Issue 6
2018 November/December

INSIDE THIS ISSUE

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

Follow us on:

Note from the President

Dear Stakeholders,

As 2018 draws to a close, I would like to thank all of you for your dedication to keeping the lights on this past year. It has been a time of significant change, but your steadfast work to ensure the reliability and resilience of the bulk electric system has continued without missing a beat. I'm optimistic that will continue, and this issue provides some great advice in regards to patching and the new Supply Chain Management Standard, and also recaps some of the important work happening on our subcommittees and the RTO's in our Region.

We recently completed our final Board Meeting of the year, and I continue to be grateful for the strength and commitment of our Board of Directors and their ongoing intelligent leadership. I'd like to thank Jim Haney and Mike Bryson for their service and guidance.

I am pleased to welcome Jennifer Curran from MISO as the new RTO representative and Robert Mattiuz Jr. to the Transmission Sector from First Energy. I am also very happy to have Lou Oberski, Simon Whitelock and Larry Irving returning for another term.

I hope each of you see the value in the important work you do, and that you are able to take some time to relax and spend time with your loved ones this holiday season.

Forward Together,

Tim

Forward Together ReliabilityFirst

From the Board

Annual Meeting of Members, Fourth Quarter Board of Directors and Committee Meetings

Kenneth DeFontes, Jr.

We were honored to have Kenneth DeFontes, Jr. and Robin Manning as our guest speakers during the 2018 Annual Meeting of Members and Fourth Quarter Board of Directors meetings in Washington, DC.

Ken DeFontes, Vice Chair of the NERC Board of Trustees and former RF Board member, provided the keynote address at the Board of Directors meeting. He discussed the evolution of the electric industry and the ERO Enterprise, and the creation of RF. Mr. DeFontes also discussed RF's collaborative relationship with NERC, and the important progress made in various areas such as event analysis, human performance, and misoperations.

Robin Manning

Robin Manning, NERC Board of Trustees member, also provided remarks at the Board of Directors meeting. He discussed NERC's current areas of focus, which include:

1. successfully transitioning from a single Reliability Coordinator to multiple Reliability Coordinators in the WECC region;
2. physical and cyber security and the completion of the E-ISAC;
3. the integration of inverter based technology; and
4. the changing resource mix.

RF Thanks and Recognizes Departing Board Member Michael Bryson

Tim Gallagher, Michael Bryson, and Lisa Barton

During RF's Board of Directors meeting in Washington, DC, RF recognized the service of Michael Bryson, whose term expired this year. Tim Gallagher, President and CEO, and Lisa Barton, Board Chair thanked Mr. Bryson for his service and leadership during his term. Mr. Bryson represented the RTO sector and served on RF's Board since 2015 and, during this time, also provided valued guidance on RF's Nominating & Governance Committee and Compliance Committee. Mr. Bryson is Vice President of Operations at PJM Interconnection, LLC.

RF Thanks and Recognizes Jason Blake

During the Board of Director's meeting, the Board adopted a resolution in recognition and appreciation of outstanding leadership by Jason Blake, who recently departed RF to become President & CEO of SERC Reliability Corporation .

Jason Blake served as RF's Vice President, General Counsel, and Corporate Secretary, and the Board recognized his valuable contributions to RF during his years of service.

Jason Blake

2018 Long Term Reliability Resource Assessment

By: Tim Fryfogle, Senior Engineer Resources

RF completes an annual resource assessment based on the data PJM and MISO provide to RF. This article will share some highlights from that assessment. Based on the data received for the next 10-year period, PJM is expected to meet its reserve margin target through 2028. The MISO reserve margin, which includes Existing-Certain and Tier 1[1] resources satisfies its reserve margin target through 2022. The MISO reserve margin projected for 2023 is 313 MW below the reserve margin target. Continuing in 2024, the projected reserve margin is 1,625 MW below the target, reaches its peak at 3,708 MW below the target in 2027 and rebounds slightly to 3,291 MW below the target in 2028. Since these projected reserve deficits are five years into the future, RF staff believes that this range of reserves should be marginally acceptable. Five years lead time should be sufficient to manage resource adequacy. However, resource adequacy issues for these years will need to be closely monitored.

PJM

Capacity and Reserves

PJM resources are projected to be 197,286 MW in 2019 and then increase to 218,672 MW by the end of 2028. The reserve margin calculations include planned generation retirements, planned generation additions and changes, and a percentage of the Tier 2 projects from the generation interconnection queue. PJM is expected to meet its reserve margin target through 2028.

Demand

PJM RTO is projected to average a 0.37 percent load growth per year over the next ten years. The PJM RTO summer peak in 2019 is projected to be 152,479 MW and increase to 157,635 in 2028 for total internal demand (TID), and 143,366 MW in 2019 and increase to 149,688 in 2028 MW for Net Internal Demand (NID), a 10-year increase of 5,156 MW and 6,322 MW, respectively.

Annualized 10-year growth rates for individual PJM transmission zones range from -0.2 percent in Atlantic Electric and Baltimore Gas and Electric companies to 0.8 percent in Dominion.

MISO

Capacity and Reserves

MISO resources are projected to be 149,226 MW in 2019 and then increase to 190,293 MW by the end of 2028. This reserve margin calculation includes planned generation retirements, planned generation additions and changes, Tier 2 and Tier 3 projects from the generation interconnection queue. MISO anticipated reserve margin, which includes existing generation and Tier 1 resources, satisfies the reserve target through 2022.

The MISO anticipated reserve margin is projected for 2023 is 313 MW below the reserve margin target. Continuing in 2024, the projected reserve margins are below the target, reach a peak of 3,708 MW in 2027, and rebound slightly to 3,291 MW below the target in 2028.

Demand

The 2017 forecasted MISO annual growth rate for 2019-2028 is approximately 0.25 percent. The MISO RTO summer peak is projected to be 125,284 MW in 2019 and 128,116 MW in 2028 for total internal demand (TID), and 119,294 MW in 2019 and 122,126 MW in 2028 for Net Internal Demand (NID), a 10-year increase of 2,832 MW in both categories.

RF

Resources

The amount of generation capability for 2019 in RF is 210,591 MW. Overall, there is an increase in capacity through 2028 to 237,184 MW.

Demand

The estimated coincident NID peak of the entire RF regional footprint for the summer of 2019 is projected to be 161,830 MW. For the summer of 2028, NID is projected to be 166,497 MW. The compound annualized growth rate (CAGR) of the NID forecast is 0.32 percent from 2019 to 2028. The TID for the summer of 2019 is projected to be 173,021 MW. For the summer of 2028, TID is projected to be 176,645 MW. The compound annualized growth rate (CAGR) of the TID forecast is 0.23 percent from 2019 to 2028.

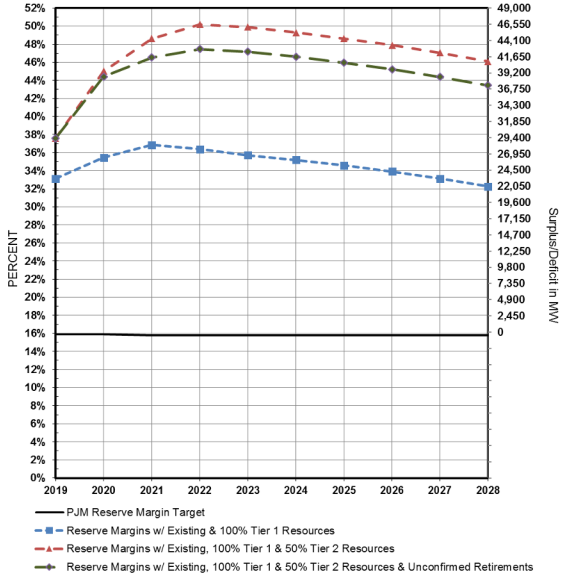
[1]Capacity categories listed in the LTRA are identified as either “Existing-Certain”, “Tier 1”, “Tier 2”, or “Tier 3” resources. “Existing-Certain” and Tier 1 resources receive 100% capacity credit, while “Tier 2” and “Tier 3” resources receive varying capacity credit, due to the uncertainty of future project completion.

Continued on page 4

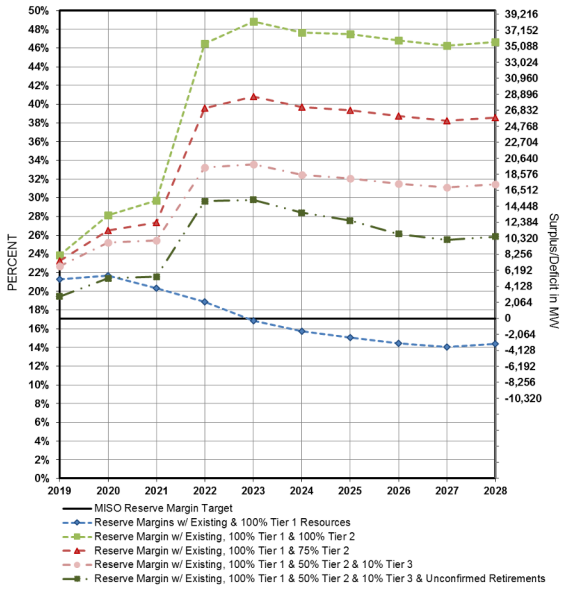
2018 Long Term Reliability Resource Assessment

Continued from page 3

FIGURE 1
PJM RTO
Summer Reserve Margin Projections
2019 - 2028



MISO RTO
Summer Reserve Margin Projections
2019 - 2028



Figures 1 and 2

The figures to the left display graphs of the reserve margins for the PJM and MISO RTOs. The graphs include different scenarios, including the unconfirmed retirements and Tier 2 capacity and, for MISO, Tier 3. The scenarios use percentages of the Tiers to gauge how much of the Generation Queue is needed to stay above the reserve margin requirement.

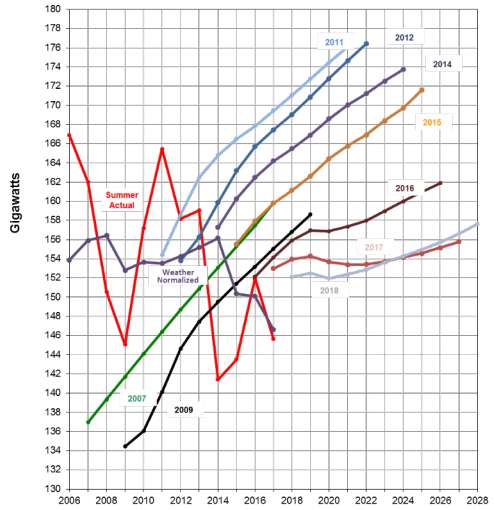
The percentages included in these scenarios are on top of the MISO confident factors. Generator retirements are evaluated by the RTOs for reliability impacts as each retirement is proposed. If the RTO determines that reliability impacts exist, the unit owner is asked to defer retirement until the reliability impacts are addressed. In this assessment, all confirmed generator retirements are assumed to occur after any reliability concerns are addressed.

Unconfirmed Retirements are resources that are considered likely to retire by resource owners, but the formal notification has not been submitted to the respective RTO or to regulatory bodies. Also included in Unconfirmed Retirements are units for which such notice has been made, but a reliability impact assessment and potential designation as a reliability must run unit by PJM or MISO, is pending.

Figures 3 and 4

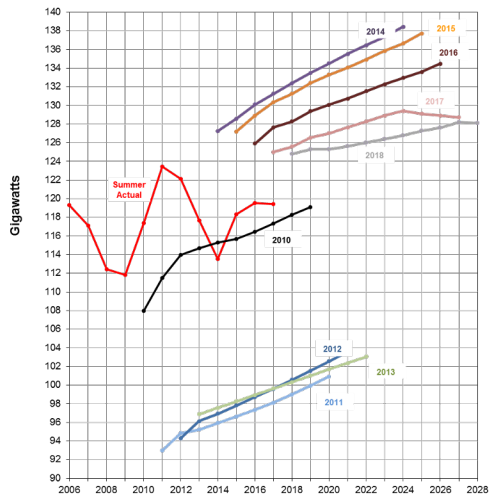
The figures to the right show comparisons of actual demand data to ten year forecasts of demand.

Figure 3
PJM RTO Peak Demand Data
Actual 2006 - 2017
Select 10 Year TID Forecasts Through 2028



2011 Includes the expansion of the PJM RTO footprint with First Energy (ATSI) and Duke Energy Ohio and Kentucky
2013 Includes the expansion of the PJM RTO footprint with East Kentucky Power Cooperative

Figure 4
MISO RTO Peak Demand Data
Actual 2006 - 2017
Select 10 Year TID Forecasts Through 2028



2011 Includes the reduction of the MISO RTO footprint with First Energy (ATSI), Cleveland Public Power and Duke Energy Ohio and Kentucky moving to PJM RTO
2014 Includes the expansion of MISO RTO footprint with MISO South

Winter 2018/2019 Reliability Resource Risk Assessment

By: Tim Fryfogle, Senior Engineer Resources

RF performs a seasonal winter resource adequacy assessment based on the results PJM and MISO provide. This article shares some highlights from the MISO, PJM, and RF assessments. For the upcoming winter of 2018/2019, both MISO and PJM are expected to have an adequate amount of resources to satisfy their respective planning reserve requirements. Below are the statistics that support our analysis on generation outage risk, which concludes that there should not be an issue supplying demand within the RF Region this winter.

PJM Capacity and Reserves

- PJM net capacity resources that include existing certain generation and net scheduled interchange for the 2018 planning year are projected to be 183,399 MW. The projected reserves for the PJM RTO during the 2018/2019 winter peak are 52,373 MW, which equates to a 40.0 percent planning reserve margin for the net internal demand (NID) of 131,026 MW. This is greater than the PJM planning reserve margin requirement for the 2018 planning year of 16.1 percent. The planning reserve margin for this winter is higher than the 2017 forecast level of 39.1 percent. This is due to a slightly negative load growth compared to last year.

MISO Capacity and Reserves

- MISO net capacity resources for the 2018 planning year are 145,959 MW. The currently projected reserves for MISO for the 2018/2019 winter peak are 35,690 MW after accounting for potential transfer limits due to the Sub Regional Export Constraint (SREC), which equates to a 35.7 percent planning reserve margin for the NID of 99,588 MW. This is greater than the MISO planning reserve margin requirement of 17.1 percent for the 2018 planning year. The planning reserve margin for this winter is lower than the 2017 forecast level of 43.0 percent. This is mostly due to a better accounting of the SREC.

RF Footprint Resources

- The net capacity resources in the RF footprint for the 2018 planning year are projected to be 201,481 MW. The projected reserves for the RF footprint during the 2018/2019 winter peak is 90,204 MW. The Total Internal Demand (TID) of 114,832 MW with demand side management of 3,555 MW equates to a NID of 111,277 MW. Since PJM and MISO are projected to have adequate resources to satisfy their respective reserve margin requirements, the RF region is projected to have sufficient resources for the 2018/2019 winter period.

Random Generator Outage Risk Analysis

The following analysis evaluates the risk associated with random generator outages that may reduce the available capacity resources below the load obligations of PJM or MISO.

The stacked bar charts in Exhibits 1 and 2 below are based on forecasted Winter 2018/2019 demand and capacity resource data for the PJM and MISO RTOs. The daily operating reserve requirement for PJM and MISO at the time of the peak demand is also included as a load obligation. The range of expected generator outages is included for scheduled and random outages. The random outages are based on actual NERC Generator Availability Data System (GADS) outage data from December, January, and February of 2013 through 2017.

The committed resources in PJM and MISO are represented by the Resources bar in shades of blue and only include the net interchange that is a capacity commitment to each market. Additional interchange transactions that may be available at the time of the peak are not included as they are not firm commitments to satisfying each RTO's reserve margin requirement.

The firm demand and the demand that can be contractually reduced as a Demand Response are shown in shades of green. The firm demand constitutes the Net Internal Demand, with Total Internal Demand including the Demand Response. The daily Operating Reserve requirement (shown in yellow) is between the NID and DR bars. There are two sets of stacked Demand bars on the chart, one each representing the 50/50 demand forecast and the 90/10 demand forecast. For instance, the 50/50 demand forecast projects a 50 percent likelihood that demand exceeds 131,026 MW. The 90/10 demand forecast is a more conservative model, with demand of 137,184 MW. Since DR is utilized first to reduce the load obligation when there is insufficient capacity, this part is at the top of the Demand bar. In the event that utilization of all DR is not sufficient to balance capacity with load obligations, system operators may first reduce operating reserves prior to interrupting firm load customers.

Between the Resources bar and the Demand bars is the Outage bar. While scheduled outages during the winter season are generally minimal, there are scheduled outages planned during the winter that is reflected in the amount of

Continued on page 6

Winter 2018/2019 Reliability Resource Risk Assessment

Continued from page 5

Forecasted Short-Term Maintenance Outages (colored gray) in the Outage bar. The remainder of the Outage bar represents the entire range of random outages (pink shows 100 percent of the random outages; rose shows less than 100 percent down to 10 percent of the random outages; and red shows less than 10 percent down to 0.2 percent of the random outages on the chart) which occurred during the five-year reference period.

In the following discussion of the random outages, the analysis of random outages exceeding certain reserve margin targets is presented as a probability. These probabilities are not based on a true statistical analysis of the available daily random outage data. Rather than statistical probabilities, these numbers represent the percentage of the daily outages during the five prior winter periods that would have exceeded the reserve margin that is listed. They are discussed as probabilities as a matter of convenience in describing the analysis results.

To the left side of the range of random outages are probability percentages related to the number of random outages that equal or exceed the number of outages shown above that line on the Outage bar. Moving from top to bottom of the Outage bar represents an increasing amount of random outages, with a decreasing probability for the amount of random outages. In Exhibit 1, the random outages of PJM are represented by the bar above the 100% point is 527 MW. This means that the probability of there being at least 527 MW of random generation outages is 100 percent. Similarly, at the 10 percent point, the outages represented by the bar above the 10 percent point is 21,969 MW (527 MW + 21,442 MW). There is a 10 percent probability that there will be at least 21,969 MW of outages. As shown by the probabilities and corresponding amounts of random outages, the distribution of random outages is not linear throughout the range of outages observed.

Exhibit 2 contains the information to perform the same analysis for MISO. The top of the 50/50 demand obligation bar for MISO represents TID with operating reserves.

Exhibit 1 - 2018/2019 Winter PJM Outage Risk Chart

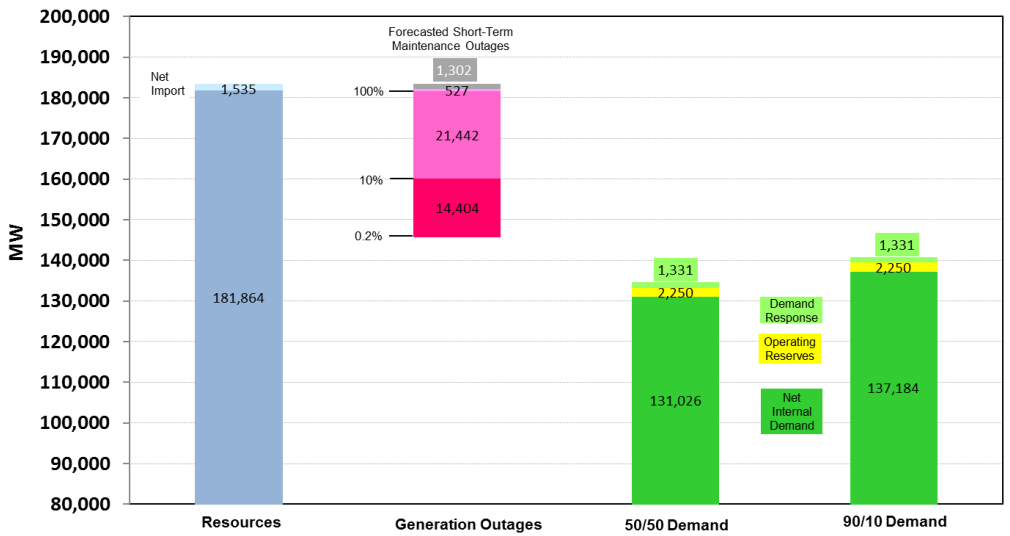
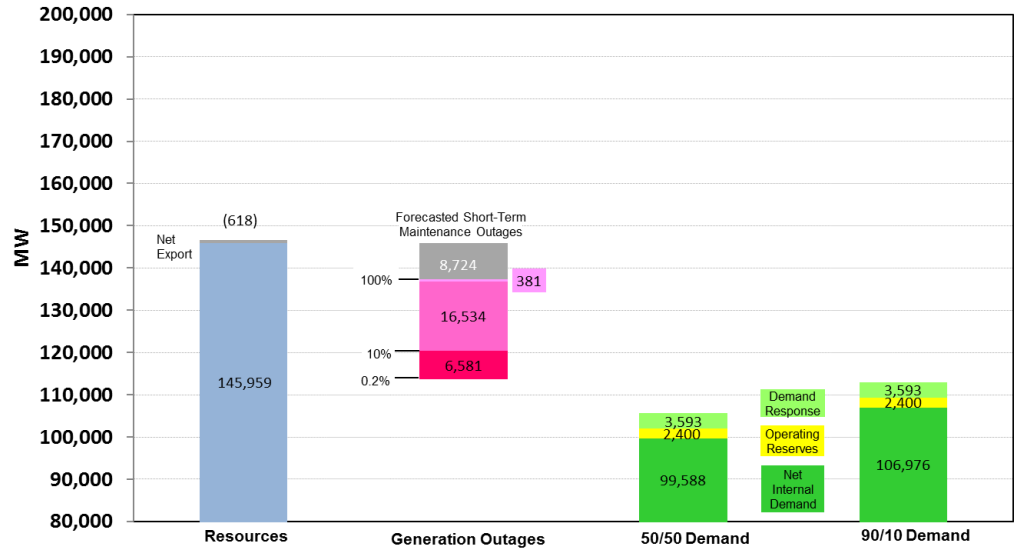
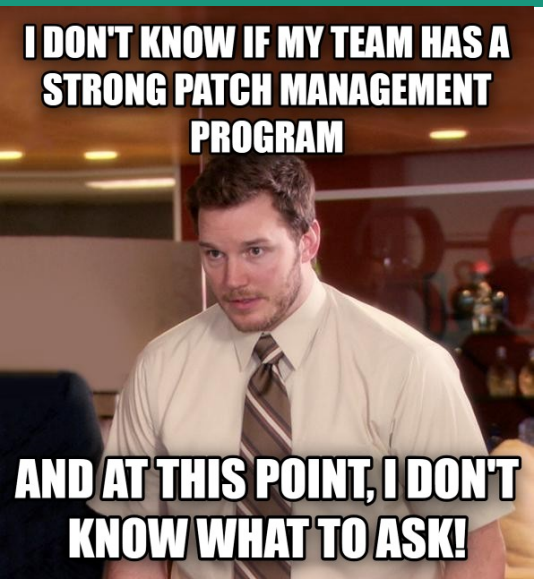


Exhibit 2 - 2018/2019 Winter MISO Outage Risk Chart



Patching like a Boss using Metrics

By: David Sopata, Senior Reliability Consultant



As discussed in the Enforcement Update and Observations article in the RF September/October 2018 Newsletter (link), Security Patch Management CIP-007-6 R2 accounted for a little under a third of the CIP violations reported or identified in 2018. Lew Folkerth has already written two Lighthouse articles on Security Patch Management.

The first article identifies Security Patch Management as one way to address vulnerabilities within a larger Software Vulnerability Management Program. (link) Lew's second article addresses the complexities and lifecycle of a Patch Mitigation Plan (link), which is an alternative method of mitigating a vulnerability when the related security patch cannot be implemented within the 35 day window per CIP-007-6 R2.

Generally, patching is the more straightforward way to mitigate a vulnerability within the software. This is especially true given that according to Dragos, Inc.'s Industrial Control Vulnerabilities 2017 In Review report, (link) which states that "72 percent of 2017 ICS-related vulnerability advisories provide no alternative mitigation guidance outside of patching, suggesting no method to reduce risk until after an update cycle."

There are a few additional points made on the Dragos report about patches. However, this quote on its own means that if the team responsible for patching and vulnerability management for BES Cyber Systems cannot patch, then more time will be needed analyzing vulnerabilities, mitigating the vulnerabilities and developing a plan within the 35 day window due to vendors not providing alternative solutions other than patching. The patch mitigation plan still needs to be created within the 35 day window. Implementation, however, is defined within the patch mitigation plan and can potentially be longer than the 70 days for assessing and implementing patches. As a result, this can leave more potential risk in place for longer periods of time.

Additionally, if this is the norm, the stack of vulnerabilities and unpatched systems will multiply every 35 days as many major software vendors provide new patches. By doing this, at least every month industry could be creating a larger attack surface and a backlog of patches. This scenario can happen when the default answer from BES Cyber Systems Asset owners is, "We can't patch now."

Creating internal controls are hard. Creating good reports and artifacts from internal controls is even harder. Many times, the difficulty is due to not tracking the right information. However, if you don't know what to track, how do you know you have the right information?

How do you know a program is working and it is truly reducing the security risk to the organization? In some instances, you may not know that the Security Patch Management Program is working until some mock audit has been performed or worse yet when you have a CIP Audit! This likely induces some fears and anxiety that some tasks are missing, not being done as scheduled or required, or not knowing what data to capture and look for between audits, spot checks, and other data submittals. Sometimes there is no check or assessment until there is some form of identified deficiency.

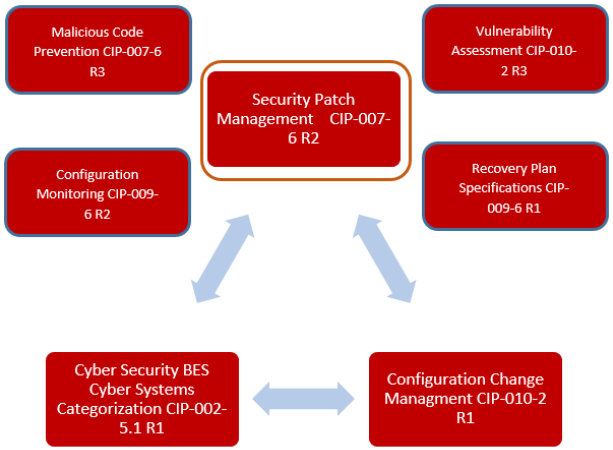
Having internal controls and performing regular checks, tracking changes, and keeping information readily available upon request, can help make compliance obligations easier. This information can be used to communicate to management the state of a particular system or program, i.e. your patch management program. This type of information is what I am going to refer to as metrics. It may be called something different within your company or even departments within your company.

It could also be known as statistics or even key performance indicators (KPIs). However, the first step is to know what items to track. Tracking the right data are key and valuable indicators that there could be an issue to look into or improve upon. In this article, I thought I would tackle metrics around a security patch management program.

Continued on page 8

Patching like a Boss using Metrics

Continued from page 7



CIP-007-6 R2 cannot be a successful program on its own!

CIP-007-6 R2 highly impacts and is impacted by other requirements within the CIP Standards as shown in figure 2. In the larger connected triangle, we have CIP-007-6 R2 which is the focus of the patch management program. In addition to the patch management program, we also have the identification of BES Cyber Systems in CIP-002.5.1a and the Creation of Baselines in CIP-010-2 R1. These three CIP Requirements are highly dependent on each other as it relates to Security Patch Management. When there is a fall down in one, there is likely a fall down in the others. If a group of BES Cyber System Assets have been misidentified, baselines will need to be developed and applied, patches will need to be applied, etc. The secondary CIP Requirements also have an impact on patch management, but it is a lesser of a connection. Vulnerability Assessments in CIP-010-2 R3 can be used as an additional validation tool to ensure that patches have been applied or if there may be potential missing patch sources.

It can also be used before commissioning a new device into production to ensure that all patches will be applied. Monitoring for changes in baselines such as CIP-010-2 R2 can be used to monitor for unauthorized changes, but can also look for potential changes that could indicate a compromise. Ensuring that backups, as required for CIP-009-6 R1, are available, up-to-date, and protected from potential changes is critical when applying patches or other changes that need to be backed out.

So where do we start with the metrics?

Now that we understand that these CIP Standards and Requirements are highly linked and are dependent on each other, let's discuss some metrics that would be useful to have on demand to get a feel for how healthy your Security Patch Management Program is. Please note that this is a start, does not guarantee compliance, and mileage may vary. Additionally, these metrics are posed as questions that should be answered through data gathered on a regular basis. This information and data should be able to produce totals and percentages in a meaningful way that can be used to either do further analysis or adjust current processes and internal controls.

It should be noted that these metrics and analysis tools and processes may be hard to implement within every organization due to the availability of information from multiple and disparate systems. However, your organization may already have these tools and reports available to gather various types of needed information and evidence. You should ensure that this data covers 100% of your BES Cyber Systems and that there are no gaps. Additionally, this information will be extremely useful, especially if it can be obtained quickly to satisfy an audit request, a spot check, extent of condition analysis for a self-report, and developing compliance mitigation plans.

First, how about metrics that help define the environment?

1. How many unique and diverse Cyber Systems and assets are there? What are they? What are their categories? What types of software and services are on these systems? This would be the same type of information that would be needed to fill out the Evidence Request Tool. (Just a reminder , there is a new version of the Evidence Request Tool on the NERC site. (link)
2. How many different patch sources are reviewed in relation to the current BES Cyber Systems and Assets?
3. How many of those BES Cyber Systems and BES Cyber Assets are solely owned and managed by the department responsible for patching? How many are co-owned and/or co-managed? What other Business Unit(s)/department(s) are involved?

Continued on page 9

Patching like a Boss using Metrics

Continued from page 8

Who per BES Cyber System and Asset:

- Identifies and categorizes the BES Cyber Systems and BES Cyber Assets?
- Identifies the different patch sources?
- Assesses the applicability of security patches?
- Applies the patches?
- Develops the patch mitigation plans when a patch is determined that it can't be applied?
- Applies the patch mitigation plans?

Next, what about metrics that can show the performance of the security patch management program?

1. How many times has a 35 day window for patch assessments been missed in the past six months for all BES Cyber Systems?
2. How many incidents have been found where a patch source has been missed either through random discovery, by regular vulnerability scans, and/or through regularly scheduled audits of assessed and applied patches?
3. How many times has a 35 day window been missed between performing the patch assessment and applying the patch for all BES Cyber Systems/Assets?
4. How many times has a 35 day window been missed between performing the patch assessment and creating/modifying the patch mitigation plan for all BES Cyber Systems/Assets?
5. When a mitigation plan has been created, what is the timeline between applying the mitigation control for all BES Cyber Systems/Assets under the mitigation plan?
6. How many mitigation plans are there? What percentage of the BES Cyber Systems/Assets are currently under a mitigation plan? What is the main reason why they are under the mitigation plan?
7. What is the current age of mitigation plans? Are any mitigation plans currently hitting their expiration date and need to be reviewed and/or extended?

Finally, how is this information tracked, kept up-to-date, and available?

- How quickly can this type of information be presented to an audit team for level 1 and level 2 information CIP audit request, spot check, internal compliance, and/or management?

These metrics and the information that is collected as a result, are one of the core elements to building quality internal controls, as noted by Denise Hunter in her article from earlier this year on internal controls (link). The information gathered from these metrics can help management make informed decisions and communicate the health of a program to other management or outside the organization.

Without them, situational awareness of a program will be low, performing the process in a blind state relying on other outside negative factors to inform on the state of the program such as an audit. Being in a state to self-identify and self-report these issues speak to a higher maturity level of a given program.

What are some of the metrics that are tracked within your organization around the CIP standards? Are there others that you track around Security Patch Management? I welcome any feedback and can be reached (here). If you have questions about other aspects of CIP Standard and potential metrics feel free to go through our Assist Visit program by clicking on the link and filling out the request form. (link)

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Supply Chain Risk Management

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: CIP-013-1 will become effective on July 1, 2020. How do I prepare for this date and what will audits of this Standard look like?

A : Preparing for CIP-013-1

CIP-013-1 is the first CIP Standard that requires you to manage risk. Entities and audit teams will both need to make adjustments to prepare for this standard's effective date. I'll give you my present views on this subject as a starting point, and I will provide updates in 2019 and 2020 as the effective date nears and audit approaches are developed.

CIP-013-1 is a *plan-based* Standard.

You are required to develop (R1), implement (R2), and maintain (R3) a plan to manage supply chain cyber security risk. You should already be familiar with the needs of plan-based Standards, as many of the existing CIP Standards are also plan-based.

CIP-013-1 is an *objective-based* Standard.

CIP-013-1, and its affiliated Standards (CIP-005-6 R2 Parts 2.4 and 2.5; and CIP-010-3 R1 Part 1.6), are intended to address four security objectives (see FERC Order 850 at P2, excerpt below):

"[R]equire each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. [T]he Reliability Standards focus on the following four security objectives:

Portage Upper Entry, MI - Photo by Lew Folkerth

1. software integrity and authenticity;
2. vendor remote access protections;
3. information system planning; and
4. vendor risk management and procurement controls."

Your actions in developing and implementing your plan should be directed toward achieving these four objectives. You should be prepared to demonstrate to an audit team that you meet each of these objectives. These objectives are not explicitly referenced in the Standard language. However, as outlined in the FERC Order, the achievement of these objectives is the reason the Standard was written.

This does not apply just to CIP-013-1. You should write every CIP-related process to achieve the security objective of the Standard, especially when the security objective is stated as clearly as it is for CIP-013-1. Keep in mind that your audit teams are required to consider your program's objectives (see GAGAS 2018 Section 8.36e) when they perform your audit. You will be on much firmer ground during your audit if you can show that your processes achieve the intended objective.

CIP-013-1 is a *risk-based* Standard.

You are required to "develop one or more documented supply chain cyber

Continued on page 11

Continued from page 10

security risk management plan(s)" and to "identify and assess cyber security risk(s)." Your plan should clearly show how you identify and address the risks in your supply chain. As CIP-013-1 is the first explicitly risk-based CIP Standard, this is new ground we'll be exploring.

You are not expected to address all areas of supply chain cyber security. You have the freedom, and the responsibility, to address those areas that pose the greatest risk to your organization and to your high and medium impact BES Cyber Systems.

You will need to be able to show an audit team that you have identified possible supply chain risks to your high and medium impact BES Cyber Systems, assessed those risks, and put processes and controls in place to address those risks that pose the highest risk to the BES. There are several sources to get you started. Approved Implementation Guidance is available on the NERC web site. Also, several National Institute of Standards and Technology (NIST) publications may be useful (see sidebar).

References

- NIST SP800-161, Supply Chain Risk Management Practices
- NIST SP800-30, Guide for Conducting Risk Assessments
- NIST SP800-39, Managing Information Security Risk
- ERO Enterprise-Endorsed Implementation Guidance

One example is NIST SP800-30. This guide discusses a risk management process. It proposes using four components for risk management: *frame* risk (establish a risk context), *assess* risk within the context of the organizational risk frame, *respond* to risk based on the assessment, and *monitor* risk over time. I expect developing a plan by implementing this document and approach would work well for CIP-013-1.

Preparing for an Audit of CIP-013-1

Fundamentally, an audit of CIP-013-1 will probably be similar to audits of other plan-based Standards, but with additional steps.

You will need to have evidence of your documented plan (or multiple plans if you've chosen that option) throughout the audit period.

Be prepared to show how your plan meets the four security objectives. You may accomplish this with a narrative internal to the plan, or by an external compliance narrative in the RSAW.

Be prepared to show how your plan manages risk. Again, a narrative will probably be needed. If you elect to use the NIST SP800-30 risk assessment process, providing detail of how you have implemented the four steps of the risk assessment might be part of this.

You will need evidence of your implementation of the plan. Do not rely on vendor contracts or contract language as evidence. Audit teams will be interested in the tangible results of what you have accomplished and how you've accomplished it, not what you've put in your contract language.

Finally, you will need evidence of your annual (15 calendar months) review of your supply chain cyber security risk management plan. This review should include the identification of any new or emerging risks since the last update of the plan. You should refresh the risk assessments in light of any new risks or changing circumstances in previously-identified risks. You should also review the steps taken to mitigate all identified risks.

Make sure your CIP Senior Manager (or delegate) approves each revision of the supply chain cyber security risk management plan.

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.

In the Industry

By: Mike Gabriel, Deputy Chief Operating Officer, NAGF

"What is the NAGF?"

The North American Generator Forum (NAGF) was founded in 2009 as a vehicle for utility and non-utility owned generator owners and/or operators to address issues related to registration, compliance, standards development and other NERC-related topics.

We provide entities who are generator owners and operators in North America a means to collaborate, communicate, and influence regulatory policy development with FERC, NERC, the Regional Entities, the Canadian Provinces and other organizations with missions similar to ours, with the ultimate goal of improving the reliability of the bulk power system.

The NAGF has the following active working groups that meet regularly to address generator concerns:

- **Peer Review:**

  The Peer Review Working Group is focused on developing and implementing the NAGF Peer Review program. Review focus areas include compliance, protection systems and maintenance activities, cyber security and physical security, operations, modeling and model verification, and training.

- **Security Practices/CIP:**

  The Security Practices/CIP Working Group is charged with reviewing physical and cyber security issues that impact the generation sector.

- **Standards Review Team:**

  The Standards Review Team (SRT) works directly with NERC to address Generator Owners and Generator Operators' concerns regarding enforceable standards and standards under development.

- **Variable Resources:**

  This working group's focus is on NERC Reliability Standards implementation and best practice sharing for utility scale Variable Resources (usually for wind & solar) connected at transmission voltages of 100 kV or greater.

The NAGF recently hosted its Annual Meeting where members discussed topics ranging from operation and planning to physical and cyber security. Additionally, the NAGF hosts periodic meetings and conference calls, both internally and with FERC's Office of Electric Reliability, NERC leadership, and FERC Commissioners. This month, there remains a Variable Resource Working Group Call on December 19, 2018 from 11-12 EST.

More information about the NAGF can be found here.

Regulatory Affairs

FERC Issues 2018 Report on Enforcement

In November, FERC released its annual Report on Enforcement. The 2018 Report highlighted FERC Enforcement staff's continued focus on serious violations of mandatory Reliability Standards, fraud and market manipulation, anticompetitive conduct, and conduct that threatens the transparency of regulated markets. The report also provides more information on the nature of non-public enforcement activities such as self-reported violations and investigations that were closed without public enforcement action. The report notes that since 2007, FERC Enforcement staff has negotiated settlements allowing for the recovery of approximately $776 million in civil penalties and $511 million in disgorgements. The full report is available here.

Bernard McNamee Nominated to Become FERC Commissioner

On October 3, 2018, President Donald Trump nominated Bernard McNamee to become a FERC Commissioner. McNamee would replace former FERC Commissioner Robert Powelson who stepped down in August. Before his nomination, McNamee headed the Department of Energy's Office of Policy. On November 27, 2018, the Senate Committee on Energy and Natural Resources advances his nomination by a vote of 13-10. McNamee is expected to get a Senate floor vote by the end of the year.

Neil Chatterjee Designated FERC Chairman

On October 24, 2018, President Donald Trump designated Commissioner Neil Chatterjee as Chairman of FERC. Chatterjee replaces former FERC Chairman Kevin McIntyre who resigned as Chairman citing health reasons. McIntyre remains on FERC as a Commissioner. Chatterjee previously served as FERC Chairman from August 2017 until December 2017 when McIntyre was sworn in as Commissioner.

FERC Acts on Cyber Security Risks with New Supply Chain-Related Reliability Standards

On October 18, 2018, FERC issued a final ruling approving CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-5 (Cyber Security – Electronic Security Perimeter(s)), and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments). FERC issued two directives to NERC.

1. NERC is to develop modifications to the standards to address Electronic Access Control and Monitoring Systems ("EACMS") associated with medium and high impact BES Cyber Systems. A significant cyber security risk remains because the new standards exclude EACMS, and EACMS control electronic access into Electronic Security Perimeters and help protect high and medium impact BES cyber systems. Once an EACMS is compromised, an attacker could more easily control the BES cyber system or protected cyber asset. FERC gave NERC 24 months to develop modifications and address this gap.
2. FERC accepted NERC's commitment to evaluate the risks of low impact BES cyber systems, Physical Access Control Systems, and Protected Cyber Assets in the study directed by the NERC Board of Trustees, and directed NERC to file the final report with FERC upon its completion.

FERC Approves 2019 Business Plans and Budgets

FERC found NERC's 2019 budget reasonable and that the associated costs of NERC's jurisdictional functions are equitably allocated among end users in the United States.

FERC found each Regional Entity's submission reasonably supports the level of expenditures identified in their respective budgets and that each was focused on adequately staffing and funding their program areas to perform the delegated, statutory functions.

FERC approves GMD Standard

FERC issued a final rule approving Reliability Standard TPL-007-2 (Transmission System Planned Performance for Geomagnetic Disturbance Events). NERC submitted TPL-007-2 for Commission approval in response to directives in Order No. 830. FERC determined that the Standard better addresses the risks posed by geomagnetic disturbances ("GMDs") to the Bulk-Power System than the currently-effective Standard.

In addition to the approval, FERC also issued two directives to NERC. The first directed NERC to develop and submit modifications to Reliability Standard TPL-007-2 (1) to require the development and implementation of corrective action plans to mitigate assessed supplemental GMD event vulnerabilities; and (2) to authorize extensions of time to implement corrective action plans on a case-by-case basis. The second directed NERC to prepare and submit a report addressing how often and why applicable entities are exceeding Corrective Action Plan deadlines as well as the disposition of extension requests. FERC directed NERC to submit the modified Reliability Standard for approval within 12 months from the effective date of Reliability Standard TPL-007-2.

Standards Update

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

General NERC Standards News

New RSAWs posted

The following five new RSAWs are now posted on NERC's RSAWs page:

- **EOP-004-4** (Event Reporting) applies to many entities and the effective date of the Standard is 4/1/2019. EOP-004-4 will replace EOP-004-3;
- **EOP-006-3** (System Restoration Coordination) applies only to Reliability Coordinators, and the effective date of the Standard is 4/1/2019. **EOP-006-3** replaces EOP-006-2;
- **MOD-026-1** (Verification of Models and Data for Generator Excitation Control System or Plant Volt/Var Control Functions) applies to Generator Owners and Transmission Planners. This RSAW includes an errata change that changes a reference to a verification date to a transmittal date in order to align with the Standard;
- **EOP-005-3** (System Restoration from Blackstart Resources) applies to Generator Operators and Transmission Operators, as well as Transmission Owners and Distribution Providers identified in the Transmission Operator's restoration plan. The effective date of the Standard is April 4, 2019. EOP-005-3 will replace EOP-005-2;
- **EOP-008-2** (Loss of Control Center Functionality) applies to Balancing Authorities, Reliability Coordinators, and Transmission Operators. The effective date of the Standard is April 4, 2019. EOP-0082 replaces EOP-008-1;

Other Resources Posted

- NERC has posted the following resources:
- the streaming webinar and slide presentation for the PRC-027-1 Requirement Training;
- a new lessons learned entitled Networking Packet Broadcast Storms;
- the streaming webinar and slide presentation of the October 16, 2018 Project 2018-02 – Modifications to CIP-008 Cyber Security Incident Reporting webinar;
- a new lessons learned entitled Incorrect Field Modification and RAS Operation Lead to Partial System Collapse;
- the streaming webinar and slide presentation for the September 6, 2018 Winter Preparation for Severe Cold Weather webinar;
- the streaming webinar and slide presentation for the November 16, 2018 Project 2018-2 – Modifications to CIP-008 Cyber Security Incident Reporting webinar;
- a new proposed Implementation Guidance document for CIP-010-2 R1, R2 – Configuration Change Management and Vulnerability Assessments (MROSC);
- the streaming webinar and slide presentation for the November 15, 2018 Project 2016-2 – Modifications to CIP Standards Virtualization and Other Technology Innovations webinar.

Notable NERC Filings

In October, NERC filed the following:

- an informational filing regarding Reliability Standard BAL-001-2 (Real Power Balancing Control Performance);
- a filing for approval of revisions to the implementation plans for Reliability Standards MOD-026-1 (Verification of Models and Data for Generator Excitation Control System or Plant Volt/Var Control Functions) and MOD-027-1 (Verification of Models and Data for Turbine/Governor and Load Control or Active Power/Frequency Control Functions); and,
- a petition for approval of proposed revisions to Appendix 4E to the Rules of Procedure (Compliance and Certification Committee – Hearing (CCCPP-004) and (CCCPP-006) – Mediation Procedures).

In November, NERC filed the following:

- its Annual Report on the Find, Fix, Track and Report and Compliance Exception Programs;
- its 2018 Frequency Response Annual Analysis Report for administration and support of Reliability Standard BAL-003-1.1 (Frequency Response and Frequency Bias Setting); and,
- a petition for approval of proposed revisions to the Standard Processes Manual, Appendix 3A to the Rules of Procedure.

NERC's filings can be found here.

Notable FERC Issuances

In October, FERC issued the following:

- an order approving Reliability Standard VAR-001-5 (Voltage and Reactive Control);
- a final rule approving supply chain risk management Reliability Standards CIP-013-1 (Cyber Security - Supply Chain Risk Management), CIP-005-6 (Cyber Security - Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security - Configuration Change Management and Vulnerability Assessments). Additionally, the Commission directed NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards includes Electronic Access Control and Monitoring Systems;
- a final rule approving proposed Reliability Standard TPL-007-2 (Transmission System Planned Performance for Geomagnetic Disturbance Events) ("GMD"). FERC also accepted the revised GMD research work plan.

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
Project 2018-01 – Canadian-specific Revisions to TPL-007-2	Final Ballots	11/29/18 - 12/10/18
Project 2016-02 Modifications to CIP Standards (Virtualization Updates for CIP-004, CIP-006, CIP-007, CIP-010, and associated definitions)	Comment Period	11/2/18 - 12/18/18

Other Active Comment Periods

Project	Action	Start/End Date
2016-02 Modifications to CIP Standards (CIP-002-6 and CIP-003-8)	Comment Period	8/23/18 - 10/9/18
2015-09 Establish and Communicate System Operating Limits	Comment Period	8/24/18 - 10/17/18

Recent and Upcoming Standards Enforcement Dates

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 (Requirements 5, 5.1-5.2); VAR-001-5 - Voltage and Reactive Control
April 1, 2019	BAL-002-3- Disturbance Control Standard - Contingency Reservice for Recorvery from a Balancing Contingency Eevent; 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	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 Peformance for Geomagnetic Distribance Events (Requirements 3,4,7)

These effective dates can be found here.

Transmission Performance Subcommittee (TPS) Recap

Front row: Karie Barczak (DTE), Leslie Krawcyzk (RF Staff), Second row: Michael Lombardi (NPCC Staff), Hung Huynh (Nova Scotia Power), Kevin Depugh (NYISO), Jeff Gindling (Duke), Mark Stevens (National Grid), Caleb Kim (Exelon), Third row: Brett Riedl (ComEd), Hamid Mamadani (Hydro One), Ray Mason (RF Staff), Neeraj Lal (NPCC Staff), Glenn Catenacci (PSE&G), George Fatu (IESO), Alex Rost (ISONE), Last row, Scott Goodwin (MISO) Ryan Ramcharan (Con Edison), Dave Conroy (Central Maine Power), Carl Benker (Eversource).

On September 18, 2018, select members of the TPS met with their transmission counterparts (the Task Force System Studies) from the NPCC region in Halifax, Nova Scotia. A few of the topics discussed during this meeting were grid resiliency, distributed energy resources, and variable generation resources.

The TPS more recently met in Newark, NJ on October 23-24, 2018. During this meeting, the TPS reviewed results from various transmission studies performed by RF staff. PJM and MISO presented their analysis of the upcoming 2018-19 winter season and PJM presented a method for performing a probabilistic cascading analysis. Finally, the group discussed how to model Geomagnetic Disturbances.

In addition to monthly conference calls, the next face-to-face TPS meeting is scheduled for the week of May 6 , 2019 and will include a joint meeting with the RF Protection Subcommittee.

The TPS serves as the Subject Matter Expert (SME) body to address the transmission reliability related activities of ReliabilityFirst. The TPS provides a forum in which to discuss transmission issues associated with the reliability of the Bulk-Power System. The TPS provides feedback on the RF Staff developed parameters and objectives for the assessment of the future transmission performance of the region and for the production of regional transmission reliability assessments.

Representatives to this subcommittee typically have a Transmission Planning (TP) background and responsibilities. FERC Orders 888, 889, and 2004 code of conduct apply to TPS proceedings; therefore, representatives from the Supplier sector are not permitted to participate in this Subcommittee's proceedings.

RF's Bhesh Krishnappa Publishes Cyber Resilience Framework Paper

Congratulations to RF's Bheshaj Krishnappa for having a paper he co-contributed to titled *Cyber Resilience Framework for Industrial Control Systems Concepts Metrics and Insights* published by IEEE. The paper was presented at the IEEE Intelligence and Security Informatics (ISI) 2018 conference held at Florida International University, Miami FL from November 8 - 10, 2018.

The paper is available in its entirety here.

Protection Subcommittee Recap

The Protection Subcommittee held its Fall meeting at the RF offices on October 10-11, 2018. Topics included an update on the MIDAS Data Reporter Instruction manual under development by the NERC MIDAS Working Group (several RF entities and staff members participate in the MIDASWG) and the results of RF staff studies on generation Misoperations and Misoperation text mining. Representatives of the NPCC regional protection group (SP-7) held a joint session with their RF counterparts to discuss best practices around the Protection System Misoperation topics. SEL University conducted the fourth session in a series on transmission line protection, this year focusing on pilot protection.

The next meeting will be a conference call on January 9, 2019 at 2:00 PM ET. The Spring meeting (still under development) will be a joint session with the RF Transmission Planning Subcommittee, tentatively scheduled for the week of May 7, 2019.

Interested in participating in the Protection Subcommittee? Meetings and calls are open to the public with dates of future meetings listed on the Upcoming Events calendar of the RF website homepage (www.rfirst.org). Member companies of RF can be represented on the Protection Subcommittee by an individual that has the necessary protection background to represent their company in discussions on protection issues. Contact either Thomas Teafatiller or Bill Crossland for further information.

Happy Holidays from RF

Ohio recognized as leader in electric grid modernization

On December 6, 2018, Ohio was recognized by GridWise Alliance with an "Outstanding Progress Award" for its achievement in rapidly expanding grid modernization efforts. GridWise noted Public Utilities Commission of Ohio (PUCO)'s PowerForward Roadmap as the major factor for Ohio's improved ranking in this year's Gridwise Modernization Index (GMI).

PowerForward includes nearly 18 months of public dialog focused on how the PUCO can enhance the electricity experience for Ohioans through innovation.

The GridWise Alliance's GMI uses data inputs and publicly available information to evaluate and rank the status of grid modernization efforts across all 50 states and the District of Columbia.

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