Public

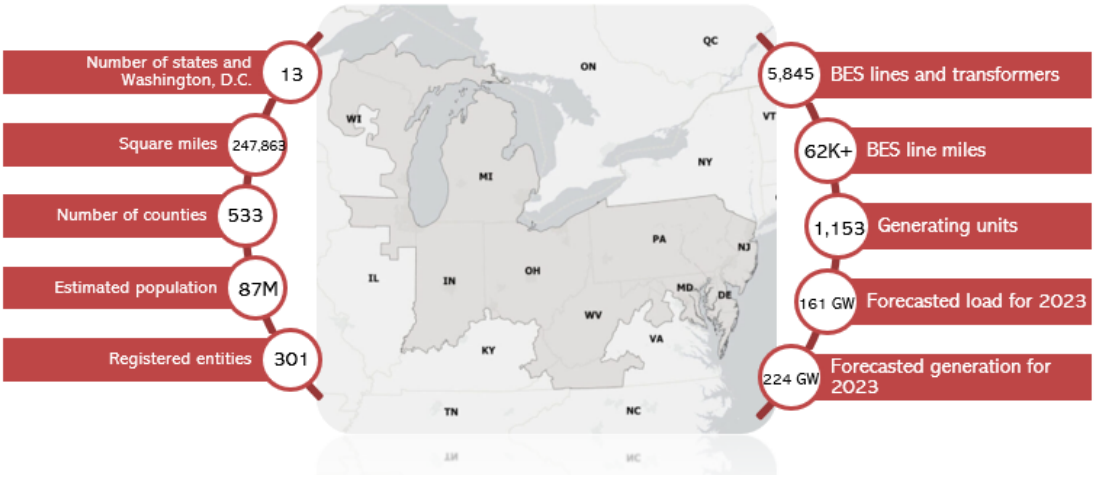
RELIABILITYFIRST

REGIONAL RISK ASSESSMENT

2023-24

3 Summit Park Dr, Ste 600
Cleveland, OH 44131
216-503-0600
rfirst.org

ABOUT RELIABILITYFIRST



ReliabilityFirst (RF) is one of six regional organizations responsible for ensuring the reliability and security of the North American Bulk Electric System (BES). Under the authority of the North American Electric Reliability Corporation (NERC) and the Federal Energy Regulatory Commission (FERC), we audit utility companies on mandated standards related to cyber security, operations, preparation for extreme weather and more. We work in tandem with NERC and the five other regions, MRO, NPCC, SERC, Texas RE and WECC (known collectively as the ERO Enterprise), toward this shared mission. This framework was born out of the Energy Policy Act of 2005, which followed the 2003 Northeast Blackout.

We are responsible for the reliability, security, and resilience of the BES in the Great Lakes and Mid-Atlantic areas of the United States of America. This region is situated within the Eastern Interconnection, and we regulate both PJM and MISO, which are the regional transmission organizations in our footprint.

ABOUT THE RRA

Our Regional Risk Assessment (RRA) summarizes and analyzes the eight greatest risks in our region that we identified in collaboration with industry stakeholders on our technical committees and subcommittees. We also examine how some of these risks can increase when they occur simultaneously and in the infographic accompanying this report we explore how the transforming electric grid is impacting how these risks interrelate.

Why we do an RRA

The goal of our RRA is to identify, analyze, and prioritize broad risk categories that impact the reliability, security, and resilience of the bulk power system (BPS) within our unique footprint. The output from the RRA informs our future work to mitigate these risks through our tools, processes, outreach and educational efforts (i.e., compliance, assist visit program, workshops, etc.).

It is designed to supplement the risk identification work done across the Electric Reliability Organization (ERO) Enterprise, including the NERC ERO Reliability Risk Priorities Report, which identifies ERO-wide risk profiles and areas of focus. RF uses the Reliability Risk Priorities Report as an input and also to confirm that

our results are in alignment with ERO work plans and strategies. The ERO-based risks are reviewed and analyzed from a regional perspective to identify region-specific risks and priorities.

We use the information to support and inform our operational plans and goals, but our RRA remains independent from entity-specific compliance monitoring and enforcement activities.

Why we share these results

The assessment of the top risks in our footprint and their relationships has been a beneficial tool for our decision making and work prioritization and we hope it will engage and inform our stakeholders and the communities in our region and offer deeper insight into the risks facing our footprint and their interrelatedness. While there are many unknowns, we know that the complex challenges of the future require collaboration and broad industry expertise and we aim to be transparent with our risks to keep key decision makers informed as we seek solutions.

Considerations for each risk

The detailed analysis of each risk is unique, and includes in its analysis four common considerations for each risk: Human Performance, Policy & Standards, Resilience, and Uncertainty. Throughout the document we spotlight one of these key considerations for each risk.

Human Performance
The capability of the workforce to complete the tasks associated with a given risk. This includes consideration of established processes and procedures, training, and capability to mitigate human error, as well as skilled workforce retention and retirements.

Policy & Standards
The implementation of rules and regulations at federal, state, and local levels that directly or indirectly impact the reliability of the Bulk Power System. This includes the NERC Reliability Standards.

Resilience
The ability to anticipate, absorb, adapt to, minimize the impact of, and/or rapidly recover from a potentially disruptive event.

Uncertainty
The confidence level associated with the overall evaluation of risk. This includes the availability of data to perform analysis, the quality of the data available, the level of expertise held by the risk analysts, and consideration of external sources that could indirectly impact risk.

Public

ENVIRONMENTAL FACTORS

Environmental Factors is a broad risk meant to include naturally occurring phenomena, such as extreme weather and vegetation related issues. The geographic location of the RF footprint makes it susceptible to a wide variety of environmental factors. The risk continues to increase as cold weather events cause generation outages.

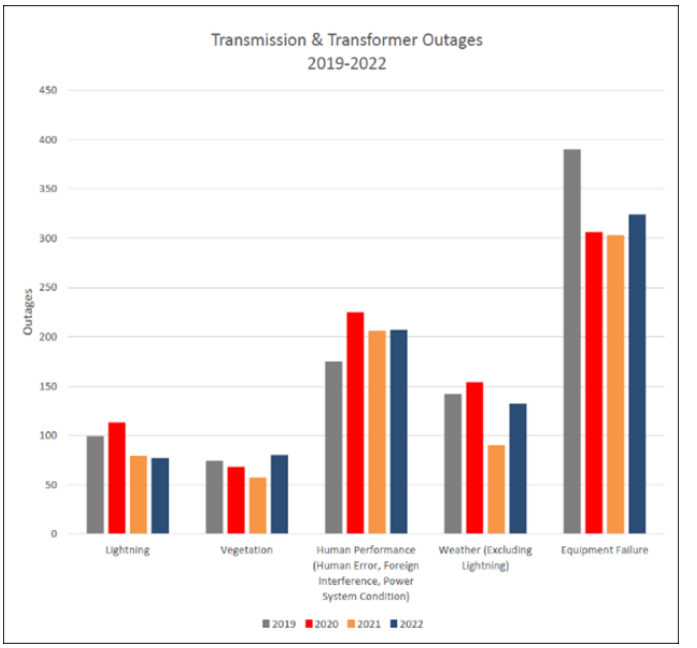
POLICY & STANDARDS

NERC is enhancing and modifying Reliability Standards related to cold weather (EOP-011, EOP-012, IRO-010, TOP-003, and TOP-005). NERC also issued a Level 3 Essential Actions alert in 2023 focused on cold weather preparations. This was the first time NERC has used this highest severity level.

There were five cold weather events in the past 11 years across North America that resulted in substantial generation unavailability or firm load shed. The most notable of these events in the RF footprint was Winter Storm Elliott, where PJM and MISO both experienced a large amount of generation outages, derates, or failures to start. RF supported the FERC and NERC joint inquiry report that followed with several recommendations to improve cold weather reliability, including standards revisions and improved gas-electric coordination and communication.

RF's plant winterization visits have proven to be effective for generation performance. NERC identified elevated risk for extreme weather events in both PJM and MISO in its 2023-2024 Winter Reliability Assessment, which RF has been monitoring closely.

Weather in the RF footprint poses a larger risk to the availability of generation resources, however it also impacts the availability of transmission lines and transformers. Although RF has the lowest outage frequency across North America, weather is one of the top causes of those outages. Lightning, weather, and vegetation accounted for 33% of transmission outages within the RF footprint over the last five years, which is almost as high as the 35% of outages caused by equipment failures. RF is continuing to monitor these outages, including the slight uptick in duration despite a multi-year downward trend. RF also offers a Vegetation Management Community of Practice to help mitigate the risk and plans to obtain more detailed data around equipment failure related audits and explore additional sources of weather data.



Public

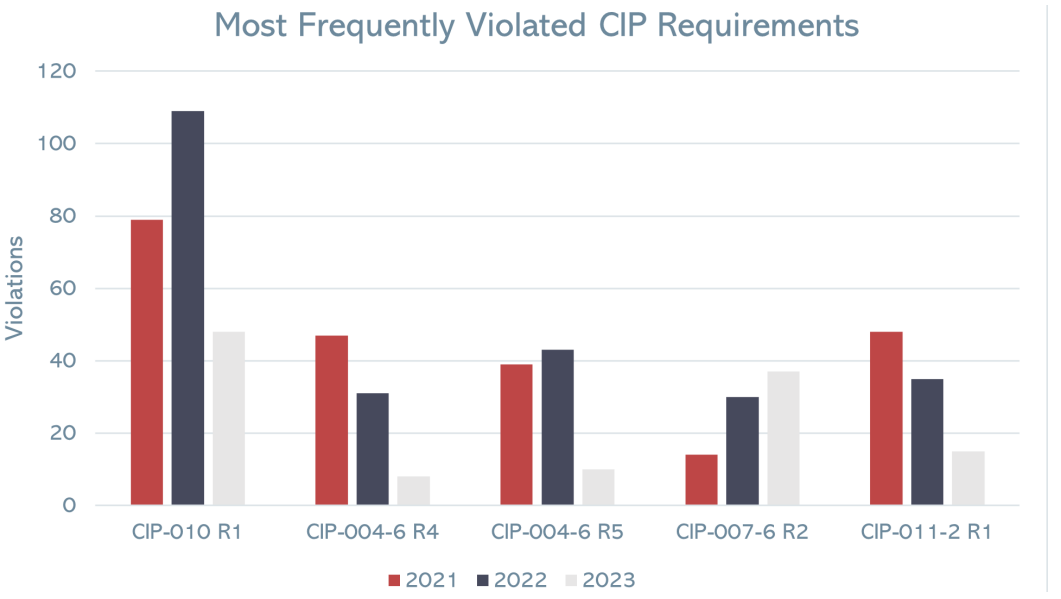
CYBER SECURITY

RESILIENCE

For cyber security risks, each asset is reviewed by registered entities for threats and vulnerabilities to ensure a holistic and redundant approach is implemented. RF offers an in-house tool to assess cyber resilience within an organization and identify performance gaps with recommendations for improvement. This tool has helped various entities review and improve their cyber resilience posture.

Cyber Security risk involves the compromise of information and operational technology systems that support, monitor and control the electric grid. Threats from this risk can range from a variety of sources including hackers, state-sponsored groups, or even disgruntled employees (i.e., insider threats). The potential impact of a successful attack could range from theft of data to widespread loss of end-use customer demand (i.e., blackouts).

Cyber security has consistently been considered a high risk. RF reviews compliance data to look for trends, including for example, most frequently violated NERC Reliability Standards and Requirements and changes in risk levels for noncompliance of specific standards and requirements. For the CIP Standards shown on the chart below, 97% of the violations are self-reported by the entities. Our footprint has a large number of CIP violations, and while a few standards showed a slight downward trend, RF is monitoring the increasing trend for CIP-007-6, Requirement 2, which covers executing documented processes to implement security patches on CIP high- and medium-classified assets.



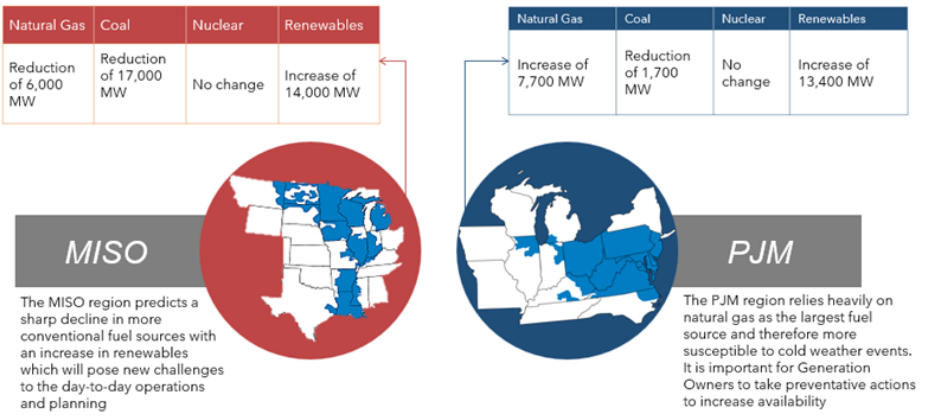
RF will continue to monitor these metrics through its compliance and mitigation efforts. RF is also focusing on vulnerability management, including patch management outreach and a recent focus on the window of vulnerability. RF is working to better understand how entities define and implement layered security measures during the period after a vulnerability is discovered and before the related vendor patch is deployed and plans to share internal controls and best practices to mitigate this risk.

Public

CHANGING RESOURCE MIX

Changing Resource Mix is a complex risk category that addresses the fact that public inputs, along with the influence of regulatory and socio-economic policies, continue to drive a significant evolution in the mix of power resources. This transformation of generating resources is creating new reliability risks, from long- and short-term planning to real-time operations.

DETAIL OF CHANGES IN GENERATION



This risk has increased significantly as the pace of change in the resource mix has increased in recent years. RF has been collecting and analyzing performance data for conventional resources since 2012 and anticipates more advanced data collection to begin this year for both wind and solar resources.

Resource adequacy analysis indicates the RF footprint is trending toward resource deficiencies as early as 2028. This timeline could be exacerbated by federal and state policies related to carbon emissions and increases in customer demand. Currently eight states in our footprint have clean energy initiatives and RF is continuing to monitor state policy changes and other developments in our footprint, like an increase in data centers. There is not sufficient wind or solar paired with energy storage within connection queues to replace conventional resources based on the duration of energy storage available from existing technologies. Accordingly, RF is closely monitoring emerging technologies and the adoption of electrification policies and the impacts government incentives may have on energy demand.

UNCERTAINTY

There is uncertainty in the implementation of both federal and state policies, which influence retirement of conventional resources, new technologies, electrification of demand, and customer behavior. RF, in partnership with the ERO Enterprise, has been performing outreach to state utility commissions and legislators to communicate risks associated with the changing resource mix.

SUPPLY CHAIN

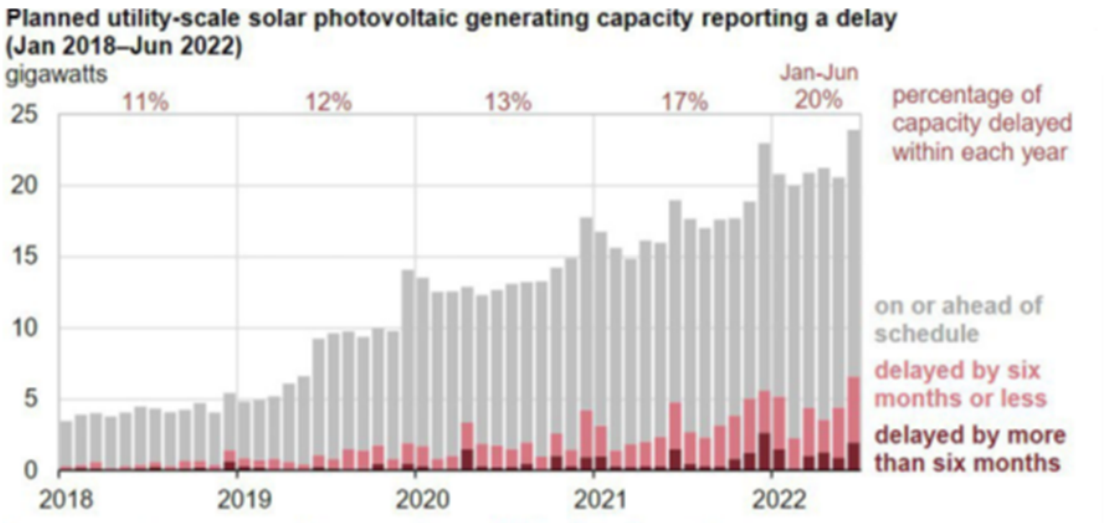
RESILIENCE

Improved resiliency on natural gas production and supply was recommended after Winter Storm Elliott. For potential low wind or solar days, the electric grid needs quick-start resources that can balance the potential unavailability. New technologies are needed (e.g., alternative to lithium-ion batteries) to ensure sufficient raw materials are available to achieve policy-related goals.

The supply chain risk involves the compromise of the availability of equipment, tools, and resources that result in the delay or disruption of system operations. These risks can originate from various sources such as geopolitical volatility, natural disasters, pandemics, cyber and physical security threats, labor shortages and economic instability. As the grid transforms, access to materials, parts, and labor may not be as abundant. RF evaluated this risk through fuel supply availability, the impacts related to raw material supply, and the delay in timely generation connections.

The demand for solar energy is increasing within the U.S. The U.S. Energy Information Administration (EIA) indicates that some of the new solar projects that developers originally planned to bring online in 2022 were either canceled or delayed because of supply chain issues. Based on the chart from the EIA below, approximately 20% of planned solar capacity was delayed in the U.S. in 2022 (from January to June). As demand increases, there seems to be a corresponding increase in solar panel delays. These delays can impact a substantial amount of generation planned for interconnection by six months or more. As retirements of conventional resources increase, these delays could impact overall reliability.

RF is also monitoring the manufacturing of renewable resource components and availability of critical minerals and raw material for energy storage technologies.

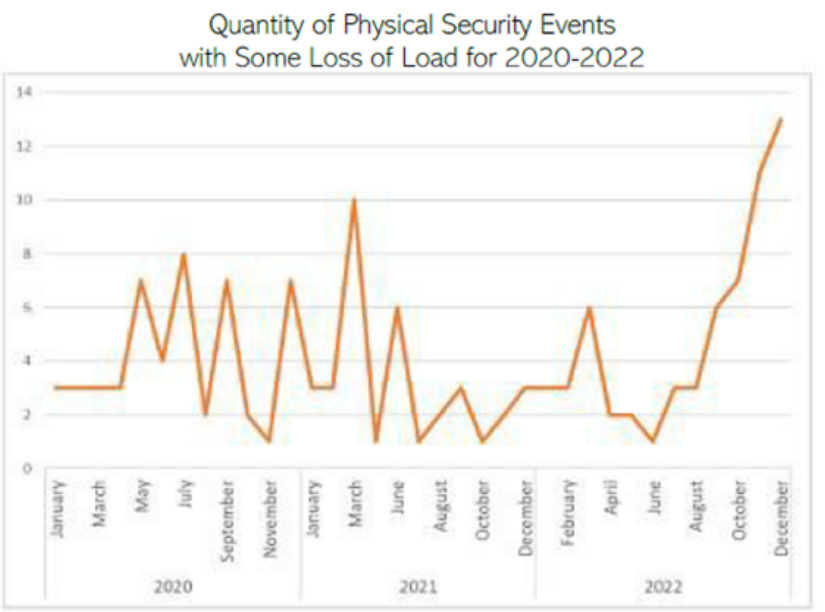


Source: U.S. Energy Information Administration (August 2022)

Public

PHYSICAL SECURITY

Physical Security is the protection of assets like substations, transformers, generating facilities, and control centers from threats that may compromise the intended operation or purpose of those assets. Guarding against this risk is crucial for ensuring the uninterrupted delivery of energy to customers due to a wide variety of threats including theft, vandalism and coordinated attacks.



Source: Electricity Information Sharing and Analysis Center (E-ISAC)

Across the U.S., there has been an increase in attacks on the bulk power system. According to recent analysis conducted by the Electricity Information Sharing and Analysis Center (E-ISAC), physical security incidents that have resulted in a measurable outage (i.e., loss of end-use customer load) have increased by 71% since 2021.

While there have been no physical attacks in the RF footprint that have led to loss in customer load, in late 2022, there were simultaneous physical attacks on two substations in North Carolina. These attacks caused equipment damage and outages resulting in 45,000 customers without electric service. As a result, FERC issued an order in December 2022 that required NERC to conduct a study of the CIP-014 physical security standard regarding the applicability criteria, required risk assessment, and the need for minimum security protections.

The grid of the future may be more susceptible to physical security threats due to the distributed and decentralized nature of the assets, especially new resources located in remote or open areas. Reasonable measures regarding monitoring, barriers, and controls must be implemented not only to protect the highest risk assets, but also the aggregate of lower risk assets from harm.

In addition to our monitoring, RF looks forward to continuing to collaborate with industry, such as partnering on targeted physical security workshops and education.

UNCERTAINTY

Changes in political climates and civil unrest have led to an increase in extremist groups and an increase in physical threats and attacks. Advances in technology provide new tools for extremist groups to perform surveillance (i.e., drones) and deploy coordinated attacks quickly. With its Threat Intelligence program, RF is constantly evaluating new data, information, and partnerships to reduce uncertainty with this risk.

MISOPERATIONS

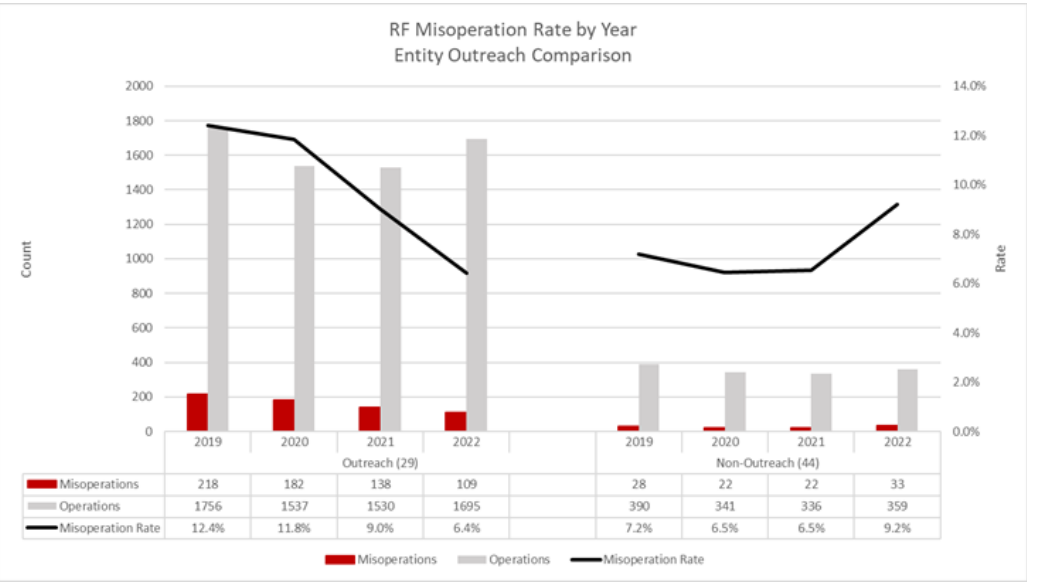
Misoperations are the failure of a protection system to operate as intended, resulting in the exacerbation of transmission outages that are not being actively monitored or planned.

HUMAN PERFORMANCE

While the RF footprint had many human performance related misoperations from 2019 to 2022 (44% of all misoperations), overall performance has improved over time. The total number of human performance related misoperations has been reduced by 58% over the last four years.

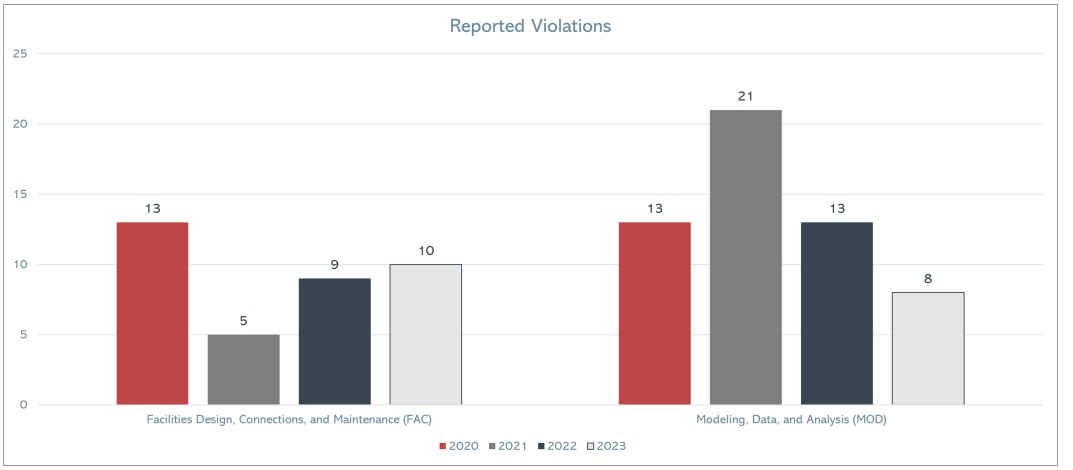
Misoperations include a Composite Protection System's failure to operate, delay in operating, or operating when not required during either a fault or non-fault conditions. Misoperations contribute to, and tend to exacerbate the impact of, automatic transmission outages, which adversely impacts the reliability of the BPS. This risk has been decreasing over time due to the improved performance. Analysis indicates that engagements between RF and several entities have been highly effective for this risk category, particularly where entities have invested time and resources and implemented system reinforcements.

RF collaborates with registered entities through the Protection Subcommittee to analyze misoperations performance. Since 2014, misoperations rate, misoperations count, and protection system operation count have significantly trended downward. RF has been working with entities with high misoperations risk since 2014 and is proud the rates for entities participating in outreach activities (appraisals, self-assessments, assist visits, and one-on-one discussions) have declined considerably. The improvements have been linked to the quarterly reviews of misoperations by the RF Protection Subcommittee and the committee-recommended webinar on best practices. Conversely, for non-participating entities, both total misoperations and misoperations rate have increased. We are continuing to encourage these entities to participate in our assist visits and other outreach programs. Ongoing Protection Subcommittee work will focus on repeat misoperations and events with multiple misoperations.



MODELING

Modeling is the sufficient representation of transmission and generation elements to model the electric grid and perform analysis that enhances situational awareness and system planning. Sufficiently planning and operating the bulk power system requires representative and accurate models to detect and prevent potential reliability and security issues. As the grid evolves with the integration of new technologies, it is critical to ensure that models are updated accordingly and effectively represent the behavior of equipment installed on the system. Modeling was not previously considered a key risk in the RF footprint, but our focus on modeling increased based on concerns about RF facility rating performance and disturbances involving inverter-based resources (IBRs) in the west.



The most relevant data to collect and assess the quality of system models within the RF footprint is data related to violations of the Modeling ("MOD") and Facility ("FAC") Standards. This includes examining the time it takes for entities to detect and report a violation (i.e., detection and response time) and violation count (i.e., frequency of occurrence). Reported violations of the MOD Standards have improved over time. For FAC Standards, the number of reported violations has displayed a slight increasing trend. RF entities have improved with performance related to FAC violation detection time.

RF will continue to monitor overall FAC violation performance. Since RF entities have improved performance related to detection time, the increasing trend may be related to improved detection control performance for entities. RF continuously monitors compliance metrics and will be looking to validate this conclusion. RF also continues to monitor IBR growth and performance as well as efforts to modify the NERC Reliability Standards and industry standards to address risks associated with modeling.

POLICY & STANDARDS

NERC has released multiple reliability guidelines and Reliability Standard changes to improve model representation of distributed energy resources and IBRs. In addition, IEEE 2800-2022 has been approved that outlines performance requirements for IBRs.

SITUATIONAL AWARENESS

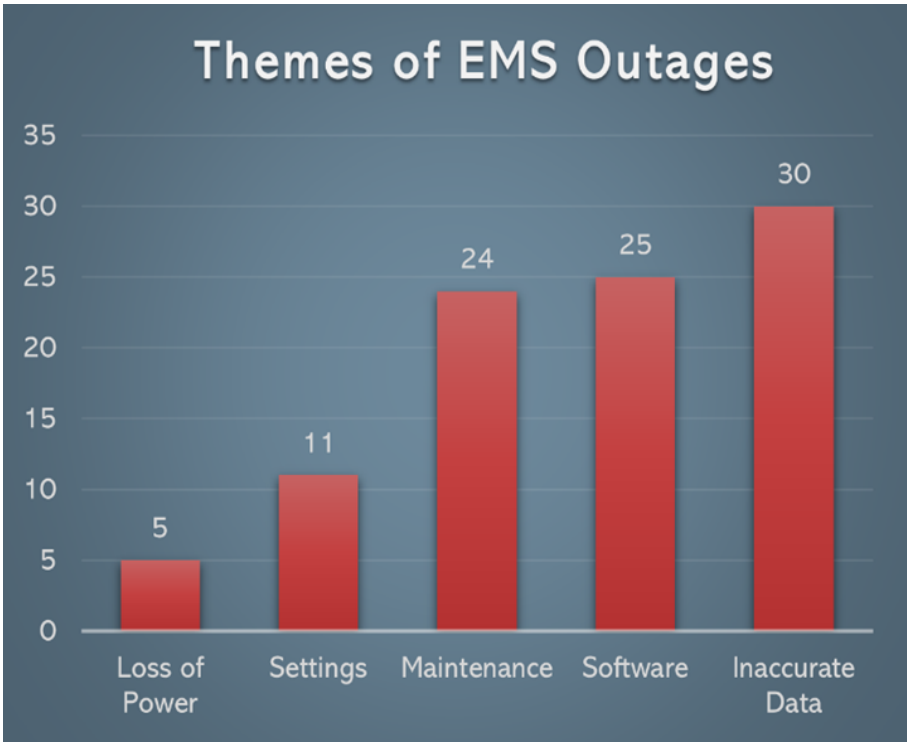
An essential component of situational awareness is the availability of real-time, accurate data on-demand. Unexpected outages of tools, or planned outages of tools without appropriate coordination or oversight, can leave system operators without visibility to some or all of the systems they operate. While the failure of situational awareness tools is rarely the cause of the system event, such failures manifest as underlying risks that hinder the decision-making capabilities of the system operator to respond and react to the situation.

HUMAN PERFORMANCE

EMS outages caused by human error are a large percentage of the total outages. However, the three largest EMS outage categories (i.e., inaccurate data, software, and maintenance) have all exhibited consistent or improved performance since 2018.

While Energy Management System (EMS) and SCADA systems have improved over the past 20 years, new complexities related to modeling, forecasting, and advanced tools such as real-time stability analysis have created situational awareness challenges that RF is addressing through the event analysis process and outreach with our entities. These systems are highly reliable overall, yet outages and disturbances to these tools may have detrimental impacts to reliability.

RF, through the Operational Analysis and Awareness (OAA) team, works closely with registered entities to review EMS/SCADA outages. Through root cause analysis, the team has worked with industry to identify common causes, issues, and mitigations. These outages are tracked and trended to monitor RF's ability to mitigate this risk. Furthermore, RF and the rest of the ERO enterprise publish lessons learned documents and host the annual NERC Monitoring and Situational Awareness Conference to collaborate with industry on reducing the number and duration of these outages.



ZOOMING OUT: RISK INTERDEPENDENCE

After analyzing each of the top risks in our footprint and their potential impact and reviewing the data, we zoomed out for a big picture view. Below we share two observations where overlapping risks can pose a greater impact in our footprint. Then, in the accompanying infographic attached to this report, we explore risk interrelatedness through a grid transformation lens.

Increasing impact of cold weather on resource availability

Extreme cold weather events in our footprint are increasing and constraining resource availability. Policy change and conventional resource retirements made natural gas a dominant fuel source, and it is extremely susceptible to cold weather events. The wind and solar that are supplementing coal retirements are also vulnerable to cold weather, increasing the impact of these events. Here's how we're monitoring and managing this increased combined risk:

Monitoring

- Tracking progress on FERC/NERC joint inquiry reports (Winter Storm Uri and Elliott)
- Following fuel source policy changes at the federal, state, and RTO/ISO level
- Performing studies examining extreme weather reliability impacts

Managing

- Utilizing Winter Readiness Program (for plants historically unavailable during extreme weather) that shares best practices and lessons learned regarding winter preparation activities
- Developing audit approach for enhanced NERC Reliability Standards

Rapid pace of change increasing resource uncertainty and supply chain issues

Aggressive federal and state policies are influencing carbon-based resource retirements. The wind and solar resources that are supplementing these retirements require energy storage to ensure improved availability. The need for storage technologies is concurrent with the prominence of electric vehicles and increasing demand. The raw materials to support both solar and lithium-ion battery storage technologies are limited, causing supply chain issues and resource uncertainty. Here's how we're monitoring and managing this increased combined risk:

Monitoring

- Tracking projected resource growth and retirements
- Following federal, state and local policies related to decarbonization, the incentivization of new technologies and manufacturing
- Researching information on raw material availability and advancements in recycling technologies and resource connection delays
- Performing planning studies that evaluate high risk scenarios in generation and load changes

Managing

- Continuing education and outreach efforts to drive policy decisions, including sharing industry and RF study results
- Obtaining additional outside data sources to better analyze the risks

OUR PATH FORWARD

This first public facing RRA reflects our efforts to be transparent with our top risks and keep key decision makers informed as we seek solutions to the complex issues that face our rapidly transforming grid.

RF strives to continually improve, and our risk assessment is no exception. Uncertainty was a consideration for each risk, where we contemplated if there were other interdependencies that could impact the risk in our footprint. We also held an internal summit where subject matter experts looked at existing data to consider whether additional third-party sources or vendors can further our understanding and reduce the risk through analytics. This initiative generated multiple deliverables that we plan to implement to enhance our work and future risk assessments.

While there will always be unknowns, we know that the complex risks of the future require collaboration and broad industry expertise. We hope throughout the year you will be reminded of this assessment through both our regulatory and non-regulatory (outreach) efforts to identify, assess, and mitigate these risks. Thank you to our committees and subcommittees for their input and collaboration in developing this RRA. Please visit our website if you would like to get involved with one of our committees or if you would like to contact RF with any questions or feedback on the report.

RELIABILITYFIRST 2023-24 RRA: TOP REGIONAL RISKS THROUGH THE LENS OF GRID TRANSFORMATION

Public

Looking at the top risks in tandem provides another important perspective on the risks in the RF region. This infographic looks at the interdependence through the lens of the transforming electric grid as the way that power is generated, transmitted and consumed evolves. As decarbonization, decentralization and digitization impact how we plan, operate and protect the grid of the future, the risk interrelatedness is increasingly important.

Changing Resource Mix

As the changing generation resource mix is moving toward a cleaner grid, coal-fired generation units are being retired at a rapid pace. This leaves natural gas as the dominant existing fuel. This mix of resources, reliant on natural gas and renewables, creates an increased vulnerability during extreme weather events.

Misoperations

The increasing penetration of inverter-based resources (IBRs) may impact grid controls systems, possibly leading to an increase in misoperations. While misoperations are not a new risk, the replacement of thermal-based generation with asynchronous generation may impact short-circuit fault currents, impacting the way protection systems and relays detect and respond to faults. Recent NERC event reports include lessons learned regarding IBRs responding to voltage and frequency disturbances, impacting reliable operations.

Cyber Security

The growth of low-impact IBRs and distributed energy resources can create new cyber security vulnerabilities. This may include aggregates of solar and wind generation being operated by foreign control centers, plus new cyber security challenges. As electrification of the grid increases, interconnectivity of electronic devices, new variable loads (such as electric vehicle charging stations), and modifications to existing IT/OT technologies (e.g., cloud and virtualization) all impact cyber security vulnerabilities. These risks can be exploited through increased usage of ransomware, malware, and other threats deployed by adversaries to grid reliability and security.

Physical Security

The grid of the future may be more susceptible to physical security threats due to the distributed and decentralized nature of the assets, especially new resources located in remote or open areas. Reasonable measures regarding monitoring, barriers, and controls must be implemented not only to protect the highest risk assets, but also the aggregate of lower risk assets from harm.

Environmental Factors

Following Winter Storm Elliott, reports recognized that the freezing equipment and subsequent failure of natural gas supply was a significant factor in power outages across the US. In addition, renewable energy availability declines sharply during these types of extreme weather conditions, adding more challenges during a time when people need power the most.

Supply Chain

As the renewable energy portfolio across the country continues to proliferate, it has been widely accepted that battery technology will be needed to maintain resource adequacy during periods when the intermittent renewables are not available. The raw materials used to make the lithium-ion batteries to support the grid are the same materials used to make electric vehicle (EV) batteries. The surge in demand for these raw materials has created supply chain constraints resulting in delays in construction of these facilities. Renewable energy developers, in a few cases, have rescinded their interconnection applications, citing supply chain constraints as a barrier to development.

Situational Awareness

Operators in the control room need tools, technology, and training to identify and mitigate the risks associated with an increase of behind-the-meter resources, both intermittent distributed energy resources plus large electric loads such as data centers, electric vehicle charging stations, heat pumps, etc. Visibility and communication are needed for balancing load and generation as the grid continues to transform, and control center technology outages (including losses of state estimation, forecasting tools, and communication tools) increase this risk profile if not mitigated.

Modeling

Situational awareness is only accurate if industry provides accurate modeling to the planners and operators of the grid. As the grid transforms, operators need to be able to anticipate how the grid will respond to faults and disturbances. Accurate models are key for performing the analysis needed to mitigate the risks.

FORWARD TOGETHER RELIABILITYFIRST