Issue 1
2019 January/February

INSIDE THIS ISSUE

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

Follow us on:

RELIABILITY FIRST

Note from the President

Dear Stakeholders,

I continue to be encouraged by NERC and specifically Jim's Robb's approach to carrying out our noble mission. We are certainly in the midst of great change. The industry continues to evolve around us at a rapid pace and we have several new leaders in the Regions (including here at RF), making it a great time for fresh perspectives and transformation. I'm pleased to see the ERO seizing the opportunity to improve our work and continue making changes for greater alignment.

Keeping with this collaborative spirit, this issue highlights recent NERC lessons learned, including one from the RF Region of an entity we are proud of for sharing their journey and embracing change to reduce misoperations. You will see other aspects of change discussed, including an update from PJM on Gas-Electric Coordination and a thoughtful piece from our Manager of Entity Development on how happiness and continuous improvement can enhance reliability. This issue also includes the start of a series on insider threats and a look at event analysis and some of the unknowns facing our industry.

We have some future dates for you to save and new workshops coming up. Of course, another change on our end is that we welcomed a new VP and GC, Rob Eckenrod, and this issue will tell you a little more about him. I am also pleased we welcomed two new Board members this year, Jennifer Curran from MISO for the RTO Sector and Bob Mattiuz from First Energy for the Transmission Sector.

And finally, you will see the details inside, but I would like to mention my personal congratulations to one of our long-standing Independent Directors, Larry Irving, for his recent recognition.

I am continually impressed by the people I am surrounded by and am excited to start the year with positive energy as we all continue to perform quality work to further our collective vision for reliability.

Forward Together,

Tim

Happiness and Continuous Improvement

By: Erik Johnson, Manager Entity Development

How Continuous Improvement Can Increase Happiness (And Improve Reliability!)

A 2011 Harvard Business Review article stated that the level of happiness has a profound impact on workers' creativity, productivity, commitment and collegiality.[1] Further studies have shown that happy employees are up to 20% more productive than unhappy employees.[2]

Let's explore these findings. There are four primary chemicals in the brain that affect happiness: dopamine, oxytocin, serotonin, and endorphins. Additionally, these are also classified as excitatory neurotransmitter chemicals,[3] meaning they stimulate brain activity. Based on this knowledge, the conclusion can be drawn that the happier you are the more dopamine, oxytocin, serotonin, and endorphins are coursing through your brain resulting in greater creativity and productivity among other attributes.

What does this have to do with reliability? Allowing employees to have a direct influence on their work while striving for continuous improvement creates a positive experience for the worker. This, in turn, makes the worker happier and raises their creativity and productivity.

Let's look at an example.

NERC Standard PRC-004-5, R5 states the following:

Each Transmission Owner, Generator Owner, and Distribution Provider that owns the Protection System component(s) that caused the misoperation shall, within 60 calendar days of first identifying a cause of the misoperation: [Violation Risk Factor: High] [Time Horizon: Operations Planning, Long-Term Planning]

- Develop a Corrective Action Plan (CAP) for the identified Protection System component(s), and an evaluation of the CAP's applicability to the entity's other Protection Systems including other locations; or
- Explain in a declaration why corrective actions are beyond the entity's control or would not improve BES reliability, and that no further corrective actions will be taken.

Notice there are no specifics related to the required Corrective Action Plan (CAP), therefore a minimal level of effort could be used to ensure the checkbox has been filled (for example, using a "cookie-cutter" approach of applying existing or prior corrective action plans to subsequent misoperations). Think about that repetitive task and the impact to someone's happiness level? No dopamine, oxytocin, serotonin, or endorphins anywhere to be found!

Conversely, think about the approach with continuous improvement activities woven in to the CAP. An example would be the development of a query that uses the characteristics of the misoperation (i.e., relay make/manufacturer and associated settings) and determines where else on the system this configuration may be in place and require review/remediation.

Or, consider a process that we have seen being used in our footprint:

When initial analysis revealed relay misoperation issues with commissioning done by a contractor, an entity proactively retested the contractor's work. This identified multiple locations with similar conditions that were remediated before a misoperation occurred.

When continuous improvement activities are woven into the historical "cookie-cutter" approach to compliance based activities, even though they are over and above what is required by the Standard, these activities provide additional meaning, creativity and happiness to an individual's work. Therefore, continuous improvement activities not only increase reliability on their own merits, they can also increase employee happiness (and from that, their productivity, creativity, and commitment). For ideas on how to integrate continuous improvement activities into your compliance program, contact the Entity Development department.

[1] https://hbr.org/2011/05/the-power-of-small-wins

[2] https://www.forbes.com/sites/forbescoachescouncil/2017/12/13/promoting-employee-happiness-benefits-everyone/#53a95272581a

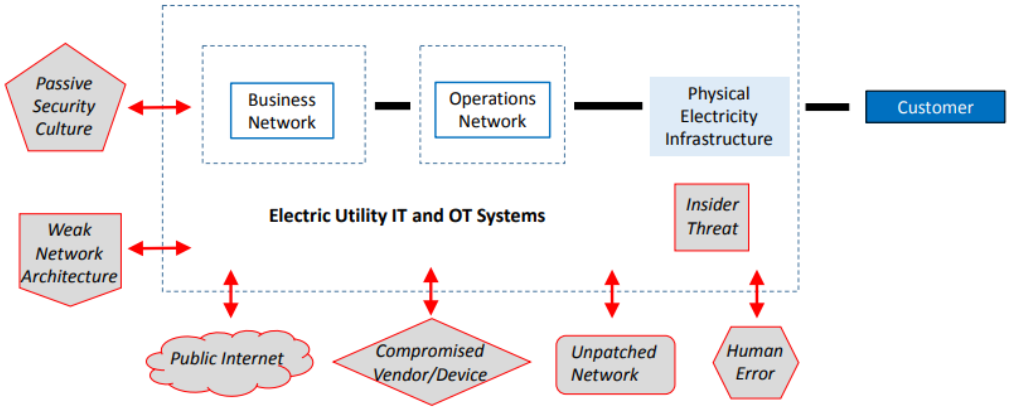
[3] https://www.ncbi.nlm.nih.gov/books/NBK21521/

Continued on page 4

Insider Threats Program - Part 1

By: Bheshaj Krishnappa, Principal Analyst and Certified Insider Threat Program Evaluator

The electricity supply chain is a complex network of people, processes, and technology. Disruptions to this supply chain can come in many forms. A recent DOE report, "Assessment of Electricity Disruption Incident Response Capabilities" includes considering human factors, such as insider threats, as one of the cyber-attack vectors to strengthen the cybersecurity of the electricity supply chain.



Cyber Attack Vectors for an Electric Utility (DOE, 2017)

A 2009 report, "Modeling the Employee Life Cycle to Address the Insider Threat" from Sandia National Laboratories, notes the motivators for insiders committing malicious activity - some of these motivators are set forth in the upper right corner of this page.

Unlike other commodities, motivation to steal electricity for personal benefit is rare, as it can be dangerous and transportation and storage costs are high. However, the societal impact of electricity disruption is high, and the economic impact on the owner of the disrupted electric facility can be high.

As the electricity supply chain includes vast geography and a diverse work force, there is a variety of personality styles to consider as potential risk factors for malicious insider activity. Some of the styles noted from the Sandia report are noted below:

Self-centered	*Arrogant*	*Adventurous*	*Manipulative*
Cold	*Grandiose*	*Self-deceptive*	*Defensive*

Motivators for Malicious Activity:

Money	**Ingratiation**
Divided loyalties	**Coercion**
Recognition	**Thrills**
Resentment (including revenge)	

The CIP Standards establish minimum requirements for utilities in securing the Bulk Electric system. The following Standards and Requirements indirectly address the risks associated with insider threats:

1. **CIP-004-6 R3 Cyber Security — Personnel & Training**

   Requires Personnel Risk Assessments (PRA) for all personnel requiring access to cyber or physical BES assets. This ensures personnel are properly vetted before they are granted access to facilities and data.

2. **CIP-007-5 Table R4 – Cyber Security - System Security Management**

   Requires entities to log and generate alerts for successful or failed access attempts and failed login attempts along with detecting malicious code.

3. **CIP-005-5 Table R1 P1.5 - Cyber Security - Electronic Security Perimeter(s)**

   Requires entities to implement methods for detecting known or suspected malicious communications for both inbound and outbound communications.

4. **CIP-006-5 Table R1 P 1.4 - Cyber Security - Physical Security of BES Cyber Systems**

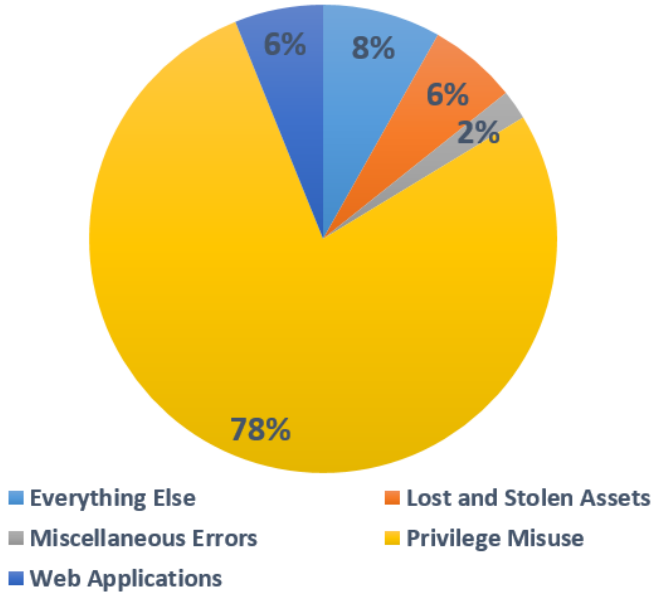
   Requires entities to implement a solution to monitor unauthorized physical access into a Physical Security Perimeter.

Continued on page 4

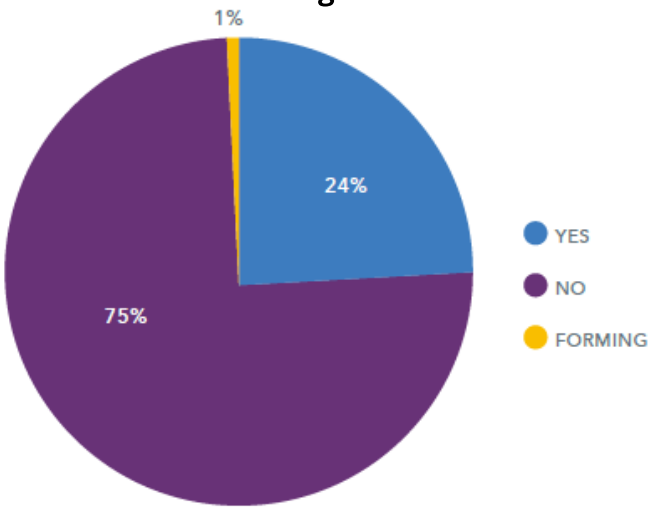
Insider Threats Program - Part 1

Continued from page 3

Types of Insider Threats Resulting in Publicly Reported Breaches



Percentage of Organizations with an Insider Threat Program Team



To help mitigate the insider threat risk, companies can implement timely detection and response mechanisms, policies and procedures, and training programs.

From the review of the VERIS Community Database, which contains about 6,700 publicly reported breaches from 2013 to 2019, a majority of events containing some form of insider threat as a core element of cyberattack showed privilege misuse as the pattern. This can be an attack vector in the electricity supply chain where individuals have authorized unescorted physical access.

Additionally, a Veriato sponsored study, "2019 Insider Threat Program Maturity Model Report" shows a majority of organizations do not have a formalized Insider Threat Program Team. Thus, there is a tremendous opportunity for entities to formalize an Insider Threat Program using the best practices and methodologies associated with CIP program management.

Even though the potential risk from malicious insiders is high and a complex challenge, there is a structured way an Insider Threat Program can be instituted in an organization depending on the critical assets to protect. In fact, several financial, healthcare, National Intelligence, and Defense organizations have already implemented an Insider Threat Program.

The CERT Insider Threat Center from Carnegie Mellon University is a leader in insider threat research and education for interested individuals. In upcoming newsletters, I will be covering how an Insider Threat Program can be instituted in the electricity industry.

References:

Assessment of Electricity Disruption Incident Response Capabilities

Modeling the Employee Life Cycle to Address the Insider Threat

2019 Insider Threat Program Maturity Model Report

Events Analysis, EMS Events, and the Great Unknowns

By: Brian Thiry, Principal Analyst

Two of the risks RF highlighted in its 2018 Regional Risk Assessment were the *Unknown Unknowns* and the Unknown Knowns. The *Unknown Unknowns* are the risks that we truly do not know anything about. These can be emerging risks and are troubling because they present blind spots which impair our ability to prepare for, and mitigate against their occurrence.

As a corollary to these risks are the Unknown Knowns, which are risks where data may be available within the organization, but it is not readily available to those requiring the knowledge.

While these may sound esoteric at first, the RF Events Analysis and Situational Awareness (EASA) Team attempts to tackle these risks. Through our Situational Awareness work, EASA monitors various channels to discover threats and vulnerabilities to the Bulk Power System (BPS).

This activity includes performing research and data-gathering across our industry and other industries to help identify emerging risks to start learning about the Unknown Unknowns. We can hereby turn them into a new category, Known Unknowns.

The Known Unknown is a risk that we know exists and we know nothing about. This work is forward-looking as we try to anticipate threats and vulnerabilities to the grid. We look at news stories and current events such as the government shutdown, climate change, and outsiders meddling with (hacking) U.S. elections and social media sites and ask the question,

> "How could this impact the grid?" and
>
> "What could we learn from this?"

Even modern innovations such as an increase in use of unmanned-aircrafts (commonly referred to as drones) has implications on how the BPS is operated.

The Events Analysis work is less forward-looking as the EASA team analyzes events that have occurred and helps review the entity's Root Cause Analysis of the event. When analyzing events with industry, the EASA team uses NERC's methodology for the Cause Code Assignment Process.

Using this tool, the root and contributing causes are broken into different A-level cause codes for Design/Engineering:

(A1), Equipment/Material
(A2), Individual Human Performance
(A3), Management/Organization
(A4), Communications
(A5), Training
A6), Other
(A7), Configuration (AX) and ***Information to determine cause less than adequate (AZ)***.

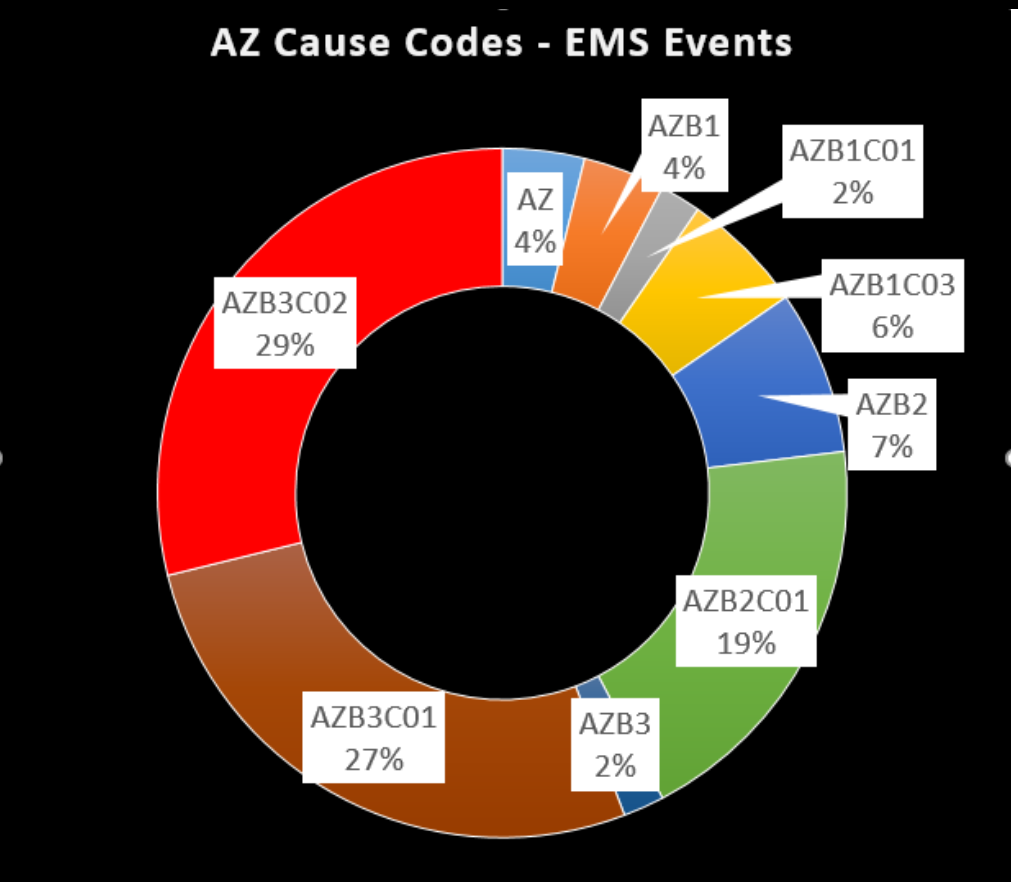
This newsletter article explores the AZ codes which are often *known unknown* Risks.

The most frequent type of event analyzed the past three years in the RF region has been the EMS (category 1h.v) events where the entity has lost situational awareness tools in their control center. When analyzing these events, there are almost always several contributing causes plus a root cause; it's almost never just one thing.

Continued on page 6

Events Analysis, EMS Events, and the Great Unknowns

Continued from page 5



When reviewing all the EMS cause codes from the past three years, of the 367 cause-codes used, 52 of them (14%) were in the **AZ** section signifying some type of *Unknown*. As per the NERC methodology, an AZ code is always a root cause as the information to determine the root cause was less than adequate (LTA). The donut chart above shows the type of AZ codes we have encountered the past three years when looking at EMS events.

Diving into the specific AZ C-level codes (*e.g.* **AZB1C01**) helps provide context on what is *Known* and what is *Unknown*.

Below are the definitions of the codes and the percentage of times they are tagged as part of the 52 AZ cause codes the past three years for EMS events.

AZB1C01: ***Multiple, parallel causal sequences exist*** (2%).

While this may seem like an Unknown, the only part Unknown is what the definitive root cause was. In these cases, there were multiple sub-events that occurred that all contributed to the overall event.

Action Item for the Entity:

Not knowing which cause was the root cause is not as problematic if the entity addresses all the mini-causes. If controls are put in place to mitigate all the contributing causes, the chances of recurrence are decreased.

AZB1C03: ***No cause uncovered after exhaustive testing*** (6%).

This code may be more problematic than its predecessor. For this K*nown Unknown*, we know what happened, and we did our best to figure out *why* it happened, but we could not reproduce the issue.

Action Item for the Entity:

The exhaustive testing is good, but not discovering the cause is the problem. Sometimes these are EMS issues where a reboot or restart of the application erased log entries or other forensics that would be useful for the vendor when analyzing the issue. If possible, take a snapshot of all error messages and log entries that may be erased when restarting applications.

Sometimes this code is used when there is a power outage that caused the EMS outage and the entity cannot determine the initiating fault after testing. In this case, the root cause of the fault is less important than the resilience of the design to switch to UPS and/or backup generators (if applicable) following the loss of power.

AZB2C01: ***Apparent cause analysis only*** (19%).

When using this code, once again we know 'what happened' but the *Unknown* is 'why it happened.'

Action Item for the Entity:

Similar to AZB1C03, it may be less important to know why something

Continued on page 7

Events Analysis, EMS Events, and the Great Unknowns

Continued from page 6

happened as long as controls are in place to detect and correct the problem. Following a risk assessment, preventing the problem may not be the best use of resources (*e.g.* how I prevent that UPS equipment failure, or how do I prevent that unknown topology change 30 busses outside of my system), however the entity installs enhanced detective controls to discover the issue and recover quickly. Unfortunately because the root cause isn't mitigated, it may be inevitable that the same problem will occur again, however next time we will be ready!

AZB3C01: ***Other entity cited as involved in event*** (27%).

This code is commonly used for data-related EMS issues where another entity sends ICCP data that appears to be of good quality but is erroneous (*e.g.* a neighboring entity sends data that indicates there are 3,000 MW of flow through a sub-transmission transformer. This data impacts the state estimator's ability to determine the voltage in that area plus the impact of contingencies. It's unreasonable that there are actually 3,000 MW on that transformer without tripping for a fault condition.) Another instance may be an ICCP communication link problem that was caused by the neighbor impacting the ability to share data.

Action Item for the Entity:

While the root cause analysis of the event does not typically go into details on 'why' the neighboring entity sent the bad data or caused the ICCP tunnel to collapse, there are two important action items the impacted entity can take. First, evaluate controls that can be implemented on your system to prevent, detect, and correct the error. For example, some entities implement reasonability limits on external data, freeze last known good values, or revert to previously known good values. Second, talk with your neighbor (and/or Reliability Coordinator) about 'why' they were sending the bad data. Was it an RTU issue or polarity issue (-60 MW instead of 60 MW)? Has their issue been resolved or will it continue to happen? Is there anything you can learn from their issue to improve your own EMS performance?

AZB3C02: ***Vendor or contractor cited as involved in event*** (29%).

The combination of AZB3C01 and AZB3C02 (other party involved in the event) accounts for over half of the AZ codes used when analyzing EMS events in the RF region. In this case, there was some type of vendor issue, often a software or code issue that caused the event. We don't know 'why' the vendor's code was wrong, but a patch, upgrade, or new line of code was provided to enhance performance.

Action Item for the Entity:

There are things entities can do to hopefully prevent this type of event. First, ensure that you have a good relationship with your EMS vendor and that contracts are in place regarding contact personnel and support. Ensure that the operations support personnel know who to call when there is a problem and what data they need to provide for troubleshooting purposes.

Second, monitor the vendor's website or portal for patches, upgrades, and other maintenance fixes. Although your system may be working fine, there may be a latent error, waiting for a trigger to cause an EMS failure that could be prevented.

Third, consider periodic reviews with the vendor's help of system parameters and settings. There are different flags and weighting levels that may need to be adjusted as models are expanded or system conditions change. Finally, get involved with EMS-related communities whether it be attending the vendor's conference, joining the NERC EMS Working Group, attending the NERC Monitoring and Situational Awareness Conference, or working with NATF as they share EMS-related Lessons Learned. All of these may be able to help identify (and hopefully prevent) a future EMS issue.

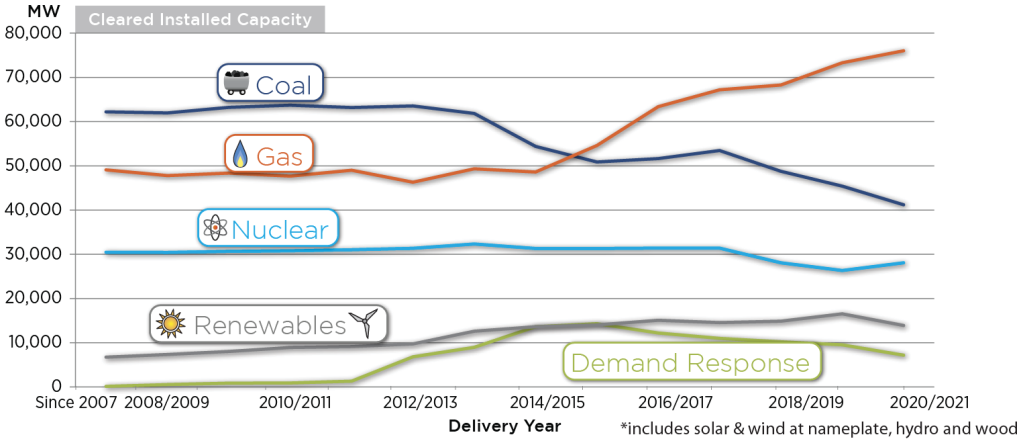
In summary, the *Great Unknowns* are not always an *Unknown* as they may appear. While these risks provide more challenges than the *Known Knowns*, there are opportunities to learn from and mitigate these types of events. The EASA team is committed to work with the entities in reviewing these events and helping to stabilize (and reduce) the frequency and occurrences of EMS-related issues.

The Seam

By: PJM Interconnection, LLC

Gas-Electric Coordination

In recent years, PJM Interconnection has seen a major shift in its generation resource profile away from coal and to natural gas. The challenging economics and environmental requirements for coal-fired generators, combined with the low cost and abundant supply of natural gas, have made natural gas-fired generators the primary new generation built in the PJM footprint.



With the growing dependence on natural gas, PJM recognized a need to focus more attention on communications and coordination with the interstate gas pipelines and local gas distribution companies that serve gas generators. The fuel delivery limitations experienced during extreme cold of the Polar Vortex winter of 2013-2014 reinforced within PJM and the industry that there was a need to gain a better understanding of the mechanics of the natural gas supply and transportation sectors.

After the Polar Vortex, PJM implemented the PJM Gas Electric Coordination Team to help increase communication and coordination. The team provides operational awareness of gas delivery and potential generator availability risks to PJM dispatch.

PJM also made a significant operational change by moving its Day-Ahead award timing from 4:00 p.m. EST to 1:30 p.m. EST. This change allowed generators to know their Day-Ahead generation requirements prior to the timely nomination deadline, giving them an opportunity to procure gas supply within the timely nomination cycle.

Around the same time, two key regulations were implemented by FERC to improve gas-electric coordination:

- **FERC Order 787** allowed the sharing of non-public operating information between interstate pipelines and electric transmission operators.
  FERC Order 809 adjusted pipeline gas nomination cycles to improve gas-electric coordination. On April 1, 2016, the deadline moved from 12:30 p.m. EST to 2:00 p.m. EST, and a third intraday nomination cycle was added to increase scheduling flexibility.

As the use of natural gas for electric generation continues to grow and supplant retiring coal-fired resources, the need for collaboration between PJM and the natural gas industry related to system reliability and resilience will also increase. Opportunities for increased collaboration include contingency analysis, tabletop exercises, system restoration drills and enhanced emergency communications.

PJM and the natural gas industry have made tremendous strides in coordination and collaboration and PJM looks forward to building on that success to ensure the safety, reliability and resilience of the bulk electric system.

Recent NERC Lessons Learned

In Section 800 of NERC's *Rules of Procedure* , NERC spells out an important objective of the Events Analysis and Situational Awareness (EASA) team: ***Analyze off-normal events on the Bulk Power System and disseminate Lessons Learned to the electric industry to improve reliability performance.*** RF's EASA Team works with NERC and our entities to create and share Lessons Learned from both our region and other regions. These can be found on NERC's homepage (NERC.com) under the *Reliability Risk Management* program area.

We find these Lessons Learned important enough to re-share here, because we believe in the value of learning from others experiences and that these truly serve as a resource to convey risks and opportunities to improve, whether by driving continuous improvement or adding resilience to existing systems.

In December 2018, NERC published three new Lessons Learned that we'd like to draw your attention to, with two specifically from the RF region.

Lessons Learned

Avoiding IROL Exceedances with Rigorous Inspections during Commissioning, Consistent IROL Alarms, and Improved Training

This comes from the NPCC region and includes two important reminders for industry:

a. Alarming in a control room should clearly differentiate between System Operating Limits (SOLs) and Interconnection Reliability Operating Limits (IROLs) so that operators know the severity and how quickly they need to respond.

b. Commissioning tests are critical to prevent latent errors and future outages.

Cascading Analysis Identifies Need for Pre-Contingent Load Shed

This comes from the RF region and this event was presented at the 2018 NERC September Operating Committee meetings. This is an interesting event with parallels to the 2003 Blackout (hot weather, misoperation, vegetation contact, EMS issues), *however* this Lessons Learned acknowledges the resilience of the system: the ability to absorb the event, detect issues, and recover quickly.

Cascading Analysis is a key control for detecting IROL or IROL-like conditions to prevent a significant outage.

Initiatives to Address and Reduce Misoperations

This lesson from the RF region started off with a specific misoperation event, but transformed into one entity's journey to improve their overall misoperations rate. This document provides a summary of one entity's individual misoperations risk assessment and how they used a multi-faceted approach to improve the dependability and security of their protection systems.

This document is somewhat similar to RF's, WECC's, and SERC's ***CIP Themes Report*** in that it can be shared with both subject-matter experts and executive leadership to develop action-oriented steps to address the root causes of misoperations in your footprint. The RF region is proud of this entity for sharing their journey with the rest of the ERO enterprise.

By: Lew Folkerth, Principal Reliability Consultant

A Structure for CIP Risk Management Plans

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.

As I discussed in the November/December 2018 issue, CIP-013-1 will become effective and enforceable on July 1, 2020. On that date CIP-013-1 will become the first explicitly risk-based CIP Standard. I do not believe it will be the last such Standard. The Project 2016-02 Standard Drafting Team has posted a set of "CIP Virtualization Updates" that are mostly risk-based as well.

Whether a Standard says "[D]evelop one or more documented supply chain cyber security risk management plan(s)" (CIP-013-1) or "[I]mplement one or more documented processes to mitigate the risk posed by unauthorized communications to and from applicable systems…" (CIP-005-7 Draft 1), you will need to have a risk management plan or process in order to fulfill the requirements of the Standard. In this column I'll explore what I think the structure of such a plan might look like.

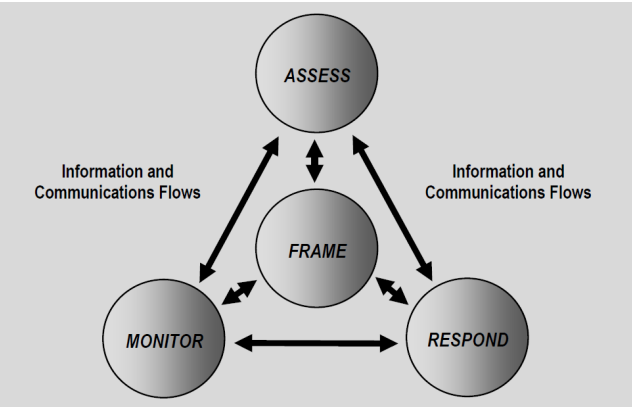


Figure 1: Risk Assessment within the Risk Management Process
Source: SP800-30

Munising Range Lights, Munising, MI - Photo by Lew Folkerth

The structure that follows (see Figure 1) is based on NIST SP800-30, the Guide for Conducting Risk Assessments (found here). I also recommend reading NIST SP800-39, Managing Information Security Risk (found here).

FRAME

Your risk management plan for a CIP Standard should provide a frame for your approach to risk management. The frame provides the context for your risk-based decisions. The frame should contain the following elements:

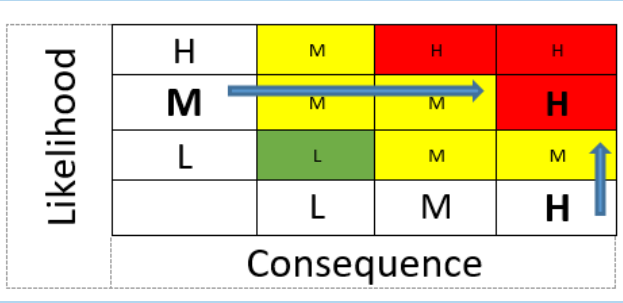
Scope:

You should carefully identify the scope for your plan. If the scope is too narrow, you risk violating the Standard by not considering all of the required risk areas. If your scope is too broad, you will expend resources and funds that may provide little benefit. You may want your scope to include an inventory of Cyber Assets that are covered by your plan, as well as a list of vendors that may be affected by implementation of the plan (such as for CIP-013-1).

Continued on page 11

Continued from page 10

Simplified Risk Assessment Methodology



In this methodology, you qualitatively estimate the likelihood of a risk being manifested and the possible consequence if it does occur. For example, you might assess the likelihood of purchasing counterfeit equipment as medium, and the consequence of implementing such equipment as high. In the methodology above, this would assess as a high risk.

Objectives:

The objectives of the risk management plan should be clearly identified. For example, your CIP-013-1 risk management plan should include the four objectives from FERC Order 850 P2, as well as any additional objectives that are appropriate for supply chain risk management at your organization.

Risk Assessment Methodologies:

The methods you use to assess risk should be spelled out in this section. Each methodology (you can use more than one) will lay out the steps you will need to take to assess the risks you identify. These steps should take into account the inputs to the process (e.g., threat sources, threat events, vulnerabilities, predisposing conditions, etc.). Simpler may be better here (see sidebar), but you will need to select the methodologies that you determine are best suited to your organization. If you create a complex methodology to assess your risks, then you will need to be able to explain that methodology to an audit team.

Definitions:

Any terms used in risk management that may be ambiguous and that are not defined in the Standard should be defined here. Try to keep to generally accepted definitions – unusual definitions will probably be questioned.

ASSESS

Your risk management plan should include a process for assessing risks within the scope of the plan. Volumes have been written about this topic, so I will sketch out a possible outline for a CIP-related assessment.

Identify possible risks:

I think the best approach to identifying possible risks is to cast a wide net and then narrow down the results. Some possible sources of threats include:

- US-CERT
- NCCIC (formerly ICS-CERT)
- E-ISAC
- Vendors

Apply the scope for this process:

Screen for only those risks that are in-scope for this process. For example, one of the risks you identify might be the risk of opening an email attachment and thereby compromising a BES Cyber System.

This technique was used in the 2015 Ukraine attacks and so should be on your list of possible risks. However, this is not a risk that pertains to supply chain cyber security, so it is out of scope for your CIP-013-1 risk assessment. Instead, that risk should be handled by a different risk assessment process.

Apply the appropriate risk assessment methodology:

Once you apply your risk assessment methodology, you should obtain a risk score or risk rating for each identified risk.

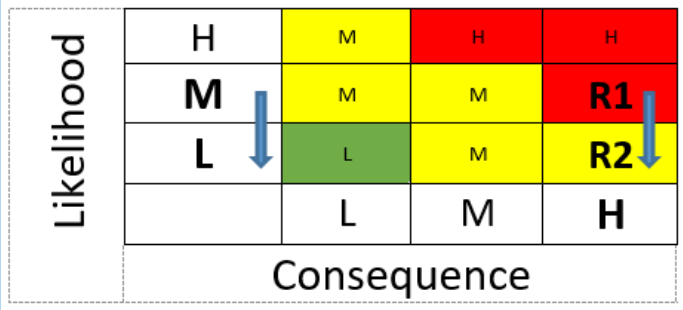
Prioritize the resulting risks:

You can't address all risks, so you will need to prioritize the risks you will address. The risk assessment methodology will result in a raw risk score, which you will need to temper with professional judgment. Analyze the risks with the highest ratings and determine how you could reduce each risk. This will help you determine the order in which you address the risks.

Continued on page 12

Continued from page 11

Reducing Risk



Based on the previous example, you might choose to reduce the likelihood of purchasing counterfeit equipment by purchasing only from the vendor or from an authorized distributor.

This changes the likelihood of the risk being realized from medium to low and also changes the original high risk (R1) to a medium risk (R2).

Evidence of this risk reduction might include your revised purchasing process that shows the acceptable equipment sources, and purchase orders showing that the process has been implemented.

RESPOND

After you have identified, assessed, and prioritized the identified risks, you will need to decide how to respond to those risks. Those responses should consider the need to produce evidence of compliance. You should also show how the actions you take reduce risk. (See the sidebar, Reducing Risk)

MONITOR

Your risk management plan should include a provision to monitor risk over time. This monitoring should:

- include an ongoing determination of the effectiveness of your risk mitigations,
- identify emerging risks and risks that were not included in the most recent assessment, and,
- ensure that sufficient compliance evidence is being produced and retained.

Disclaimer

If you choose to adopt this framework, you will need to modify it to suit your entity and your circumstances. This framework is intended only to demonstrate one possible approach to address the risk and achieve compliance.

Requests for Assistance

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

Feedback

Please provide any feedback you may have on these articles. Suggestions for topics are always welcome and appreciated.

I may be reached here.

Protection Settings Evaluation Tool

Automated Wide-Area Protection Coordination Studies with EPRI's Protection Settings Evaluation Tool (PSET)

Wide-area coordination studies are an essential part of maintaining dependable and secure protection across the transmission network, helping to proactively identify potential misoperations before they occur as well as other opportunities for improvement. However, performing these studies manually requires a significant time investment and can leave the door open for mistakes and inconsistencies. While individual changes to the transmission network normally trigger a review of protection in the local area, the cumulative effect of multiple network changes across a larger area can result in protection breakdowns that may go unnoticed.

Automating the wide-area study process significantly reduces the time required to perform the study and to compile, analyze, and prioritize results. The parameters of an automated study can be standardized to maintain consistency, identify changes in results from one study to the next, as well as allowing tracking and trending of results over time to quantify improvement.

The Protection Settings Evaluation Tool (PSET) was developed by the Electric Power Research Institute (EPRI) as part of project P40.018: Transmission System Protection Support Tools, to perform automated wide-area protection coordination studies. The present implementation of this tool is in the form of a macro for two of the most commonly used protection simulation programs: CAPE (Computer-Aided Protection Engineering) by Siemens, and OneLiner by ASPEN (Advanced Systems for Power Engineering).

The PSET study parameters are highly customizable by the end-user, including the ability to specify the areas to be studied, voltage levels, fault types, fault locations, network contingencies, and various other criteria to define what constitutes a violation based on your methodology.

The PSET study results are compiled into an XML output file, which can be reviewed using a web browser, spreadsheet, or database. EPRI has developed a customized Microsoft Excel spreadsheet and Microsoft Access database to facilitate advanced analysis and reporting. Multiple results files can be loaded into the spreadsheet or database for comparison and tracking. The PSET output file also stores fault current magnitudes at each bus involved in the study. EPRI's custom spreadsheet includes a tool to identify any buses where the fault current magnitude has changed more than a user-specified percentage between two results files, which can be used to signal the need for a protection review.

Automated wide-area protection coordination study tools, such as the PSET by EPRI, provide tremendous value by reducing the time and effort required to perform in-depth protection studies across a large network, allowing proactive action to be taken to mitigate the issue prior to a real misoperation occurring, and thereby increasing the reliability of the protection system as well as the transmission network.

For more information on the solution contact Sean McGuinness, Grid Operations and Planning, EPRI.

EPRI ELECTRIC POWER RESEARCH INSTITUTE

NERC, Water Sector Launch Security Information Sharing Effort to Promote Cross-Sector Collaboration

On January 16, 2019, NERC announced its Electricity Information Sharing and Analysis Center (E-ISAC) is collaborating with the Water Information Sharing and Analysis Center (WaterISAC) to enhance energy security.

The collaboration will include staff from WaterISAC joining E-ISAC in Washington, D.C., to improve coordination on potential security risks related to the supply of electricity to water and wastewater treatment plants, and the supply of water to electric utilities for cooling power plant turbines and for office operations.

The teamwork between the E-ISAC and WaterISAC is based on developing a robust information exchange on security risks.

Some of the goals under the partnership include:

- improving security collaboration between the two industries,
- jointly analyzing security concerns, and
- enhanced information sharing and situational awareness

The E-ISAC and WaterISAC have agreed to use existing policies and procedures for safeguarding sensitive information under the partnership.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

WATER ISAC

Standards Update

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

General NERC Standards News

Process Changes for SARs and RFIs Coming Soon

In the next couple months, NERC will be implementing changes in how all Standard-related inquiries and submissions, including Standard Authorization Requests (SARs) and Requests for Interpretations (RFIs), are processed. These inquiries and submission will have to submitted via the Help Desk. Additionally, separate sites for SARs and RFIs will be available on the Standards page to keep a record of submissions that have been rejected by the Standards Committee.

Implementation Guidance Posted

NERC posted the following compliance guidance documents on its Compliance Guidance page:

- ERO Enterprise-endorsed Implementation Guidance document addressing PRC-024-2, R2 Generator Frequency and Voltage Protective Relay Settings;
- A Proposed Implementation Guidance document addressing MOD-025-2, R1, R2, R3 – Verification and Data Reporting of Generator Real and Reactive Power Capability; and,
- An ERO Enterprise CMEP Practice Guide: Information to be Considered by CMEP Staff Regarding Inverter-Based Resources, which outlines information related to BES inverter-based resources that should be considered by CMEP staff in understanding how registered entities have mitigated reliability risk, including risk that may not be addressed in specific Requirements.

Other Resources Posted

NERC has posted the following resources:

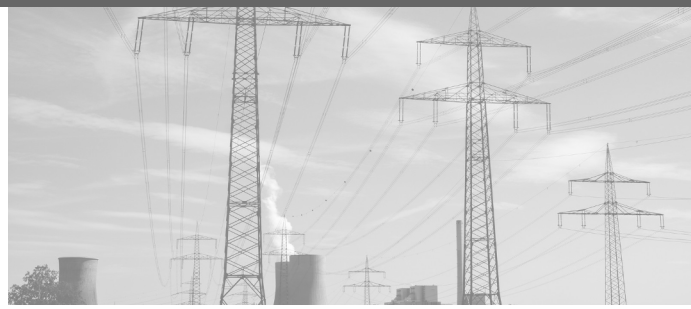
- The streaming webinar and slide presentation for the December 18, 2018 Project 2017-07 – Modifications to BAL-003-1.1 webinar.
- The April and May 2018 Fault Induced Solar Photovoltaic Resource Interruption Disturbances Report, which documents the analyses of two disturbances involving the loss of solar photovoltaic facilities in response to normally cleared transmission line faults.

Notable NERC Filings

In December, NERC filed the following:

- Petition for Approval of Proposed Reliability Standard TPL-001-5; and,
- Informational Filing regarding the Reliability Standards Development Plan 2019-2021.

NERC's filings can be found here.



General NERC Standards News

FERC Approves Errata Change

FERC approved an errata correction to the Implementation Plans for the Reliability Standards MOD-026-1 and MOD-027-1 to align the Implementation Plans' periodicity reference to the date of "submittal" rather than "verification."

Notable FERC Issuances

In December, FERC filed the following:

- Letter Order Approving Registration Request of Wisconsin Public Service Corporation (WPSC) and Upper Michigan Energy Resources Corporation (UMERC) from the Midwest Reliability Organization Regional Entity footprint to the ReliabilityFirst Regional Entity footprint.

FERC's issuances can be found here.

Standards Update

New Standards Projects

Several new Standards projects and new project phases are underway. Projects are described on the NERC Standards website, along with links to all drafts, voting results, and similar materials. Recent additions include the following projects:

Project	Action	Start/End Date
Comment Period Open for Primary Frequency Control – Reliability Guideline and Balancing Authority Area Footprint Change Tasks – Reference Document	Submit comments via email using the appropriate comment matrix: Primary Frequency Control-Reliability Guideline Comment Matrix; Balancing Authority Area Footprint Change Tasks - Reference Document Comment Matrix	1/3/19 - 2/18/19

Recent and Upcoming Standards Enforcement Dates	
April 1, 2019	BAL-002-3- Disturbance Control Standard - Contingency Reserve for Recovery from a Balancing Contingency Event; 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
July 1, 2019	CIP-003-7 – Cyber Security – Security; Management Controls; PRC-026-1 – Relay Performance During Stable Power Swings (Requirements 2-4)
January 1, 2020	CIP-003-7 – Cyber Security – Security Management Controls; PRC-026-1 – Relay Performance During Stable Power Swings (Requirements 2-4); PRC-026-1- Relay Performance During Stable Power Swings (Requirements 3-4)
July 1, 2020	CIP-005-6 – Cyber Security – Electronic Security Perimeter(s); CIP-010-3 – Cyber Security – Configuration Change Management and Vulnerability Assessments; CIP-013-1 – Cyber Security – Supply Chain Risk Management PRC-002-2 – Disturbance Monitoring and Reporting Requirements (50% compliance for Requirements 2-4, 6-11)
October 1, 2020	PER-006-1 – Specific Training for Personnel ; PRC-027-1 – Coordination of Protection Systems for Performance during Faults
January 1, 2021	PRC-012-2 – Remedial Action Schemes; TPL-007-1 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements 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 (100% compliance for Requirements 2-4, 6-11)

These effective dates can be found here.

RF Board member, Larry Irving, receives the Charles B. Rangel Innovative Person Award and is recognized by International Internet Society

Silicon Harlem has named RF Board Member Larry Irving as the recipient of the Charles B. Rangel Innovative Person Award. Silicon Harlem helps enable the technological accessibility necessary to transform the Harlem/Upper Manhattan community into a technology and innovation hub.

Mr. Irving, having originated from Brooklyn, is particularly passionate about these efforts. Congressman Rangel himself presented the award to Mr. Irving, describing Larry as “a credit to humanity.”

Additionally, the Internet Society incorporated Irving’s remarks made at Silicon Harlem for the Innovative Person Award presentation in their year ending "12 Streams" video. The Internet Society is a nonprofit organization dedicated to providing global leadership in internet related matters. In his remarks, Mr. Irving discussed contemporary innovation – virtual reality, autonomous vehicles, robotics, facial recognition, data control – and the related social implications looking forward.

RF is proud to have accomplished and innovative individuals such as Mr. Irving as part of our Board of Directors. In addition to serving as a board member at RF, Mr. Irving is a board member at the Education Networks of America, Northwestern University, and the Public Broadcasting Service. He is also the co-founder of The Mobile Alliance for Global Good and CEO of The Irving Group. He has served as Vice President for Global Government Affairs for the Hewlett-Packard Company, and also served for almost seven years as Assistant Secretary of Commerce for Communications and Information and Administrator of the National Telecommunications and Information Administration (NTIA), where he was a principal advisor to the President, Vice President and Secretary of Commerce on domestic and international telecommunications and information technology issues.

ReliabilityFirst's Board of Directors and Committee Meetings will be held at the RF Offices in Cleveland, OH on March 13-14, 2019.

Click here for details

Meet our New Vice President and General Counsel

RF is pleased to announce that as of January 7, 2019, Rob Eckenrod has assumed the role of Vice President and General Counsel.

Rob joins us from PJM Interconnection, LLC (PJM) where he most recently served as the Chief Compliance Officer. In that role he was responsible for implementing and maintaining PJM's enterprise-wide compliance management and enforcement program as well as providing legal and policy advice and advocacy on behalf of PJM for all reliability compliance functions.

Mr. Eckenrod accomplished this via overseeing multiple compliance business units and chairing PJM's compliance committee that reported directly to the PJM Board.

On a personal level, Rob has three children: Alexandrea, Tiffini, and Haileigh, with his wife, Bridget. The Eckenrod home also includes a dog (Ginger), two cats (Pebbles and Bam Bam) and a red-footed tortoise (Taco), as well as assorted Bob Ross paraphernalia. Mr. Eckenrod is new(ish) to the Cleveland area, having spent some time here during his first year of law school. He is excited to return to the "small, big city" atmosphere that reminds him of his hometown and alma mater (and favorites sports teams), Pittsburgh.

Q: How did you get into the energy industry?

My first experience with the energy industry was as an attorney at the PA Public Utility Commission soon after I graduated law school. There, I was assigned to the agency's Energy Group during a time of significant change in the retail electric industry with the introduction of retail electric competition. After serving several years in that capacity, I was chosen to serve as an advisor to a Commissioner and ultimately found myself adjudicating utility rate cases before the Commission.

Q: How do you think your industry background will play into your new role?

I like to think I bring a unique perspective because of the broad-based experience I've encountered throughout my career. I was employed by a regulatory agency overseeing not only the energy industry but all other utilities, each of which had their own nuances in terms of regulation and governance. While there, I served in several different capacities which allowed me to see different facets of utility regulation, including the ratemaking process. Couple that with the experience I gained as, initially, an attorney, and ultimately the Chief Compliance Officer of PJM, one of our registered entities, and I think it will serve the organization well to have those experiences come into play. My hope is that my background will serve to benefit the people on my team, or, indeed, anyone here at RF who may have not had similar experiences.

Q: What are you looking forward to accomplishing at RF?

I am excited to be working with the people here and to learn more about what they do on a daily basis. Even though I have interacted with many of the folks here over the years in different capacities, I have found in my short time here that there's much about RF that works behind the scenes. More importantly, I see it as a great opportunity to work with Tim and help the organization implement his strategic vision to position the company as an industry resource partner rather than solely as a regulator. With that in mind, I plan to emphasize doing what I can to assist the organization in identifying areas of improvement and developing more efficient and effective compliance and risk assessment programs. That, and of course, exploring the varied micro-breweries in and surrounding Cleveland.

Watt's Up at RF - Save the Date

New! Substation Maintenance Group, A Community of Practice Initial Conference Call March 22, 2019 at 9:00 am ET

ReliabilityFirst is forming a Community of Practice for substation maintenance personnel. This includes, but is not limited to: substation supervisors, substation electricians, substation field engineers, relay technicians, and relay engineers. A Community of Practice (CoP) is a group of people who share an interest or a passion for something they do and learn how to do it better as they interact regularly with other colleagues in their field of expertise. This is an informal gathering of substation maintenance experts to debate current issues, share lessons learned, and discuss success stories and/or near-misses in a confidential, technical environment. This group is purposed to help individuals and entities involved in substation maintenance work to continuously improve efforts and to build relationships among entities. ReliabilityFirst staff will facilitate the meetings and will develop an agenda for an initial conference call. RF staff will maintain a roster to notify everyone of the dates and times of meetings and will provide an email group address to make sending group emails easier. This group is voluntary and available at no cost.

If interested, please contact Thomas Teafatiller to receive information about the initial CoP Webex.

Short Circuit Data Modeling Workshop Tentatively June 5-6, 2019 • Cleveland, OH

This workshop will focus on the various aspects of the modeling and calculation of short circuit values for the front-line data modelers and coordination with your neighbors. Those with a focus on front-line activities in short circuit data and modeling areas are the intended audience for this workshop: short circuit data and modeling personnel, transmission planning, protection system modeling, and breaker duty calculations. Representatives from CAPE and ASPEN are anticipated to be on the agenda. RF via its Protection Subcommittee will conduct a short circuit survey in the fall of 2019; this workshop is intended to encourage the entity data modelers to participate in that effort. There is no fee to attend this workshop and it is open to neighboring Regional Entity staff, members, and others. Participation will be limited. Registration information will be available in the near future.

Should you have any questions, they may be directed to John Idzior.

Fifth Annual Protection System Workshop August 13-14, 2019 • Cleveland, OH

The RF Reliability Assessment and Performance Analysis (RAPA) will be holding its fifth annual protection system workshop. The event is intended for technical personnel: substation supervisors, substation electricians, substation field engineers, relay technicians, relay engineers, and company trainers. This is a highly interactive workshop with the attendees providing ideas, suggestions, and stories for the benefit of everyone. There will also be vendor presentations and displays available both days. There is no fee to attend this workshop and it is open to neighboring Regional Entity staff, members, and others. More information will be available in the Spring.

Should you have any questions, please contact Thomas Teafatiller .

Human Performance Workshop August 14-15, 2019 • Cleveland, OH

This workshop will focus on practical application of human performance techniques and concepts for front-line activities that attendees can retain and use in transmission reliability related work areas such as operations, asset management, design, protection, maintenance, and others. Monika Bay and Jake Mazulewicz, Ph.D. are two of the featured speakers of the event. Those with a focus on front-line activities in reliability related work areas are the intended audience for this workshop: substation and transmission maintenance, protection and controls, operations control rooms, asset design groups, and asset management groups. There is no fee to attend this workshop and it is open to neighboring Regional Entity staff, members, and others. More information will be available in the Spring.

Should you have any questions, they may be directed to Jeff Mitchell or Kellie Anton.

Calendar of Events

The complete calendar of RF Upcoming Events is located on our website here.

Date	RF Upcoming Events	Location
February 18	Reliability and Compliance Open Forum Call	Conference Call
March 13	Board of Directors and Committee Meetings	Cleveland, OH
March 14	Board of Directors and Committee Meetings	Cleveland, OH
March 18	Reliability and Compliance Open Forum Call	Conference Call
April 15	Reliability and Compliance Open Forum Call	Conference Call
May 1-3	RF Spring Workshop	Baltimore, MD

Industry Events:

Date	Industry Upcoming Events
February 12-14	NERC Inverter-Based Resource Performance and Analysis Technical (Folsom, CA)
February 21	FERC Open Meeting
March 21	FERC Open Meeting
March 26-28	NERC Human Performance Conference & Workshop (Atlanta, GA)
April 3-4	NATF/EPRI/NERC Resiliency Summit (Charlotte, NC)
April 18	FERC Open Meeting
May 16	FERC Open Meeting
May 18-19	NERC/NATF Modeling Workshop (Novi, MI)
June 20	FERC Open Meeting

Michigan solidifies long-term efforts for safe and reliable energy

In 2018, the Michigan Public Service Commission (MPSC) modernized its infrastructure and regulatory perspective by quickly adapting to changes in Michigan's energy and communications industries.

Some of MPSC's key accomplishments in 2018 include:

- Electric grid resiliency: reviewed numerous energy infrastructure proposals to ensure the best value to customers.
- Cybersecurity protections: adopted protections to formalize processes for electric utilities - both investor-owned and electric cooperatives - to assess and report to MPSC annually on their cybersecurity efforts. The rules also provide protocols for reporting cyber breaches or events.
- New power plants, investments to replace coal-fired generation: reviewed numerous energy infrastructure proposals to ensure they provide the best value to customers. Also approved the expansion of energy waste reduction programs that defer or displace costly infrasture and cut emissions in the power sector.

In 2019, MPSC will consider additional integrated resource plans, decide major issues in several rate cases, determine updates to standards for generators connecting to the electric grid, and implement new rules.

ReliabilityFirst Members

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

Forward Together RF ReliabilityFirst

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