Issue 2
2018 March/April

INSIDE THIS ISSUE

A Note from the President 1
From the Board 2
Analyzing EMS Outages 3-5
EMS Outages and Compliance . . 6
EMS News 7
EMS Reference Document 8
Control Center Ergonomics . . 9-10
E-ISAC 11-12
The Seam 13
The Lighthouse 14-16
Regulatory Affairs 17
Standards Update 18-19
Watt's up at RF 20-21
Calendar 22
RF Members 23

ReliabilityFirst Corporation
3 Summit Park Drive
Suite 600
Cleveland, OH 44131
Main Phone: (216) 503-0600

Web: www.rfirst.org
Follow us on

RELIABILITY FIRST

A Note from the President

Tim Gallagher, President and CEO

Dear Stakeholders:

Event Analysis and Situational Awareness is an area I know is on many of your minds, and is also an area where a lot of work is happening behind the scenes at RF and across the ERO. This issue is designed to highlight some of that work, particularly regarding EMS events. The decision to focus this issue, and part of our upcoming Reliability Workshop, on Situational Awareness and EMS issues is to ensure our entities have an understanding of these types of events so we can work together to reduce the number that occur. It also allows us to share lessons learned and themes we have gathered from our work with you and highlight the hard work taking place across the ERO to fully understand and mitigate risks related to situational awareness.

For example, we highlight our work with NERC on the Risk and Mitigations for Losing EMS Functions Reference Document. Event Analysis is an area where we partner closely with NERC so we can get a holistic view, which is part of what we think makes this reference document so valuable. We also share insight on Standards to consider after an EMS outage and some takeaways from working with Hoosier on how ergonomics can impact control room design. I personally thank the Hoosier team for their collaboration with us.

Another article I would like to draw your attention to is written by Bill Lawrence, the Director of Electric Information Sharing and Analysis Center (E-ISAC) at NERC. In the article, he provides an overview of our industry security communications channel and related activities.

On the topic of situational awareness, my position provides a unique visibility that I would like to share more proactively. In the next few weeks, I will issue the first Leadership Letter to CEO's in the RF footprint. We have a long history of collaborating with companies and helping to communicate challenges that we see in the field and approaches that have proven successful to address them. In this spirit, I intend to share important things that cross my desk that I would want to know if I was one of our stakeholder's CEOs. These communications will be succinct, written at a high level, and may range from a few data points for your awareness to potential questions a CEO may find useful to ask his or her staff. My hope is that this additional awareness will prove valuable and useful for our stakeholders.

Finally, I will close with personally congratulating Jim Robb as he transitions to NERC CEO this week. I am pleased to have him leading us into the future and look forward to working to support his vision of the ERO. Jim is an outstanding leader, a deep thinker, and a good friend. I am very confident Jim will do an outstanding job working with the industry, Regions, and regulatory agencies toward advancing our performance and achieving our collective mission.

Tim

From the Board

RF Holds First Quarter Board of Directors Meetings in Cleveland, OH

RF held its First Quarter Board of Directors meetings at its offices in Cleveland, OH from March 14-15, 2018. RF staff and special guests provided presentations on various topics. Highlights included the following:

David Godfrey

Rob Eckenrod

Tim Aliff

- During the Compliance Committee meeting, David Godfrey, Vice President of Entity Oversight at WECC, and Kristen Senk, Senior Counsel at RF, discussed the 2018 CIP Themes Report, a joint effort of ReliabilityFirst, WECC, and SERC to identify common deficiencies and mitigation strategies related to compliance with the CIP Standards. The 2018 CIP Themes Report is now available on the RF website.
- During the Board of Directors meeting, Rob Eckenrod, Chief Compliance Officer at PJM Interconnection, LCC (PJM), and Tim Aliff, Director of System Operations, Midcontinent Independent System Operator (MISO) discussed the performance of the Bulk Electric System (BES) in the MISO and PJM footprints during the 2017-2018 winter weather events and how it compared to the 2014 polar vortex. They also discussed lessons learned from the 2017-2018 winter.
- Rob Eckenrod and Tim Aliff also presented on PJM and MISO's perspectives on resilience, and PJM and MISO's filings in response to the recently opened FERC proceeding (Docket No. AD18-7-000) to evaluate the resilience of the BES in Regions operated by Regional Transmission Organizations.
- Brian Thiry, Principal Analyst, Event Analysis and Situational Awareness at RF, presented and led a discussion on trends, themes, and mitigation strategies identified during EMS-related events. He also discussed NERC and RF's EMS outreach efforts and events, and recently published EMS Lessons Learned documents and reference documents.
- Jeff Mitchell, Director of Reliability Assessment and Performance Analysis at RF, discussed Wisconsin Public Service's recent request to transfer to ReliabilityFirst, and the timeline and next steps in the process.
- Ray Sefchik, Director of Reliability Assurance and Monitoring at RF, provided an overview of GridEx IV and ReliabilityFirst's participation in the exercise.

RF Board of Directors

and

Committee Meetings

will be held

at the RF offices in

Cleveland, OH on

May 23-24, 2018

Click here for details

Analyzing EMS Outages

By: Brian Thiry, Principal Analyst

Outages and the Events Analysis Process Overview, Themes, and Lessons Learned

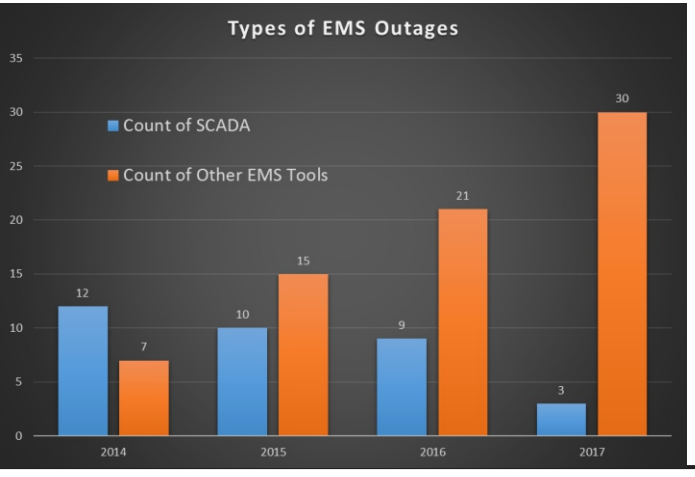
Last year, RF's Events Analysis and Situational Awareness (EASA) team analyzed EMS outages going back to 2014 to better determine the breadth and severity of these events.

Through the Event Analysis Process (EAP) , the Regions analyze these outages, also known as category 1h events, to determine the root cause, contributing causes, and mitigating circumstances. This is done through NERC's Cause Code Assignment Process (CCAP).

The purpose of this article is to share our findings and give you an idea of what we do with the data collected through the EAP.

Last year, RF analyzed 107 new and historical EMS outages to discover trends, lessons learned, and best practices. These events are typically communicated to RF through the EOP-004 process where an entity submits a disturbance report upon the loss of EMS functionality for greater than 30 minutes.

Some of the events submitted involved a complete loss of monitoring and control, while others were an outage of EMS tools and capabilities such as State Estimation, Real-Time Contingency Analysis, or Inter-



Lessons Learned 2017 (4)

LL20170503	Loss of SCADA Operating and Monitoring Ability	Communications	5/16/2017
LL20170502	Line Frequency Excursion Causes UPS Shutdown and Control Center Evacuation	Communications	5/16/2017
LL20170501	Loss of Monitoring Due to Authentication Software Update	Communications	5/16/2017
LL20170302	Loss of State Estimator due to Propagated Database Values With Invalid Data	Communications	3/14/2017

Lessons Learned 2016 (10)

LL20161202	SCADA System Software Design Flaw Prevented Processing of Alarms and Events	Communications	12/6/2016
LL20161201	Loss of ICCP – Local Control Center Notifications	Communications	12/6/2016
LL20161103	Loss of ICCP due to Database Sizing Issue	Communications	11/1/2016
LL20161102	Failover Configuration Leads to Loss of EMS	Communications	11/1/2016
LL20161101	Redundant Systems May Not Cold-Start Unless Fully Intact to Prevent Dual Primary Operation	Communications	11/1/2016
LL20160701	Unavailability of the Transmission Stability Limits Calculation Application	Communications	7/5/2016
LL20160604	ICCP Communication Failure Due to Firewall Patch Update	Communications	6/14/2016
LL20160603	Loss of Monitoring Capabilities Due to FEP Hardware Malfunction	Communications	6/14/2016
LL20160602	SCADA Failover Event	Communications	6/14/2016
LL20160501	Control Center Loss of SCADA Control and Monitoring Capability	Communications	5/24/2016

Control Center Protocol. For more information regarding the types of EMS outages, please see RF's newsletter article on the Operating Committee Reference Document Risks and Mitigations for Losing EMS Functions.

Following the submittal of an EOP-004 form, the registered entity typically submits a Brief Report to RF which includes details of the EMS outage. These details include the causes, a sequence of events, and the mitigating circumstances. The EASA team then works with the entity to document the root-cause, contributing causes, and mitigating circumstances.

If an event includes facts and information that may be particularly useful to share with the industry, RF may work with the entity to create a Lessons Learned document. Currently there are over 40 such Lessons Learned documents that are posted on NERC's website with the category "Communications," most regarding category 1h events. The table below show EMS-related Lessons Learned documents from 2017 and 2016.

Types of EMS outage occurrences

RF analyzes the number of EMS outage occurrences, by type. Even though there has been an overall increase in the number of EMS-related outages, a significant trend is that there are less SCADA outages (which involve the loss of monitoring and control). However, there was an increase in State Estimator outages, which could be the result of the following:

- Changing reporting requirements (eliminating the category 2b and creating the category 1h.v events),
- Requirements for Transmission Operators to run Real-Time Assessments introducing new EMS tools and technologies,
- Expanding external models to create visibility overlaps with neighbors, and
- EMS tuning issues where settings needed to be calibrated due to changing dispatches and generation retirements.

Continued on page 4

Analyzing EMS Outages

Continued from page 3

Causes of EMS Events

Next, RF looked at the 2014-2017 events to determine if there were trends with the causes. To organize the data, RF developed five general themes to classify each event.

1.) **Software:** Outages due to a software bug or database issue with the EMS. Sometimes software crashes or fails, and the entity works with the vendor (typically GE, Siemens, OSI, or ABB) to repair, patch, or fix the software related concern.

2.) **Data:** Outages due to external data that results in the State Estimator not converging. This could be data that is not accurately modeled, data of poor quality, or a lack of data due to a communications-type issue. These issues are resolved by communicating with neighboring entities to upgrade the external model and reconcile any data errors.

3.) **Loss of Power:** Power outages to a control center or data center that result in the loss of EMS functionality. Mitigating actions include looking at the design and redundancy of power supplies to ensure there is not a single point of failure.

4.) **Maintenance:** Any type of change to the EMS or supporting systems that results in a SCADA, ICCP, or State Estimator outage. These outages are often due to change-management issues.

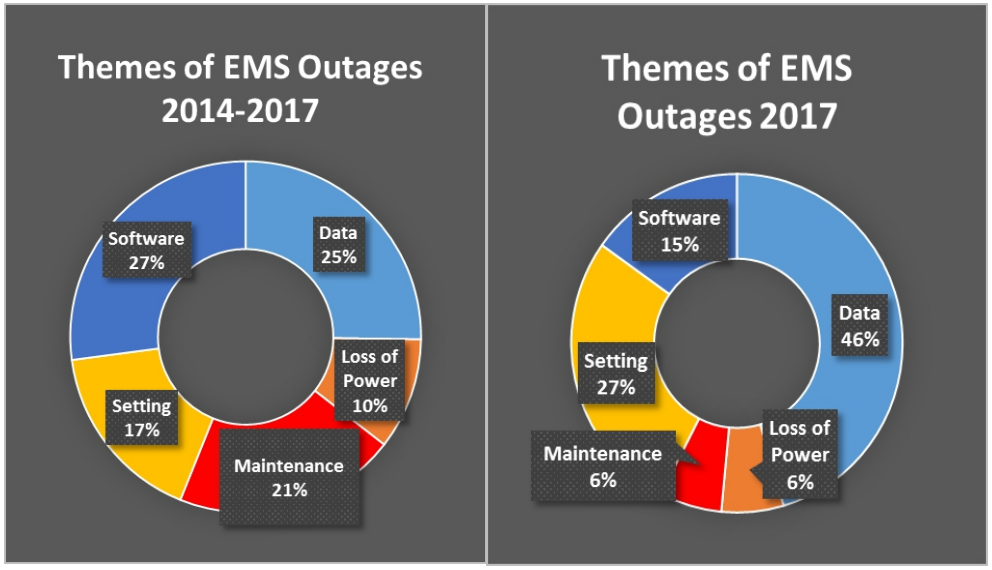
5.) **Settings:** Any type of EMS outage due to less-than-adequate EMS system settings or parameters. Oftentimes settings are adequate upon installation, but due to topology changes or dispatch changes, settings need to be adjusted (tuned/calibrated) to help the State Estimator converge while maintaining a quality solution.

The first pie graph shows the distribution for all the EMS events from 2014, and the second graph shows the 2017 data. In the RF Region, there has been a significant reduction of maintenance and loss of power events.

Based on these events, change-management controls appear to be improving and RF is seeing less instances of outages caused by software patches or changes to the EMS. However, RF has seen an increase in data and settings-related outages. This has caused the increase of State Estimator outages as there are times where the data or settings result in non-convergence.

RF is actively engaged with NERC to write two new Lessons Learned documents covering these issues; further communication will follow when these are posted.

Next, RF looked at the cause-codes that are developed via the CCAP process to determine which codes were coming up most often and when. The cause-codes have



nine general categories (called A-level categories), indicated below.

- A1: Design/Engineering
- A2: Equipment/Material
- A3: Individual Human Performance
- A4: Management/Organization
- A5: Communication
- A6: Training
- A7: Other (External)
- AX: Overall Configuration
- AZ: Information to determine cause less-than-adequate (LTA)

The cause-codes are broken into more detailed categories (called B and C-level categories) for more granular causes. However, RF focused on the A-level causes and how they were mapped to the five categories listed above. This helps determine not only what happened, but why.

The mitigations can then focus on these contributing causes to reduce the number and duration of EMS occurrences. For example, data issues need to focus on design/engineering while maintenance issues are often attributed to management/organization (specifically change-management, work planning, and job scoping).

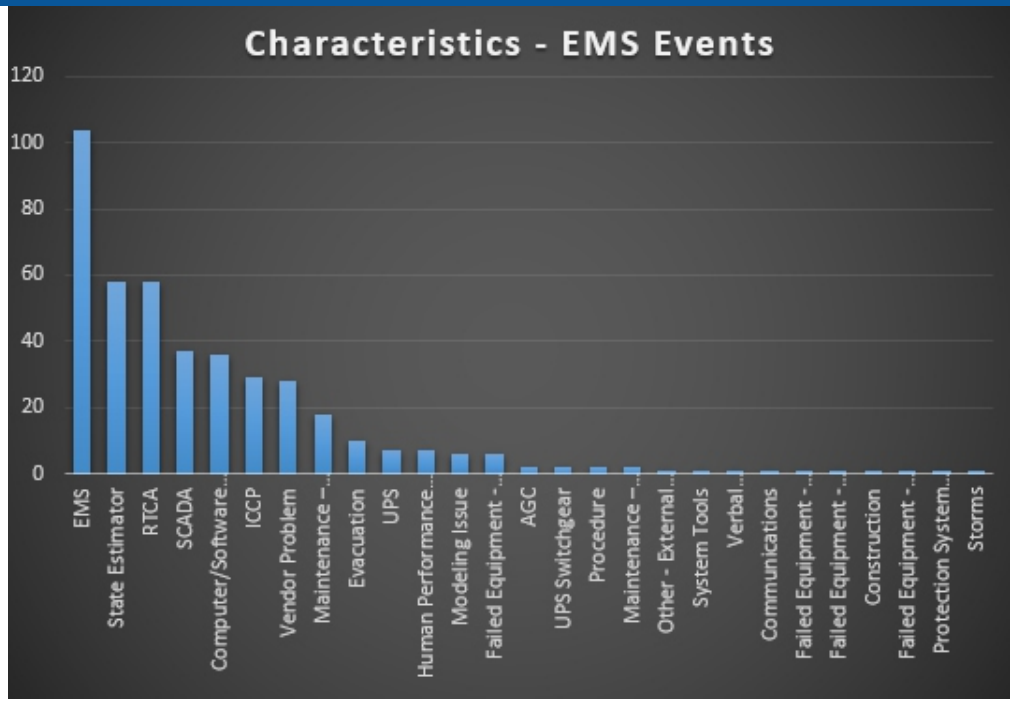
Continued on page 5

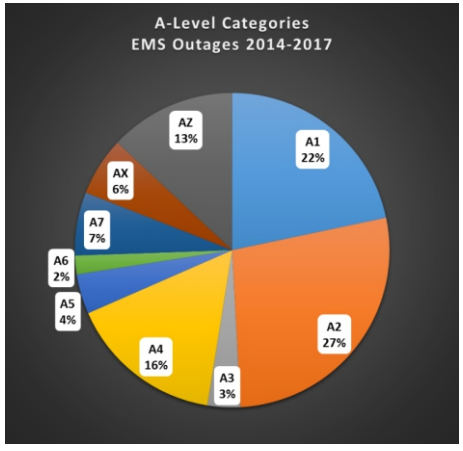
Analyzing EMS Outages

Continued from page 4

From the charts below, almost half of the causes were due to design and equipment. Approximately 13% of the cause-codes were AZ (unknown) where the vendor and entity could not determine a specific root-cause following a review of logs and circumstances. Very few EMS-related outages analyzed 2014-2017 are due to training or communication being LTA.

Finally, RF analyzed the characteristics of the EMS outages. Looking at the chart to the right, the largest characteristics are the natures of occurrence (type) such as EMS, State Estimator, RTCA and SCADA. One interesting characteristic that occurred over a quarter of the time was Vendor Problem. In these cases, the entity flagged some type of vendor issue with the EMS system that contributed to the outage. As NERC collects these events, the data provides the opportunity to give vendor feedback. Vendors are also invited to the annual NERC Monitoring and Situational Awareness Conference held every fall where industry meets and discusses not only EMS-outages, but EMS enhancements, lessons learned, and best practices.





A Codes	A1 Design / Engineering	A2 Equipment / Material	A3 Individual Human Performance	A4 Mgt / Org	A5 Communication	A6 Training	A7 Other	AX Overall Configuration	AZ Information LTA
Data	28	28	1	4	1	1	3	4	10
Software	15	33	1	6	4	4	9	2	18
Loss of Power	15	17	2	12	4	1	6	0	7
Setting	16	7	6	8	3	1	3	14	9
Maintenance	16	29	4	36	5	1	6	5	10

Analyzing this data has been useful as it helps RF in its collaboration with NERC on the EMS Working Group, writing Lessons Learned Documents, and participating in the Monitoring and Situational Awareness Conference.

It allows RF to answer questions on why EMS-related events are happening and work with entities on mitigation.

RF will continue posting documents and publications regarding EMS-outages on our updated website in the Knowledge Center as part of our process for disseminating information regarding the risks and mitigations involving the loss of Situational Awareness.

RF is proud that recent studies have shown EMS run-time to be at 99.99%, and we will continue to analyze the 0.01% of the time these systems are not working as they should.

Note: in the Operating Committee Reference document, NERC uses four categories (Communications, Software, Facility, and Maintenance).

EMS Outages and Compliance Concerns

By: Derek Kassimer

Standards to Consider following an EMS Outage Part I

The Operating Committee Reference Document "Risk and Mitigations for Losing EMS Functions" highlights the work the Event Analysis Program (EAP) does with analyzing EMS outage events, tracking and trending data, creating Lessons Learned documents, and hosting the Monitoring and Situational Awareness Conference. However, a very common question following an EMS outage is, ***"Is the EMS outage a violation or not?"*** There is not a NERC Reliability Standard directly related to the functionality of an EMS, so this is not a simple answer. This article walks you through a compliance assessment (CA) and the NERC Standards to consider following an EMS outage.

The CMEP Implementation Plan[1] recommends conducting a voluntary CA following all events, including EMS outage events. The CA process is a complementary review of an event or disturbance that focuses on the reliability impact of the event, followed by an evaluation of compliance with related Reliability Standards. The CA's are particularly useful if Compliance Monitoring were to ask for a review of an event during an audit or spot-check. The CA would help the entity remember the event details, what standards were considered in the review and the entity's rationale on deciding whether or not to self-report any issues.

The first standard to consider following an EMS outage is EOP-004-3 (Event Reporting Standard). Requirement 2 mandates that entities report events per their Operating Plan within 24 hours. This Operating Plan must include the event types listed in Attachment A of the standard which includes reporting the "Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (i.e. State Estimator or Contingency Analysis) is rendered inoperable." This may be confusing because the loss of State Estimator or Contingency Analysis is not a "complete loss of monitoring" as the entity typically still has SCADA. It is RF's position that State Estimator and Contingency Analysis outages (while not a complete loss of monitoring) should be reported in accordance with EOP-004-3. The CA should ensure that all proper notifications and reporting are performed in accordance with EOP-004-3

Another standard to consider is TOP-001-3 (Transmission Operations Standard). Requirement 9 discusses the responsibility to notify the Reliability Coordinator (RC) for both planned and unplanned outages of telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between the affected entities. Following an EMS outage, discuss with operations personnel if the proper notifications were made to the RC. This is important because the RC provides overlapping coverage regarding the situational awareness of your footprint when you are unable to monitor your system, or if there is a loss of State Estimation or Contingency Analysis. If controls are not already in place to ensure that this notification takes place, consider additional alarming to help remind the operators or shift supervisor to make this notification. Additionally, if you are using the monitoring and assessment capabilities of the RC to serve as a backup, ensure that the RC's EMS is fully functional for your area. Corrupted or missing data from your system may negatively impact the RC's systems.

When a CA is completed for an EMS event and an entity determines that all compliance responsibilities have been met, there may be an opportunity to reflect on other items outside of compliance. Review how well your personnel, procedures, policies, controls, etc. performed during the event and determine if modifications need to be made.

[1] See Appendix B - Compliance Assessment Report of the 2017 ERO Enterprise Compliance Monitoring and Enforcement Implementation Plan.

NERC Standards to Consider with an EMS Outage Part 1

The highlighted Standards are covered in this issue, the remaining ones will be covered in Part II in our next issue.

NERC Standard	Req	Topic
TOP-001-3	13	Performance of Real-Time Assessments every 30 minutes
TOP-001-3	9	Notify Reliability Coordinator and known impacted interconnected entities of all planned outages, and unplanned outages of 30 minutes or more, for telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between the affected entities.
TOP-001-3	10,14	Determination of System
IRO-010-2	3	Providing data to Reliability Coordinator
EOP-4-3	2	Operations Assessment
EOP-008-1	1,4,6	Backup functionality

Are you registered as a TOP, BA, or RC?

When answering that question did you consider that you may be registered as a TO but be delegated TOP tasks?

If you answered yes to any of these questions you should be aware of NERC RoP Appendix 5a and what it requires.

Consider a certification if any of the following occurs:

a. Changes to a Registered Entity's Footprint or operational challenges (i.e., TLRs) due to the changes

b. Organizational restructuring that could impact BPS reliability

c. Relocation of the control center

d. Changes to Registered Entity ownership requiring major operating procedure changes

e. Significant changes to JRO/CFR assignments or agreements

f. Addition or removal of member JRO/CFR utilities or entities

*g. Complete replacement of a Supervisory, Control and Data Acquisition (SCADA)/Energy Management System (EMS) system

*RF believes that system hardware changes qualify under complete replacement and does not limit this criterial to changing vendors.

If you have concerns about whether a certification/ recertification is required please contact Erik Johnson in the Entity Development department.

Planning Restoration Absent SCADA or EMS

This issue is focused on Energy Management Systems (EMS) and Supervisory Control and Data Acquisition (SCADA) systems that are used daily to maintain and operate the BPS. They are an integral part of daily operations and system restoration following a blackout.

RF participated with the other Regional Entities in NERC and FERC's effort to assess industry's ability to restore the system from blackout, absent the use of SCADA/EMS.

The industry's risk of cyber intrusions make this scenario important to consider. We encourage you to view the final report and consider your own restoration and recovery plans, here.

EMS Reference Document

By: Brian Thiry, Principal Analyst

Risk and Mitigations for Losing EMS Functions

RF had the pleasure of substantially contributing to the recently published NERC Operating Committee Reference Document titled Risks and Mitigations for Losing EMS Functions.

Developed by the EMS Working Group (EMSWG), this document discusses the risk associated with losing Energy Management System (EMS) functions and shares mitigation strategies used to reduce these risk when operators lose situational awareness tools. The purpose of this Reference Document is to:

- identify and discuss the risk of losing EMS functions,
- analyze the causes of EMS events reported through the ERO Event Analysis Process (EAP), and
- share mitigation strategies to reduce these risks to EMS reliability.

The paper begins with a short summary of "What is an EMS and why is it important?" It defines and explains the components of an EMS system including but not limited to State Estimation (SE), Contingency Analysis (CA), and Inter Control Center Protocol (ICCP). Figures 1 and 2 provide illustrations showing a simplified EMS configuration and the inter-dependencies among EMS applications.

The paper details the risks associated with losing EMS functions. The most impactful EMS risk is the loss of System Control and Data Acquisition (SCADA). Without SCADA, the operators do not have the ability to remotely operate devices, nor do they have the metered data points from the RTUs to monitor system stability. Different challenges are presented for the loss of SE, CA, or ICCP such as the inability to determine non-metered data points, the impact of the worst credible contingency, and data from neighboring systems. Even though the loss of SCADA had the highest number of occurrences over the four years analyzed, the RF region is seeing a significant trend of fewer SCADA outages, but a rise of more SE outages.

The paper goes on to analyze the underlying reasons for these EMS outages. The EAP process includes cause coding to determine the root and contributing causes of the EMS events. Four underlying categories were developed:

- Software failures,
- Communication failures,
- Facility outages, and
- Maintenance outages

These four categories are used to explain that there are different reasons for EMS outages, each involving different mitigating strategies. If every outage was a software failure, the industry could point at the vendors and demand more resilient platforms, or work internally through their own IT department to ensure that the architecture for their EMS system (including databases and memory allocations) is suitable for their needs. However, EMS outages have different causes. Some outages are due to external modeling issues, while other outages reveal settings that need to be fine-tuned for convergence. Sometimes the loss of a communications path or supply power to the control center (or data center) results in an EMS outage. In other cases, a system upgrade or patch disables EMS functionality.

Whatever the reason, all of these events are analyzed through the Events Analysis Process (EAP) and cause-coded. During the cause-coding process, the entities provide details on the corrective actions and mitigation strategies to address the root and contributing causes (e.g., software upgrades, additional training, verifying the model, enhancing the loss of data procedure, or calibrating settings with the help of the vendor).

Mitigation strategies, specifically detective and corrective controls are discussed to explain how the loss of EMS functions has not directly led to the loss of generation, transmission lines, or customer load. Possibly the biggest change from the early advent of EMS systems has been the overlapping coverage of situational awareness. Reliability Coordinators and neighboring Transmission Operators and Balancing Authorities work together to help monitor member and neighboring systems during the loss of EMS functionality. The paper highlights ten good-utility practices including manning substations and implementing conservative operations that help maintain reliability while EMS systems are being repaired.

Finally, the reference document highlights the NERC Monitoring and Situational Awareness Conference where industry gathers annually to provide awareness of current and emerging EMS issues, exchange best practices, and collaborate with the vendors. Past Lessons Learned from the EAP are shared, plus entities highlight some of their own best practices for EMS resiliency.

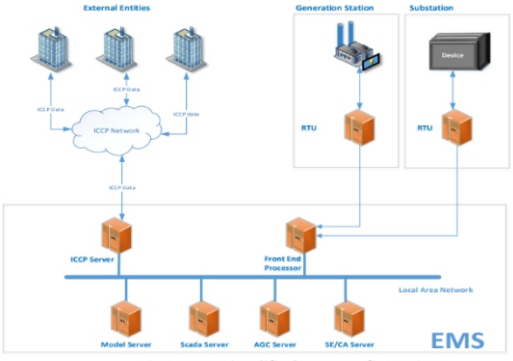


Figure 1 A simplified EMS configuration

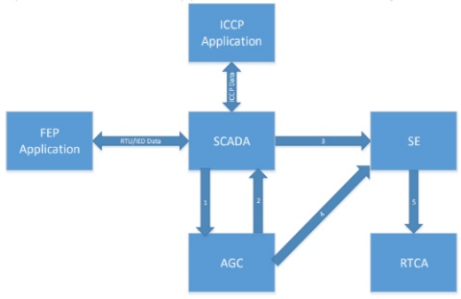


Figure 2 Typical dependency between main EMS Applications

[1] Note: while the EMS Reference Document introduced four main categories, RF's analysis of EMS events included five categories (Software, Data, Settings, Maintenance, and Facilities). Overall, performance in RF reflected performance across the ERO enterprise.

Control Center Ergonomics

By: Renata Fellmeth, ReliabilityFirst; Matt Mabrey and Karen McEwen-Lawrie, Hoosier Energy

Old Control Room

New Control Room

Hoosier Energy Rural Electric Cooperative, Inc.

As an industry, utilities invest financial resources in reducing reliability-related risk by training personnel and upgrading equipment in the control centers. Utilizing ergonomics, which is the study of people's efficiency in their working environment, is an additional way to optimize performance.[1]

Investing in ergonomics in a control center will reduce injuries and human error by building a better working environment. Considering ergonomics during the many phases of designing a control room can lessen mistakes and injuries. Incorporating ergonomics in the design of any workspace helps maximize human performance.

By developing plans to embrace ergonomics we can begin to minimize human performance issues. This article explores real-life examples based on lessons learned by Hoosier Energy during the design and implementation of their new control center.

WHAT IS ERGONOMICS?

Ergonomics, a globally recognized science of designing a better workplace for people and their working environment, is used by such well-known companies as Blue Cross/Blue Shield, Dow Chemical Company, Exxon Mobil, Liberty Mutual, and Siemens Automotive.[2 3] Ergonomics focuses on the work environment and the interaction of people and equipment, which includes the design and function of work area layouts, displays, controls, lighting, noise, sound, physical requirements, sight lines, furniture design, traffic flow, and more.

In addition to a number of general benefits, a review of 250 case studies, from industries such as manufacturing, office environments and healthcare, found an overall cost-benefit ratio of 1 to 18.7, in favor of the use of ergonomics.[4]

ERGONOMICS AND RISK

Ergonomics addresses health and safety risks associated with preventing musculoskeletal disorders. Carpal tunnel syndrome, tendonitis, muscle/tendon strain, and tension neck syndrome injuries accounted for 32% of all cases reported to the Bureau of Labor Statistics in 2014.[5]

Ergonomics is an integral part of designing and updating control rooms. Control room operators perform critical situational tasks under stressful conditions including:

- poorly designed control boards and rooms,
- 16-hour shifts including overnight shifts,
- poor illumination,
- glare from monitors,
- noise,
- uncomfortable chairs

Applying ergonomics to a control center can help prevent eye strain, fatigue, neck and back injuries, and musculoskeletal disorders.

Lessons learned were identified through in-person interviews at Hoosier with the former and current Manager of Facilities, a former System Control Manager, the current System Control Coordinator, System Control Coordinator Operations and Training, as well as surveys and questionnaires completed by seven System Control Supervisors. Below are some highlights organized by mitigation strategy.

DESIGN

- Interview and involve a cross section of management,

Continued on page 10

GENERAL BENEFITS

Reduced Injuries
Fewer Workers Compensation claims
Improved Productivity
Decreased Employee Turnover
Increased Employee Satisfaction
Work Efficiency

OPERATOR RECOMMENDATIONS

"Ask the operators.They are the ones here 24 hours and that should be important." – Donnie Campbell

"Chairs need to be comfortable to sit in for long periods of time yet be very durable." – Stan Elmore

"Soft walls need to be installed, and white noise." – Bobby Hill

"We have problems with the wireless headset; others do not know when you are on the phone." – Scott McClarney

Control Center Ergonomics

Continued from page 9

supervisors, engineers and operation's personnel to include their input on the process - create a shared vision.

- Involve all uses of the space in the layout and design of the room while allowing additional space for growth to accommodate factors such as changing technology or to resolve issues that may emerge after building and occupying the space.
- Involve all uses of the space in the selection of furniture, work stations, desktop monitors, computers, phones.
- Provide full-scale mock-ups of the spaces to operators.

WORK AREA

- Design space to limit visual perception with tour groups of unintended access to confidential information.
- Design the work console for control operators to work freely within the work station, and create enough desktop surface for large blueprints.
- Place equipment, phone devices, and computers within reach for easy access and viewing.

DISPLAYS

- Dedicate a screen to a weather and/or general news station for situational awareness and to monitor extreme weather situations.

LIGHTING

- Emulate natural lighting frequency if space does not have access to natural lighting. Placement of lighting over control operator stations, foot candle (a unit of illumination) and glare are key considerations to avoid.

NOISE AND SOUND

- Consider Sound Transmission Class (STC) ratings (which dampen noise by using specific materials) and noise cancelling or dampening design such as flooring and ceiling tile selection, sound masking systems, sound attenuation blankets, fabric, building walls to the deck, door sweeps.
- Consider hands-free communications, such as headsets, for control operators to help prevent neck strain and the danger of tripping over long cords.

PHYSICAL REQUIREMENTS

- Design a control room for both the minimum and maximum number of occupant loading, including emergency situations.
- Utilities (electric, water, sewer, HVAC) need to be redundant to assure operator sustainability and comfort.
- Design a kitchenette and bathroom close to the control room center. Control room operators cannot leave their work station for long periods of time, especially the night staff, which is usually one control room operator.
- Place support staff (IT, communication techs, etc.) outside the physical security perimeter (PSP), so help can be provided in a timely manner.
- CIP Standards require separation of business computer and SCADA equipment, which increases the amount of space that is needed.

SIGHT LINES

- Place video map boards and stacked monitors in the line of sight for easy viewing to avoid neck strain and musculoskeletal disorders.

FURNITURE DESIGN

- Provide print cabinets and/or additional surface space so operators can lay out drawings to prevent cluttered workstations and to ensure visibility of the entire document.
- Buy ergonomic chairs and stand-up desks for comfort and flexibility. Standing allows the body to adjust and move easily, flex muscles, and keep blood circulating. Control operators work extended shifts, so comfort, fit, body posture, and repetitive motion need consideration. A sedentary lifestyle and a job that requires sitting can lead to many health problems.

TRAFFIC FLOW

- Design the control room so tours can be given from the outside eliminating disruption/distraction to the control room operators.

---

[1] Oxford Dictionaries. (2016).

[2] United States Department of Labor. (2016) Occupational Safety and Health Administration (OSHA). Solutions to Control Hazards/Case Studies.

[3] P Puleio, J. & Zhao, J. (2016) Return on Investment for Ergonomics Interventions.

[4] R.W. Goggins et al. Estimating the effectiveness of ergonomics interventions through case studies: Implications for predictive cost-benefit analysis. In Journal of Safety Research. 39 (2008). [Table 2] 341.

[5] Bureau of Labor Statistics. (November, 2015). 2014 Nonfatal Occupational Injuries and Illnesses: Cases with days away from work. [Chart 19].

E-ISAC

By: Bill Lawrence, Director Electric Information Sharing and Analysis Center, NERC

The North American Electric Reliability Corporation takes the security of the grid seriously and remains vigilant against constantly changing threats and vulnerabilities. One way we do this is through our Electricity Information Sharing and Analysis Center (E-ISAC).

The E-ISAC serves as the primary security communications channel for the electricity industry, and enhances industry readiness and its ability to respond to cyber and physical threats, vulnerabilities, and incidents—each of which has the potential to impact the bulk power system.

The E-ISAC's secure portal, which was recently redesigned, allows for the exchange of information with E-ISAC members toward accomplishing its mission to reduce cyber and physical security risk across North America by providing unique insight, leadership, and collaboration with its public and private partners.

The E-ISAC, which was created in 1999 at the request of the Department of Energy (DOE), conducts trend analysis of all information shared to build the security "big picture" and identify possible threats to the entire industry.

The E-ISAC operates in collaboration with DOE and the Electricity Subsector Coordinating Council (ESCC), which is made up of industry chief executive officers, and with government partners including the Department of Homeland Security, the FBI and the Federal Energy Regulatory Commission.

The E-ISAC has a comprehensive set of activities designed to strengthen North America's grid security posture. A few of note include the Cybersecurity Risk Information Sharing Program (CRISP); the annual grid security conference, GridSecCon; and the biennial grid security exercise, GridEx.

CRISP is a voluntary program that facilitates the exchange of detailed cyber security information between the industry, the E-ISAC, DOE and its Pacific Northwest National Laboratory.

The program enables owners and operators to better protect their business networks from sophisticated cyber threats. Utilities serving 75 percent of U.S. electricity consumers participate in CRISP. Anonymized information and data from CRISP benefits all E-ISAC members and is shared via the E-ISAC portal.

NERC's annual GridSecCon brings together cyber and physical security experts from industry and government to share emerging security trends, policy advancements, and lessons learned related to the electricity industry. The next conference is scheduled for October 16-19, 2018.

GridEx began in 2011 and takes place every two years. The severe, simulated, cyber and physical attack scenario of the exercise allows utilities, government partners and other critical infrastructure participants to:

- engage with local and regional first responders;
- exercise cross-sector impacts; improve unity of messages and communication;
- identify lessons learned; and
- engage senior leadership.

The attack scenario is designed to overwhelm even the most prepared organizations, and allows learning from "real world" attacks and impacts on critical infrastructure, such as those seen in Ukraine in 2015 and 2016. NERC uses input from participants to develop observations and propose recommendations to help industry enhance the security, reliability, and resilience of North America's bulk power system.

One of the best indicators of the success of GridEx is the steady increase in engagement by industry stakeholders and government officials.

However, member engagement is key to gathering and sharing information that is valuable and actionable with industry members. Voluntary information sharing allows the E-ISAC to identify emerging threats and to provide members with early warnings, and potentially reach other subject

Continued on page 12

E-ISAC

Continued from page 11

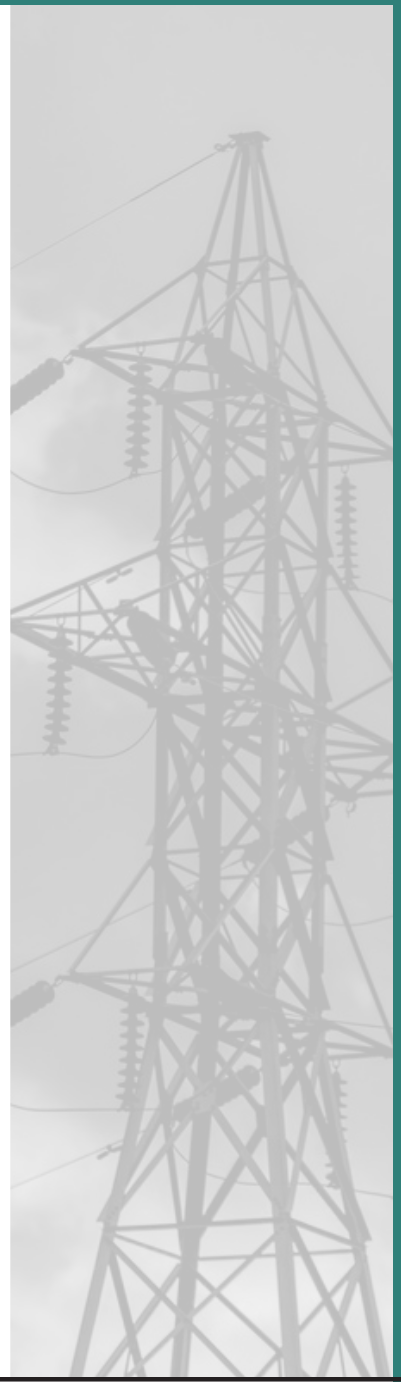
matter experts.

As member organizations increase information sharing with the E-ISAC, the E-ISAC, in turn, is better able to identify trends that will allow members to proactively reduce cyber and physical risk. All information shared with the E-ISAC is protected and never shared with any personnel with roles in the Compliance Monitoring and Enforcement Program.

A specific program to designed to increase trust in the E-ISAC's protection of information shared by members, as well as providing a knowledge exchange between analysts, is the Industry Augmentation Program. This program embeds security experts from electric utilities at the E-ISAC for a week at a time, and participants share information on their own crisis response procedures and incident handling experience.

NERC's E-ISAC continues to build and refine its products and services in its quest to be a world-class, trusted source for quality analysis and rapid sharing of electricity industry security information in the manner that is best for grid security in North America.

To become a member of the E-ISAC or for questions on the programs and services available to members, please send an email to here.



Members see how the E-ISAC functions to take in and analyze information, the tools available, and care taken by the staff to safeguard shared information. The E-ISAC's expertise includes:

- **Understanding the intent behind attacks and campaign attribution of indicators: By identifying adversary campaign tactics, techniques, and procedures (TTP), the E-ISAC can share actionable indicators and specific strategies that members can take to mitigate the threat. Additionally, increased sharing from industry allows the E-ISAC to do predictive analysis on future threat TTPs.**

- **Reverse-engineering malware and assisting in better understanding an event: The E-ISAC has access to closed-environment malware analysis systems that perform static and dynamic analysis on files submitted for malware analysis, and has strong partnerships with government organizations such as the National Laboratory system to increase analytical capability.**

- **Identifying additional information within the industry or other critical sectors: The E-ISAC works with other cross-sector ISACs to share indicators of compromise that may pose a threat to the electricity industry and our stakeholders.**

PJM Designs Interactive Map Application for Dispatchers

PJM has developed a geographic information systems tool for dispatchers to visually assess the grid in real time.

The Dispatch Interactive Map Application (DIMA) was designed to improve situational awareness for PJM dispatchers, but personnel across organizations can also use the interface in order to transition from tabular to real-time geospatial views. Users can view integrated grid data that includes:

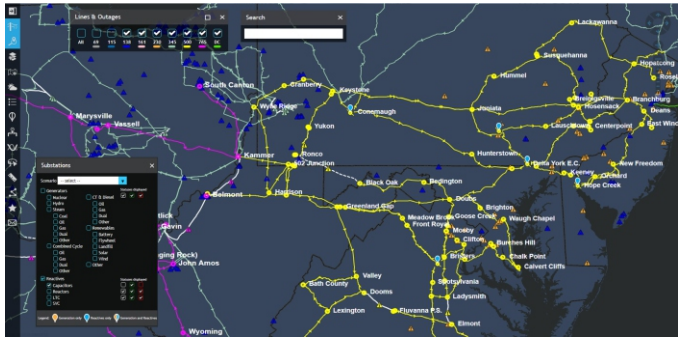
- Transmission line status
- Generator status
- Reactive power equipment status
- Demand response availability
- Behind-the-meter generation
- Gas-electric coordination
- Weather

DIMA provides an intuitive interface and controls for dispatchers with an at–a-glance view of layered information. The geospatial map shows high-level locations of transmission zones, transmission lines by voltage, and substations.

Users can also utilize geospatial filters to view specific types of substations which can be filtered by:

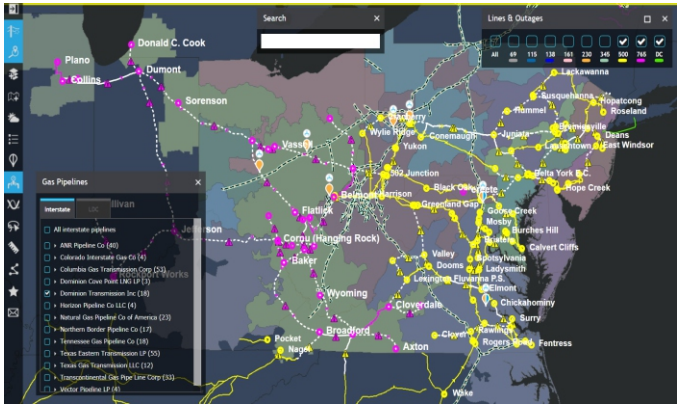
- Equipment type and status
- Unit type and status
- Fuel type
- Real time MW
- EcoMax
- Demand Response MW by zip code
- Real-time and historical weather

The DIMA equipment filter allows users to identify locations of specific types of equipment by their current status. In a situation with localized low voltage, a dispatcher can search for nearby capacitors that are not currently online but are available. Prior to DIMA, a dispatcher would click through multiple one-line diagrams to find capacitors but would not always be aware of the electrical or geospatial distance. In this example, you can see blue balloons indicating that at least one capacitor is offline and available at these substations per the

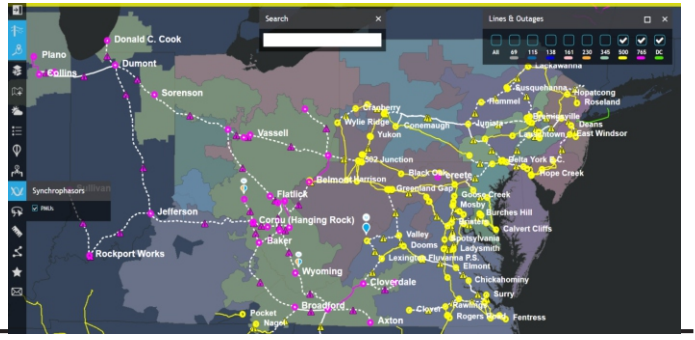


filters selected in the substation filter window.

The DIMA interface also allows users to view natural gas pipelines in the region. In the winter, PJM's gas team routinely notifies dispatchers of gas constraints impacting gas generators, including a picture of a DIMA screen and links that any dispatcher can easily open.



Synchrophasor locations and measurements have recently been added as a layer in DIMA. With this feature, users can display location and signal types. PJM plans to add more features in future project phases, including voltage magnitude and angle, frequency heat maps, and data trends to the signal metadata layer, and real-time outage statuses to the PMU metadata.



The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

CIP Exceptional Circumstances

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity strive to improve your compliance posture and work toward continuous improvement in the reliability, security, resiliency, and sustainability of your CIP compliance programs.

There are times that I may also discuss areas of the standards that other entities may be struggling with and share my ideas to overcome their known issues. As with lighthouses, I can't steer your ship for you, but perhaps I can help shed light on the sometimes stormy waters of CIP compliance.

Q What evidence do I need to retain if I invoke CIP Exceptional Circumstances? Can I declare a CIP Exceptional Circumstance for a Requirement that does not contain that provision?

When referencing CIP-003, Security Management Controls, I will provide references to CIP-003-7, even though it is not yet enforceable.

A The provisions for CIP Exceptional Circumstances are an acknowledgement that responding to an emergency takes precedence over compliance. This makes sense when we list the top three priorities I think every electric utility should have:

1. Safety – The ability to keep people safe, whether it's our workers, customers, or someone passing by on the street, must be at the top of our priority list at all times.
2. Reliability – A reliable source of electric power is essential to our way of life. Reliability has both short-term and long-term aspects. In the CIP world, we focus on preventing widespread or long-term outages caused by malicious actors.
3. Compliance – The standards we set for our performance support the reliable operation of the electric grid. Compliance with mandatory and enforceable standards ensures we meet the standards consistently.

Reliability vs. Compliance

Compliance exists to help ensure the reliability of the BES, not as an end in itself. In recognition of this, FERC included this language in Order 706: "… allowing limited exceptions, such as during emergencies, subject to documentation and mitigation." [FERC Order 706 P 431] This was implemented in CIP Version 5 as CIP Exceptional Circumstances.

What is a CIP Exceptional Circumstance?

The definition of CIP Exceptional Circumstance (see sidebar) is one very long sentence. Let's see if we can break it down so it makes a little more sense.

Big Bay Lighthouse, MI - Photo: L. Folkerth

Figure 1 will help in our analysis of the definition. If we cut out all the modifier language, a CIP Exceptional Circumstance is a situation (orange) that involves (green) a condition (yellow). Now we start considering the modifiers. The condition may consist of any of eight listed items (blue).

One or more (yellow) of those items (blue) may occur, or a similar (yellow) condition may exist to trigger the CIP Exceptional Circumstance. Those items (blue) must also have an impact (purple) on safety or BES reliability. The conditions may exist now ([does] involve, green) or be impending (threatens to involve, green).

What isn't a CIP Exceptional Circumstance?

There are some things to note that do not fall into the definition of a CIP Exceptional Circumstance:

- A condition that impacts only compliance. For example, allowing a repair tech unescorted access into a PSP to perform routine HVAC maintenance.
- A situation that arises from lack of planning. For example, leaving insufficient time for completion of an active vulnerability assessment before

CIP Exceptional Circumstance [NERC Glossary]

A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.

Continued on page 15

Continued from page 14

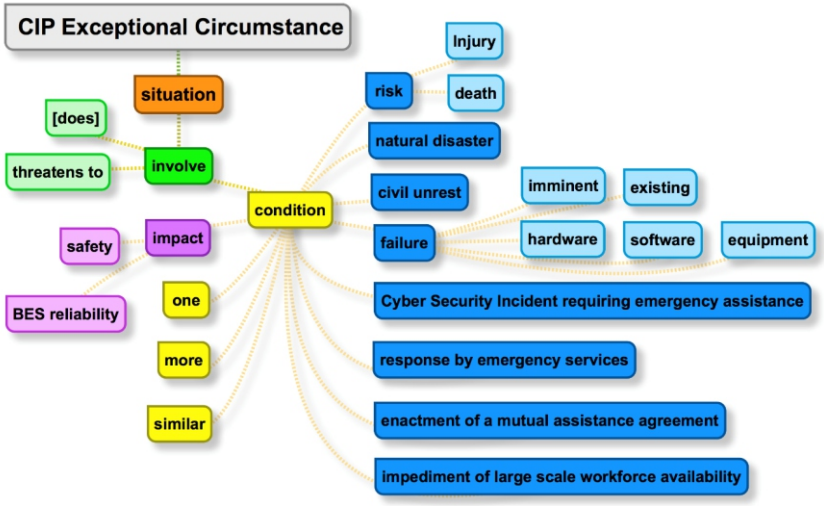


Figure 1 CIP Exceptional Circumstance Definition Analysis

placing a new high impact BES Cyber System into production. (CIP-010-2 R3 Part 3.3)

- A situation that arises from lack of resources. For example, security event logs are not retained for 90 days due to insufficient disk space being allocated.

Cyber Security Policy

CIP-003-7, Security Management Controls, Requirement R1 requires your cyber security policy to address declaring and responding to CIP Exceptional Circumstances. Your policy should discuss the goals, objectives, and expectations for the management of CIP Exceptional Circumstances. It should also establish a governance framework for CIP Exceptional Circumstances.

For example, the policy might discuss how your entity views the relationship between safety, reliability, and compliance. In this case the policy could establish a goal of ensuring compliance that does not impact safety or reliability in an emergency by establishing a CIP Exceptional Circumstances plan. The policy might also address how CIP Exceptional Circumstances will be governed: who can declare a CIP Exceptional Circumstance, who is responsible for the CIP Exceptional Circumstances plan, who must approve the closure of a CIP Exceptional Circumstance, and what documentation must be kept.

CIP Exceptional Circumstances Plan

In order to address the possibility of needing a CIP Exceptional Circumstances Plan I strongly recommend that you establish a plan for handling these types of exceptional circumstances. While a plan is not explicitly required by the Standard, there is far too much detail to be discussed that would fit well into a policy. This plan could well be an emergency response plan similar to a Cyber Security Incident response plan (CIP-008-5) or a recovery plan (CIP-009-6), but need to cover an emergency response from a broader perspective.

Although not required by the Standards, you may want to establish a CIP Exceptional Circumstances plan or include provisions for CIP Exceptional circumstances in a more general emergency response plan. In either event, I suggest that your plan address the topics discussed below at a minimum:

Scope

The CIP Standards explicitly permit a CIP Exceptional Circumstance to be invoked in six program areas:

1. Training before access is granted (CIP-004-6 R2 Part 2.2)
2. Access authorization (CIP-004-6 R4 Part 4.1)
   a. Cyber
   b. Physical
   c. BCSI
3. Visitor program (CIP-006-6 R2 Part 2.1, 2.2)
   a. Escorted access
   b. Visitor logging
4. Security event log retention (CIP-007-6 R4 Part 4.3)
5. Active vulnerability assessments prior to production use for high impact (CIP-010-2 R3 Part 3.3)
6. Transient Cyber Assets (CIP-003-7 R2 Att 1 Sec 5, CIP-010-2 R4)

The plan should address how each program area might be affected in an emergency. For example, if a mutual assistance crew must have access to a substation's medium impact BES Cyber Systems, you won't be able to put the crew through your cyber security training before they are given access. Your plan could provide guidance on how to grant this access, how to remove it when no longer needed, how to return to normal operations, and how to document the CIP Exceptional Circumstance.

Out-of-scope Requirements

In the case of Requirements not listed above, I recommend that your plan include provisions for foreseeable extensions into areas not explicitly permitted to be part of a CIP Exceptional Circumstance. For example, the mutual assistance crew from the above example will not have personnel risk assessments performed by your entity. You will need to grant the crew access knowing that this is not strictly permitted by the Standard.

Your plan should also address how you will handle unforeseen circumstances, whether explicitly permitted by the Standard or not.

Continued on page 16

Continued from page 15

Lifecycle

Your plan should address all aspects of a CIP Exceptional Circumstance. I suggest you include the entire lifecycle of a CIP Exceptional Circumstance as shown in Figures 2 and 3.

1. **Declaration**
   Your CIP Exceptional Circumstance plan should have a clearly defined method for declaring a CIP Exceptional Circumstance. The declaration may occur before the emergency (see Figure 2), such as in preparation for a hurricane, during the emergency, or after the emergency has ended (Figure 3).

2. **Emergency Response**
   During an emergency, you attend to the emergency. Compliance is a lower priority than an emergency.

3. **Recovery**
   After the emergency has ended, you return to normal (compliant, reliable, secure state) operations.

4. **Assessment and Mitigation**
   After returning to normal operations your work is not done. You have been in violation of the Standards, so cleanup is required. Your plan should require an assessment of possible impacts to your cyber security posture, and you should implement mitigations for any areas that may have been weakened.

   For example, if a mutual assistance crew was granted password access to Cyber Assets belonging to medium impact BES Cyber Systems in a substation, then those passwords should be reset after the emergency is over.

   Be sure you find and mitigate any area that may have gone out of compliance while you are still protected by the CIP Exceptional Circumstance. If you find additional areas of noncompliance after the CIP Exceptional Circumstance is terminated, you may need to self-report such areas.

5. **Termination**
   Once you have recovered to normal operations and mitigated any noncompliance, you should terminate the CIP Exceptional Circumstance.

6. **Documentation**
   The documentation you keep should describe the need for the CIP Exceptional Circumstance, the significant dates associated with it, all actions taken during emergency response, how you recovered to normal operations, and how you assessed and mitigated any possible noncompliance. Save this documentation as evidence.

Figure 2 CIP Exceptional Circumstance Lifecycle Example A

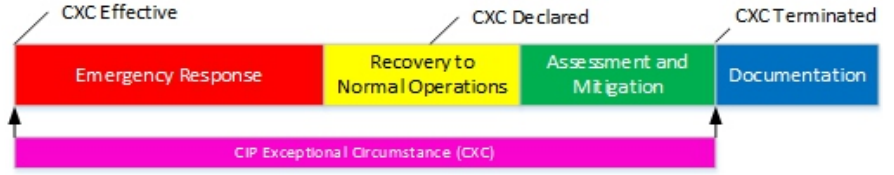


Figure 3 CIP Exceptional Circumstance Lifecycle Example B

Communications

In addition to any communications your CIP Exceptional Circumstance requires, I recommend informally communicating any declaration of CIP Exceptional Circumstances to the ReliabilityFirst Enforcement group as soon as practicable. In addition, if you have been out of compliance in any program area not explicitly permitted by the CIP Standards during a CIP Exceptional Circumstance, you should submit a self-report of that occurrence. Again, if you have communicated the circumstances surrounding the emergency and your response, RF will be in a better position to assess whether any additional actions are needed.

Requests for Assistance

If you are an entity registered within RF and believe you need assistance in sorting your way through this or any compliance related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the rfirst.org web site here.

Feedback

Please share any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached here.

FERC extends comment period for interested entities in Grid Resilience and Reliability Proceedings

Beginning April 9th, FERC will provide a 30-day extension for energy industry groups to respond to resilience plans filed by grid operators. Plans were filed within 60 days of FERC's January 8th grid resilience proceeding in which commissioners rejected a proposal from the Department of Energy (DOE) to subsidize coal and nuclear plants.

While the proposal was rejected, the Commission did believe that a holistic examination of the resilience of the bulk power system was needed. Thus, they issued a new proceeding requiring Regional Transmission Organizations and Independent System Operators to provide information on how grid resiliency can be improved.

Originally, the 30-day response window was to begin on March 9th, the deadline for grid operators to submit their resilience plans. However, several energy industry associations explained to FERC that more time was needed as they are preparing for two technical conferences in April. FERC granted their request to submit finalized responses by May 9th.

NERC Appoints New President and CEO

RF would like to congratulate Jim Robb for being selected as President and CEO of NERC. Mr. Robb was the President and CEO of WECC since 2014 and will be starting his new role at NERC on April 9, 2018.

Mr. Robb has a Master of Business Administration from the Wharton School of Business at the University of Pennsylvania and a Bachelors of Science in Chemical Engineering from Purdue University – both degrees were awarded with honors.

Mr. Robb has over 30 years of experience in the energy sector as an engineer, consultant and a senior executive. He worked as a top management consultant to the power and gas sector for 14 years, and as a senior executive for both Reliant Energy and Northeast Utilities (now Eversource Energy) over an 11-year period.

In his role at WECC, Mr. Robb helped to improve member relations, strengthen the management team and expand the collaboration with NERC and other Regional Entities. He worked closely with key electric power companies and energy consumers in California, western Canada, the Pacific Northwest, and the Rocky Mountain states.

The NERC Board engaged in a comprehensive nationwide search that resulted in the unanimous selection of Jim Robb. NERC's Board Chair stated "We are confident that Jim will provide the combination of strong leadership, vision and commitment to the reliability and security of the bulk power system across North America that is essential to NERC's continuing success."

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Update

This recurring column provides our Registered Entities with relevant and recent updates to the Reliability Standards and Requirements.

General NERC Standards News

Updates to Compliance Guidance Documents

NERC posed the following ERO Enterprise-Endorsed Implementation Guidance documents:

- CIP-014-2 R5 - Developing and Implementing Physical Security Plans (NATF)
- CIP-002-5.1a, R1 - Shared Ownership of BES Facilities (CIPC)

NERC also posed the following Proposed Implementation Guidance documents:

- PRC-024-2 R2 - Generator Voltage Protective Relay Settings (PC_SPCS)
- PRC-023-4, R1 - Determination of Practical Transmission Relaying Loadability Settings (PRC)
- CIP-002-5.1a R1 - Voice Communications in a CIP Environment (CIPC)

These resources can be found on NERC's Compliance Guidance page.

Three New RSAWs Posted

NERC posed three new Reliability Standard Audit Worksheets (RSAWs):

- TOP-001-4
- INT-009-2.1
- INT-010-2.1

These resources can be found on NERC's RSAW page under the heading "Current RSAWs for Use."

Resources Posted

The ERO Enterprise recently conducted an industry webinar regarding the Compliance Guidance program and, more specifically, guidelines for developing Implementation Guidance. The webinar was tailored to Pre-Qualified Organizations, Standard Drafting Team members, and any other personnel involved in the development of Implementation Guidance. A new Implementation Guidance Development Aid was introduced during
the webinar. The slide presentation, webinar recording, and the new Implementation Guidance Development Aid are now available.

NERC also posted the streaming webinar and slide presentation for the February 14, 2018 CIP-002-6 and CIP-012-1 Planned and Unplanned Change Language webinar.

NERC posted one new lesson learned titled Inadequate Battery Configure Management Damaged a Generating Station and Tripped an HVDC Conversion Station, which is available on NERC's Lessons Learned page.

Notable NERC Filings

NERC Filings

In January, NERC filed the following:

- Comments in response to the notice of proposed rulemaking proposing to approve: (1) Reliability Standards PRC-027-1 (Coordination of Protection Systems for Performance During Faults) and PER-006-1 (Specific Training for Personnel); and (2) the retirement of Reliability Standard PRC-001-1.1(ii).
- A petition for approval of proposed Reliability Standard TPL-007-2 – Transmission System planned Performance for Geomagnetic Disturbance Events.

In February, NERC filed the following:

- A petition for approval of amendments to the SERC Reliability Corporation Regional Reliability Standard Development Procedure.
- An amended petition to its December 9, 2016 petition for approval of proposed revisions to the NERC Rules of Procedure.
- Comments in response to a notice of proposed rulemaking in Docket No. RM18-2-000.

NERC's filings to FERC can be found here, organized by year.

Notable FERC Issuances

At its February 16 open meeting, FERC issued Order No. 842, revising FERC's pro forma Large Generator and Small Generator Interconnection Agreements (LGIA and SGIA, respectively) to require that all new generating facilities install, maintain, and operate a functioning governor or equivalent controls in support of primary frequency response as a precondition of interconnection. The order also revises the pro forma LGIA and SGIA to impose certain operating requirements developed by NERC, while allowing for the possibility of a future NERC Reliability Standard with equivalent or more stringent operating requirements. Further, FERC was persuaded by NERC's suggestion to require that interconnection customers provide relevant balancing authorities with the status and settings of their governor or equivalent controls upon request or when those controls are out of service.

FERC also issued FERC issued Order No. 841, in which FERC directed each ISO and RTO to revise its tariff to accommodate the participation of electric storage resources in the wholesale electric markets. FERC directed each ISO and RTO to establish a participatory model that will: (1) ensure that a resource using the participation model is eligible to provide all capacity, energy, and ancillary services that the resource is technically capable of providing in the RTO/ISO markets; (2) ensure that a resource using the participation model can be dispatched and can set the wholesale market clearing price as both a wholesale seller and wholesale buyer consistent with existing market rules that govern when a resource can set the wholesale price; (3) account for the physical and operational characteristics of electric storage resources through bidding parameters or other means; and (4) establish a minimum size requirement for participation in the RTO/ISO markets that does not exceed 100 kW. FERC has created a separate docket (Docket No. RM18-9-000) to address whether similar reforms should be implemented with respect to the participation of distributed energy resource aggregations in the wholesale electric markets.

Standards Update

Recent and Upcoming Standards Enforcement Dates

April 1, 2018
- IRO-018-1 Reliability Coordinator Real-time Reliability Monitoring and Analysis Capabilities
- TOP-010-1 Real-time Reliability Monitoring and Analysis Capabilities

July 1, 2018
- CIP-009-6 Cyber Security Recovery Plans for BES Cyber Systems (Requirement 2.3)
- CIP-010-2 Cyber Security Configuration Change Management and Vulnerability Assessments (Requirements 3.2, 3.2.1, 3.2.2)
- MOD-026-1 Verification of Models and Data for Generator Excitation Control System or Plant Volt/Var Control Functions (Requirements R2, 2.12.1.6)
- MOD-027-1 Verification of Models and Data for Turbine/Governor and Load Control or Active Power/Frequency Control Functions (Requirements R2, 2.1-2.1.5)
- TOP-001-4 Transmission Operations
- TPL-007-1 Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirement 2)

September 1, 2018
- CIP-003-6 Cyber Security Security Management Controls (Requirement 2, Att. 1, Sec. 2 and 3);

January 1, 2019
- BAL-005-1 Balancing Authority Control
- FAC-001-3 Facility Interconnection Requirements
- TPL-007-1 Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirement 5)

April 1, 2019
- EOP-004-4 – Event Reporting
- EOP-005-3 – System Restoration from Blackstart Resources
- EOP-006-3 – System Restoration Coordination
- EOP-008-2 – Loss of Control Center Functionality

January 1, 2020
- PRC-026-1 Relay Performance During Stable Power Swings (Requirements 2-4)

July 1, 2020
- PRC-002-2 – Disturbance Monitoring and Reporting Requirements (50% compliance for Requirements 2–4, 6–11)

January 1, 2021
- PRC-012-2 – Remedial Action Schemes
- TPL-007-1 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirement 6, 6.1-6.4)

January 1, 2022
- TPL-007-1 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements 3,4,7)

July 1, 2022
- PRC-002-2 – Disturbance Monitoring and Reporting Requirements (Requirements 2–4, 6–11)
- VAR-501-WECC-3 – Power System Stabilizer (Requirement 3 has an effective date of July 1, 2022 for units placed in service prior to final regulatory approval.)

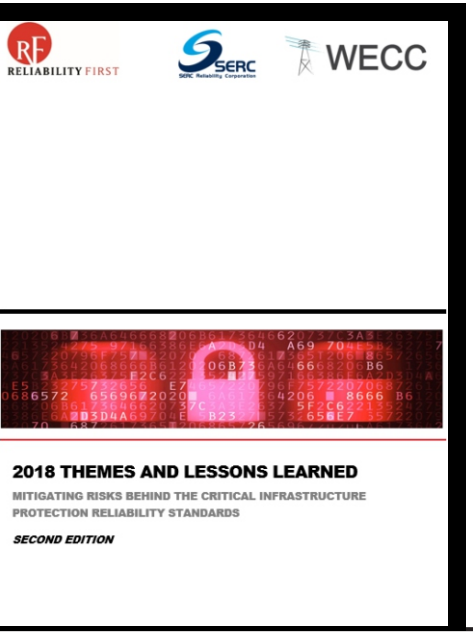
More information on these and other upcoming Standards is available here.

RF, WECC, and SERC Issue Joint Report on CIP Themes

To combat the ever changing physical and cyber-threats landscape, entities continue to improve their tools, expertise, and defense strategies. Yet, despite these efforts to stay ahead of security threats, entities are sometimes held back by deficiencies or limitations in their corporate structure, culture, or resources.

RF, WECC, and SERC (the Regions) have been working together to analyze the data in all three Regions around potential themes in these deficiencies and limitations. The Regions handle large volumes of noncompliance and their territories cover all or parts of 36 states, Washington D.C., and parts of Canada and Mexico. This collaboration has helped identify new areas for improvement and potential resolutions to some of the deficiencies and allowed for validation of the data in each Region.

The Regions, in coordination with NERC and multiple stakeholders from the Regions, have issued a joint report identifying the themes and possible resolutions in order to help drive entities to continue to assess and strengthen their CIP programs and thus mitigate security risks. The four themes the Regions have identified are:



- disassociation between compliance and security;
- development of organizational silos;
- lack of awareness of an entity's needs or deficiencies; and
- inadequate tools or ineffective use of tools.

View the full report here.

Protection System Workshop
August 14-15, 2018
Cleveland, OH

Click here to Register

Human Performance Workshop
August 15-16, 2018
Cleveland, OH

Click here to Register

Follow RF on

@RFirst_Corp

Watt's Up at RF

We hope you can attend our 2018 Spring Workshop
April 24-26, 2018

Nationwide Hotel and Conference Center • Lewis Center, OH

Day 1: April 24, 2018 Reliability Workshop **8:30 am – 4:30 pm**

Event Analysis & Situational Awareness

Sam Chanoski (NERC) will highlight the importance of situational awareness in the industry and offer insights on related emerging technology and innovations to enhance the reliability and security of the BES.

EMS Outages and the Events Analysis Process

A panel of RF and NERC experts will explore EMS outage trends throughout ReliabilityFirst and North America as discovered through the Event Analysis Process (EAP).

Compliance Concerns around EMS Outages

A review of possible compliance concerns associated with EMS outages, recommendations for performing Compliance Self Assessments, and the impact of EMS outages may have on real time assessments.

Internal Controls and EMS systems

A brief review of what Internal Controls are with an emphasis on those associated with EMS systems, how to identify and develop controls and what the RF Compliance Team looks for when reviewing them.

EMS Certifications

Information on the certification/recertification process and the application of the criteria related to EMS changes (ROP Appendix 5A).

EMS Outages: Management Practices and Assist Visits

Examine ties between EMS outages and the RF management practices as well as corresponding ties to Standards.

Guided Self-Certification Process

Consider why we use Guided Self-Certification as a compliance tool and how it is different from a Self-Certification and an Audit.

Entity Issues, Questions, Inquiries from 2017

Review various compliance monitoring approaches and frequently asked questions from Entities in 2017.

ERO Enterprise Program Alignment Process

NERC will walk through its alignment process.

Day 2: April 25, 2018

Compliance User Group Meeting (CUG) **8:15 am – 5:00 pm**

RF Critical Infrastructure Protection Committee Meeting (CIPC) Closed Meeting **1:00 pm – 5:00 pm**

Day 3: April 26, 2018 **8:30 am – 4:30 pm**

CIP Themes

An update from RF's Enforcement Team on recent violation trends with a focus on how to track continuous improvement.

Security Patch Management under CIP-007-6 R2

PPL will explain their CIP patching strategy from vendor source inventory to controls including their strengths and struggles.

GridEx IV Exercise Overview

RF will provide an overview of the 2017 Q4 GridEx IV Exercise

Modifications to CIP Standards

NERC will provide the current status of the Modifications to the CIP Standards project.

Industrial Control Threat Intelligence

Sergio Caltagirone of Drago's Inc. will provide an overview of the threat environment in which adversaries are outpacing defenders. We'll discuss what threat intelligence is, how it's used, and why it's necessary.

NERC CIPC Roadmap

NERC will walk through its CIPC Roadmap.

AEP Security Operations & Event Monitoring Center (SOEMC)

AEP will give an overview of its Security Operations & Event Monitoring Center, including set-up, roles and best practices.

Calendar of Events

Complete calendar of RF Upcoming Events is located on our Website:

Date	RF Upcoming Events	Location
April 16	Reliability and Compliance Open Forum Call	Conference Call
April 24-26	RF Spring Reliability Workshop and CIP Workshop	Columbus, OH
May 21	Reliability and Compliance Open Forum Call	Conference Call
May 24	ReliabilityFirst Board of Directors Meeting	Cleveland, OH
June 5-6	ReliabilityFirst CIPC Meeting	Philadelphia, PA
June 18	Reliability and Compliance Open Forum Call	Conference Call

Industry Events:

Date	Industry Upcoming Events
April 19	FERC Open Meeting
May 2	NERC Inverter-Based Resource Webinar Series - Inverter-Based Resources Connected to the Bulk Power System
May 8	BOTCC Executive Session
May 17	FERC Open Meeting
May 17	NERC Inverter-Based Resource Webinar Series - Inverter modeling for protection, harmonics, EMT studies, and review of real-world VER related events
June 13	NERC Inverter-Based Resource Webinar Series - Recommended Performance for Inverter-Based Resources Connected to the Bulk Power System – NERC Reliability Guideline
June 14	BOTCC Executive Session
June 18-22	NERC – GADS Conventional and Wind Training
June 21	FERC Open Meeting

SHARE YOUR FEEDBACK

Please email any ideas or suggestions for the newsletter to prcommrequest@rfirst.org

SUBSCRIBE TO THE NEWSLETTER

Click Here

The Kentucky Public Service Commission approved the Regional Equipment Sharing for Transmission Outage Restoration, ("RESTORE") agreement allowing participating electric utilities to respond more quickly to power outages and other emergencies and provide greater flexibility to transfer equipment to each other.

The Commission agreed to pre-approve emergency transfers of large transmission system transformers with a value of more than $1 million. A total of 28 utilities in the South and Midwest now participate in the RESTORE agreement.

The agreement also covers less expensive equipment like circuit breakers and gives participating utilities the ability to quickly obtain the equipment needed to complete repairs. Large transformers typically need to be ordered in advance, and the ability to purchase spares from other utilities will greatly speed restoration.

ReliabilityFirst Members

Forward Together RF ReliabilityFirst

AEP ENERGY PARTNERS
AES NORTH AMERICA GENERATION
ALLEGHENY ELECTRIC COOPERATIVE, INC
AMERICAN ELECTRIC POWER SERVICE CORP
AMERICAN TRANSMISSION CO, LLC
APPALACHIAN POWER COMPANY
BUCKEYE POWER INC
CALPINE ENERGY SERVICES, LP
CITY OF VINELAND, NJ
CLOVERLAND ELECTRIC COOPERATIVE
CMS ENTERPRISES COMPANY
CONSUMERS ENERGY COMPANY
DARBY ENERGY, LLP
DATACAPABLE, INC
THE DAYTON POWER & LIGHT CO
DOMINION ENERGY, INC
DTE ELECTRIC
DUKE ENERGY SHARED SERVICES INC
DUQUESNE LIGHT COMPANY
DYNEGY, INC
EDISON MISSION MARKETING AND TRADING, INC.
EXELON CORPORATION
FIRSTENERGY SERVICES COMPANY
HAZELTON GENERATION LLC
HOOSIER ENERGY RURAL ELECTRIC COOPERATIVE, INC
ILLINOIS CITIZENS UTILITY BOARD
ILLINOIS MUNICIPAL ELECTRIC AGENCY
INDIANA MUNICIPAL POWER AGENCY
INDIANAPOLIS POWER & LIGHT COMPANY
INTERNATIONAL TRANSMISSION COMPANY
LANSING BOARD OF WATER AND LIGHT
LINDEN VFT, LLC
MICHIGAN ELECTRIC TRANSMISSION CO, LLC
MICHIGAN PUBLIC POWER AGENCY
MIDCONTINENT INDEPENDENT SYSTEM OPERATOR, INC
MORGAN STANLEY CAPITAL GROUP, INC
NEPTUNE REGIONAL TRANSMISSION SYSTEM, LLC
NEXTERA ENERGY RESOURCES, LLC
NORTHERN INDIANA PUBLIC SERVICE COMPANY
OFFICE OF PEOPLE'S COUNSEL, DISTRICT OF COLUMBIA
OHIO POWER COMPANY
OHIO VALLEY ELECTRIC CORPORATION
OLD DOMINION ELECTRIC COOPERATIVE
PENNSYLVANIA OFFICE OF CONSUMER ADVOCATE
PJM INTERCONNECTION, LLC
PPL ELECTRIC UTILITIES CORPORATION
PROVEN COMPLIANCE SOLUTIONS, INC
PUBLIC SERVICE ENTERPRISE GROUP, INC
ROCKLAND ELECTRIC COMPANY
SOUTHERN MARYLAND ELECTRIC COOPERATIVE, INC
TALEN ENERGY
TENASKA, INC
TENNESSEE VALLEY AUTHORITY
UTILITY SERVICES, INC
VECTREN ENERGY DELIVERY OF INDIANA, INC
WABASH VALLEY POWER ASSOCIATION, INC
WISCONSIN ELECTRIC POWER COMPANY
WOLVERINE POWER SUPPLY COOPERATIVE, INC