Issue 4
2021 Q4

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:

Note from the President

Dear Stakeholders,

As we wind down another year of great highs and lows, I'm reminded to look at the big picture of the positive impact our industry has on so many people. The past two years have been difficult to say the least, but 2021 marks RF's 15-year anniversary – and it's been a wonderful collective 15! Please stay tuned for a special anniversary issue to commemorate the occasion.

The evolution of our industry over the past 15 years is astounding to me. We've seen NERC and the Regions come together in recent years in a way I could have only hoped for in our early days, and the strong partnerships we've built with Entities and stakeholders are something that gives me great pride. While the risks and threats have changed at a dizzying speed, our industry-wide commitment to collaboration for the greater good only gets better with time.

Some 2021 highlights include welcoming a number of new teammates across the organization and awarding multiple well-deserved promotions. We successfully executed our strategic plan during a pandemic, officially rolled out the Align tool, and maintained our focus on culture, innovation and continuous improvement. We also are fortunate to have new Board members who bring a breadth and depth of experience that is sure to benefit the ERO and industry.

I also want to acknowledge some tough things we dealt with in 2021. I thank and commend everyone for overcoming the difficulties of another year keeping the lights on during the pandemic. We weren't able to host any in-person events or meet our new RF teammates face-to-face, which is unfortunate because I truly value our time together. Also, we've had quite a few retirements at RF which pains me professionally and personally because we're such a tightknit group.

I'm thrilled to welcome Beth Dowdell as our new Sr. Director of Corporate Services and Marcus Noel as our new Chief Security Officer. You can get to know both of them through feature articles in this issue. This is bittersweet though because it means that my longtime colleague and friend Larry Bugh is retiring. After 15 years at RF and nearly 50 in the industry, Larry's steadfast leadership and vast contributions to reliability and security cannot be overstated. Please join me in wishing him a happy retirement!

Since I'm a firm believer in the importance of being grateful for each day, I won't say that I'm glad 2021 is coming to a close, but I'm looking forward to what I hope will be a brighter 2022 filled with health, happiness and peace. And by now you know I preach continuous improvement to you, to the RF organization, and to myself. I am personally looking forward to applying what we all learned during the pandemic to making ourselves and our work even better than it was before we added "Covid" to our vocabularies.

I wish all of you and your families a joyous holiday season, and I hope you will have an opportunity to enjoy time with them and reflect on what truly matters most.

Be safe and be well.

Forward Together,

Tim

From the Board

RF 2021 Annual Meeting of Members and December Board

On December 2, 2021, RF Board Chair Simon Whitelocke welcomed attendees to the Annual Meeting of the Members and introduced the keynote speaker.

Jim Robb, NERC President and CEO, discussed the rapid changes in the industry – from weather to decentralization – and the inherent uncertainty and challenges these changes pose for grid operators. He said the past two years brought some clarity to risks, sharing examples of extreme weather, supply chain and ransomware.

He also highlighted some major questions looking forward from balancing resources, having necessary infrastructure, improving resilience, and ensuring cyber and people resources. He closed by sharing NERC priorities and the continued need for diligence, vigilance and collaboration.

Tim Gallagher, RF President and CEO, announced the 15-year anniversary of RF, expressed his pride in the industry pandemic response, and provided assurance that future decisions will be carefully considered and communicated in advance. Internally, he noted the pandemic impact on staffing, including early retirements.

Mr. Gallagher highlighted topics on the agenda for the Board meeting that followed. This included a presentation with NERC and FERC on cold weather and the focus on risk and response, as well as a presentation discussing RF's focus on diversity, equity and inclusion and the caliber of staff joining RF.

Mr. Gallagher paused to express sincere appreciation to departing RF CSO, Larry Bugh, and welcomed incoming CSO, Marcus Noel, who joins RF from FirstEnergy.

Then the Members elected At-Large Director Simon Whitelocke for another term and Independent Directors Courtney Geduldig and Joanna Burkey, who were appointed by the Board earlier in the year.

During the Board Meeting, outgoing Directors Lynnae Wilson, the former Vice Chair, and Jennifer Curran were thanked for their service to the RF Board.

Jennifer Curran
MISO
RTO Sector

Lynnae Wilson
CenterPoint Energy
Transmission Sector

2022 Q1

ReliabilityFirst

Board of Directors

and Committee

Meetings

will be held

April 27-28, 2022

Continuous Improvement

By Sam Ciccone, Principal Reliability Consultant

Long Lead Time Spare Equipment

The Journey to Reliability, Resilience and Security

Due to challenges like supply chain disruptions, pandemics and security risks, spare equipment has never been more important than the times we live in now.

The loss of long lead time equipment can severely impact an Entity's operations with delays in the supply chain. NERC's annual document (2021 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Plan, Version 2.0, November 2020[1]) discusses potential reasons for long lead times, such as the pandemic, aging infrastructure and others. "The failure to properly commission, operate, maintain, prudently replace, and upgrade BPS assets generally could result in more frequent and wider-spread outages, and these could be initiated or exacerbated by equipment failures."[2] The purpose of the NERC CMEP IP is to tie risk to the NERC standards.

What are ways to plan for and mitigate spare equipment challenges? This article will provide some insight with several references and organizations you can use to learn more.

NAESB

The North American Energy Standards Board (NAESB) wrote a guide called "ERO Reliability Risk Priorities RISC Recommendations to the NERC Board of Trustees November 2016." Risks that may impact industry's ability to replace or repair critical transmission equipment include natural events and physical security vulnerabilities.

Natural events, such as storms, are impactful, probable, and provide a challenge with spare equipment strategies. NAESB discusses the risk of equipment damage during these events and warns, "the industry does not have full knowledge or coordination in accessing the existing spare equipment inventory." To mitigate this risk, they suggest, "the Department of Energy, the industry, trades, and forums should identify appropriate mitigations to prevent spare equipment gaps and improve transportation logistics."

Furthermore, the risk of physical security vulnerabilities also may be aggravated by industry's spare equipment inventory and strategy. The NAESB suggests mitigations, such as initiatives to develop a robust spare equipment strategy.

NATF

Regarding ties to NERC standards, the North American Transmission Forum (NATF) ties spare equipment strategy to the NERC standards and starts with TPL-001. Requirement 2.1.5. states, "when an Entity's spare equipment strategy could result in the unavailability of major Transmission equipment that has a lead time of one year or more (such as a transformer), the impact of this possible unavailability on System performance shall be studied."

NATF recommends "strategies for consideration may include but are not limited to One-for-one (i.e., in-kind) for one spare transmission equipment in stores and their availability/mobility, the ability to temporarily move/transfer redundant transmission equipment (i.e., a substation in which no TPL-001-4 system performance deficiencies are caused by temporary movement or transfer of the transmission equipment) until ordered replacements arrive, and available partnerships with neighboring Transmission Planners to cover each other for certain types of transmission equipment."[3]

[1] https://www.nerc.com/pa/comp/CAOneStopShop/ERO%20CMEP%20Implementation%20Plan%20v2.0%20-%202021.pdf

[2] 2021 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Plan, Version 2.0, November 2020

[3] NERC Standard TPL-001-4

Continued on page 4

Continuous Improvement

Continued from Page 3

After identifying critical equipment (e.g., power transformers) through analysis and studies, it is helpful to develop field expertise in storing, transporting and implementing a spare.

For example:

- Would removing an old and installing a new transformer require emergency bus outages for clearance?
- Would mobiles be needed during the time-delta, and do you have documented plans on where the mobile would be staged during the work?

These are all important considerations beyond being able to locate the spare equipment. You don't want to be developing the plan in the middle of the emergency.

In addition, the voluntary NATF RESTORE Program[4] helps ensure that long lead time spare equipment is available when needed. Although voluntary, this program has formal initiatives, such as transmission owners committing to own, maintain and sell to one another available spare equipment (e.g., transformers and potentially other transmission equipment), for an event that results in major damage to the transmission grid.

This program is supplemental to, and not intended to be a replacement for, any current industry programs, such as EEI's Spare Transformer Equipment Program (STEP) or Grid Assurance.[5]

Collaboration

Over the last several years, there has been much collaboration among industry representatives and other agencies through sharing of best practices around spare equipment programs. It is recommended that your organization get involved in this collaborative approach to increase your knowledge and learn from industry peers. Collaboration includes partnering with "key suppliers and customers to synchronize operations to priorities within constraints, deploy an extended network beyond tier 1 suppliers, and determine levels of collaborative intensity."[6]

Utility Dive recently discussed an initiative by Grid Assurance to ensure spare equipment supplies, especially long lead equipment such as transformers, are "stockpiled" and ready for installation, particularly during urgent and emergency grid reliability situations.

Grid Assurance is an industry initiative to have adequate spare parts inventory on critical long lead equipment. "The U.S. Department of Energy released its Strategic Transformer Reserve Report last year, recommending an industry-led approach. In total the companies involved represent 31 transmission-owning affiliates."[7]

Maturing your Spare Parts Program

Keys for maturing your spare parts program include defining your spare parts requirements and maintaining appropriate spare parts inventory. After an organization identifies its list of historical trends and emerging trends in equipment failure modes, it can adjust or supplement its maintenance program to best prevent the occurrence of these equipment failure modes. It can also use the lists of historical and emerging trends to help define its spare part requirements.

It is important to maintain an appropriate spare part inventory. To do this, an organization can establish a process to purchase the spare parts it needs for the future to maintain the spare part inventory pursuant to the spare part requirements.

Additionally, spare parts can age in inventory, so it is important to track the age and maintenance records for those parts. This will help the organization avoid the unfortunate scenario where a spare part is installed and does not function properly.

[4] https://www.natf.net/docs/natf/documents/natf-restore-program-overview.pdf

[5] https://www.natf.net/docs/natf/documents/natf-restore-program-overview.pdf

[6] Resilient Spare Parts Management: Click Here

[7] https://www.energy.gov/ceser/downloads/strategic-transformer-reserve-report-congress-march-2017

Continued on Page 5

Continuous Improvement

Continued from Page 4

Conclusion

A robust spare part equipment strategy will increase the reliability and resilience of the grid. This takes planning, testing the plan, checking your current state from results of testing the plan, and then acting on any gaps in your strategies (Plan, Do, Check, Act [PDCA], Deming Wheel). Using tips in this article on maturing your spare equipment strategy program will build your program to mitigate the effects of long lead time equipment. Also, collaboration is important to share best practices and lessons learned from your peers and other governmental agencies. Lastly, there is a plethora of articles, guides and white papers developed by NERC, NAESB, NATF and others that will provide more detailed insight on spare equipment strategies. Some are found in this article's footnotes plus the **Learn More** section.

Thank you for reading our CI articles this year. As we ring in the New Year, I hope all of our readers have a happy and safe holiday season!

Learn More

Utilities join grid recovery initiative to stockpile transmission equipment, May, 2018:
https://www.utilitydive.com/news/utilities-join-grid-recovery-initiative-to-stockpile-transmission-equipment/523709/

EPRI- Development of Substation Equipment Spares Strategy Methodology, Analytics, and Guidelines, April 2016:
https://www.epri.com/research/products/3002008655

MLGW Eliminates Long Lead Times, Dec. 23, 2013, Jason Simon:
https://www.tdworld.com/overhead-transmission/article/20963909/mlgw-eliminates-long-lead-times

Grid Assurance Announces Major U.S. Utilities Sign on to Transmission Grid Resilience Solution, May 16, 2018
:https://www.prnewswire.com/news-releases/grid-assurance-announces-major-us-utilities-sign-on-to-transmission-grid-resilience-solution-300649354.html

Utilities subscribe to Grid Assurance transmission spare parts joint venture, Clarion Energy Content Directors, 5.16.2018:
https://www.power-grid.com/td/utilities-subscribe-to-grid-assurance-transmission-spare-joint-venture/#gref

Enhancing the Security of the North American Electric Grid, March 2020:
https://www.cbo.gov/publication/56254

NERC Posts Two Documents to Assist Organizations Preparing for Registration

NERC recently posted the two new resource documents on their Organization Registration and Organization Certification webpage for your reference. If you have any questions, please contact your RE, send an email to compliance@rfirst.org or contact Bob Folt, Principal Analyst, Registration, at 216-503-0625.

NEW! ERO Enterprise Informational Package - New Registered Entities 101

This informative package is a collaborative effort between NERC, the Regional Entities (REs) and industry. It provides a framework to assist organizations with becoming a NERC Registered Entity, including some additional steps that will need to be taken by a new Registered Entity shortly after the registration process has been formally completed.

This comprehensive welcome package introduces new Entities to the NERC Registration process and assists any Entities that are interested in learning about what is required of them to be registered as a new NERC Registered Entity or preparing to register with NERC for the first time.

It also provides new and current Registered Entities alike with a wealth of valuable information and reference materials pertinent to NERC Registration and Certification, compliance, Entity profile questionnaires and risk assessments, Section 1600 mandatory reporting requirements and much more.

This is one resource every Entity should keep on hand and readily available for easy reference.

ERO Enterprise Registration Procedure (Revised and Updated)

This procedure was updated to help new Entities that are candidates for registration with NERC understand key terminology, how the Registration process works, and initial responsibilities for the Entities, NERC and REs.

In accordance with the regional delegation agreement, the REs have been assigned the responsibility of initiating the registration process for Entities functioning as owners, operators and users of the BPS.

While this document primarily outlines Registration and other related processes, it also contains important information regarding certain Registration processes that are relevant to existing Registered Entities.

Zero-Day Vulnerabilities

By Segun Adebayo, PhD, Sr. Analyst, and Sam Ciccone, Principal Reliability Consultant

The term "zero-day" refers to a newly discovered flaw in a system and the fact that the system owners have zero days to fix the flaw because it has already been, has the potential to be, or is currently being exploited by a threat actor.

Key definitions to understand a zero-day

A **zero-day vulnerability** is a flaw that is unknown or not publicly disclosed to the vendor such that the system involved cannot be patched and anti-virus products are unable to detect its exploitation through signature-based scanning (Bilge and Dumitras, 2012). It would be missed by most/all signature-based tools, which include intrusion detection systems (IDS) and intrusion prevention systems (IPS), whether network or host-based.

A **zero-day exploit** is when security researchers or threat actors take advantage of a zero-day vulnerability and create either a proof-of-concept exploit for demonstration and remediation purposes, or weaponize it with a suite of other tools used for command and control (C2), persistence, data exfiltration, and pivoting into other systems once they are inside the environment.

A **zero-day attack** is when a threat actor uses any of these unknown and unpatched vulnerabilities to commit a cyberattack, often resulting in losses to the affected system.

When put together, a zero-day attack occurs when a zero-day exploit is carried out on a zero-day vulnerability within a system. Discussions on the subject of zero-day exploits are critical because very little is known about such exploits due to the absence of data until after the attacks are discovered.

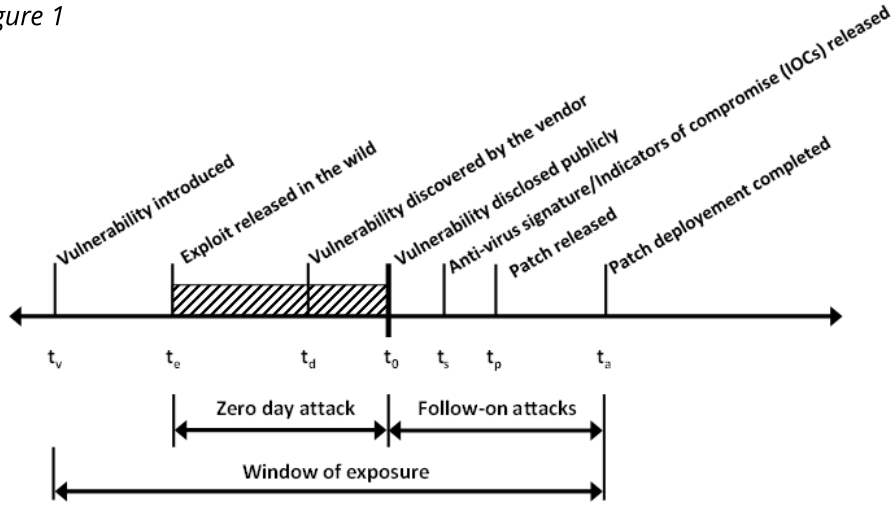
What about the NERC CIP Standards?

NERC standard CIP-007-6 governs patch management in requirement R2, sub-requirement 2.2., which states, "at least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1."[1] Unfortunately, by this point, the vulnerability has been exposed for a significant period, allowing threat actors to attack the system if you are relying on patching as your only vulnerability management mitigation strategy.

Some of the most important concerns around zero-day exploits are the duration, prevalence and characteristics of the attack (Bilge and Dumitras, 2012). The phrase "window of exposure" of a vulnerability is commonly used to describe the duration until all vulnerable hosts are patched (Schneier, 2000).

Figure 1 shows a schematic diagram of the attack timeline. These events do not always occur in this order, although the time of vulnerability disclosure to public (t0) and time

Figure 1



of patch release (tp) may be greater than or equal to the time of vulnerability discovery by the vendor (td). The relationship between the time of vulnerability discovery by vendor (td) and time of exploit release in the wild (te) cannot be determined in most cases. For a zero-day attack, the time of vulnerability disclosure to public (t0) is greater than the time of exploit release in the wild (te). (Source: Click Here)

Who conducts zero-day attacks?

Zero-day vulnerabilities are often discovered by security researchers (i.e., anyone who hacks at a system until they identify vulnerabilities) who may provide the information on this vulnerability to the system owners or vendors by means of "responsible disclosure"[2] (i.e., they work with the system owners or vendors) for a "reward," publish or present the finding at security conferences, and/or sell to governments or criminals for profits.

The zero-day attack resulting from the vulnerability may have any of the following motivations:

- Financial gains, as is the case with cybercriminals
- Social or political motives, as with hacktivists
- Corporate spying conducted on companies by corporate espionage hackers

[1] NERC CIP Standard CIP-007-6

[2] https://www.sentinelone.com/cybersecurity-101/zero-day-vulnerabilities-attacks/

Continued on Page 8

Zero-Day Vulnerabilities

Continued from Page 7

- Cyberwarfare, which involves governments or state actors

Victims of zero-day attacks include individuals, companies and governments. The attacks are often delivered as malware by way of social engineering or phishing.

What are the consequences?

The havoc resulting from a zero-day attack may include loss of data (e.g., sensitive propriety data, personal identifiable information, financial data, etc.), unauthorized remote access, unauthorized system control, access denial, files corruption, spyware installation, and data encryption.

Examples of recent zero-day exploits include:

- Google chrome, 2021: Unauthorized data access
- Zoom, 2020: Remote code execution
- Apple, 2020: Unauthorized remote access
- Microsoft Windows 2019: Government espionage operation
- Stuxnet, 2010: Unauthorized system control
- SolarWinds, 2020: Supply chain attack with Command and Control (C2)

The reported market value of a new vulnerability ranges between $500 - $250,000 (Miller, 2007; Greenberg, 2012). The lowest value is from Mozilla's bug bounty program, whereas the highest value is from an iOS exploit between a developer and a U.S. government contractor.

Are there examples of lessons learned?

In the Stuxnet breach of 2010, attackers were able to access Natanz systems without internet connectivity. In his thesis on the Stuxnet attack, Ronald L. Lendvay identified three main lessons learned: system access, system security and policy.

One of the lessons centered on policy and failure to abide by security protocols. "Effective technology security policy should focus inward on vulnerabilities rather than outward toward threats, due to the ever-evolving nature of cyber threats."(Lendvay, 2016)

Are there other things you can do?

As an example, when a vulnerability is identified, the first response could be to look for a "workaround" (including disabling services or uninstalling applications) until a patch is ready for deployment. For example, when the Print Nightmare vulnerability was identified over the summer, the first response was to disable the print spooler on all devices (a task that can be accomplished quickly) to eliminate the threat. The patch was available almost two months later.

Additional recommendations include increasing network visibility, identifying and prioritizing crown jewels, boosting incident response capabilities, validating network segmentation, and improving secure credentials management.

(Dragos: ICS CYBERSECURITY YEAR IN REVIEW 2020)

Conclusion

Borrowing the words of a NortonLifeLock employee, "just because zero-day exploits are meant to fly under the radar doesn't mean you should let these stealthy cyberattacks fall off your own radar." There are still measures you can take to hone in on cybersecurity best practices to avoid zero-day exploits. Those include such things as learning from other attacks and their subsequent lessons learned, continuously improving your cybersecurity program to find gaps in vulnerabilities and increase competencies of your staff around vulnerability management.

Also, looking for workarounds can help mitigate the impact of these vulnerabilities and attacks. Dave Sopata, Principal Reliability Consultant at RF, puts it this way: "although zero-day are very important, understanding the baseline and normal operational conditions of a system are very critical, as these enable prompt identification of deviations from the norm." Please review the Learn More and References sections, which have a plethora of information around these subjects.

Learn More

- Zero-day Brokers Podcast: https://darknetdiaries.com/episode/98/
- Examining Public ICS OT Exploits - Dragos 2021.pdf
- Understanding the Challenges of OT Vulnerability Management and How to Tackle Them (dragos.com)
- Dragos_2020_ICS_Cybersecurity_Year_In_Review.pdf
- Global Electric Cyber Threat Perspective - Dragos 2021.pdf

References

Bilge Leyla, and Tudor Dumitraş. "Before we knew it: an empirical study of zero-day attacks in the real world." In*Proceedings of the 2012 ACM conference on Computer and communications security*, pp. 833-844. 2012.

B. Schneier. Cryptogram September 2000 - full disclosure and the window of exposure. Click Here

A. Greenberg. Shopping for zero-days: A price list for hackers' secret software exploits. Forbes, 23 March 2012. Click Here

C. Miller. The legitimate vulnerability market: Inside the secretive world of 0-day exploit sales. In Workshop on the Economics of Information Security, Pittsburgh, PA, June 2007.

Ronald L. Lendvay. Shadows of STUXNET: Recommendation for U.S. Policy on Critical Infrastuure Cybe Defense Derived from the STUXNET Attack, March 2016

MISO Participates in GridEx VI

The GridEx VI exercise wrapped up on November 17, 2021, a culmination of work from more than 700 planners across the United States. The exercise, hosted by E-ISAC every two years, allows utilities and RTOs to exercise response and recovery plans in the face of simulated, coordinated attacks on the North American bulk power system and other critical infrastructure. This year, the simulation included both cyber and physical attacks.

MISO coordinated with five member utilities, two Reliability Coordinators, and the Federal Bureau of Investigation for GridEx VI, allowing the organizations to continue strengthening lines of communication and cooperation. The GridEx program allows member utilities and RTOs/ISOs the opportunities to define roles and responsibilities during an emergency response, as well as develop and manage expectations when it comes to policies, philosophies, process and communication to support the shared goal of system reliability.

The ability to practice response capabilities, actions, and integration prior to an actual event allows for lessons learned to be implemented for a better response to an incident.

Planning for GridEx VI began in mid-2020, identifying large operational events to serve as the foundation for exercise play. Lessons learned from the February 2021 cold weather event were integrated, allowing members to test updated procedures.

Vendor-produced dispatchable intermittent resource forecasts were also chosen as a scenario based on the continued movement to renewables within the industry. All organizations worked to develop specific injects to create immersive, informative scenarios.

The MISO planning team worked closely with partners to establish and validate a robust schedule, allowing for sufficient curveballs to keep players busy in all three of MISO's regions. Through the exercise, MISO players identified several areas where existing procedures could be enhanced and noted that further testing of concurrent major events within the System Operations training simulator would have provided a more seamless testing environment for operators.

The exercise provided a valuable opportunity to discuss and identify potential solutions for further implementation.

E-ISAC is currently gathering documentation from participants on exercise play, and the GridEx VI report is expected in March 2022. Although planning for GridEx VII won't begin for some time, utilities and RTOs should consider beginning to discuss and coordinate early in the process to identify organizational capabilities to test and allow for robust training opportunities for staff at all levels.

The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

Keeping Up with a Changing World

In the last five years, our electricity industry has seen significant changes. We're seeing a whole new generation mix driven by the reduction in use of fossil fuels and the increasing use of renewable energy sources. Our operational systems are evolving. Non-substation based monitors located mid-span on transmission lines are being used to determine line ratings dynamically. Advanced Distribution Management Systems (ADMS) are driving new efficiencies and increased reliability at the sub-transmission and distribution levels. Synchrophasor measurements are beginning to be used in real-time systems. The technologies that drive our operational systems are being revolutionized by the expanding use of virtualization, containers and cloud computing. At the same time, new threats have arisen, such as ransomware and the public release of advanced cyberattack tools.

However, our current CIP Standards went into effect more than five years ago. Yes, we've seen the addition of Standards for supply chain and for communications security. And we've seen additional, but relatively minor, changes in other areas. But the core fabric of the CIP Standards remains unchanged since mid-2016. The CIP Standards are Reliability Standards, and Reliability Standards change slowly. This is a good thing in many ways. We have a stable set of cyber and physical security Standards that are effective in reducing risk to the Bulk Electric System (BES). On the other hand, some see the CIP Standards as getting in the way of new technologies and new forms of cyber protections. Let's see if there's a way to incorporate some of these new technologies or address new threats while staying within the bounds of compliance with the existing Standards.

In this recurring column, I explore various questions and concerns related to the NERC Critical Infrastructure Protection (CIP) Standards. I share my views and opinions with you, which are not binding. Rather, this information is intended to provoke discussion within your Entity. It may also help you and your Entity as you 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 also may 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.

Pt Iroquois, MI – Photo: Lew Folkerth

Risk-based Standards

In my opinion, one way to keep pace with the rapid changes our industry is seeing is to develop a risk-based approach to the present CIP Standards. We already have a fully risk-based Standard in CIP-013-1, Supply Chain Risk Management. In CIP-013-1, you're required to develop, implement and maintain a risk management plan for certain areas of supply chain risk. I believe we can adopt risk-based techniques in our approach to compliance for most CIP requirements.

How do we begin? Let's start by choosing one area to improve using a risk-based approach. Figure 1 illustrates some of the areas we might consider. I'll choose a non-prescriptive Requirement, CIP-009-6, Recovery Plans for BES Cyber Systems, R1 Parts 1.3 and 1.4 covering backups and verification of backups.

Next, we'll need to identify the risks that we'll be addressing. This is somewhat backwards to the usual risk approach where we would identify and mitigate the highest risks in our risk register. In this case, one of the classic threats that can be mitigated by performing backups is the loss of a building by fire or other disaster. A new, at least in our context, threat is the encryption of systems and backups by ransomware.

Continued on page 11

Continued from page 10

Plan of Action

Figure 1 shows a modified risk management process. We'll use our known mitigation, backups, to select the risks that can be mitigated by backups. Then we will assess and prioritize these risks and design our backup systems to mitigate the highest priority risks.

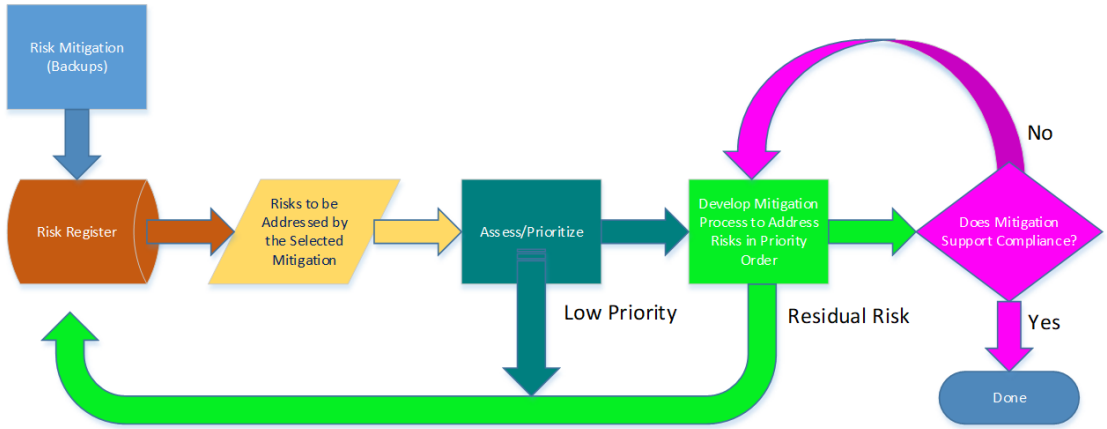


Figure 1

We'll partially mitigate the threat of fire by keeping the backups in a data center that is at a different location than the operational systems we're backing up. Mitigating the threat of ransomware will require a different approach. Ransomware works by encrypting all files accessible to a compromised system. If we keep our backups online, as is common practice, those backups are at risk of being encrypted along with the live files on our operational systems. In addition to keeping our backups at a different site, those backups must also either be offline or not writable by online systems.

When we have a process to mitigate the selected risks, we need to make sure that the process will meet the needs of our compliance program. If not, we need to re-design the mitigation process until it does meet our compliance needs. For example, we will need to make sure that all backup media is stored in a manner that conforms to our information protection program as required by CIP-011-2/3.

Requests for Assistance

If you are an Entity registered within the RF Region and believe you need assistance in sorting your way through this or any compliance related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the RF website here. Back issues of The Lighthouse, expanded articles and supporting documents are available in the RF CIP Knowledge Center.

Candidates for Risk-based Approach

Explicitly risk-based Requirements

- Supply chain
- Communications between Control Centers

Implicitly risk-based Requirements

- Vulnerability assessments
- Malicious code prevention
- Low impact BES Cyber Systems

Less-prescriptive Requirements

- Firewall rules
- Security event monitoring and alerting
- Incident response
- Recovery capability (backups)
- Information Protection

Risks not addressed by CIP (out of scope)

- Below the radar
  - ADMS
- Not operational technology
  - IT/corporate systems
- Historically out of scope but changing
  - PMU/PDC
- Beyond reach
  - Cloud infrastructure

Feedback

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

Lew Folkerth, Principal Reliability Consultant, can be reached here.

Winter 2021-2022 Resource Reliability Risk Assessment

RF performs an annual seasonal winter reliability assessment to ensure that its footprint has adequate resources to serve anticipated load demand. RF developed this assessment collaboratively with data provided from both PJM and MISO. This article shares some highlights from MISO, PJM and RF assessments.

For the upcoming winter of 2021-2022, both MISO and PJM are expected to have an adequate amount of resources to satisfy their respective planning reserve requirements. However, if the upcoming winter of 2020-2021 experiences a higher than anticipated load demand and outages, there is a small likelihood that the MISO area will need to utilize Demand Response (DR) to meet resource adequacy.

The outage risk assessment outlined below further assesses the capability of both MISO and PJM to meet their planning reserve requirements under a random outage scenario based on actual Generator Availability Data System (GADS) outage data.

PJM Capacity and Reserves

Net Capacity Resources[1]	176,309 MW
Projected Peak Reserves	52,143 MW
Net Internal Demand (NID)	124,166 MW
Planning Reserve Margin	42.0%

The PJM forecast planning reserve margin of 42.0% is greater than the 14.7% margin requirement for the 2020 planning year. The planning reserve margin for this winter is lower than the 2020 forecast level of 49.5%. This is due to a decrease in existing certain generation and the increase of sales of capacity to entities outside of PJM.

A decrease in generation produced by burning coal participating in PJM capacity market is the largest driver of a decrease in existing generation.

As a result of increasing reports of existing and future supply shortages of fuel and non-fuel consumables going into the 2021-2022 winter season, PJM has initiated a Generation Resource Weekly Fuel Inventory and Supply Data Request.

The weekly requests start October 11, 2021 and will run through February 28, 2022, and they apply to all coal and oil resources (including dual-fuel units).

MISO Capacity and Reserves

Net Capacity Resources	140,818 MW
Projected Peak Reserves	43,486 MW
Net Internal Demand (NID)	97,322 MW
Planning Reserve Margin	44.7%

The MISO forecast planning reserve margin of 44.7% is greater than the margin requirement of 18.3% for the 2021 planning year. The planning reserve margin for this winter is lower than the 2020 forecast level of 48.5%. This is mostly due to a decrease in existing certain generation in MISO's footprint. A decrease in generation produced by burning coal participating in MISO market is the largest driver of a decrease in existing generation.

RF Footprint Resources

Net Capacity Resources	192,668 MW
Projected Peak Reserves	57,436 MW
Net Internal Demand (NID)	135,232 MW
Total Internal Demand (TID)	143,860 MW

Since both PJM and MISO projections have adequate resources to satisfy their respective forecasted planning reserve margin requirements, the RF Region is projected to have sufficient resources for the 2021-2022 winter period.

Random Generator Outage Risk Analysis

The following analysis evaluates the risk associated with planned and random forced outages that may reduce the available capacity resources below the load demand obligations of PJM or MISO. Please see the full report on our website for a detailed explanation regarding how the analysis was performed.

[1]Net capacity resources include existing certain generation and net scheduled interchange.

Continued on page 13

Winter 2021-2022 Resource Reliability Risk Assessment

Continued from page 12

Exhibits 1 and 2 are based on forecasted winter 2021-2022 demand and capacity resource data for the PJM and MISO areas. The daily operating reserve requirement for PJM and MISO at the time of the peak demand is also included as a load obligation.

The firm demand and the demand that can be contractually reduced as a DR are shown in shades of green. The firm demand constitutes the Net InternalDemand (NID), with Total Internal Demand (TID) including the effects of DR. 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 representing the 50/50 demand forecast and one representing the 90/10 demand forecast. For instance, the 50/50 demand forecast projects a 50% likelihood that demand exceeds the forecast (e.g., 124,166 MW for PJM). The 90/10 demand forecast is a more conservative model, projecting a 10% chance that demand exceeds the forecast (e.g., 134,599 MW for PJM).

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.

While scheduled outages during the winter season are generally minimal, there are a small number of outages that extend during the winter, which are reflected in the Scheduled Maintenance (colored gray) in the Outage bar.

The probability percentages related to the amount of random forced outages that equal or exceed the amount 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 forced outages, with a decreasing probability for the amount of random forced outages.

In the PJM chart, the random forced outages represented by the bar above the 100% point is 520 MW. This means that the probability of there being at least 520 MW of random generation outages is 100%. Similarly, at the 10% point, the outages represented by the bar above the 10% point is 20,094 MW (520 MW + 19,574 MW). There is a 10% probability that there will be at least 20,094 MW of outages.

As shown by the probabilities and corresponding amounts of random forced outages, the distribution of random forced outages is not linear throughout the range of outages observed. To the right of the Outage bar are the probabilities of the random generation outages that correspond to different levels of demand obligation.

In Exhibit 1 for PJM, there is a minimal risk that the amount of outages would require demand response for both the 50/50 and the 90/10 demand forecast for the upcoming winter.

Exhibit 1 - 2021/2022 Winter PJM Resource Availability Risk Chart

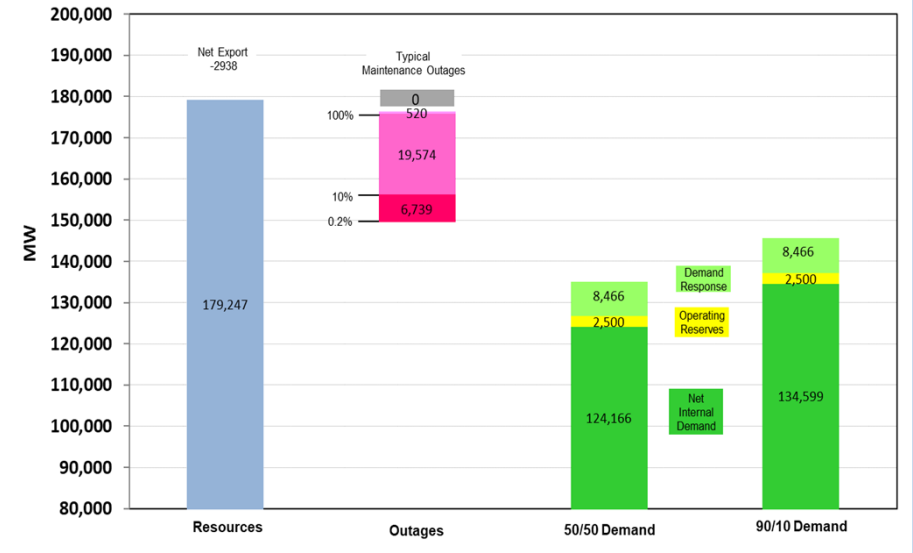
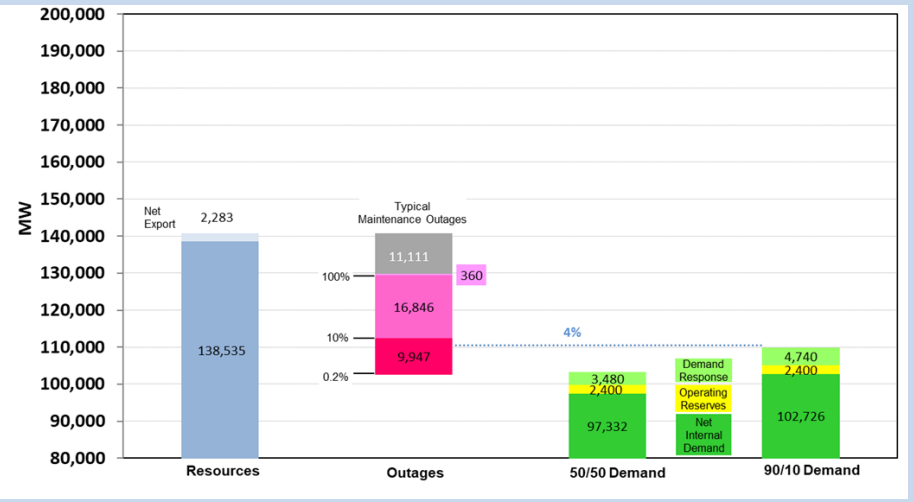


Exhibit 2 contains the information to perform the same analysis for MISO. The top of the 90/10 demand obligation with the operating reserves has a 4% probability that DR will be required during high demand.

Exhibit 2 - 2021/2022 Winter MISO Resource Availability Risk Chart



2021 Long Term Resource Assessment for the ReliabilityFirst Region

RF performs an annual assessment to ensure its footprint has adequate resources to serve anticipated load demand for the next 10-year period. Each assessment area within RF (i.e., PJM and MISO) has a targeted reserve margin level, which identifies the minimum amount of resources needed to meet a loss of load expectation (LOLE) of one day in 10 years. The results of this assessment express each areas' ability to meet the targeted level. RF developed this assessment collaboratively with data provided from both PJM and MISO. This article shares some highlights from the assessment.

Frequently Used Terms

Existing-Certain: Includes operable capacity expected to be available to serve load during the peak hour with firm transmission

Tier 1: Includes capacity that is either under construction or has met the required milestones

Tier 2: Includes capacity that has been requested but has not met some required milestones or executed certain agreements

Tier 3: Other planned capacity that does not meet the requirements of Tier 1 and Tier 2

Confirmed Retirements:

Capacity with formalized and approved plans to retire (Please note that generator retirements are evaluated on a case-by-case basis by PJM or MISO for potential reliability impacts. If it is determined that reliability impacts exist, the Generation Owner is requested 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:

Capacity that is considered likely to retire by resource owners, but the formal notification has not been submitted to the respective party; units for which such notice has been made also are included, but a reliability impact assessment or mitigation is pending

Key Findings

PJM is projected to have a 0.28% load growth rate over the next 10 years and will meet its target reserve margin requirement of approximately 15%, which includes both Existing-Certain and Tier 1 resources.

MISO is projected to average a 0.28% load growth rate for 2022 through 2031.

The MISO target reserve margin, which includes both Existing-Certain and Tier 1 resources, satisfies its reserve margin target through 2024.

For 2025 through 2031, the MISO projected reserve margin, which includes both Existing-Certain and Tier 1 resources, is below the target reserve margin. The largest deficit was identified in 2031, which was 13,226 MW below the target. Since these projected deficits start three years into the future, it is probable that up to 28% of Tier 2 and Tier 3 resources will be needed for MISO to meet their target reserve margin requirement.

Continued on page 15

2021 Long Term Resource Assessment for the ReliabilityFirst Region

Continued from page 14

PJM

Capacity and Reserve Margin

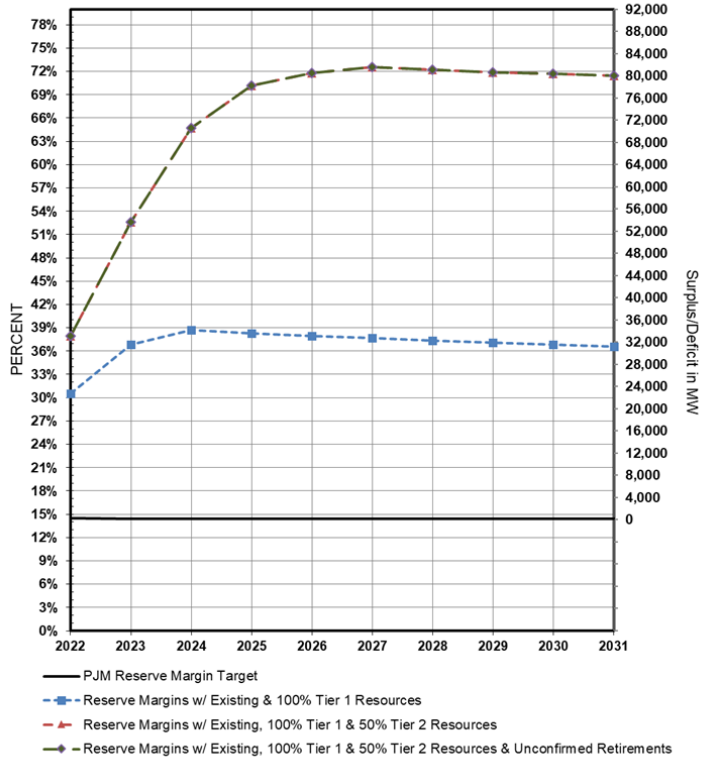
PJM resources are projected to be 194,723 MW in 2022 and then increase to 248,174 MW by the end of 2031. The reserve margin calculations include planned generation retirements, planned generation additions and changes, and 50% of the Tier 2 projects from the generation interconnection queue.

The summer reserve chart shows the reserve margin for PJM from 2022 through 2031. Please note that varying resource scenarios are used to gauge how much of the generation queue (i.e., generation that is yet to be built) is needed to stay above the target reserve margin. The blue line represents PJM's reserve margin with both Existing-Certain and all Tier 1 resources. On average, PJM has a 36.8% reserve margin and is expected to meet its target reserve margin (approximately 15%) from 2022 through 2031.

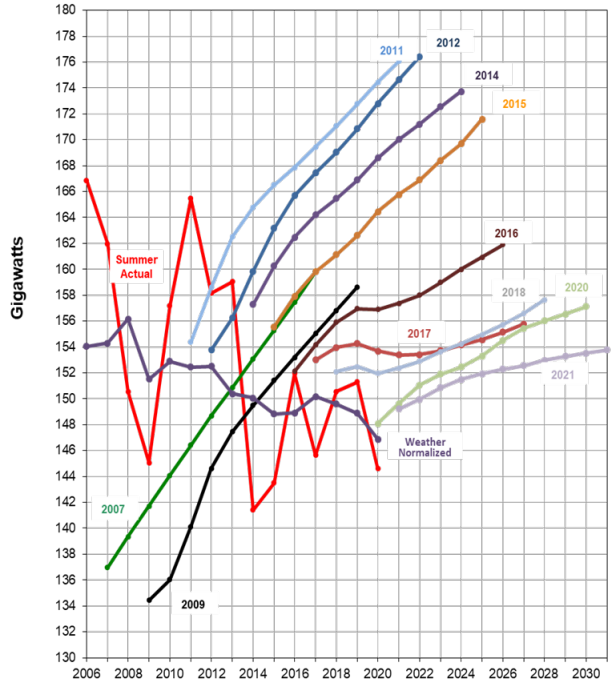
Peak Demand

The peak demand chart displays actual demand data with a 10-year forecast of demand. PJM's 10-year forecasted growth indicates that peak demand has flattened over time. Based on the latest 2021 forecast, PJM is projected to average a 0.28% load growth per year over the next 10 years. The PJM 2022 summer peak demand is projected to be 149,966 MW and increase to 153,759 MW in 2031 for total internal demand (TID). Annualized 10-year growth rates for individual PJM transmission zones range from -1.2% in Potomac Electric Power Company to 0.9% in Pennsylvania Electric Company.

PJM RTO
Summer Reserve Margin Projections
2022 - 2031



PJM RTO Peak Demand Data
Actual 2006 - 2020
Select 10-year TID Forecasts Through 2031



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
2019 Includes the expansion of the PJM RTO footprint with Ohio Valley Electric Cooperative

Continued on page 16

2021 Long Term Resource Assessment for the ReliabilityFirst Region

Continued from page 15

MISO

Capacity and Reserve Margin

MISO resources are projected to be 157,800 MW in2022and then increase to 173,470 MW by the end of 2031. This reserve margin calculation includes planned generation retirements, planned generation additions and changes, and Tier 2 and Tier 3projects from the generation interconnection queue.

Since last year, MISO has received 1.5 GW of formal retirement requests of largely coal and gas – 1.3 GW coal, 0.2 GW gas. In order to be proactive, MISO conservatively solicits voluntary responses to assess potential resource outcomes via the Organization of MISO States (OMS)-MISO Survey process. This approach allows MISO and its members to discuss potential future resource deficiencies well in advance. The larger retirement values in this LTRA are indicated by the voluntary OMS-MISO Survey process. If only firm retirements were reported, MISO would be resource sufficient throughout the period.

The MISO generator interconnection queue continues to show a steady increase of variable energy resources, which includes battery storage and hybrid resources. This trend along with the potential retirements from the survey indicate a decarbonization of the fleet seen across the industry. As decarbonization efforts progress, the next decade may bring large levels of fleet change similar to the reduction in reserve margins observed between 2010 to 2015 due to compliance with Mercury and Air Toxics Standards, Hazardous Air Pollutants Standard and other emissions regulations.

The projected five-year out Anticipated Reserve Margins indicate a regional generation shift. In the unlikely event that all potential retirements occur without new replacement capacity, a shortfall below the Reference Margin Level in 2024 and beyond may occur, but is not anticipated by MISO, its members and state regulators. Also, the extreme weather events of the past several years continue to stress the importance of ensuring the MISO Resource Adequacy construct sends the appropriate planning and operating signals that ensure members continue to perform reliably.

The summer reserve chart shows the reserve margin for MISO from 2022 through 2031. MISO's anticipated reserve margin, which includes Existing-Certain and all Tier 1 resources, satisfies the target for 2023. The MISO anticipated reserve margin projected for 2024 is 565 MW below the reserve margin target. Continuing in2025, the projected reserve margin is 2,966 MW below the target, and continues to decline to 13,226 MW below the target in 2031. These values are represented in the chart with the blue line.

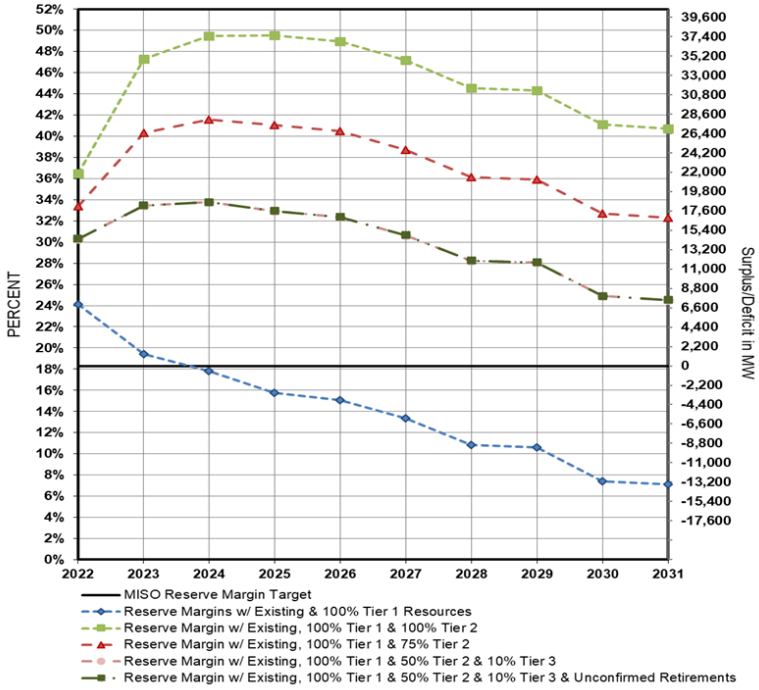
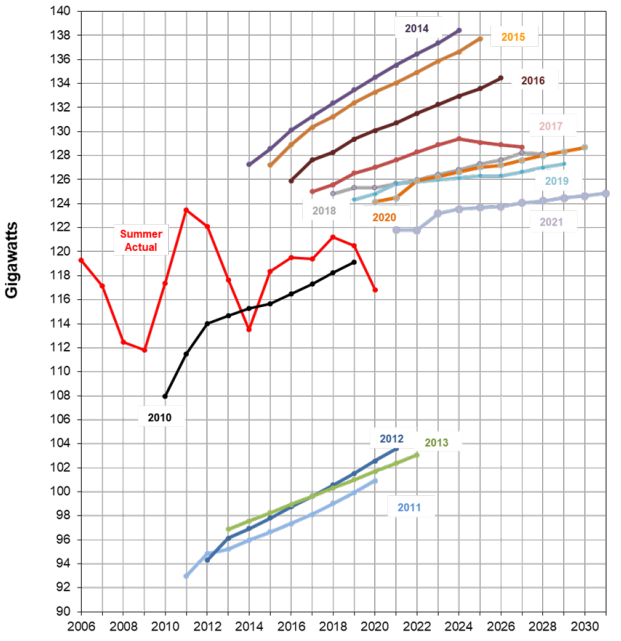


Figure 2 - MISO RTO Summer Reserve Margin Projections 2022 - 2031

MISO RTO Peak Demand Data Actual 2006 - 2020 Select 10-year TID Forecasts Through 2031



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

Continued on page 9

FERC, NERC and Regions Release Report on February 2021 Cold Weather Outages

On November 16, 2021, FERC, NERC and the Regions released the final Report on the February 2021 Cold Weather Outages in Texas and the South Central United States. The report discusses the severe cold weather event, which caused generating plant failures and led to more than 20,000 MW of rolling blackouts and loss of power for more than 4.5 million people in Texas.

The report finds that during the event, 1,045 generating units experienced outages, derates or failures to start (of these, 44.2% were caused by freezing issues and 31.4% were caused by fuel issues). The types of generation affected were 58% natural gas-fired, 27% wind, 6% coal, 2% solar, 7% other fuels and less than 1% nuclear.

In addition to analyzing what happened during the event, the report provides recommendations to help prevent future events from occurring. These recommendations include revising the Reliability Standards to require Generators Owners (GO) and Operators (GOPs) to:

- Identify and protect cold-weather-critical components;
- Operate to specific ambient temperatures and weather based on extreme temperature and weather data, and account for effects of precipitation and cooling effect of wind;
- Perform annual training on winterization plans;
- Develop Corrective Action Plans after experiencing freeze related outages;
- Provide the Balancing Authority (BA) with the percentage of the total generating unit capacity that the BA can rely upon during the "local forecasted cold weather;" and
- Account for effects of precipitation and accelerated cooling effect of wind when providing temperature data to BAs.

The report also recommends that GOs should be able to be compensated for retrofitting their units to perform at ambient temperatures, and that GOs and GOPs should include specific cold weather inspection and maintenance requirements.

To address the natural gas fuel issues that contributed to the event, the report recommends:

- Legislatures and regulatory agencies with jurisdiction over natural gas infrastructure facilities should require them to implement and maintain cold weather preparedness plans;
- Natural gas facilities should take voluntary measures to prepare for cold weather;
- GOs/GOPs should identify reliability risks related to their natural gas fuel contracts and provide the BAs with the percentage of total generating unit capacity that the BA can rely upon during forecasted cold weather;
- FERC should consider establishing a forum to identify actions to improve the reliability of the natural gas infrastructure system;
- Additional revisions to the Reliability Standards to protect critical natural gas infrastructure from manual and automatic load shedding;
- To require BAs' operating plans to prohibit use of critical natural gas infrastructure loads for demand response; and
- To separate circuits that will be used for manual load shed from circuits used for underfrequency load shed (UFLS) and use the UFLS circuits only as a last resort.

Continued on page 18

Continued from page 17

NERC Releases 2021-2022 Winter Reliability Weather Assessment

NERC recently released its 2021-2022 Winter Assessment, which covers the upcoming three-month (December–February) 2021–2022 winter period. The Assessment notes that reliability risk is elevated in areas that are vulnerable to extreme cold weather and natural gas disruptions. The Assessment also advises that generators are facing challenges in obtaining coal and oil fuels as supply chains are stressed.

Recommendations to help address these risks include the following:

- Grid operators, GOs and GOPs should review the NERC Level 2 Alert and NERC's Generating Unit Winter Weather Readiness Guideline, taking recommended steps prior to winter.
- BAs should poll their generating units periodically and in advance of approaching severe weather to understand their readiness level for normal and extreme conditions, giving consideration for unit weatherization, as well as fuel supply risk.
- BAs and Reliability Coordinators should conduct drills on alert protocols to ensure they are prepared to signal need for conservative operations, restrictive maintenance periods, etc.
- BAs and GOPs should verify protocols and operator training for communication and dispatch.
- Distribution Providers and Load-Serving Entities should review non-firm customer inventories and rolling blackout procedures to ensure that no critical infrastructure loads (e.g., natural gas, telecommunications) would be affected.

Report on FERC, NERC and the Regions' Joint Review of Protection System Commissioning Programs

On November 2, 2021, FERC, NERC and the Regions issued their Joint Review of Protection System Commissioning Programs report. The report summarizes the results of a project to review Entity protection system testing or protection system commissioning (PSC) programs and procedures.

The project was initiated after a sample of MIDAS data indicated that between 18% and 36% of misoperations could be attributed to issues that should have been detected through PSC. The goal of the project was to reduce these misoperations by identifying opportunities for improvement and developing recommendations and best practices for Entity PSC programs.

The report identifies these common issues that occurred in participants' PSC programs:

- Lack of independent review of protection system designs by the commissioning group prior to construction;
- Lack of centralized overarching PSC programs that serve as a tool for the execution of PSC procedures; and/or
- Lack of feedback controls to prevent repeated problems in future PSC projects.

The team also identified 16 different recommendations for improvement and 23 observed best practices, which are summarized in pages 2-9 of the report.

FERC Staff Report on Lessons Learned from FERC-led CIP Reliability Audits

In October, FERC released its 2021 Staff Report on Lessons Learned from Commission-led CIP Reliability Audits. The anonymized report finds that overall, most of the cybersecurity protection processes and procedures adopted by the audited Entities met the requirements of the CIP standards. The report also includes voluntary recommendations on cybersecurity practices and a recap of lessons learned from past years. There are 14 lessons learned discussed (see pages 9-17 of the report).

Standards Update

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

General NERC Standards News

NERC Board Emphasizes the Need to Address Cold Weather Risks and Extreme Events

On November 4, 2021, in anticipation of the release of the FERC, NERC and Regional Entity Staff Report on the 2021 Cold Weather Outages, the NERC Board discussed related priorities. Among the actions taken, the Board approved the 2022-2024 Reliability Standards Development Plan but with one important caveat. The NERC Board provided in a resolution that the Development Plan should include a cold weather operations, preparedness and coordination standard as a high priority item. This resolution was adopted to reflect the recommendations of the FERC, NERC, and Regional Entity recommendations from the joint inquiry.

The NERC Board also approved the 2022 ERO Enterprise Work Plan Priorities. These priorities are identified and designed to align with the focus areas in the ERO Enterprise's Long-Term Strategy. Below are the four risk elements addressed in the 2022 Work Plan Priorities:

- Improve Bulk Electric System resilience for widespread, long-term extreme temperature events.
- Deepen planning and operating focus beyond capacity adequacy toward energy sufficiency.
- Enhance the structure of the CIP Standards, including review and improvement of the bright-line risk criteria.
- Expand the impact of the E-ISAC through information sharing, communications and monitoring of critical security threats.

Notable NERC Filings

In September-November, NERC filed the following with FERC:

On October 12, 2021, NERC with the Regions submitted comments on an Advance Notice of Proposed Rulemaking (ANOPR). The ANOPR itself introduced "potential proposals intended to holistically reform regional transmission planning and cost allocation and generator interconnection procedures." The ERO submitted comments to:

- Propose enhancements for modeling and studies under pro forma generator interconnection procedures, particularly through the inclusion of electromagnetic transient ("EMT") modeling and studies;
- Propose enhancements to the Commission's pro forma interconnection agreements to incorporate recommendations from NERC Reliability Guidelines pertaining to integration of inverter-based resources; and
- Support the Commission's exploration of better coordinated transmission planning.

On September 29, 2021, NERC submitted a petition to FERC for approval of revisions to the NERC Rules of Procedure. The proposed revisions include, among other things, change to the following items:

- The review and disposition of self-logged items
- Time and location requirements for Compliance Audits of RCs, BAs and TOPs
- Eliminating the posting of the annual Self-Certification schedule in favor of Self-Certifications tailored and scheduled according to specific risks

Notable FERC Orders

On November 2, 2021, FERC issued an order accepting both NERC and the Regions' 2022 Business Plans and Budgets.

Standards Update

New Standards Projects

New Standards projects are described on the NERC Standards website, along with links to all drafts, voting results, and similar materials. Please take note that some Enforcement Dates relate to specific requirements and sub-requirements of the Standard and are detailed below. Recent additions include the following:

Project	Action	Start/End Date
Project 2021-07- Extreme Cold Weather Grid Operations, Preparedness, and Coordination	Comment Period	11/22/2021-12/21/2021

Recent and Upcoming Standards Enforcement Dates	
January 1, 2022	TPL-007-4 - Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements 6, 6.1-6.4, 10, 10.1-10.4); PRC-012-2 - Remedial Action Schemes (Requirement R9)
July 1, 2022	PRC-002-2 – Disturbance Monitoring and Reporting Requirements (100% compliance for Requirements 2-4, 6-11) CIP-012-1 - Cyber Security - Communications between Control Centers
October 1, 2022	PRC-024-3 – Frequency and Voltage Protection Settings for Generation Resources; CIP-005-7 – Cyber Security – Electronic Security Perimeter(s); CIP-010-4 –Cyber Security – Configuration Change Management and Vulnerability Assessments; CIP-013-2 – Cyber Security – Supply Chain Risk Management
January 1, 2023	TPL-007-4 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements R3, R4, 4.1, 4.1.1-4.1.2, 4.2, 4.3, 4.3.1, R8, 8.1, 8.1.1-8.1.2, 8.2, 8.3, and 8.3.1)
January 1, 2024	TPL-007-4 – Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements R7, 7.1, 7.2, 7.3, 7.3.1-7.3.2, 7.4, 7.4.1-7.4.3, 7.5, 7.5.1, R11, 11.1, 11.2, 11.3, 11.3.1-11.3.2, 11.4, 11.4.1-11.4.3, 11.5, and 11.5.1)

These effective dates can be found here.

Best Wishes to our 2021 Retirees

Larry Bugh Retires from RF

The RF team would like to extend our heartfelt congratulations to Larry Bugh on his retirement! After 15 years at RF and nearly 50 in our industry, Larry is retiring as the Chief Security Officer, and his steadfast leadership has made him a valuable pillar of our executive team.

Larry has held various positions at RF and also has the important role of staff liaison for the RF Critical Infrastructure Protection Committee (CIPC). Larry has been a key contributor and planner for each of the industry-wide GridEx exercises. He is routinely sought out by NERC for guidance on security matters, the latest being asked to help author the ERO-wide Crisis Action Response Plan. Additionally, Larry has led RF's Pandemic Response Team since March 2020 to ensure the health and safety of staff, ERO and Entity personnel and our stakeholders remains a top priority.

One of the many notable aspects of his career is his role in the first-ever approved NERC Reliability Standard. Larry was the chairperson for the Standard Drafting Team for Version 1 of the Cyber Security Standards (CIP-002 thru CIP-009), the Version 1 Violation Severity Levels, Version 2 Violation Severity levels and Violation Risk Factors, and the Order 706B Implementation plan. He also participated in drafting the Urgent Action Cyber Security Standard (1200).

"Larry has been an outstanding and steadfast contributor to the reliability and security of our industry his entire career," said Tim Gallagher, RF President and CEO. "His quest to learn, ability to stay current, energy level and work ethic are so very impressive, and he served our country with honor and distinction as a member of our armed forces. Larry, thank you for all you have done for me and RF, our industry and our country. RF and our industry are losing a true friend. My very best wishes to you in retirement."

Larry began his career in the planning department for Ohio Edison, and prior to RF, he served as Manager, Information Technology for ECAR. He holds an Associate degree in Electrical Engineering from Kent State University and a BA in Business Management from Malone College. He is a graduate of the United States Army Sergeants Major Academy and served our country for many years with distinction in the Army National Guard.

Additional Retirees

The entire RF teams sends our warmest wishes for a happy retirement to the following members of staff. Our farewell is full of gratitude for all they have done over the years to advance the RF mission, as well as the wonderful camaraderie they brought to the RF family.

- Renata Fellmeth was with RF for 15 years and retired as a Process Coordinator.
- Joyce Lemmon was with RF for 15 years and retired as a Process Coordinator.
- Ray Sefchik was with RF for 9 years and retired as the Director of Entity Engagement.
- Don Urban was with RF for 13 years and retired as a Principal Analyst, Risk Analysis & Mitigation.

All of our 2021 retirees will be greatly missed!

Technical Talk with RF

RF offers a regularly scheduled monthly call to provide Entities and stakeholders with a forum for addressing topics and questions relevant to reliability, resilience and security. These calls are held on the third Monday of each month from 2:00 to 3:30 p.m. EST.

New Date: The January 10, 2022 call is one week earlier than our regular schedule to accommodate Martin Luther King Jr. Day.

In addition to compliance-related content, these calls cover other risk areas, such as cybersecurity, misoperations, situational awareness and much more. Please invite your Operations, Planning, Cyber, Design, IT, and/or Maintenance personnel, if you see an agenda topic they would be interested in!

January 10 Tentative Agenda Topics

Align Update

Tony Jablonski – Manager, Risk Analysis and Mitigation (RAM)

- This update is especially relevant for Primary Compliance Contacts (PCC) and their alternates who are responsible for using Align and the Secure Evidence Lockers.

2022 Keynote Address and Tech Talk Kickoff

Jeff Craigo – Vice President, Reliability & Risk, RF

- This discussion is especially relevant for organizational leaders and anyone interested in understanding how RF partners with industry to preserve and enhance reliability, resilience and security with an emphasis on continuous improvement and operational excellence.

Mental Wellness, Human Performance and the Impact on Reliability

Tanya Hickey – Senior Manager, Health & Safety Strategies, Ontario Power Generation (OPG)

- During the RF Human Performance (HP) workshop in August, we received a large volume of questions and interest in the presentation regarding OPG's Total Health Strategy. This Tech Talk revisits the strategy, identifies the business case model, and highlights successful results to date.
- This presentation is especially relevant for HR personnel, HP specialists, field supervisors and all levels of management that are interested in the impact of mental health on their workforce.

Recent Presentations

In case you missed the October, November or December Tech Talks, or would like to reference the slides, the materials presented are posted on the RF website.

- Self-Certifications for O&P Standards (Oct)
- Field Walk-downs for Facility Ratings (FAC-008) and Vegetation Management (FAC-003) (Oct)
- Odessa Disturbance Report (Nov)
- The Real Risks of Patching (Nov)
- Compliance Oversight Plans (Dec)
- ERO Practice Guide on the CIP-014-02 Requirement 1 Risk Assessments (Dec)
- Align presentations from each month are under the Align Updates tab at the bottom of the page

Watt's Up at RF

Welcome Marcus Noel

As an integral part of RF's continued dedication to security, the organization is pleased to welcome Marcus Noel as the new CSO. In this role, he is responsible for establishing and maintaining the organization's cybersecurity and physical security management program to ensure that information and physical assets are adequately protected. Additionally, he will manage the critical task of elevating industry relationships to understand, address and communicate emerging threats and security trends.

Previously, Marcus spent 10 years at FirstEnergy Corp. where he worked on the Cybersecurity Governance Team, the Security Operations Center, Security Technologies, and ultimately served as Manager of the Cybersecurity Organization. Prior to FirstEnergy, he worked in cybersecurity at PNC Bank and Cuyahoga Community College.

Marcus is a graduate of Bryant & Stratton College with an associate degree in Accounting, Baldwin-Wallace University with a bachelor's degree in Business Administration, and Cleveland State University with a master's in Business Administration and a Juris Doctorate in Law. He has held the Certified Information Systems Security Professional certification since 2009.

He will succeed current CSO, Larry Bugh, who will retire at the end of this year.

Welcome Beth Dowdell

RF is thrilled to welcome Beth Dowdell as the new Senior Director of Corporate Services. In this role, she will oversee the Human Resources, Finance and Information Technology teams, as well as spearhead and implement high-value strategic initiatives for the organization. Her thoughtful leadership and change management skills will support succession planning, talent assessment, corporate goal setting, business and strategic plans, as well as financial projections, analysis and budget planning.

Beth has more than 15 years of management experience leading high-performing teams in high-growth companies. She has developed strategies to improve productivity while meeting operating and fiscal targets. Prior to RF, she was the Senior Director of Operations at American Endowment Foundation where she drove efficiency through process improvement and automation, created KPIs and standardized reporting and mentored other leaders. Before that, she was the Vice President of Operations then Vice President of Enterprise Products at Asurint. Within those roles she led multiple teams focusing on employee development, improving efficiency through technology and product development.

Beth has a Bachelor of Science degree in Management from Indiana Wesleyan University.


Happy Holidays from RF

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
CENTERPOINT ENERGY
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
EXELON CORPORATION
FIRSTENERGY SERVICES COMPANY
HAZELTON GENERATION LLC
HOOSIER ENERGY RURAL ELECTRIC COOPERATIVE, INC
ILLINOIS CITIZENS UTILITY BOARD
ILLINOIS MUNICIPAL ELECTRIC AGENCY
INDIANAPOLIS POWER & LIGHT COMPANY
INTERNATIONAL TRANSMISSION COMPANY

Forward Together RF ReliabilityFirst

LANSING BOARD OF WATER AND LIGHT
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
WABASH VALLEY POWER ASSOCIATION, INC
WISCONSIN ELECTRIC POWER COMPANY
WOLVERINE POWER SUPPLY COOPERATIVE, INC