Regional Risk Assessment

February 2024

MIDWEST RELIABILITY ORGANIZATION

380 St. Peter St, Suite 800
Saint Paul, MN 55102

651-855-1760

MRO.net

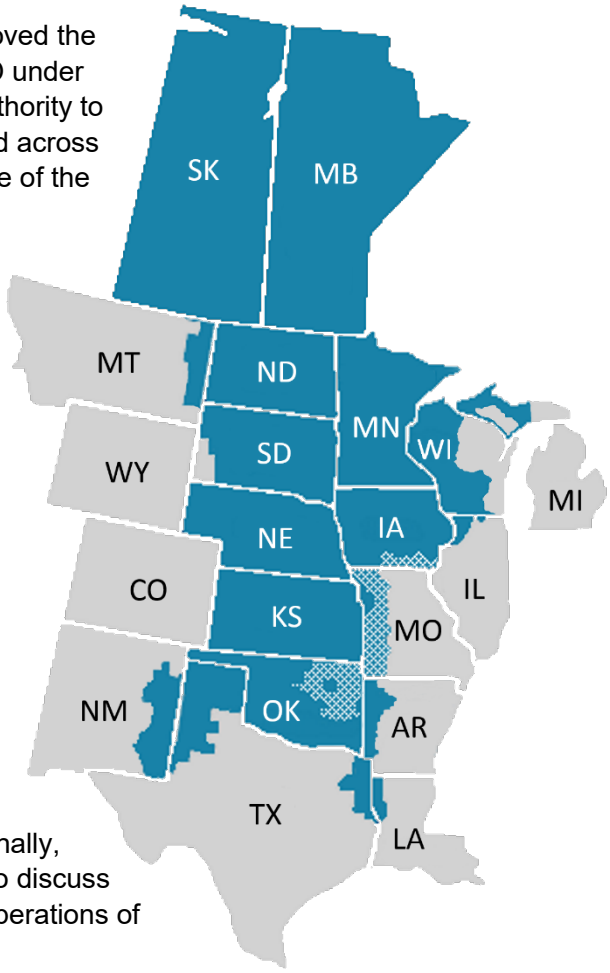
Public

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 225 organizations that participate 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: monitor and enforce 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. EXECUTIVE SUMMARY

The North American bulk power system is the most complex machine ever created and remains one of the most reliable. MRO is one of six organizations charged with protecting the reliability and security of the international power grid as part of the ERO Enterprise (the six regional entities and NERC, collectively) within its regional footprint. MRO publishes a Regional Risk Assessment (RRA or assessment) each year to identify and prioritize risks to the reliable and secure operations of the regional bulk power system.

The assessment is developed collaboratively with industry experts that serve on MRO's three advisory councils (Compliance Monitoring and Enforcement Program, Reliability, and Security) using a wide variety of continent-wide and regional resources. Risks are prioritized by a team of advisory council members and staff using a reliability risk matrix that was developed by the Reliability Advisory Council.

A total of 15 risks were identified in 2024. Uncertain Energy Availability (formally Energy Reliability Planning) rose from a High priority in 2023 to an Extreme priority in 2024, making it the first Extreme risk in the RRA's history. The Extreme priority was designated because of the severe impact and likely occurrence of this particular risk. It leads seven other risks prioritized as High in 2024. The following table lists the Extreme and High risks in priority order from highest to lowest risk.

Risk	Priority
Uncertain Energy Availability	EXTREME
Generation Unavailability During Extreme Cold Weather	HIGH
Supply Chain Compromise	HIGH
Inadequate Inverter-based Resource and Distributed Energy Resource Performance and Modeling	HIGH
Material and Equipment Availability	HIGH
Physical Attacks	HIGH
Malicious Insider Threat	HIGH
Loss of Essential Reliability Services	HIGH

The following common themes and trends are called out in this report.

- Conventional, baseload generation that is available on demand is being retired and replaced with resources with limited energy availability due to uncertain fuel supplies that are increasingly weather dependent.
- New generation resources are largely inverter-based and perform much differently than conventional resources, reducing essential reliability services to the grid and requiring new modeling assumptions.

- Increasing global conflicts threaten cyber security of the bulk power system and domestic terror threats work to disrupt normal operations of the grid.
- Extreme weather continues to cause generating resource outages, limiting energy supply at the same time as demand increases.
- Increasing amounts of generation that are physically distant from load are straining transmission capacity and increasing reliance on remote generation to serve load.

MRO is committed to leveraging its unique position to raise awareness, provide guidance, and develop mitigations for the highest risks to reliability and security of the regional bulk power system. Collaboration from multiple stakeholders is needed to manage through the unprecedented pace of change and confront challenging trends to achieve the goal of maintaining a reliable and secure power grid.

3. INTRODUCTION

The objective of the RRA is to identify the highest risks to reliability and security within the MRO region, communicate the findings to industry through outreach, and work with NERC and industry to develop mitigation strategies and improve the effectiveness of controls, where possible.

The RRA is developed by MRO staff, with input from industry subject matter experts, to identify risks to the reliable and secure operations of the bulk power system within MRO's regional footprint. There are several resources used to develop the RRA including: bulk power system event reports, regional summer and winter assessments, and ERO Enterprise-wide reports. Specifically, the 2023 ERO Reliability Risk Priorities Report was highly leveraged to develop this assessment.

Several of the North American-wide risks identified in the 2023 ERO Reliability Risk Priorities Report broadly present themselves in any of the ERO regional footprints. However, some of these risks may be more geographic (regional or registered entity-specific), and certain areas, regions or registered entities may have a higher exposure or be more susceptible to a specific risk. Extreme weather conditions or high concentrations of variable 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 may be regionally unique.

This assessment presents recommendations and suggestions for mitigation to help registered entities become more aware of and reduce risk to their individual systems.

Figures 1 and 2 illustrate the NERC planning assessment areas compared to 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. Typically, planning assessment areas mirror Reliability Coordinator (RC) boundaries.

Figure 1: NERC Planning Assessment Areas

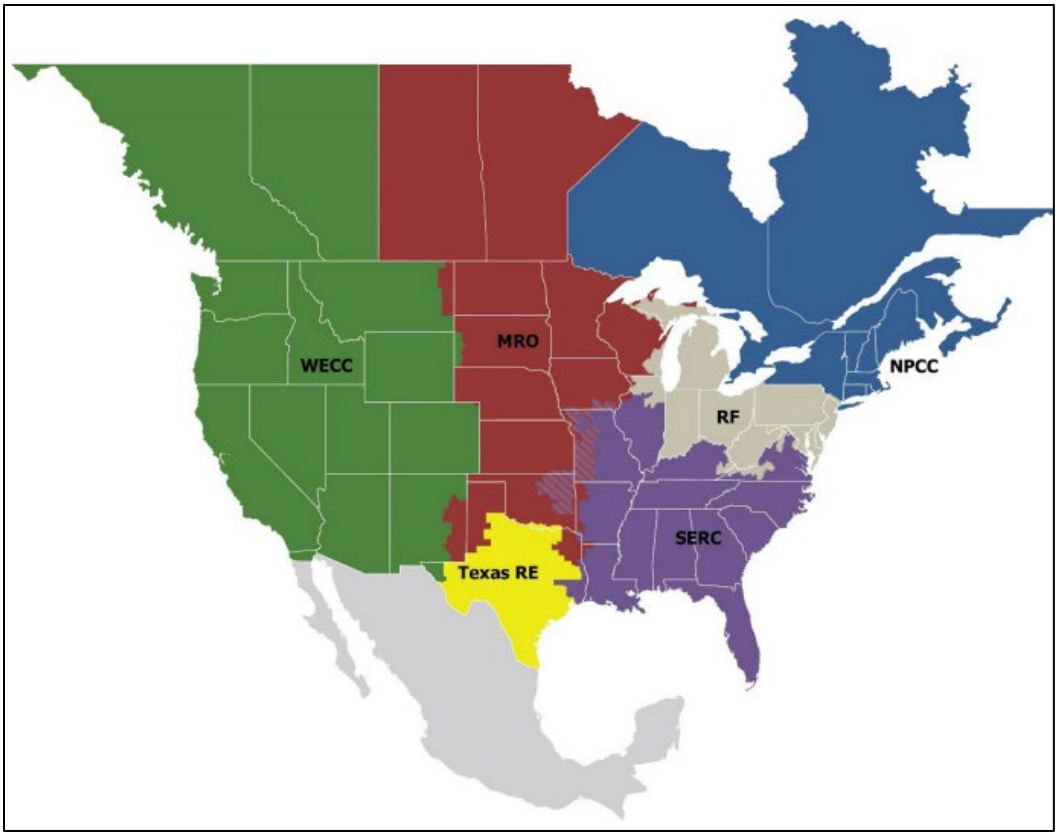


Figure 2: NERC Regional Entity Boundaries

MRO Regional Risk Ranking Process

The Reliability Advisory Council (RAC) developed a reliability risk matrix that provides a relative ranking of the various risks identified by MRO. The relative rank of each risk (location on the matrix) is the result of assessing the likelihood and impact of the risk on the regional bulk power system. Impact is determined by how widespread a particular event or risk would be on the bulk power system. It is centered on the determination of a typical event for each risk so as to not overly focus on worst-case scenarios that might elevate all risks to a higher impact.

Likelihood is assessed by evaluating three criteria:

- Mandatory Controls - Is a NERC standard in place to effectively mitigate the risk?
- Emerging Trends - Are the occurrences (or is the likelihood of occurrence) increasing?
- Event History - Are there any documented occurrences of the risk?

The MRO Reliability Risk Matrix used to prioritize the risks identified in the 2024 RRA is shown in Figure 3. The thresholds for the risk priority levels were modified in 2024 to better represent the categories of risk defined by the impact and likelihood. Risks with a Negligible impact are now considered a Low priority risk, whereas previously, Negligible impact risks with higher likelihoods were considered Medium priority. Higher impact risks considered Very Unlikely were also modified, with Severe impact risks now being High priority and Moderate impact risks being a Low priority. Lastly, and most impactful for the prioritization of risks in the 2024 RRA, the Moderate impact and

Possible likelihood categories were reclassified as a Medium priority risk, where previously this category combination was classified as High.

Consequence/Impact – How could a typical event due to this risk affect BPS reliability?	
Severe (C5)	Impacts may have widespread effects to the BPS across North America.
Major (C4)	Impacts may have widespread effects to the RC area
Moderate (C3)	Impacts may have widespread effects to portions of the RC area.
Minor (C2)	Impacts may have effects on the local entity
Negligible (C1)	Impacts may have small or non-existent effects to the BPS

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

Likelihood – What is the reasonable probability that consequences will occur?	
Almost Certain (L5)	Mandatory Controls – No NERC reliability standards in place for mitigation. Emerging Trends – Increasing trends have been identified. Event History – Documented events or widely publicized exploits have been recorded.
Likely (L4)	Mandatory Controls – No NERC reliability standards in place for mitigation. Emerging Trends – Some trends have been identified. Event History – Documented events or generally publicized exploits have been recorded
Possible (L3)	Mandatory Controls – NERC reliability standards in place for limited mitigation. Emerging Trends – Some trends have been identified. Event History – No documented events, or moderately publicized exploits have been recorded.
Unlikely (L2)	Mandatory Controls – NERC reliability standards in place for mitigation. Emerging Trends – Some trends have been identified. Event History – No Documented events or minimally publicized exploits have been recorded.
Very Unlikely (L1)	Mandatory Controls – No NERC reliability standards in place for mitigation. Emerging Trends – No known trends have been identified. Event History – No Documented events or publicized exploits have been recorded.

Figure 3: MRO Regional Reliability Risk Matrix

Industry Coordination and Collaboration

As mentioned previously, MRO's three advisory councils (CMEP, Reliability, and Security) were leveraged heavily to develop this assessment. A survey was conducted of council members to gather feedback on the previous year's RRA results, followed by two information sessions where all council members could learn more and ask questions about identified risks. A risk ranking workshop

was then held, attended by subject matter experts from the advisory council members and staff, to score and rank each risk. Finally, the CMEP Advisory Council conducted an analysis of NERC standard effectiveness in mitigating each of the 2024 RRA risks. The results of this analysis are mentioned for applicable risks in this report.

4. 2024 MRO REGIONAL RISKS AND RANKINGS

The following section summarizes the 15 regional risks assessed. Table 4 and Figure 5 list the risks in the 2024 RRA and show the relative ranking of each risk. The risks are listed alphabetically and not according to risk priority.

Reliability Risks	
1 Generation Unavailability During Extreme Cold Weather	**8** Misoperations Due to Human Errors
2 Inadequate Inverter-based Resource (IBR) and Distributed Energy Resource (DER) Performance and Modeling	**9** Phishing / Malware / Ransomware
3 Increased Penetration of Internet-Connected Devices	**10** Physical Attacks
4 Insufficient Physical Access Controls	**11** Supply Chain Compromise
5 Loss of Essential Reliability Services	**12** Tight Supply of Expert Labor
6 Malicious Insider Threat	**13** Uncertain Energy Availability
7 Material and Equipment Unavailability	**14** Use of Inaccurate Transmission Facility Ratings
	15 Vulnerabilities of Unpatched Systems

Table 4: List of MRO Reliability Risks in the 2024 MRO RRA

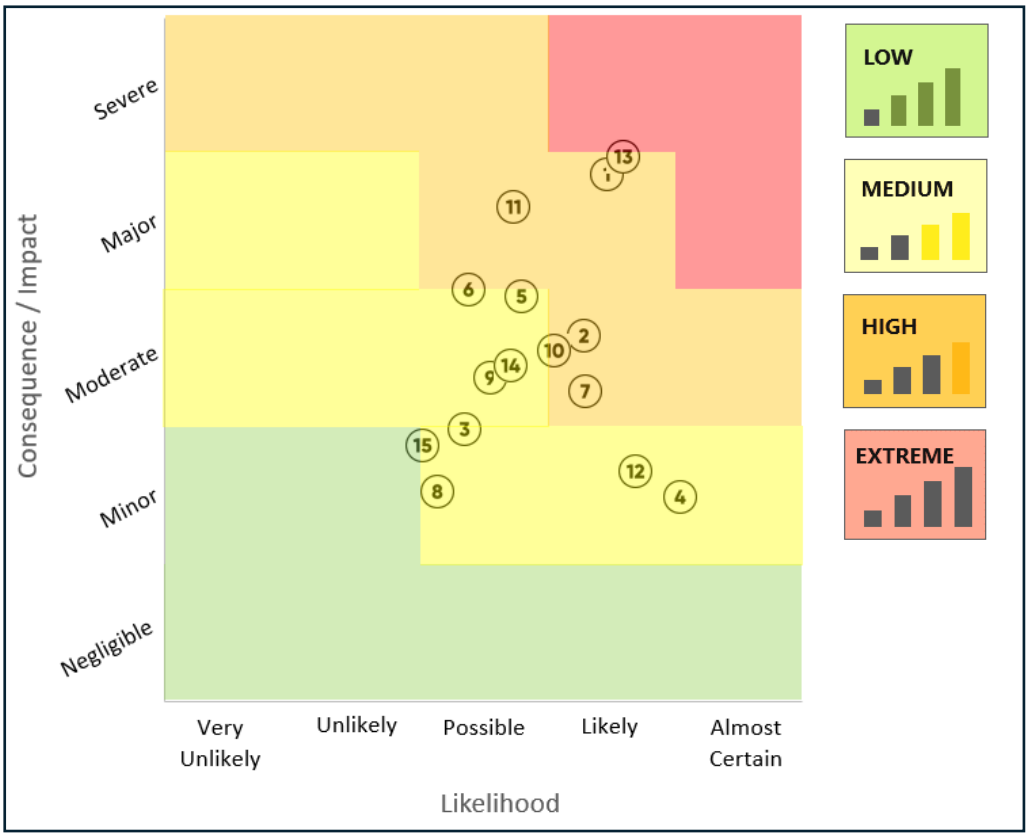


Figure 5: Ranked MRO Reliability Risks Heat Map

The risk of Uncertain Energy Availability is partially in the red portion of the heat map in Figure 5 and has been prioritized as an Extreme risk in the 2024 RRA. This is the first time in the history of the RRA that a risk has been identified in the Extreme risk priority. This Extreme risk is likely to have a widespread impact on bulk power system reliability across North America.

The following seven risks are fully or partially within the orange (High priority) section of the heat map and are listed in order of priority from highest to lowest:

- Generation Unavailability During Extreme Cold Weather
- Supply Chain Compromise
- Inadequate Inverter-based Resource and Distributed Energy Resource Performance and Modeling
- Material and Equipment Availability
- Physical Attacks
- Malicious Insider Threat
- Loss of Essential Reliability Services

Much of MRO's work in 2024 will be dedicated to reducing the Extreme and High priority risks identified in the RRA. Mitigation action plans will be developed, existing controls will be improved, or new controls added, and outreach will be conducted to raise awareness of these risks across the region.

Figure 6 shows changes in impact or likelihood of the 2024 Extreme and High risks from the 2023 RRA. Reasons for the changes in designation are described below. Arrows indicate the direction of the change from the 2023 to 2024 assessment.

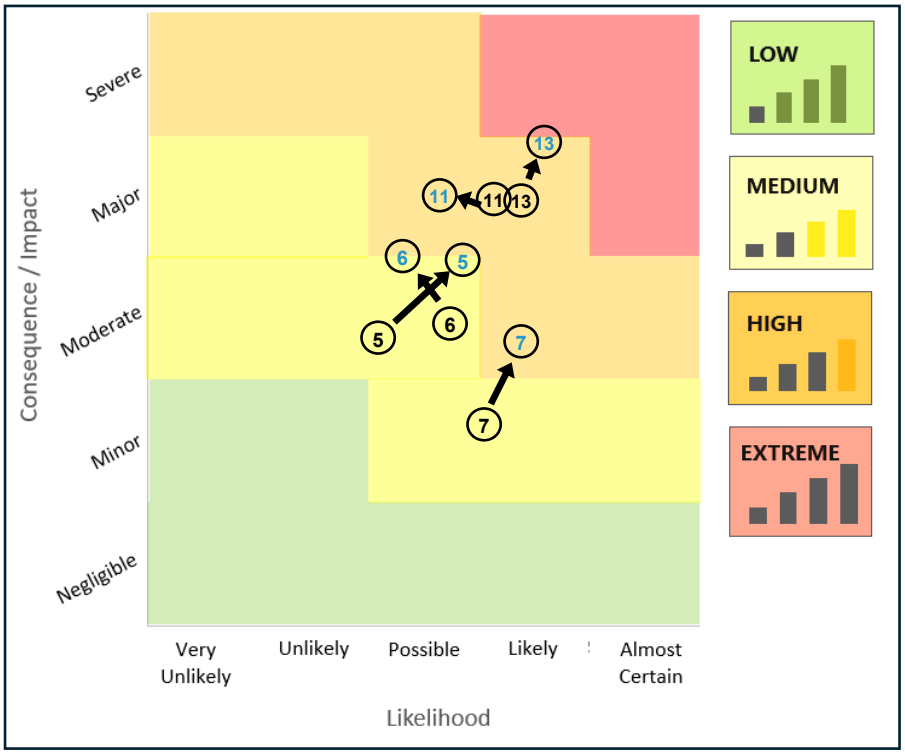


Figure 6: Extreme and High Priority Risks that Changed Impact or Likelihood Categorization in 2024

Risk #13 – Uncertain Energy Availability
The potential impact on reliability of the regional bulk power system increased due to the wide-spread effects of this risk across North America.

Risk #11 – Supply Chain Compromise
The likelihood of occurrence decreased due to modest improvements in the effectiveness of the Critical Infrastructure Protection Supply Chain Standard (CIP-013) and security guidelines published by NERC.

Risk #6 – Malicious Insider Threat
The potential impact on security of the regional bulk power system increased with the assumption that a threat actor would pursue maximum impact on the grid. The likelihood decreased because there is little event history of this risk within the electric utility industry.

Risk #7 – Material and Equipment Availability
The potential impact on reliability of the regional bulk power system increased from Minor to Moderate due to continued equipment shortages, which can affect large portions of a Reliability Coordinator area (multiple utilities simultaneously). The likelihood of such an event also increased due to persistently long equipment lead times.

Figure 7 shows changes in impact and likelihood of 2024 Medium and Low risks from the 2023 RRA. Reasons for the changes in designation are described below.

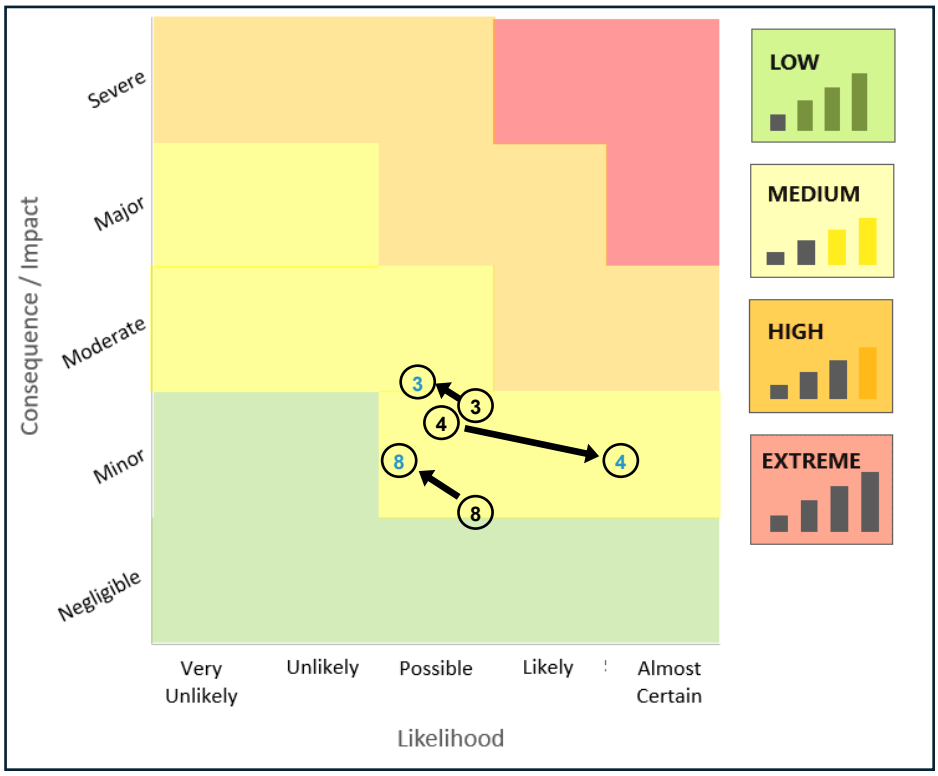


Figure 7: Medium and Low Priority Risks that Changed Impact or Likelihood Categorization in 2024

Risk #3 – Increased Penetration of Internet-Connected Devices

The potential impact on security of the regional bulk power system increased due to broad deployment of internet-connected devices, which could affect multiple areas of the region in the event of a cyberattack.

Risk #4 – Insufficient Physical Access Controls

The likelihood of occurrence increased when this risk was modified to differentiate it from the Physical Attack risk to focus on unauthorized physical access of facilities. A history of vandalism, theft, and intrusion events in the MRO region drives this risk to a higher likelihood.

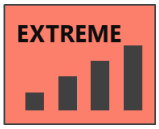
Risk #8 – Misoperations Due to Human Errors

The potential impact on reliability of the regional bulk power system increased because misoperations can result in unnecessary facility outages affecting a local entity's bulk power system that limit power transfers or generation output.

5. DETAILED RISK INFORMATION

This section provides a detailed summary of each of the risks identified in the 2024 RRA in priority order starting with the Extreme risk. Information on emerging trends, event history, impact of risk to bulk power system reliability, and mitigating controls and activities, is provided for each risk if applicable.

Uncertain Energy Availability



Impact: Severe

Likelihood: Likely

A reliable bulk power system requires system operators to maintain a constant balance between electricity supply and demand. Historically this has been accomplished by planning generation capacity around peak demand forecasts and including a reserve margin to account for random uncertainties, like unexpected generation unavailability (i.e., due to failure) or inaccurate load forecasts. As the generation fleet transitions from dispatchable resources that are available on demand to variable resources that are weather-dependent and not always available when needed, the availability of energy to meet demand is more uncertain and existing methods used to determine adequate energy are less valid.

Federal, provincial, and state policies, along with electric utility companies' own initiatives to decarbonize the generation fleet, have accelerated proposed retirements of fossil-fuel generation (predominantly natural gas and coal). These generation sources are being replaced by variable resources like wind and solar that are energy constrained. Certain areas of North America are experiencing higher rates of fossil-fuel retirements, as is the case with the Midcontinent Independent System Operator (MISO), which represents a significant portion of the MRO region. NERC's Long-term Reliability Assessment (LTRA) projects a 38% reduction in coal generation and an 11% reduction in gas-fired generation in MISO between 2024 and 2033. Figure 8 shows projections of MISO's generation fleet from the NERC LTRA.

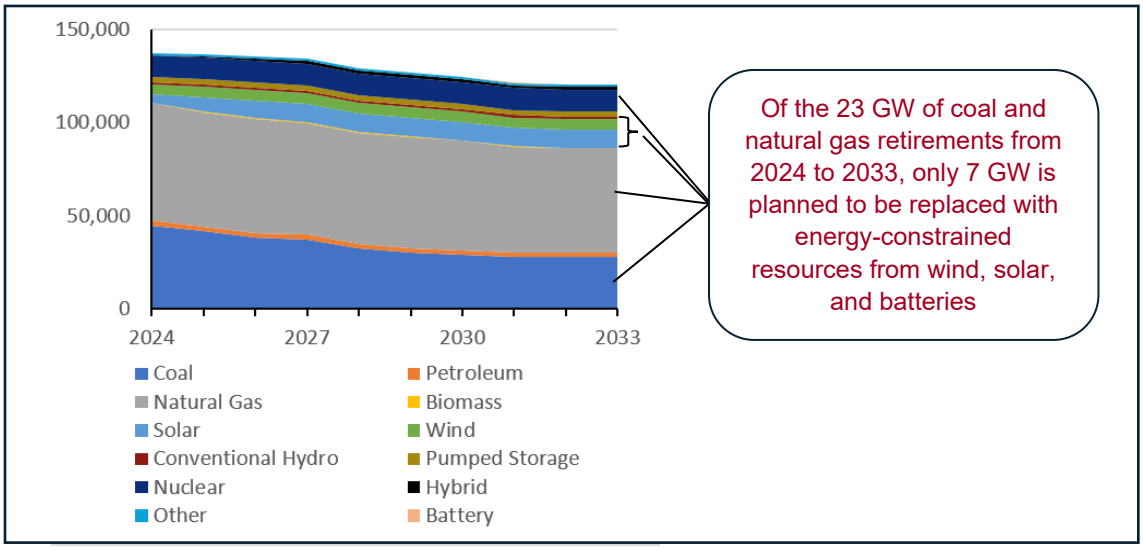


Figure 8: MISO Generation Fuel Mix 2024-2033 from NERC LTRA

Shifting to the load side of the balance equation, sharp increases in the number of large data centers connecting to the electric grid is driving increased load growth the industry has not seen for decades. Federal, provincial, and state initiatives to electrify transportation and space heating will also have a profound effect on both load volume and pattern of use in future years. Moving away from natural gas to electric heat pumps will drive winter system loads higher—so much so that they may outpace the summer loads used to determine peak load—in certain areas. Growth in electric vehicle charging will increase variability of load requirements throughout the day in the location of use. The emergence of distributed energy resources, like rooftop solar and customer-site battery installations, provide an energy resource close to the demand. These resources need to be carefully managed within the balance of supply and demand to maintain a reliable bulk power system.

Significant changes on both the supply and demand side of the reliability equation, when coupled with energy deliverability constraints on the transmission system, call for the need to re-evaluate the operations and planning methods that ensure energy is available when needed. The capacity-based assessments currently used to determine adequate generation supply were designed around a fleet of dispatchable resources that have an assured fuel supply, whereas variable resources do not. These assessments do not account for correlating factors like the effect of weather on both generation supply and load demand. Because dispatchable resources are being retired at a much faster rate than replacement resources—that can serve the same amount of load—are being added, capacity assumptions are less relevant in today's complex operating environment. A new way of understanding what energy is available (from a variety of different resources) to meet demand must be developed. Continuing to rely on traditional generation resource adequacy assessments places the industry at greater risk of inadequate supply to meet demand, which would require load interruptions to maintain system balance.

NERC established an industry-led Energy Reliability Assessment Working Group (ERAWG) to address this risk. The working group proposed development of standards that require energy reliability assessments be performed to determine sufficient energy availability. As a result, NERC is undertaking this as a standards project. A first draft of the standard for system operations was posted for comment in September 2023. A subsequent draft of the standard was posted on January 25, 2024, to address comments and is planned for initial ballot. Work on a standard for long-term planning of the system will follow the operations standard. More details on this project can be found in Section 8.

This risk is a combination of the Energy Reliability Planning and Conservative Practices to Calculate Planning Reserve Margin (PRM) risks from the 2023 RRA. These risks were directly related and frequently discussed together, which warranted the combination of the two in 2024. As the industry grapples with transitioning to a new and different method of resource adequacy that better accounts for energy availability, it is important to highlight the uncertainty the industry is facing. While there is agreement that traditional methods are outdated and less effective, there is no clear and agreeable solution for which to move forward. Because of this, and related challenges with conforming to a new and unfamiliar generation fleet, the impact of this risk increased from the 2023 RRA to the Extreme priority.

Generation Availability During Extreme Cold Weather

Impact: Major

Likelihood: Likely

Recent winter storms Elliott in 2022 and Uri in 2021 have shown that both the electric generation fleet and natural gas supply infrastructure are significantly challenged during extreme cold weather. Both of those storms resulted in a lack of adequate generation supply and unprecedented calls to shed firm load to maintain the electric supply and demand balance and avoid significant system reliability issues. In fact, since 2011, there have been five major extreme cold weather events that greatly impacted electric system operators' ability to meet customer load obligations with sufficient energy supply from generators. Bulk power system performance during each of these storms was jointly reviewed by FERC, NERC, and the Regional Entities. Significant, unplanned loss of generation was identified as a common failure. Figure 9 shows the causes of unplanned generation outages, derates, and fails to start during Winter Storm Elliott. Outages, derates, and fails to start due to freezing issues, loss of fuel supply, and mechanical/electrical issues correlated to the decrease in ambient temperature accounted for 96% of issues encountered.

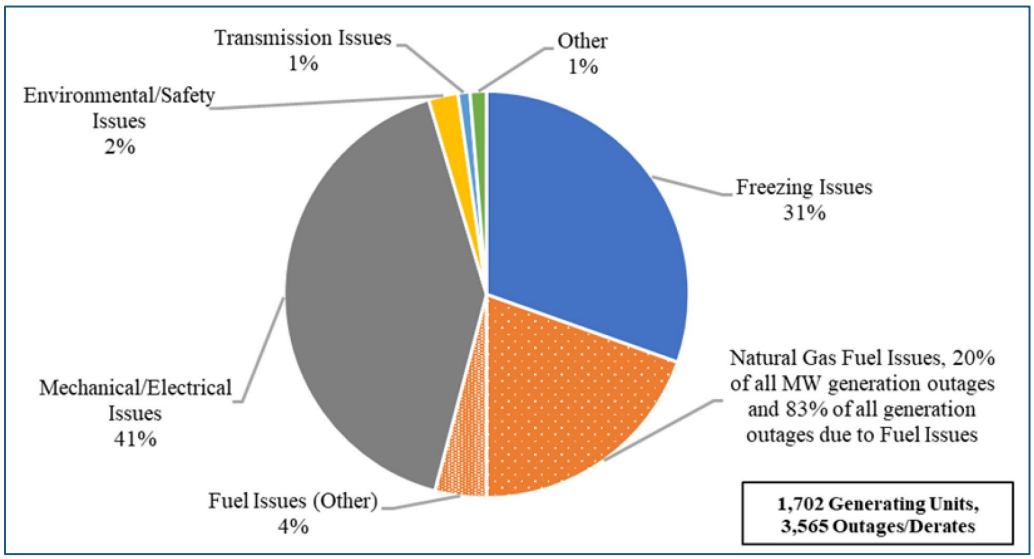


Figure 9: Causes of Unplanned Generation Outages, Derates, and Fails to Start during Winter Storm Elliott

Natural gas-fired generation experienced the majority of issues during winter storm Elliott, due in part to significant fuel supply challenges. Production of natural gas from the Marcellus and Utica share basins dropped considerably during Elliott because of frozen equipment. This freezing added to delivery infrastructure challenges that caused pipeline pressures to drop and threatened service to end-use customers of natural gas, including electric generating units. The reliability issues experienced during winter storms Uri and Elliott exposed the interconnectedness between the electric and natural gas sectors, which are so dependent on each other that a system failure in one inevitably impacts the other.

NERC Standard EOP-011-2, which requires Generator Owners to have cold weather preparedness plans and personnel training to improve generation cold weather performance, became effective in April 2023. Enhancements to this standard are planned in 2024 (and beyond) to create a new EOP-012 standard that requires generator owners to implement freeze protection measures on relevant facilities and create corrective action plans if cold weather performance is not as expected. While these requirements will no doubt improve cold weather generation performance in the electric sector, they do not address the cold weather challenges related to natural gas supply. Retirements of coal-fired generation has resulted in an increased reliance on natural gas-fired generation, further emphasizing the need for natural gas systems to account for the increased supply needed to meet demand during periods of extreme cold weather. Further details on the EOP-012 project can be found in Section 8.

MRO implemented a Generator Winterization Program in 2021 to bring awareness of winterization best practices to industry. Eight generator site visits, representing a diverse location and fuel mix, were performed by MRO staff in 2023, the results of which are shared with program participants.

The potential impact of Generation Unavailability during Extreme Cold Weather risk increased in 2024 and remains at the high-end of the Major impact categorization. This is due to extreme cold weather systems that continue to affect wide portions of North America. Possible occurrence of this risk remains Likely due to a history of extreme cold weather events affecting MRO's region and the recency of cold weather regulations.

Supply Chain Compromise

Impact: Major

Likelihood: Possible

Supply chain compromise is a manipulation of hardware, software, or related delivery mechanisms by a malicious actor before the end user receives the product. It can also signify a malicious vendor employee acting in the capacity of an employee of the end-use organization (Malicious Insider Threat crossover). Supply chain compromises can impact both information technology (IT) and/or operational technology (OT) systems depending on the vendor or manufacturer. Supply chain compromise brings third-party risk to the organization as it is not possible to extend security controls all the way to the vendor's development environment.

This risk has the potential to have a broad impact across MRO's region due to the limited number of vendors of industrial control equipment and commonly deployed digital equipment models. For example, in 2020, SolarWinds software was manipulated to send sensitive information to the Russian Foreign Intelligence Service. SolarWinds software is used in many industrial control system environments, including the electric utility industry.

NERC's CIP-013-2 standard requires registered entities to develop and implement supply chain security risk management plans for high and medium impact Bulk Electric System (BES) Cyber Systems and the associated physical and electronic access controls. An analysis performed by MRO's industry experts suggest these requirements are moderately effective at reducing this risk. There continues to be industry discussion as to whether it is more effective to expend resources on vendor assessments and controls, or simply assume compromise and allocate those resources to other technical risk mitigations within an organization's direct control.

NERC has published a series of security guidelines focused on this risk:

- Product Security Sourcing Guide
- Risk Considerations for Open Source Software
- Electricity Sector – Supply Chain Secure Equipment Delivery
- Vendor Risk Management Lifecycle
- Cyber Security Risk Management Lifecycle

Collectively, these guidelines provide valuable information on different approaches for both entity and vendor risk management, the risks of using open-source software, and security measures for shipped equipment.

MRO staff reviewed the expansion of NERC's supply chain standards to include low-risk entities during the 2023 Risk Assessment and Mitigation (RAM) Conference. The presentation included vendor remote access changes to include low impact BES devices. A Midwest Reliability Matters article published in July 2023 highlights the need for a defense-in-depth approach to supply chain hygiene. This includes extending defense practices beyond the required BES assets to also include business support functions that could impact bulk power system operation. The article strongly recommends that equipment procurement should be subject to a vendor risk assessment like what is done to protect BES assets.

The potential impact of this risk on security of the regional bulk power system increased slightly in 2024 and sits firmly in the Major impact category. This is due to the regional impact that would occur if a major industry vendor were breached, affecting multiple utilities within the MRO region. The likelihood of this risk occurring reduced slightly to the Possible category, driven by the moderate effectiveness of the CIP-013 standard and the recommendations provided by NERC guidelines.

Inadequate IBR and DER Performance and Modeling

Impact: Moderate

Likelihood: Likely

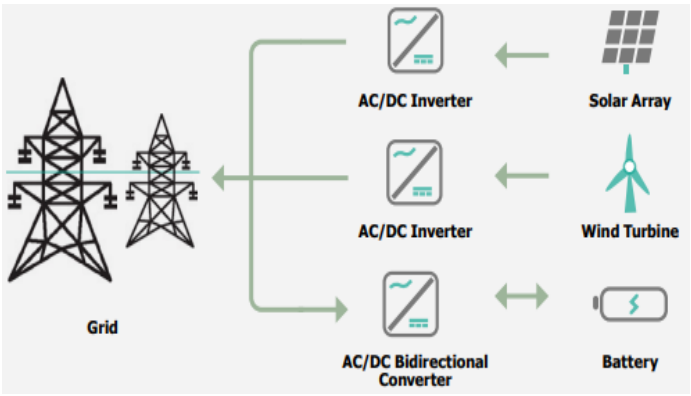


Figure 10: Illustration of Inverter-based Resources

Source: NERC's Guide to Inverter-based Resources

Inverter-based Resources (IBR) are generation resources that utilize an inverter (power electronic interface) to convert a direct current (dc) electricity supply to alternating current (ac) for connection to the grid. Figure 10 shows examples of IBR that are predominantly solar, wind, and battery resources.

Inverters are also prevalent in Distributed Energy Resources (DER) that connect to the grid at customer sites since most of these resources are solar photovoltaic arrays or batteries. IBRs behave much differently than conventional generation and respond to grid conditions based on configured controls versus a physical

response experienced by rotating machines found in the conventional fleet of generation. The unique behavior of these resources and limited industry experience has created modeling and performance challenges.

There have been 13 system disturbances since 2016 analyzed by NERC that involved performance issues with IBRs, as shown in Figure 11. Each event was characterized by significant loss of real power output following a system electrical fault. Each of these disturbances involved multiple solar and/or wind resources, which use inverters to generate into the grid. Some of these events also included the loss of real power from DER, which simultaneously increases load requirements of the grid.

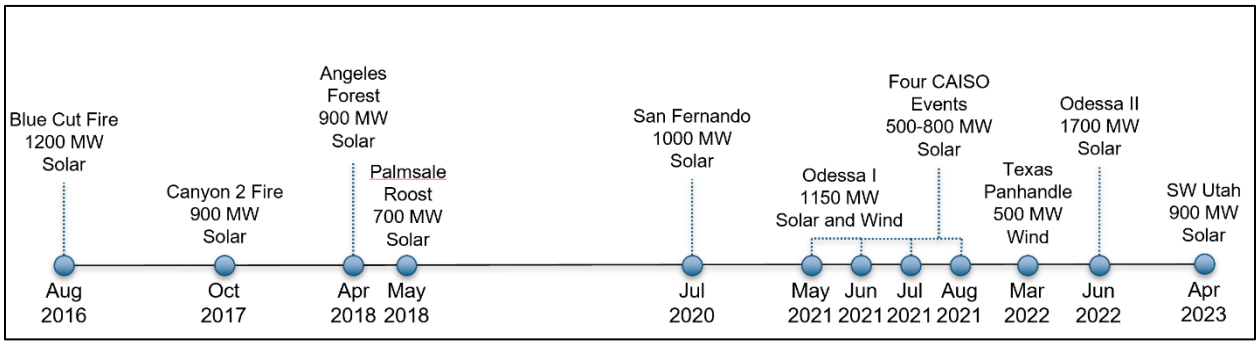


Figure 11: Timeline of System Disturbances from IBR Performance Issues

Through NERC's analysis of early system disturbances impacting IBRs, numerous issues were found with the dynamic models used to analyze performance of IBRs in bulk power system operational and planning studies. The inadequate modeling of these resources has the potential to mask performance issues with IBRs that led to the system events experienced since 2016. There are similar concerns with the modeling of DERs. Dynamic models for loads are generally aggregated based on assumptions of the makeup of the load (residential, commercial, and industrial). As DER generation is increasingly being interconnected to the distribution system, these assumptions are no longer valid. Dynamic performance of loads that include DERs are unique and if they are not accounted for in operational and planning analysis, there could be detrimental impacts on reliability of the bulk power system.

The sudden, unexpected loss of real power from these resources impacts the overall generation and load balance critical to maintaining reliable system operations and avoiding system frequency collapse. This is an emerging risk for the MRO region. While the region has a high penetration of wind resources, most of these resources use turbines that synchronously connect to the grid and only use an inverter to modulate power output for wind speed changes (type 3 wind turbine). This type of wind turbine is less susceptible to performance issues than resources that rely solely upon an inverter for grid connection, which are type 4 wind turbines, solar farms, or battery installations.

MRO partnered with MISO and Southwest Power Pool (SPP) in 2023 to analyze system disturbances within those entities' respective footprints for any signs of IBR performance issues. The results showed few issues isolated to individual windfarms and no widespread issues like those seen in the California and Texas events. However, without proper mitigations in place, the MRO region will be at increased risk of IBR performance issues within the next ten years due to expected growth of solar farms and batteries. As these resource types grow, risks realized during events over the

past eight years will be amplified with larger generation losses that could collectively drive a supply and load imbalance from which the system cannot recover.

MRO's Reliability Advisory Council published a Midwest Reliability Matters article in June 2023 on the adoption of the IEEE 1547-2018 standard for Distributed Energy Resources. This article highlighted a reliability guideline developed by NERC's System Planning Impacts from DER Working Group (SPIDERWG) on the same topic. The article listed key perspectives focused on the ride-through capability of DERs and the need to coordinate settings and controls with expected grid operations to maintain reliability.

NERC's Inverter-Based Resource Strategy charts a path towards improving IBR performance issues, which includes supporting improvements to interconnection procedures and requirements, improving modeling, clarifying performance requirements, and increasing event analysis for abnormal performance. These efforts are in progress. One recent development is the issuance of FERC Order 2023 that in part requires IBR developers to provide models required for transmission providers to do accurate interconnection studies and to configure inverter controls to ride-through system disturbances. There are also several NERC standard projects in development to address some elements of the strategy, which can be found in Section 8 of this report.

This risk in the 2024 RRA combines the risks of Inadequate IBR Ride-Through Capability and Bulk Power Model Assumption Accuracy from the 2023 RRA. This was done because the Bulk Power Model Assumption Accuracy risk centered around risks driven by IBRs and thus combining these risks streamlines the risk definitions. The risk prioritization for this combined risk remains High, which elevates the IBR and DER ride-through performance aspect of this risk to a higher level than the previously reported Medium priority in 2023. This risk has the potential to have a Moderate impact on reliability of the regional bulk power system because the penetration of directly-connected inverter-based resources is currently low, likely only affecting a portion of a Reliability Coordinator's footprint. This risk is Likely to occur due to the lack of applicable standards to help reduce IBR risk and the extensive event history of performance issues.

Material and Equipment Availability

Impact: Moderate

Likelihood: Likely

The global supply chain remains strained beyond its capabilities since the onset of the COVID-19 pandemic. Continued high demand for electrical equipment needed to support increased generation interconnections and transmission system buildout has challenged the manufacturing capability of producers, leading to extended delivery times for many materials and equipment. This is especially true for major equipment like power transformers and circuit breakers. Extended delivery times across the entire spectrum of materials and equipment have eroded industry's inventory of critical equipment, limiting utilities' ability to leverage mutual aid partnerships to source materials following storms or equipment failures. This risk has also spread to IT and network equipment essential for protecting critical assets from cyber-attacks.

The trend of this risk is increasing because lead times for critical equipment are even longer today than a year ago. Generation and transmission buildout is expected to remain at the current pace and could accelerate as the grid continues to transform. MISO's long range transmission plans include a

$10.3 billion portfolio of projects that are planned in the next 10 years. Tranche 2 of MISO's transmission plans are expected to eclipse that amount for future investment. Additionally, MISO and SPP have identified an estimated $1.65 billion in jointly developed transmission projects as part of a Joint Targeted Interconnection Queue (JTIQ) study.

Lack of materials to replace failed or damaged equipment extends outage durations thereby reducing availability of transmission facilities to maintain reliability. Lack of materials and equipment also can delay planned projects that are necessary to address identified reliability issues or bring online additional generation capacity needed to serve customer load. There are several voluntary programs within the industry that provide a mechanism for utilities to share or sell spare equipment in times of need. However, these programs are not widely used and do not include the entire industry.

The continued extension of delivery times for critical equipment has increased the likelihood of this risk occurring from Possible in 2023 to Likely in 2024. The potential impact of this risk on reliability of the regional bulk power system also increased from Minor to Moderate given concerns that continued equipment shortages can affect large portions of a Reliability Coordinator area versus a localized impact. The combination of these ranking changes has raised this risk to a High priority for 2024.

Physical Attacks

Impact: Moderate

Likelihood: Likely

Physical attack is the risk of a threat actor motivated to cause harm to the power grid using low cost means such as guns or bombs (referred to as ballistics attacks) or vehicular impacts. Threat actors target high value or long lead time equipment, which may be located at critical facilities. The typical physical controls deployed at most facilities focus on denying unauthorized access to within the facility. Those controls are fences, gates, locks, and cameras. Those controls can prevent the opportunistic threat actor intent on criminal activity such as theft and vandalism as captured in Insufficient Physical Access Controls, but are not effective at stopping attacks from outside a facility.

Preventing physical attacks from outside a facility from weapons and ballistic attacks require controls that deter, detect, and delay a threat actor. That combination reduces the probability of a threat actor targeting a critical facility to begin with, but also buys time to get law enforcement response during an active attack. The ready availability of open-source information exacerbates this risk because it helps inform threat actors of potential targets to attack.

The number of reported ballistic attacks since 2016 (Figure 12) has been increasing according to an E-ISAC report.

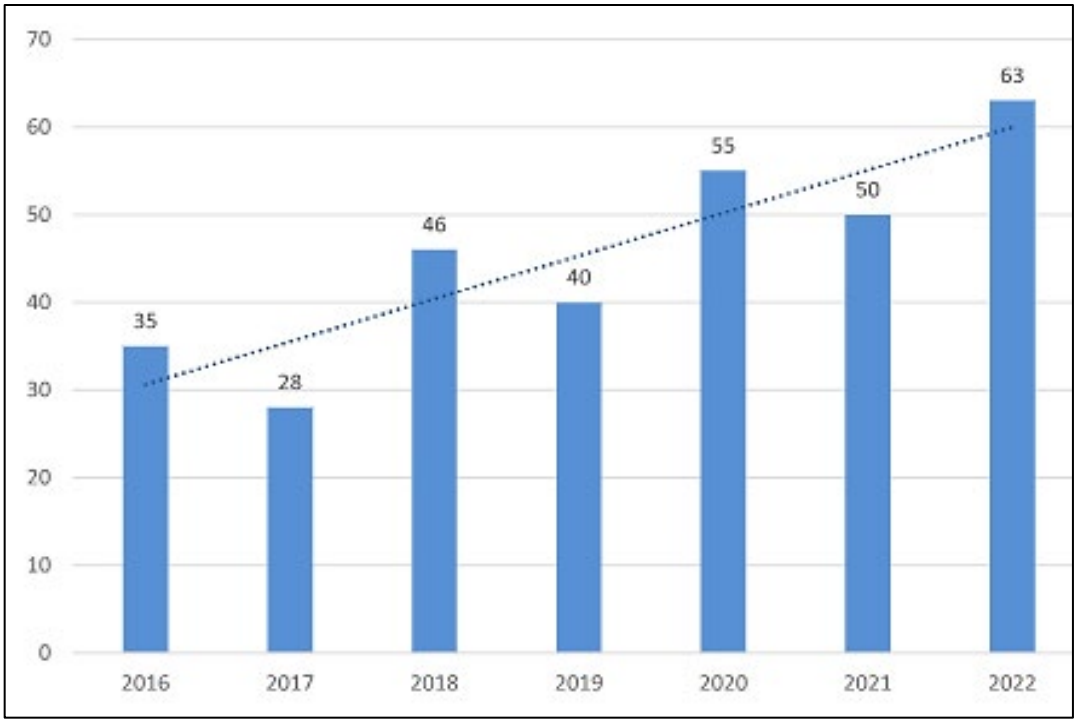


Figure 12: Number of Ballistic Attacks from 2016 to 2022 Reported to E-ISAC
Source: E-ISAC restricted Physical Security Report on Ballistic Attacks at Substations (used with permission)

There was a widely publicized attack in December 2022 on two substations in Moore County, North Carolina. Ballistics were used in that attack to damage and take substation equipment out of service, leading to tens of thousands of customer outages, some of which lasted for multiple days. Bulk Electric System equipment was not targeted; thus, customer outages were localized. This attack followed a similar attack on the Metcalf substation in California in 2013 and is a reminder that electric facilities are a valuable target for threat actors.

The NERC CIP-014 standard is focused on identifying and protecting transmission facilities from physical attack. However, this standard has limited effectiveness against a threat actor who is acting outside the perimeter of a facility. It is impractical and cost prohibitive to fully protect transmission equipment from all levels of physical attack. In addition to existing perimeter controls and protections put on critical transmission equipment, reliability and resiliency measures should be pursued to limit the impact of equipment attacks. Increasing redundancy in the system and adding controls that offer delay and detection provide time for authorities to respond to the attack.

A joint NERC/FERC technical conference on physical security of the bulk power system was held in August 2023. There were panel discussions on the effectiveness of the CIP-014 standard, physical security best practices, operational preparedness, and planning for physical security beyond the standard. MRO compliance staff published a Midwest Reliability Matters article that provided insights and key conference takeaways like industry's proactive efforts to enhance physical security, the importance of collaboration between federal and state entities, and the integration of security and resiliency into future grid planning.

This is a new risk identified in the 2024 RRA. It was split from the Physical Security Protections from Incidents risk in the 2023 RRA since a physical attack from outside the facility using guns, bombs, and vehicle strikes has a much different impact and likelihood than unauthorized physical access to facilities. The impact of this risk on security of the regional bulk power system is Moderate because an attack would only impact a portion of a Reliability Coordinator footprint. This risk is Likely to occur due to event history and as part of critical infrastructure, the electric grid is a prime target for disrupting society in North America.

Malicious Insider Threat

Impact: Major

Likelihood: Possible

Malicious insider threats are presented in trusted employees, contractors, or vendors with knowledge and access to systems and the capability of bypassing security controls to cause harm to the bulk power system. A malicious insider could be manipulated by a threat actor external to an organization or may act on their own. The malicious insider often has underlying motivating factors such as unmanaged workplace dissatisfaction, ideology, or financial motivation. Impacts can be physical or cyber. This risk does not include unintentional insiders because they lack motivation. The risk caused by the unintentional insider should be considered with other cyber risks, such as Phishing/Ransomware/Malware.

There have been no known malicious insider threats to the bulk power system in the past. However, an insider with motivation could cause detrimental impact to the bulk power system directly by manipulating control systems that operate the grid or indirectly by disrupting business functions that hamper grid operations. The impact to the bulk power system depends on the size and function of the organization attacked.

From an analysis by MRO industry experts, a suite of NERC CIP standards provides limited controls for this risk. CIP-004 requires background checks every seven years on personnel with access to BES Cyber Systems, however, the seven-year timeframe is lengthy and provides limited coverage. Role-based access restrictions in CIP-004 Requirement 4 also provide limited control since the malicious insider would be a trusted individual with authorized access. The standards CIP-005, CIP-009, CIP-010, and CIP-011 provide a defense-in-depth strategy to limit movement of a threat actor to segments of a BES Cyber System. However, a malicious insider with broad, administrative rights may be able to traverse multiple systems easily, which reduces the effectiveness of these standards. CIP-006 regarding physical access to BES Cyber Assets or facilities is focused on monitoring for unauthorized access, which in the case of an insider would not apply since they would typically have authorized access. There is an active NERC standards project on internal network security monitoring that could help mitigate this risk by requiring monitoring of activities within a network, helping to identify malicious behavior on a network system even by an insider with authorized access. More details on this project can be found in Section 8.

Companies with comprehensive insider threat programs that include a process for responding to potential insider threats can also help mitigate this risk. MRO published a Midwest Reliability Matters newsletter article in May 2023 on insider threats. This article defines an insider threat and provides considerations for an insider threat program. MRO's Security Department, with support of the Security Advisory Council, created a checklist and benchmarking tool aligned with these

considerations. The Insider Threat Program Checklist, released in November 2023, is intended to help MRO entities develop or enhance their existing insider threat policies and procedures. More information can be found in the newsletter article from November 2023 promoting the checklist.

The risk remains High in 2024 due to a Possible likelihood of occurrence associated with limited NERC standard controls and could have a Major impact on security of the regional bulk power system given potential disruption to the grid.

Loss of Essential Reliablity Services

Impact: Major

Likelihood: Possible

NERC published a whitepaper in 2016 that defined essential reliability services as frequency support, ramping and balancing, and voltage support. Until now, these services have been provided by the large and dispatchable fleet of generation resources. New inverter-based and variable resources (wind and solar) do not inherently provide essential reliability services at the same level as conventional resources. As the proportion of conventional generation resources declines, and inverter-based and variable resources grow, essential reliability services will be in shorter supply and have an increased likelihood of causing bulk power system reliability problems. Quantifying the level of essential reliability services needed to maintain system stability is unfortunately not straightforward. It is a new engineering challenge as the system enters uncharted territory with fewer conventional resources able to provide these services inherently.

To understand the overall impact and likelihood of this risk, it is important to analyze each of these services individually. The inertia from the large, spinning mass of conventional generation aids frequency support to arrest the decline in frequency following a system disturbance. Since inverter-based resources have little to no spinning mass, frequency declines will be larger and more sudden if alternative frequency support is not acquired. To maintain grid reliability, the supply and demand of electricity must always remain in balance. This is accomplished by a fleet of generators that are dispatchable and can be ramped up and down to match changes in load. The variable nature of wind and solar generation creates challenges with dispatchability and ramp up capability, while also increasing ramp requirements that strain the diminishing fleet of dispatchable resources. If there are not sufficient dispatchable resources online to meet the ramp requirements, reduction in load (voluntary or non-voluntary) is necessary to maintain system balance.

Lastly, the transmission system has been designed and built around centralized generation that provides the bulk of the dynamic reactive power into the grid to support voltages. New generation interconnections are being installed further from load centers, which puts additional strain on the grid to maintain voltages. The electric grid in the MRO footprint is characterized by long transmission lines connecting generation to load, making the region more susceptible to this risk. New interconnections are more distributed and smaller, which change the location and size of available reactive power that can be injected or consumed by generation. These changing supply and requirements for reactive power will require additional, non-generation resources to avoid areas of voltage instability.

There are several NERC standards related to the different aspects of this risk. NERC resource and demand balancing standards (collectively referred to as BAL standards), are moderately effective at

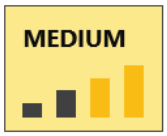
reducing the frequency support, ramping, and balancing aspects of this risk per analysis by MRO industry experts. These standards do a good job defining standard calculations for system inertial response and balancing performance requirements. They are very effective for operating the system on a real-time basis. However, they are very limited in providing planning requirements for an adequate amount of these services in the future with the changing resource mix. The MOD-025 standard provides reactive power testing requirements that include testing for IBR. This standard is moderately effective at identifying reactive power capabilities.

Transmission operations and planning standards address requirements to perform analysis to ensure adequate voltage is maintained on the bulk power system. However, these standards do not provide detail on specific scenarios that represent future strained grid conditions, which might identify deficiencies in system voltage performance that require mitigation.

In the 2023 RRA, this risk was focused on only the voltage support element of the essential reliability services. The 2024 RRA includes all three essential reliability services needed to maintain grid reliability as all three are at risk of dropping below necessary levels. With the inclusion of all three services, the impact and likelihood scores of this risk increased, warranting a High priority in the 2024 RRA.

The impact of this risk is Major because frequency response and ramping and balancing issues will impact the entirety of a Reliability Coordinator area. Voltage support is more of a localized issue, but local voltage support issues can also create transfer limitations that can extend to a Reliability Coordinator-wide impact. The Likelihood of this risk is Possible due to the lack of detailed standards around planning for essential reliability services and the increasing trend of resource retirements that provide these services.

Use of Inaccurate Transmission Facility Ratings



Impact: Moderate

Likelihood: Possible

The NERC FAC-008 standard requires transmission and generation operators to maintain accurate facility ratings to ensure individual equipment ratings comprising a facility are respected. These facility ratings are used in the reliable operations and planning of the bulk power system. From 2021 through Q3 of 2022, FAC-008 had the fifth most serious risk violations as shown in Figure 13 from NERC's Compliance Monitoring and Enforcement Program and Organization Registration and Certification Program Quarterly Report.

Only a series of CIP standards eclipsed FAC-008 for the most serious risk violations. This is indicative of methodology or process deficiencies that can lead to the inaccurate calculation of facility ratings. The use of inaccurate ratings by operational and planning personnel can lead to unnecessary equipment damage (facility ratings higher than actual), or lead system operators to make decisions that hurt system reliability (facility ratings lower than actual).

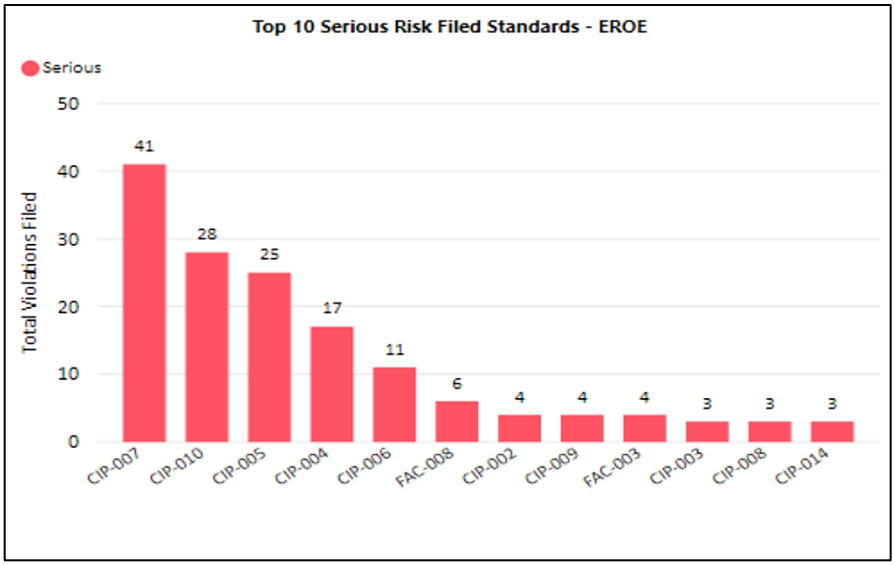


Figure 13: Most Violated Reliability Standards by Serious Risk in 2021-Q3 2022

Further challenging the accurate calculation of facility ratings is FERC Order 881, which directs the use of ambient-adjusted ratings and uniquely determined emergency ratings. While FERC 881 mandates emergency ratings, the absence of which has been identified as a significant risk across MRO, it also introduces system complexity. The Order increases the number of rating sets required on a facility, subsequently increasing the possibility of rating errors that need to be carefully managed to ensure the correct set of ambient-adjusted ratings are used by system operators. Adopting FERC Order 881 into Transmission Owners' facility rating methodologies will require significant changes in policies and technologies to maintain accurate ratings used for reliable grid operations.

Analysis of the FAC-008 standard by MRO industry experts indicates it is a highly effective for establishing accurate facility ratings. However, as previously stated, this standard has had a high serious risk violation rate in recent years. Further, it is not clear how FAC-008 will apply to ratings determined for compliance with FERC Order 881, even though those ratings will be used for the real-time operation of the bulk power system.

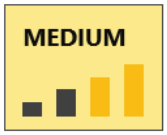
Building effective programs to manage accurate facility ratings and implement preventative controls is necessary to be more successful in calculating accurate Facility Ratings. The ERO Enterprise published a report on themes and best practices for sustaining accurate facility ratings to help entities develop an effective program. MRO hosted a facility ratings best practices panel with four industry experts during the 2023 Reliability Conference. Topics discussed include:

- use of ambient adjusted ratings,
- ratings management and controls when equipment changes are made,
- controls to manage facility rating data, and
- the North American Transmission Forum's Facility Ratings Practices Guides

MRO compliance monitoring and enforcement staff performed several activities in 2023 related to facility rating risk. They held guided self-certifications with medium and low-inherent risk transmission operators on the FAC-008 requirements. Self-certifications on FAC-008 requirements of medium and low inherent risk generator operators are planned for 2024. MRO's Risk Assessment and Mitigation department implemented process changes to its mitigation strategy for FAC-008 violations to put focus on internal controls to verify facility ratings.

In the 2023 RRA, this risk was focused on the need for seasonal and emergency ratings for use in system operations. The risk was broadened in 2024 beyond seasonal and emergency ratings because any inaccurate rating can be detrimental to reliability. The high occurrence of FAC-008 violations further justifies this change. The transition to complying with FERC Order 881 increases the amount of data required to maintain accurate facility ratings, which in turn increases the possibility of error. This broadened risk has a slight reduction in both impact and likelihood, dropping the risk priority from High to Medium in 2024. This is due to the changes in the risk matrix (Moderate Impact and Possible Likelihood becoming Medium and not High) and not the slight change in impact or likelihood of the risk itself.

Phishing / Malware / Ransomware



Impact: Moderate

Likelihood: Possible

Malware and ransomware use malicious software to execute unauthorized actions on the victim's system. These attacks are frequently initiated by phishing, which uses emails containing malicious code, attachments, or links that compromise systems and can spread. When a threat actor phishes an employee, they successfully convince that employee to click on a malicious link or open a malicious file contained in a message. In doing so, the threat actor can encrypt an organization's system and hold those systems hostage through ransomware until the organization pays for the decryption key. Phishing can also lead to damage, disruption, or unauthorized access to systems through the deployment of malware.

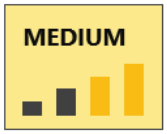
These threats are constantly evolving, can impact critical systems resulting in adverse impacts to operations, and can often spread through networks. While this risk is more prevalent in Information Technology (IT) systems, most Operational Technology (OT) systems have connections to IT so there could be a direct impact on operations. An attack on IT systems may also have business continuity implications that hamper operations. Phishing/Malware/Ransomware may be the delivery mechanism for an attack aimed at inhibiting the response functions of a utility. An adversary could use techniques to hinder safeguards put in place for reliable operation of the grid, such as protective relays. Further, an adversary could inject malicious code that could prevent expected alarms in SCADA systems, making system operators unaware of worsening conditions on the grid during escalated operations.

A suite of NERC CIP standards (CIP-005, CIP-007, CIP-009, and CIP-010) provide technical methods for a defense-in-depth strategy and are collectively designed to limit the penetration of malicious code and malicious communication through perimeter defense, system hardening, detection, active mitigation, and system recovery. Analysis performed by MRO's industry experts indicate these standards provide highly effective controls for ransomware and malware on operational systems. However, these standards do not apply to phishing directly nor to IT systems

that may support operational systems or that could impact business operations since they are not part of the bulk power system.

The risk would affect individual organizations, but the impact to the bulk power system is dependent on the function and/or size of the affected organization. The risk priority dropped from High to Medium in 2024 due to the changes in the risk matrix (Moderate impact and Possible likelihood dropping from High to Medium) and not the slight change in impact or likelihood of the risk itself.

Increased Penetration of Internet-Connected Devices



Impact: Moderate

Likelihood: Possible

Driven by technological innovations and grid transformation, utilities continue to deploy internet-connected devices such as smart meters in homes, responsive load devices, and transmission line sensors. The number of devices is expected to increase due to continued innovation and development (e.g., electric vehicles, DERs, demand response), and potential future deployment of equipment to support dynamic line ratings. These systems are increasingly used to provide valuable data to operate the changing grid and, in some cases, provide the ability to control aspects of the grid through load management. Deployment of these devices presents new risks to power system operations through:

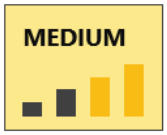
- devices in physically unprotected locations
- common vulnerabilities across large areas
- limited number of manufacturers and models
- cloud aggregation systems
- internet used for data transport

These devices present more opportunities for threat actors to gain access and affect operations because the confidentiality and availability of the devices may not be under the utility's direct control, placing more emphasis on the controls needed to ensure the integrity of the data. This risk has the potential to impact the bulk power system through automated or operator-initiated actions at bulk power system controls centers. For operator-initiated actions, manipulated data through a breach of internet connected devices presented to a system operator may cause them to make operating decisions detrimental to the grid without their knowledge.

This risk is not covered by NERC standards since the internet-connected devices typically are not identified by the CIP-002 standard as being Bulk Electric System cyber assets.

The impact of this risk on security of the regional bulk power system increased in the 2024 RRA to Moderate as internet-connected devices will continue to be deployed broadly, resulting in a wider impact area. The likelihood of this risk occurring decreased slightly but remains Possible because of the lack of NERC standards in place to mitigate the risk. The likelihood of occurrence is tempered slightly because of the small penetration of these devices used today for real-time operation.

Tight Supply of Expert Labor



Impact: Minor

Likelihood: Likely

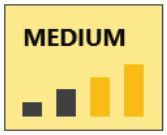
This risk represents the importance of adequate expertise and resources to maintain reliable operation of the bulk power system. It persists due to a competitive job market, low unemployment, and competing business factors. According to U.S. Bureau of Labor Statistics, the number of job openings in the transportation, warehousing, and utilities sector has lessened in the past year to 484,000 openings. While this is less than the 579,000 openings reported in 2022, it is still double the number of openings in 2020. As reported by Cyberseek.org, a site that provides cybersecurity jobs data, there was a drop in cybersecurity job openings from 720,727 in 2022, to 572,392 in 2023. This is more in line with the job opening levels seen since 2018. Anecdotally, many leaders in the utility industry have indicated difficulty in finding and hiring qualified staff for open positions.

An insufficient number of trained staff may result in operational impacts and the ability to position the power system for the changing resource mix or to address present and future security risks. Business decisions to prioritize work become more important with staffing level challenges. Organizations need to be strategic to ensure compliance with mandatory standards while also developing risk-based programs and innovating new solutions to address complex reliability risks.

There is not a NERC standard to address this risk and it is unlikely a standard would be an effective mitigation. Instead, companies should continue to build partnerships between the public and private sectors to educate, recruit, and retain talent in the electric industry.

The impact of this risk increased in the 2024 RRA, due to the persistence of the short supply of labor and the sub-regional impact.

Insufficient Physical Access Controls



Impact: Minor

Likelihood: Almost Certain

Unlike the Physical Attack risk, this risk encompasses activities including copper theft, intrusion, and vandalism inside utility facilities. The threat actor intent on those activities often is motivated by economic and media trends, and actions are localized and random. As compared to threat actors executing a Physical Attack from outside the facility, the threat actors perpetrating copper theft, intrusion, and vandalism need unauthorized access within a facility, therefore perimeter controls such as fences, gates, locks, and cameras may be effective at deterring or denying access.

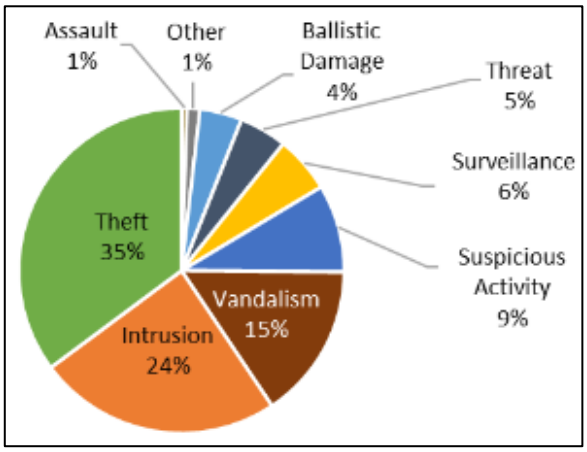


Figure 14: Causes of Physical Security Incidents Reported to E-ISAC

Source: E-ISAC restricted Physical Security Monthly Outlook for November 2023 (used with permission)

As Figure 14 from the E-ISAC's Physical Security Report shows, most physical security incidents are due to theft, vandalism, and intrusion. These physical incidents are much more likely than a physical attack.

Copper theft or vandalism have impacted the bulk power system and caused loss of life, which highlights the importance of perimeter controls that deny access. Rural facilities, including substations and renewable generation plants, have increased difficulty maintaining contiguous perimeter controls. These facilities often have unreliable network communications that prevent the use of an effective control to detect activity, or the unreliable network connectivity delays the transmission of video and alarm notifications to the security operations center.

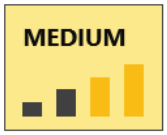
Additionally, deterrence is difficult at geographically expansive facilities, such as solar or wind farms, because a fence is difficult to maintain and monitoring all approaches may be cost prohibitive.

The risk has primarily manifested at individual substations, transmission lines, distribution lines, and generation plants. The impact to the bulk power system is dependent on the facility. Impact is limited on facilities with continuous staffing because these are typically not targeted by threat actors' intent on copper theft, intrusion, and vandalism.

NERC standard CIP-006 requires physical security plans for critical equipment supporting the bulk power system. This standard defines a physical security perimeter around critical facilities and establishes awareness of who is crossing that boundary. According to MRO industry experts, the standard does a moderate job of helping to mitigate this risk as the physical security controls are effective against threat actors looking to gain unauthorized access to facilities.

This risk was split from Physical Attacks in the 2024 RRA and redefined as the more frequent and lower impact variety of vandalism, theft, and intrusion. The likelihood of this risk occurring is Almost Certain due to extensive event history. Correspondingly, the potential impact of this risk on security of the regional bulk power system is Minor as it only impacts a single entity per incident.

Misoperations Due to Human Error



Impact: Minor

Likelihood: Possible

Protective relays are installed on facilities to isolate failed equipment and maintain grid reliability during disturbances. However, for a myriad of reasons, protective relays sometimes misoperate and either isolate more facilities than needed or do not isolate failed equipment as designed. MRO tracks and reports the causes of misoperations in both summer and winter regional assessments.

Misoperations due to human errors like incorrect settings, logic errors, design errors, or personnel as-left errors have ranged from 28% to 48% of all reported misoperations within the MRO footprint (shown in Figure 15). Misoperations due to human errors have been lower in the past two MRO seasonal assessments.

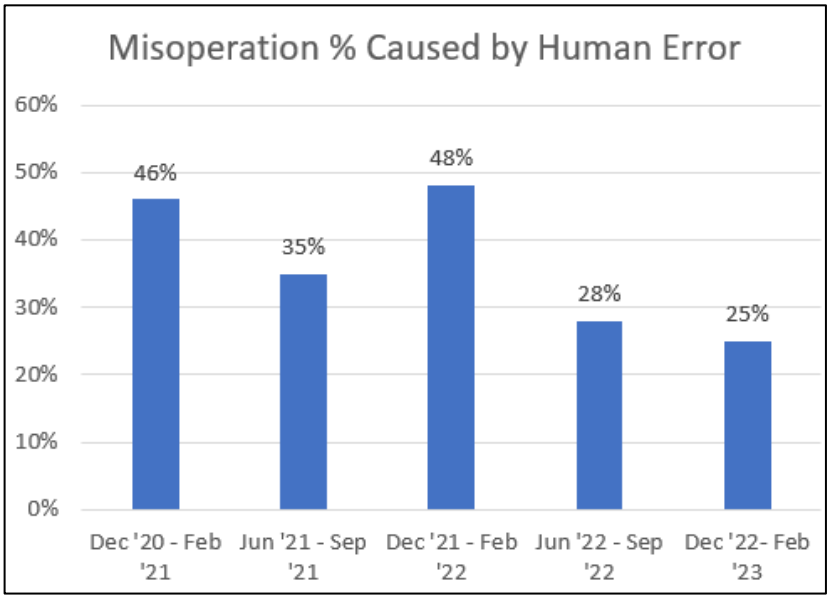


Figure 15: Misoperation % Caused by Human Error Reported by MRO Seasonal Assessments

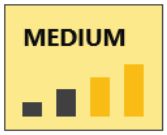
It is typical for additional facilities beyond the failed equipment to be isolated when protective relays misoperate, which broadens the impact to the larger areas of the grid and can cause unnecessary increased loss of load or generation.

There are several Protective Relay and Control (PRC) standards that provide a mix of low and moderately effective controls for this risk per an analysis performed by MRO's industry experts. PRC-004 aggregates misoperations for further analysis to help identify causes of misoperations and highlights human errors that can be addressed through human and organizational performance initiatives. CIP-005 provides an opportunity through normal maintenance intervals to verify correct relay settings and to develop corrective actions if settings are found to be in error. Lastly, PRC-019, 024, and 025 establish requirements for proper setting and coordination of relays that are the basis for testing programs to detect errors prior to the initial energization of transmission assets.

MRO held a webinar on July 14, 2022, on the Joint Review of Protection System Commissioning Programs report released by FERC and the ERO Enterprise. This webinar shared best practices for commissioning protective relays, which are often relied upon to identify incorrect installations of protective relays. The goal of the report is to help registered entities improve commissioning programs to decrease the number of misoperations that should be caught in the commissioning process. Improvements in design practices and other engineering solutions when establishing relay settings can also help to reduce human-error driven misoperations.

This risk was elevated from a Low priority in the 2023 RRA to a Medium priority in 2024. The risk was scored as having a Negligible (small or non-existent) impact on reliability of the regional bulk power system in previous reports. However, the potential impact was increased to Minor in 2024 to reflect the effect a misoperation can have on a local entity's bulk power system, including additional unnecessary facility outages that can limit power transfers or generation output. The likelihood portion of the risk score dropped slightly to Possible as transmission owners continue to improve relay design, installation, and commissioning practices.

Vulnerabilities of Unpatched Systems



Impact: Minor

Likelihood: Possible

Unpatched software or systems are a security vulnerability often exploited by threat actors and are the result of unavailability of a patch or failure to apply a patch. This may occur because of limited workforce resources, legacy unsupported devices, or the manufacturer not yet having released a patch. A survey by Tripwire in 2019 revealed that between 27% and 34% of organizations admitted they suffered a data breach due to unpatched vulnerabilities. Failure to patch vulnerabilities can lead to compromised industrial control systems, including protective relays and Energy Management Systems used to operate the bulk power system.

A series of attacks on the Danish power system in 2023 exploited an unpatched vulnerability on firewall equipment protecting industrial control systems that controlled the Danish grid. There was no direct impact to the grid in these attacks as the threat actors only accessed the firewalls and obtained configurations and credentials to attempt denial of service attacks that would shut down the firewall. Hackers did access industrial control systems behind the firewall but did not escalate the attack.

The impact of this risk is highly dependent on patch and vulnerability management programs and other mitigating controls that are already in place. Because of this, related events may affect a single organization (or system within that organization) or the wider bulk power system depending on the threat actor's targets.

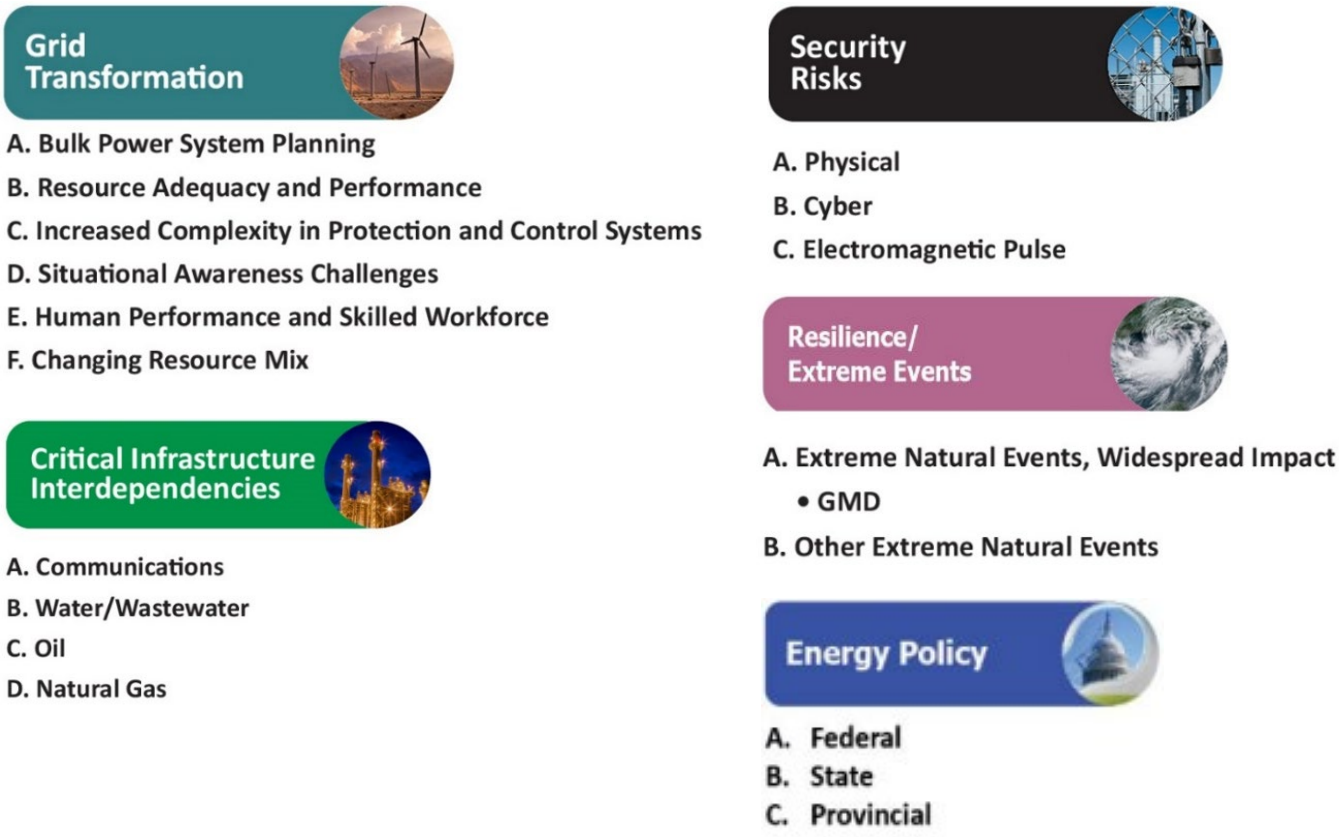
An analysis performed by MRO's industry experts indicates the NERC CIP-007 standard is moderately effective in addressing this risk. The standard requires entities to have patch management processes for important operational assets that control the bulk power system. This standard does not consider IT infrastructure that may be shared with operational systems for addressing vulnerabilities since it is not part of the bulk power system. Also, the 35-day window allowed to discover updated patches and an additional 35-day window to implement patches may be too long for critical control systems. The CIP-010 standard also requires vulnerability assessments

be conducted periodically to discover vulnerabilities. The 15-month periodicity requirement does not occur frequently enough to be a timely control for this risk. Like some of the other security risks, NERC's standard project on internal network security monitoring may help reduce risk by identifying unauthorized behavior within a system's network. More details on this project can be found in Section 8.

The likelihood of this risk occurring dropped slightly from the 2023 RRA but remains Possible for 2024. The impact of this risk on security of the regional bulk power system remains Minor since it would affect a single entity and affect the grid locally.

6. CORRELATION BETWEEN ERO-WIDE RISKS AND MRO REGIONAL RISKS

The 2023 ERO Reliability Risk Priorities Report (RISC Report)[1] highlights forward-looking risks to the North American bulk power system that merit attention and recommends actions to mitigate those risks. This biennial report consolidates the identified risks into five high level categories: 1) Grid Transformation, 2) Resilience to Extreme Events, 3) Security Risks, 4) Critical Infrastructure Interdependencies, and 5) Energy Policy.



The 2023 RISC report introduced Energy Policy as a new risk category. It recognizes that federal, provincial, state, and local policies are providing incentives and targets for resource changes and end-use applications of electricity that are impacting bulk power system reliability. These policies are accelerating the grid transformation as the industry grapples with how to maintain reliability during the transition.

[1] The charts and figures in this section were taken from the 2023 RISC Report and are shared with permission.

The Individiual risks highlighted in the 2023 RISC report were ranked by industry stakeholders from highest to lowest in Figure 16.

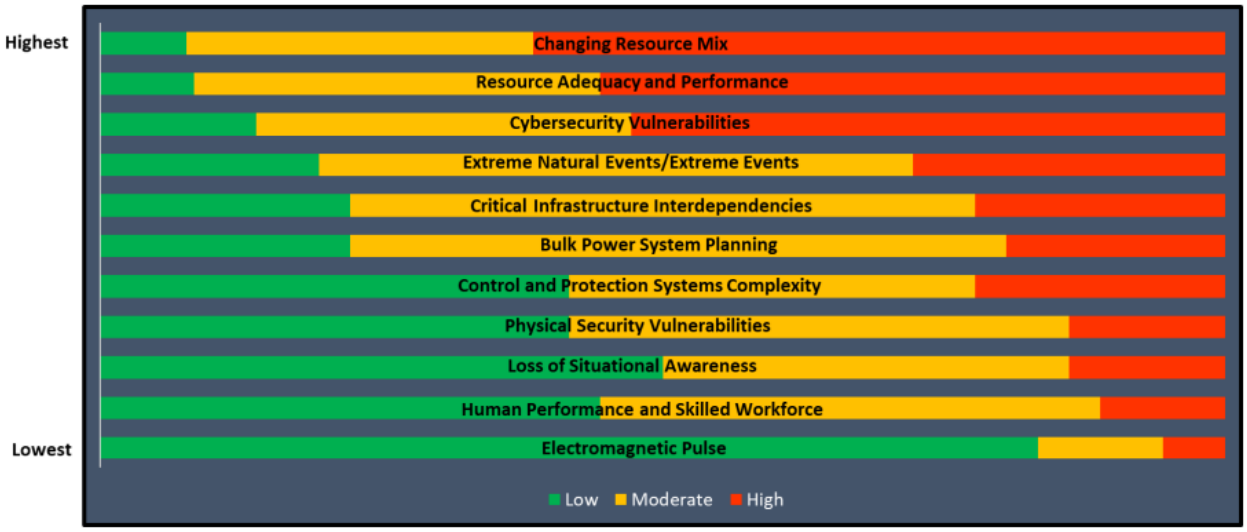


Figure 16: 2023 RISC Risk Rankings per the ERO-Wide Industry Stakeholder Survey

Figure 16 reveals that Changing Resource Mix, followed by Resource Adequacy and Performance, lead industry's perception on the criticality of these risks. The Resource Adequacy and Performance risk has steadily increased since 2021, with more industry stakeholders indicating this a high or moderate risk. Industry perception of the severity of this risk aligns with the 2024 RRA in that the closely related Uncertain Energy Availability was elevated to Extreme this year.

The Cybersecurity Vulnerabilities risk, which held the second spot in the 2021 RISC Report, dropped to third with stakeholders shifting their perception from a high risk to a moderate risk.

Figure 17 depicts the classification of the identified risks, based on the ranking. Risks identified as "manage" are emerging, imminent, and pose significant threats. Collaborative efforts across the industry continuum are needed to mitigate these complex challenges. Risks identified as "monitor" are of critical importance to bulk power system reliability but are managed with established industry practices.

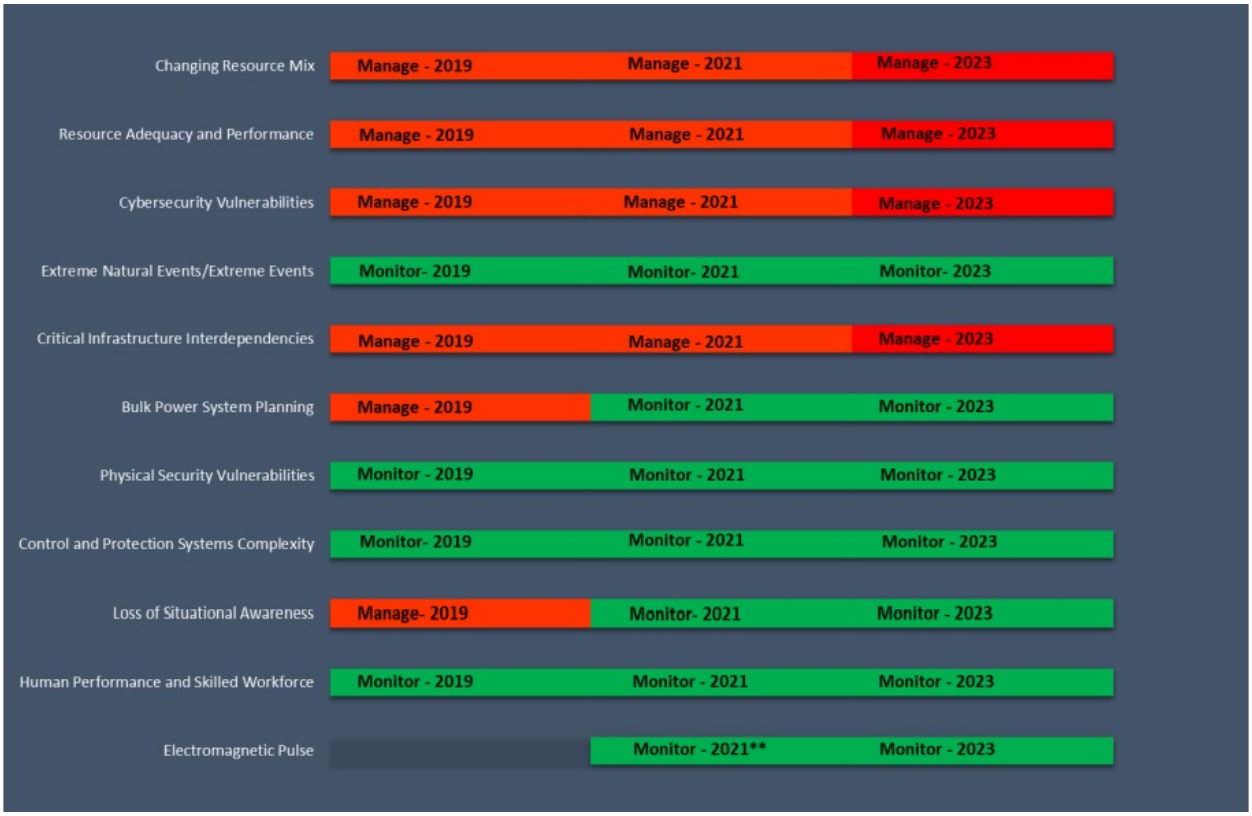


Figure 17: 2023 RISC Risk Rankings: Manage vs. Monitor

Figure 18 shows the correlation between the reliability and security risks identified in the 2023 ERO-wide RISC Report and the 2024 RRA. The regional risks identified in the RRA are more granular (as shown in the gray boxes) and are mapped to the ERO-wide risks in the colored boxes by RISC category. As can be seen, the results of the two analyses are complimentary to one another.

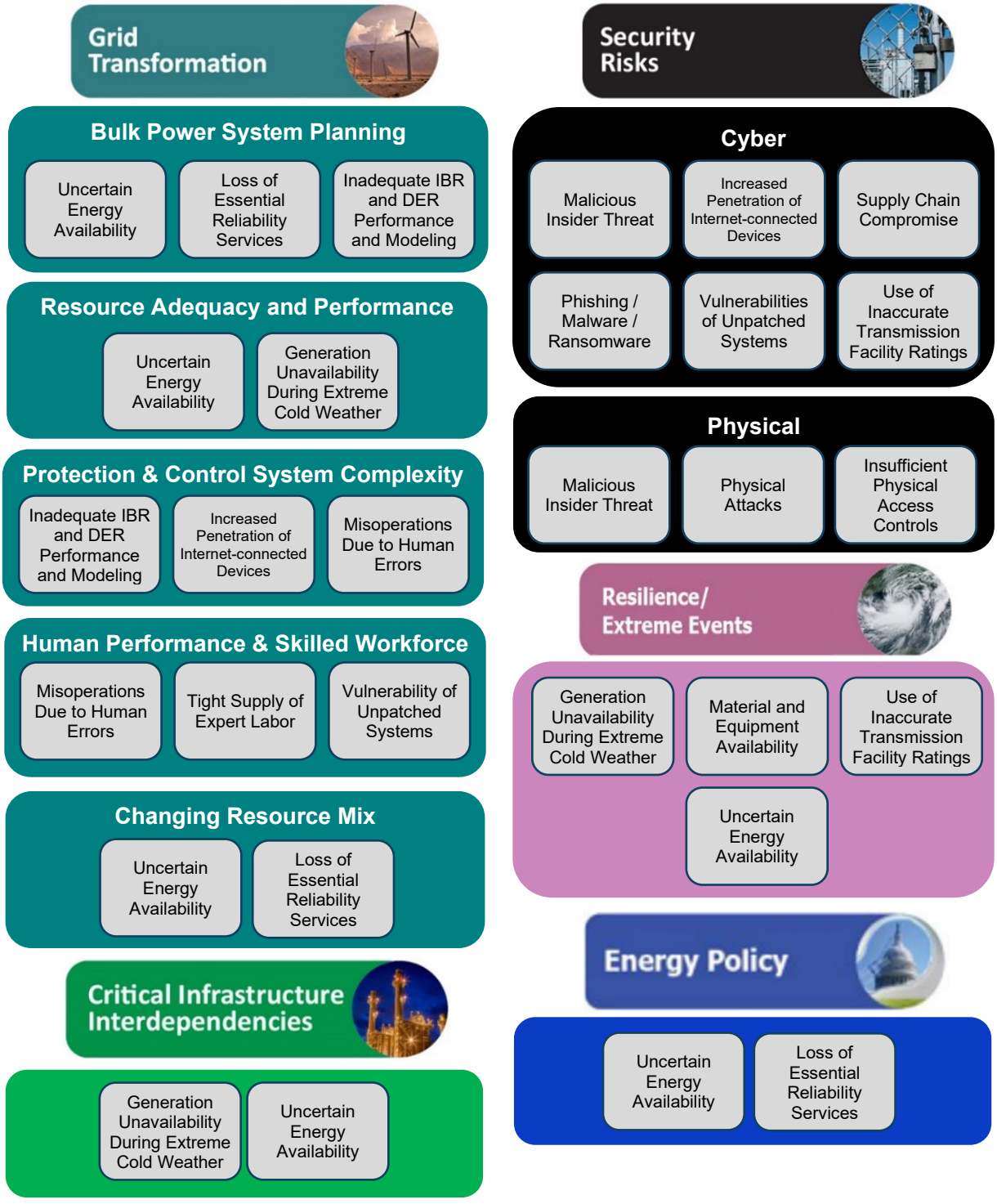


Figure 18: ERO and MRO Reliability Risks Correlation

7. GRID TRANSFORMATION TRENDS

Electric Load Growth and Uses

From a recent Grid Strategies, LLC report, electricity demand is forecast to grow by 4.7% over the next 5 years according to 2023 FERC filings by utilities. This is nearly double the 2.6% growth rate reported in 2022. Growth in demand is attributed to a surge in data centers and industrial development and electrification of transportation and buildings.

Electrification is the process of changing a device's power source to electricity. In the days of Thomas Edison, electrification was producing light via electricity versus traditional methods of gaslights and candles. Today, there is a strong decarbonization push to electrify transportation and space heating.

Electrification of transportation and space heating will have profound effects on the electric demand served by utilities' load shapes (daily and seasonal) are also likely to change and be less predictable. The use of electric heat pumps to heat homes and businesses could shift some peak loads from the summer to the winter season. Charging large numbers of electric vehicles at different times of the day adds to future demand uncertainty.

The increased load variability further complicates the balance between supply and demand. That said, greater electrification presents an opportunity to leverage demand-side management tools to maintain system balance. Systems and incentives to use electricity (i.e., charge electric vehicles) during periods where supply is abundant can help offset the challenges with variable resources.

Grid Forming Inverters

Managing the abundance of inverter-based resources is becoming increasingly more challenging for grid planners and operators. Most inverter-based resources interconnected with the grid deploy "grid-following" technology that is heavily dependent on a strong voltage and frequency reference source, which today is provided by conventional, large synchronous machines providing inertia to the system. As the future grid is expected to rely less upon large synchronous machines, a strong voltage and frequency source is not assured to allow grid following inverter-based resources to continue to operate normally.

"Grid-forming" inverters improve upon grid-following inverters in that they provide a voltage and frequency source into the grid, instead of relying on the grid to provide a reference. These resources adjust power and voltage output in response to grid conditions to support reliability. Grid following inverters can be configured to mimic the inertial response of synchronous machines and provide frequency response through grid disturbances. They also have the capability to restore the system from a blackout since they produce a voltage and frequency reference for other resources to synchronize with. While these are benefits to grid-forming inverters, there are also challenges with coordinating these inverters with existing resources to avoid creating unstable conditions. Further, there is no standard for the control methodology of these resources and desired behavior defined for how they are expected to respond to changing grid conditions.

Hybrid Facilities

As battery technologies and other energy storage options mature and related capital costs decline, storage technologies will be combined with renewable resources to form hybrid resources. The energy output of a renewable resource can be directed to the grid or to charging batteries located onsite at the renewable facility. The battery can then be discharged during periods of low wind speeds or at night to supplement solar power. This operating flexibility increases resource availability for the bulk power system. Battery storage can also provide essential reliability services (ERS), such as voltage support, frequency response, and system inertia, to replace the ERS that synchronous resources typically provide. The storage of variable resource output will facilitate better management of the increasing penetration of renewable energy and is necessary to maintain reliability of the bulk power system. Hybrid resources have started to populate the interconnection queues. Figure 19 shows the MW amount of hybrid resources entered the interconnection queues ERO-wide.

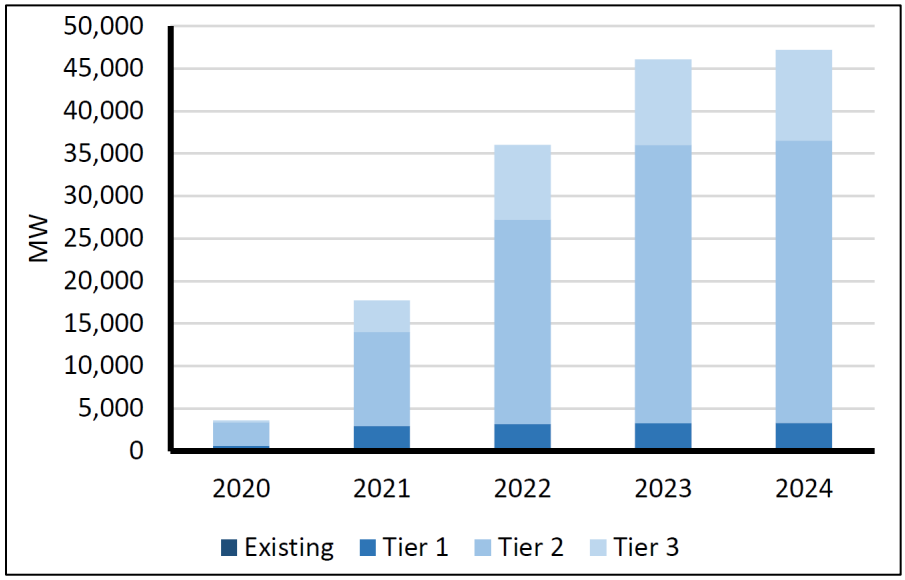


Figure 19: NERC-Wide Hybrid Resources in Generation Queues

Participation of Aggregated DER in RTO Markets

FERC issued a final rule (Order 2222) on September 17, 2020, that requires Regional Transmission Organizations (RTOs) to revise their tariffs to facilitate the participation of distributed energy resource (DER) aggregations in organized wholesale electric markets. Participation in markets streamlines possibilities for this growing asset class to help address resource adequacy challenges by allowing large-scale dispatch of DERs under normal and emergency conditions. Aggregated DERs can be a mix of energy supply and load resources that enable load reduction, generation supply, or both, to respond to imbalance conditions on the grid.

Much of today's DERs net with load and blur the utilities and RTO's ability to accurately forecast load. Another benefit of Order 2222 is that it provides RTOs visibility into the capabilities and performance of DER by requiring certain information, data, metering, and telemetry. This will make it easier to separate DERs from traditional loads, therefore improving future load forecasting. Impacts of changing weather patterns on DERs will also be better understood with an increase in the data available. Information obtained through the aggregated DERs will be incorporated into bulk power

planning models which will improve their accuracy and assessment capabilities to understand the impact of DER on transmission power flows.

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 on their own roof or property. This physical aggregation of DERs allows the local utility to provide real-time data to the RTO. Aggregated DERs will also likely include Demand Side Management programs, such as price-based or time-of-day electric vehicle charging, further providing operational flexibility to manage real-time operations.

RTOs are proactively collaborating with states and members in their respective footprints to prepare for FERC Order 2222. MISO has developed a public document titled MISO and DER: Ensuring Grid Reliability Through Visibility and Communication that provides a comprehensive discussion on this topic.

Small Modular Reactors

A newer type of nuclear power technology called small modular reactors (SMRs) is under development in a range of countries, including the U.S., Canada, South Korea, Argentina, and several countries in Europe. The U.S. government has not yet approved the reactors, but U.S. national labs are actively participating in research and development of this new technology. SMRs have been hailed as a way the U.S. could help boost the nation's production of nuclear power, which emits no carbon dioxide, and provides operational flexibility that is similar to current baseload units (coal, oil) that are being retired.

Since SMRs are modular, they can be manufactured off site and then shipped to a location for installation. This modular aspect is expected to reduce manufacturing time as well as the cost of the units. Typically, each modular reactor is expected to range from about 30 to 300 MW and could be grouped together to form a larger power plant. These units would have fast-ramping and load following capabilities, which would work well with variable generation and help ensure energy adequacy throughout the entire year.

Safety is a major focus of SMR development. Traditional reactors use pumps to maintain a constant flow of water to cool their cores and are equipped with backup diesel generators to keep that process going in the event of a power outage. SMRs rely on the natural forces of heating and cooling that combine with gravity to circulate water through its system, eliminating the need for pumps as a failure point, in addition to multiple layers of safety features.

The Nuclear Regulatory Commission (NRC) certified the first SMR design in February 2023 and is reviewing several other SMR designs. NRC approval is required before a manufacturer can license its design for construction. This clean, synchronous, fast-ramping resource has the potential to significantly improve the reliability of the bulk power system. However, there are challenges with the costs to affordably construct this type of resource.

Storage as a Transmission-Only Asset

Batteries can also be used as a transmission asset on the bulk power system. In this application, the primary use of the battery is not to supply energy to the grid but to mitigate a transmission performance issue like voltage stability or thermal overload. Batteries can be installed more quickly and economically than traditional wire reinforcements and with fewer issues related to permitting and easements than building new overhead transmission lines. Storage as a transmission-only asset is limited to solving performance issues that occur for only brief periods of time (only a few hours) due to the limited discharge capability of batteries.

An RTO like MISO or SPP will have functional control of the asset to address transmission issues, like any other transmission asset. An operating guide would be developed for each storage unit as transmission-only asset specifying operating use consistent with the need identified in the RTO's regional transmission planning process. The owner of the storage asset would follow RTO instructions regarding the state of charge of the battery and charging/discharging cycles. In the right scenario, storage as a transmission-only asset brings increased reliability to an area faced with a short duration challenge in a cost-effective manner.

8. COMPLIANCE ACTIVITIES ADDRESSING RISKS

The following section discusses Compliance Monitoring and Enforcement Program (CMEP) activities related to the highest risks identified in the 2024 RRA. NERC prioritized each of the following projects in 2023 to focus on initiatives with the greatest impact on reducing risk to the bulk power system. High priority projects are targeted for completion in 2024. Medium and low priority projects would be completed in 2025 and beyond, respectively. The priority of each project is referenced below to provide clarity on expected project completion.

NERC Project 2020-02 Modifications to PRC-024 (Generator Ride-through) – HIGH priority

A Standard Authorization Request (SAR) has been drafted to retire the PRC-024-3 standard and replace it with a performance-based ride-through standard that ensures generators remain connected to the bulk power system during system disturbances. This SAR is the result of numerous system events related to the Inadequate IBR and DER Performance and Modeling risk presented in this RRA. These events indicate that standard PRC-024-3, which focuses on voltage and frequency protection, is not adequate to address the tripping and output reductions of inverter-based resources. The new standard proposed goes beyond voltage and frequency protection settings to include any generator protection or control system that could result in the reduction or disconnection of a generating resource during a system disturbance. A draft standard has not been posted yet for industry review. The NERC Standards Committee accepted a waiver to reduce the formal comment and ballot periods to expedite the standard review process.

Information relating to this project can be found at Project 2020-02 Modifications to PRC-024.

NERC Project 2020-06 Verifications of Models and Data for Generators – MEDIUM priority

A review by the NERC Inverter-based Resource Performance Task Force (IRPTF) in 2020 found that the MOD-026-1 and MOD-027-1 standards are not applicable to inverter-based resources. A SAR was developed to revise these standards to clarify requirements related to IBRs and require sufficient model verification to ensure accurate representation of IBR dynamics. Multiple drafts of the MOD-026 standard have been posted for balloting and comment, with the latest draft garnering 44% approval. This project will help address the Inadequate IBR and DER Performance and Modeling risk by providing clarity to Generator Owners on modeling parameters that are necessary to be validated and provided to Transmission Planners to accurately depict bulk power system dynamic response.

Information relating to this project can be found at Project 2020-06 Verifications of Models and Data for Generators.

NERC Project 2021-07 Extreme Cold Weather Grid Operations, Preparedness, and Coordination – HIGH priority

This project was created in 2021 in response to the findings from the FERC, NERC, and Regional Entity Joint Staff Inquiry into the February 2021 Cold Weather Grid Operations report and relates to the Generation Unavailability During Extreme Cold Weather risk. This project has been broken into multiple phases. Phase 1 culminated on February 16, 2023, when FERC approved the revised EOP-011-3 and a new EOP-012-1 standard with an effective date of November 1, 2024. FERC directed NERC to develop further modifications in the EOP-012-1 standard to clarify ambiguous requirements

and provide modifications to FERC within 12 months. NERC has prioritized subsequent drafts of the EOP-012-2 standard to meet this deadline.

Phase 1 of this project moves newly added Generation Owner/Operator requirements from EOP-011-2 to a new standard, EOP-012-1. The new standard requires Generator Owners to implement freeze protection measures to operate at a defined extreme cold weather temperature for the unit for a specified continuous duration depending on the commercial operation date of the unit. Generator Owners will also be responsible for calculating the extreme cold weather temperature every five years and updating their preparedness plans or creating correction action plans accordingly based on the new calculated temperature.

These requirements should help mitigate the Generation Unavailability During Extreme Cold Weather risk by setting clear expectations of winter generation performance and mandating action plans to address any deficiencies.

Information relating to this project can be found at Project 2021-07 Extreme Cold Weather Grid Operations, Preparedness, and Coordination.

NERC Project 2022-02 Modifications to TPL-001-5.1 and MOD-032-1 – LOW priority

This project includes a series of SARs that address the impacts of the rising number of inverter-based resources and distributed energy resources on planning assessments. This project helps to address the Inadequate IBR and DER Performance and Modeling risk. Both the NERC IRPTF and System Planning Impacts from Distributed Energy Resources Working Group (SPIDERWG) contributed SARs to this project.

The IRPTF SAR for TPL-005-5.1 recommends language changes to include the uniqueness of inverter-based resources in planning assessments. The SPIDERWG SAR for TPL-001-5.1 targets the need to consider the performance of DER, in particular dynamic behavior, to ensure accuracy of transmission planning assessments. Subsequently, the SPIDERWG SAR for MOD-032-1 seeks to address gaps in data collection to adequately model aggregate levels of DERs in planning assessments.

There have been two rounds of drafts for the MOD-032-2 standard changes, with the latest ballot reaching 40% approval. There has been no draft put forward for TPL-001.

Information relating to this project can be found at Project 2022-02 Modifications to TPL-001-5-1 and MOD-032-1.

NERC Project 2022-03 Energy Assurance with Energy-Constrained Resources – HIGH priority

NERC published a whitepaper in December 2020 entitled Ensuring Energy Adequacy with Energy Constrained Resources that highlighted the need for a new method of assessing resource adequacy to ensure energy availability for all hours of the year. This project was born from that whitepaper and includes two SARs–one for the planning horizon and one for the operations/operations planning horizon. Both SARs have the same objective to require entities to perform reliability assessments evaluating energy assurance by analyzing the expected resource mix availability and fuel availability. The intent of the project is to create a consistent approach for how to conduct these analyses. This project addresses the Uncertain Energy Availability risk.

A first draft of the Transmission Operations (TOP) standard relating to this project was posted for comment in September 2023. A subsequent draft of the standard was posted on January 25, 2024, to address initial comments and modify the standard designation to BAL-007. An initial ballot is scheduled for March 1, 2024. A standard for long-term planning of the system is under development and will follow the operations standard.

Information relating to this project can be found at Project 2022-03 Energy Assurance with Energy-Constrained Resources.

NERC Project 2023-03 Internal Network Security Monitoring (INSM) – HIGH priority

FERC issued Order 887 in January 2023 that directs NERC to develop requirements for internal network security monitoring. This project is the result of that order and is intended to provide requirements to detect unauthorized activity within a network of a high impact BES Cyber System and medium impact BES Cyber Systems with external routable connectivity. This will allow for detection of a cyber-attack if network perimeter controls are bypassed. This will help mitigate a myriad of security risks but can be the most valuable for the Malicious Insider Threat and Supply Chain Compromise risk.

Information relating to this project can be found at Project 2023-03 Internal Network Security Monitoring (INSM).

FERC Order 881

FERC issued Order 881 in December 2021 to improve the accuracy and transparency of transmission line ratings. A subsequent order, Order 881-A, issued in May 2022 clarified the original order but left the main tenets intact. At the center of Order 881 is the requirement to implement ambient-adjusted ratings and seasonal ratings, as well uniquely determined emergency ratings. This order directly addresses the Use of Inaccurate Transmission Facility Ratings risk. Utilities will have until 2025 to develop and document their programs to comply with Order 881.

9. CONCLUSION

The 2024 RRA assesses key risks from North American-wide assessments and reports to determine which risks would have a greater impact or be more likely to occur within the MRO region. The culmination of insights shared in this report represents a significant amount of collaboration and coordination across multiple industry stakeholders.

Eight top risks were identified in this report. The one Extreme priority risk, Uncertain Energy Availability, underscores the need for timely action to redefine how the bulk power system is planned and operated as the electric generation fleet and energy use transforms. This is the first time in the report's history that a risk has risen to the Extreme designation. The seven High priority risks represent a mix of different, important challenges to the reliability of the bulk power system.

Common risk themes are:

- **Ongoing grid transformation** is retiring conventional generation in favor of inverter-based resources that behave much differently and are less energy dense.
- **Global and domestic conflicts** threaten cyber and physical security of the bulk power system and have potential to disrupt normal operations.
- **Longer duration extreme weather** presents significant challenges to grid operating conditions and both the supply and delivery of power.

MRO will continue to play a key role in studying, understanding, and communicating the reliability impacts associated with these challenges.

The 2024 RRA supports MRO's mission to identify, prioritize and assure effective and efficient mitigation of risks to the reliability and security of the North American bulk power system within the region. It establishes the foundation for MRO's risk monitoring and mitigation work and ensures we focus both our and industry resources on the risks that are most critical.

10. REFERENCES

1. MRO Reliability Risk Matrix
   https://www.mro.net/document/mro-reliability-risk-matrix-2021/
2. 2023 ERO Reliability Risk Priorities Report
   https://www.nerc.com/comm/RISC/Related%20Files%20DL/RISC_ERO_Priorities_Report_2023_Board_Approved_Aug_17_2023.pdf
3. 2023 NERC State of Reliability Technical Assessment
   https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2023_Technical_Assessment.pdf
4. 2023 NERC Long-Term Reliability Assessment
   https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_LTRA_2023.pdf
5. NERC Event Analysis Program
   https://www.nerc.com/pa/rrm/ea/Pages/EA-Program.aspx
6. 2023 MRO Regional Summer Assessment
   https://www.mro.net/document/mro-2023-regional-summer-assessment/?download
7. 2023/2024 MRO Regional Winter Assessment
   https://www.mro.net/document/mro-2023-regional-winter-assessment/?download
8. NERC-WECC Joint Report on Inverter-based Resource Modeling Report
   https://www.nerc.com/comm/PC/InverterBased%20Resource%20Performance%20Task%20Force%20IRPT/NERC-WECC_2020_IBR_Modeling_Report.pdf
9. NERC 2023 Summer Reliability Assessment
   https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_SRA_2023.pdf
10. NERC 2023-2024 Winter Reliability Assessment
    https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_WRA_2023.pdf
11. 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
12. NERC/FERC/RE February 2021 Cold Weather Outages in Texas and the South Central United States Report
    https://www.ferc.gov/media/february-2021-cold-weather-outages-texas-and-south-central-united-states-ferc-nerc-and
13. NERC/FERC/RE December 2022 Winter Storm Elliott Report
    https://www.ferc.gov/media/winter-storm-elliott-report-inquiry-bulk-power-system-operations-during-december-2022
14. MRO Generator Winterization Program
    https://www.mro.net/program-areas/reliability-analysis/generator-winterization-program/
15. NERC Security Guideline on Product Security Sourcing Guide
    https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Product%20Security%20Sourcing%20Guide.pdf
16. NERC Security Guideline on Risk Considerations for Open Source Software
    https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Risk_Considerations_Open_Source_Software.pdf

17. NERC Security Guideline on Supply Chain Secure Equipment Delivery https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Risk_Considerations_Open_Source_Software.pdf
18. NERC Security Guideline on Vendor Risk Management Lifecycle https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Vendor_Risk_Management_Lifecycle.pdf
19. NERC Security Guideline on Cyber Security Risk Management Lifecycle https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Cyber_Security_Risk_Management_Lifecycle.pdf
20. MRO Risk Assessment and Mitigation (RAM) Conference Materials https://www.mro.net/event/2023-mro-hybrid-ram-conference/
21. Joint NERC and Texas RE Staff Report on the Panhandle Wind Disturbance https://www.nerc.com/pa/rrm/ea/Documents/Panhandle_Wind_Disturbance_Report.pdf
22. Reliability Perspectives on the Adoption of IEEE 1547-2018, Midwest Reliability Matters article, June 12, 2023 https://www.mro.net/reliability-perspectives-on-the-adoption-of-ieee-1547-2018/
23. NERC Reliability Guideline on Bulk Power System Reliability Perspectives on the Adoption of IEEE 1547-2018 https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Guideline-IEEE_1547-2018_BPS_Perspectives_PostPubs.pdf
24. NERC Introduction to Inverter-based Resources on the Bulk Power System https://www.nerc.com/pa/Documents/2023_NERC_Guide_Inverter-Based-Resources.pdf
25. FERC, NERC, and RE Joint Review of Protection System Commissioning Programs https://www.ferc.gov/sites/default/files/2021-11/Protection%20System%20Commissioning%20Program%20Review%20Project.pdf
26. NERC Inverter-based Resource Strategy Document https://www.nerc.com/comm/Documents/NERC_IBR_Strategy.pdf
27. FERC Order 2023 Improvements to Generator Interconnection Procedures and Agreements https://www.ferc.gov/media/e-1-order-2023-rm22-14-000
28. FERC/NERC Joint Technical Conference Regarding Physical Security of the Bulk Power System https://www.ferc.gov/news-events/events/joint-technical-conference-regarding-physical-security-bulk-power-system
29. Enhancing Physical Security for Critical Substations, Midwest Reliability Matters article, August 31, 2023 https://www.mro.net/enhancing-physical-security-for-critical-substations/
30. Understanding Insider Threats, Midwest Reliability Matters article, May 5, 2023 https://www.mro.net/understanding-insider-threats/
31. Insider Threats Remain a High Priority, Midwest Reliability Matters article, November 17, 2023 https://www.mro.net/insider-threats-remain-a-high-priority/
32. NERC whitepaper on Essential Reliability Services https://www.nerc.com/comm/Other/essntlrlbltysrvcstskfrcDL/ERSWG_Sufficiency_Guideline_Report.pdf

33. NERC CMEP and ORCP Quarterly Report, Q3 2022 https://www.nerc.com/pa/comp/CE/ReportsDL/Q3%202022%20Quarterly%20CMEP%20and%20ORCP%20Report.pdf
34. FERC Order 881 Managing Transmission Line Ratings https://www.ferc.gov/news-events/news/ferc-rule-improve-transmission-line-ratings-will-help-lower-transmission-costs
35. ERO Enterprise Themes and Best Practices for Sustaining Accurate Facility Ratings https://www.nerc.com/comm/RSTC/Documents/ERO%20Enterprise%20Themes%20and%20Best%20Practices%20for%20Sustaining%20Accurate%20FR%20-%20Final%20-%20Oct-20-22.pdf
36. MRO Reliability Conference Materials https://www.mro.net/event/2023-mro-hybrid-reliability-conference/
37. U.S. Bureau of Labor Statistics Job Openings and Labor Turnover Survey https://www.bls.gov/jlt/
38. Cyber Seek Interactive Job Openings Heat Map https://www.cyberseek.org/heatmap.html
39. MRO Protective Relay Subgroup Webinar on Protection System Commissioning https://www.mro.net/event/mro-protective-relay-subgroup-webinar-on-protection-system-commissioning/
40. NERC Reliability Guideline on BESS and Hybrid Power Plant Performance Modeling Studies https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Reliability_Guideline_BESS_Hybrid_Performance_Modeling_Studies_.pdf
41. The Era of Flat Power Demand is Over, Grid Strategies Report, December 2023 https://gridstrategiesllc.com/wp-content/uploads/2023/12/National-Load-Growth-Report-2023.pdf
42. FERC Order 2222 Participation of DER Aggregations in Markets Operated by RTOs and ISOs https://www.ferc.gov/news-events/news/open-access-order-no-2222
43. MISO and DER: Managing Grid Reliability through Transparency and Communication https://cdn.misoenergy.org/MISO%20and%20DER%20-%20Visibility495365.pdf
44. Compliance Monitoring and Enforcement Program and Organization Registration and Certification Program Quarterly Report – Q3 2022 https://www.nerc.com/pa/comp/CE/ReportsDL/Q3%202022%20Quarterly%20CMEP%20and%20ORCP%20Report.pdf
45. Sektor Cert Report on Danish Critical Infrastructure https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/sektorcert-the-attack-against-danish-critical-infrastructure-tlp-clear.pdf
46. Tripwire article, Unpatched Vulnerabilities Caused Breaches in 27% of Orgs, Finds Study Unpatched Vulnerabilities Caused Breaches in 27% of Orgs, Finds Study | Tripwire
47. Project 2020-02 Modifications to PRC-024
48. Project 2020-06 Verifications of Models and Data for Generators
49. Project 2021-07 Extreme Cold Weather Grid Operations, Preparedness, and Coordination
50. Project 2022-02 Modifications to TPL-001-5-1 and MOD-032-1

51. Project 2022-03 Energy Assurance with Energy-Constrained Resources
52. Project 2023-03 Internal Network Security Monitoring (INSM)