2016 Fall Workshop

Download Materials and Submit Questions @
SPP.org -> Regional Entity -> 2016 Fall Workshop:

Online question box submits generates anonymous email to staff from info@spp.org

You can also email questions/comments to reworkshop@spp.org
2016 Fall Workshop

Tuesday, September 20

8:00-8:20  Welcome and Intro Remarks  
           Emily Pennel, SPP RE  
           Mark Maher, SPP RE Trustee

8:20-9:20  1 - Synchrophasors in SPP  
           Jay Caspary, SPP & Austin White, OGE

9:20-9:30  BREAK

9:30-10:20  2 - Never Underestimate the Power of the E-Side:  
           E-Learning the Applied Fiction Way  
           Chris Lazarro & Charlie Evans, MetaMythic

10:20-10:40  NETWORKING BREAK

10:40-11:30  3 - Cleco’s Local Internal Control Evaluation Strategy  
             Betty Deans, Cleco

11:30-Noon  4 - AEP’s Five-Year Compliance Strategy  
             Mike Deloach, AEP

12:00-1:00  LUNCH

1:00-1:40  5 - NERC’s State of Reliability Report  
           Mike Hughes, SPP RE

1:40-2:10  6 - O&P Audit Success and Lessons Learned  
           Matt Caves, Western Farmers

2:10-2:20  BREAK

2:20-3:30  7 - TOP-001-3, TOP-002-4, TOP-003-3  
           Mike Hughes, SPP RE  
           Allen Klassen, Westar

3:30-4:00  NETWORKING BREAK

4:00-5:00  8 - CIP Update  
           Shon Austin, SPP RE

5:30-7:00  NETWORKING RECEPTION
The workshop is followed by the RTO Compliance Forum for members and Registered Entities, which requires separate registration.
Synchrophasors at

Austin White P.E.
Oklahoma Gas & Electric Company
SPP RE Workshop 2016
Outline

• OG&E Background
• Synchrophasor Applications
• Example Events
• Synchrophasor Based Protection
• Renewables Integration
PMU Deployment 2008-2016

PMUs Online

PMU Locations
PMU Coverage Stats

• 100% of EHV System
  • 83 Line Terminals, 19 Autotransformers
• 100% of Wind Farms
  • 4053MW, 23 Plants
• 90% of Fossil Generation
  • 6200MW, 17 Units
• 37% of HV System
  • 221 Line Terminals

363 PMUs Total
Large Deployment Challenges

• Protocols – C37.118 limited to ~150 PMUs, no security, frame based
• Performance – PDC limits are CPU burden starting at ~300 PMUs
• Data Storage – 350 PMUs, positive sequence need 15GB/day comp, 50GB uncompressed
• Network Bandwidth – Circuit needs 64kbps per PMU, no data caps, low latency
Synchrophasor Applications

- Situational Awareness
- Disturbance/Misoperation Analysis
- State Estimator Enhancement and LSE
- Voltage Recovery Assessment (reactive reserves, FIDVR)
- Proactively Find Equipment Problems
- Stability Assessment
- Renewables Integration/Monitoring
Situational Awareness
Disturbance/Fault Location

Voltage Magnitude

Current Magnitude
Fault Visibility

• 0.7 Second, 12.5kV Distribution Fault

(69 KV 3 Miles Away)
Delta Volts 2.1%

(138 KV 8 Miles Away)
Delta Volts 0.7%

(345 KV 65 Miles Away)
Delta Volts 0.06%

(345 KV 140 Miles Away)
Delta Volts 0.02%

(1 second) (1 minute)
Long Duration Fault Events

- EM Relay failed to detect a permanent ground fault (problem with polarizing CT circuit)
- Took 19 breakers to remotely clear fault.
- Finally cleared when the fault went phase to phase
- 32,000 Customers effected
- 2hr 17min restore time
- 4.38 Million CMI
- Continuous recording needed!

Voltage Magnitude

(16 seconds)
Failed EHV Reclosing Attempt

- Observed an unusual reclosing event following a fault on a 345kV line
- Able to diagnose multiple reclose attempts when only one reclose was expected
- Recent construction work changed the configuration
- Found that relay settings were not properly updated
Discovery of Failing Equipment

- Discovered many loose connections in the potential circuits at fuses or terminal blocks
- This has caused misoperations in the past (relays get confused)
- Proactively finding these helps prevent future outages and misoperations
PT Problem Report

• Our daily PT Problem report performs a dV/dT to help identify abnormal voltage fluctuations

Failing analog input
Stability Assessment - FFT

• FFT algorithm used to detect oscillations in real time
• Sends email or text message when the oscillations reach an objectionable level
• This PMU shows a sustained oscillation at 3Hz
Stability Assessment - Redbud Oscillations

• Discovered voltage oscillations on EHV system (0.2Hz)
• Signal is most pronounced on the MVAR plot
• Suspected a generation problem
• Determined to be a problem with Redbud Unit 4 when in VAR control mode
• VAR control mode used during unit startup, oscillations stop when operator switches to voltage control scheme
Wind Farm Oscillations

- Only during high winds
- FFT analysis shows 13-14Hz
- Voltage fluctuations as high as 5%
- Interaction between wind farms?
- Switching performed to electrically isolate the wind farms
- Determined it was a problem at different wind farms with the same turbine model
- The only solution was to curtail output
Customer Impact

- Using IEEE 141, the oscillations were well into the objectionable flicker zone
- Called the Woodward service center to ask if they could see the lights flickering
- They confirmed visible flicker and noted numerous customer complaints
- We successfully worked with the manufacturer to resolve the issue
Sensitivity to System Changes

- One line was out of service for maintenance
- Fault on another line started the oscillations
- Had to curtail output to stop oscillations
- Shows wind farm sensitivity to system impedance changes
Monitoring Power Quality

- It has been observed that large loads inject noise onto the system.
- Large refineries and arc furnaces are the worst offenders.
- Synchrophasors allow for real time power quality monitoring.
PMU Assisted Tripping

- 69kV loop around Ardmore, OK
- Sensitive Industrial customers
- No traditional carrier/fiber tripping (0.5 sec step distance)
- Network available
- New relays available
- Why not use synchrophasors to speed up tripping 5x?
PMU Assisted Tripping

PTP Network Tunnel

POTT Scheme utilizing dual PMU server/client channels to transmit and receive KEY

Transmission Line
No Traditional Comm Channel (carrier, fiber)
Wind Resources in SPP
OG&E Wind Penetration > 4000MW

• SPP record peak of 45% and 10,783MW on 3/21/2016
• 60° angle spread across OG&E from west to east
Oklahoma Ranks #7 in Solar Potential
Utility Scale Solar 2.5MW Pilot at Mustang
Comparing Days (Synchrophasor Data)

June 27 (Highest)  | July 6 (Cloudy)  | June 17 (Lowest)
Output With Cloud Coverage

KW

10 AM 11 AM 12 PM 1 PM 2 PM 3 PM 4 PM 5 PM 6 PM

Partly Cloudy Clear Sky Rainy

OG&E
Questions?

• Thanks! Feel free to contact me if you have any questions.
  – Austin White
  • whitead@oge.com (405-553-5996)
OG&E’s PhasorView
SEVENTY-FIVE YEARS OF RELIABILITY THROUGH RELATIONSHIPS
Synchrophasors at SPP

2016 Fall RE Workshop

September 20, 2016
What are Synchrophasors?

• Synchrophasors are time-synchronized measurements of both the magnitude and phase angle of voltage and current on the grid.

• They are measured by devices called Phasor Measurement Units (PMUs) that record samples 30 to 60 times a second. These devices also measure system frequency.

• PMU measurements record grid conditions with great accuracy and offer insight into grid stability or stress. Synchrophasor technology is used for real-time operations and off-line engineering analyses to improve grid reliability and efficiency and lower operating costs.
Why Synchrophasors?

- Measurement of system variables was on the order of seconds (SCADA)
- Samples of variables at different locations did not occur at the same time
- Voltage, Power, and Reactive Power normally don’t change abruptly, unless a large disturbance occurs nearby
- System monitoring is critical during disturbances
- Faster synchronized data needed to capture system dynamics
- Fast real time control is possible only with real time situational awareness

Source: EIA, 2012
# Older vs Newer Way

<table>
<thead>
<tr>
<th>SCADA data</th>
<th>Phasor data (PMU)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh rate 2-5 seconds</td>
<td>Refresh rate 30-60 samples/sec</td>
</tr>
<tr>
<td>Latency and skew</td>
<td>Time tagged data, minimal latency</td>
</tr>
<tr>
<td>‘Older’ legacy communication</td>
<td>Compatible with modern communication technology</td>
</tr>
<tr>
<td>Responds to quasi-static behavior</td>
<td>Responds to system dynamic behavior</td>
</tr>
</tbody>
</table>

**Freq change means:**
- Sudden Gen-Load MW imbalance somewhere in the grid

**Angle-pair change means:**
- Sudden MW change in a specific location of the grid

**X-ray**

**MRI**

---

**Radical Change in Grid Monitoring Paradigm**

Source: NASPI, EIPP
The Real Value of Synchrophasor Data

- Through synchrophasor data, we can gain unprecedented knowledge and understanding into power system behavior.
- As these understandings occur, the aha! moments multiply, i.e. connectedness.
- SPP’s grid can be operated and enhanced at levels of efficiency and reliability not seen before.
Example of Recent Research

• **3 Year EPRI/Baylor Pilot Project**
  - Installed Phasor Measurement Units (PMUs) at Gentlemen and Cooper Stations in NPPD, 2 distribution substations in Kansas City MO by KCPL, Garden City KS in Sunflower and SPP Offices
  - OG&E sharing PMU data in western OK, OKC and western AR
  - EMDE recently installed a PMU in Joplin area
  - WAPA is working to share DOE-funded synchrophasor data from equipment installed in Bismarck ND; Dawson County, MT; Ft Thompson, SD; and Sioux City IA
  - Xcel Energy/SPS adding 4 data streams soon from Finney, Harrington, Roosevelt and Yoakum substations in KS, TX and NM.
  - Baylor researchers collecting/mining data and providing reports of events for calibration efforts
  - Tools and data at Baylor are now available for SPP Staff to access.
Synchrophasor Strike Team

• The Synchrophasor Strike Team has been formed to help in the development of:
  • Member use cases
  • Member roadmap for PMU deployments
  • Requirements and criteria for sending PMU data to SPP
  • Reviewing SPP roadmap for Synchrophasor applications

• Strike Team members and others from the industry are sharing their knowledge and experiences with PMU technology and applications
Strike Team – Key Questions

- How will Synchrophasor data be used in SPP (real-time monitoring, wide-area situational awareness, model validation, etc.) and shared among members?
- What are current and planned uses by members?
- What are the best locations for PMU equipment and priorities of installations?
- What are the data latency and quality requirements and other specifications?
- Who should install and own the PMUs?
- Who is responsible for communications from the PMUs and PDCs?
2016 Goals & Accomplishments

• Accomplishments
  • Evaluate software vendors and purchase PMU Starter Package
  • Evaluate Network Capabilities
  • Receive Existing PMU Data from Members
  • Identify Primary Use Cases
  • Synchrophasor Strike Team Formed

• Next Steps
  • Further Research and Develop Primary Use Cases
  • Deploy PMU Starter Package in Development
  • Determine Baseline and Alarm Thresholds
  • Data Quality Processes

• On Going
  • SPP Road Map Development
  • Revision Request for Generation Interconnection Agreement
  • Setting up new data feeds
  • Analyze data quality
  • Event Knowledge Base
Use Cases Under Review

- **Real-Time Analysis**
  - Wide Area Situational Awareness
  - Oscillation Detection and Monitoring
  - Voltage Stability

- **Offline Analysis**
  - Model Validation
  - Post-Event Analysis
  - NERC Reliability Standards
  - Operator Training

- **System Integration**
  - EMS State Estimator
  - Macomber Map
  - TSAT/VSAT
  - Sharing Data and Displays with members

- **Other Activities**
  - Data Quality
  - PMU Registration
  - PMU Placement
Dates are for discussion purposes only and meant to highlight simultaneous research and development activities.

<table>
<thead>
<tr>
<th>PMU High Level Gantt Chart</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2016</strong></td>
</tr>
<tr>
<td>PMU Starter Package</td>
</tr>
<tr>
<td>Member Activities</td>
</tr>
<tr>
<td>openECA Testing (DOE Project)</td>
</tr>
<tr>
<td>Data Streaming from External Parties</td>
</tr>
<tr>
<td>Data Quality</td>
</tr>
<tr>
<td>Wide Area Situational Awareness</td>
</tr>
<tr>
<td>Voltage Stability Monitoring</td>
</tr>
<tr>
<td>Oscillation Detection and Monitoring</td>
</tr>
<tr>
<td>Post-Event Analysis</td>
</tr>
<tr>
<td>Planning Model Validation</td>
</tr>
</tbody>
</table>

**PENDING PROJECT WORK**

| Member Portal | Analysis | Design | Procure | Install | Production |
| HIGHLY AVAILABLE ARCHITECTURE | Analysis | Testing | Implementation* | Production |
| MOVE TO ESP, EMS INTEGRATION AND CIP CONTROLS | Analysis | Implementation* | Production |

*Implementation includes Development of Processes and Training
Oct 11th AM MOPC Workshop
Draft Agenda

• Intro to SPP PMU Project (15 mins)
  • Presented by Philip Bruich

• Understanding Synchrophasor Technology (45 mins)
  • Presented by Doug Bowman, SPP

• Industry Background (45 mins)
  • Presented by Alison Silverstein, NASPI
  • Possible Topics: Starter Kit, PMU Placement\Costs\Communications, Value Proposition

• SPP Use Case Walkthrough (30 mins)
  • Presented by Cody Parker, SPP

• Synchrophasor Strike Team Overview (15 mins)
  • Presented by Jay Caspary, SPP

• Member Use Case Walkthrough (30 mins)
  • Presented by SST Member(s)

• Roadmap, Timelines and Deliverables (15 mins)
  • Presented by Cody Parker and Philip Bruich, SPP
Cleco’s Local Internal Control Evaluation Strategy
About Betty …

Career Path
- KPMG
- Northwestern State University
- Cleco
  - Senior Auditor
  - NERC Compliance & Audit Analyst

Education & Credentials
- Northwestern State University
  - B.S. – Accounting
  - Minor – Business Administration
- CPA, CIA, CCEP, and CITP
About Cleco …

- Regulated utility headquartered in Pineville, Louisiana
- Approximately 1,200 employees serving approximately 286,000 customers
- Registered with NERC as a BA, DP, GO, GOP, RP, TO, TOP, and TP
  - MISO performs certain coordinated BA, RP and TP functions on Cleco’s behalf
About Cleco …

Departmental Reporting Structure

Chief Compliance Officer & General Counsel

NERC Compliance & Training

NERC

FERC

FRCC  MRO  NPCC  RFC  SERC  TRE  WECC

CLECO
Course Objectives

✓ Review Cleco’s local Internal Control Evaluation (ICE) strategy
✓ Review Cleco’s local ICE framework
✓ Share documents developed
✓ Discuss ICE outcome for PRC-005
  - It’s impact on SPP RE audit
  - Lesson(s) learned
Cleco’s Local ICE Strategy

- Seek benefits from having an ICE by Regional Entity
- Bring an *Internal Control SME* into the department
- Develop and implement internal controls
- Request ICE by SPP RE as internal controls are developed and implemented (by NERC Standard)
Cleco’s Local ICE Strategy
Goal: Reap ICE Benefits

✓ Possible reduction in RAT-STATS sampling
✓ Possible shift from audit to self-certification
✓ Scalable (pick/choose requirements)
✓ Not an audit (non-binding recommendations)
✓ Internal control consultation
Cleco’s Local ICE Strategy

Risk-Based Compliance Oversight Framework

- Risk based “right-sized” audits by Regional Entities
- No more one-size-fits-all audits (Actively Monitored Lists)
Cleco’s Local ICE Framework

- **Risk Assessment**
  - Prioritize review of controls by NERC Standard

- **Compilation**
  - Identify, recommend, and compile controls

- **Evaluation**
  - Test the design and effectiveness of controls

- **Rating Assessment**
  - Translate test results into a logical, consistent format

- **Reporting**
  - Feedback to stakeholders

- **Follow-up**
  - Corrective action, if any
# Cleco’s Internal ICE Process

## ICE Framework Document Share

### Policy

<table>
<thead>
<tr>
<th><strong>Policy</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong>: Provides direction, guidance, and consistency</td>
</tr>
</tbody>
</table>

### Procedure

<table>
<thead>
<tr>
<th><strong>Procedure</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong>: Provides direction, guidance, and consistency</td>
</tr>
</tbody>
</table>

---

**Cleco’s Local ICE Framework – Policy and Procedure**

---

### NERC Compliance and Training

#### Policy

**Purpose:** This policy provides the framework for documenting and assessing internal controls already in place, recommending opportunities for improving internal controls, and conducting Internal Control Evaluations (ICE) for selected NERC standards.

**Policy:** The intent of this policy, and any associated procedures, is to provide direction, guidance, and consistency in the identification, recommendation, and evaluation of internal controls established for the mitigation of risks associated with System (IES) and compliance with NERC Standards.

**Risk Assessment**

Through formal or informal procedures, NERC Compliance and Training will prioritize the review of internal controls. Consideration will be given to the likelihood of non-compliance with NERC Standards and the impact of non-compliance, changes in the requirements of NERC Standards, and areas of non-compliance at the regional level, upon associated systems and controls.

**Identification / Compilation of Internal Controls**

Based on the formal or informal risk assessment, it will be determined which areas of work in which the review of internal controls will occur. This review will include the identification, evaluation, and recommendation (as deemed necessary) of internal controls associated with the NERC Standard. NACAT shall obtain an understanding of the internal controls in place, and where deemed appropriate, recommend opportunities to strengthen internal controls.

The controls shall be summarized utilizing the Internal Control Evaluation Template (Control Summary Worksheet).

**Evaluation of Internal Controls**

Cleco’s ICE program was established as a means of assessing the adequacy of the Company's NERC-related internal controls, identifying opportunities for better managing or mitigating risks, and providing a tool for external entities to better understand the controls in place at Cleco. NACAT shall perform evaluation of internal controls utilizing the Internal Control Evaluation Template. Similarly, NACAT shall make both an overall and a NERC requirement assessment of internal controls utilizing various worksheets in the Status of Controls Template.

**Reporting Requirements**

NACAT shall document the results of the overall assessment and evaluation of internal controls utilizing the Internal Control Evaluation report template. The ICE report shall be distributed in a manner deemed appropriate by the Manager – NERC Compliance and Training.

The Internal Controls Summary Template (an abbreviated version of the Control Summary worksheet), and subsequent updates, should be distributed to personnel deemed appropriate by the Manager – NERC Compliance and Training.

---

### NERC Compliance and Training

#### Procedure

**Purpose:** The purpose of this procedure is to provide guidance and consistency in the documentation and assessment of internal controls, and the preparation of Internal Control Evaluations for selected NERC Standards.

**Procedure:** NERC Compliance and Training (NACAT) should give consideration to each of the items noted below to facilitate direction and consistency in the identification, recommendation, and evaluation of internal controls, and the completion of Internal Control Evaluations.

- **Understanding of the NERC Standard**: Providing an understanding of the requirements of the NERC Standard.
- **Observing Activities of Subject Matter Experts (SME)**, other operating personnel (e.g., responsible NERC personnel), and other individuals necessary to perform the Evaluation.

**Compiled Internal Controls**

As controls are identified, NACAT should associate the control with the specific NERC Standard requirement and assign a reference number to the control. Controls should be documented on the Internal Control Evaluation spreadsheet, using the Control Summary Worksheet. All columns on the Control Summary worksheet should be completed, however, all pertinent data may not be initially available. For example, SME and responsible NACAT personnel should be consulted when determining if a control is considered a risk.

In addition, if the Evaluation of Controls worksheet identifies a control that is required but not in place, NACAT should document in the System Owner Assessment if the control is required and the reason for not having the control in place.

**Evaluation of Controls**

The Evaluation of Controls worksheet, which is located on the Internal Control Evaluation spreadsheet, should be used to evaluate each control. Based on NACAT’s understanding of each control, NACAT designs tests that are sufficient in nature to evaluate the control (e.g., design, effectiveness, etc.). Tests may include, but are not limited to, the following:

- Verification of records (e.g., report contents, application screen shots, system output, log files, etc.)
- Observations and/or walkthroughs
- Interviews to appropriate personnel
- Verification of (e.g., supervisory review, appropriate access levels, etc.)
Cleco’s Local ICE Framework

Risk Assessment
Cleco’s Local ICE Framework
Risk Assessment

✓ Used to prioritize the review of internal controls by NERC Standard

✓ Helps manage the risk of non-compliance with NERC Standards

✓ Process may be formal or informal (depends on needs of the Registered Entity and its available resources)
Cleco’s Local ICE Framework
Risk Assessment Considerations …

✓ Prior audit’s potential violations
✓ Self-reported potential violations
✓ New and/or major Standard revisions
✓ Confidential SPP RE documents
  ▪ SPP RE Inherent Risk Assessment Summary report (entity-specific; marked private and confidential)
  ▪ SPP RE Internal Controls Evaluation Summary report (entity-specific; marked private and confidential)
Cleco’s Local ICE Framework
Risk Assessment Considerations …

✓ Widely Available SPP RE documents
  - SPP RE 10 Most Violated Standards
  - SPP RE 2016 Monitoring Scope Plan
Cleco’s Local ICE Framework

Risk Assessment Document Share

Content and formality depend on the Registered Entity’s needs

Cleco’s Local ICE Framework – Risk Assessment
Compilation
Cleco’s Local ICE Framework
Compilation Basics: Internal Control defined

✓ A process
✓ Effected by people
✓ Designed to provide reasonable assurance
✓ Regarding the achievement of objectives
  - Operations
  - Reporting
  - Compliance
Internal Controls provide reasonable assurance that ...

Objectives will be met !!!
Cleco’s Local ICE Framework
Compilation Basics: Reasonable Assurance

COSO Framework (Internal Control Components) and NERC Reliability Standards

Adequate internal controls lead to reasonable assurance of compliance with NERC Standards

Cleco’s Local ICE Framework – Compilation Basics
SPP Report’s Opinion

<table>
<thead>
<tr>
<th>No findings of non-compliance</th>
<th>≠</th>
<th>Being in compliance</th>
</tr>
</thead>
</table>
Initially ...

✓ Determine how controls are catalogued (database, spreadsheet, etc.)

✓ If controls are not catalogued, identifying controls will take longer

✓ How much longer?
Cleco’s Local ICE Framework

 Compilation

It depends on the entity’s prior emphasis regarding internal controls
Cleco’s Local ICE Framework
Compilation

By Standard ...

✓ Review and obtain understanding of the Standard’s requirements

✓ Request list of documented controls (may or may not exist) and SMEs
Cleco’s Local ICE Framework
Compilation

By Standard …

✓ Inquire and observe compliance related activities
   (may disclose undocumented controls)

✓ Review applicable operating plans, policies, and procedures
   (may disclose non-catalogued controls)
Cleco’s Local ICE Framework
Compilation

By Standard ...

✓ Consider IT systems and associated internal controls directly related to Standard (general and application)

✓ Recommend controls, as needed
Cleco’s Local ICE Framework
Compilation

By Standard …

- Link each control to a specific NERC requirement
- Categorize controls as key or not
By Standard ...

- Verify expressed instances of requirements not being applicable (could actually be applicable)

- Prior to testing, verify accuracy of new controls (verbiage and frequency)
Cleco's Local ICE Framework
Compilation Document Share

- Control Number
- Key Control (or not)
- Control Type
- Description of Control
- Frequency
- Performed By
- COSO Component
- RSAW information

If controls are documented elsewhere, Entity may wish to customize this tab, (e.g., revise columns or omit in its entirety)
The familiarity of stakeholders with control types dictates whether or not this tab is needed.

### Control Types

<table>
<thead>
<tr>
<th>Control Type</th>
<th>Description of Control Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preventative</td>
<td>A preventative internal control is designed to discourage non-compliance with the Reliability Standards. They are proactive internal controls that help ensure the management objective of a tracking tool that notifies management that a noncompliance and return an advisory to a Voltage Regulator (AVR) status indicator in a Control Center indicating an AVR status monitoring unit, thus providing notification to the required by Reliability Standard VAR-002.</td>
</tr>
<tr>
<td>Detective</td>
<td></td>
</tr>
<tr>
<td>Corrective</td>
<td></td>
</tr>
<tr>
<td>Preventative, Detective</td>
<td></td>
</tr>
<tr>
<td>Preventative, Corrective</td>
<td></td>
</tr>
<tr>
<td>Preventative, Detective, Corrective</td>
<td></td>
</tr>
<tr>
<td>Detective, Corrective</td>
<td>See above for individual descriptions of control types</td>
</tr>
<tr>
<td>N/A</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>
The familiarity of stakeholders with the COSO framework dictates whether or not this tab is needed.
Cleco’s Local ICE Framework

Evaluation
Cleco’s Local ICE Framework
Evaluation

✓ Determine expected documentation for compliance with control

✓ Design tests to evaluate compliance with control
  - Review records
  - Observe compliance actions
  - Make inquiries of appropriate personnel
  - Verify performance (e.g., supervisory reviews, appropriate access levels, etc.)
  - Compare validating documentation
Cleco’s Local ICE Framework – Evaluation

✔ Perform test(s) and document results

✔ Based on tests performed, evaluate test results
  ▪ Control performed as expected (or not)
  ▪ Adequacy of control’s design
  ▪ Effectiveness of control

✔ Document evidence reviewed
  ▪ Should form the basis of evaluation
Cleco’s Local ICE Framework – Evaluation Document Share

<table>
<thead>
<tr>
<th>Control Number</th>
<th>Key Control</th>
<th>Control Type</th>
<th>Description of Control</th>
<th>Frequency</th>
<th>Performed By</th>
<th>Expected Documentation</th>
<th>Test(s) To Be Performed</th>
<th>Results of Test(s) Performed</th>
<th>Evaluation of Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRC-005.2.R1</td>
<td>Yes</td>
<td>Key</td>
<td>Description of control</td>
<td></td>
<td>Employee’s Name</td>
<td>Describe expected documentation</td>
<td>1. Describe test 2. Describe test</td>
<td>Based on the test results, evaluate this control</td>
<td>Performing as expected</td>
</tr>
<tr>
<td>PRC-005.2.R1-A</td>
<td>No</td>
<td>No</td>
<td>Description of control</td>
<td></td>
<td>Employee’s Name</td>
<td>Describe expected documentation</td>
<td>1. Describe test 2. Describe test</td>
<td>Based on the test results, evaluate this control</td>
<td>Not implemented as designed</td>
</tr>
</tbody>
</table>

- Control Description
- Frequency
- Performed By
- Expected Documentation
- Test(s) To Be Performed
- Results of Test(s) Performed

Evaluation of Control
- Performing as expected
- Not implemented as designed
- Not functioning as expected
Include evidence of documentation reviewed

- Test results go here.
- State whether the control is functioning as intended.
- Note any exceptions.

Compliance

Cleco’s Local ICE Framework – Evaluation (Evidence Reviewed tabs)
“An effective program has individual internal controls that prevent, detect, or correct non-compliance with Reliability Standards. Though individual internal controls may fail, a well-designed internal control program can sustain failures and continue to operate effectively by properly aligning preventative, detective, and corrective controls and promoting a culture of compliance.”

NERC’s ERO Enterprise Internal Control Evaluation Guide (October 2014)
Reasonable Assurance

Internal controls provide "reasonable assurance" -- but not absolute assurance -- regarding the achievement of objectives.
## Cleco’s Local ICE Framework – Rating Assessment

### Assessment of Controls Matrix

<table>
<thead>
<tr>
<th>Rating Assessed</th>
<th>Percentage Range</th>
<th>Description of Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>By NERC Requirement</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Most Likely</td>
<td>90.0% - 99.9%</td>
<td>Compliance with this NERC requirement is most likely to occur.</td>
</tr>
<tr>
<td>Probable</td>
<td>70.0% - 89.9%</td>
<td>Compliance with this NERC requirement is more likely than not to occur.</td>
</tr>
<tr>
<td>Possible</td>
<td>40.0% - 69.9%</td>
<td>Compliance with this NERC requirement is more than remote but less than probable to occur.</td>
</tr>
<tr>
<td>Remote</td>
<td>1.0% - 39.9%</td>
<td>Compliance with this NERC requirement has a slight chance of occurrence.</td>
</tr>
<tr>
<td><strong>Overall</strong></td>
<td></td>
<td>Based on all controls tested, and the percentage of controls having no exceptions noted, overall compliance with this NERC Standard is believed to be most likely.</td>
</tr>
<tr>
<td>Most Likely</td>
<td>90.0% - 99.9%</td>
<td>Based on all controls tested, and the percentage of controls having no exceptions noted, overall compliance with this NERC Standard is believed to be more likely than not.</td>
</tr>
<tr>
<td>Probable</td>
<td>70.0% - 89.9%</td>
<td>Based on all controls tested, and the percentage of controls having no exceptions noted, overall compliance with this NERC Standard is believed to be more than remote but less than probable.</td>
</tr>
<tr>
<td>Possible</td>
<td>40.0% - 69.9%</td>
<td>Based on all controls tested, and the percentage of controls having no exceptions noted, overall compliance with this NERC Standard is believed to have a slight chance of occurrence.</td>
</tr>
</tbody>
</table>
| Remote          | 1.0% - 39.9%     | Based on all controls tested, and the percentage of controls having no exceptions noted, overall compliance with this NERC Standard is believed to be most likely.
Cleco’s Local ICE Framework Reporting

✓ Introduction

✓ Summary Results – ICE
  ▪ By Standard
  ▪ By Individual Requirement

✓ Detailed Results – ICE
  ▪ Controls with Exceptions Noted
  ▪ Other Opportunities to Improve Internal Controls
Cleco’s Local ICE Framework

Reporting

✓ Appendix A
  - Assessment of Controls Matrix

✓ Appendix B
  - Summary of Controls (by requirement)
    - Control Number
    - Control Description
    - Key
    - Result
    - # of X controls passed
Cleco’s Local ICE Framework

Follow-up
Cleco’s Local ICE Framework

Follow-up

✓ Follow-up should occur on those controls which had exceptions noted (allow appropriate time for corrective action)

✓ If ICE performed by SPP RE, consider feedback for potential follow-up action
Cleco requested that SPP RE perform an ICE for PRC-005
Outcome - Local ICE, PRC-005

Documentation Sent to SPP RE

Attached is the documentation for SPP’s consideration of Cleco’s ICE report and processes used in generating the ICE report for NERC Standard PRC-005-2.

Betty

Betty J. Deans, CPA, CIA, CITP, CCEP
NERC Compliance & Audit Analyst
CLECO Corporation
P. O. Box 5003
2030 Donahue Ferry Road
Pineville, LA 71361
(318) 484-7688 Telephone
(318) 484-7642 Facsimile

Outcome of ICE reviewed by SPP RE
“Great job to Cleco on the PRC-005 controls. As a result, we will not be conducting any fieldwork on PRC-005-1 or PRC-005-2.”

SPP RE
Greg Sorenson

Outcome of ICE reviewed by SPP RE
Cleco’s Local ICE Framework
Subsequent Follow-up with SPP RE

Overlapping of controls helped SPP RE get to a point where reliance could be placed on Cleco’s internal controls (good mix of internal control types, multiple control points)

Outcome of ICE reviewed by SPP RE
Cleco’s Local ICE Framework
Subsequent Follow-up with SPP RE

As controls are set-up, balance performance of controls by operations and the compliance department

Outcome of ICE reviewed by SPP RE
Cleco’s Local ICE Framework

Subsequent Follow-up with SPP RE

Placed reliance on Cleco’s ICE Report

- Independence
- Experience
- Credentials

3.0 ICE Process

3.1.1.4 Using the Work of Others
Many registered entities employ an independent team to assess compliance with their risk management strategy that includes adherence to NERC Reliability Standards. An independent internal control evaluation may be conducted by a specialist, government entity (such as the Government Accountability Office or Nuclear Regulatory Commission), a contractor who has been commissioned by the registered entity as a disinterested third party, or by an internal department within the registered entity that is independent of the department performing reliability standards operations. If a registered entity seeks to have the CEA rely on the “work of others” based on any of these scenarios, the CEA team may review the independence, capabilities and competencies of the individuals performing the review and relevant Independent Audit Report (IAR) documentation for consideration of use as part of ICE evaluation. The information regarding a registered entity’s independent review shall be gathered during the Key Control Identification and Walkthrough stage. Any additional information requests necessary will be sent to the registered entity, as necessary.

NERC’s ERO Enterprise Internal Control Evaluation Guide (October 2014)

Outcome of ICE reviewed by SPP RE
Cleco’s Local ICE

Lessons Learned
Cleco’s Local ICE Framework

Lesson(s) Learned

1. Internal Control training needed

Made two presentations to various stakeholders

Internal Controls

- Internal Controls Overview
- FAC-008-3 (Facility Ratings) and Beyond
- Internal Control Evaluation (ICE) Process

NERC Compliance and Training
Betty J. Deans, CPA, CIA, CITP, CCEP

Posted on Cleco’s SharePoint intranet
2. Need to educate stakeholders on Cleco’s local ICE process and its benefits
3. Need to incorporate more internal controls into compliance efforts.
Questions

Thank You !!!!
Resource Links

2016 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Program
North American Electric Reliability Corporation (NERC)

ERO Enterprise Internal Control Evaluation Guide; October 2014
North American Electric Reliability Corporation (NERC)

SPP RE’s Internal Control Evaluation Overview; April 7, 2015
Southwest Power Pool Regional Entity (SPP RE); Jeff Rooker
https://www.spp.org/documents/28953/spp%20re%20%20internal%20control%20evaluation%20overview.pdf

SPP RE Audit Processes and Sampling; March 16, 2016
Southwest Power Pool Regional Entity (SPP RE); Shon Austin, Mike Hughes

SPP RE 2016 Monitoring Scope Plan
Southwest Power Pool Regional Entity (SPP RE)
SPP RE General Manager’s Report (page 120/365); 2015 Spring Workshop
Southwest Power Pool Regional Entity (SPP RE); Ron Ciesiel

SPP RE 2016 Monitoring Scope Plan
Southwest Power Pool Regional Entity (SPP RE)
Contact Information

Betty J. Deans, CPA, CIA, CITP, CCEP

Certified Public Accountant
Certified Internal Auditor
Certified Information Technology Professional
Certified Compliance & Ethics Professional

Betty.Deans@cleco.com
(318) 484-7566
2016 State of Reliability

September 20, 2016
SPP RE Fall Workshop

Mike Hughes
SPP RE Lead Compliance Engineer
State of Reliability 2016

May 2016
State of Reliability Report

• Provides an objective view of reliability performance
• Identifies trends and risks to reliability
• Serves as risk-informed input to:
  – Prioritize steps to manage risk
  – Standards projects
• Enforcement Metrics
NERC Severity Risk Index (SRI)

- Generation
- Transmission
- Load Loss
### 2015 Top Ten SRI Days

#### Table 3.1: Top Ten SRI Days in 2015

<table>
<thead>
<tr>
<th>Date</th>
<th>SRI</th>
<th>Weighted Generation</th>
<th>Weighted Transmission</th>
<th>Weighted Load Loss</th>
<th>G/T/L</th>
<th>Weather Influenced Verified by OE-417(^1) or Other sources(^2)</th>
<th>Rank</th>
<th>Event Type</th>
<th>Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/17/2015</td>
<td>4.45</td>
<td>1.24</td>
<td>1.49</td>
<td>1.72</td>
<td></td>
<td>Yes(^3)</td>
<td>1</td>
<td>Storm, Flooding, Straightline Winds</td>
<td>WECC</td>
</tr>
<tr>
<td>6/30/2015</td>
<td>4.40</td>
<td>2.87</td>
<td>1.47</td>
<td>0.10</td>
<td></td>
<td>Yes(^3)</td>
<td>2</td>
<td>Severe Weather</td>
<td>WECC</td>
</tr>
<tr>
<td>1/8/2015</td>
<td>4.02</td>
<td>3.52</td>
<td>0.25</td>
<td>0.24</td>
<td></td>
<td>Yes(^3)</td>
<td>3</td>
<td>Severe Winter Weather</td>
<td>SERC</td>
</tr>
<tr>
<td>10/23/2015</td>
<td>3.79</td>
<td>1.32</td>
<td>2.43</td>
<td>0.43</td>
<td></td>
<td>Yes(^4)</td>
<td>4</td>
<td>Excessive Rainfall, Thunder/Lightning Storm</td>
<td>TRE, SPP, SERC</td>
</tr>
<tr>
<td>7/18/2015</td>
<td>3.38</td>
<td>1.37</td>
<td>1.20</td>
<td>0.80</td>
<td></td>
<td>Yes(^5)</td>
<td>5</td>
<td>Severe Weather</td>
<td>MRO, WECC</td>
</tr>
<tr>
<td>7/20/2015</td>
<td>3.30</td>
<td>1.89</td>
<td>1.31</td>
<td>0.05</td>
<td></td>
<td>Yes(^2)</td>
<td>6</td>
<td>Thunderstorm/Showers</td>
<td>Widespread</td>
</tr>
<tr>
<td>6/23/2015</td>
<td>3.24</td>
<td>1.49</td>
<td>0.81</td>
<td>0.94</td>
<td></td>
<td>Yes(^4)</td>
<td>7</td>
<td>Severe Weather</td>
<td>RFC, NPCC</td>
</tr>
<tr>
<td>7/13/2015</td>
<td>3.20</td>
<td>2.12</td>
<td>0.70</td>
<td>0.42</td>
<td></td>
<td>Yes(^5)</td>
<td>8</td>
<td>Severe Weather</td>
<td>RFC</td>
</tr>
<tr>
<td>7/30/2015</td>
<td>3.10</td>
<td>2.06</td>
<td>0.68</td>
<td>0.37</td>
<td></td>
<td>Yes(^5)</td>
<td>9</td>
<td>Summer Weather</td>
<td>Widespread</td>
</tr>
<tr>
<td>2/20/2015</td>
<td>3.10</td>
<td>2.73</td>
<td>0.21</td>
<td>0.18</td>
<td></td>
<td>Yes(^5)</td>
<td>10</td>
<td>Severe Winter Weather</td>
<td>SERC</td>
</tr>
</tbody>
</table>
SRI Comparison

Figure 3.1: NERC Annual Daily Severity Risk Index Sorted Descending
Key Finding 1: Protection
System Misoperations Decline

Recommendation: NERC should, in collaboration with industry, improve knowledge of risk scenarios by focusing education on the instantaneous ground overcurrent protection function and on improving relay commissioning tests.
Key Finding 2: BPS Resiliency to Severe Weather Improved

Recommendation: NERC should consider performing daily SRI calculations on a regional basis.
Key Finding 3: Human Error Has Decreased

Recommendation: NERC should focus on human performance training and education through conferences and workshops that increase knowledge of possible risk scenarios.
Key Finding 4: No Category 4 or 5 Events in 2015

Recommendation: NERC should continue to develop and publish lessons learned from qualifying system events.
Key Finding 5: Improved Modeling of Blackout Risk Assessments

Recommendation: NERC should provide leadership in collaborative efforts to improve dynamic model validation, including the use of synchrophasor technology.
Key Finding 6: Essential Reliability Services Trend is Stable; Faces Potential Challenges

Recommendation: The ERO should lead efforts to monitor [and mitigate] the impacts of resource mix changes.
Key Finding 7: No Load Loss Due to Cybersecurity Events

Recommendation: NERC should support collaborative efforts to strengthen situational awareness for cyber and physical security while providing timely and coordinated information to industry.
There was a violation or PV and it led to:

**Tier 3: Major BES Disturbances**
- Caused or contributed to a major BES disturbance

**Tier 2: Moderate Impact**
- IROL exceeded
- BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for > 30 minutes
- BES facilities tripped unexpectedly
- Emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation
- Equipment damage
- Major (> 50%) loss of visibility, control, state estimation, or contingency analysis for over 30 minutes

**Tier 1: Minor Impact**
- Observations similar to those in in tier 2 but of lesser magnitude
- Loss of ability to monitor cybersecurity intrusions

**Tier 0: No Impact**
- No observed impact

Figure 5.4: Impact Observations Mapped to the Impact Pyramid Tiers
Most Frequently Filed Standards

Figure 5.6: Most Frequently Filed Standards and Requirements (2014-2016 Data)
Questions
Mike Hughes
Lead Compliance Engineer
501.688.1712
mhughes.re@spp.org
O&P Audit Success and Lessons Learned

Presented to the SPP RE Fall Workshop
September 20, 2016

Matthew A. Caves
Manager, Legal & Regulatory Compliance
Disclaimer

• No Attorney-Client Relationship or Legal Advice

Communication of information by, in, to or through this presentation and your receipt or use of it (1) is not provided in the course of and does not create or constitute an attorney-client relationship, (2) is not intended as a solicitation, (3) is not intended to convey or constitute legal advice, and (4) is not a substitute for obtaining actual or implied legal advice from a qualified attorney. You should not act upon any such information without first seeking qualified professional counsel on your specific matter. The hiring of an attorney is an important decision that should not be based solely upon forum, discussion, communications or advertisements.
Disclaimer (cont’d)

• Audit Findings Specific to WFEC

The facts and circumstances reviewed, presented and/or audited were specific to WFEC prior to, during, and after the specific O&P audit in question. Individual results may vary.
Operational Disclaimer

• All of the WFEC SME’s and technical staff have operational duties in addition to compliance.

• If an operational issue comes up and they are the best or only person that can adequately address the issue, they may need to leave the audit for a period of time.

• We have asked that any and all interruptions (from their staff) be kept to an absolute minimal because of the importance of the NERC O&P Standards Compliance Audit.
Compliance Structure

• Board Policy No. 3-9
  - WFEC demonstrates commitment to ensuring compliance with NERC Reliability Standards.
  - Policy requires development, implementation, and monitoring of compliance monitoring and enforcement program.
  - Appoints the Manager, Legal & Regulatory Compliance as Compliance Officer.
Compliance Team

• Compliance Team – Six Members
  - Manager, Legal & Regulatory Compliance/Compliance Officer
  - Records Coordinator
  - CIP Compliance Specialist
  - Generation Compliance Specialist
  - Operations Compliance Specialist
  - Transmission Compliance Specialist

*Also receive technical and operational assistance from functional areas – Subject Matter Experts (SMEs) and department managers.
Audit Preparations

- Develop (Positive) Relationships
- Third Party Review of Evidence is Important
- WFEC Utilized SPP RTO Outreach prior to NERC CIP Audit and NERC O&P Audits in 2015
- Prepare SMEs (and technical staff) as if “Witness Testimony”
- Set Expectations and Ground Rules
- Control and Maintain Audit Environment
- ** Maintain Detailed Revision Histories **
Audit Logistics

• WFEC utilizes SharePoint to gather and organize evidence.
• SharePoint allows control or limit access to review and edit.
• Have SMEs Utilize Business Process Models (BPMs)
• Locate Technical Staff Close to SMEs
• Control and Maintain Audit Environment
  - Break and Caucus to Control Tempo
• Use Screens (in lieu of projectors) if Possible
  - One for evidence, one for the standards or data request
• Have One Person Assigned to Evidence Retrieval
O&P Compliance Audit Findings

- The audit team (SPP RE and Texas RE) reviewed 29 NERC Standards with 61 requirements that applied to WFEC registered functions
  - 53 No Findings of Non-Compliance
  - 7 Not Applicable
  - 0 Possible Violations
  - 1 Open Enforcement Action
    - Self-report prior to the 693 Audit
    - Mitigation efforts have been completed
Auditors’ Positive Observations

- Knowledgeable SMEs
- Responsive to evidence requests
- Protection System inventory lists
- Development of internal controls
  - 3-Part communication reviews
- Generation Facility Rating spreadsheets had descriptive comments within the cells
- Facility Ratings sheet revision history
- Development of new forms – Misoperations and DC circuitry testing
Recommendations

• COM-001-1.1 – Telecommunication
  - Add titles and revision history to telecommunication diagrams.
  - *Comment* – Diagrams will include titles and revision histories in the future.

• EOP-001-2.1b – Emergency Operation Planning
  - R4 – If an element in Attachment 1-EOP-001 is not applicable provide an explanation in procedure.
  - *Comment* - WFEC will address the recommendation when EOP-001 is consolidated with EOP-011.
Recommendations

• EOP-005-2 – System Restoration from Blackstart Resources
  - R6 – During the monthly test of the Blackstart Resource, record the hour meter’s start and stop times.
  - R9.3 – Add verbiage in the procedure that defines the duration of the Blackstart Resource test.
  - R17 – Revise the Blackstart Resource training presentation to say, during the monthly test, the Blackstart Recourse is ran for a “minimum” of 30 minutes (rather than approximately 30 minutes) and consider using a training tracking tool for generator operators.
  - Comment – WFEC is adding additional training and a test to the Learning Management System (LMS).
Recommendations

• FAC-003-3 – Transmission Vegetation Management Plan
  - R2 - Revise the last sentence on page 5 of Section V of the TVMP for the mitigation of access issues with landowners.
  - R7 – Include the regularly occurring work in the annual vegetation work plan.
  - Comment – WFEC has clarified the wording of Section V and has included regularly occurring work in the annual work plan.
Recommendations

• FAC-008-3 – Facility Ratings
  - Include a reference for the 345kV in the WFEC’s Facility Rating Methodology.
  - Update the one-line diagrams to reflect correct ratings.
  - Remove planning limits from the ratings sheets.
  - *Comment* – WFEC revised the language in the methodology and has revised rating sheets to include only one set of limits.

• TOP-002-2.1b - Normal Operations Planning
  - Review the modeling/contingency definition of WFEC’s line segments with SPP RTO (Contingency analysis).
  - *Comment* – WFEC reviewed and revised as needed.
Recommendations

• TOP-004-2 – Transmission Operations
  - Use the definition of unknown operating state in the NERC Standard.
  - Comment – The definition of “unknown operating state” in the NERC Standard is an example. WFEC has defined “unknown operating state” to be consistent with SPP RTO’s definition.

• TPLs
  - Clearly address the sub-requirements in the planning assessments.
  - Comment – The sub-requirements were incorporated into the most current TPL report and will be included in future reports.
Areas of Concern

- FAC-008-3 – Facility Ratings
  - R3 – The Transmission Facility Rating Methodology should specify that the relay setting is used when more limiting than the relay rating.
  - R6 – The audit team reviewed a sample of Facility Rating sheets and identified missing elements and two discrepancies between the nameplate data and rating sheets. The discrepancy on one did result in a change in the Facility Rating. WFEC should conduct a review of the rating sheets to confirm all elements are included with the correct ratings.
  - Comment – WFEC has revised the methodology to clarify how ratings for relay protective devices and other applicable equipment are determined. A review of Facility Rating sheets was conducted along with the revisions to the methodology.
Areas of Concern

• PRC-001-1.1 – System Protection Coordination
  - R4 - WFEC did not coordinate protection system changes with the SPP BA. WFEC should develop a process for notifying neighboring entities of protection system changes.
  - *Comment* – WFEC has adopted a procedure outlining the notification process for protection system changes.

• TOP-002-2.1b – Normal Operations Planning
  - R11 – The audit team identified two incorrect Facility Ratings with neighboring TOPs. WFEC should ensure that Facility Rating changes are communicated when they occur.
  - *Comment* – Completed. WFEC has clarified the Facility Ratings usage with neighboring TOPs.
Areas of Concern

• FAC-008-3 – Facility Ratings
  - R8 – WFEC should verify the SPP RC utilizes the correct Facility Ratings for the SPP flowgates.
  - Comment – WFEC developed internal control process to ensure Facility Ratings are checked at set intervals.
Self-Report

- EOP-004-2 R2 – Event Reporting
  - Contractors were replacing the generator and transformer protection relays at a switch station (while a plant was off-line for scheduled maintenance). Contractors tripped seven breakers, causing loss of three Bulk Electric System (BES) Elements.
  - Comment – WFEC now includes contractor training and contract language informing contractor about the potential sensitivity of the equipment (electromechanical relays, etc.).
Questions?
TOP-001-3
TOP-002-4
TOP-003-3

September 20, 2016
Fall Workshop

Allen Klassen, Westar
Mike Hughes, SPP RE
Use of Presentation

• For simplicity, some wording from the standard has been shortened, paraphrased, or omitted

• Due to space and time constraints, some topics, special cases, and notes have not been addressed

• It is important to read each standard in its entirety
Overview

- Enforcement Dates
- Relevant Definitions
- TOP-003-3 Operational Reliability Data
- TOP-002-4 Operations Planning
- TOP-001-3 Transmission Operations
- Compliance
Enforcement Dates

- November 2015  FERC approval
- January 1, 2017  TOP-003-3 (Except R5)
- April 1, 2017  TOP-003-3 R5
- April 1, 2017  TOP-002-4
- April 1, 2017  TOP-001-3
Definitions – Glossary of Terms

• Operational Planning Analysis (OPA) NEW
  – “An evaluation of projected system conditions to assess anticipated (pre-Contingency) and potential (post-Contingency) conditions for next-day operations. The evaluation shall reflect applicable inputs including, but not limited to, load forecasts, generation output levels, Interchange, known Protection System and Special Protection System status or degradation, Transmission outages, generator outages, Facility Ratings, and identified phase angle and equipment limitations (Operational Planning Analysis may be provided through internal systems or through third-party services.)”

• Requirements to perform OPA are in IRO-008-2 and TOP-002-4

• RCs and TOPs must have Operating Plans for next-day operations to address potential SOL exceedances identified in the OPA
Definitions – Glossary of Terms

• Real-time Assessment (RTA) New Term
  “An evaluation of system conditions using Real-time data to assess existing (pre-Contingency) and potential (post-Contingency) operating conditions. The assessment shall reflect applicable inputs including, but not limited to: load, generation output levels, known Protection System and Special Protection System status or degradation, Transmission outages, generator outages, Interchange, Facility Ratings, and identified phase-angle and equipment limitations. (Real-time Assessment may be performed through internal systems or through third-party services.)”

• New definition includes specific inputs for RTA that address issues from the 2011 Southwest Outage Report

• Requirements to perform RTA are in IRO-008-2 and TOP-001-3

• Use of Third-party services may provide an efficient alternative to conducting RTA for some entities
Definitions – Glossary of Terms

• Operating Plan
  – “A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan.”
TOP-003-3 Operational Reliability Data

• **R1** – “Each TOP shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments”
  
  – 1.1 - needed data and info including non-BES data and external network data
  
  – 1.2 - provisions for notification of current Protection System status or degradation
  
  – 1.3/1.4 – periodicity and deadline
TOP-003-3 Operational Reliability Data

- **R3 [R4].** “Each TOP [BA] shall distribute its data specification to entities that have data required by the TOP’s [BA’s] Operational Planning Analyses, Real-time monitoring, and Real-time Assessment.”

- **R5.** “Each TOP, BA, GO, GOP, LSE, TO and DP receiving a data specification in R3, R4 shall satisfy the obligations of the documented specifications..”
TOP-002-4 Operations Planning

• **R1.** “Each TOP shall have an Operational Planning Analysis (OPA) that will allow it to assess whether its planned operations for the next day within its TOP area will exceed any of its System Operating Limits (SOLs).”

• **R2.** “Each TOP shall have an Operating Plan(s) for next-day operations to address potential SOL exceedances identified as a result of its Operational Planning Analysis as required in R1.”
TOP-002-4 Operations Planning

• **R3.** “Each TOP shall notify entities identified in the Operating Plan... of their role...”

• **R6[R7].** Each TOP [BA] shall provide its Operating Plan for next day operations ... to its RC.

• TOPs shall notify entities of roles (R3) and provide plans to RC (R6)
TOP-001-3 Transmission Operations

• **R10.** Each TOP shall perform the following as necessary for determining SOL exceedances within its TOP area:
  
  – 10.1 - within, monitor Facilities and status of SPS
  
  – 10.2 - outside, obtain status, voltage, and flow and status of SPS
TOP-001-3 Transmission Operations

• **R13.** Each TOP shall ensure a Real-Time Assessment (RTA) is performed at least once every 30 minutes.

• **R14.** Each TOP shall initiate its Operating Plan to mitigate a SOL exceedance identified as part of its Real-time monitoring or Real Time Assessment.
Lessons Learned
NARROWS BRIDGE COLLAPSES

THE TACOMA NEWS TRIBUNE

Exclusive News Tribune Photographs of Spectacular Crash of $6,740,000 Narrows Bridge

Plunge Of Big Span Pictured

Center Span, Torn by Wind, Falls to Water

Great Nares' Structure, Twisted, and Whipped by 40 Mile Gale, Partly Disintegrates; Catastrophe Blamed on Failure of Cables to Move in Unison

By NELSON E. BECHTEL

The two ends of the Nares' Narrows bridge temporarily united by the force of the winds at 12:00 o'clock Thursday afternoon.
“Without adequate planning and situational awareness, entities responsible for operating and overseeing the transmission system could not ensure reliable operations within System Operating Limits (SOLs) or prevent cascading outages in the event of a single contingency.”
2011 Southwest Blackout

Finding 1 – Failure to Conduct and Share Next Day Studies

Recommendation 1 – “All TOPs should conduct next-day studies and share the results with neighboring TOPs and the RC (before the next day) to ensure that all contingencies that could impact the BPS are studied.”

TOP-002-4 R6, R7
2011 Southwest Blackout

Finding 12 – Inadequate Real-Time Tools

Recommendation 12 – “TOPs should take measures to ensure that their real-time tools are adequate, operational, and run frequently enough to provide their operators the situational awareness necessary to identify and plan for contingencies and reliably operate their systems.”

TOP-001-3 R13
2011 Southwest Blackout

Finding 13 – Reliance on Post-Contingency Mitigation Plans

Recommendation 13 – “TOPs should review existing operating processes and procedures to ensure that post-contingency mitigation plans reflect the time necessary to take mitigating actions, including control actions, to return the system to a secure N-1 state as soon as possible but no longer than 30 minutes following a single contingency. As part of this review, TOPs should consider the effect of relays that automatically isolate facilities without providing operators sufficient time to take mitigating measures.”

TOP-001-3 R10, R14
Questions about TOP-001-3 R13 & R14

- **R13.** “Each TOP shall ensure a Real-Time Assessment (RTA) is performed at least once every 30 minutes.”
- **R14.** “Each TOP shall initiate its Operating Plan to mitigate a SOL exceedance identified as part of its Real-time monitoring or Real Time Assessment.”

**Project 2014-03 Revisions to TOP and IRO Standards**
FERC Order Approving TOP Standards

**Docket No. RM15-16-000, Order No. 817** (issued November 19, 2015)

NERC’s petition noted improvements in **situational awareness**, as well as reliability issues identified in the 2011 Southwest Blackout. (FERC Order pages 5, 6)
Situational Awareness
Q: Can the Real-time Assessment be performed by a third party?

A: Yes. The NERC Glossary of Terms for RTA clarifies...

“Realtime Assessment may be provided through internal systems or through third-party services.”
Q: When using the SPP RC real time contingency analysis (RTCA), is the TOP required to look at the RTCA solution every 30 minutes?

FERC Order ¶ 70 “we agree with NERC that [TOP-001-3] Requirement R13 specifies that transmission operators must perform a real-time assessment at least once every 30 minutes, which by definition is an evaluation of system conditions to assess existing and potential operating conditions.” (page 51)

A: Some type of evaluation or assessment must be performed every 30 minutes, but as explained later, there are other options besides the RTCA.
Q: Is the RTCA the only acceptable method to perform a RTA?
A: No.

“...[TOP-001-3] does not specify a system or tool. This gives the TOP flexibility to perform its real-time assessment.” (FERC Order ¶ 65, page 47)

“...if a transmission operators’ tools are unavailable for 30 minutes or more, the transmission operator has the flexibility to meet the requirement to assess system conditions through other means.” (FERC Order ¶ 65, page 48)
Standard Drafting Team (SDT) Comments

“SDT comment responses have made clear that it doesn’t expect automated methods to be perfect and run as designed every 30 minutes. It has stated that it is assuming that an entity will have or develop an Operating Plan to cover the situation where normal methods aren’t operational. And the SDT has provided documentation in that regard in Section F of proposed TOP-001-3 where it describes what an Operating Plan should be and what it should cover for this situation. Now, any Operating Plan is probably going to require manual intervention, for example, to call up needed data, to bring into play a backup procedure, etc. The SDT further believes that if an entity has made a good faith effort to exercise its Operating Plan within the 30-minute timeframe that the entity shouldn’t be found to be out of compliance.” (partial from note 2, page 13)
Rationale for Requirement R13

“The Operating Plan should contain instructions as to how to perform Operational Planning Analysis and Real-time Assessment with detailed instructions and timing requirements as to how to adapt to conditions where processes, procedures, and automated software systems are not available (if used). This could include instructions such as an indication that no actions may be required* if system conditions have not changed significantly and that previous Contingency analysis or Real-time Assessments may be used in such a situation.” (TOP-001-3 page 19)

* “No action” only if allowed by the Operating Plan, and note the decision to take “no action” needs to be documented as the RTA for that 30 minute interval.
Q: What type of evidence is required?

A: M13 “Each Transmission Operator shall have, and make available upon request, evidence to show it ensured that a Real-Time Assessment was performed at least once every 30 minutes. This evidence could include but is not limited to dated computer logs showing times the assessment was conducted, dated checklists, or other evidence.”
Operating Plan

Operating Plans can be general in nature; in addition they can address specific reliability issues. The general portion does not contain a prescription for the specific set-up for tomorrow but contains a treatment of all the processes, procedures, and automated software systems that are at the operator’s disposal. The existence of an Operating Plan, however, does not preclude the need for creating specific action plans for specific SOL or IROL exceedances identified in the Operational Planning Analysis (OPA). (continued)
Operating Plan

(continued)

The Operating Plan may contain a description of the process by which specific prevention or mitigation plans for day-to-day SOL or IROL exceedances identified in the OPA are handled and communicated. This approach could alleviate any potential administrative burden associated with perceived requirements for continual day-to-day updating of “the Operating Plan document” for compliance purposes.

(see more information Section F, page 17, of TOP-001-3)
Q: What data retention period is required?

A: “Each Transmission Operator shall keep data or evidence for Requirement R13 and Measure M13 for a rolling 30-day period, unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.” (TOP-001-3 page 7)
RSAW (draft)

Auditors are encouraged to monitor compliance during critical events on the entity’s system occurring during the compliance monitoring period.
Helpful Reference

- NERC One-Stop-Shop: Implementation Plan; FERC Order; RSAW
CIP Update

September 20, 2016

Shon Austin
Lead Compliance Specialist
CIP Compliance Monitoring

- CIP Compliance Audit Schedule
  - CIP compliance audits
    - Three already completed this year
    - One more scheduled for this year
  - Four additional audits pushed into 2017 due to delayed effective date of Revised CIP V5 Standards
    - No word yet on any FERC-led CIP compliance audits
  - Will resume auditing non-BA, non-TOP Registered Entities with only low Impact BES Cyber Systems beginning 2Q 2017
    - Will pick up cancelled 2014 – 2016 audits
CIP Compliance Monitoring

- Non-BA, non-TOP Registered Entities with high or medium Impact BES Cyber Systems will be shifted to a three-year cycle
CIP Compliance Monitoring

- Microsoft is transitioning to a single “Monthly Rollup”
  - Second Tuesday of each month
  - Addresses all security and non-security issues
  - Applicable operating system
    - Currently used for Windows 10
    - Windows 7 SP1
    - Windows 8.1
    - Windows Server 2008 R2
    - Windows Server 2012
    - Windows Server 2012 R2
CIP Compliance Monitoring

- Initially “Monthly Rollup” patches contain fixes for the operating system released since October 2016
- Plans to add older patches to this rollup
- Eventually fully cumulative patch
  - Completely unpatched system could apply a single rollup patch
  - Plus any prerequisites that rollup requires
  - Will be fully up to date with everything the “Monthly Rollup” covers
CIP Compliance Monitoring

- Impact to CIP-007-6 Table R2 (Security Patch Management)

- Benefit
  - Reduced monthly patch patches
    - Possible reduction of compliance documentation and efforts

- Issues
  - All or nothing
    - Fully cumulative update
  - Previously excluded patches may be installed
    - Plans to add older patches to this rollup
    - Any prerequisites that rollup requires will be installed
Characterization of Violations
Ingress/Egress Authentication

- **CIP-005-5 R1 Part 1.3** - Require inbound and outbound access permissions, including the rationale for granting access, and deny all other access by default.
  - Issues left over from CIP-005-3
    - Ingress rules are too broad and/or unnecessary
    - Ingress rules allows bypass of the Intermediate System for Interactive Remote Access
    - Inter-ESP communication implemented without considering access controls
Multi-Factor Authentication

- **CIP-005-5 R2 Part 2.3** - Use multi-factor (i.e., at least two) authentication to manage all Interactive Remote Access sessions

  - Implement multi-factor authentication to use authentication factors from at least two of three generally accepted categories.
    - **Something you know** (the knowledge factor)
      - (e.g., a password or personal identification number or PIN)
    - **Something you have** (the possession factor)
      - (e.g., a one-time password token or a smart-card)
    - **Something you are** (the inherence factor)
      - (e.g., fingerprint or iris pattern)
Potential Issue with Multi-Factor Authentication

- Storing remote user's digital certificate on a separate server and not on the Cyber Asset initiating Interactive Remote Access
  - Removes the "something you have" attribute of the authentication factor

- Guidance for Secure Interactive Remote Access
  - Developed by NERC in July 2011
  - Did not consider V5 CIP requirements
Encryption

• **CIP-005-5 R2 Part 2.2** - Use encryption that terminates at an Intermediate System for all Interactive Remote Access
  
  – Encryption between the Cyber Asset initiating communication and the Intermediate System(s)
  
  – Where is encryption required to terminate?
    
    ▪ There is confusion regarding where encryption must terminate
    ▪ Encryption only required on the “non-secure” side of the Intermediate System
Potential Issue with Encryption

- Interruption in the encrypted path from the remote user's Cyber Asset to the Intermediate System
  - Not terminating on an Intermediate System
Modified CIP-003-7 LERC Definition

• FERC ORDER 822
  – “… the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term “direct” as it is used in the proposed definition.”
  – FERC “direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule…”
  – The “Low Impact External Routable Connectivity definition [is now required to be] consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.”
Modified CIP-003-7 LERC Definition

- Standard Drafting Team made the following changes to address the directive:
  1. Revised the definition of Low Impact External Routable Connectivity (LERC)
  2. Retired Low Impact BES Cyber System Electronic Access Point (LEAP)
  3. Revised the requirement language (Requirement R2) of Sections 2 and 3 in Attachment 1 of CIP-003-7
  4. Modified and added new LERC Reference Models
Modified CIP-003-7 LERC Definition

- SDT revised the definition of LERC
  - Currently defined as:
    - “Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bidirectional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC61850 GOOSE or vendor proprietary protocols).”
Modified CIP-003-7 LERC Definition

• SDT revised the definition of LERC
  – Revised Definition:
    ▪ “Routable protocol communication that crosses the boundary of an asset containing one or more low impact BES Cyber System(s), excluding communications between intelligent electronic devices used for time-sensitive protection or control functions between non-Control Center BES assets containing low impact BES Cyber Systems including, but not limited to, IEC 61850 GOOSE or vendor proprietary protocols..”
Modified CIP-003-7 LERC Definition

- SDT retired the term Low Impact BES Cyber System Electronic Access Point (LEAP)
  - A Cyber Asset interface that controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems.
Modified CIP-003-7 LERC Definition

• SDT revised the requirement language (R2) of Sections 2 in Attachment 1 of CIP-003-7

• Changes to Section 2:

  – Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset and (2) the Low Impact BES Cyber System Electronic Access Points (LEAPs), and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.
Modified CIP-003-7 LERC Definition

• SDT revised the requirement language (R2) of Sections 3 in Attachment 1 of CIP-003-7

• Changes to Section 3:
  
  – 3.1. **For** implement electronic access control(s) for LERC, if any, implement a LEAP to permit only necessary inbound and outbound bi-directional routable protocol access; and electronic access to low impact BES Cyber System(s).
CIP-002 Issues

• Identify all assets that contain low impact BES Cyber Systems
  – Even if the asset is already identified as containing high and/or medium impact BES Cyber Systems
CIP-002 Issues

• An entity owns renewable assets and a control center.
  
  A. Both the windfarm and Control Center were registered as GOPs, but both assets are registered in a separate regions.
  
  B. Both the Windfarm and Control Center are registered as GOPs and are registered in the same region.
  
  C. Only the Windfarm is registered as a GOP, but the control center sometimes acts as a GOP. The control center is not registered in any region.
  
  D. Only the Control Center is registered as a GOP

• Solution
  
  • A – No issue  
  • B – No issue  
  • C – Registration issue  
  • D – Possible CIP issue
SPP RE CIP Team

- **Kevin Perry**, Director of Critical Infrastructure Protection  
  (501) 614-3251
- **Shon Austin**, Lead Compliance Specialist-CIP  
  (501) 614-3273
- **Jeremy Withers**, Senior Compliance Specialist-CIP  
  (501) 688-1676
- **Robert Vaughn**, Compliance Specialist II-CIP  
  (501) 482-2301
- **Sushil Subedi**, Compliance Specialist II-CIP  
  (501) 482-2332
EOP-011-1, IRO-017-1, IRO-010-2, PRC-026-1, new RAS definition

Jeff Rooker
Lead Compliance Engineer
jrooker.re@spp.org
501.614.3278

Thomas Teafatiller
Senior Compliance Engineer
tteafatiller.re@spp.org
501.688.2514
Use of Presentation

• The standards are discussed as filed with FERC
• This presentation covers highlights from multiple NERC Reliability Standards
• For simplicity, some wording from the standard has been shortened, paraphrased, or omitted
• Due to space and time constraints, some topics, special cases, and notes have not been addressed
• It is important for you to read each standard and associated documentation (implementation plan, project page, technical justification, etc.)
Overview

- **EOP-011-1:**
  - *Emergency Operations*
  - *Implementation Plan*

- **IRO-010-2:**
  - *Reliability Coordinator Data Specification and Collection*
  - *Implementation Plan*

- **IRO-017-1:**
  - *Outage Coordination*
  - *Implementation Plan*

- **PRC-026-1:**
  - *Relay Performance During Stable Power Swings*
  - *Implementation Plan*
NEW: EOP-011-1 Emergency Operations

- Consolidates requirements from EOP-001, 002, and 003 into one Standard addressing 7 FERC directives
- **Purpose:** Address effects of operating Emergencies by ensuring each Transmission Operator (TOP) and Balancing Authority (BA) has developed Operating Plans to mitigate operating Emergencies and that plans are coordinated with the Reliability Coordinator (RC)
- 6 requirements effective 4/1/17
- EOP-001, 002, and 003 will be retired 4/1/17
- Evidence shall be retained since the last audit for all requirements
EOP-011-1 Emergency Operations

- Revised Definition
  - Energy Emergency - A condition when a Load-Serving Entity or Balancing Authority has exhausted all other resource options and can no longer provide meet its customers’ expected energy requirements Load obligations
EOP-011-1 R1

• **R1 - TOP** develop, maintain and implement Emergency Operating Plan(s)- Reviewed by RC. Shall include:
  
  • **1.1** Roles and responsibilities to activate the Plan
  
  • **1.2** Processes to prepare for and mitigate Emergencies
    
    • Notification of RC (real-time and expected conditions) during Emergency
    
    • Cancellation/recall of outages
    
    • Transmission system reconfiguration, gen. redispacht
    
    • Manual load shed minimizing overlap with UFLS
    
    • Impacts of extreme weather conditions
EOP-011-1 R2

• **R2** - Basically the same as R1 except for **BA Capacity and Energy** Emergency Operating Plan(s)

• **R2.2.2** - Shall include the process for requesting an Energy Emergency Alert (EEA)

• **R2.2** - Processes to mitigate Emergencies
  - Replicates many of those listed in EOP-001-2.1b Attachment 1 (to be retired)

• **R2.2.9** - Includes plan for extreme weather events (plans to winterize units)

• Can have one plan to address both R1 and R2 if both a TOP and BA
EOP-011-1 R1 and R2 Evidence

• Dated Operating Plan reviewed by RC
• Revision history
• If Emergency occurs, maintain operator logs, voice recordings/documentation of implementation
EOP-011-1 Emergency Operations

- R2 and R6 incorporate Attachment 1, which describes three EEA levels used by the RC and process for communicating condition of BA experiencing EEA.

- For R1 and R2 if any sub-requirement is not applicable, note so in Plan with rationale.
EOP-011-1 R3, R4

- **R3** - RC review TOP or BA plan within 30 days
  - Review reliability risk addressed for **compatibility** with other TOP/BA Plans
  - Not required to approve plans but provide results of review
- **R4** - TOP and BA address reliability risks identified by RC in R3
  - Resubmit within RC specified timeframe
  - Evidence:
    - Dated emails on receipt from RC
    - TOP/BA response with updated Plan with version history
EOP-011-1 R5, R6

• **R5** - Implementation- RC notify other BA/TOP and adjacent RCs within 30 minutes of receiving BA/TOP Emergency notification

• **R6** - Implementation- RC issues EEA for BA with potential or actual Energy Emergency per Attachment 1

• Evidence RC must provide:
  – Operator logs
  – Voice recordings
  – Dated documentation of notification to entities and issuance of EEA
IRO-010-2 RC Data Specification and Collection

• Purpose “To prevent instability, uncontrolled separation, or Cascading outages that adversely impact reliability, by ensuring the Reliability Coordinator has the data it needs to monitor and assess the operation of its Reliability Coordinator Area”

• 3 requirements
IRO-010-2 RC Data Specification and Collection

• **R1 and R2**
  – **Effective 1/1/17**
  – Applicable to RC
  – **R1** - RC develops specs and deadline for data for Operational Planning Analysis, Real-time monitoring, Real-time Assessments and **R2** - distributes to entities

• **R3**:  
  – **Effective 4/1/17**
  – Applicable to RC, BA, GO, GOP, TOP, TO, DP, LSE
  – Provide Evidence that you provided data as specified by RC in required timeframe
NEW IRO-017-1 Outage Coordination

• Purpose “To ensure that outages are properly coordinated in the Operations Planning time horizon and Near-Term Transmission Planning Horizon.”

• MISO and SPP both have defined processes as RC

• 4 requirements effective 4/1/17

• Replaces TOP-003-1 Planned Outage Coordination
IRO-017-1 R1

- **R1**: RC specifies roles and responsibilities, communication of outage schedules, coordination of responsibilities between TOPs and BAs
- **R1.2** - RC specifies outage submission timing requirements
- **R1.3** - RC specifies process to evaluate the impact of outages based on wide area view
- **R1.4** - RC defines process for resolving conflicts between entities
IRO-017-1 R2, R3

- **R2** “Each TOP and BA shall perform the functions specified in its RC’s outage coordination process”
  - Caution on outage submission timing – now enforceable by the standard, not just RC criteria

- **R3** “Each PC and TP shall provide its Planning Assessment to impacted RCs”
  - No longer “as requested” by RC
  - Technical Basis- Planning Assessment is not a list of load flow studies, but a textual summary of what was found in studies including rationales and assumptions
IRO-017-1 R4

- **R4** “Each PC and TP shall *jointly* develop solutions with its respective RC for identified issues or conflicts with planned outages in its Planning Assessment for the Near-Term Transmission Planning horizon.”
  
  - Planning Assessment – Documented evaluation of future Transmission System performance (see TPL-001-4)
  - **R2.1.3** - Near Term (years 1-5)
  - **R1.1.2** - 6 month outages
New PRC-026-1 Relay Performance During Stable Power Swings

• Purpose “To ensure that load-responsive protective relays are expected to not trip in response to stable power swings during non-Fault conditions.”

• 4 requirements
• R1 effective 1/1/18
• R2, R3, R4 effective 1/1/20; Entities must be compliant by 1/1/20
PRC-026-1 Relay Performance During Stable Power Swings

- **R1**: PC notifies GOs and TOs of BES Elements related to angular instability
  - Applicable to Planning Coordinator (PC)
  - We do not expect many Registered Entities to have BES Elements that meet R1 requirements
PRC-026-1 Relay Performance During Stable Power Swings

**R1.** PC notifies GOs and TOs of each generator, transformer, and transmission line BES Element that meets one or more of these criteria:

1. Generator where angular instability constraint exists that is addressed by SOLs or RAS

2. An Element that is part of an SOL because of angular stability

3. An Element that forms the boundary of an island in the most recent UFLS assessment, only if the island is formed by tripping the Element due to angular instability

4. An Element identified in the Planning Assessment that tripped during a PC simulated disturbance
2.1 – If PC notifies TO or GO of an applicable BES element from R1, entity must determine whether the load-responsive protective relay(s) applied to that BES Element meet the criteria in Attachment B

- Evaluation must be done within 12 calendar months
- Evaluation must be done at least once every five years
PRC-026-1 Relay Performance During Stable Power Swings

• **2.2** – If a GO or TO becomes aware of any BES Element that tripped in response to a stable or unstable power swing, it must determine whether its associated load-responsive protective relay(s) meet the criteria in Attachment B
  – Evaluation must be done within 12 calendar months
PRC-026-1 Relay Performance During Stable Power Swings

- **R2 Attachment B Criterion A:**
  - An impedance-based relay used for tripping is expected to not trip for a stable power swing, when the relay characteristic is completely contained within the unstable power swing region.\(^6\) The unstable power swing region is formed by the union of three shapes in the impedance (R-X) plane; (1) a lower loss-of-synchronism circle based on a ratio of the sending-end to receiving-end voltages of 0.7; (2) an upper loss-of-synchronism circle based on a ratio of the sending-end to receiving-end voltages of 1.43; (3) a lens that connects the endpoints of the total system impedance (with the parallel transfer impedance removed) bounded by varying the sending-end and receiving-end voltages from 0.0 to 1.0 per unit, while maintaining a constant system separation angle across the total system impedance where:
    - 1. The system separation angle is:
      - At least 120 degrees, or
      - An angle less than 120 degrees where a documented transient stability analysis demonstrates that the expected maximum stable separation angle is less than 120 degrees.
    - 2. All generation is in service and all transmission BES Elements are in their normal operating state when calculating the system impedance.
    - 3. Saturated (transient or sub-transient) reactance is used for all machines.
Attachment B Criterion A

**Shape 2** – Upper Loss of Synchronism Circle With Sending to Receiving Voltage Ratio of 1.43

**Shape 3** – Lens with Constant 120 Degree Angle and Both Sending and Receiving Voltages Varied from 0 to 1 Per Unit

**Shape 1** – Lower Loss of Synchronism Circle With Sending to Receiving Voltage Ratio of 0.7

*Graph showing various electrical characteristics with annotations.*
Attachment B Criterion A

Non-Tripping Region of Mho Element Characteristic

Non-Tripping Region of Mho Element Characteristic

Mho Element Characteristic

Load Encroachment Blinders

X (ohms)

R (ohms)
Attachment B Criterion A

Breaker opens. If breaker hadn't opened, the swing would have continued past the 180 degree point as depicted by the dashed line.

Zone 2 is not contained within the unstable power swing region.

Unstable swing enters zone 2.
Attachment B Criterion A

Stable swing enters then leaves zone 2, but zone 2 trips
Lens Characteristic Tool

- **PRC-026-1 Project page** has tools that allow you to enter data and calculate the power swing stability lens characteristics per the PRC-026-1 Application Guidelines
  - **Stable Power Swing Calculation Tool**
  - **Generator Stable Power Swing Calculation Tool**
• The pickup of an overcurrent relay element used for tripping, that is above the calculated current value (with the parallel transfer impedance removed) for the conditions below:

1. The system separation angle is:
   - At least 120 degrees, or
   - An angle less than 120 degrees where a documented transient stability analysis demonstrates that the expected maximum stable separation angle is less than 120 degrees

2. All generation is in service and all transmission BES Elements are in their normal operating state when calculating the system impedance

3. Saturated (transient or sub-transient) reactance is used for all machines

4. Both sending-end and receiving-end voltages at 1.05 per unit
PRC-026-1 Relay Performance During Stable Power Swings

- **R3**: Within six months of determining a relay does not meet Attachment B criteria, GO or TO must develop a Corrective Action Plan (CAP) to meet specific technical details outlined in the Requirement language.

- **R4**: GO or TO shall implement each CAP and update each CAP if actions or timetables change.
New Definition for Remedial Action Scheme (RAS)

- Effective 4/1/17
- Updated Definition in NERC Glossary of Terms
- Combining Special Protection System (SPS) with RAS
- Definition has been broadened and includes a list of exclusions
- [Project page]
Standards Updated due to new RAS definition

- EOP-004-3
- FAC-010-3
- FAC-011-3
- MOD-029-2a
- MOD-030-3
- PRC-015-1
- PRC-016-1
- PRC-023-1
New RAS Definition

• Scheme designed to detect predetermined System conditions and automatically take corrective actions that may include, but are not limited to:
  – Adjusting or tripping generation (MW and Mvar)
  – Tripping load,
  – Or reconfiguring a System(s).
New RAS Definition

- RAS accomplish objectives such as:
  - Meeting standard requirements
  - Maintaining BES stability
  - Maintaining acceptable BES voltages
  - Maintaining acceptable BES power flows
  - Limiting the impact of Cascading or extreme events
Does Not Individually Constitute RAS

A. Protection Systems installed to detecting Faults on BES Elements and isolating faulted Elements

B. Schemes for automatic UFLS and automatic UVLS comprised of only distributed relays

C. Out-of-step tripping and power swing blocking

D. Automatic reclosing schemes

E. Schemes applied on an Element for non-Fault conditions, such as, but not limited to
   - Generator loss-of-field
   - Transformer top-oil temperature
   - Overvoltage
   - Overload to protect the Element against damage by removing it from service
Does **Not** Individually Constitute RAS

F. Controllers that switch or regulate one or more:
   - Series or shunt reactive devices,
   - Flexible alternating current transmission system (FACTS) devices
   - Phase-shifting transformers,
   - Variable-frequency transformers
   - Or tap-changing transformers;
   - And, that are located at and monitor quantities solely at the same station as the Element being switched or regulated

G. FACTS controllers that remotely switch static shunt reactive devices located at other stations to regulate the output of a single FACTS device
Does **Not** Individually Constitute RAS

H. Schemes or controllers that remotely switch shunt reactors and shunt capacitors for voltage regulation that would otherwise be manually switched

I. Schemes that automatically de-energize a line for a non-Fault operation when one end of the line is open

J. Schemes that provide anti-islanding protection

K. Automatic sequences that proceed when manually initiated solely by a System Operator

L. Modulation of HVdc or FACTS via supplementary controls, such as angle damping or frequency damping applied to damp local or inter-area oscillations
Does **Not** Individually Constitute RAS

M. Sub-synchronous resonance (SSR) protection schemes that directly detect sub-synchronous quantities

N. Generator controls such as, but not limited to
   - automatic generation control (AGC)
   - generation excitation
   - fast valving
   - speed governing
Process for New RAS Approvals

• SPP System Control and Protection Working Group (SPCWG) reviews and approves all new or modified RAS

• SPCWG is working on RAS data requirements

• Contact Thomas Teafatiller, SPCWG Staff Secretary Doug Bowman, or SPCWG representative for more information
Implementation Plan for Newly Classified RAS

- Entities with newly classified RAS must be compliant with all applicable standards 24 months from the RAS effective date of 4/1/17
  - Additional 24 months applies only to existing schemes that must transition to RAS due to revised definition
  - Additional time does not apply to future RAS that may be created following implementation of revised definition
Questions or Comments

Jeff Rooker
Lead Compliance Engineer
501-614-3278
jrooker.re@spp.org

Thomas Teafatiller
Senior Compliance Engineer
501-688-2514
Tteafatiller.re@spp.org
2017 CMEP Implementation Plan

Jim Williams
jwilliams.re@spp.org
501.614.3261

Jeremy Withers
jwithers.re@spp.org
501.688.1676
Compliance Monitoring and Enforcement Program (CMEP) Implementation Plan (IP)

• Electric Reliability Organization (ERO) IP is the annual operating plan
  – ERO includes NERC and the Regional Entities

• SPP RE’s Regional IP is Appendix A6 of the ERO IP

• NERC is responsible for collecting and reviewing each region’s IP by October 2016

• During the implementation year, NERC and the Regional Entities may update the IP
  – Emerging issues
  – Monitoring schedules
ERO RISK ASSESSMENT PROCESS

ERO Risk Elements
SPP RE Risk Elements & IP
Registered Entity Risk Assessment
NERC Risk Element Process

- *NERC Risk Elements Guide* will be folded into a new *NERC Guide for Risk-Based Compliance Monitoring Framework* document
- Each year, ERO assesses Bulk Power System (BPS) reliability risks and emerging issues
- NERC develops a matrix and prioritizes risks based on facts and circumstances
NERC Risk Element Process

• NERC identifies standards/requirements and registration categories related to identified risks

• Out of the many NERC requirements, we are focusing on standards that:
  – Encourage proactive compliance to identified risks
  – Strongly contribute to reliability
  – If violated, have a moderate or significant impact on the BPS

• The results of these steps determined which risk elements went into the ERO IP
## 2015, 2016, 2017 Risk Elements Comparison

### Table 2: Critical Comparison of 2015, 2016, and 2017 Risk Elements

<table>
<thead>
<tr>
<th>2015 Risk Elements</th>
<th>2016 Risk Elements</th>
<th>2017 Risk Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cybersecurity</strong></td>
<td>Critical Infrastructure Protection</td>
<td>Critical Infrastructure Protection</td>
</tr>
<tr>
<td><strong>Extreme Physical Events</strong></td>
<td>Extreme Physical Events</td>
<td>Extreme Physical Events</td>
</tr>
<tr>
<td><strong>Infrastructure Maintenance</strong></td>
<td>Maintenance and Management of BPS Assets</td>
<td>Maintenance and Management of BPS Assets</td>
</tr>
<tr>
<td><strong>Monitoring and Situational Awareness</strong></td>
<td>Monitoring and Situational Awareness</td>
<td>Monitoring and Situational Awareness</td>
</tr>
<tr>
<td><strong>Protection System Misoperations</strong></td>
<td>Protection System Failures</td>
<td>Protection System Failures</td>
</tr>
<tr>
<td><strong>Uncoordinated Protection Systems</strong></td>
<td>Event Response/Recovery</td>
<td>Event Response/Recovery</td>
</tr>
<tr>
<td><strong>Long-Term Planning and System Analysis</strong></td>
<td>Planning and System Analysis</td>
<td>Planning and System Analysis</td>
</tr>
<tr>
<td><strong>Human Error</strong></td>
<td>Human Performance</td>
<td>Human Performance</td>
</tr>
<tr>
<td><strong>Workforce Capability</strong></td>
<td>(N/A for 2017)</td>
<td>(N/A for 2017)</td>
</tr>
</tbody>
</table>
ERO Risk Elements: Critical Infrastructure Protection (CIP)

• Remains an area of significant importance

• Risk includes threats and vulnerabilities that result from
  
  (1) System downtime
  
  (2) Unauthorized access
  
  (3) Corruption of operational data

• Requirements:
  
  – **BES Cyber System Categorization**: CIP-002-5.1 R1, R2
  
  – **Electronic Security Perimeter(s)**: CIP-005-5 R1, R2
  
  – **Physical Security of BES Cyber Systems**: CIP-006-6 R1, R2, R3
  
  – **Systems Security Management**: CIP-007-6 R1, R2, R3, R5
ERO Risk Elements: Extreme Physical Events

- Acts of nature or man-made events that cause extensive damage to equipment and systems
- Potential consequences are high enough to warrant increased focus
- Requirements:
  - **Physical Security**: CIP-014-2 R1, R2, R3
  - **Geomagnetic Disturbances**: EOP-010-1 R1, R3
EROb Risk Elements: Maintenance and Management of BPS Assets

- Infrastructure maintenance
- Misalignment between design and actual construction
- We have seen a slight increase in vegetation-related outages

Requirements:
- **Protection Systems**: PRC-005-6 R3, R4, R5
- **Facility Ratings**: FAC-008-3 R6
- **Vegetation Management**: FAC-003-4 R1, R2, R6, R7
ERO Risk Elements: Monitoring and Situational Awareness

- Operators must have the right tools and data to ensure reliability

- Requirements:
  - **Reliability Coordination - Current Day Operations:**
    IRO-005-3.1a R1, R2 (inactive 3/31/2017)
  - **Reliability Coordination Monitoring and Analysis:**
    IRO-002-4 R3, R4 (Enforceable 4/1/2017)
  - **Monitoring System Conditions:** TOP-006-2 R1, R2, R7 (inactive 3/31/2017)
  - **Transmission Operations:** TOP-001-3 R10, R11 (Enforceable 4/1/2017)
ER0 Risk Elements: Protection System Failures

- Ensure system protection is coordinated among operating entities
- Ensure misoperations are analyzed and mitigated
- Requirements:
  - **System Protection Coordination:**
    PRC-001-1(ii) R3, R4, R5
  - **Protection System Misoperation Identification and Correction**
    PRC-004-4(i) R1, R2
ERO Risk Elements: Event Response/Recovery

• Timely restoration following events and preventing events by monitoring SOLs and IROLs

• Requirements:
  – **Emergency Operations Planning**: EOP-001-2.1b R1, R2, R3 (Inactive 3/31/2017)
  – **Emergency Operations**: EOP-011-1 R1, R2 (Enforceable 4/1/2017)
  – **Reporting SOL and IROL Violations**: TOP-007-0 R1, R2, R3, R4 (Inactive 3/31/2017)
  – **Transmission Operations**: TOP-001-3 R12, R14 (Enforceable 4/1/2017)
  – **Reliability Coordination – Responsibilities**: IRO-001-4 R1 (Enforceable 4/1/2017)
ERO Risk Elements: Planning and System Analysis

• Coordinated planning

• Requirements:
  – **Transmission System Planning Performance Requirements**: TPL-001-4 R1, R2, R3, R4
  – **Establish and Communicate System Operating Limits**: FAC-014-2 R1, R5
ERO Risk Elements: Human Performance

• Reducing and preventing errors made by operations personnel

• Requirements:
  – Operating Personnel Communications Protocols: COM-002-4 R5
  – Operations Personnel Training: PER-005-2 R3, R4
SPP RE RISK ELEMENTS AND IMPLEMENTATION PLAN
SPP RE Risk Elements

• SPP RE-specific risk elements based on:
  – Compliance findings
  – Regional events
  – Regional assessments
  – SPP RE staff’s professional judgement
2017 SPP RE Risk Elements: Voltage Support

• Due to the number of Self-Reports indicating failure to maintain reactive support and voltage control

• Ensuring generators provide reactive support and voltage control to protect equipment and maintain reliable operation

  – Generator Operation for Maintaining Network Voltage Schedules: VAR-002-4/R1, R2
Additional Areas of Focus for ERO Risk Elements

• SPP RE is expanding 4 ERO Risk Elements
  – Critical Infrastructure Protection
    ▪ CIP-004-6 R6, CIP-007-6 R6
  – Human Performance
    ▪ COM-002-4 R1, R6
  – Maintenance and Management of BPS Assets
    ▪ FAC-008-3 R1, R2, R3
  – Event Response/Recovery
    ▪ EOP-005-2 R6, R10, EOP-008-1 R4, TOP-001-3 R13
    ▪ TOP-002-2.1b R6, R11 (Inactive 3/31/2017)
    ▪ TOP-002-4 R2 (Enforcement 4/1/2017)
    ▪ VAR-001-4.1 R1
SPP RE Implementation Plan

- SPP RE IP, Appendix A6 in ERO IP, will be posted by Nov. 1
- Continue to engage Registered Entities that request Internal Control Evaluations, Self-Logging and Coordinated Oversight Program for Multi-Regional Registered Entities
- SPP RE will continue to develop and refine tools and templates used for compliance monitoring
- SPP RE will continue to collaborate with NERC, other REs and Registered Entities to identify changes to enhance processes
SPP RE IP

• SPP RE CIP monitoring will focus on Registered Entities with high, medium, and low impact BES Cyber Systems

• Periodic data submittals, and Self-Certification according to the *SPP RE 2017 Reporting Requirements Schedule*
REGISTERED ENTITY RISK ASSESSMENT
Inherent Risk Assessment

- Registered Entity Functions
- ERO & Regional Characteristics
- Events
- RISC

Risk Elements

Initial Scope

Inherent Risk Assessment

Internal Controls Evaluation

Oversight Tool Selection

Input

Scope

Focus

Scope and Focus for Entities not participating in ICE

CMEP Tools

Entity Compliance Oversight Plan
IRA Risk Factors

• When developing IRAs, we apply 18 risk factors to the Registered Entity, such as its critical transmission and load
  – These risk factors are common across all REs, with some regional differences
• Each risk factor has criteria for high, medium and low risk
• Each risk factor has associated standards and requirements
<table>
<thead>
<tr>
<th>Risk Factors</th>
<th>Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td>UFLS Equipment</td>
<td>TO, DP</td>
</tr>
<tr>
<td>UFLS Development and Coordination</td>
<td>PC</td>
</tr>
<tr>
<td>UVLS</td>
<td>TOP, TO, DP</td>
</tr>
<tr>
<td>Load</td>
<td>TO, TSP, DP</td>
</tr>
<tr>
<td>Transmission Portfolio</td>
<td>TO, TOP, BA, RC, TP, PC, Specific GO (as found in applicability sections about long lead lines)</td>
</tr>
<tr>
<td>Voltage Control</td>
<td>TO, TOP, GO, GOP</td>
</tr>
<tr>
<td>Largest Generator Facility</td>
<td>GO</td>
</tr>
<tr>
<td>Variable Generation</td>
<td>BA</td>
</tr>
<tr>
<td>Total Generation Capacity</td>
<td>GO, GOP</td>
</tr>
<tr>
<td>Planned Facilities</td>
<td>TO, GO, TP, RP</td>
</tr>
<tr>
<td>CIP - Control Center Influence</td>
<td>RC, BA, TOP, TO, GOP, GO, DP</td>
</tr>
<tr>
<td>CIP Connectivity</td>
<td>RC, BA, TOP, TO, GOP, GO</td>
</tr>
<tr>
<td>Critical Transmission</td>
<td>TO, TOP, BA, RC, TP</td>
</tr>
<tr>
<td>BA Coordination</td>
<td>BA</td>
</tr>
<tr>
<td>RAS/SPS</td>
<td>TO, GO, DP, RC, TOP</td>
</tr>
<tr>
<td>Workforce Capability</td>
<td>TOP, BA, RC, GOP</td>
</tr>
<tr>
<td>Monitoring and Situational Awareness Tools</td>
<td>TOP, RC, BA, GOP</td>
</tr>
<tr>
<td>System Restoration</td>
<td>RC, TOP, GO, GOP</td>
</tr>
</tbody>
</table>
SPP RE Inherent Risk Assessments (IRA)

- 2016 SPP RE goal is to initiate all Registered Entities IRAs
- “Inherent” is what the Registered Entity is:
  - Control centers, transmission levels, generation, load, etc.
- We consider performance:
  - Compliance history, compliance culture, events
- We put this information into risk factor spreadsheet to determine where entity is on each risk factor
Compliance Oversight Plan

• SPP RE will determine a Registered Entity’s Compliance Oversight Plan based on its IRA

• Compliance Oversight Plan includes:
  – Frequency
  – Method
  – Scope of monitoring activities

• Registered Entities on 2017 monitoring schedule will have IRAs refreshed
Compliance Oversight Plan

• Monitoring Methods
  – On-site audits, Off-site audits, Spot-Checks
  – Self-Certification may be required in conjunction with other monitoring activities
  – Registered Entity is responsible for self-monitoring all applicable requirements

• Monitoring Scope
  – Determined by Registered Entity’s IRA
  – Not limited to the ERO and SPP RE Risk Elements and associated standards
2017 Compliance Monitoring Frequency

- BA/TOP/RC will continue 3-year cycle
- Registered Entities that had a previous compliance monitoring activity 6 years ago
- SPP RE determines a Registered Entity’s IRA indicates the need for monitoring more frequently than every 6 years
- Every Registered Entity will be monitored at least every 6 years
THE SCHEDULE
## 2017 Implementation Plan – Ops & Planning

<table>
<thead>
<tr>
<th>Entity Name</th>
<th>Type of Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>City Utilities Of Springfield, MO (SPRM)</td>
<td>O&amp;P</td>
</tr>
<tr>
<td>AES Shady Point, LLC (AESSP)</td>
<td>O&amp;P</td>
</tr>
<tr>
<td>Kansas Electric Power Cooperative, Inc. (KEPC)</td>
<td>O&amp;P</td>
</tr>
<tr>
<td>Central Valley Electric Cooperative, Inc. (CVEC)</td>
<td>O&amp;P</td>
</tr>
<tr>
<td>City Of Gardner (GARDNER)</td>
<td>O&amp;P</td>
</tr>
<tr>
<td>Oklahoma Gas And Electric Co. (OKGE)</td>
<td>O&amp;P</td>
</tr>
<tr>
<td>City Of Ottawa (OTTAWA)</td>
<td>O&amp;P</td>
</tr>
<tr>
<td>Farmers' Electric Cooperative, Inc. Of New Mexico (FARMCOOPNM)</td>
<td>O&amp;P</td>
</tr>
<tr>
<td>Grand River Dam Authority (GRDA)</td>
<td>O&amp;P</td>
</tr>
<tr>
<td>Green Country Energy, LLC (GREENCOGO)</td>
<td>O&amp;P</td>
</tr>
<tr>
<td>Green Country Operating Services, LLC (GREENCOGOP)</td>
<td>O&amp;P</td>
</tr>
<tr>
<td>Oneta Power, LLC (ONETA)</td>
<td>O&amp;P</td>
</tr>
<tr>
<td>Rita Blanca Electric Inc.</td>
<td>O&amp;P</td>
</tr>
<tr>
<td>USACE - Kansas City District (COEKS)</td>
<td>O&amp;P</td>
</tr>
<tr>
<td>Llano Estacado Wind, LP (LLANOEWIND) SPPRE LRE</td>
<td>O&amp;P-MRRE-SPP</td>
</tr>
<tr>
<td>Northern Iowa Wind Power 1, LLC SPPRE LRE</td>
<td>O&amp;P-MRRE-SPP</td>
</tr>
<tr>
<td>Southwestern Power Administration (SWPA)</td>
<td>O&amp;P</td>
</tr>
<tr>
<td>Louisiana Energy &amp; Power Authority (LEPA)</td>
<td>O&amp;P</td>
</tr>
<tr>
<td>Lafayette Utilities System (LAFA)</td>
<td>O&amp;P</td>
</tr>
<tr>
<td>Lubbock Power And Light (LPLTX)</td>
<td>O&amp;P</td>
</tr>
<tr>
<td>The Empire District Electric Company (EDE)</td>
<td>O&amp;P</td>
</tr>
</tbody>
</table>
## 2017 Implementation Plan - CIP

<table>
<thead>
<tr>
<th>Entity Name</th>
<th>Type of Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Empire District Electric Company (EDE)</td>
<td>CIP</td>
</tr>
<tr>
<td>Cleco Corporation (CLECO)</td>
<td>CIP</td>
</tr>
<tr>
<td>Midwest Energy, Inc. (MIDW)</td>
<td>CIP</td>
</tr>
<tr>
<td>Caney River Wind Project, LLC (CRWP)</td>
<td>CIP</td>
</tr>
<tr>
<td>Sikeston Board Of Municipal Utilities (SIKESTONMO)</td>
<td>CIP</td>
</tr>
<tr>
<td>City Of Ottawa (OTTAWA)</td>
<td>CIP</td>
</tr>
<tr>
<td>Dogwood Power Management, LLC (DPM)</td>
<td>CIP</td>
</tr>
<tr>
<td>North American Energy Services - Dogwood (NAESDOGW)</td>
<td>CIP</td>
</tr>
<tr>
<td>Green Country Energy, LLC (GREENCOGO)</td>
<td>CIP</td>
</tr>
<tr>
<td>Green Country Operating Services, LLC (GREENCOGOP)</td>
<td>CIP</td>
</tr>
<tr>
<td>Lubbock Power And Light (LPLTX)</td>
<td>CIP</td>
</tr>
<tr>
<td>Kansas City Power &amp; Light Company (KCPL)</td>
<td>CIP</td>
</tr>
<tr>
<td>Llano Estacado Wind, LP (LLANOEWIND) SPPRE LRE</td>
<td>CIP-MRRE-SPP</td>
</tr>
<tr>
<td>Northern Iowa Wind Power 1, LLC SPPRE LRE</td>
<td>CIP-MRRE-SPP</td>
</tr>
<tr>
<td>Flat Ridge 2 Wind Energy LLC (FRWEII)</td>
<td>CIP</td>
</tr>
<tr>
<td>KODE Novus Wind I, LLC (KODE)</td>
<td>CIP</td>
</tr>
<tr>
<td>Canadian Hills Wind, LLC (CHW)</td>
<td>CIP</td>
</tr>
<tr>
<td>NAES Corporation - Goodman Energy Center (NAESGEC)</td>
<td>CIP</td>
</tr>
<tr>
<td>Post Rock Wind Power Project, LLC (PRWP)</td>
<td>CIP</td>
</tr>
<tr>
<td>Board Of Public Utilities (Kansas City KS) (BPU)</td>
<td>CIP</td>
</tr>
<tr>
<td>Spearville 3, LLC (SPEAR3)</td>
<td>CIP</td>
</tr>
<tr>
<td>Spinning Spur Wind, LLC (SPINSPUR)</td>
<td>CIP</td>
</tr>
</tbody>
</table>
# 2017 Coordinated Oversight

<table>
<thead>
<tr>
<th>Coordinated Oversight</th>
<th>Type of Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>American Electric Power Service Corp. (AEPW) / RF LRE</td>
<td>CIP-MRRE</td>
</tr>
<tr>
<td>Arbuckle Mountain Wind Farm LLC (AMWF) / RF LRE</td>
<td>O&amp;P/CIP-MRRE</td>
</tr>
<tr>
<td>Blue Canyon II Windpower LLC (BCWII) / RF LRE</td>
<td>O&amp;P/CIP-MRRE</td>
</tr>
<tr>
<td>Blue Canyon Windpower LLC (BCWI) / RF LRE</td>
<td>O&amp;P/CIP-MRRE</td>
</tr>
<tr>
<td>Blue Canyon Windpower V, LLC (BCWV) / RF LRE</td>
<td>O&amp;P/CIP-MRRE</td>
</tr>
<tr>
<td>Blue Canyon Windpower VI, LLC (BC6) / RF LRE</td>
<td>O&amp;P/CIP-MRRE</td>
</tr>
<tr>
<td>Cimarron Windpower II, LLC (CIMW) / Texas RE LRE</td>
<td>O&amp;P/CIP-MRRE</td>
</tr>
<tr>
<td>Cloud County Wind Farm, LLC, (CCWF) / RF LRE</td>
<td>O&amp;P/CIP-MRRE</td>
</tr>
<tr>
<td>Duke Energy Generation Services, Inc. (DEGS) / Texas RE LRE</td>
<td>O&amp;P/CIP-MRRE</td>
</tr>
<tr>
<td>Ironwood Windpower, LLC (IRONWOOD) / Texas LRE</td>
<td>O&amp;P/CIP-MRRE</td>
</tr>
<tr>
<td>ITC Great Plains, LLC (ITCGP) / RF LRE</td>
<td>O&amp;P/CIP-MRRE</td>
</tr>
<tr>
<td>Southwestern Public Service Co. (Xcel Energy) (SPS) / LRE MRO</td>
<td>O&amp;P/CIP-MRRE</td>
</tr>
<tr>
<td>Waverly Wind Farm LLC (Waverly) / RF LRE</td>
<td>O&amp;P/CIP-MRRE</td>
</tr>
</tbody>
</table>
2017 Implementation Plan

• IP development:
  – ERO Risk Elements
  – SPP RE Risk Elements
  – Registered Entity Inherent Risk Assessment
  – Compliance Oversight Plan

• We have covered many of the new standards in previous workshops and videos:
  – 2015 workshop materials
  – 2016 workshop materials (on left)
  – Video Library

• 2017 Compliance documents will be posted here
Root Cause Analysis

Chris Bills
Compliance Enforcement Attorney
cbills.re@spp.org
501.482.2091
Root Cause

An initiating cause of a causal chain which leads to a violation of NERC standards where an intervention could reasonably be implemented to change performance and prevent future violations.
Root Cause Analysis

- Process for identifying Root Cause(s) of a violation
- Development of actionable changes to prevent future violations

- Includes:
  - Contributory factors
  - Risk reduction strategies
  - Action plans
  - Measurement strategies
  - Evaluation of the effectiveness of the plans
Goals of Root Cause Analysis

1) Identify the problem
2) Identify the Root Cause
3) Access the scope of the Root Cause
4) Identify possible solutions
5) Select and implement the solution
6) Evaluate the solution selected
7) Standardize the Process
Goals of Root Cause Analysis

• What happened
• How it happened
• Why it took place
• What changes can be made to prevent reoccurrence
  – Reasonable cost and resources used
  – Reasonable solution to the issue, not always optimal
• Create an outline for mitigating the violation
• Identify other areas the identified Root Cause may be exposing the organization to NERC violations

In your organization...Always ask Why, not Who
Example of Root Cause Analysis

While mowing my yard, my mower suddenly starts violently shaking.

• Drive shaft is bent and blade is damaged
• Hit something mowing
• Only exposed obstacles above the grass in the area are tree roots

Root Cause to the mower damage is the roots!
Example of Root Cause Analysis, cont.

Possible solutions to the Root Cause

• Ask an Arborist why the roots are above ground and how to prevent this from happening
  – What is the cost and time?

• Relocate the roots underground
  – What is the cost?
  – Is it even possible?

• Remove the exposed roots
  – Risk damaging the tree?
Example of Root Cause Analysis, cont.

Other issues that may cause a repeat of the same “violation”

• Do other trees have the same type of exposed roots (or will they in the future)?

• Are there other objects in the yard that can damage the mower? (rocks, children, toys, utility access)

• Is this a sign of soil erosion? (could cause other problems like damage to the house’s foundation, cracked drive, etc.)
Example of Root Cause Analysis cont.

Reasonable mitigation of the Root Cause

• Mow around the roots and any other exposed objects to prevent mower damage

I must also mitigate the actual “violation”

• Repair or replace the mower in time to mow again
Common Performance Categories

Organizational

• Policies and Procedures
  – Even if they were followed, the violation would still have occurred

Physical

• System Operation and Equipment

Human

• Actions or inactions of people
Policies and Procedures

• Are there policies and procedures that apply to the violation?
• Do the policies and procedures cover all the Requirements of the NERC Standards?
• Are the policies and procedures written to eliminate ambiguity?
System Operation and Equipment

• Did the equipment function properly?
• Were test and maintenance outcomes within acceptable standards?
• Is the appropriate equipment utilized for the expected function?
Human Performance

• Was the employee trained?
• Did the employee follow the processes and procedures?
• Was there appropriate management oversight?
• Does the employee and manager understand the associated NERC Standard and Requirement?
Types of Root Cause Analysis

- “5 Whys” analysis
- “5 Whys” expanded
- Fault tree diagram
- Fishbone diagram
“5 Whys”

You discover coolant leaking from a machine.

Coolant is leaking from the machine.  

WHY?

A seal was damaged.

WHY?

Metal shavings got into the coolant.

WHY?

A screen on a coolant recycling pump was broken.

WHY?

The screen is located in a place where it was likely to be damaged by dropped parts.

Root Cause
“5 Whys” Expanded

My car won’t start

Battery is Dead

Battery is 5 years old

Battery won’t hold a charge if the car is not driven daily

Time for a new battery

Alternator belt is weather checked

Replace alternator belt

Original alternator on my 1997 Subaru

Time for a new alternator

Alternator has been making noise
Fish-Bone Diagram

<table>
<thead>
<tr>
<th>Cause</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equipment</td>
<td>Problem</td>
</tr>
<tr>
<td>Process</td>
<td></td>
</tr>
<tr>
<td>People</td>
<td></td>
</tr>
<tr>
<td>Materials</td>
<td></td>
</tr>
<tr>
<td>Environment</td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td></td>
</tr>
</tbody>
</table>

Secondary cause
Primary cause
## 5 Why Root Cause Analysis Template

### Violation:

<table>
<thead>
<tr>
<th>Why 1</th>
<th>Why 2</th>
<th>Why 3</th>
<th>Why 4</th>
<th>Why 5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**What caused the specific violation?**

**List the deficient action**

**Proposed Remediation**

---

List Steps to Mitigate the Root Cause of the Violation

---

What Other Areas May be Affected by the Failures Listed Above - SCOPE

---

How Will the Mitigating Steps Prevent Future Occurrences of This Violation?
## 5 Why Root Cause Analysis Template

### Violation: PRC-005-6 R1

<table>
<thead>
<tr>
<th>Why</th>
<th>What caused the specific violation?</th>
<th>List the deficient action</th>
<th>Proposed Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Why 1</td>
<td>Reynolds Substation battery bank electrolyte levels were not checked (4 months)</td>
<td>Only checked every 6 months, was performed at the previous 6 month interval</td>
<td>Battery inspections and tests must be scheduled at least one month in advance of the deadline with a reminder notice sent two weeks prior to the deadline.</td>
</tr>
<tr>
<td>Why 2</td>
<td>Technician was not aware of the change in the Procedure Manual changing the check interval from 6 months to 4 months</td>
<td>Technician signed off that he received the manual but did not have to acknowledge that he understood the changes.</td>
<td>Memo or email must be distributed to all pertinent staff at the time of procedural changes</td>
</tr>
<tr>
<td>Why 3</td>
<td>New Procedural Manual was distributed but not explained</td>
<td>Training only conducted annually (in Jan.) and change made July 1.</td>
<td>New Procedural Manuals must be distributed and acknowledged within one week of changes.</td>
</tr>
<tr>
<td>Why 4</td>
<td>Training not conducted each time there is a substantive change to the Procedure Manual</td>
<td>Training manager did not know that the changes in the Procedure Manual were due to a change in the NERC Standards</td>
<td>Change the policy to ensure that there is training provided each time there is a change in the Procedure manual</td>
</tr>
<tr>
<td>Why 5</td>
<td>Training Manager did not know of changes to the NERC Standards</td>
<td>The training manager was not part of the Procedural Manual drafting team</td>
<td>Training Manager is to be added to the Procedural Manual drafting team</td>
</tr>
</tbody>
</table>
Original Root Cause Statement

The Root Cause of this violation was that the technician did not change the inspection interval to 4 months.

Mitigation Milestones

1. Change the inspection interval to 4 months on the technicians calendar by 12/1/2016

2. Check the Reynolds electrolyte levels by 11/1/2016
Root Cause Statement and Milestones

The Root Cause of this PRC-005-3 Violation was that the training manager did not know about NERC Standards changes and did not provide supplemental training throughout the year to ensure technicians understand changes to the Procedure Manual reflecting NERC Standards changes.

Mitigation Plan Milestones:

1. Inspect the Reynolds Battery electrolyte levels by 9/30/2016
2. Training on the New PRC-005-3 requirements shall be completed by 10/1/2016
3. Policy Manual will be changed to require training within one week of changes to the Procedural Manual by 11/15/2016
4. Training Manager will be added to the invitation email list by 12/1/2016
5. The Battery test for 12/31/2016 must be scheduled by 12/1/2016
## 5 Why Root Cause Analysis Template

### Violation: FAC-008-3 RG

<table>
<thead>
<tr>
<th>Why 1</th>
<th>Why 2</th>
<th>Why 3</th>
<th>Why 4</th>
<th>Why 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmission facility rating was not consistent with the Facilities Rating Methodology</td>
<td>Engineering did not change the Facility Ratings Spreadsheet after the substation technician changed a bad ASCR jumper to a AAC jumper</td>
<td>Engineering did not know the jumper was changed</td>
<td>Technician did not note the new equipment specification on the work order</td>
<td>Thought the jumpers on his truck had the same rating as those in service.</td>
</tr>
</tbody>
</table>

### What caused the specific violation? | List the deficient action | Proposed Remediation |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Facilities Rating Spreadsheet did not show all current equipment in production</td>
<td>Assumed the equipment passed inspection and was not replaced</td>
<td>Any substation equipment changes must be updated in the spreadsheet within 5 days of receiving the completed work order</td>
</tr>
<tr>
<td>New equipment was not mentioned on the work order</td>
<td></td>
<td>Look for affirmative language on the work order outlining the equipment change or that no equipment was replaced</td>
</tr>
<tr>
<td>No Field on the work order to list changed equipment</td>
<td></td>
<td>All work orders must state results of equipment inspections</td>
</tr>
<tr>
<td>Not enough experience with equipment ratings</td>
<td></td>
<td>Work orders must state that no equipment was replaced or state equipment was replaced with specifics on both the old and new equipment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Get manager verification when changing equipment and work order sign-off</td>
</tr>
</tbody>
</table>
FAC-008-3 R6

Transmission Facility Rating was not consistent with the Facilities Rating Methodology

- Engineering did not change the Facility Ratings Spreadsheet after the substation technician changed a bad ASCR jumper to a AAC jumper
- Technician did not replace the bad jumper with the same type and size jumper
- Technician did not have a ASCR jumper on his truck
- Facilities storage was over an hour drive away to get the same ASCR jumper that is being replaced

- Engineering did not know the jumper was changed
- Technician did not note the new equipment specification on the work order
- Not practicable to keep all types of equipment on the truck. ASCR and AAC jumpers perform the same task for this function
Original Root Cause Statement

The Root cause of this violation was that the Engineering department did not update the Facilities Rating Spreadsheet

Mitigation Milestones

1. Update the Facility Ratings Spreadsheet by 11/1/2016
Root Cause Statement and Milestones

The Root Cause of this FAC-008-3 R6 is that the work order form does not provide all the necessary information to the engineering team to make necessary changes to the facilities ratings spreadsheet.

Mitigation Plan Milestones:

1. Change work order form to include fields stating what equipment was removed and what equipment was placed into service by 11/1/2016.

2. Change work order form to include fields stating what equipment was inspected and the results of the inspection by 11/1/2016.

3. Change the Policy Manual to require a manager to sign off on all work orders prior to them being sent to engineering by 12/15/2016.

No evaluation of potential threats and vulnerabilities of physical attack to the S-Austin transmission Substation. Thought we could use the evaluation from the K-Perry substation. Did not consider unique external (environmental) differences of location. Did not consider the sub-requirements of R4 when conducting evaluations.

<table>
<thead>
<tr>
<th>Why 1</th>
<th>Why 2</th>
<th>Why 3</th>
<th>Why 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>No evaluation of potential threats and vulnerabilities of physical attack to the S-Austin transmission Substation.</td>
<td>Thought we could use the evaluation from the K-Perry substation.</td>
<td>Did not consider unique external (environmental) differences of location.</td>
<td>Did not consider the sub-requirements of R4 when conducting evaluations.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>List the deficient action</th>
<th>Proposed Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Same design as the K-Perry Substation.</td>
<td>Perform risk evaluation on S-Austin substation.</td>
</tr>
<tr>
<td>Did not consider risks outside physical perimeter.</td>
<td>Develop risk analysis for environmental risks.</td>
</tr>
<tr>
<td>Only considered threats from fence line inward.</td>
<td>Evaluate our physical perimeter as well as other local threats unique to this location.</td>
</tr>
<tr>
<td>A copy of the Standard and all requirements was not provided to the team performing evaluations.</td>
<td>Provide the standard and requirements to the evaluation team and perform risk evaluation on S-Austin.</td>
</tr>
</tbody>
</table>
Original Root Cause

The Root Cause of this violation was that the evaluation team used the same physical evaluation for S-Austin substation as K-Perry substation

Mitigation Milestones

1. Perform the evaluation on S-Austin
Root Cause Statement and Milestones

The Root Cause of this CIP-014-2 R4 violation was that the risk evaluation team did not know all the requirements and sub-requirements of the standard, so they failed to consider and document all the external security risks.

Mitigation Milestones

1. Provide the evaluation team with all the standards and requirements required for the re-evaluation of S-Austin by 10/1/2016
2. Perform an R4.1-R4.3 risk analysis for S-Austin by 12/31/2016
3. Create the full evaluation of potential threats and vulnerabilities of physical attack for S-Austin by 2/1/2017
4. Review all evaluations of other transmission stations and substations to ensure compliance with the R4 requirement and sub-requirements by 5/1/2016
Paths To Mitigation

• When can I submit Mitigating Activities?
• When is a Mitigation Plan required?
• When must Evidence be submitted?
• When should I submit Certification of Completion?
Key Take-Aways

• Root cause analysis is a requirement
• Root cause must be addressed in Mitigation Plan or Mitigating Activities
• Addressing root cause prevents recurrence of violation
• Thorough root cause analysis is a good practice for improving reliability and preventing future violations
• Communicate with the Enforcement Engineers
  – Bob Reynolds, O&P
  – Jenny Anderson, CIP
Questions?

Chris Bills
Compliance Enforcement Attorney
501.482.2091
cbills.re@spp.org
General Manager’s Report

Sept. 21, 2016

Oklahoma City, Oklahoma

Ron Ciesiel
SPP RE General Manager
Risk-Based Compliance

• 40 Inherent Risk Assessments (IRA) completed
  – Summary report submitted to NERC
• 4 Internal Control Assessments completed
  – Removed requirements from auditors’ review
  – Reduced sample size
• Operations & Planning has completed:
  – 3 of 4 on-site audits
  – 14 off-site audits
    ▪ 9 off-site completed
    ▪ IRAs reduced 4 off-site audits to Spot-Checks
• CIP has 4 on-site V6 audits that began in July
**Most Violated Standards**

Based on rolling 12 months through 8/31/16 [Represents ~ 72% of total violations]

<table>
<thead>
<tr>
<th>SPP RE Rank</th>
<th>Standard</th>
<th>Description</th>
<th>Violations Current Period</th>
<th>Violations Previous Period</th>
<th>Δ</th>
<th>Risk Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1*</td>
<td>PRC-005</td>
<td>Protection System Maintenance</td>
<td>18</td>
<td>4</td>
<td>+14</td>
<td>High/Med.</td>
</tr>
<tr>
<td>2*</td>
<td>CIP-007</td>
<td>Systems Security Management</td>
<td>8</td>
<td>20</td>
<td>-12</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>3*</td>
<td>FAC-008</td>
<td>Facility Ratings</td>
<td>6</td>
<td>2</td>
<td>+4</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>4*</td>
<td>CIP-004</td>
<td>Personnel &amp; Training</td>
<td>6</td>
<td>5</td>
<td>+1</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>5*</td>
<td>VAR-002</td>
<td>Network Voltage Schedules</td>
<td>6</td>
<td>5</td>
<td>+1</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>6</td>
<td>CIP-005</td>
<td>Electronic Security Perimeters</td>
<td>5</td>
<td>13</td>
<td>-8</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>7</td>
<td>PRC-006</td>
<td>Automatic UFLS</td>
<td>4</td>
<td>0</td>
<td>+4</td>
<td>High/Lower</td>
</tr>
<tr>
<td>8*</td>
<td>CIP-006</td>
<td>Physical Security - Cyber Assets</td>
<td>4</td>
<td>12</td>
<td>-8</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>9</td>
<td>EOP-004</td>
<td>Event Reporting</td>
<td>3</td>
<td>0</td>
<td>+3</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>10</td>
<td>PER-005</td>
<td>Operations Personnel Training</td>
<td>3</td>
<td>0</td>
<td>+3</td>
<td>Med./Lower</td>
</tr>
<tr>
<td>All</td>
<td>SPP RE Top 10 Total Incoming</td>
<td>63</td>
<td>61</td>
<td>2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The current period is the most recent 12 months.
The previous period is the previous 12 months.
* 2016 NERC Top 10
VEGETATION CONTACTS

**REPORTABLE**
- NERC: Q2-2016
- SPP RE: Q4-2015

**ACTIONABLE**
- NERC: Q3-2015
- SPP RE: Q3-2010

(Q2-2016 LAST OFFICIAL REPORT)
SPP RE Regional Events Q3 Through 9/12/16

• One category 1a. *Outage of multiple elements*
SPP RE Misoperation Report as of Q2-16

Relay Operational Performance - Success Rate

- **Correct Operations**
  - Q1-11: 85.2%
  - Q2-11: 88.8%
  - Q3-11: 82.9%
  - Q4-11: 84.6%
  - Q1-12: 85.7%
  - Q2-12: 86.3%
  - Q3-12: 86.0%
  - Q4-12: 87.3%
  - Q1-13: 88.2%
  - Q2-13: 92.3%
  - Q3-13: 92.3%
  - Q4-13: 91.8%
  - Q1-14: 90.6%
  - Q2-14: 90.1%
  - Q3-14: 90.8%
  - Q4-14: 88.8%
  - Q1-15: 87.8%
  - Q2-15: 90.1%

- **Rolling 4 Quarter Average**
  - Q1-11: 89.8%
  - Q2-11: 91.2%
  - Q3-11: 91.8%
  - Q4-11: 89.3%
  - Q1-12: 87.2%
  - Q2-12: 86.3%
  - Q3-12: 86.0%
  - Q4-12: 88.3%
  - Q1-13: 88.3%
  - Q2-13: 92.3%
  - Q3-13: 91.8%
  - Q4-13: 88.8%
  - Q1-14: 90.6%
  - Q2-14: 90.8%
  - Q3-14: 90.1%
  - Q4-14: 87.8%
  - Q1-15: 87.8%
  - Q2-15: 90.1%

- **Overall Trends**
  - The overall trend shows an improvement in the success rate over the quarters.
  - The rolling 4 quarter average gives a clearer picture of the performance trends over time.
Rolling 4 Quarter Operation Success Rate by Voltage Category
SPP RE
Ending Second Quarter 2016
Outreach

• **Workshops**
  – Mar. 28-29, Spring 2017 Workshop: Little Rock
  – June 27-28, CIP 2017 Workshop: Little Rock
  – Oct. 24-25, Fall 2017 Workshop: Dallas

• **Trustee Meeting**
  – Jan. 30, 2017: Dallas
  – Apr. 24, 2017: Tulsa
  – July 24, 2017: Denver
  – Oct. 30, 2017: Little Rock
New Standards: October 1, 2016

- **CIP-004-6 Cyber Security – Personnel & Training (Requirement 4.2)**
- **FAC-003-4 Transmission Vegetation Management**
- **MOD-31-2 – Demand and Energy Data**
New Standards: January 1, 2017

- IRO-010-2 Reliability Coordinator Data Specifications and Collection (Requirements R1 and R2)
- TOP -003-3 Operational Reliability Data (all Requirements except R5)
New Standards: April 1, 2017

- CIP-003-6 - Cyber Security - Security Management Controls (Requirements 1.2-2)
- CIP-010-2 – Cyber Security Configuration change Management and Vulnerability Assessments (Requirement 4)
- EOP-004-3 – Event Reporting
- EOP-010-1 — Geomagnetic Disturbance Operations
- EOP-011-1 – Emergency Operations
- FAC-010-3 – System Operating Limits Methodology for the Planning Horizon
New Standards: April 1, 2017

- FAC-011-3 – System Operating Limits Methodology for the Operations Horizon
- IRO-001-4 – Reliability Coordination: Responsibilities
- IRO-002-4 – Reliability Coordination: Monitoring and Analysis
- IRO-008-2 – Reliability Coordinator Operational Analyses and Real-time Assessments
- IRO-010-2 – Reliability Coordinator Data Specification and Collection (Requirement R3)
- IRO-014-3 – Coordination Among Reliability Coordinators
New Standards: April 1, 2017

• IRO-017-1 – Outage Coordination
• MOD-029-2a – Rated System Path Methodology
• MOD-030-3 – Flowgate Methodology
• PRC-010-1 – Undervoltage Load Shedding
• PRC-015-1 – Remedial Action Scheme Data and Documentation
• PRC-016-1 – Remedial Action Scheme Misoperations
• PRC-017-1 – Remedial Action Scheme Maintenance and Testing
New Standards: April 1, 2017

- PRC-023-4 – Transmission Relay Loadability
- TOP-001-3 – Transmission Operations
- TOP-002-4 – Operations Planning
- TOP-003-3 – Operational Reliability Data (Requirement R5)
New Standards: April 2, 2017

- PRC-004-5(i) – Protection System Misoperation Identification and Correction
- PRC-010-2 – Undervoltage Load Shedding
New Standards: July 1, 2017

- **CIP-004-6-Cyber Security – Personnel & Training** (Requirements 2.3, 4.3, 4.4)
- **CIP-006-6-Cyber Security - Physical Security of BES Cyber Systems** (Requirement 3.1)
- **CIP-008-5-Cyber Security – Incident Reporting and Response Planning** (Requirement 2.1)
- **CIP-009-6-Cyber Security – Recovery Plans for BES Cyber Systems** (Requirement 2.1-2.2)
- **CIP-010-2-Cyber Security Configuration Change Management and Vulnerability Assessments** (Requirement 3.1)
New Standards: July 1, 2017

- MOD-033-1 — Steady-State and Dynamic System Model Validation