script ssl-cert,ssl-enum-ciphers [-Pn] –p[port] [host]
```

Results:

1. The output results of testing on port 636 of SF-AD component:

```
Starting Nmap 6.00 ( http://nmap.org ) at 2014-06-12 06:47 CDT

Nmap scan report for dc-sf.epg.secfab.org (129.118.26.37)

Host is up (0.0069s latency).

PORT    STATE SERVICE

636/tcp open  ldapssl

| ssl-cert: Subject: commonName=DC-SF.EPG.SECFAB.ORG

| Issuer: commonName=EPG-DC-SF-CA

| Public Key type: rsa

| Public Key bits: 2048

| Not valid before: 2014-05-30 18:56:29

| Not valid after:  2015-05-30 18:56:29
```

```
| MD5:   0a7d 977e a844 ae8c a409 ea60 fb44 e075
|_SHA-1: e75f f634 dda9 1458 ba51 3f31 26c2 82e2 717b 29fa
| ssl-enum-ciphers:
|   SSLv3
|     Ciphers (3)
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_RC4_128_MD5 - unknown strength
|       TLS_RSA_WITH_RC4_128_SHA - strong
|     Compressors (1)
|       NULL
|   TLSv1.0
|     Ciphers (7)
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - unknown strength
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - unknown strength
|       TLS_RSA_WITH_RC4_128_MD5 - unknown strength
|       TLS_RSA_WITH_RC4_128_SHA - strong
|     Compressors (1)
|       NULL
|_  Least strength = unknown strength


Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds
```

Suggestions: Restrict the use of certain cryptographic algorithm and protocols. For more details on the restriction see http://support.microsoft.com/kb/245030/.

B.6 TLS/SSL Server Supports SSL version 2.0

Descriptions: Although the server accepts clients using TLS or SSLv3, it also accepts clients using SSLv2. SSLv2 is an older implementation of the Secure Sockets Layer protocol. It suffers from a number of security flaws allowing attackers to capture and alter information passed between a client and the server, including the following weaknesses:

- No protection from against man-in-the-middle attacks during the handshake
- Weak MAC construction and MAC relying solely on the MD5 hash function
- Exportable cipher suites unnecessarily weaken the MACs
- Same cryptographic keys used for message authentication and encryption
- Vulnerable to truncation attacks by forged TCP FIN packets

SSLv2 has been deprecated and is no longer recommended. Note that neither SSLv2 nor SSLv3 meet the U.S. FIPS 140-2 standard, which governs cryptographic modules for use in federal information systems. Only the newer TLS (Transport Layer Security) protocol meets FIPS 140-2 requirements. In addition, the presence of an SSLv2-only service on a host is deemed a failure by the PCI (Payment Card Industry) Data Security Standard.

Findings: As shown below, there is only one service in the tested system that provides TLS/SSL Server, which supports SSL version 2.0.

Component	IP Address	Result
SF-AD	129.118.26.37:636	SSL version 2.0 is supported

Table 11. Affected Components and checking result on TLS/SSL support SSL version 2.0

Scripts for testing vulnerabilities: The result from Table 11 is generated by running the following script:

```
$ nmap --script sslv2 [-Pn] –p[port] [host]
```

Results:

1. The output results of testing on port 636 of SF-AD component:

```
Starting Nmap 6.46 ( http://nmap.org ) at 2014-07-07 04:29 CDT

NSE: Loaded 1 scripts for scanning.
```

```
NSE: Script Pre-scanning.
Initiating Parallel DNS resolution of 1 host. at 04:30
Completed Parallel DNS resolution of 1 host. at 04:30, 0.00s elapsed
Initiating Connect Scan at 04:30
Scanning dc-sf.epg.secfab.org (129.118.26.37) [1 port]
Discovered open port 636/tcp on 129.118.26.37
Completed Connect Scan at 04:30, 0.00s elapsed (1 total ports)
NSE: Script scanning 129.118.26.37.
Initiating NSE at 04:30
Completed NSE at 04:30, 0.00s elapsed
Nmap scan report for dc-sf.epg.secfab.org (129.118.26.37)
Host is up (0.0030s latency).
PORT    STATE SERVICE
636/tcp open  ldapssl
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5


NSE: Script Post-scanning.
Read data files from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

Suggestions: Restrict the use of certain cryptographic algorithm and protocols. For more details about the restriction see http://support.microsoft.com/kb/245030/.

B.7 Database Open Access

Descriptions: The database allows any remote system the ability to connect to it. It is recommended to limit direct access to trusted systems because databases may contain sensitive data, and new vulnerabilities and exploits are discovered routinely for them. For this reason, it is a violation of PCI DSS section 1.3.7 to have databases listening on ports accessible from the Internet, even when protected with secure authentication mechanisms.

Findings: There are two services provided in testing system that provided database open access as shown in the table below.

Component	IP Address	Result
ePDC	129.118.105.44:1433	Running Microsoft SQL Server 2012
SF-ePO	129.118.19.210:1433	Running Microsoft SQL Server 2008 R2

Table 12. Affected Components and checking result on database open access

Scripts for testing vulnerabilities: The results from the table above are generated by running the following script:

```
$ nmap –sV –p[port] [host]
```

Results:

1. The output results of testing on port 1433 of ePDC component:

```
Starting Nmap 6.46 ( http://nmap.org ) at 2014-07-18 05:39 CDT

Nmap scan report for p3eepdc.ttu.edu (129.118.105.44)

Host is up (0.00088s latency).

PORT     STATE SERVICE  VERSION

1433/tcp open  ms-sql-s Microsoft SQL Server 2012

1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
http://www.insecure.org/cgi-bin/servicefp-submit.cgi :

SF-Port1433-TCP:V=6.46%I=7%D=7/18%Time=53C8F956%P=i686-pc-linux-gnu%r(ms-s

SF:ql-s,25,"\x04\x01\0%\0\0\x01\0\0\0\x15\0\x06\x01\0\x1b\0\x01\x02\0\x1c\
```

```
  SF:0\x01\x03\0\x1d\0\0\xff\x0b\0\x08\xaa\0\0\0\0");

  Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

  Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

  Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds
```

2. The output results of testing on port 1433 of SF-ePO component:

```
  Starting Nmap 6.46 ( http://nmap.org ) at 2014-07-18 05:43 CDT

  Nmap scan report for epo-sf.epg.secfab.org (129.118.19.210)

  Host is up (0.00072s latency).

  PORT     STATE SERVICE  VERSION

  1433/tcp open  ms-sql-s Microsoft SQL Server 2008 R2 10.50.1600; RTM

  Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows



  Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

  Nmap done: 1 IP address (1 host up) scanned in 6.16 seconds
```

Suggestions: To remove this vulnerability, the database server needs to be configured to only allow access from trusted systems. For example, the PCI DSS standard requires you to place the database in an internal network zone, segregated from the DMZ.

B.8 Heartbleed Vulnerability

Descriptions: Heartbleed is a security bug in the OpenSSL cryptography library. OpenSSL is a widely used implementation of the Transport Layer Security (TLS) protocol. Heartbleed may be exploited whether the party using a vulnerable OpenSSL instance for TLS is a server or a client.

Heartbleed results from improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension, the heartbeat being the basis for the bug's name. The vulnerability is classified as a buffer over-read, a situation where software allows more data to be read than should be allowed.

Findings: There are six potential services provided in testing system that might be affected by Heartbleed vulnerability as shown below.

IP Address	Service	Heartbeat support	Exploitable
129.118.19.210:443 (SF-ePO)	ssl/http	Yes	No
129.118.19.210:8443 (SF-ePO)	ssl/http	No	No
129.118.19.210:8444 (SF-ePO)	ssl/http	No	No
129.118.26.40:443 (SF-ESM)	ssl/http	Yes	No
129.118.26.37:636 (SF-AD)	ssl/ldap	No	No
129.118.26.37:3269 (SF-AD)	ssl/ldap	No	No

Table 13. Potential services that might be affected by Heartbleed vulnerability and the testing result.

Scripts for testing vulnerabilities: The result of checking the supporting Heartbeat extension from Table 13 is generated by running the following script:

```
$openssl s_client –connect [host]:[port] -tlsextdebug
```

Results:

1. The output results of testing on port 443 of SF-ePO component (support Heartbeat):

```
CONNECTED(00000003)

TLS server extension "renegotiation info" (id=65281), len=1

0001 - <SPACES/NULS>

TLS server extension "session ticket" (id=35), len=0

TLS server extension "heartbeat" (id=15), len=1

0000 - 01                                                .

depth=0 O = McAfee, OU = ePO, CN = AH_EPO-SF

verify error:num=20:unable to get local issuer certificate

verify return:1

depth=0 O = McAfee, OU = ePO, CN = AH_EPO-SF

verify error:num=27:certificate not trusted

verify return:1
```

```
depth=0 O = McAfee, OU = ePO, CN = AH_EPO-SF

verify error:num=21:unable to verify the first certificate

verify return:1
```

2. The output results of testing on port 8443 of SF-ePO component (not support Heartbeat):

```
CONNECTED(00000003)

TLS server extension "EC point formats" (id=11), len=2

0000 - 01                                                .

0002 - <SPACES/NULS>

depth=1 O = McAfee, OU = Orion, CN = Orion_CA_EPO-SF

verify error:num=19:self signed certificate in certificate chain

verify return:0
```

3. The output results of testing on port 8444 of SF-ePO component (not support Heartbeat):

```
CONNECTED(00000003)

TLS server extension "EC point formats" (id=11), len=2

0000 - 01                                                .

0002 - <SPACES/NULS>

depth=1 O = McAfee, OU = Orion, CN = Orion_CA_EPO-SF

verify error:num=19:self signed certificate in certificate chain

verify return:0
```

4. The output results of testing on port 443 of SF-ESM component (support Heartbeat):

```
CONNECTED(00000003)

TLS server extension "renegotiation info" (id=65281), len=1

0001 - <SPACES/NULS>

TLS server extension "session ticket" (id=35), len=0
```

```
  TLS server extension "heartbeat" (id=15), len=1

  0000 - 01                                                .

  depth=0 C = US, ST = TX, L = Plano, O = McAfee, OU = Enterprise Security
Manager, CN = esm.mcafee.local, emailAddress = support@nitrosecurity.com

  verify error:num=18:self signed certificate

  verify return:1

  depth=0 C = US, ST = TX, L = Plano, O = McAfee, OU = Enterprise Security
Manager, CN = esm.mcafee.local, emailAddress = support@nitrosecurity.com

  verify return:1
```

5. The output results of testing on port 636 of SF-AD component (not support Heartbeat):

```
  CONNECTED(00000003)

  TLS server extension "renegotiation info" (id=65281), len=1

  0001 - <SPACES/NULS>

  depth=0 CN = DC-SF.EPG.SECFAB.ORG

  verify error:num=20:unable to get local issuer certificate

  verify return:1

  depth=0 CN = DC-SF.EPG.SECFAB.ORG

  verify error:num=27:certificate not trusted

  verify return:1

  depth=0 CN = DC-SF.EPG.SECFAB.ORG

  verify error:num=21:unable to verify the first certificate

  verify return:1
```

6. The output results of testing on port 3269 of SF-AD component (not support Heartbeat):

```
  CONNECTED(00000003)
```

```
TLS server extension "renegotiation info" (id=65281), len=1

0001 - <SPACES/NULS>

depth=0 CN = DC-SF.EPG.SECFAB.ORG

verify error:num=20:unable to get local issuer certificate

verify return:1

depth=0 CN = DC-SF.EPG.SECFAB.ORG

verify error:num=27:certificate not trusted

verify return:1

depth=0 CN = DC-SF.EPG.SECFAB.ORG

verify error:num=21:unable to verify the first certificate

verify return:1
```

Scripts for testing exploits:

For each service that supports Heartbeat extension, the following scripts from Metasploit framework are used to verify the exploitable of Heartbleed vulnerabilities:

```
msf> use auxiliary/scanner/ssl/openssl_heartbleed

msf auxiliary(openssl_heartbleed)> set rhosts [hosts]

msf auxiliary(openssl_heartbleed)> set rport [port]

msf auxiliary(openssl_heartbleed)> set tls_version [tls_version]

msf auxiliary(openssl_heartbleed)> run
```

Results:

1. The output results of exploiting on port 443 of SF-ePO component:

```
[*] 129.118.19.210:443 - Sending Client Hello...

[!] SSL record #1:

[!]     Type:    22
```

```
  [!]     Version: 0x0301

  [!]     Length:  54

  [!]     Handshake #1:

  [!]             Length: 50

  [!]             Type:   Server Hello (2)

  [!]             Server Hello Version:           0x0301

  [!]             Server Hello random data:
b348b1b1a94512858f8685805a0694a04e2e3a6d1c8894ef844ad43f3cc38c60

  [!]             Server Hello Session ID length: 0

  [!]             Server Hello Session ID:

  [!] SSL record #2:

  [!]     Type:    22

  [!]     Version: 0x0301

  [!]     Length:  838

  [!]     Handshake #1:

  [!]             Length: 834

  [!]             Type:   Certificate Data (11)

  [!]             Certificates length: 831

  [!]             Certificate #1:

  [!]                     Certificate #1: Length: 828

  [!]                     Certificate #1: #<OpenSSL::X509::Certificate:
subject=/O=McAfee/OU=ePO/CN=AH_EPO-SF, issuer=/O=McAfee/OU=
AH/CN=AH_CA_EPO-SF, serial=5957554068034109659, not_before=1970-01-01
00:00:00 UTC, not_after=2043-09-04 08:13:09 UTC>

  [!] SSL record #3:

  [!]     Type:    22
```

```
  [!]     Version: 0x0301

  [!]     Length:  525

  [!]     Handshake #1:

  [!]             Length: 521

  [!]             Type:   Server Key Exchange (12)

  [!] SSL record #4:

  [!]     Type:    22

  [!]     Version: 0x0301

  [!]     Length:  4

  [!]     Handshake #1:

  [!]             Length: 0

  [!]             Type:   Server Hello Done (14)

  [*] 129.118.19.210:443 - Sending Client Hello...

  [!] SSL record #1:

  [!]     Type:    22

  [!]     Version: 0x0301

  [!]     Length:  54

  [!]     Handshake #1:

  [!]             Length: 50

  [!]             Type:   Server Hello (2)

  [!]             Server Hello Version:           0x0301

  [!]             Server Hello random data:
2d38960b433d847cfe645621629474bdc575b92e64566268fd9549dd720cfa60

  [!]             Server Hello Session ID length: 0

  [!]             Server Hello Session ID:
```

```
  [!] SSL record #2:

  [!]     Type:    22

  [!]     Version: 0x0301

  [!]     Length:  838

  [!]     Handshake #1:

  [!]             Length: 834

  [!]             Type:   Certificate Data (11)

  [!]             Certificates length: 831

  [!]             Certificate #1:

  [!]                     Certificate #1: Length: 828

  [!]                     Certificate #1: #<OpenSSL::X509::Certificate:
subject=/O=McAfee/OU=ePO/CN=AH_EPO-SF, issuer=/O=McAfee/OU=
AH/CN=AH_CA_EPO-SF, serial=5957554068034109659, not_before=1970-01-01
00:00:00 UTC, not_after=2043-09-04 08:13:09 UTC>

  [!] SSL record #3:

  [!]     Type:    22

  [!]     Version: 0x0301

  [!]     Length:  525

  [!]     Handshake #1:

  [!]             Length: 521

  [!]             Type:   Server Key Exchange (12)

  [!] SSL record #4:

  [!]     Type:    22

  [!]     Version: 0x0301

  [!]     Length:  4

  [!]     Handshake #1:
```

```
  [!]             Length: 0

  [!]             Type:   Server Hello Done (14)

  [*] 129.118.19.210:443 - Sending Heartbeat...

  [-] 129.118.19.210:443 - No Heartbeat response...

  [-] 129.118.19.210:443 - Looks like there isn't leaked information...

  [*] Scanned 1 of 1 hosts (100% complete)

  [*] Auxiliary module execution completed
```

2. The output results of exploiting on port 443 of SF-ESM component:

```
  [*] 129.118.26.40:443 - Sending Client Hello...

  [!] SSL record #1:

  [!]     Type:    22

  [!]     Version: 0x0301

  [!]     Length:  86

  [!]     Handshake #1:

  [!]             Length: 82

  [!]             Type:   Server Hello (2)

  [!]             Server Hello Version:           0x0301

  [!]             Server Hello random data:
c4e23b82387803b7f00891353e6336f4f6e3506e535eaf88fd039675f74b1dd5

  [!]             Server Hello Session ID length: 32

  [!]             Server Hello Session ID:
2201cf9cb3a59d265c7f2149c2aa99354c9c80be4596e30de21c115cc04c3fb7

  [!] SSL record #2:

  [!]     Type:    22

  [!]     Version: 0x0301
```

```
  [!]     Length:  1961

  [!]     Handshake #1:

  [!]             Length: 1957

  [!]             Type:   Certificate Data (11)

  [!]             Certificates length: 1954

  [!]             Certificate #1:

  [!]                     Certificate #1: Length: 974

  [!]                     Certificate #1: #<OpenSSL::X509::Certificate:
subject=/C=US/ST=TX/L=Plano/O=McAfee/OU=Enterprise Security
Manager/CN=esm.mcafee.local/emailAddress=support@nitrosecurity.com,
issuer=/C=US/ST=TX/L=Plano/O=McAfee/OU=Enterprise Security
Manager/CN=esm.mcafee.local/emailAddress=support@nitrosecurity.com,
serial=13709899052840045994, not_before=2013-05-15 04:11:47 UTC,
not_after=2023-05-15 04:11:47 UTC>

  [!]             Certificate #2:

  [!]                     Certificate #2: Length: 974

  [!]                     Certificate #2: #<OpenSSL::X509::Certificate:
subject=/C=US/ST=TX/L=Plano/O=McAfee/OU=Enterprise Security
Manager/CN=esm.mcafee.local/emailAddress=support@nitrosecurity.com,
issuer=/C=US/ST=TX/L=Plano/O=McAfee/OU=Enterprise Security
Manager/CN=esm.mcafee.local/emailAddress=support@nitrosecurity.com,
serial=13709899052840045994, not_before=2013-05-15 04:11:47 UTC,
not_after=2023-05-15 04:11:47 UTC>

  [!] SSL record #3:

  [!]     Type:    22

  [!]     Version: 0x0301

  [!]     Length:  525

  [!]     Handshake #1:

  [!]             Length: 521

  [!]             Type:   Server Key Exchange (12)
```

```
  [!] SSL record #4:

  [!]     Type:    22

  [!]     Version: 0x0301

  [!]     Length:  4

  [!]     Handshake #1:

  [!]             Length: 0

  [!]             Type:   Server Hello Done (14)

  [*] 129.118.26.40:443 - Sending Client Hello...

  [!] SSL record #1:

  [!]     Type:    22

  [!]     Version: 0x0301

  [!]     Length:  86

  [!]     Handshake #1:

  [!]             Length: 82

  [!]             Type:   Server Hello (2)

  [!]             Server Hello Version:           0x0301

  [!]             Server Hello random data:
337acc7669ec433106d31c05b5ca1dbe77349f1bef9bd4c84e6cfd55f73e95e9

  [!]             Server Hello Session ID length: 32

  [!]             Server Hello Session ID:
b27ce41b4a135dec4106a958c999c7c7f51405e27a3021f453a7cd9a6f49964e

  [!] SSL record #2:

  [!]     Type:    22

  [!]     Version: 0x0301

  [!]     Length:  1961
```

```
  [!]     Handshake #1:

  [!]             Length: 1957

  [!]             Type:   Certificate Data (11)

  [!]             Certificates length: 1954

  [!]             Certificate #1:

  [!]                     Certificate #1: Length: 974

  [!]                     Certificate #1: #<OpenSSL::X509::Certificate:
subject=/C=US/ST=TX/L=Plano/O=McAfee/OU=Enterprise Security
Manager/CN=esm.mcafee.local/emailAddress=support@nitrosecurity.com,
issuer=/C=US/ST=TX/L=Plano/O=McAfee/OU=Enterprise Security
Manager/CN=esm.mcafee.local/emailAddress=support@nitrosecurity.com,
serial=13709899052840045994, not_before=2013-05-15 04:11:47 UTC,
not_after=2023-05-15 04:11:47 UTC>

  [!]             Certificate #2:

  [!]                     Certificate #2: Length: 974

  [!]                     Certificate #2: #<OpenSSL::X509::Certificate:
subject=/C=US/ST=TX/L=Plano/O=McAfee/OU=Enterprise Security
Manager/CN=esm.mcafee.local/emailAddress=support@nitrosecurity.com,
issuer=/C=US/ST=TX/L=Plano/O=McAfee/OU=Enterprise Security
Manager/CN=esm.mcafee.local/emailAddress=support@nitrosecurity.com,
serial=13709899052840045994, not_before=2013-05-15 04:11:47 UTC,
not_after=2023-05-15 04:11:47 UTC>

  [!] SSL record #3:

  [!]     Type:    22

  [!]     Version: 0x0301

  [!]     Length:  525

  [!]     Handshake #1:

  [!]             Length: 521

  [!]             Type:   Server Key Exchange (12)

  [!] SSL record #4:
```

```
[!]     Type:    22

[!]     Version: 0x0301

[!]     Length:  4

[!]     Handshake #1:

[!]             Length: 0

[!]             Type:   Server Hello Done (14)

[*] 129.118.26.40:443 - Sending Heartbeat...

[-] 129.118.26.40:443 - No Heartbeat response...

[-] 129.118.26.40:443 - Looks like there isn't leaked information...

[*] Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed
```

Appendix C: Service Scanning

Service scanning is useful for both parts of the TTU testing activities. For verification of given security requirement specifications, the results of scanning help identify relevant services to test and for penetration testing, scanning results are the starting point of vulnerability exploits. We used *nmap* (network mapper)* as our service scanner. In our testing environments, there are 73 services, 25 of which are in the original network setup without Security Fabric Framework and 48 of which are in the Security Fabric-enabled (SF-enabled) network. The table below gives a summary of service components, where the top two are those in non-SF-enabled environment and the rest (highlighted) are those in the SF-enabled environment.

Component	Number of Services
RTDMS	11
ePDC	14
SF-RTDMS	2
SF-ePDC	2
SF-ePO	15
SF-ESM	5
SF-AD	23

Table 14. Summary of Service Components in non-SF-enabled and SF-enabled environments.

The following provides detailed scanning results of each of the relevant system components mentioned above in the table.

RTDMS Server at TTU Main Campus (11 Services)

```
Starting Nmap 6.00 ( http://nmap.org ) at 2014-04-21 09:33 CDT

Nmap scan report for p3ertdms.ttu.edu (129.118.19.167)

Host is up (0.00031s latency).

Not shown: 989 filtered ports

PORT      STATE SERVICE       VERSION

80/tcp    open  http          Microsoft IIS httpd 7.5

| http-methods: Potentially risky methods: TRACE
```

* Lyon, G. F., 2009. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Nmap Project at www.nmap.org.

```
   |_See http://nmap.org/nsedoc/scripts/http-methods.html

   |_http-title: IIS7

   135/tcp   open  msrpc         Microsoft Windows RPC

   445/tcp   open  netbios-ssn

   808/tcp   open  ccproxy-http?

   1801/tcp  open  msmq?

   2103/tcp  open  msrpc         Microsoft Windows RPC

   2105/tcp  open  msrpc         Microsoft Windows RPC

   2107/tcp  open  msrpc         Microsoft Windows RPC

   3389/tcp  open  ms-wbt-server Microsoft Terminal Service

   49154/tcp open  msrpc         Microsoft Windows RPC

   49165/tcp open  msrpc         Microsoft Windows RPC

   Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port

   Device type: general purpose

   Running: Microsoft Windows 2008|Vista|7

   OS CPE: cpe:/o:microsoft:windows_server_2008::beta3
cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
cpe:/o:microsoft:windows_7

   OS details: Microsoft Windows Server 2008 Beta 3, Microsoft Windows Vista SP0 or
SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2 or Windows
Server 2008

   Network Distance: 2 hops

   Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows



   Host script results:

   | smb-security-mode:

   |   Account that was used for smb scripts: guest
```

```
|   User-level authentication

|   SMB Security: Challenge/response passwords supported

|_  Message signing disabled (dangerous, but default)

|_smbv2-enabled: Server supports SMBv2 protocol

| smb-os-discovery:

|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2
Standard 6.1)

|   NetBIOS computer name: P3ERTDMS

|   Workgroup: WORKGROUP

|_  System time: 2014-04-21 15:36:22 UTC-5



TRACEROUTE (using port 80/tcp)

HOP RTT     ADDRESS

1   2.09 ms cprt01-v162.ttu.edu (129.118.163.254)

2   0.31 ms p3ertdms.ttu.edu (129.118.19.167)



OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 96.92 seconds
```

ePDC Server at Reese Center (14 Services)

```
Starting Nmap 6.00 ( http://nmap.org ) at 2014-04-21 09:42 CDT

Nmap scan report for p3eepdc.ttu.edu (129.118.105.44)

Host is up (0.00090s latency).

Not shown: 986 filtered ports

PORT     STATE SERVICE              VERSION

80/tcp   open  http                 Microsoft IIS httpd 7.5
```

```
|_http-title: IIS7

| http-methods: Potentially risky methods: TRACE

|_See http://nmap.org/nsedoc/scripts/http-methods.html

135/tcp  open  msrpc               Microsoft Windows RPC

139/tcp  open  netbios-ssn

445/tcp  open  netbios-ssn

1027/tcp open  msrpc               Microsoft Windows RPC

1028/tcp open  msrpc               Microsoft Windows RPC

1037/tcp open  msrpc               Microsoft Windows RPC

1433/tcp open  ms-sql-s            Microsoft SQL Server 2011 11.00.2218.00

1801/tcp open  msmq?

2103/tcp open  msrpc               Microsoft Windows RPC

2105/tcp open  msrpc               Microsoft Windows RPC

2107/tcp open  msrpc               Microsoft Windows RPC

3389/tcp open  ms-wbt-server       Microsoft Terminal Service

8500/tcp open  msexchange-logcopier Microsoft Exchange 2010 log copier

Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port

Device type: general purpose

Running: Microsoft Windows 7|Vista|2008

OS CPE: cpe:/o:microsoft:windows_7::professional cpe:/o:microsoft:windows_vista::-
cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1

OS details: Microsoft Windows 7 Professional, Microsoft Windows Vista SP0 or SP1,
Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2 or Windows Server
2008

Network Distance: 3 hops

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
  Host script results:

  |_nbstat: NetBIOS name: P3EEPDC, NetBIOS user: <unknown>, NetBIOS MAC:
d4:ae:52:a6:39:3a (Dell)

  |_smbv2-enabled: Server supports SMBv2 protocol

  | smb-security-mode:

  |   Account that was used for smb scripts: guest

  |   User-level authentication

  |   SMB Security: Challenge/response passwords supported

  |_  Message signing disabled (dangerous, but default)

  | smb-os-discovery:

  |   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2
Standard 6.1)

  |   NetBIOS computer name: P3EEPDC

  |   Workgroup: WORKGROUP

  |_  System time: 2014-04-21 15:45:38 UTC-5

  | ms-sql-info:

  |   [129.118.105.44:1433]

  |     Version: Microsoft SQL Server 2011

  |       Version number: 11.00.2218.00

  |       Product: Microsoft SQL Server 2011

  |_    TCP port: 1433



  TRACEROUTE (using port 445/tcp)

  HOP RTT     ADDRESS

  1   6.36 ms cprt01-v162.ttu.edu (129.118.163.254)
```

```
   2   0.43 ms 129.118.251.123

   3   1.12 ms p3eepdc.ttu.edu (129.118.105.44)



   OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

   Nmap done: 1 IP address (1 host up) scanned in 100.52 seconds
```

SF-RTDMS at TTU side (2 Services)

```
   Starting Nmap 6.00 ( http://nmap.org ) at 2014-01-29 06:24 CST

   Nmap scan report for eewrb001.ttu.edu (129.118.26.8)

   Host is up (0.00037s latency).

   Not shown: 998 filtered ports

   PORT     STATE SERVICE       VERSION

   22/tcp   open  ssh           OpenSSH 6.0 (protocol 2.0)

   | ssh-hostkey: 1024 b5:2f:09:18:61:ba:28:d7:4f:9d:1f:3c:5d:b2:87:6d (DSA)

   |_2048 7d:ff:f9:ac:d6:03:8a:3a:9c:2b:6a:39:ee:8a:72:42 (RSA)

   3389/tcp open  ms-wbt-server Microsoft Terminal Service

   Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port

   Device type: general purpose

   Running (JUST GUESSING): Linux 3.X|2.6.X (91%)

   OS CPE: cpe:/o:linux:kernel:3 cpe:/o:linux:kernel:2.6

   Aggressive OS guesses: Linux 3.0 (91%), Linux 2.6.39 (88%), Linux 2.6.32 - 2.6.38
(88%), Linux 2.6.38 (88%), Linux 2.6.32 - 2.6.35 (88%), Linux 2.6.38 - 3.2 (85%)

   No exact OS matches for host (test conditions non-ideal).

   Network Distance: 2 hops

   Service Info: OS: Windows
```

```
   TRACEROUTE (using port 3389/tcp)

   HOP RTT      ADDRESS

   1   16.58 ms cprt01-v162.ttu.edu (129.118.163.254)

   2   0.35 ms  eewrb001.ttu.edu (129.118.26.8)



   OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

   Nmap done: 1 IP address (1 host up) scanned in 15.52 seconds
```

SF-ePDC at Reese side (2 Services)

```
   Starting Nmap 6.00 ( http://nmap.org ) at 2014-01-29 06:19 CST

   Nmap scan report for 129.118.105.50

   Host is up (0.00093s latency).

   Not shown: 998 filtered ports

   PORT     STATE SERVICE       VERSION

   22/tcp   open  ssh           OpenSSH 6.0 (protocol 2.0)

   | ssh-hostkey: 1024 c5:2d:c4:eb:89:b2:1b:a3:33:5f:e0:68:e8:8d:f4:3d (DSA)

   |_2048 b4:87:98:d2:a2:4a:d2:b2:e0:a0:c3:63:11:ab:55:30 (RSA)

   3389/tcp open  ms-wbt-server Microsoft Terminal Service

   Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port

   Device type: general purpose

   Running (JUST GUESSING): Linux 3.X|2.6.X (93%)

   OS CPE: cpe:/o:linux:kernel:3 cpe:/o:linux:kernel:2.6

   Aggressive OS guesses: Linux 3.0 (93%), Linux 2.6.39 (88%), Linux 2.6.32 - 2.6.38
(88%), Linux 2.6.38 (88%), Linux 2.6.32 - 2.6.35 (88%), Linux 2.6.38 - 3.2 (85%)

   No exact OS matches for host (test conditions non-ideal).
```

```
Network Distance: 3 hops

Service Info: OS: Windows



TRACEROUTE (using port 22/tcp)

HOP RTT     ADDRESS

1   0.16 ms cprt01-v162.ttu.edu (129.118.163.254)

2   0.41 ms 129.118.251.123

3   0.93 ms 129.118.105.50
```

SF-ePO (15 Services)

```
Starting Nmap 6.00 ( http://nmap.org ) at 2014-01-29 06:27 CST

Nmap scan report for epo-sf.epg.secfab.org (129.118.19.210)

Host is up (0.00040s latency).

Not shown: 985 closed ports

PORT      STATE SERVICE        VERSION

80/tcp    open  http           Microsoft IIS httpd 7.5

| http-methods: Potentially risky methods: TRACE

|_See http://nmap.org/nsedoc/scripts/http-methods.html

135/tcp   open  msrpc          Microsoft Windows RPC

139/tcp   open  netbios-ssn

443/tcp   open  ssl/http       Apache httpd

| ssl-cert: Subject: commonName=AH_EPO-SF/organizationName=McAfee

| Not valid before: 1970-01-01 00:00:00

|_Not valid after:  2014-01-29 06:29:01

|_http-title: 403 Forbidden

|_http-methods: No Allow or Public header in OPTIONS response (status code 403)
```

```
445/tcp   open  netbios-ssn

1433/tcp  open  ms-sql-s       Microsoft SQL Server 2008 R2 10.50.1600.00; RTM

2383/tcp  open  ms-olap4?

3389/tcp  open  ms-wbt-server?

8080/tcp  open  http           Apache httpd

|_http-title: 403 Forbidden

|_http-methods: No Allow or Public header in OPTIONS response (status code 403)

8081/tcp  open  tcpwrapped

8443/tcp  open  ssl/http       McAfee ePolicy Orchestrator http interface

|_http-title: Site doesn't have a title (text/html).

| ssl-cert: Subject: commonName=EPO-SF/organizationName=McAfee

| Not valid before: 1970-01-01 00:00:00

|_Not valid after:  2014-01-29 06:29:01

| http-methods: Potentially risky methods: PUT DELETE

|_See http://nmap.org/nsedoc/scripts/http-methods.html

49152/tcp open  msrpc          Microsoft Windows RPC

49153/tcp open  msrpc          Microsoft Windows RPC

49154/tcp open  msrpc          Microsoft Windows RPC

49155/tcp open  msrpc          Microsoft Windows RPC

Device type: general purpose

Running: Microsoft Windows 2008|7

OS CPE: cpe:/o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:windows_7

OS details: Microsoft Windows Server 2008 SP2, Microsoft Windows 7 or Windows
Server 2008 SP1

Network Distance: 2 hops

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
  Host script results:

  |_nbstat: NetBIOS name: EPO-SF, NetBIOS user: <unknown>, NetBIOS MAC:
00:50:56:94:70:69 (VMware)

  | smb-security-mode:

  |   Account that was used for smb scripts: guest

  |   User-level authentication

  |   SMB Security: Challenge/response passwords supported

  |_  Message signing disabled (dangerous, but default)

  |_smbv2-enabled: Server supports SMBv2 protocol

  | smb-os-discovery:

  |   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2
Standard 6.1)

  |   NetBIOS computer name: EPO-SF

  |   Workgroup: EPG

  |_  System time: 2014-01-29 12:29:50 UTC-6

  | ms-sql-info:

  |   [129.118.19.210:1433]

  |     Version: Microsoft SQL Server 2008 R2 RTM

  |       Version number: 10.50.1600.00

  |       Product: Microsoft SQL Server 2008 R2

  |       Service pack level: RTM

  |       Post-SP patches applied: No

  |_    TCP port: 1433



  TRACEROUTE (using port 5900/tcp)

  HOP RTT      ADDRESS
```

```
   1   14.29 ms cprt01-v162.ttu.edu (129.118.163.254)

   2   0.94 ms  epo-sf.epg.secfab.org (129.118.19.210)

   OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

   Nmap done: 1 IP address (1 host up) scanned in 74.41 seconds
```

SF-ESM (5 Services)

```
   Starting Nmap 6.00 ( http://nmap.org ) at 2014-01-29 06:35 CST

   Nmap scan report for 129.118.26.40

   Host is up (0.00049s latency).

   Not shown: 995 filtered ports

   PORT     STATE  SERVICE        VERSION

   22/tcp   open   ssh            (protocol 2.0)

   |_ssh-hostkey: 2048 d0:11:53:36:4b:b0:91:00:b9:7d:4f:d3:5a:f8:2c:bf (RSA)

   23/tcp   open   ssh            libssh 0.5.2 (protocol 2.0)

   |_ssh-hostkey: 2048 44:de:b2:ba:46:e3:10:48:43:e2:8f:34:4f:06:4e:26 (RSA)

   80/tcp   open   http           Apache httpd

   | http-title: 302 Found

   |_Did not follow redirect to https://129.118.26.40/

   |_http-methods: No Allow or Public header in OPTIONS response (status code 302)

   443/tcp  open   ssl/http       Apache httpd

   | ssl-cert: Subject:
commonName=esm.mcafee.local/organizationName=McAfee/stateOrProvinceName=TX/countryName
=US

   | Not valid before: 2013-05-15 04:11:47

   |_Not valid after:  2023-05-15 04:11:47

   | http-robots.txt: 1 disallowed entry

   |_/
```

```
   |_sslv2: server supports SSLv2 protocol, but no SSLv2 cyphers

   |_http-title: McAfee Enterprise Security Manager

   4242/tcp closed vrml-multi-use

   1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-
submit.cgi :

   SF-Port22-TCP:V=6.00%I=7%D=1/29%Time=52E8F5B2%P=i686-pc-linux-gnu%r(NULL,1

   SF:2,"SSH-2\.0-SSH_FIPS\r\n");

   Device type: WAP|media device|webcam|specialized|general purpose|storage-
misc|broadband router

   Running (JUST GUESSING): Netgear embedded (94%), Western Digital embedded (94%),
AXIS Linux 2.6.X (93%), Crestron 2-Series (91%), Linux 2.6.X|2.4.X (90%), Thecus
embedded (89%), Linksys Linux 2.4.X (89%)

   OS CPE: cpe:/o:axis:linux:2.6 cpe:/o:crestron:2_series cpe:/o:linux:kernel:2.6.32
cpe:/o:linux:kernel:2.6.22 cpe:/o:linux:kernel:2.4 cpe:/o:linksys:linux:2.4
cpe:/o:linux:kernel:2.6

   Aggressive OS guesses: Netgear DG834G WAP or Western Digital WD TV media player
(94%), AXIS 210A or 211 Network Camera (Linux 2.6) (93%), Crestron XPanel control
system (91%), Linux 2.6.32 (90%), Linux 2.6.31 (90%), OpenWrt Kamikaze 7.09 (Linux
2.6.22) (89%), OpenWrt Kamikaze 8.09 (Linux 2.4.35.4) (89%), Linux 2.6.26 (89%),
OpenWrt Kamikaze 8.09 (Linux 2.6.26) (89%), Thecus 4200 or N5500 NAS device (Linux
2.6.33) (89%)

   No exact OS matches for host (test conditions non-ideal).

   Network Distance: 2 hops



   TRACEROUTE (using port 4242/tcp)

   HOP RTT     ADDRESS

   1   0.16 ms cprt01-v162.ttu.edu (129.118.163.254)

   2   0.46 ms 129.118.26.40



   OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
```

```
   Nmap done: 1 IP address (1 host up) scanned in 39.82 seconds
```

SF-AD (23 Services)

```
   Starting Nmap 6.00 ( http://nmap.org ) at 2014-01-29 06:44 CST

   Nmap scan report for dc-sf.epg.secfab.org (129.118.26.37)

   Host is up (0.00032s latency).

   Not shown: 977 closed ports

   PORT     STATE SERVICE       VERSION

   53/tcp   open  domain        Microsoft DNS 6.1.7601

   | dns-nsid:

   |_  bind.version: Microsoft DNS 6.1.7601 (1DB14556)

   88/tcp   open  Kerberos-sec  Windows 2003 Kerberos (server time: 2014-01-29
18:45:31Z)

   135/tcp  open  msrpc         Microsoft Windows RPC

   139/tcp  open  netbios-ssn

   389/tcp  open  ldap

   445/tcp  open  netbios-ssn

   464/tcp  open  kpasswd5?

   593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0

   636/tcp  open  ssl/ldap

   | ssl-cert: Subject: commonName=DC-SF.EPG.SECFAB.ORG

   | Not valid before: 2014-01-11 15:44:59

   |_Not valid after:  2014-02-10 23:29:17

   |_sslv2: server still supports SSLv2

   1025/tcp open  msrpc         Microsoft Windows RPC

   1026/tcp open  msrpc         Microsoft Windows RPC

   1028/tcp open  msrpc         Microsoft Windows RPC
```

```
   1029/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0

   1030/tcp open  msrpc         Microsoft Windows RPC

   1031/tcp open  msrpc         Microsoft Windows RPC

   1040/tcp open  msrpc         Microsoft Windows RPC

   1042/tcp open  msrpc         Microsoft Windows RPC

   1043/tcp open  msrpc         Microsoft Windows RPC

   1051/tcp open  msrpc         Microsoft Windows RPC

   3268/tcp open  ldap

   3269/tcp open  ssl/ldap

   |_sslv2: server still supports SSLv2

   | ssl-cert: Subject: commonName=DC-SF.EPG.SECFAB.ORG

   | Not valid before: 2014-01-11 15:44:59

   |_Not valid after:  2014-02-10 23:29:17

   3389/tcp open  ms-wbt-server Microsoft Terminal Service

   8081/tcp open  tcpwrapped

   No exact OS matches for host (If you know what OS is running on it, see
http://nmap.org/submit/ ).

   TCP/IP fingerprint:

   OS:SCAN(V=6.00%E=4%D=1/29%OT=53%CT=1%CU=31931%PV=N%DS=2%DC=T%G=Y%TM=52E8F7F

   OS:9%P=i686-pc-linux-gnu)SEQ(SP=FC%GCD=2%ISR=10B%TI=I%CI=I%II=I%SS=S%TS=7)O

   OS:PS(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW8ST11%O5=M5B4N

   OS:W8ST11%O6=M5B4ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)E

   OS:CN(R=Y%DF=Y%T=81%W=2000%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=81%S=O%A=S+%F

   OS:=AS%RD=0%Q=)T2(R=Y%DF=Y%T=81%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=8

   OS:1%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=81%W=0%S=A%A=O%F=R%O=%RD=0%Q

   OS:=)T5(R=Y%DF=Y%T=81%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=81%W=0%S=A
```

```
   OS:%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=81%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y

   OS:%DF=N%T=81%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T

   OS:=81%CD=Z)



   Network Distance: 2 hops

   Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows



   Host script results:

   |_nbstat: NetBIOS name: DC-SF, NetBIOS user: <unknown>, NetBIOS MAC:
00:50:56:94:6f:1b (VMware)

   | smb-security-mode:

   |   Account that was used for smb scripts: guest

   |   User-level authentication

   |   SMB Security: Challenge/response passwords supported

   |_  Message signing required

   |_smbv2-enabled: Server supports SMBv2 protocol

   | smb-os-discovery:

   |   OS: Windows Server 2008 R2 Enterprise 7601 Service Pack 1 (Windows Server 2008
R2 Enterprise 6.1)

   |   NetBIOS computer name: DC-SF

   |   Workgroup: EPG

   |_  System time: 2014-01-29 12:46:29 UTC-6



   TRACEROUTE (using port 993/tcp)

   HOP RTT     ADDRESS

   1   0.15 ms cprt01-v162.ttu.edu (129.118.163.254)
```

```
   2   0.29 ms dc-sf.epg.secfab.org (129.118.26.37)



   OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

   Nmap done: 1 IP address (1 host up) scanned in 75.03 seconds
```