2021 MRO Regional Risk Assessment

February 2021

MIDWEST RELIABILITY ORGANIZATION

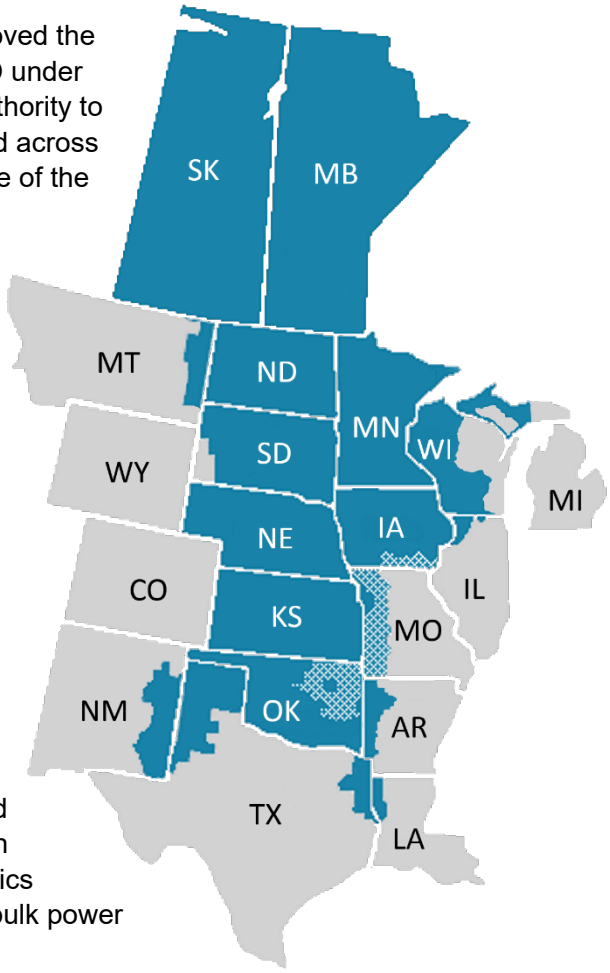
380 St. Peter St, Suite 800
Saint Paul, MN 55102
651-855-1760
MRO.net

Table of Contents

1. PREFACE

Midwest Reliability Organization (MRO) is dedicated to its vision of ***a highly reliable and secure North American bulk power system***. To ensure reliability of the bulk power system in the United States, Congress passed the Energy Policy Act of 2005, creating a new regulatory organization called the Electric Reliability Organization (ERO) to establish mandatory Reliability Standards and monitor and enforce compliance with those standards on those who own, operate or use the interconnected power grid.

In 2006, the Federal Energy Regulatory Commission (FERC) approved the North American Electric Reliability Corporation (NERC) as the ERO under section 215(e)(4) of the Federal Power Act. NERC delegates its authority to monitor and enforce compliance to six Regional Entities established across North America, including MRO. Recognizing the international nature of the grid, NERC as the ERO, along with MRO, established similar arrangements with provincial authorities in Canada.



The MRO region spans the provinces of Saskatchewan and Manitoba, and all or parts of the states of Arkansas, Illinois, Iowa, Kansas, Louisiana, Michigan, Minnesota, Missouri, Montana, Nebraska, New Mexico, North Dakota, Oklahoma, South Dakota, Texas, and Wisconsin. The region includes approximately 200 organizations that are involved in the production and delivery of electric power, including municipal utilities, cooperatives, investor-owned utilities, transmission system operators, federal power marketing agencies, Canadian Crown Corporations, and independent power producers.

MRO's primary responsibilities are to: ensure compliance with mandatory Reliability Standards by entities who own, operate, or use the North American bulk power system; conduct assessments of the grid's ability to meet electric power demand in the region; and analyze regional system events. Additionally, MRO creates an open forum for stakeholder experts in the region to discuss important topics related to addressing risk and improving reliable operations of the bulk power system.

2. INTRODUCTION

The MRO Regional Risk Assessment (RRA or assessment) is a document that MRO staff, with input from industry subject matter experts, prepares annually to identify risks to the reliable and secure operations of the bulk power system within MRO's regional footprint. Several ERO Enterprise-wide risk reports are used as a resource for this assessment and include:

- 2019 ERO Reliability Issues Steering Committee (RISC) Priorities Report (RISC report)
- 2021 ERO Compliance Monitoring and Enforcement Program Implementation Plan (CMEP IP)
- 2020 NERC State of Reliability Report (SOR report)
- 2020 NERC Long-Term Reliability Assessment (LTRA report)
- 2020 NERC/WECC Inverter-based Resource Modeling Report (IBR Modeling Report)

In addition to the above ERO Enterprise (collectively NERC and the Regional Entities, aka ERO) and NERC reports, MRO staff also reviewed several regional entity Regional Risk Assessments to capture any other region-specific identified risks that might also pertain to the MRO footprint. Some risks identified North American-wide can broadly present themselves in any of the ERO regional footprints, such as Human Performance and Skilled Workforce. However, other risks may be more geographic, regional, or registered entity-specific, that is, certain areas, regions or registered entities may have a higher exposure to, or are more susceptible to, a specific risk. Severe weather conditions or high concentrations of renewable generation are examples of these. Therefore, this assessment identifies which risks to the bulk power system may have a higher probability of occurrence within the MRO region or that may be regionally unique. This RRA also identifies which risks highlighted in the 2021 ERO-wide Compliance Monitoring and Enforcement Program (CMEP) Implementation Plan should be a focus of MRO's CMEP activities. Figures 1 and 2 illustrate the NERC planning assessment areas versus the NERC Regional Entity footprints. The planning assessment areas of SPP, the northwestern portion of MISO, SaskPower and Manitoba Hydro, all comprise the MRO region.

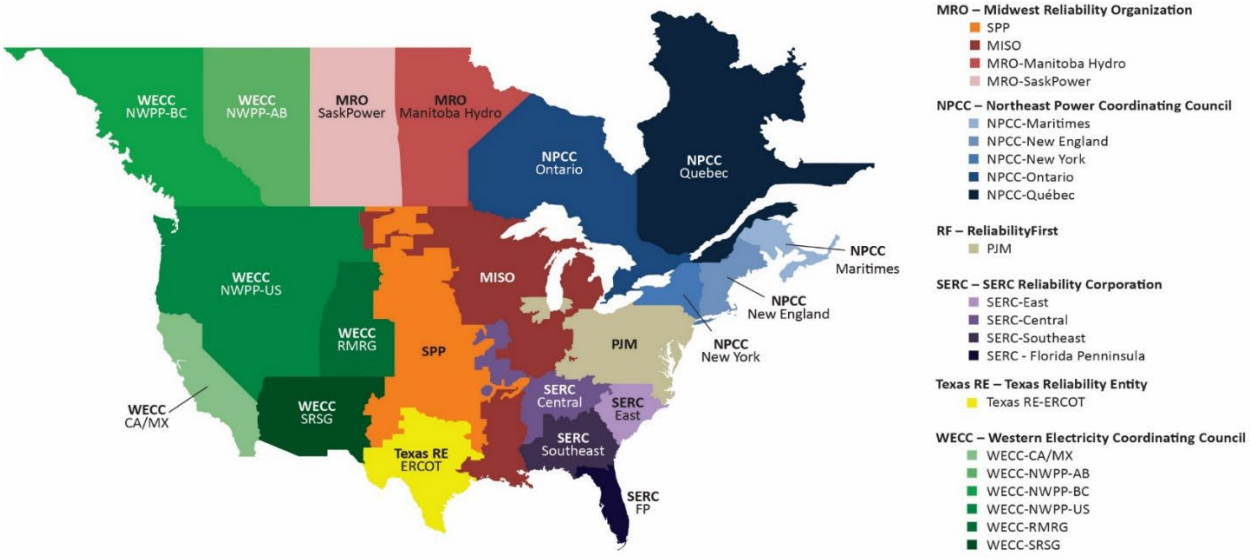


Figure 1: NERC Planning Assessment Areas

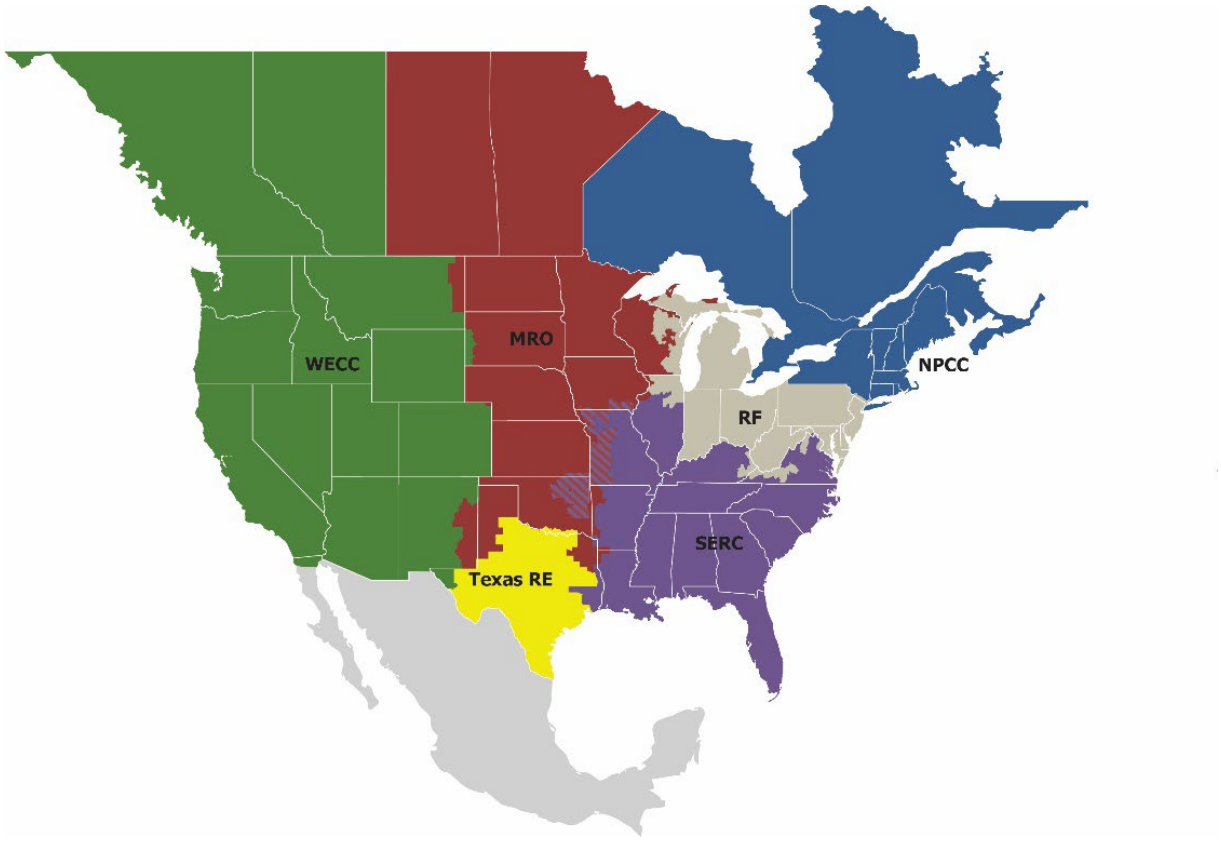


Figure 2: NERC Regional Entity Boundaries

MRO staff leveraged the expertise of the members of MRO's three advisory councils (Reliability, CMEP, and Security), each comprised of industry volunteers that help identify risks that the MRO region may be susceptible to experiencing.

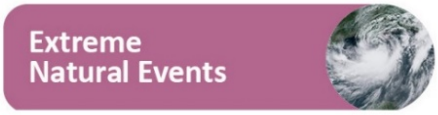
To the extent possible, recommendations and suggestions presented in this assessment are to help registered entities become more aware of and reduce risk to their individual systems. However, not all risk topics identified in the RRA include mitigation recommendations to reduce the risk.

3. ERO AND MRO REGIONAL RISK IDENTIFICATION AND RANKINGS

3.1 2019 ERO RISC Priorities Report: Risks and Rankings

The 2019 RISC Report[1] highlights forward-looking risks to the bulk power system that merit attention and then recommends actions that align with those risks. This biennial report consolidates the identified risks into four high level categories: 1) Grid Transformation, 2) Extreme Natural Events, 3) Security Vulnerabilities, and 4) Critical Infrastructure Interdependencies.

A. Bulk Power System Planning
B. Resource Adequacy and Performance
C. Increased Complexity in Protection and Control Systems
D. Situational Awareness Challenges
E. Human Performance and Skilled Workforce
F. Changing Resource Mix



A. Extreme Natural Events, Widespread Impact
   • GMD
B. Other Extreme Natural Events

A. Physical
B. Cyber
C. Electromagnetic Pulse

A. Communications
B. Water/Wastewater
C. Oil
D. Natural Gas

The risks are then classified as to whether they should be actively managed or monitored:

MANAGE 1. Changing Resource Mix	MANAGE 6. Loss of Situational Awareness
MANAGE 2. Bulk Power System Planning	MONITOR 7. Extreme Natural Events
MANAGE 3. Resource Adequacy and Performance	MONITOR 8. Physical Security Vulnerabilities
MONITOR 4. Increasing Complexity in Protection and Control Systems	MANAGE 9. Cybersecurity Vulnerabilities
MONITOR 5. Human Performance and Skilled Workforce	MANAGE 10. Critical Infrastructure Interdependencies

Following this classification, the risks are prioritized based on an industry-wide survey of bulk power system experts across the ERO footprint. The heat map shown in Figure 3 summarizes the results of

[1] The charts and figures in this section were taken from the 2019 RISC Report and are shared with permission.

the survey, with each individual risk mapped with the likelihood of the risk occurring (X-axis) and the impact if the occurred risk (Y-axis). Therefore, the upper right quadrant of the graph indicates higher risk and the lower left quadrant indicates lower risk.

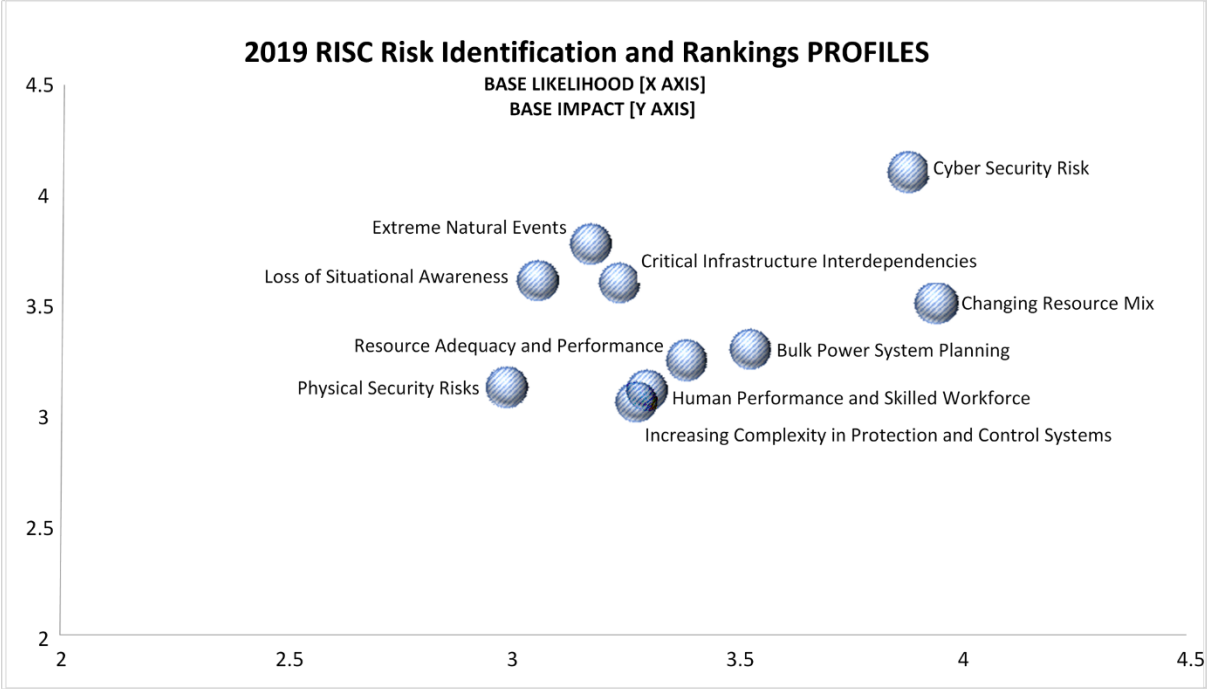


Figure 3: 2019 RISC Risk Rankings per the ERO-Wide Industry Stakeholder Survey

3.2 2020 NERC State of Reliability Report

Analyses of past bulk power system performance serves to document system adequacy and to identify performance trends. The NERC 2020 SOR Report[2] provides these detailed analyses of past performance while providing technical support for those interested in the underlying data and detailed analytics.

The SOR Report also provides objective and concise information to policymakers, industry leaders, and the NERC Board of Trustees on issues affecting the reliability, security and resilience of the North American bulk power system. Specifically, the report does the following:

- Identifies system performance trends and emerging reliability risks
- Reports on the relative health of the interconnected system
- Measures the success of mitigation activities deployed

In Figure 4, several of the data sources primarily used for the SOR Report are shown. The SOR also contains analysis and trending of primary frequency response as measured by actual frequency excursion events on the various interconnections in North America.

[2] The charts and figures in this section are pulled directly from the 2020 State of Reliability Report and used here with permission.

Transmission Availability Data System (TADS)

TADS inventory and outage data are used to study the initiating cause codes (ICCs) and sustained cause codes (SCCs) of transmission outages. Metrics are developed that analyze outage frequency, duration, causes, and many other factors related to transmission outages. This analysis can shed light on prominent and underlying causes affecting the overall performance of the BPS.

Transmission 100kV and greater

Generation Availability Data System (GADS)

GADS contains information that can be used to compute generation-related reliability measures, such as Weighted-Equivalent Forced Outage Rate (WEFOR). WEFOR is a metric measuring the probability that a unit will not be available to deliver its full capacity at any given time due to forced outages and derates. NERC's GADS maintains operating histories on more than 5,000 generating units in the North America.

Conventional Generators 20 MW and larger

Misoperation Info Data Analysis System (MIDAS)

MIDAS collects protection system relay operations and misoperations. Metrics are developed to assess protection system performance. Trends are evaluated and can be used to identify remediation techniques to reduce the rate of occurrence and severity of misoperations. Misoperations exacerbate event impacts on the BPS. The data collection is granular and allows NERC to identify specific trends associated with certain geographies, technologies, human performance, and management.

Transmission Owners, Generator Owners, Distribution Providers

The Event Analysis Management System (TEAMS)

TEAMS is used to track and process records originating from the EOP-004 reporting, OE-417 reporting, Event Analysis Process and the ERO Cause Code Assignment Process. Relevant reports are recorded, uploaded and tied together into a single event. The data in TEAMS is used to support event cause coding, general system performance analysis and key performance indicators for the bulk power system.

Balancing Authorities, Reliability Coordinators, Transmission Owner/Operators, Generation Owner/Operators, Distribution Providers

Figure 4: Data Sources used in the SOR Report

For the purposes of this RRA, the following two sections on system protection misoperations and physical security risks are included to illustrate how the entities within the MRO region are performing in aggregate as compared to other regions. Information is also provided on activities within MRO and NERC that can help reduce the risk.

NERC 2020 SOR Report: System Protection Misoperations Trending

NERC and the Regional Entities have been actively monitoring system protection misoperations across the ERO footprint by using a database called the Misoperation Information Data Analysis System (MIDAS). In the past five years, NERC and the individual Regional Entities have provided significant outreach through workshops and webinars dedicated to misoperations, specifically on how to accurately and consistently report the data into MIDAS and on ways to reduce misoperations. The five-year trending for misoperations (per Region) is shown in Figure 5.

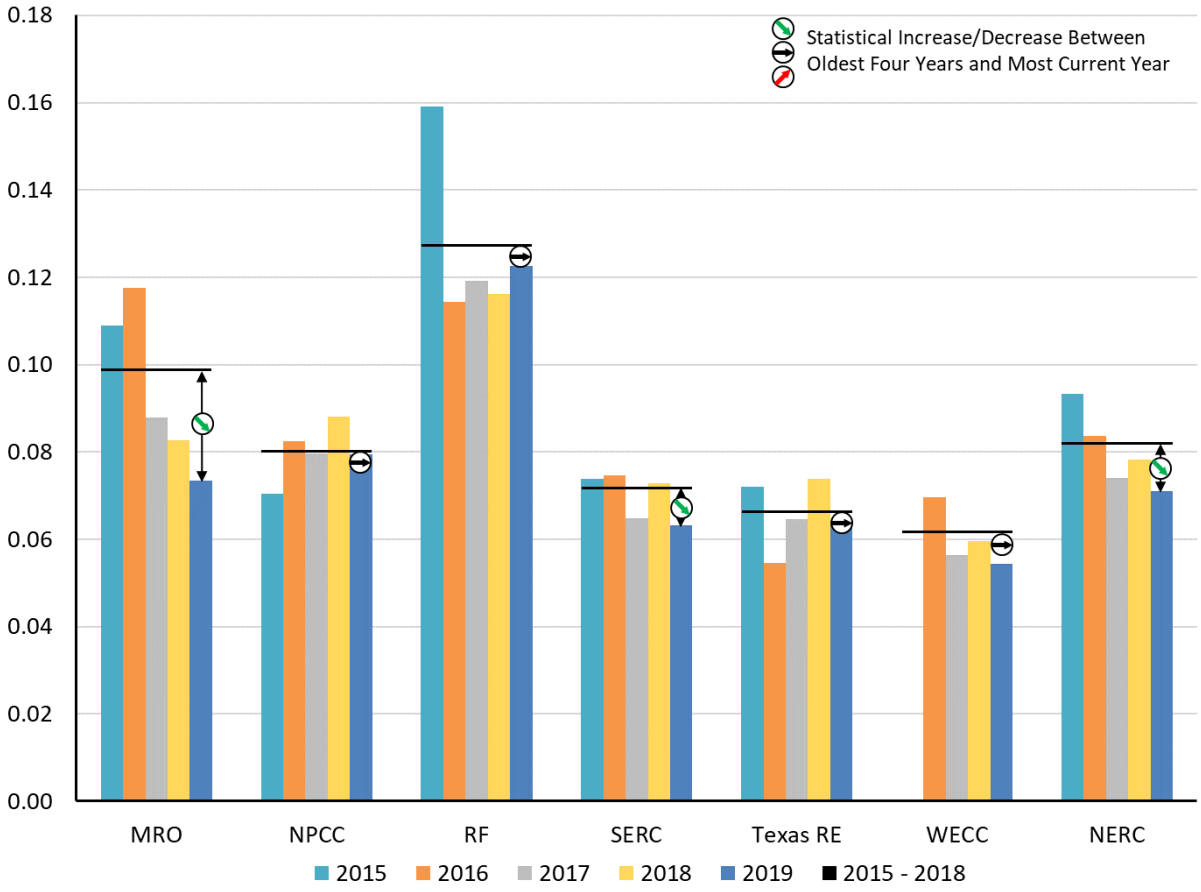


Figure 5: Year-Over-Year Changes and Trends in the Annual Misoperations Rate by Region

Figure 5 indicates that the MRO misoperations rate has been trending downward for each of the past four years, and is close to the NERC-wide misoperations rate for all Regional Entities combined. However, the MRO misoperation rate for 2020 through the first three quarters is higher than 2019, as shown in Figure 6.

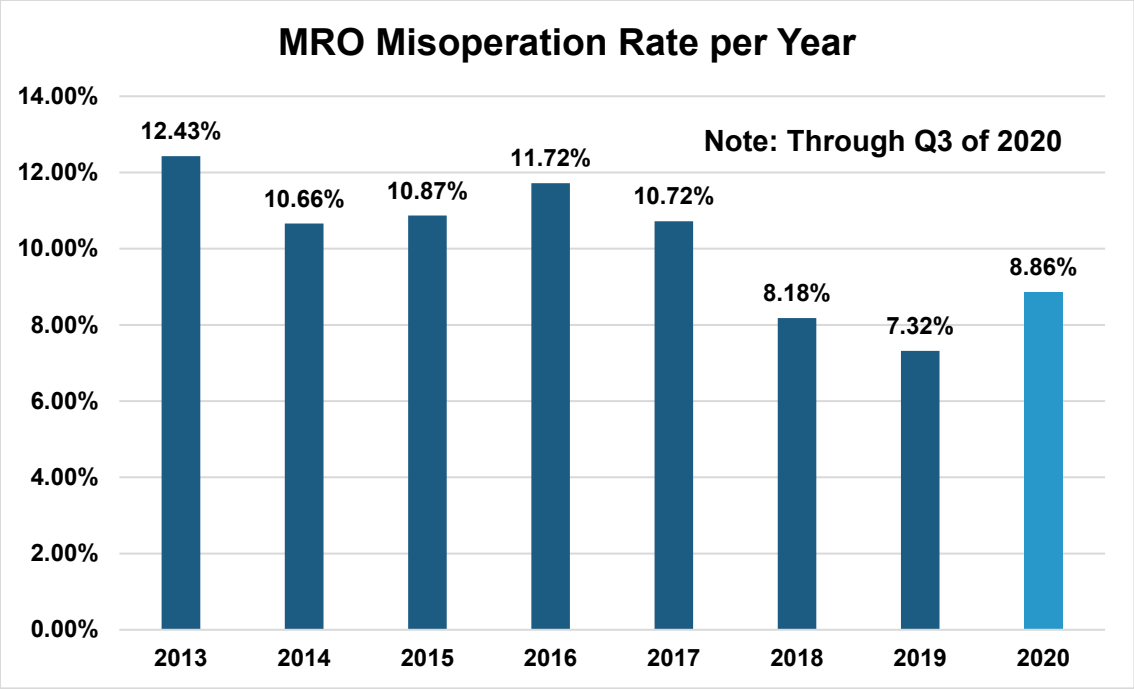


Figure 6: MRO Region Annual Misoperation Rate Through Q3 of 2020

In June 2017, the MRO Protective Relay Subgroup (PRS) authored a technical paper on how to improve the security of two high impact misoperations: breaker failure schemes and bus differential schemes. This technical paper was circulated throughout the industry and presented at several reliability conferences. This is an example of how the ERO can leverage the knowledge and expertise of its collective staff and registered entities, and then through coordinated, broad outreach, help to improve reliability of the bulk power system across North America. In July 2020, MRO conducted a webinar to reintroduce this technical paper to help entities reduce the occurrences of breaker failure schemes and bus differential misoperations, which were on the rise.

One of the risk elements identified by the MRO CMEP IP was that misoperations must be thoroughly reviewed, investigated or mitigated. This holds true for not only the registered entities that experience misoperations, but also for Regional Entity staff that have an obligation to review the MIDAS submittals within their region and assure that they are properly investigated and mitigated to prevent reoccurrence. In the MRO region, staff in conjunction with PRS members, review each misoperation that occurs to verify that it has been effectively studied and mitigated. Often times, MRO staff will contact the submitting entity for clarity on the misoperation details or to request additional information. MRO registered entities also actively share misoperation experiences at PRS meetings and often seek out technical help or alternative mitigation methods during round table discussions. The PRS will review and discuss any NERC Lessons Learned that are system protection related. This collaboration of MRO staff and members has been successful in improving the accuracy of MIDAS submittals and has helped to steadily reduce misoperation rates.

NERC 2020 SOR Report: Physical Security Risks

In 2019, as in previous years, there were no reported cyber or physical security incidents on the bulk power system that resulted in a loss of load per the 2020 NERC SOR. This is the single most important security measure as it reflects the combined efforts of industry, the ERO Enterprise, the Electricity Information Sharing and Analysis Center (E-ISAC), and government partners in successfully protecting bulk power system reliability. Nonetheless, grid security (particularly cyber security) is an area where the ERO Enterprise and industry must continually improve defenses as threats and technologies rapidly evolve. Figure 7 demonstrates the ERO-wide types of physical security incidents that are reported to E-ISAC:

Types of Physical Security Incidents Reported to the E-ISAC	
Theft	Theft incidents were predominately copper theft, but also included electronic equipment, materials, vehicles, keys, and other items. A majority of thefts took place at substations.
Intrusion	42% of intrusions took place at substations, and over half of those included break-in damage only. Fifteen incidents included tampering of some type, all of which were assessed to be mischief rather than intentional attempts to impact the BPS.
Suspicious Activity	A majority of suspicious activity reports took place at administrative buildings, such as commercial sites or office buildings, and generally included suspicious objects or packages, impersonation of company employees, social engineering attempts and a variety of unexplained behavior.
Vandalism	Most vandalism incidents in 2019 involved transmission and distribution systems, though it is worth noting that theft incidents commonly involve some measure of vandalism as well. Of note, one entity reported a series of apparently related instanced of vandalized pad-mount transformers by cutting or drilling holes into the bases of transformers leading to equipment failure and customer outages.
Surveillance	Photography and unmanned aircraft systems (UAS) accounted for a majority of surveillance incidents. UAS incidents were typically fly-overs where the UAS's intent could not be determined, discovering drones on their property or in their facility, or clearly being used to conduct surveillance. In one case, an entity reported several UASs flying in a stack formation over their property for over three hours, two nights in a row. Visually interesting sites such as generation plants, substations, administrative buildings and communication sites were popular targets of surveillance.
Threat	Threat incidents targeting specific companies or employees were mostly bomb related, from disgruntled customers or members of the public. Other threats targeting the industry in general typically came from various activist groups.
Gunfire	Gunfire incidents are primarily discovered during routine inspections or transmission line maintenance. Most incidents are assessed as accidental or non-malicious vandalism (target practice).
Sabotage	An entity characterized a series of cuts to fiber optic cables associated with a coal analyzer system as potential sabotage.
Other	Other physical security incidents included activist activity on entity properties, arson, apparent accidental crashes, and in one case, a small plane becoming entangled in power lines.

Figure 7: Types of Physical Security Incident Reports sent to E-ISAC (ERO-Wide)

Figure 8 shows the physical risks as reported to E-ISAC broken down per region. The diameter of each regional circle reflects the count of incidents reported:

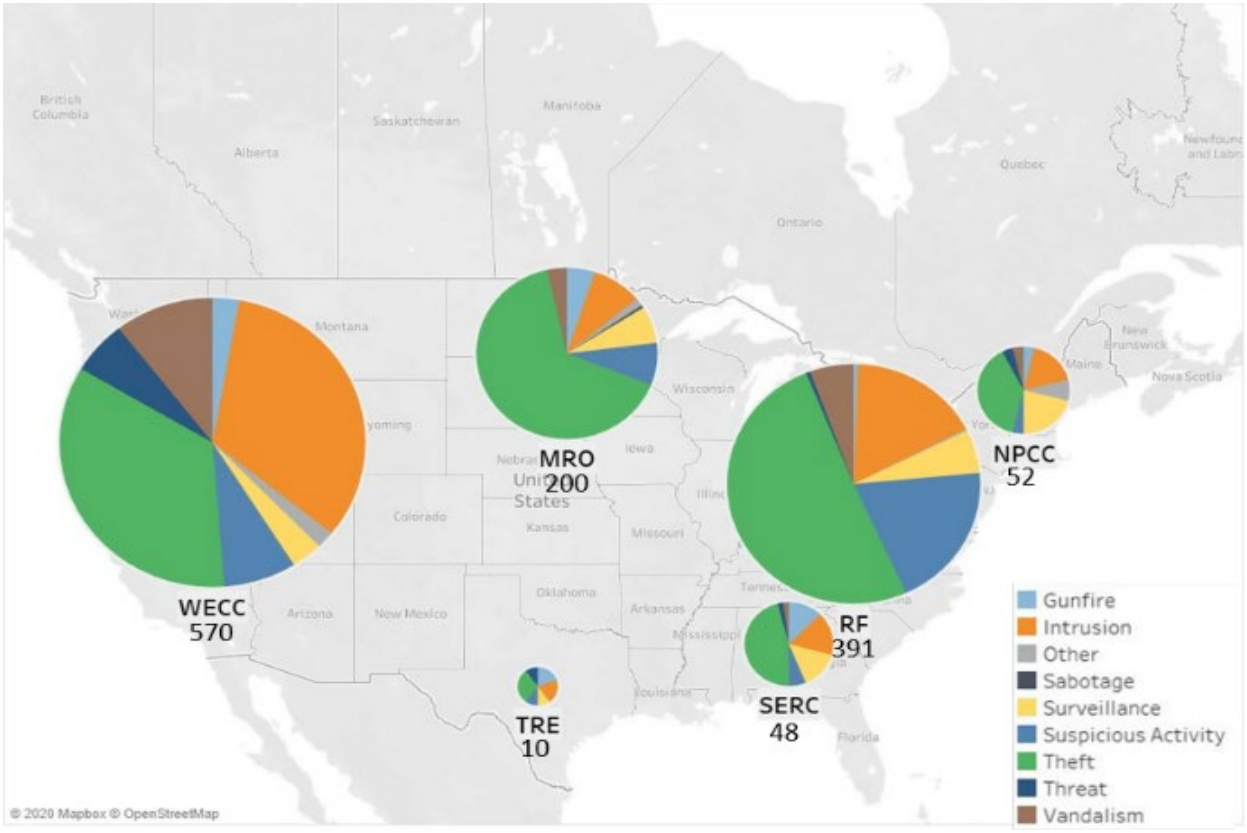


Figure 8: 2019 Physical Security Incidents by Region

3.3 2020 NERC Long-Term Reliability Assessment Report

NERC's Long Term Reliability Assessment (LTRA) Report[3] is a forward-looking report that assesses the long-term reliability (including planning reserve margins and resource adequacy) of the North American BPS while identifying trends, emerging issues, and potential risks during the upcoming 10-year assessment period. The report is not a prediction of future conditions, but rather an assessment of what changes are occurring with respect to generation and load and the availability of capacity or load modifying resources.

As identified in section 3.4.2, planning reserve margins are highly sensitive to the assumptions that are considered in the calculations. Overly optimistic assumptions can introduce risk. Retirements of conventional synchronous generation and the rapid addition of variable resources, more so in some areas than others, are altering the operating characteristics of the various interconnections.

Figure 9 shows the ERO-wide conventional generation changes from 2012 to present and projected retirements through 2030. The 10-year projected retirements are based on committed retirements known to date and are expected to increase as the time horizon progresses. Generator retirements

[3] Some of the charts and figures in this section are pulled directly from the Long-Term Reliability Assessment and are used here with permission.

have historically been understated and therefore additional retirements beyond what is shown as confirmed are to be expected and will increasingly alter the resource mix.

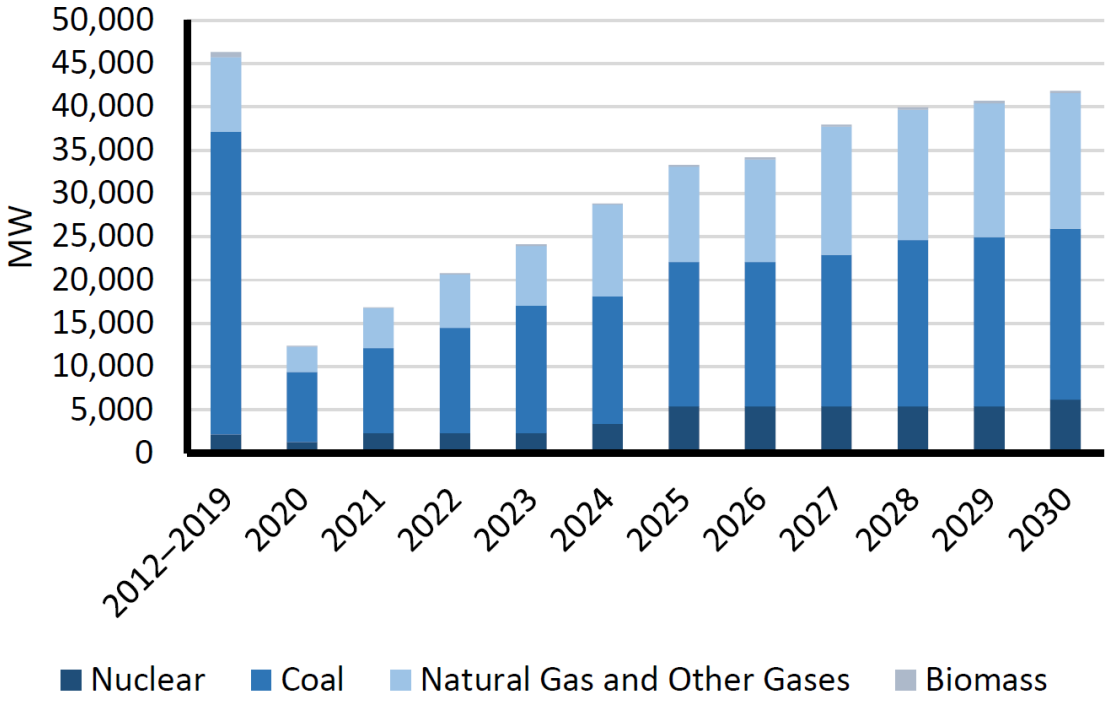


Figure 9: Capacity Retirements since 2012 and Projected Cumulative Retirements through 2030

The MRO region is highly impacted by resource changes. For example, the 10-year projection for natural gas generation in 2030 is less than the existing installed capacity. With other forms of conventional generation (nuclear/coal/oil) being retired over the next 10 years (MISO has indicated an 11.4% reduction in conventional synchronous generation by 2030; SPP is not projecting any retirements in the next 10 years), it is clear that renewable/variable generation and energy storage will likely make up the difference in future years.

MISO Conventional Generation Capacity Resources (MW)	2021	2030	% Diff:
Coal	53,771	43,966	-18.2%
Petroleum	2,737	2,507	-8.4%
Natural Gas	65,396	60,802	-7.0%
Nuclear	12,982	12,169	-6.3%
Total	**134,886**	**119,444**	**-11.4%**

Table 1: MISO Conventional Generation Capacity Projections 2021 through 2030

SPP Conventional Generation Capacity Resources (MW)	2021	2030	% Diff:
Coal	23,172	23,172	0.0%
Petroleum	1,440	1,440	0.0%
Natural Gas	29,148	29,148	0.0%
Nuclear	1,944	1,944	0.0%
Total	**55,704**	**55,704**	0.0%

Table 2: SPP Conventional Generation Capacity Projections 2021 through 2030

The interconnection queues of SPP and MISO are used to analyze future planning reserve margins. Resources within these interconnection queues are categorized into three tiers:

1. Tier 1 resources are typically in progress, funded, and are highly likely to occur.
2. Tier 2 resources are typically under study for feasibility and a fair portion of Tier 2 generation projects can materialize.
3. Tier 3 projects are typically still in the investigative stage.

Table 3 reflects the magnitude of solar and wind generation nameplate capacity in the MISO and SPP interconnection queues (Manitoba and Saskatchewan have minimal planned additions). It can be clearly seen that future generation in the Midwest interconnection queues almost entirely consist of renewables. To provide comparison with a region similar to MRO in terms of renewable generation prospects, ERCOT is also shown below. However, ERCOT expects to retain the majority of their 69 GW of conventional synchronous generation through 2030.

	Nameplate Capacity of Solar (MW)					Nameplate Capacity of Wind (MW)				
Assessment Area	**Existing**	**Tier 1**	**Tier 2**	**Tier 3**	**Total**	**Existing**	**Tier 1**	**Tier 2**	**Tier 3**	**Total**
MISO	204	1,718	49,292	7,025	**58,239**	22,062	4,119	19,281	2,921	**48,383**
Manitoba Hydro	0	0	0	0	**0**	259	0	0	0	**259**
SaskPower	0	11	10	57	**78**	242	385	0	400	**1,027**
SPP	273	284	11,103	0	**11,660**	21,892	2,646	15,641	5,253	**45,432**
ERCOT	3,249	12,738	37,031	20,990	**74,008**	24,895	12,426	10,772	8,361	**56,453**

Table 3: Solar and Wind Nameplate Capacity, Existing and Planned Additions through 2030

Table 3 provides additional evidence that the risk identified as *Changing Resource Mix* in the RISC Report has significant implications within the MRO region. The interconnection queues of MISO and SPP are predominantly filled with wind and solar interconnection requests. Any gas generation or other conventional synchronous generation in the interconnection queue that is realized will be offset by the retirements of existing/aged conventional generation. The projections for new gas generation are starting to trend downward as well. For example, the 2019 NERC LTRA showed 88 GW of gas generation in Tier 1 and Tier 2 over the 10-year period (NERC-wide); the 2020 LTRA shows about 70 GW over the next 10 yrs. It will be imperative for the two Independent System Operator/Regional Transmission Operator (ISO/RTO) within MRO to manage future generation installations with rigorous planning studies to continue to reliably serve and follow load within the Balancing Authorities (BA) to meet performance criteria.

3.4 2020 MRO Regional Risks and Rankings

The following sections summarize the regional risks identified by MRO staff in collaboration with the MRO advisory council members. Note that some risks identified in this section may apply to the Midwest portion of the continent (which is largely congruent with the MRO footprint). In some cases, the risk identified may apply to a functional entity such as an ISO/RTO, Planning Coordinator (PC), Reliability Coordinator (RC), Generator Owner/Operator (GO/GOP), or Transmission Owner/Operator (TO/TOP) that might span multiple regions.

3.4.1 MRO Physical and Cyber Security Risks

Each year, the MRO Security Advisory Council (SAC) conducts a regional security risk assessment to engage physical, cyber, and operational security subject matter experts from across the MRO region to assess the security risks most impactful to the region. The SAC conducted a survey ahead of the assessment to help identify the most prominent risks for discussion during the regional security risk assessment. MRO staff, industry security experts, and staff from the Electricity Information Sharing and Analysis Center (E-ISAC), all participated in the assessment and helped to categorize the resulting risks into three security areas: cyber, operational, and physical.

The security risks shown in Table 4 were identified through various security analysis tools used by the ERO Enterprise as risks applicable to the MRO footprint. Seven of the ten risks shown were also identified and discussed during the course of MRO's regional security risk assessment.

Security Risks
1. Adequate Security Staffing & Funding*
2. CIP Compliance Fatigue
3. Combined Cyber and Physical Attack
4. Communication (Backhaul)*
5. Drones / Unmanned Aerial Systems (UAS)*
6. Insider Threat*
7. Sabotage*
8. Supply Chain*
9. Unsupported / Legacy Devices
10. Vulnerability Management*

**Also identified in the 2020 MRO Regional Risk Assessment*

Table 4: MRO Security Risks

The following security risks were identified in the regional security risk assessment as risks that could have a medium or high level of impact on the MRO region (as depicted in the heat map following the risk section below). Additional 'lower-level' risks identified in the assessment are not reflected in this RRA.

Adequate Security Staffing & Funding

There are several Critical Infrastructure Protection (CIP) Reliability Standards in place to address operational, cyber, and physical security. However, the specific staffing structure, security budget,

and technologies used are up to each organization to define. The amount of funding and the technologies used to implement an organization's security strategy are not necessarily indicators of the organization's security strength. However, having inadequate security funding or too few trained security staff may cause operational impacts due to many factors. Some factors affecting operations include delayed implementation of security measures, inadequate security hygiene, delayed threat detection and response, inaction on threat intelligence, aging infrastructure, and compliance overhead. Security funding can also be insufficient due to limited awareness of the need by upper management.

Not providing adequate funding or staff may impact the overall security posture of the organization. Oftentimes, trained security staff are focused on compliance overhead activities, such as evidence gathering, in place of other more important security work. In addition to the need for funding to support systems and training, the competitive job market for security professionals and a lack of training programs related to cybersecurity in Operational Technology (OT) environments are a concern for MRO registered entities. Attracting talent may be difficult due to the perceived amount of compliance work involved in this industry, as further detailed in the "CIP Compliance Fatigue" risk.

To reduce these risks, consider the following:

- Increase leaders' awareness of security issues
- Cultivate a culture of security within the organization
- Grow the security workforce through training programs
- Implement effective risk identification/assessment/mitigation programs to prioritize security initiatives
- Develop compliance tools and automation
- Increase staff retention through creative HR strategies

MRO staff is considering, through the SAC, compiling a confidential baseline to benchmark entity security systems and workforce size to provide entities with more awareness of this risk.

CIP Compliance Fatigue

Similar to the risk of having adequate security staff and funding, MRO entities communicated that the amount of resources committed to CIP compliance is not a reflection of how well an organization manages its security risks. CIP standards were established in 2008, and since then, have undergone many changes. Due to the rapid advances in technologies and risk, it is difficult for the standards to remain current. One way that MRO entities have had success in managing this problem is to focus on the standard's purpose. For example, the purpose statement for the CIP-004-6 Reliability Standard is:

CIP-004-6 — Cyber Security – Personnel & Training

A. Introduction

1. **Title:** Cyber Security — Personnel & Training
2. **Number:** CIP-004-6
3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

Source: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-004-6.pdf

The CIP-004-6 purpose statement uses the language "requiring an appropriate level of personnel risk assessment." Suppose this is the focus of the organization. In that case, the "appropriate level" of a personnel risk assessment will change over time based on new threats and vulnerabilities related to who has access to the systems and the function and criticality of the systems themselves. Users with access to an organization's cloud systems and third-party access pose more significant risk now than ten years ago. Therefore, focusing on the purpose *and* the standard will help organizations better prepare their compliance programs for future changes and offset compliance fatigue.

Organizations focusing only on the standard language (instead of the risk addressed through the standard or the standard's purpose) may lose focus on why they are performing the standard's requirements. For example, extra time may be spent trying to understand how often to perform a review due to the standard's language, which may not be clear. When the focus should be on the review itself and the frequency should be based on risk if not prescribed in the standard. Some standards may be implemented with overtly manual and repetitive processes that require more time to gather evidence to demonstrate compliance, such as CIP-004, CIP-007, and CIP-010. Furthermore, sometimes these compliance areas can rely on automation, and there are no systematic manual reviews to confirm the automated controls are operating effectively.

CIP compliance fatigue leads to the possibility that a singular focus on CIP compliance (review frequency) may introduce complacency, as the emphasis is not on the risk. It may result in a false sense of security and the assumption that being compliant also means that you are secure, which might not always be the case. In addition, a focus on compliance overhead like evidence gathering may reduce resources needed for other security work. CIP compliance fatigue is increased by continually moving the goalposts (shifting regulatory landscape) that change and impact the workload. The issue is compounded if there is not adequate staff available.

To reduce this concern, consider the following:

- Standardize existing processes
- Develop functional compliance tools
- Simplify and automate a periodic manual control review
- Share best practices for compliance efficiency within your organization

Combined Cyber and Physical Attack

Combined cyber and physical attacks are of great concern to MRO registered entities. This type of event could overwhelm incident response plans and cause widespread and extended power system outages. The concern increases with a lack of coordinated and practiced combined cyber and physical incident response plans across the organization. A large portion of MRO's footprint is more rural than urban, and remote substations with limited physical security controls could be more vulnerable to this risk.

NERC's biennial grid security exercise (GridEx) provides an opportunity for entities to practice emergency response and recovery efforts as a way of mitigating this risk. GridEx is a distributed play exercise with tabletop scenarios and simulated real-world cyber and physical attacks on the electricity grid and other critical infrastructure. Numerous organizations in the MRO region participate in GridEx, and the scenarios used as part of the exercise can help prepare organizations well for this type of risk. There is a Lessons Learned Report from the most recent GridEx V LINK that addresses

the kinds of combined attacks that GridEx participants experienced. An excerpt from the report states: *"The executive tabletop played a scenario that focused on the extraordinary operational measures necessary to restore the grid in the northeast United States and southern Ontario, Canada,* ***following a severe combined cyber and physical attack*** *on the electricity and natural gas transmission systems. U.S. and Canadian chief executive officers and executives worked with government officials to establish restoration priorities, achieve unity of effort with the natural gas and telecommunications industries, and ensure proper coordination with Canadian authorities."*

In the CMEP section, "Oversight of Risks in Aggregate under Risk of Coordinated Cyber Attack on Geographically Distributed Targets (Page 43)," there are further details to elaborate on this area and the gaps that may exist in the CIP standards for this risk. To reduce the risk of a combined cyber and physical attack, entities should consider:

- Participate in GridEx and internal coordinated exercises across multiple departments with focused drills
- Enhance physical security controls (e.g., video analytics and alarms)
- Enhance and leverage security partnerships to gain threat intelligence

Communication Network (Backhaul)

A communication network (backhaul) refers to the communication network that supplies connectivity to remote systems. Attackers may target communication networks and connectivity to gain initial access to critical systems, steal credentials, or modify network traffic in real-time. MRO's risk is increased with a lack of path diversity and redundancy for critical communications, unknown or unacceptable third party communication backhaul provider availability and security, the use of shared infrastructure, and lack of security controls and incident response plans.

There is not a CIP standard that directly relates to this issue. In addition, this area can have a large impact due to the vast number of remote locations in the MRO region. To reduce this concern, consider the following:

- Increase monitoring and controls on communication backhauls
- Perform a business impact analysis on the communication network and have a service level agreement in place with communication backhaul providers
- Rely on an organization's own private communication network and provide interconnected data circuits where possible
- Perform an inventory of all external connections to prioritize projects to address the risk

Drones / Unmanned Aerial Systems (UAS)

Threat actors may use drones to conduct surveillance, gain sensitive information to plan an attack, as weapons, to carry payloads with the potential intent to harm people and industry assets, and disrupt power system operations by attacking energy facilities. MRO entities have particular concern related to inadequate laws and a lack of authority to regulate and control drone use near critical infrastructure, coupled with limited technology to detect UASs, and limited ability to respond to drones when detected (other than reporting to law enforcement), particularly in remote areas. This concern is growing as physical drone size, payload capacity, and flight time increase.

There are CIP standards in place to provide physical security. However, technology and infrastructure limits make it difficult for entities to address UASs. Therefore, the mitigations to

implement for this particular risk are up to each organization and heavily depend on resources. To reduce risk, consider:

- Develop and implement a drone policy that addresses reporting and response
- Implement a process for downed drones that are found
- Collaborate with local authorities.

Some MRO entities are also exploring the process for declaring areas around critical infrastructure as no-fly zones.

Insider Threat

Insiders pose a substantial threat to organizations with their knowledge and access to proprietary systems that allow them to bypass security measures through legitimate means. Insiders can pose both accidental/unintentional and intentional threats to organizations. This risk increases if there are inefficient processes, controls, and training for insider threats. Economic changes, political changes, and other factors may create new insider motivations to engage in malicious conduct. With more remote work, behavioral indicators of misconduct are more easily missed.

The CIP-004 Reliability Standard requires criminal background checks. However, the background check periodicity of seven years for people with access to CIP assets should be evaluated by each entity to ensure that it meets the company's risk tolerance, which may vary by asset. Other common methods of assessing personnel with critical access not required by the standards, but commonly performed, is the use of social media monitoring and online research to evaluate the risk of an insider threat. Additionally, trusted employees that may not necessarily have direct access to CIP assets, with the proper credentials and/or knowledge, could traverse corporate networks into the control center space more easily than an outsider could.

To reduce this risk, consider the following:

- Develop an insider threat program that includes a process for reviewing and responding to potential insider threats
- Conduct training on recognizing and reporting the signs of an insider threat
- Perform reoccurring background checks
- Enhance detection methods for unauthorized access and privilege escalation
- Implement access management practices, such as segregation of duties, least privilege, and the two-person rule for high-risk system actions

Sabotage

Saboteurs may disrupt operations, causing damage to assets, safety risks, and adverse financial and reputational impacts. The risk increases with insufficient situational awareness of saboteur groups and current events and corresponding response plans and training, inadequate physical access controls, remote locations with long incident response times, and new facility construction.

The attack in April 2013 to the Metcalf substation is often called an act of sabotage. It is important to note that the mitigation efforts to increase security for facilities similar to Metcalf includes the following:

> "…to enhance the security of critical substations [like Metcalf]…efforts include:

• Security guards to provide 24/7 coverage;
• Trimming back undergrowth around substations to remove potential hiding places;
• Fencing and shielding to obstruct views and protect critical substation components;
• Enhanced camera technology; and
• Increased lighting."

Source:
https://www.pge.com/en/about/newsroom/newsdetails/index.page?title=20140410_pge_announces_reward_for_information_on_metcalf_substation_attack

Because there is no CIP standard to mitigate sabotage, and considering there have been historical incidents in this sector (Metcalf) and sabotage remains a physical threat to Bulk Electric System assets, this risk has been placed in the high-risk section of the risk matrix.

The chances of a saboteur causing harm to Bulk Electric System assets are reduced when organizations adhere to the defense in depth mindset and use many controls in aggregate to mitigate the risk. Addressing the above security risks and reviewing the section below titled "Critical Infrastructure Protection Risk Considerations," will establish a complete defense in depth posture.

Supply Chain

Reliability Standard CIP-013 is specifically focused on supply chain risks and became effective in 2020. When available, the lessons learned from the 2020 supply chain compromise can be utilized by MRO entities to determine if they may be susceptible, regardless of compliance with CIP-013. The 2020 incident is described as a very large and highly impactful attack on the software supply chain. Given the breadth and impact of the event, and considering the CIP-013 standards are new, this risk has been placed in the high-risk section of the risk matrix.

Technology (hardware and software) supply chain concerns include embedded software and intentional or unintentional vulnerabilities, including hard-coded credentials, remote access backdoors, malicious code, surveillance, and data exfiltration capability that could enable an attacker to cause adverse impact on critical systems. Supply chain concerns are increased by the degree of difficulty in completing a comprehensive assessment of all components and sub-components in highly complex systems. Reliance on a single vendor to complete these assessments within an organization or across multiple organizations increases supply chain risk. The current pandemic has also increased this risk by making it more challenging to source specific equipment and increasing lead times.

There are additional areas that address supply chain risk in this report under the section titled "Critical Infrastructure Protection Risk Considerations," which includes details from page 49 of the NERC Supply Chain project titled "Project 2019-03 Cyber Security Supply Chain Risks." To reduce this risk, consider the following:

- Implement CIP-013
- Assess vendor security maturity
- Know where and how a vendor will store data
- Know the existing environment, and monitor for anomalies
- Ensure vendors have a vulnerability management program (third-party certification also provides assurance in this area)

- Seek to diversify equipment vendors and use segregated networks for critical systems
- Develop an understanding of risk tolerance as part of the supply chain process

Unsupported / Legacy Devices

Unsupported devices often have security vulnerabilities that are not addressed by the vendor. In addition, some systems were installed during a time when designing for security may not have been as heavily considered. Failure to mitigate security vulnerabilities exposes companies to potential cyber attacks that can disrupt operations, damage assets, result in financial loss and/or loss of sensitive information. Threat actors exploit known vulnerabilities on unpatched systems to gain initial access and escalate privileges. MRO entities noted particular concern with this risk due to the long-life span of equipment found on their systems. The long life span may lead to maintenance and security staff supporting a wide range of aging equipment with limited experience. In addition, MRO entities identified the need for better tracking of vendor support across asset inventories.

The CIP standards do not address legacy devices. For entities that must continue to use legacy equipment, consider the following:

- Add layers of security controls and increased monitoring to mitigate vulnerabilities
- Keep a robust asset inventory that tracks the level of support for individual assets

Vulnerability Management

Unaddressed vulnerabilities may lead to threat actors gaining initial and persistent access to critical systems. Compromised systems may lead to adverse impacts on the bulk power system.

Reliability Standard CIP-008 requires organizations to have a process to manage security incidents. The most robust security incident programs should be closely coordinated with entities' implementation efforts to support other CIP requirements, such as CIP-004, CIP-005, CIP-007, and CIP-013. MRO organizations that have more dynamic vulnerability management programs are more comfortable with their cyber resiliency. Due to the dynamic nature of vulnerabilities, there are no real protections in the CIP standards against a zero-day vulnerability. (Zero-day vulnerability describes a vulnerability that has never been seen before and for which known mitigation of a fix or software patch does not exist. Zero-days can be used to compromise a system without detection.) The section in this RRA titled "Anomalies and Events, and Mitigation" compliments this section and can be used to improve vulnerability management risk further.

This risk is aggravated by having unpatched devices exposed to the internet, having insufficiently trained security personnel to assess vulnerabilities and address them using risk-based prioritization, the rising volume of patches, and the lack of a comprehensive asset inventory. Unlike traditional IT systems, many OT systems do not have remote management and discovery features. This leads to more resources and time required to patch remote systems. The unique operational environment presents some additional challenges noted by MRO entities. These include the inability to validate patches in a test environment and vendor restrictions on third party patches. These challenges may introduce reliability risks or delay patch deployment to critical systems.

To reduce this risk, consider the following:

- Implement and resource robust vulnerability and inventory management programs to apply patches based on risk and the entity's specific environment

- Have additional layers of security controls that can mitigate the vulnerability if patching cannot be completed in a timely manner

3.4.2 MRO Operational and Planning Risks

The following operational and planning risks in Table 5 were identified through various reliability analysis tools used by the ERO Enterprise as specific risks applicable to the MRO footprint.

Operations and Planning Risks
1. Overhead Transmission Line Ratings During Cold Weather*
2. Voltage Stability and Reactive Management of the BPS*
3. Reactive Capability of Inverter Based Resources*
4. BPS Modelling Accuracy*
5. Sunset of Telecommunication Circuits*
6. Uncertainty of Planning Reserve Margins*
7. Vegetation Management of 100-200 kV Circuits
8. Cold Weather Operation of SF6 Gas Insulated Circuit Breakers
9. Wind Plant Modelling and Ride-Through Capability During Faults*
10. Misoperations Involving Directional Comparison Blocking Schemes
11. Misoperations Due to Errors Occurring During Commissioning

**Also identified in the 2020 MRO Regional Risk Assessment*

Table 5: MRO Operational and Planning Risks

Overhead Transmission Line Ratings

Since being identified in the FERC inquiry report for the January 17, 2018 cold weather event and highlighted at the FERC Transmission Line Ratings Conference on September 10-11, 2019, overhead transmission line ratings and methodologies continue to be a reliability concern for MRO.

NERC Reliability Standard FAC-008-3 focuses on assuring that overhead transmission line ratings do not exceed their most limiting thermal element, most limiting operating limit, or the protection setting to assure reliability. However, neither FAC-008-3 nor any other NERC standard/requirement necessitates that transmission line owners/operators provide normal and emergency ratings for both summer and winter seasons. Additionally, for those entities that do have seasonal ratings, there is no requirement that the owner/operator establish seasonal ratings that are reflective of temperatures that are common during high load times, when the capacity of these facilities becomes most key to reliability.FAC-008-3 is also not applicable to the Planning Coordinator (PC) and/or Reliability Coordinator (RC), and therefore these entities must use the ratings that are provided to them by the Transmission Owner/Transmission Operator (TO/TOP) for expansion planning and operating the bulk power system, with no real ability to verify the basis of the rating. Consequently, the RC and PC make real-time operating decisions, and decisions regarding future facility needs, without the ability to ensure that the true capacity of the system is accurate for these analyses.

To address this issue, on November 19, 2020, FERC approved Notice of Proposed Rulemaking (NOPR) RM-20-16-000) titled "Managing Transmission Line Ratings." It intends to require:

- The use of Ambient Adjusted Ratings (AARs), developed by TOs, and used by the Regional Transmission Organizations (RTO).
- Independent System Operators/RTOs to be able to update/accommodate its TOs' ambient adjusted ratings in EMS systems and daily operations.
- TOs to share detailed ambient adjusted ratings methodology with its RTO and Market Monitor, if applicable, for transparency and consistency.

The commission accepted industry comments on the NOPR for 60 days (until January 19, 2021). If approved, the NOPR will be implemented within one year of the final ruling for historically congested lines (defined as congested within the last five years). All other overhead transmission lines would require implementation within two years of final ruling.

Reactive Resource Management and Voltage Stability

During severe cold weather in the southern half of the U.S. on January 17, 2018, large amounts of natural gas generation became abruptly unavailable due to an inability to operate in the cold temperatures that occurred that day. The only option to continue to serve firm load was to transfer large amounts of power from the upper Midwest to the southern U.S. Large imports of power from remote areas can create a voltage stability issue that is not typically studied in the planning arena and may not be readily identified in the operation horizon. During unusually high transfer conditions, and when bulk power system voltages are declining, RCs should compare actual voltage conditions to an on-line or off-line model for that day, and perform voltage stability analysis to assure they have sufficient reactive margin to avert a voltage collapse for the next most severe single contingency. RCs should communicate with their TOPs and Generator Operators (GOPs) to use all available reactive resources proactively (early) to maintain and manage voltages levels at acceptable levels. Adjacent RCs and TOPs should jointly establish voltage stability criteria that is based on credible events when voltage stability may be at risk.

Reactive Capability of Renewable Generation

Wind and solar plants connected to the bulk power system are included in bulk power system powerflow and stability planning models. Sufficient model information needs to be provided by these generator owners to accurately model the reactive capabilities of these plants to ensure reliability going forward as more and more of these types of assets come online. For example, detailed modeling information of leading and lagging power factor capability will be needed to assure that a given transmission bus voltage schedule can be maintained under various steady state conditions. Similarly, accurately modeling the plant's dynamic reactive capability to help maintain voltage stability under various contingencies will be necessary to assure that the bulk power models are correctly reflecting the actual dynamic reactive capability of these renewable energy plants.

Accuracy of Bulk Power Models (Offline Powerflow and Short Circuit)

The PCs and Transmission Planners presently build their portions of the Eastern Interconnection (EI) powerflow and stability models, per Reliability Standard TPL-001-5. An EI-wide model is then assembled by a third party (presently the Multi-Regional Modeling Working Group, or MMWG). The integrity of the models must be maintained through these various handoffs to ultimately generate an EI model. When combined with the difficulties of accurately modeling renewable generation, the

changing characteristics of load, distributed energy resources netting with load, interchange assumptions between each modeling area, market flow assumptions, the bulk power model building process will continue to be challenging and may be subject to errors and inaccuracies. Similarly, short circuit models will need to capture and evaluate reduced short circuit strength and the lack of negative sequence current from inverter-connected generation that is becoming increasingly prevalent as these resources become more abundant. This will present increasing challenges for protection engineers to continue to provide dependable and secure protection to the bulk power system in the future, as the majority of protection systems heavily rely upon these attributes that many renewable resources do not provide, thus creating uncertainty about the ability of protection systems to accurately operate. For the reasons explained in this section and the previous risk section, MRO has ranked both the *Reactive Capability of Renewable Generation* as well as *Bulk Power Model Accuracy* as two of the higher, more impactful planning risks that exist within the MRO region.

Critical Communication Sunset (Leased Lines)

Telecommunications providers are starting to discontinue support of aging leased facilities, such as VG-36 copper four wire circuits used widely by the bulk power industry. Specifically, these telecomm facilities are often used for Supervisory Control and Data Acquisition (SCADA), metering, and Frequency Shift Key Tone circuits used for transmission protection in high-speed pilot schemes or direct transfer trip remote clearing of transformer or breaker failure schemes. Telecommunications companies are moving towards discontinuing support of telecomm repairs, parts, and personnel related to these aging facilities, posing a risk to the bulk power industry of finding a suitable replacement. Present protection systems require latency in the millisecond timeframe, while telecomm alternatives often focus on available bandwidth over latency. Further, replacement network-based telecom solutions are in some cases early in development and adoption. Telecomm facility sunset schedules can be ambiguous, with the full scope of impacted equipment uncertain. As the likelihood of telecomm facility sunsets appear to be an eventuality, risk mitigation will likely include the execution of a complex communication facility replacement project over a multi-year timeframe.

Planning Reserve Margins and DSM

The deployment of accurate and timely Demand Side Management (DSM) of sufficient amount can help RCs reconcile the uncertainty associated with seasonal planning reserve margins and help them manage real-time energy shortages within their RC footprint. In 2020, three of the four PCs/BAs within the MRO region experienced a shortage of generation capacity that resulted in either Energy Emergency Alerts (EEAs) or BA resource alerts on multiple occasions such that operating reserve requirements were being approached. This occurred during load conditions below the forecast peak levels. Part of the cause was a significant number of generation outages that were not accounted for or anticipated in the summer assessment and, at times, when wind generation was below its anticipated output level assumed in capacity planning and reserve margins. Deferred generator maintenance and supply chain issues during spring 2020 related to the pandemic may likely have also caused some forced or operational unit outages during the summer season. Note that the 2020 summer anticipated planning reserve margins for these three BAs (per the NERC Summer Reliability Assessment) were well above target reserve margin levels.

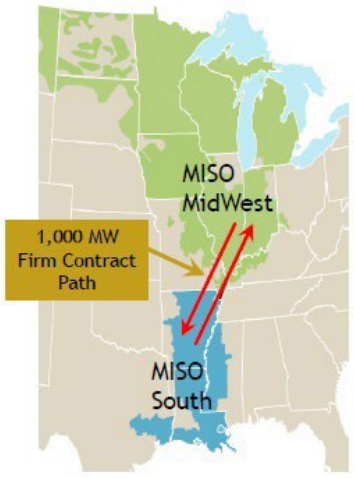


Figure 10: MISO RDT Limit

MISO: DSM within the MISO BA amounts to about 5% of total summer peak load forecast. However, most of this is confined to MISO-Midwest. Because MISO-South has limited firm deliverability from MISO-Midwest (the 1,000 MW Regional Directional Transfer (RDT) limit has been extended to 2023) and has limited import capability from SPP and SERC BAs, it continues to be at additional risk of not having sufficient capacity to serve load during severe cold weather events when unanticipated generation outages can occur. Additional DSM in MISO-South that can be deployed quickly could help to reduce the risk of firm load shed during resource capacity shortages in MISO-South. In the meantime, MISO, SPP and the other parties have enhanced the RDT operating procedures per the recommendations from the FERC and NERC 2018 inquiry report to pre-emptively manage high MISO intra-RTO transfers. Additionally, MISO and SPP have commenced with a joint transmission study that began in December 2020. The joint study is designed to identify transmission projects that will help alleviate this intra-RTO transfer limit.

SaskPower: DSM within the SaskPower BA amounts to about 1.6% of its summer peak load forecast. SaskPower also has very limited import capability from the Western Interconnection, the US, and Manitoba Hydro, and therefore largely relies on its own generation to serve load. Additional DSM in SaskPower would help reduce the risk of firm load shed during resource capacity shortages within the province.

SPP-RTO (Eastern Interconnection): DSM within the SPP BA amounts to about 1.6% of its summer peak load forecast (and 0.6% of winter peak load forecast). The majority resides in the northern portion of the RTO footprint. SPP anticipated a 32.8% planning reserve margin for summer 2020, well above the 12% target margin criteria. However, unanticipated generator outages combined with low wind output resulted in several resource alerts during 2020, even with demand below 100% forecast peak. Additional DSM within the SPP BA, particularly in the southern half of the BA where the majority of the wind generation exists, would help reduce the risk of firm load shed during resource capacity shortages within the BA.

Based on the history and monitoring of this risk, and the lack of controls that exist to assure generation is available under peak load conditions or during critical system conditions, this risk ranks as one of the higher risks in the MRO region.

Vegetation Management

Vegetation contact in the 100-200 kV voltage range occurs significantly more often per circuit than the 200 kV and above EHV voltage levels. Multiple contacts at the 100-200 kV transmission voltage level can still pose a significant risk to the bulk power system as witnessed by the cascading outage in the eastern Texas portion of MRO's footprint in August 2019. This category 2 event was the largest loss of firm load event (non-weather related) ERO-wide in 2019, with approximately 1,170 MW of firm load interrupted.

Transmission Availability Data System (TADS) data, which tracks BES forced outages and their causes, provides supporting evidence that there may be undue risk to the bulk power system due to the lack of mandatory compliance at the 100-200 kV voltage levels in NERC Standard FAC-003-4.

Figure 11 shows the NERC-wide sustained outages caused by vegetation contact, broken down by voltage level. Figure 12 shows the NERC-wide sustained outages due to all causes tracked, broken down by voltage level. Both charts reflect sustained outages collected since 2013. The following conclusions can be made from Figures 11 and 12:

- On average, the number of outages caused by vegetation (per line) is significantly higher for 100-199 kV circuits than for any voltage class that is subject to NERC Standard FAC-003-4.
- For all sustained outages (all causes combined), the frequency of outages on 100-199 kV circuits is smaller than for other voltage classes except 200-299 kV.
- Comparison of the 100-199 kV circuits (not subject to the standard) with the 200 kV and above circuits (subject to the standard) clearly shows that NERC Standard FAC-003-4 standard is effective in reducing risk to reliability, when applied.

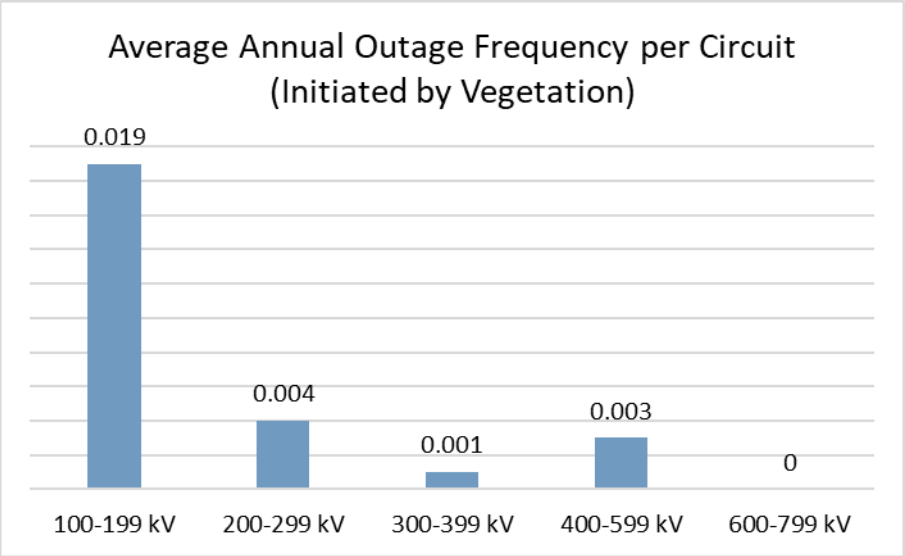


Figure 11: NERC-Wide Sustained Outages due to Vegetation Contact (per Voltage Level)

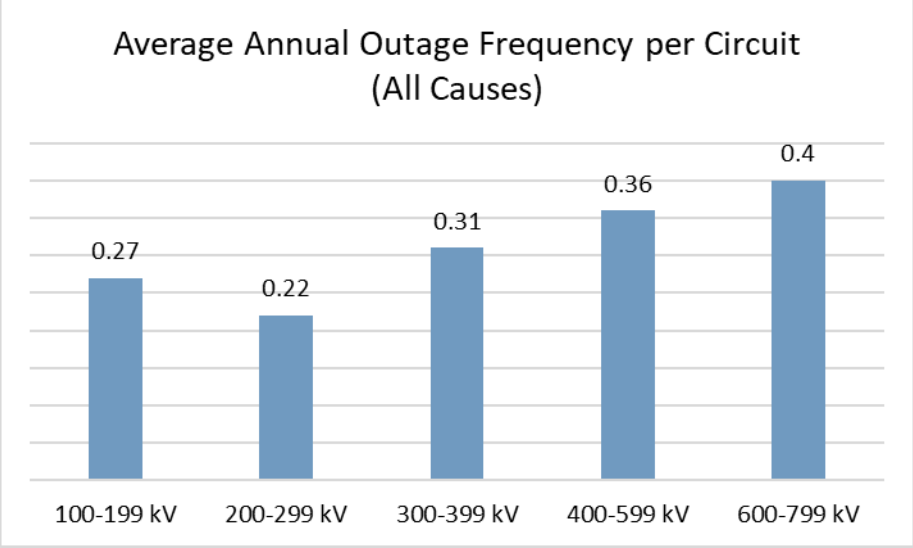


Figure 12: NERC-Wide Sustained Outages due to all Causes (per Voltage Level)

The ERO regions RF, SERC and WECC have identified vegetation management as a serious risk to their regions as well in their regional risk assessments.

Cold Weather Limits of SF_6 Substation Equipment

As discussed in the MRO 2020 RRA, a severe cold weather event hit the upper Midwest on January 29-30, 2019. Not only did many wind plants throughout the upper Midwest hit their cold weather temperature limits and automatically shut down, but many SF_6 insulated circuit breakers also hit their critical low pressure alarms due to the condensing of the SF_6 within the circuit breaker. Because the full interrupting capability of SF_6 circuit breakers is compromised when they reach critical low pressure, they are designed to either auto-open or block their trip and rely on adjacent breakers to open to clear a fault. MRO staff sent out a data query to the TOs in the upper Midwest to gather information on this event. It was determined that SF_6 circuit breakers heavily rely on their tank heaters during severe cold weather to avoid hitting critical pressure. It was also identified that the best way to assure tank heaters are operating is with pre-season inspections and to also send an alarm to the control center if/when a tank heater fails (for operational awareness). This effort led to a NERC Lesson Learned being developed and issued to industry. It provided recommendations on how TOs that can experience severe cold weather can be best prepared going into the winter season. It also emphasizes that updates to RTCA files in the EMS models can be necessary if/when a circuit breaker has blocked its trip function (effectively placing the system in breaker failure clearing mode) to accurately reflect the impact and severity of that contingency.

Wind Plant Modeling and Ride-Through Capability

Figure 13 shows the MW of nameplate capacity of wind plant installations per state throughout the U.S. Of the six ERO regions, the MRO region has the most wind plant installed capacity, about 44,800 MW, or 40% of the U.S. total. A recent NERC/FERC/WECC report on the bulk power system modeling practices of wind and solar plants throughout WECC has shown there are deficiencies in accurately representing renewable generation in the Western Interconnection bulk power models. The report identified and recommended a number of steps that should be taken to improve the modeling of this inverter connected generation in the bulk power system powerflow and dynamics models. The accuracy of the modeling of these wind plants is unknown to MRO, as well as the wind plant settings for voltage ride through capability.

Due to the magnitude of wind generation in the MRO region, and the uncertainties regarding modeling accuracy and ride through capabilities, MRO is planning to initiate a project to work with NERC and the MRO PCs to verify the accuracy of the wind plant modeling in PSS/e with the wind plant owners. MRO staff has identified this risk as being one of the higher operations and planning risks within MRO.

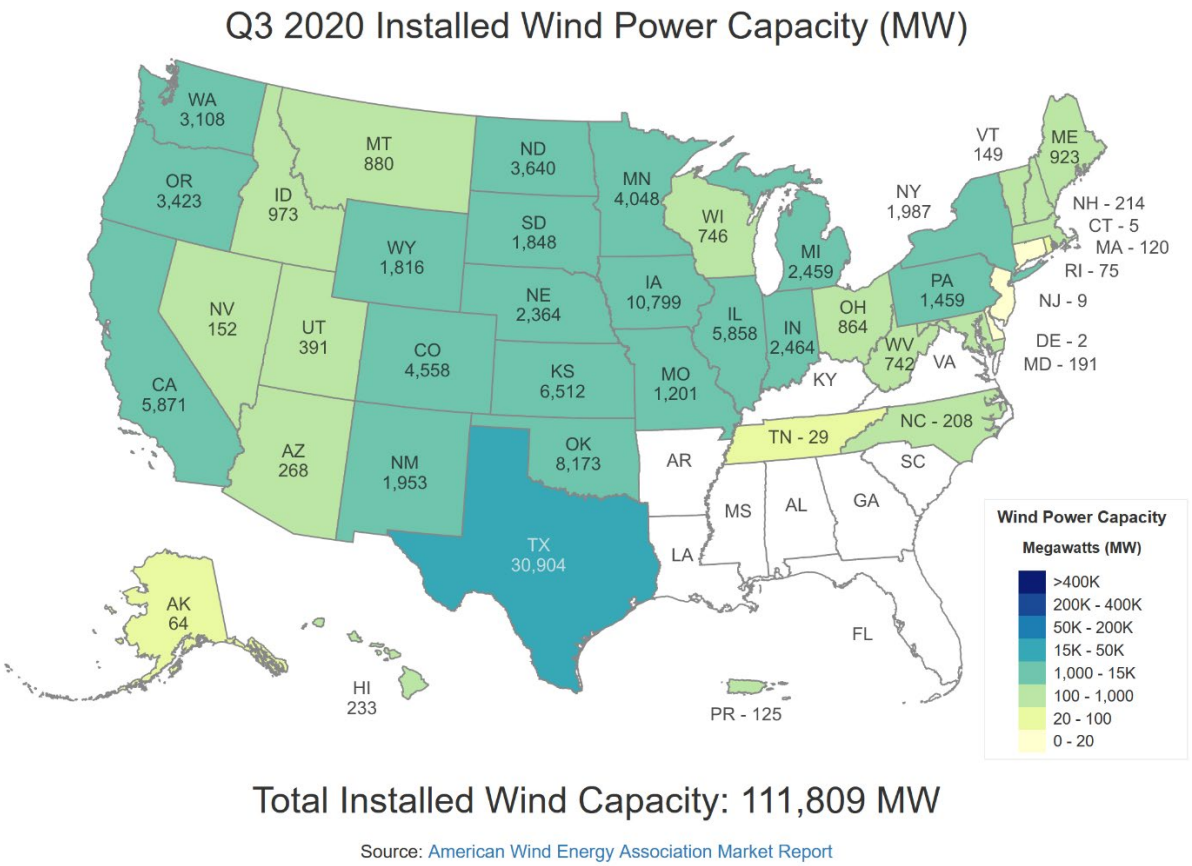


Figure 13: Nameplate Wind Capacity- Approximately 44,800 MW within MRO Footprint

Misoperations associated with DCB Schemes

Directional Comparison Blocking (DCB) schemes are a prevalent system protection scheme used within the MRO footprint. DCB schemes make up approximately 22% of the high-speed transmission line communication assisted schemes within MRO. However, since 2018, DCB schemes have comprised about 63% of high-speed transmission line communication assisted misoperations in the footprint. Although DCB scheme misoperations are typically not as high impact as breaker failure misoperations or bus differential misoperations, they are numerous and many could have been prevented. MRO continues to work with the entities and provide outreach on this topic, including the MRO PRS white paper on how to reduce misoperations associated with DCB schemes.

Misoperations Due to Errors Occurring during Commissioning

As system protection misoperations are reported into the TADS and MIDAS databases, trending results show that human errors are occurring during commissioning that result in latent risk on the bulk power system. The ERO and FERC have launched an effort to visit with industry to help identify this risk and develop findings and recommendations that will help entities mitigate errors that are occurring during commissioning. The results of this joint FERC/ERO report will be presented to MRO stakeholders during a webinar in early 2021.

Since misoperations caused by commissioning errors can have a higher impact on the BPS than other types of misoperations, and due to the lack of controls to help mitigate this risk (there presently is no NERC Standard that addresses commissioning of equipment), MRO considers this risk to be one of the higher operational risks within the ERO.

3.4.3 MRO Regional Risk Rankings

In 2019, the MRO Reliability Advisory Council (RAC) developed a reliability risk matrix to provide a relative ranking of the various risks that are identified by MRO. The relative rank of each risk (location on the matrix) would be the result of assessing the likelihood and impact of each risk. Each risk is assessed by evaluating three criteria:

- History- Are there any documented occurrences of the risk?
- Monitoring- Are the occurrences (or is the likelyhood of occurrence) increasing?
- Controls- Is a NERC standard in place to effectively mitigate the risk?

The risk matrix was then shared with the Security Advisory Council (SAC) to assure that it could be used to also address security risks that are annually identified by the SAC. The goal was to be able to assess both reliability and security risks on the same platform, as best as possible. If controls are not in place or are not effective, then a controls gap exists and MRO can then identify ways to help reduce the risk through stronger controls, outreach efforts, and increased situational awareness.

As a part of the preparation work for this 2021 RRA, MRO staff reviewed the annual risk assessments of several other regional entities, who are also ranking risks by using a risk matrix, often referred to as a heat chart. In particular, ReliabilityFirst (RF) has implemented a unique method for this, leading to collaboration between RF and MRO on developing a process that could be deployed more broadly. MRO staff recently presented the MRO risk matrix to the ERO Operations Leadership Team (OLT), which includes executive staff from all six of the NERC regions, which has begun discussions of creating a risk ranking matrix that could be used uniformly across the ERO Enterprise. This idea will continue to be explored further in 2021.

MRO staff applied the reliability risk matrix shown in Figure 14, to each of the operations, planning and security risks identified in sections 3.4.1 and 3.4.2 of this RRA, to produce a heat chart with relative rankings of each risk. The goal was to identify the highest risks, communicate the findings to industry through outreach, and ultimately work with NERC and industry to develop mitigation strategies by improving the effectiveness of controls where possible.

Reliability Risk Matrix						
Consequence/Impact (C)		Likelihood (L)				
		L1	L2	L3	L4	L5
		Very Unlikely	Unlikely	Possible	Likely	Almost Certain
C5	Severe	Medium	High	High	Very High	Very High
C4	Major	Medium	Medium	High	High	Very High
C3	Moderate	Low	Medium	High	High	High
C2	Minor	Low	Low	Medium	Medium	High
C1	Negligible	Low	Low	Low	Medium	Medium

Consequence/Impact – What could go wrong? How could it effect the BPS Reliability?	
Severe (C5)	Impacts may have widespread effects to the BPS across North America.
Major (C4)	Impacts may have widespread effects to the MRO footprint.
Moderate (C3)	Impacts may have widespread effects to portions of the MRO footprint.
Minor (C2)	Impacts may have effects on the local entity.
Negligible (C1)	Impacts may have small or non-existent effects in nature.
Likelihood – What is the reasonable probability that consequences will occur?	
Almost Certain (L5)	Control – No NERC reliability standards in place for mitigation. Monitoring – Increasing trends have been identified. History – Documented events or widely publicized exploits have been recorded.
Likely (L4)	Control – No NERC reliability standards in place for mitigation. Monitoring – Some trends have been identified. History – Documented events or generally publicized exploits have been recorded.
Possible (L3)	Control – NERC reliability standards in place for limited mitigation. Monitoring – Some trends have been identified. History – No documented events or moderately publicized exploits have been recorded.
Unlikely (L2)	Control – NERC reliability standards are in place for mitigation. Monitoring – Some trends have been identified. History – No documented events or minimally publicized exploits have been recorded.
Very Unlikely (L1)	Control – NERC reliability standards are in place for mitigation. Monitoring – No known trends identified. History – No documented events or no publicized exploits have been recorded.

Figure 14: MRO Regional Reliability Risk Matrix

Figure 15 shows the security risk rankings after applying the MRO risk matrix:

MRO Reliability Risk Matrix - Physical and Cyber Security Risks						
Consequence/ Impact (C) to the BPS		Likelihood of Occurring (L)				
		L1	L2	L3	L4	L5
		Very Unlikely	Unlikely	Possible	Likely	Almost Certain
C5	Severe					
C4	Major		3	8		
C3	Moderate		10	6, 4, 7		
C2	Minor			1, 2, 9		
C1	Negligible				5	

	Physical and Cyber Security Risks
1	Adequate Security Staffing & Funding
2	CIP Standard Compliance Fatigue
3	Combined Cyber and Physical Attack
4	Communication Network (Backhaul)
5	Drones / Unmanned Aerial Systems (UAS)
6	Insider Threat
7	Sabotage
8	Supply Chain
9	Unsupported/Legacy Devices
10	Vulnerability Management

Figure 15: MRO Physical and Cyber Security Risk Rankings

The four risks in the orange section of the security risk heat chart have been identified as having the highest relative risk and are:

- Supply Chain
- Insider Threat
- Communication Network Backhaul
- Sabotage

The Operations and Planning risk rankings are show in the next heat chart, Figure 16.

MRO Reliability Risk Matrix- Operations and Planning Risks						
Consequence/ Impact (C) to the BPS		Likelihood of Occurring (L)				
		L1	L2	L3	L4	L5
		Very Unlikely	Unlikely	Possible	Likely	Almost Certain
C5	Severe					
C4	Major			6		
C3	Moderate		2	3, 4, 9	11	
C2	Minor			1	5, 7, 8, 10	
C1	Negligible					

	Operations and Planning Risks
1	Overhead Transmission Line Ratings During Cold Weather
2	Voltage Stability and Reactive Management of the BPS
3	Reactive Capability of Inverter Based Resources
4	BPS Modelling Accuracy
5	Sunset of Telecommunication Circuits
6	Uncertainty of Planning Reserve Margins
7	Vegetation Management of 100-200 kV Circuits
8	Cold Weather Operation of SF6 Gas Insulated Circuit Breakers
9	Wind Plant Modelling and Ride-Through Capability During Faults
10	Misoperations Involving Directional Comparison Blocking Schemes
11	Misoperations Due to Errors Occurring During Commissioning

Figure 16: MRO Operational and Planning Risk Rankings

The five risks in the orange region of the Operations and Planning heat chart have been identified as having the highest relative risk and are:

- Reactive Capability of Inverter Based Resources
- BPS Modelling Accuracy
- Uncertainty of Planning Reserve Margins
- Wind Plant Modelling and Ride-Through Capability During Faults
- Misoperations Due to Errors Occurring During Commissioning

Finally, the combined set of Security and Operations and Planning risks are shown in the Figure 17 heat chart.

MRO Reliability Risk Matrix – Operations and Planning Risks + Physical and Cyber Security Risks						
Consequence/ Impact (C) to the BPS		Likelihood of Occurring (L)				
		L1	L2	L3	L4	L5
		Very Unlikely	Unlikely	Possible	Likely	Almost Certain
C5	Severe					
C4	Major		3	6 8		
C3	Moderate		2 10	3, 4, 9 6, 4, 7	11	
C2	Minor			1 1, 2, 9	5, 7, 8, 10	
C1	Negligible				5	

Figure 17: MRO Combined Security and Operations/Planning Risk Rankings

The nine risks shown in the orange cells of Figure 16 above will be included in a mitigation action plan that will help improve the controls, and increase the awareness of these risks within MRO.

4. EMERGING TRENDS THAT CAN HELP MANAGE RESOURCE TRANSFORMATION

4.1 Hybrid Facilities

As Lithium Ion battery technology and other energy storage technology matures and related capital costs decline, these storage technologies will be combined with renewable resources to form hybrid resources. When the energy output of a renewable resource can be directed to the grid or to charging batteries located right at the renewable facility, it provides operating flexibility to the bulk power system and can increase resource availability during times of low wind speeds (or nights for solar plants). Battery storage also has the capability to provide essential reliability services (ERS) to the bulk power system, such as voltage support, frequency response, and system inertia, allowing for battery storage to help replace the ERS that synchronous resources typically provide. Ultimately, the storage of variable resources is a necessity to maintain reliability and operating flexibility of the bulk power system and it will help facilitate better management of the increasing penetration of renewable energy. Hybrid resources have started to populate the interconnection queues. Figure 18 shows the MW amount of hybrid resources entered into the interconnection queues NERC-wide.

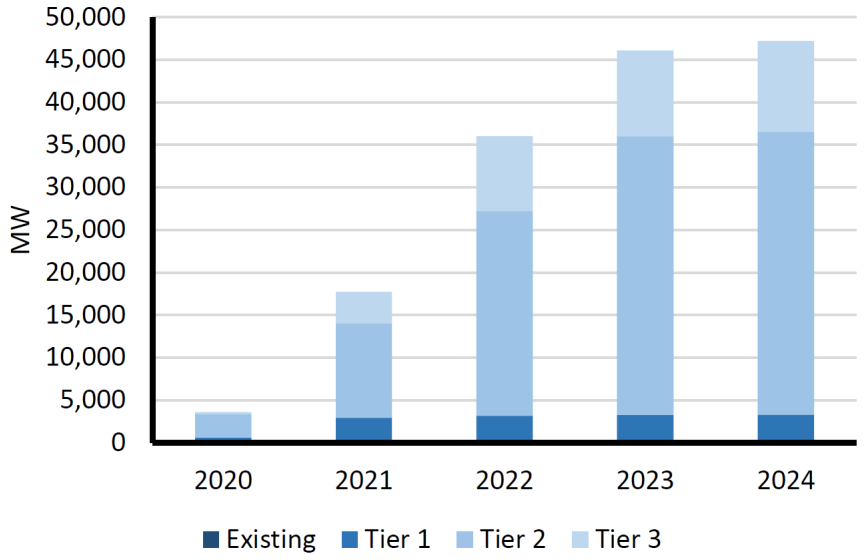


Figure 18: NERC-Wide Hybrid Resources in Generation Queues

4.2 Storage as a Transmission Only Asset

As Lithium Ion battery and other energy storage technology matures and related capital costs decline, these storage technologies are quickly becoming a viable choice for use as a transmission asset on the bulk power system. From a performance standpoint, they are very flexible, very fast, and often can be installed more quickly and economically than traditional wire reinforcements and with fewer issues related to permitting and easements that new overhead transmission lines often have.

The primary use of storage as a Transmission Only Asset is to mitigate transmission performance issues. An RTO like MISO or SPP would have functional control of the site to address transmission

issues, similar to any other transmission asset. Per an operating guide developed for each Storage as Transmission Only Asset specifying operating practices consistent with what was shown as needed in the RTO's regional transmission planning process, the storage owner would coordinate with and follow the RTO's instructions on state of charge and operating the site. MRO believes this will bring increased reliability to the bulk power system because transmission issues can be addressed quickly and economically with storage when it is the right application for a given scenario.

4.3 Participation of Aggregated DER in RTO Markets

On September 17, 2020, FERC issued a final rule (Order 2222) that will require RTOs to revise their tariffs to facilitate the participation of distributed energy resource (DER) aggregations in organized wholesale electric markets. When resource assets such as aggregated DER don't participate in the day-ahead and real-time market, an RTO has no direct mechanism to monitor the performance, scheduling, or capabilities of these resources or their effect on transmission system flows. Today's DER nets with the load and blurs the utility's and RTO's ability to accurately forecast actual load. FERC Order 2222 will help separate aggregated DER from the load, and therefore improve future load forecasting. This will ultimately be incorporated into the bulk power planning models and improve the accuracy of offline planning models as well. Since most existing DER is solar generation, an RTO will also be better positioned to forecast the impacts of changing weather patterns with DER explicitly participating in the day-ahead and real-time markets.

Acquiring the visibility of aggregated DERs will require developing new methods of communication across the transmission/distribution boundary. Some utilities promote DER in the form of solar gardens. This allows distribution customers to purchase a portion of a community solar garden site (typically between 1-5 MW aggregate), as compared to installing them on their own roof or property. This physical aggregation of DER allows the local utility to efficiently and cost effectively provide the real-time data to the RTO. In the near future aggregated DER will also include Load Modifying Resources, such as electric vehicle charging. This will further provide the RTO with operational flexibility to manage real-time operations.

MISO is proactively collaborating with its states and members to prepare for FERC Order 2222. The MISO document titled *MISO and DER: Ensuring Grid Reliability Through Visability and Communication* provides a comprehensive discussion on the efforts to prepare for Order 2222.

5. MEASURING RESILIENCY OF THE BULK POWER SYSTEM

The definition of resilience is the ability to recover quickly or "bounce back" from a disruption or disturbance. The term "recover" can mean that the system or item may be responding to a disturbance during, or after, the disturbance or event. The term "quickly" means that the system or item must be designed/planned/prepared in advance of the disturbance or event to carry out the recovery in an efficient and timely manner. In the electric industry, the response time may therefore be in terms of cycles to seconds for real-time disturbances, or it may mean days to weeks to months in the case of widespread or catastrophic system disruption or damage.

The National Infrastructure Advisory Council (NIAC) defines infrastructure resilience as the ability to reduce the magnitude and/or duration of disruptive events. The NIAC framework for resilience is built on four areas:

1. Robustness - to absorb shocks and continue operating
2. Resourcefulness - to detect and manage a crisis as it unfolds
3. Rapid Recovery - to get services back as quickly as possible in a coordinated and controlled manner
4. Adaptability - to incorporate lessons learned from past events to improve resilience

Figure 19: Infrastructure Resilience Framework (EIA Energy Conference)

So how does the electric industry today prepare in advance of an event to be resilient and respond quickly? One example of high resilience today would be how utilities respond to severe weather events. Reciprocity agreements between utilities, sharing of crews, trucks and equipment across companies, maintaining spare equipment inventory, effective communications, all have proven to be highly effective at efficiently, safely and rapidly restoring/rebuilding facilities and restoring system load.

Because severe weather events can be high impact and are often high probability events that occur multiple times per year, the electric industry has had many years of experience learning how to be resilient after severe weather damage. However, there are several high impact/lower probability events that this industry faces today that also require resilience. Some examples of these lower likelihood events are geomagnetic disturbances (GMD), electromagnetic pulses (EMP), physical and/or cyber attacks, and natural gas disruptions.

These and other low probability events are being carefully studied by NERC and the industry to gauge potential impact to reliability and to identify ways to proactively mitigate/reduce the impact,

assure a quick response to such an event, and restore bulk power system reliability as expeditiously as possible. The careful analyses and preparation in advance of a high-impact low probability event on the bulk power system will serve to increase the resiliency of the bulk power system by effecting quicker restoration of the load it serves.

5.1 NERC Event Severity Risk Index to Measure Resiliency

In each annual NERC State of Reliability Report (SOR), the top ten highest impact events are determined by calculating the event Severity Risk Index, or eSRI. The eSRI is determined by combining the weighted transmission outages caused by the event, the weighted generation outages caused by the event, and the weighted firm load loss caused by the loss of the bulk power system source during the event. Table 6 is from the 2020 SOR Report and lists the ten most severe events in the past five years based on eSRI value. It can also be seen that eight of the ten worst events were severe weather-related, verifying that severe weather events are high-impact, high probability events. Hurricane Florence on September 14, 2018, was the highest impact event in the past five years with an event SRI of 4.34. Note that the transmission, generation, and firm load loss components have values of 1.34, 0.47, and 2.53, respectively.

Top 10 SRI Days 2015–2019 NERC-Wide							
Rank	Date	NERC SRI and Weighted Components				Event Type	Region(s)
		SRI	Weighted Generation	Weighted Transmission	Weighted Load Loss	(*Weather Influenced)	
1	9/14/2018	4.34	1.34	0.47	2.53	Hurricane Florence*	SERC
2	3/2/2018	4.22	0.90	0.42	2.90	Winter Storm Riley*	NPCC
3	1/2/2018	4.06	3.81	0.16	0.10	Winter Storm Grayson*	SERC, RF, MRO, NPCC, Texas RE
4	11/15/2018	4.05	1.84	0.26	1.95	Winter Storm Avery*	RF, NPCC
5	1/8/2015	3.86	3.33	0.23	0.30	Winter Storm Juno*	SERC, NPCC
6	11/17/2015	3.85	1.03	1.02	1.80	Weather Conditions across Northwest*	WECC
7	10/11/2018	3.71	0.98	0.54	2.19	Hurricane Michael*	SERC
8	5/1/2017	3.61	1.76	0.32	1.53	Coincidental Generator Outages	SERC, RF
9	9/11/2017	3.55	1.61	1.74	0.20	Hurricane Irma*	SERC
10	6/20/2016	3.49	1.86	0.29	1.35	Coincidental Generator Outages	WECC, RF, SERC, MRO

Table 6: Top Ten Event Severity Risk Indices for Past Five Years

It takes considerable time and effort to identify and aggregate the transmission, generation, and firm load loss data associated with a specific event. For example, the NERC Transmission Availability Database (TADs) can be used to acquire the transmission outages associated with a weather related event. Similarly, the Generation Availability Database (GADs) can be used for generation

outages. Depending on the event type, firm load loss is obtained from an event analysis report (if it exists) or from customer outage information that can be used as a proxy for MW of firm load loss.

To gauge the resiliency of the bulk power system during Hurricane Florence, we can look at the transmission component as an example. In Figure 20, transmission outage data are aggregated and graphed using the start time of each circuit lockout and the end time of each circuit outage. As time progresses, the total # of circuit outages is compared to the # of circuits restored. There are two parts to evaluating the resiliency of the system to this event:

- Did the total number of transmission outages exceed expected performance and design criteria, for the severity of the event?
- Was transmission restoration timely for the conditions at hand, after assessing the magnitude of damage that occurred?

It can be seen that assessing bulk power system resiliency and determining its adequacy by using the magnitude of and restoration times of transmission outages, generation outages, and firm load loss (due to the loss of bulk power supply, excluding distribution facility outages) will be challenging.

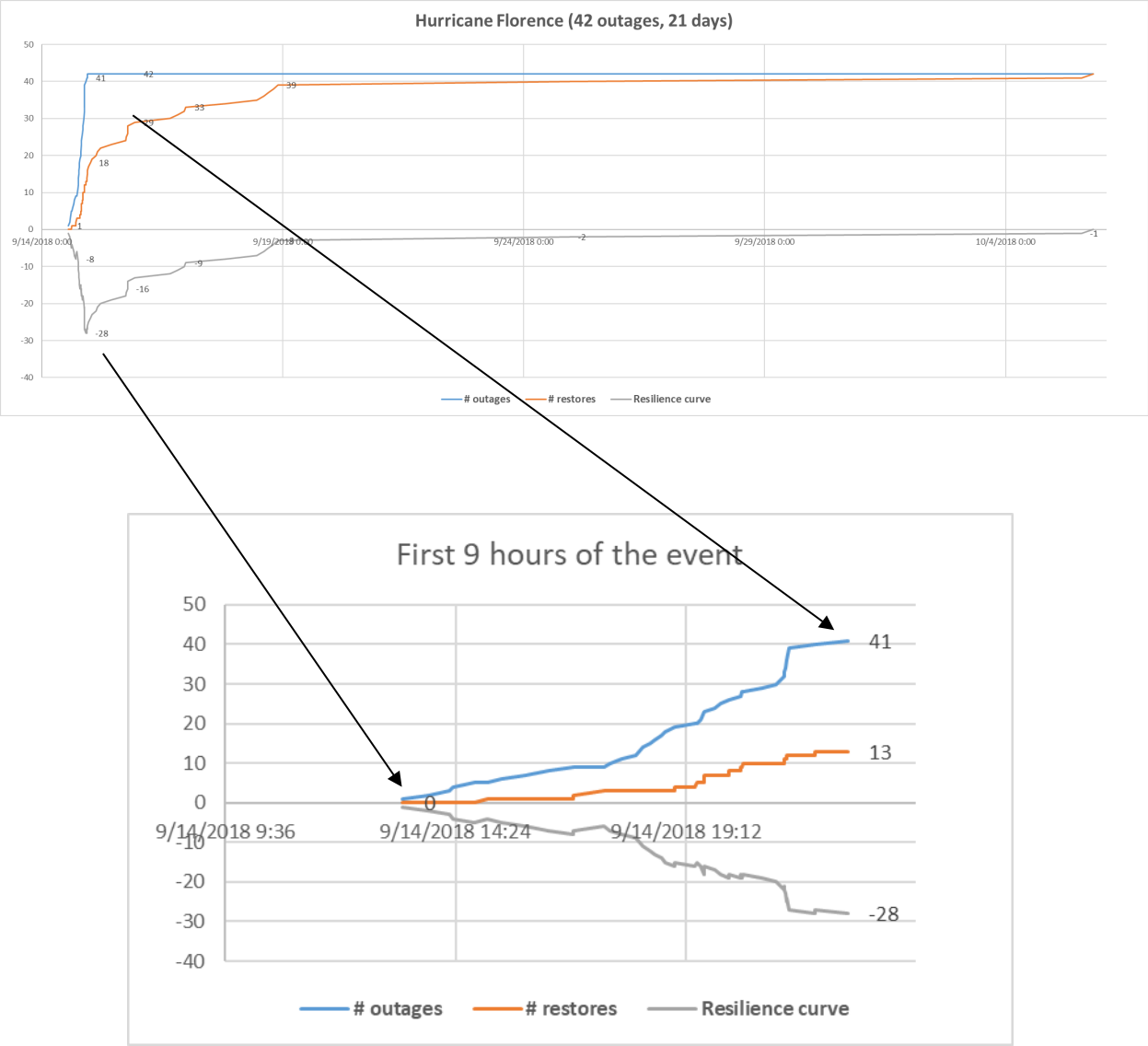


Figure 20: Transmission Resilience During Hurricane Florence

6. 2021 ERO CMEP IMPLEMENTATION PLAN

6.1 Pandemic Effects on CMEP Activities

In March 2020, in response to the coronavirus pandemic, the ERO Enterprise postponed on-site audits and other on-site activities. The ERO Enterprise will continue to defer on-site activities through at the least the second quarter of 2021 to allow registered entities to continue to focus resources on keeping workforces safe and the lights on. Since March 2020, the ERO Enterprise has coordinated with registered entities on remote compliance monitoring and certification activities enabled by video technology and virtual meeting platforms.

In May 2020, the ERO Enterprise released guidance[4] that provided additional regulatory relief related to registered entities' coronavirus response and temporarily expanded the Self-Logging Program. Due to the ongoing pandemic, the ERO Enterprise extended this expansion through December 31, 2020, to allow all registered entities to self-log instances of potential noncompliance with minimal or moderate risk related to their coronavirus response.

During 2021, the ERO Enterprise recognizes the importance of prioritizing the health and safety of personnel and the continued reliability and security of the bulk power system, and will evaluate the circumstances to determine the need for additional guidance or extensions. When conditions allow, the ERO Enterprise will prioritize monitoring activities and risks that benefit the most from on-site components, including some on-site activities deferred from 2020

6.2 2021 ERO Risk Elements

As part of its 2021 CMEP IP (CMEP) Implementation Plan (IP), the ERO establishes Risk Elements that it uses to identify and prioritize interconnection and continent-wide risks to the reliability and security of the bulk power system. The ERO Risk Elements establish a continent-wide risk baseline, and the risks discussed in this RRA may further refine MRO's compliance monitoring and oversight activities. When risks are identified in the MRO region that may have an impact at the ERO level, the RRA is the conduit to provide this risk feedback through the annual CMEP Implementation Plan development process. While MRO will determine individual monitoring decisions for each registered entity based on its unique characteristics, registered entities should consider the Risk Elements identified in the 2021 CMEP IP and the associated areas of focus, as well as specific regional risks identified in the RRA, in the evaluation of opportunities to prioritize and enhance internal controls and compliance operations focus.

For 2021, the ERO Risk Elements provide more focus on supply chain and on the prevention of misoperations. The 2020 and 2021 ERO Risk Elements are show in Table 7.

[4] https://www.nerc.com/news/Pages/ERO-Enterprise-Releases-New-Guidance-Temporarily-Expanding-Self-Logging-Program-Due-to-Coronavirus-Impacts.aspx

Comparison of 2020 Risk Elements and 2021 Risk Elements	
2020 Risk Elements	**2021 Risk Elements**
Management of Access and Access Controls	Remote Connectivity and Supply Chain
Insufficient Long-Term and Operations Planning Due to Inadequate Models	Poor Quality Models Impacting Planning and Operations
Loss of Major Transmission Equipment with Extended Lead Times	Loss of Major Transmission Equipment with Extended Lead Times
Inadequate Real-time Analysis During Tool and Data Outages	Inadequate Real-time Analysis During Tool and Data Outages
Improper Determination of Misoperations	Determination and Prevention of Misoperations
Gaps in Program Execution	Gaps in Program Execution
Texas RE: Resource Adequacy	

Table 7: Comparison of CMEP Risk Elements, 2020 vs. 2021

6.3 Requirements with High Risk Violations

In order to evaluate progress toward a key reliability goal of less severe instances of noncompliance, MRO developed the Compliance Severity Index (CSI) to represent the total risk that all instances of noncompliance present to the reliability and security of the bulk power system in the MRO region. MRO Risk Assessment and Mitigation staff undertake a rigorous process to evaluate each instance of noncompliance, based upon an analysis of the facts and circumstances, to determine the potential and actual risk to the reliability and security of the bulk power system. The product of this evaluation is a risk determination with an assigned risk level of minimal, moderate, or serious. MRO uses the risk determination and the finding discovery method (Audit Finding, Self-Certification, Self-Report, etc.) to calculate the CSI.

MRO has mapped all historic instances of noncompliance into the current, equivalent Reliability Standards and requirements. This allows analysis of the same risk associated with varying instances of noncompliance, regardless of new associated Reliability Standards or requirements.

Figure 21 provides the fifteen highest risk requirements based on the total CSI, which reflects noncompliance history in the entire MRO region back to 2007. Figure 22 provides the fifteen highest risk requirements for the past three years, allowing MRO to shape oversight using trends that are more recent.

MRO uses the CSI to evaluate trends in instances of noncompliance of higher risk requirements. If a requirement indicates a year over year increase in total CSI, MRO may prioritize the oversight for that requirement through modification of an entity's Compliance Oversight Plan.

Figures 21 and 22 indicate a new trend in where the entities are struggling with compliance. Historically, Figure 21 indicates the focus on the maintenance of substation protection equipment (PRC-005-6 R3). The CSI leaders for 2018-2020 (Figure 22) are high volume, high activity requirements addressing Cyber Asset patch and baseline management on a monthly basis.

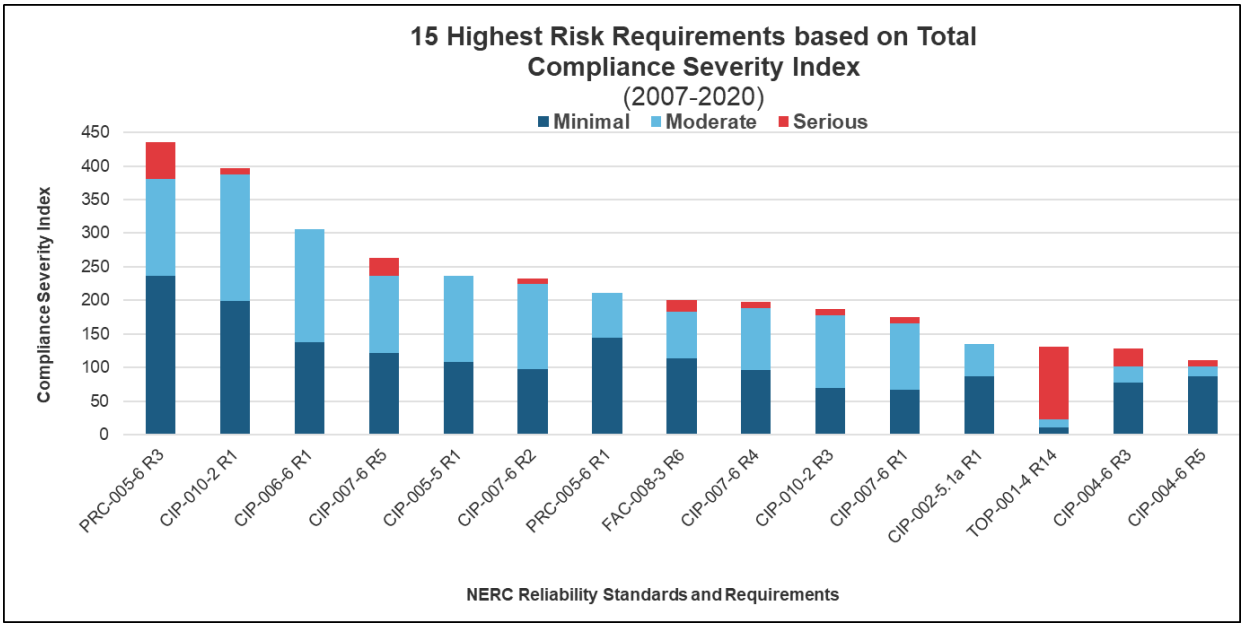


Figure 21: Fifteen Highest Risk Requirements Based on Total CSI

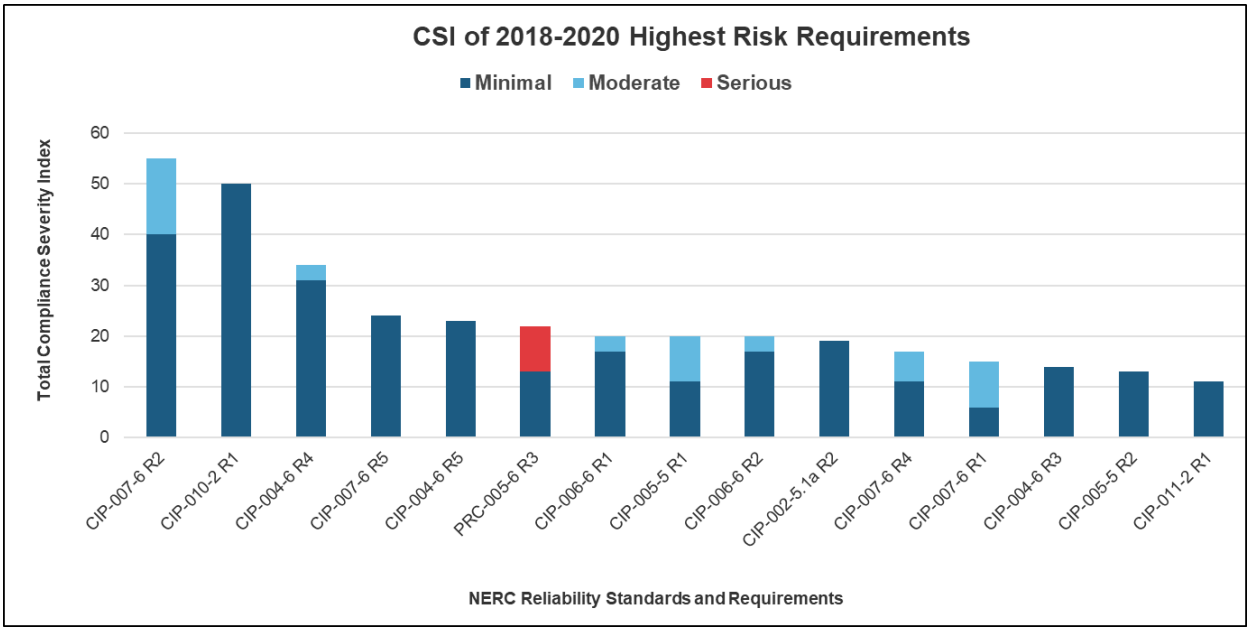


Figure 22: Fifteen Highest Risk Requirements- CSI for Last Three Years

Compliance Severity Index = (Risk Determination) x (Discovery Method)		
Risk Determination	**Discovery Method**	
	Internal (1)	External (3)
Serious (9)	**9**	**27**
Moderate (3)	**3**	**9**
Minimal (1)	**1**	**3**

Figure 23 - Compliance Severity Index

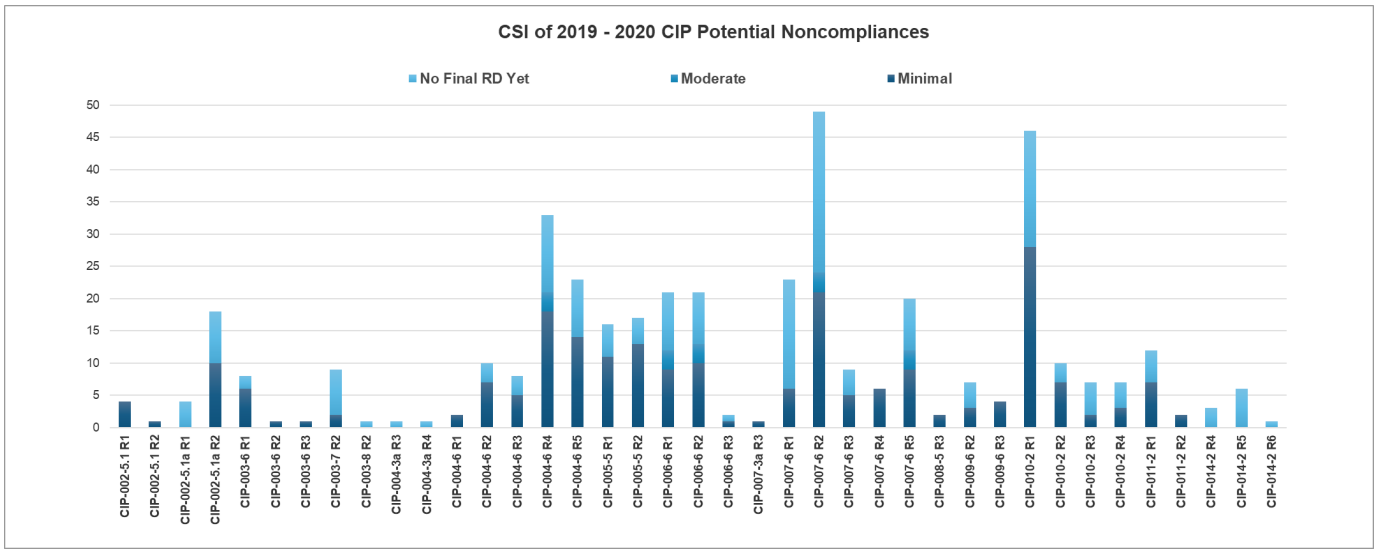


Figure 24 - 2019 2020 Weighted risk, all CIP Potential Noncompliances

6.4 Reliability Standards and Requirements

Oversight of "Risks in Aggregate"

As part of the ongoing refinement of Risk Based Monitoring, last year MRO developed a new initiative to address aggregated risks across multiple low inherent risk registered entities. The intent of the initiative is to identify any critical Reliability Standards that, when evaluated across multiple low inherent risk registered entities, rises to a level that supports active monitoring. This risk in aggregate concept would primarily affect those entities whose Compliance Oversight Plans (COPs) do not presently include any standards or requirements for monitoring, typically either small GO/GOPs or small TO/TOPs. Some examples of the types of risk MRO has observed which are elevated when evaluated in aggregate may include; voltage control and ride through, protection system settings and maintenance, frequency response and ride through, and response to directives.

MRO's initial evaluation of aggregated risk to be considered for oversight in 2021 includes four focused risks for this initiative:

1. Cyber Security for Low Impact BES Cyber Systems

2. Protection System Maintenance
3. Generator Frequency and Voltage Relay Settings
4. Generator Operation for Maintaining Network Voltage Schedules

In 2021, MRO intends to conduct a series of Self-Certifications targeting those entities where individual inherent risk is low, but may be impactful to the bulk power system when evaluated in aggregate with other entities.

A comparison of figures 21 and 22 details that Critical Infrastructure Protection (CIP) has overtaken Operations and Planning noncompliances for presenting a higher risk to the MRO region. With this in mind, this year MRO has placed a larger focus on CIP for the RRA.

Operations and Planning Standards

PRC-027-1 – U.S. Enforceable Date October 1, 2020

PRC-027-1 is a new standard developed as part of Project 2007-06 System Protection Coordination. The purpose of PRC-027-1 is to maintain the coordination of Protection Systems installed to detect and isolate Faults on BES Elements, such that those Protection Systems operate in the intended sequence during faults. PRC-027-1 also introduces a new term that will be included in the *Glossary of Terms Used in NERC Reliability Standards:*

> ***Protection System Coordination Study*:** An analysis to determine whether Protection Systems operate in the intended sequence during Faults.
>
> As part of Project 2007-06, and in conjunction with the approval and adoption of TOP-009-1, Reliability Standard PRC-001-1.1(jj) will be retired.

Planning Standard TPL-001-5 (approved but not enforceable until 2023)

FERC approved Reliability Standard TPL-001-5 (Transmission System Planning Performance) on January 23, 2020, and it will become effective on July 1, 2023. While the new TPL-001-5 does not address the PC coordination or market-based dispatch issues noted above, it incorporates modifications that address the study of single points of failure of protection systems, as well as more thorough analysis of planned maintenance outages, including stability analysis for spare equipment strategies.

Critical Infrastructure Protection Risk Considerations

The threat landscape continues to evolve with the introduction of new technologies, increasing supply chain complexity, regulations that lag technology, etc. The willingness and ability of threat actors to exploit new scenarios in an increasingly complex environment is ever present. The current suite of NERC CIP Standards is robust, and provides defense in depth through focus on gate keeping, post mortem, and analysis. With the evolution of the standards towards objective requirements, many of the real-time considerations are captured by objective statements that an entity's plan is required to address. While this grants entities flexibility to adopt best practices, the standards themselves are generally silent to the methods, technologies, and performance metrics of those plans. With the evolving threat landscape, it may be worthwhile to consider additional definitions, and codifying real-time requirements, thus including in the CIP suite operations and planning requirements for cyber systems. Topics could include such items as data system capacity,

response time metrics during a detected cyber events, and system performance characteristics including availability and restoration. There have been recent FERC Notice of Inquiries that echo these concerns including *RM20-12-000 Potential Enhancements to the Critical Infrastructure Protection Reliability Standards*, *RM20-19-000 Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security*, *and RM20-8-000 Virtualization and Cloud Computing Services*. It will continue to be a challenge as development of the standards lag technology and the evolving threat landscape. Additionally, 2021 looks to have unique challenges brought on by the COVID-19 pandemic and other socioeconomic events.

The forward-looking risks in the following sections are not all inclusive.

Physical Security and COVID-19

Continued focus on physical security of BES Cyber Systems (BCS) is warranted as always, but in particular, MRO draws attention to the physical threat landscape in 2020. Industry intelligence indicates increased activity of extremist groups, including lone wolf, political, and eco terrorism like domestic actors. Historical data from 2019-2020 shows a moderately high weighted risk at sites containing medium and high impact BCS, and a moderately high count of potential noncompliances at sites containing low impact BCS; see Figure 24 – 2019 2020 Weighted Risk, all CIP PNC. At medium and high impact sites, the issues overwhelmingly involve visitor control programs, including unescorted visitors, unlogged visitors, or incorrect logging issues. Medium and high impact sites have secondary issues with locks, bypassed physical access controls, and failures of PACS equipment. At sites containing low impact BCS, the majority of issues are overwhelmingly regarding unlocked perimeters and equipment.

Physical security will continue to be degraded due to complications from COVID. Entities could consider mitigations that counter COVID complications where full security plans are no longer in place, maintenance is delayed, training is not up to date, and physical security mechanisms are overridden. Risk mitigation is warranted because these are not just compliance risks, they translate to security risk as well.

Similar issues affecting physical security due to COVID-19 exist for BCS. As entities experience forced transitions to remote work, MRO has observed the following potential issues:

- Periodic activity delays: training, patch management
- Complications from reduced staffing
- Complications while deploying remote access systems
- Potential for CIP Exceptional Circumstances,
- Control center interactive remote access
- Security operations center implications – alarm monitoring and response
- New standards effective dates during the COVID timeframe

Coordinated Cyber Attack Vulnerability on Geographically Distributed Targets

The current CIP Reliability Standards could be enhanced to address grid transformation by including additional objectives, controls, and criticality assessment criteria, thus increasing protection to widespread geographic cyber attack to both low impact, and medium/high impact assets.

As the deployed BCS at low impact assets evolve to have the same cyber equipment and complex connectivity as that of a medium or high impact asset, it becomes harder to accept less stringent CIP

controls on those assets as currently defined in CIP-002-5.1a. Protection against widespread geographic cyber attack could be enhanced by:

- Altering the traditional electrical / facility based criteria to cause more low impact assets to fall into the medium and high category.
- For those assets that remain in the low impact classification, additional controls from CIP Standards 005 through 013 could be included in CIP-003 R2

Assets of all impact classifications are affected by future wide area control systems that go beyond the well-known power system line protection functions and SCADA. Wide area control system functions may include: 1. Syncrophasor based power system stability; 2. Conductor thermal management; 3. Transformer thermal management; 4. Energy storage integration; 5. Volt/VAR optimization, and; 6. Aggregated generation; et al. Wide area control systems will: 1. Utilize data collection from low and medium impact BCS, including deployment of vendor specific solutions; 2. Communicate to control centers via owned private, lease private, and leased public telecommunications infrastructure, and; 3. Require control center systems to make critical near-real-time operation decisions. BES control system design such as this causes what were once considered independent BES Cyber System at individual assets to start behaving as one large BCS. To help mitigate those risks, the evaluation criteria in CIP-002 could be enhanced by:

- Criteria that consider BCS encompassing multiple assets such as:
    - Cyber interconnectivity
    - Probability/impact of event propagation
    - Dependencies between cyber functions
    - Common mode vulnerability.
    - Reliance on non-CIP communications infrastructure

Regarding NERC CIP required training and recovery drills, they are focused on post mortem analysis and recovery. It is recommended that training and drills include real life cyber-attack scenarios - red team versus blue team type training. As suggested in the introductory paragraphs of the Critical Infrastructure Protection section, it may be time to include CIP operations and planning (O&P) requirements in the standards.

Industry is faced with the following issues as aging electric plant control systems are modernized:

- Supply chain
    - Limited BES cyber equipment vendors
    - Common subcomponent vendors such as silicone manufacturers
    - Foreign sourced components
- Technology change
    - Increased use of virtualization
        - Network functions
        - Protective relays
        - General computational platforms
        - Single point failures (hypervisors) for multiple BES reliability functions
    - Increased use of general computational platforms in BCS – as the hypervisors and as guests
    - Deeper penetration of communication based power system protection and control protocols such as IEC 61850.
    - Software defined networking using centralized control plane servers to make switching and routing decisions for multiple field devices

    - Cloud services
        - BCSI repositories
        - EACMS and PACS servers
        - Backup control center functionality
        - Multi-tenant environments and associated data protection issues
        - Provider misconfiguration allowing inadvertent access
        - Data cleansing – data available to the wrong tenant through reused storage assets
        - Data sovereignty – inability of an entity to control where its data is stored
        - Increased internet facing operations
- Reliance on infrastructure outside the purview of NERC CIP
    - Telecommunications providers backhauling the following functions:
        - SCADA
        - Power system protection
        - Security
    - Cloud service providers
        - Insight into provider's back end infrastructure. Reliant solely on service agreements.

Ultimately, the deployment of modern systems leads to a larger attack surface area, and the ability for common mode attack scenarios, similar to attackers exploiting vulnerabilities in IT scenarios. There are more ways in, more exploits available, and those exploits are deployed at a larger population of assets.

Data Security

The NERC CIP Reliability Standards address this through a combination of objective and prescriptive requirements for medium and high impact BCS that: address BCSI while in storage, use, or transit; system recovery plans; configuration monitoring, and; software integrity through supply chain. The risks and gaps occur because the requirements are mostly objective and thus will be subject to varying interpretation between entities, and the objectives focus on passive protection and post mortem recovery. Data security through long-term availability is not equivalent to maximizing BCS availability during an event. There are industry best practices and accepted technologies that could be included in the objective requirements to bring more consistency among entity programs. There are additional topics not currently addressed by the CIP Standards (which could be considered future CIP O&P) requirements including:

- Information system capacity
- Information system recovery / re-convergence time requirements
- Requiring active defenses such as traffic patterning and prescribed security actions for preset conditions
- Software hash verifications
- Encryption performance
- Requirements to protect / inspect communications between redundant systems
- Application layer inspection

Important to note is future CIP-012 Communication between Control Centers requirements objectively addresses real-time assessment and monitoring of data transmissions. However, topics listed above could be considered in the objectives.

Low-impact BCS are addressed in CIP-003-8, and with the current revision are largely silent to data security beyond malicious code mitigation in Transient Cyber Assets and Removable Media. A future revision in *Project 2020-03 Supply Chain Low Impact Revisions* is slated to address malicious communications for both inbound and outbound traffic, and detection and disablement of vendor remote access. The current and future objective requirements are not equivalent to those in the CIP standards as they apply to medium and high impact BCS. As discussed in *Coordinated Cyber Attack Vulnerability on Geographically Distributed Targets*, as the cyber systems deployed at low impact sites continue their evolution towards the same risk as medium and high impact sites, the aggregate risk and thus protection requirements needs to be re-evaluated.

Anomalies and Events, and Mitigation

Event detection, analyzing, and reporting is covered objectively in CIP-008-5 for medium and high impact BCS and CIP-003-8 for low impact BCS. The risk in the objectives are mainly with assessment and reporting. The industry still has to come to consensus on the incident severity, what constitutes a necessary report, and how to distribute and utilize the threat information. As with all objective standards, the assessment will vary per entity. Real-time mitigation of a cyber security event is highly dependent on an entity's cyber systems and organizational structure, and as such, it may not be possible to be prescriptive on the requirements.

Future deployment of virtualized and cloud computing solutions will bring increased complexity, which may decrease visibility in to the operation of the system, which in turns makes it more difficult to detect anomalous behavior. Issues may include more complex networking infrastructure, over provisioning degrades malicious code/communication detection, dormant virtual machines that do not receive security updates, and deployment of images that are not updated.

CIP Standards Changes in 2020 – 2021 –Risk Considerations

U.S. Enforceable Date April 1, 2020

- CIP-003-8

U.S. Enforceable Date Oct 1, 2020

- CIP-005-6
- CIP-010-3
- CIP-013-1

U.S. Enforceable Date January 1, 2021

- CIP-008-6

CIP-003-8, Security Management Controls

Regarding Low Impact BES Cyber Systems, CIP-003-8 is replacing CIP-003-7 pursuant to FERC Order No. 843[5]. In issuing the order and approving version 7, FERC directed NERC to "develop and submit modifications to Reliability Standard CIP-003-7 to include an explicit requirement that responsible entities implement controls to mitigate the risk of malicious code that could result from third-party transient electronic devices."

[5]https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20No.%20743%20-%20Final%20Rule%20RM17-11-000.pdf

The revisions to the standard affect Attachment 1, Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems. In Section 5, Part 5.2.2 was added where if deficiencies are identified (via methods in 5.2.1 that carried over from version 7), the risk of malicious code introduction is mitigated prior to connecting the Transient Cyber Asset to an applicable system. The standard recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity, but mitigation for identified deficiencies should still be deployed even if the use of a technical method such as anti-virus scan by the entity is not possible. Attachment 2, Number 3 addresses evidence of compliance for Attachment 1, Section 5, Part 5.2.2.

Transient Cyber Assets connecting to Low Impact BES Cyber Systems are considered a risk in the MRO region because:

- Entities are currently not required to apply Supply Chain Risk Management plans to low impact assets and R2 will likely have Supply Chain involvement to verify vendor controls and mitigate discovered risks.
- A significant percentage of generation is low impact and allows third party access.
- A significant percentage of transmission substations are low impact and allow third party access.
- The controls and evidence of compliance for R2 are likely highly procedural in nature.
- On-going vs on-demand management of TCAs

Project 2016-03 Cyber Security Supply Chain Risk Management

Project 2016-03 Cyber Security Supply Chain Risk Management addresses directives from FERC Order No. 829[6] to develop new more modified standards to address "supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations". Subsequently, CIP-013-1 was newly created; CIP-010 and CIP-005 were revised. The standards were approved in FERC Order No. 850[10]. The new and revised standards were originally enforceable on July 1, 2020, but due to the pandemic NERC filed a motion[7] to delay the implementation of these Reliability Standards to October 1, 2020. FERC granted deferred implementation on April 17, 2020[8].

CIP-013-1 Supply Chain Risk Management

This is the core standard developed in Project 2016-03. The standard attempts to mitigate cyber security risks to the BES by requiring entities to implement security controls on the supply chain. The standard is objective in nature, and MRO through its participation in outreach and the Supply Chain Working Group anticipates the following as actual BES and compliance risks:

- Varying levels of depth on vendor risk analysis, likely dependent on the resources of the entity. It is unknown whether entities will go to the subcomponent level, such as discussed in the recent FERC Notice of Inquiry *RM20-19-000 Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security* where risks were identified in the silicone of foreign supplied components, or whether the analysis will end at a system level. Programs between entities likely will not converge until there are several audits

[6] https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order_SupplyChain_20160721_RM15-14.pdf

[7] https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Motion%20to%20Defer%20Implementation%20of%20Reliability%20Standards.pdf

[8] https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/order%20granting%20motion%20to%20defer%20the%20implementation%20dates.pdf

completed where MRO can form a professional judgement, and industry starts to share its results.
- Timeframe or triggering conditions for reassessment of vendor risk.
- Risk transferal from the entity to the vendor based on contract. Entities will need to distinguish between the transferal of actual BES risk (not permitted) versus transferal of financial risk via contract.
- Risk assessments performed on the contract versus on the actual procurement.
- How is a procurement defined – some entities may consider the contract the actual procurement, while MRO will look for evidence of compliance based on actual cyber assets that become a member of a BCS regardless of contract status.
- The definition of 'transitions from one vendor(s) to another vendor(s)' and its applicability, and evidence of compliance.
- Application of third party assessments.

CIP-010-3 Configuration Change Management and Vulnerability Assessments

The new revision adds Requirement 1.6 to verify software sources and integrity of said software. There is no contention over the new requirements, but since technical methods are not stipulated, the risk will be to the BES versus compliance risk. BES risks may vary per entity due to the use of either procedural or technical methods to verify the integrity of the software, and the effectiveness of those measures.

Additional risks observed in 2020 not related to the new requirements:

- Correct classification of custom software
- Implementation of baseline creation and verification procedures that do not have manual detective controls to verify correct implementation of automated systems

CIP-005-6 Electronic Security Perimeter(s)

The new revision adds Requirements 2.4 and 2.5 that require methods for determining and disabling active vendor remote access sessions. The need for the requirements aren't contested, but not having a definition of "active vendor remote access session" will cause risk to the BES and risk of compliance until audits are completed and the industry converges on an acceptable understanding. MRO anticipates the following risks:

- Entity's understanding of what individuals constitute a vendor
- Entity's understanding of what constitutes vendor remote access – web conferencing, proxy servers, screen scraping, IRA, system-system. When technical or procedural controls permit remote control or remote modification by design that would constitute access, regardless of the means through which it occurs.
    - Future vulnerabilities that are capable of changing the nature of read only session – such as CVE-2020-16898 where an attacker can transfer executable code through an established IPV6 session
- How R2.4 and R2.5 could map to an existing employee remote access program and meet the requirements. Technical methods to control unintentionally granting remote access, and associated evidence of compliance
- Focus on the origination source of the vendor remote access session, versus focus on the vendor and access
- The time required to disable a vendor remote access session is not defined

CIP-008-6 Cyber Security – Incident Reporting and Response Planning

This standard revision addresses directives from FERC Order No. 848[9] including: EACMS and PACS; information in Cyber Security incident reports; and filing time requirements. The revisions are largely prescriptive, but Requirement 1 Part 1.2 requires entities have criteria to evaluate cyber security incidents and if those incidents are reportable, thus having a decision matrix. There is no additional BES risk directly, but there will be risk in the effectiveness of the reported information and therefore its utilization. The updates to the standard are part of a larger goal to promote threat information sharing, and until the industry aligns its subjective lens though CEA lead audits and continued collaboration, there will instances of under reporting (probability and impact not deemed high enough) and over reporting to E-ISAC and NCCIC.

Project 2019-03 Cyber Security Supply Chain Risks

This project addresses directives from FERC Order No. 850[10] to modify the Supply Chain Reliability Standards to address EACMS for high and medium impact BES Cyber Systems. Additionally, NERC recommended addressing PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems. Subsequently, CIP-013, 010, and 005 were revised to version 2, 4, and 7 respectively. The final revisions went to ballot on October 16, 2020 and were approved by voting members. The newly revised standards are still pending regulatory filing.

2019 - 2020 Observed Risks from Non-compliance Trends

All 2019 through 2020 potential noncompliances were weighted as follows (noting that if RAM has not assessed risk yet, an MRO Assessed Severity of minimal was assigned):

CIP-007-6 R2, CIP-010-2 R1, and CIP-004-6 R4 are generally manually intensive processes that are transactional in nature, and as such see a large aggregate of weighted risk. As entities look for opportunities to introduce automated processes and tools to assist in reporting, MRO anticipates the level of risk will decrease. However, applying automation introduces risk if the tool is not verified, but process adjustments can provide manual checks on the functionality of the automation.

CIP-007-6 R2 – Patch Management

During the evaluation timeframe, Potential Noncompliances in this category had the primary outcome of patches not being applied in a timely manner. This was driven by: 1. Failure to identify patches within the required timeframe, and; 2. Failure to apply the patches within the required timeframe. The risk to the BES includes threat actors taking advantage of open security vulnerabilities.

The cause ultimately is insufficient process or failure to follow process, however, analysis yields the following general risks that can be improved upon where entity programs utilize overtly manual or highly automated processes:

1. Risk in manual process
    a. Human single point of failure

[9] https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/E-1_Order%20No.%20848.pdf

[10] https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20No.%20850%20Supply%20Chain%20Risk%20Management%20Reliability%20Standards.pdf

        i. No other resources assigned
        ii. No back-checking of work
    b. Unidentified fringe scenarios that procedures do not capture
        i. Configuration errors cause secondary / downstream effects
    c. All patch sources not identified
    d. Procedure lacks sufficient details wherein all required baseline parameters are not recorded.
    e. Clarity of procedures while onboarding new or replacing failed equipment
    f. Disconnects in procedural stages cause drift in due dates
    g. Disconnects in procedural stages during handoff; no overall process owner
2. Reliance upon automated processes without verification
    a. Failure of secondary controls
        i. Reporting tools that indicate patch assessment and application status
        ii. Patch level reported incorrectly by applications
    b. Failure of entity developed assessment tools
    c. Failure of third party assessment tools
    d. Failure of patch application programs

CIP-010-2 R1 – Configuration Change Management

During the evaluation timeframe, risks outcomes due to change control process were primarily driven by: 1. Manual process absentia; 2. Failure to follow established manual process, and; 3. Broad reliance on automated tools without verification. Change control process is essential in detecting unauthorized changes by threat actors, or unauthorized changes due to authorized actions that can lead to open vulnerabilities that threat actors can utilize.

Manual process absentia includes items such as:

- Managing devices individually versus by group
- Process issues where security patches can be applied without specialist evaluation
- Missing process steps to verify other affected Standard requirements during software / firmware changes
- Handoff between procedural steps lacking clarity

Failure to follow manual process includes items such as:

- Verification of CIP-005 and CIP-007 controls that could be impacted by the changes
- Detection of altered network port configuration due to software / firmware changes
- Not following all change control process steps leading to documentation issues
- General lack of understanding the BES risk and Compliance impact of change control process.

Broad reliance on automated tools without verification where the process ultimately is insufficient because functionality of the tool is not verified. MRO has observed items such as:

- Configuration of change management tools causes incorrect baseline reporting
- Reboots causing software package configuration changes
- Updates causing unintentional software package configuration changes

CIP-004-6 R4 – Access Management Program

In the observation time frame, the risk associated with this was largely related to unauthorized access to BES Cyber System Information. The risk manifested itself largely through system complexity, inadequate process, and human processing error.

System complexity included such items as:

- Redundancy of systems leading to undocumented BCSI storage locations, thus users having unintentional access.
- IAM system configuration
- Process surrounding internal transfers
- Nested permissions leading to unintentional provisioning
- System reconfiguration causing errors in records, thus errors in provisioning

Inadequate process including items such as:

- Non-redundant human process failures; resources
- Lacking verification
- Lack of business justification associated with personnel actions

Human processing error related to training, thus failure of individuals to follow existing documented processes. Process enhancements to provide secondary verification of work could mitigate this. Common human errors were related to:

- Quarterly access reviews
- Misunderstanding of group permissions
- Similarly named roles within IAM systems cause confusion
- Failure to action the next step in a process due to missed notifications

7. CONCLUSION

The 2021 MRO Regional Risk Assessment has assessed key risks that are brought forth from ERO-wide assessments and reports to identify how they might impact the MRO region. The ERO sources used for this year's RRA include:

- 2019 ERO RISC Priorities Report
- 2020 ERO Compliance Monitoring and Enforcement Program Implementation Plan
- 2020 NERC State of Reliability Report
- 2020 NERC Long-Term Reliability Assessment
- 2020 NERC/WECC Inverter-based Resource Modeling Report

In addition to assessing which ERO-wide risks may be more prevalent for the MRO Region, MRO staff leveraged the expertise of the three MRO advisory councils (Reliability, Security, and Compliance Monitoring and Enforcement Program (CMEP)) to identify any additional risks that the MRO region may be susceptible to experiencing.

The operational and planning risks and the physical and cyber security risks identified for the MRO region were then ranked by using the MRO risk matrix developed by the MRO Reliability Advisory Council. This risk matrix served to identify which risks were highest in terms of their impact and likelihood to occur. The impact to the bulk power system and probability of occurring was assessed by evaluating each risk's history and trending as well as whether controls are in place to mitigate the risk.

MRO then assessed compliance risk by trending the noncompliance history of higher risk requirements. When possible, the compliance risk was linked back to the operations and planning risks, and physical and cyber security risks, to identify and relationships between the two and close any potential gaps. These efforts will further refine MRO's compliance monitoring and oversight activities to be effective as possible.

Each year, MRO staff will continue to conduct and publish a regional risk assessment to identify and monitor risks posed to the bulk power system within the MRO region. MRO will ensure that efforts are properly focused in order to best monitor and mitigate those risks. MRO staff will communicate key findings and recommendations to registered entities and NERC in order to promote effective mitigation activities, future standards development, and other process improvements to improve the reliability of the bulk power system.

8. REFERENCES

1. 2019 ERO Reliability Risk Priorities Report https://www.nerc.com/comm/RISC/Related%20Files%20DL/RISC%20ERO%20Priorities%20Report_Board_Accpeted_November_5_2019.pdf#search=ERO%20RISC
2. 2021 ERO Compliance Monitoring and Enforcement Program Implementation Plan https://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/2020%20ERO%20CMEP%20Implementation%20Plan%20V%201.0.pdf
3. 2020 NERC State of Reliability Report https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2019.pdf
4. 2020 NERC Long-Term Reliability Assessment https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_LTRA_2019.pdf
5. Inverter Based Resource Modeling Report https://www.nerc.com/comm/PC/InverterBased%20Resource%20Performance%20Task%20Force%20IRPT/NERC-WECC_2020_IBR_Modeling_Report.pdf
6. MRO Phase II Misoperations White paper https://www.mro.net/MRODocuments/PRS%20Phase%20II%20Misoperations%20White%20Paper%206-26-17%20Final.docx.pdf
7. Managing Transmission Line Ratings https://elibrary.ferc.gov/idmws/common/downloadOpen.asp?downloadfile=20190823%2D4002%2833750704%29%2Epdf&folder=16052723&fileid=15333745&trial=1
8. NERC Lessons Learned- Cold Weather Operation of SF6 Gas Circuit Breakers https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/LL20201101_SF6_CB_Operation_during_Cold_Weather.pdf
9. MISO and DER: Managing Grid Reliability through Transparency and Communication https://cdn.misoenergy.org/MISO%20and%20DER%20-%20Visibility495365.pdf
10. NERC Event Analysis Program https://www.nerc.com/pa/rrm/ea/Pages/EA-Program.aspx
11. NERC Standard PRC-024-2, “Generator Frequency and Voltage Protective Relay Settings” https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf
12. NERC Lessons Learned: Loss of Wind Turbines due to Transient Voltage Disturbances on the Bulk Transmission System https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/LL20170701_Loss_of_Wind_Turbines_due_to_Transient_Voltage_Disturbances.pdf
13. NERC Alert “Loss of Solar Resources during Transmission Disturbances due to Inverter Settings” https://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/NERC%20Alert%20Loss%20of%20Solar%20Resources%20during%20Transmission%20Disturbance.pdf
14. NERC/FERC January 17, 2018 Cold Weather Event Inquiry Report https://www.ferc.gov/legal/staff-reports/2019/07-18-19-ferc-nerc-report.pdf
15. MRO Standard Application Guides https://www.mro.net/assurance/StandardsandRules/Pages/Standards-Guidance.aspx
16. ERO Endorsed Implementation Guidance CIP-013-1, CIP-010-3 R1.6

17. NERC 2019 Small Group Advisory Sessions FAQ
18. NERC Cyber Security Supply Chain Risks Report
19. RSTC - Supply Chain Working Group
20. NERC Supply Chain Mitigation Program Website