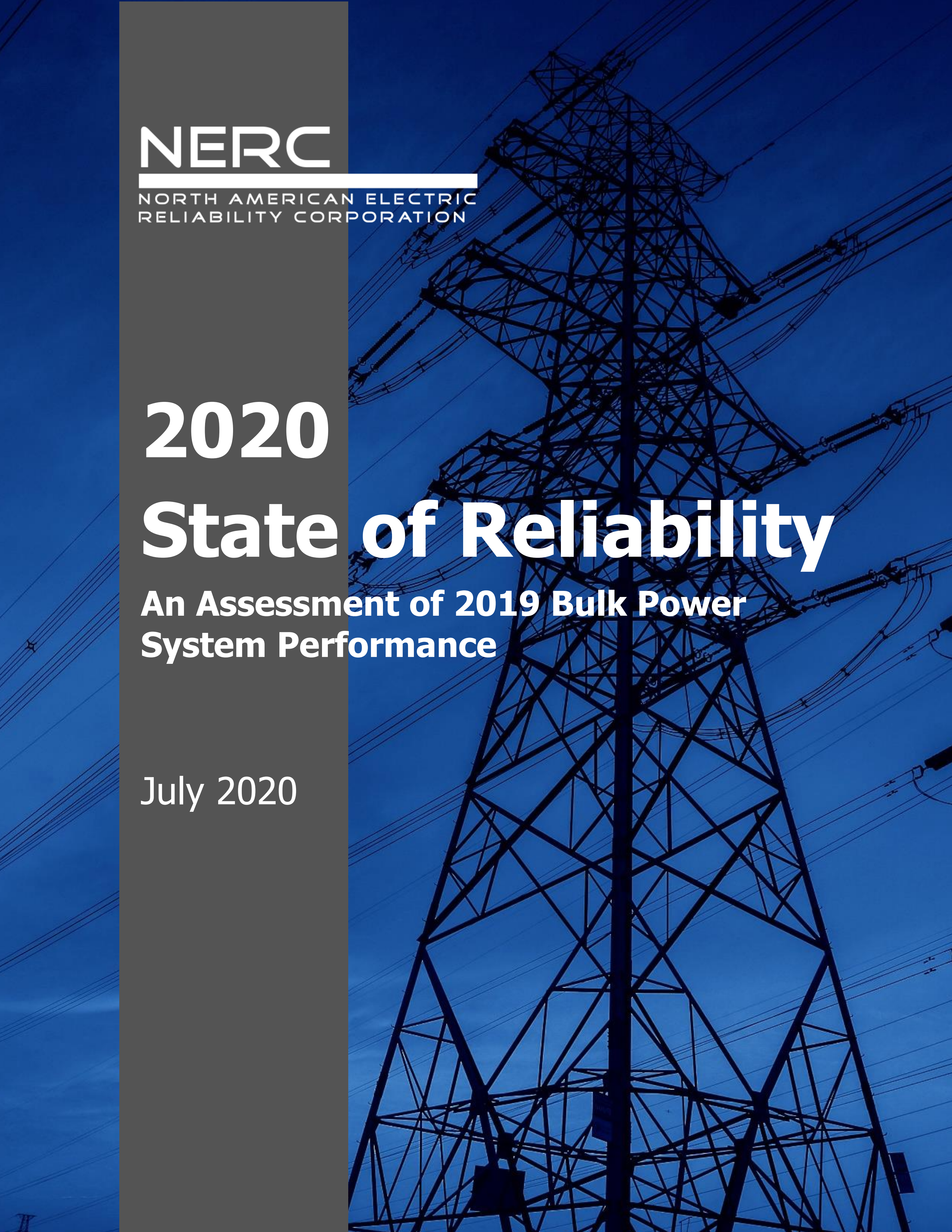


NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

2020
State of Reliability

An Assessment of 2019 Bulk Power System Performance

July 2020

Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security

Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one RE while associated Transmission Owners (TOs)/Transmission Operators (TOPs) participate in another.

MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

About This Report

The purpose of this annual report is to provide objective and concise information to policymakers, industry leaders, and the NERC Board of Trustees (Board) on issues affecting the reliability and resilience of the North American BPS. Specifically, the report does the following:

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

NERC, as the ERO of North America, assures the effective and efficient reduction of risks to reliability and security for the North American BPS. Annual and seasonal risk assessments that look to the future and special reports on emergent risks serve to identify and mitigate potential risks. Additionally, analyses of past BPS performance serve to document BPS adequacy and to identify positive or negative performance trends. The annual State of Reliability report is one such analysis of past performance that informs regulators, policymakers, and industry leaders while providing strong technical support for those interested in the underlying data and detailed analytics.

Development Process

The ERO staff developed this independent assessment with support from the Performance Analysis Subcommittee. The *2020 State of Reliability* report focuses on BPS performance during the prior complete year as measured by a predetermined set of reliability indicators and more detailed analysis performed by ERO staff and technical committee participants. This report has been endorsed by the Reliability and Security Technical Committee and accepted by the NERC Board.

Primary Data Sources

In addition to a variety of information-sharing mechanisms—including (but not limited to) the NERC Planning Committee, Operating Committee, Critical Infrastructure Protection Committee, and the Electricity Information Sharing and Analysis Center (E-ISAC)—the ERO administers and maintains the information systems described in **Figure AR.1**.

Impacts of COVID-19 Pandemic

The global health crisis has elevated the electric reliability risk profile due to potential workforce disruptions, supply chain interruptions, and increased cyber security threats. An in-depth evaluation of any impacts due to COVID-19 on BPS operations in 2020 will be a focus of the 2021 State of Reliability report, which is typically published mid-year. *The 2020 Long-Term Reliability Assessment*, which is expected to be published in December 2020, will also assess any longer-term reliability issues that need to be considered in future operations and planning of the BPS. The NERC *Pandemic Preparedness and Operational Assessment*[1] (April 2020) specifically covered pandemic preparedness, possible risks to system operations, maintenance and resource planning, ERO Enterprise business continuity, and lessons learned from outside North America; NERC did not identify any specific threat or degradation to the reliable operation of the BPS for the spring time frame. The ERO continues to assess risks and conditions and is pursuing all available avenues to continue coordination with federal, state, and provincial regulators as well as to work with industry to identify reliability implications and lessons learned.

---

1 https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_Pandemic_Preparedness_and_Op_Assessment_Spring_2020.pdf

Transmission Availability Data System (TADS)

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

Transmission 100kV and greater

Generation Availability Data System (GADS)

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

Conventional Generators 20 MW and larger

Misoperation Info Data Analysis System (MIDAS)

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

Transmission Owners, Generator Owners, Distribution Providers

The Event Analysis Management System (TEAMS)

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

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

Figure AR.1: Information Systems Administered and Maintained by the ERO

Reading this Report

This report is divided into five chapters (see **Table AR.1**).

Table AR.1: State of Reliability Major Parts	
The North American BPS—By the Numbers[2]	Detailed statistics on peak demand, energy, generation capacity, fuel mix, transmission miles, and functional organizations
Event Analysis Review	A detailed review of qualified events analyzed by NERC, including root cause statistics, historical trends, and highlights of published lessons learned
Reliability Indicators	A set of reliability metrics that evaluate four core aspects of system performance: resource adequacy, transmission performance and availability, generation performance and availability, and system protection and disturbance performance
Severity Risk Index	A composite daily severity index based on generation, transmission, and load loss and compared to prior years
Trends in Priority Reliability Issues	Data and analysis from various NERC data sources compiled to provide clear insights on a variety of priority reliability issues (included assessments help provide guidance to policy makers, industry leaders, and the NERC Board)

[2] Definition of BPS: https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

Additional Considerations

- The data in this report represents the performance for the January–December 2019 operating year unless otherwise noted.
- Analysis in this report is based on 2015–2019 data and provides a basis to evaluate 2019 performance relative to performance over the last five years.
- This report is a review of industry-wide trends and not a review of the performance of individual entities. Accordingly, information presented in this report is always aggregated to the Interconnection level or the regional level in order to maintain the anonymity of individual reporting organizations.
- The background on approaches, methodologies, statistical tests, and procedures are available by request.
- When analysis is presented by Interconnection, the Québec Interconnection is included in the Eastern Interconnection unless specific analysis for Québec is shown.

Executive Summary

The *2020 State of Reliability* report is NERC's independent assessment focused on BPS performance during 2019 as measured by a predetermined set of reliability indicators. This annual report is an analysis of past performance that informs regulators, policymakers, and industry leaders of reliability and performance trends, needed actions to address known and emerging risks, and whether mitigating actions have led to positive improvements on the system.

Overall, 2019 was a very good year for BPS reliability. Performance trends in terms of generation, transmission, and protection and control measures are generally positive. The electricity sector is undergoing significant and rapid changes to the generation resource mix that present new challenges and opportunities for reliability. In addition, persistent cyber and physical security threats present critical challenges to BPS reliability that require industry and regulators to remain vigilant. With appropriate insight, careful planning, and continued support, the sector will continue to navigate the challenges in a manner that maintains reliability. As a core element of the ERO's mission, NERC remains focused on identifying emerging risks in order to maintain a proactive posture to assure that the BPS remains highly reliable.

Metrics showed improvement in numerous areas. Declining performance areas, while noted, did not show significant change. Reliability indicators detailed in **Chapter 3** show the following:

Metrics That Show Improving Performance

- The Weighted-Equivalent Generation Forced Outage Rate (WEFOR) is declining.
- The impact of transmission outages on the Bulk Electric System (BES) is decreasing.
- The number of automatic transmission outages from ac circuits and transformers caused by human error is decreasing.
- The rate of Protection System Misoperations has decreased.

Metrics That Indicate Declining Performance

- The count and severity of energy emergency alerts (EEAs) is increasing.
- The Planning Reserve Margin continues to not meet expected thresholds in some areas.
- The instances of transmission-related events resulting in loss of load increase in number and severity from 2018.
- Element unavailability for ac circuits and transformers showing an increase due to operational outages.[3]
- Interconnection reliability operating limit exceedances in the expanded Eastern Interconnection[4] increase in number and duration.

Metrics That Show No Major Change

- Interconnection frequency response has been stable.

[3] Operational Outage: A nonautomatic outage for the purpose of avoiding an emergency (i.e., risk to human life, damage to equipment, damage to property) or to maintain the system within operational limits and that cannot be deferred. Includes non-automatic outages that result from manual switching errors.
[4] The expanded Eastern Interconnection includes the Eastern and Québec Interconnections

Key Findings

Based on data and information collected for this assessment, NERC has identified the following key findings for 2019:

Key Finding 1

The system was highly reliable in 2019.

2019 was a year of high reliability with no Category 3, 4, or 5 events and only two EEA Level 3 conditions that led to firm load shedding of 250 MW. Firm load was interrupted 0.005% of the time due to EEAs Level 3. For more detailed information, refer to **Chapter 2**.

Key Finding 2

In Texas, the projected capacity deficit remains a reliability risk in 2020; however, better than expected performance from the generation fleet helped meet 2019 summer peak demand.

Texas continues to have insufficient resources to meet the Reference Margin Level but still successfully met demand throughout the 2019 summer season. Despite having set a new system-wide peak demand record of 74,666 MW on August 12, 2019, sufficient resources were available throughout the peak day to remain above reserve requirements; this was primarily due to higher than average contribution from wind generation resources and lower than average total generation outages. For more detailed information, refer to **Chapter 3**.

Key Finding 3

Local energy-assured generation remains necessary for reliability.

In 2019, the Western Interconnection experienced its most extreme transmission day in the past five years, consisting of a combination of the loss of a major dc flow line, repeated outages of 500 kV ac circuits, and inverter-based resource unavailability related to the Saddleridge Fire. Impacts of the event were minimized due to the availability of local thermal generation and good operator judgment. These observations emphasize the need for adequate local energy-assured generation. For more detailed information, refer to **Chapter 5**.

Key Finding 4

NERC and industry stakeholders are advancing solutions to the addition of more inverter-based resources.

Inverter-based resources include solar photovoltaic (PV), battery storage, and many forms of wind generation. As more of these resources are added to the system, NERC and industry stakeholders are working to identify solutions to emerging reliability challenges. In 2017, NERC established the Inverter-Based Resource Performance Task Force (IRPTF) to study the issue and inform industry of the risks posed and options for mitigating them. In 2019, industry continued implementation of the *Inverter-Based Resource Performance Guideline*.[5] This, along with wide-spread recognition of the challenge, has gathered the industry's best technical experts to develop solutions through a variety of new protection and control requirements, clarification to NERC Reliability Standards, and technical specifications through IEEE. For more detailed information, refer to **Chapter 5**.

Key Finding 5

Frequency response improved or remained stable in all Interconnections.

Frequency response arrests and stabilizes frequency during system disturbances. NERC closely monitors the frequency response of each of the four Interconnections and measures the margin at which under-frequency load shedding (UFLS) would be activated. UFLS provides a vital safety net for preserving Interconnection reliability, and measuring the margin allows NERC and the industry to ensure there is adequate frequency response on the system. For all Interconnections, frequency response performance improved or was stable in the arresting and stabilizing periods. For more detailed information, refer to **Chapter 3**.

---

[5] https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Reliability_Guideline_IBR_Interconnection_Requirements_Improvements.pdf

Key Finding 6

Protection System Misoperations rate continues to decline.

Protection system misoperations exacerbate the severity of transmission outages. The overall misoperations rate was slightly lower in 2019 vs. 2018 (7.95%, down from 8.0% in 2018). Over the past five-year period, the misoperations rate shows a statistically significant downward (positive) trend. The three largest causes of misoperations in 2019 have remained consistent during this time: Incorrect Settings/Logic/Design Errors, Relay Failure/Malfunctions, and Communication Failures. For more detailed information, refer to **Chapter 3**.

Key Finding 7

There were no reportable cyber or physical security incidents in 2019.

Despite continually evolving threats to the BPS, no cyber or physical security incidents led to unauthorized control actions or loss of load occurred in 2019. The industry should continue to drive improvements in its security posture through technological hardening, growing a culture of security, and increasing effective information exchange between entities, the E-ISAC, and trusted partner organizations. For more detailed information, refer to **Chapter 5**.

Recommendations

Based on these key findings, NERC formulated the following high-level recommendations:

- The ERO and industry should continue improving their ability to model, plan, and operate a system with a significantly different resource mix. Priority should be given to understanding the implications of the following:
    - Frequency response under low inertia conditions
    - Contributions of inverter-based resources to essential reliability services
    - Increasing protection system and restoration complexities with increased inverter-based resources
- System planners should evaluate the need for flexibility as conventional generation retirements are considered by industry and policymakers. Retirement planning studies should consider Interconnection-level impacts and sensitivity assessments associated with the loss of critical transmission paths and the loss of local generation in larger load pockets.
- The ERO and industry should develop comparative measurements and metrics to understand the different dimensions of resilience (e.g., withstanding the direct impact, managing through the event, recovering from the events, preparing for the next event) during the most extreme events and how system performance varies with changing conditions.
- The ERO and industry should continue to work closely together to understand and share information on cyber and physical security threats and mitigate the risks posed by these threats through a variety of approaches, including resilient system design, consequence-informed planning and operation, and practicing response and recovery processes.

Emerging Risk Areas

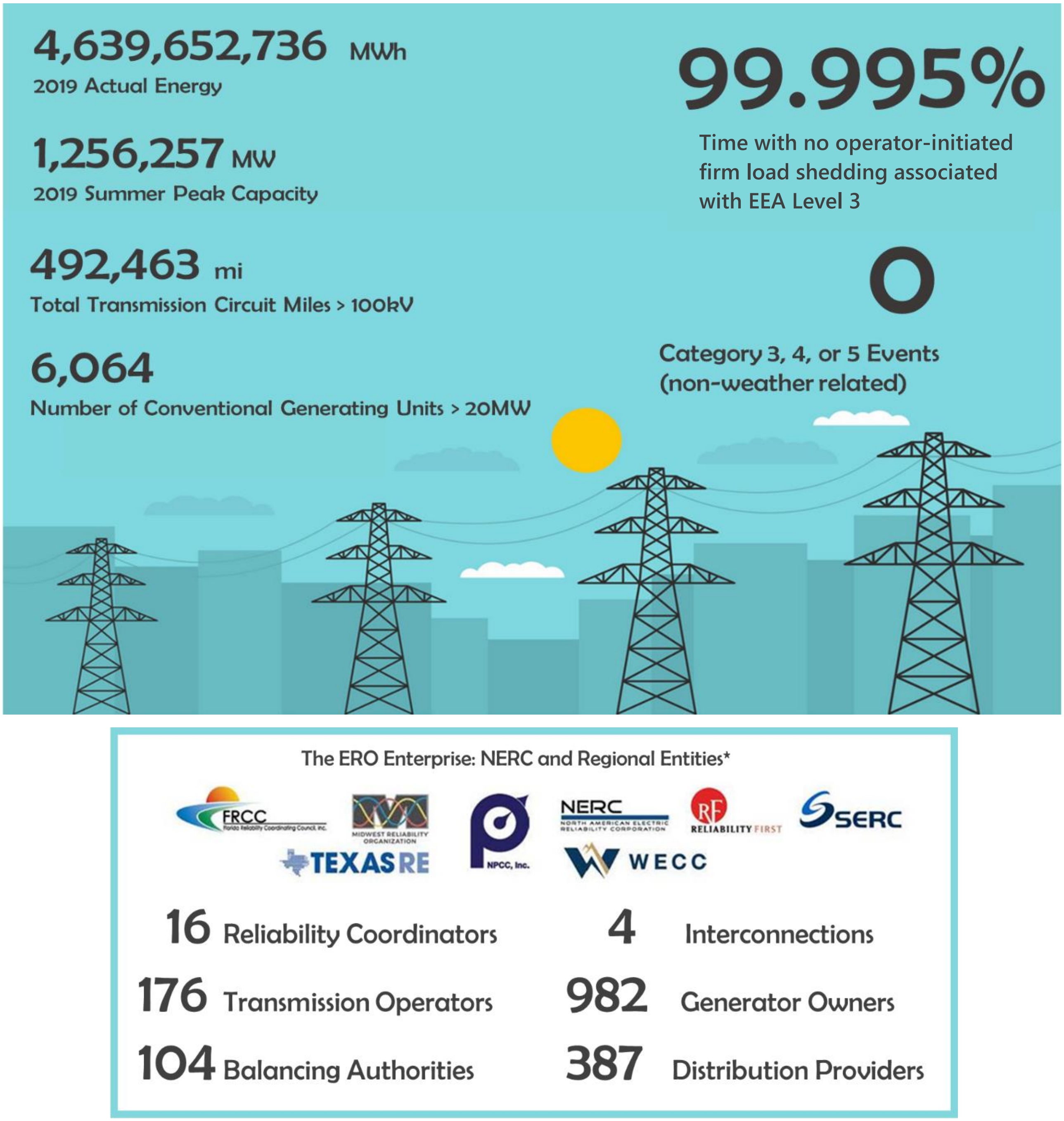
In addition to these high-level recommendations, **Chapter 5** includes more detailed and tactical recommendations for each of the identified four high level risks from the *2019 ERO Reliability Risk Priorities Report*:[6]

- **BPS Planning and Adapting to the Changing Resource Mix**
- **Impacts of Inverter-Based and Distributed Energy Resources on the BPS**
- **Increasing Complexity in Protection and Control Systems**
- **Human Performance and Skilled Workforce**
- **Loss of Situation Awareness**
- **Bulk Electric System Impact of Extreme Event Days**
- **Cyber and Physical Security**
- **Critical Infrastructure Interdependencies: Electric-Gas Working Group**

[6] https://www.nerc.com/comm/RISC/Related%20Files%20DL/RISC%20ERO%20Priorities%20Report_Board_Accpeted_November_5_2019.pdf

Chapter 1: The North American BPS—By the Numbers

Figure 1.1 shows some numbers and facts about the North American BPS. The **text box** on the next page defines BPS reliability.



* FRCC RE responsibilities were transferred to SERC in July 2019

Figure 1.1: 2019 BPS Inventory and Performance Statistics and Key Functional Organizations

How NERC Defines BPS Reliability*

NERC defines the reliability of the interconnected BPS in terms of three basic and functional aspects as follows:

Adequacy: The ability of the electric system to supply the aggregate electric power and energy requirements of electricity consumers at all times while taking into account scheduled and reasonably expected unscheduled outages of system components

Operating Reliability: The ability of the electric system to withstand sudden disturbances, such as electric short circuits or unanticipated loss of system components

Regarding adequacy, system operators can and should take controlled actions or introduce procedures to maintain a continual balance between supply and demand within a balancing area (formerly known as a control area). Emergency actions in a capacity deficit condition include public appeals and the following:

- Interruptible demand that the end-use customer makes available to its load-serving entity via contract or agreement for curtailment
- Voltage reductions (often referred to as “brownouts” because incandescent lights will dim as voltage is lowered, sometimes as much as 5%)
- Rotating interruptions/outages where a preplanned set of distribution feeders is interrupted for a limited time and put back in service and another set is interrupted, thus, “rotating” the outages

Under the heading of operating reliability are all other system disturbances that result in the unplanned and/or uncontrolled interruption of customer demand, regardless of cause. When these interruptions are contained within a localized area, they are considered unplanned interruptions or disturbances. When these interruptions spread over a wide area of the grid, they are referred to as “cascading blackouts” (uncontrolled successive loss of system elements triggered by protective systems).

The intent of the set of NERC Reliability Standards is to deliver an adequate level of reliability (ALR).

Adequate Level of Reliability: The state that the design, planning, and operation of the BES will achieve when the following reliability performance objectives are met with the following considerations:

- The BES does not experience instability, uncontrolled separation, cascading, and/or voltage collapse under normal operating conditions when subject to predefined disturbances.
- BES frequency is maintained within defined parameters under normal operating conditions and when subject to predefined disturbances.
- BES voltage is maintained within defined parameters under normal operating conditions and when subject to predefined disturbances.

Adverse reliability impacts on the BES following low-probability disturbances (e.g.., multiple contingencies, unplanned and uncontrolled equipment outages, cyber security events, malicious acts) are managed.

Restoration of the BES after major system disturbances that result in blackouts and widespread outages of BES elements is performed in a coordinated and controlled manner.

For less probable severe events (i.e., losing an entire right of way due to a tornado, simultaneous or near simultaneous multiple transmission facilities outages due to a hurricane, sizeable disruptions to natural gas infrastructure impacting multiple generation resources, or other severe phenomena), BES owners and operators may not be able to apply economically justifiable or practical measures to prevent or mitigate an adverse reliability impact on the BES even if these events can result in cascading, uncontrolled separation or voltage collapse.

Definition of BES: https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

Chapter 2: Event Analysis Review

The *ERO Event Analysis Process* (EAP)[7] is used when examining disruption events that occur on the BPS. The EAP makes use of the ERO Bulk Power System Awareness (BPSA) program to feed the voluntary process with real-time reporting of potential events on the BPS. Information is gathered and applied to set definitions that meet a threshold considered significant enough to inform risk monitoring and mitigation of daily operations on the BPS. Review and analysis of this information helps identify potential reliability risks or emerging threats. The ERO and partner entities can address these threats by promoting reliability through collaboration with each other and by being learning organizations.

The primary reason for participating in an event analysis is to determine if there are lessons to be learned and shared with the industry. The analysis process involves identifying what happened, why it happened, and what can be done to prevent recurrence. Identification of the sequence of events answers the "what happened" question, and determination of the root cause of an event answers the "why" question. Event analysis ultimately informs the identification of trends on the BPS. These trends may identify the need to take action, such as the issuance of a NERC alert to the owners and operators of the system to take an action or initiate the need for the development of or revisions to Reliability Standards.

Bulk Power System Awareness, Inputs, and Products

NERC BPSA collects and analyzes information on system disturbances and other incidents that have an impact on the North American BPS and disseminates this information to internal departments, registered entities, regional organizations, and governmental agencies as necessary. Also, BPSA monitors ongoing storms, natural disasters, and geopolitical events that may potentially impact or are currently impacting the BPS.

Figure 2.1 illustrates a number of monitoring sources, which includes owners and operators submitting a U.S. Department of Energy – Office of Electricity (DOE-OE) Form 417 and/or the event reporting form found in NERC Reliability Standard EOP-004. NERC also processes data coming in from intelligent alarms, GPS-synchronized frequency sensors via the FNET that is operated by the University of Tennessee, and messages through the Reliability Coordinator Information System (RCIS). As a result of the gathering and analysis of BPSA data, a NERC alert may be published.

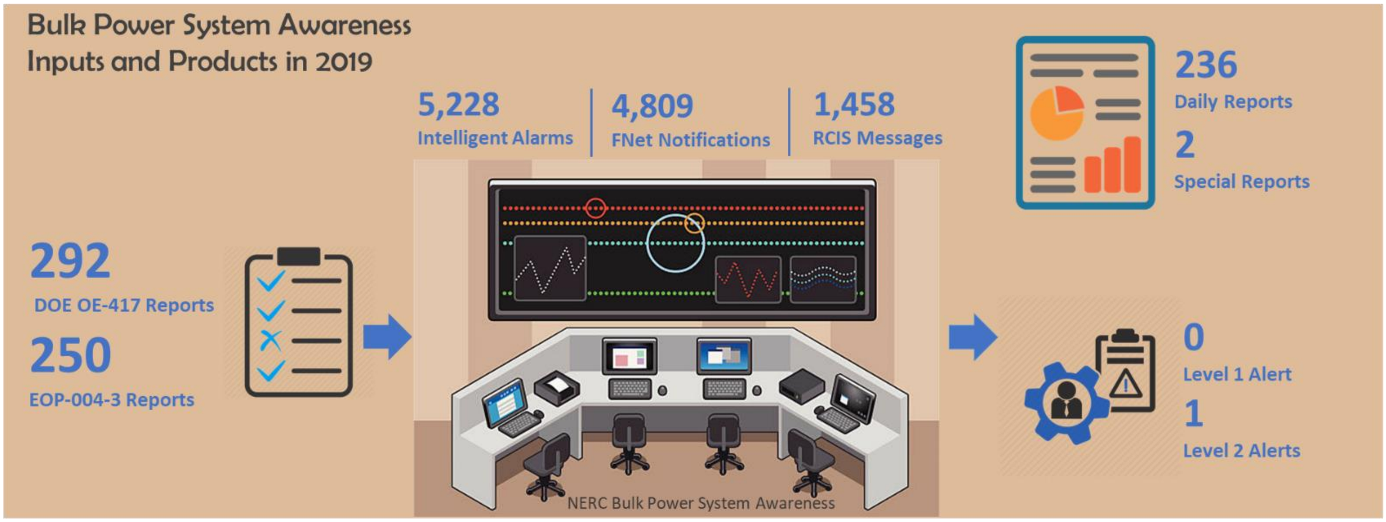


Figure 2.1: Bulk Power System Awareness by the Numbers

---

[7] For purposes of this report, the EAP in effect was version 3.1: http://www.nerc.com/pa/rrm/ea/ERO_EAP_Document/ERO_EAP_v3.1.pdf

NERC Alerts

NERC is responsible for issuing alerts to registered entities and the electricity sector when NERC discovers, identifies, or is provided with information that is critical to ensuring the reliability of the BPS. One alert was issued in 2019 concerning supply chains.

Level 2 Recommendation NERC Alert Based on Section 889 of the National Defense Authorization Act for Fiscal Year 2019

On July 16, 2019, NERC released a Level 2 (recommendation) alert to raise awareness among NERC registered entities of persistent supply chain risks related to certain Chinese manufacturers and to request information to assess the extent of exposure of the BPS to these risks. Analysis of the responses suggest minimal exposure of the BPS through branded products from the named Chinese telecommunications and video surveillance manufacturers and a somewhat more common use of Chinese manufactured or supplied unmanned aerial systems (UASs) for maintenance or asset management activities.

NERC continues to address these supply chain risks through the Critical Infrastructure Protection Reliability Standards and through information sharing and collaboration by the E-ISAC.

2019 Event Analysis Summary

In 2019, industry reported 148 qualified events[8] to the ERO Enterprise. The majority of the reports (145) were Category 1 events. The most common event categories reported in 2019 were energy management system (EMS) events and the loss of three or more BPS facilities. See **Figures 2.2–2.4** for a summary of events and definitions for event categories in the **text box** on the next page.

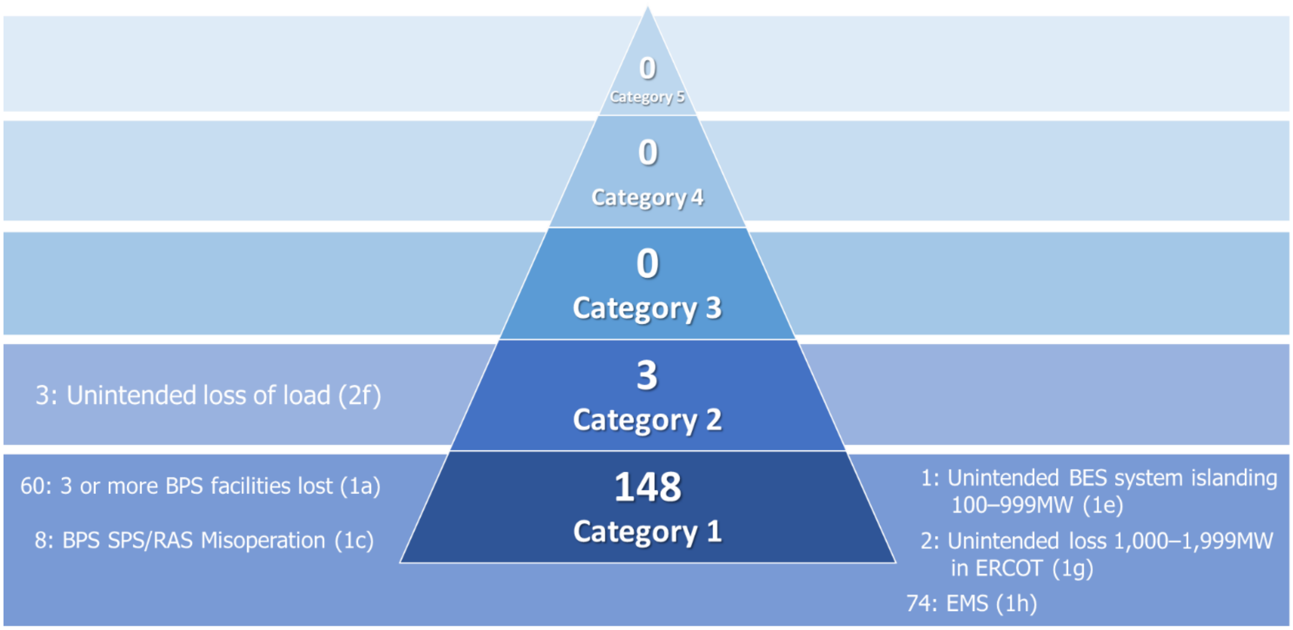


Figure 2.2: 2019 Qualified Events by Category

Events are assigned a category with Category 1 (the least severe) through Category 5 (the most severe). For the full definition of the categories used in 2019 refer the **text box** on the next page[9] that comes out of the ERO EAP Version 3.1.[10]

---

[8] For a list of definitions of Qualified Events, see the **text box** on the next page.
[9] Category 1f and 2b were retired as of version 3.0 of the *ERO Event Analysis Process*
[10] https://www.nerc.com/pa/rrm/ea/ERO_EAP_Documents%20DL/ERO_EAP_v3.1.pdf

Categories and Subcategories for Qualifying Events

Category 1: An event that results in one or more of the following

a. An unexpected outage that is contrary to design of three or more BES facilities caused by a common disturbance, listed here:

i. The sustained outage of a combination of three or more BES facilities

ii. The outage of an entire generation station of three or more generators (aggregate generation of 500 MW to 1,999 MW); each combined-cycle unit is counted as one generator

b. Intended and controlled system separation by the proper operation of a special protection system (SPS) or remedial action scheme (RAS) in New Brunswick or Florida from the Eastern Interconnection

c. Failure or misoperation of a BES SPS/RAS

d. System-wide voltage reduction of 3% or more that lasts more than 15 continuous minutes due to a BES emergency

e. Unintended BES system separation that results in an island of 100 MW to 999 MW. This excludes BES radial connections and non-BES (distribution) level islanding

g. In ERCOT, unintended loss of generation of 1,000 MW to 1,999 MW

h. Loss of monitoring or control at a control center such that it significantly affects the entity's ability to make operating decisions for 30 continuous minutes or more. Some examples that should be considered for Event Analysis reporting include, but are not limited to, the following:

i. Loss of operator ability to remotely monitor or control BES elements

ii. Loss of communications from supervisory control and data acquisition (SCADA) remote terminal units (RTUs)

iii. Unavailability of inter-control center protocol (ICCP) links, which reduces BES visibility

iv. Loss of the ability to remotely monitor and control generating units via automatic generator control

v. Unacceptable state estimator or real time contingency analysis solutions

Category 2: An event that results in one or more of the following

a. Complete loss of interpersonal communication and alternative interpersonal communication capability affecting its staffed BES control center for 30 continuous minutes or more.

c. Voltage excursions within a Transmission Operator's (TOPs) footprint equal to or greater than 10%, lasting more than 15 continuous minutes

d. Complete loss of off-site power to a nuclear generating station per the Nuclear Plant Interface Requirement

e. Unintended system separation that results in an island of 1,000 MW to 4,999 MW

f. Unintended loss of 300 MW or more of firm load for more than 15 minutes

g. Interconnection reliability operating limit (IROL) violation for time greater than T_v

Category 3: An Event that Results in One or More of the Following

a. Unintended loss of load or generation of 2,000 MW or more.

b. Unintended system separation that results in an island of 5,000 MW to 10,000 MW

c. Unintended system separation (without load loss) that islands Florida from the Eastern Interconnection

Category 4: An Event that Results in One or More of the Following

a. Unintended loss of load or generation from 5,001 MW to 9,999 MW

b. Unintended system separation that results in an island of more than 10,000 MW (with the exception of Florida as described in Category 3c)

Category 5: An Event that Results in One or more of the Following

a. Unintended loss of load of 10,000 MW or more

b. Unintended loss of generation of 10,000 MW or more

While the number of events per year has not changed significantly since 2016, it is notable that a large percentage of events each year are Category 1 events. The five-year trends are shown in **Figure 2.3**.

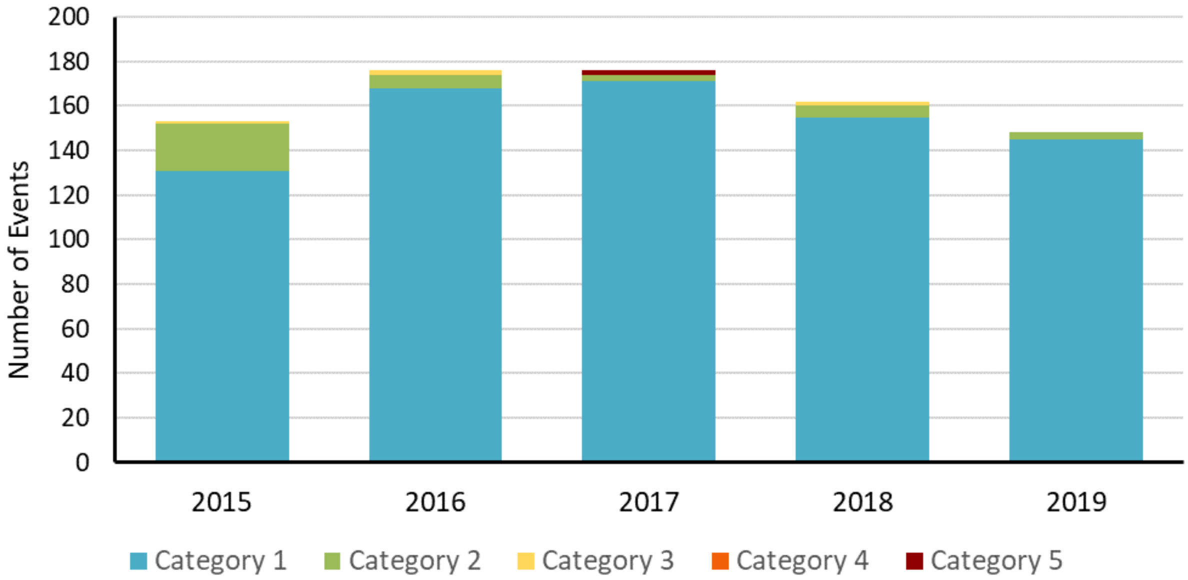


Figure 2.3: Number of Events per Category by Year

Figure 2.4 indicates the event root cause trend to date. Of particular note, the largest contributors remain Management/Organization and Design/Engineering causes and are discussed in more detail in the **Event Trends** section.

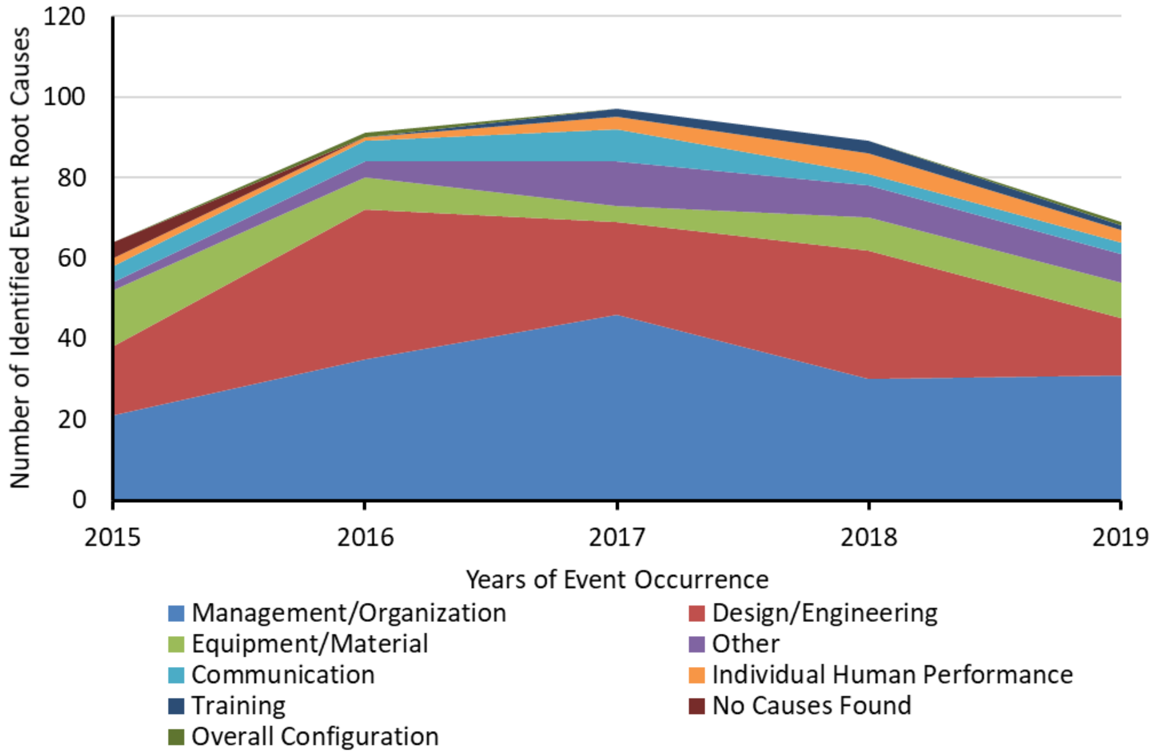


Figure 2.4: 2015–2019 Identified Event Root Causes (Processed to Date)

Event Trends

There were 148 BPS events reported to NERC in 2019; this is comparable to the number of events reported per year in the preceding four-year period. In total, 815 event reports were submitted between 2015 and 2019. A large portion of analyzed events (50%) over the past five years did not yield a root cause, resulting in dependence on the contributing causes for insights into the associated events; the trend for this scenario is in steady decline since 2015 (see **Figure 2.5**, but note that processing of 2019 events is incomplete), potentially indicating increased familiarization with event analysis reporting system-wide. Continued focus on reporting needs and information quality will reinforce the downward trending year-over-year. Some common reasons for the less-than-optimal root cause yield include the inability to discern among competing contributing causes, reporting limited to “what” rather than “why,” and a third party (beyond the reporting entity's control/direction) influenced the outcome of the event (preventing an entity-controlled corrective action).

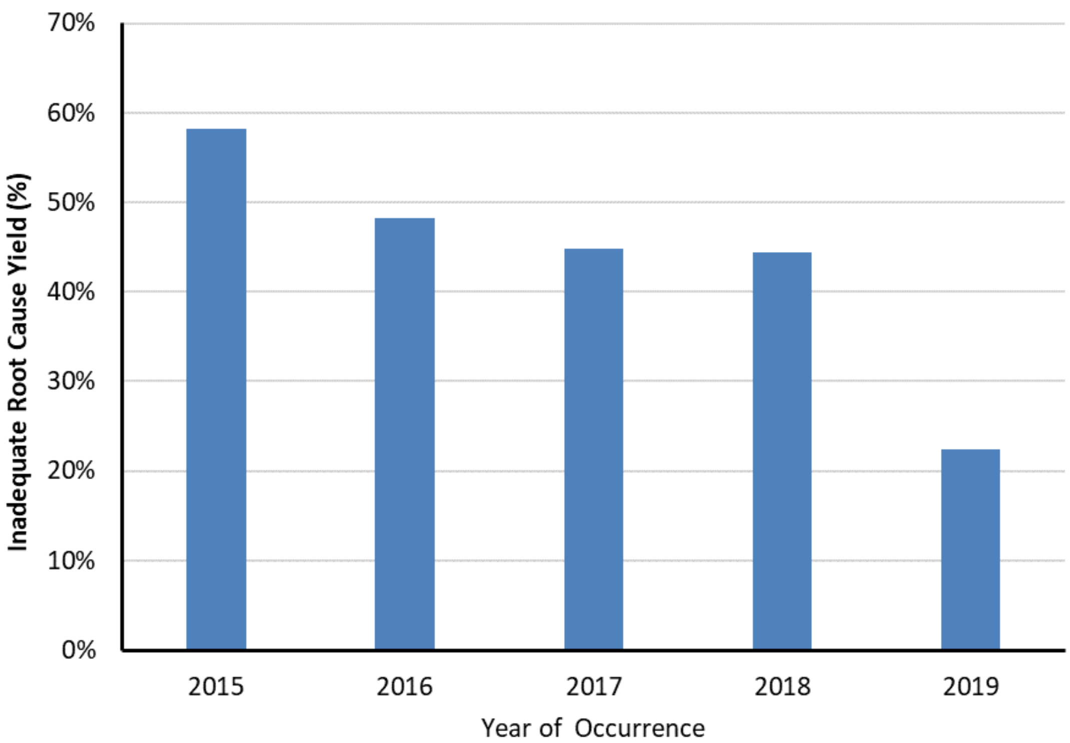


Figure 2.5: Percentage of Events with No Root Cause Identified

Of the 410 identified root causes, Management/Organization was identified as the leading root cause in 40% (see **Figure 2.6**), a total of 163 events, of all identified root causes. Some topics considered in Management/Organization causes are management/supervisory methods, resource management, work organization and planning, and change management efforts. Some examples of these causes are the correct identification of a cause for a previous event but failure to implement a good corrective action plan prior to another similar event occurring, not identifying a special circumstance that needed to be addressed during work, and failure to recognize that a second system might be impacted by work currently being performed.

Design/Engineering was the second leading cause in 30%, 123 events (see **Figure 2.6**, upper right), of all identified root causes. Cause considerations include design input, design output, documentation, installation, verification, and operability of design and/or environment issues. Some examples of these causes are shortfall in the scoping of the design because of failure to realize that a protection system was not configured to account for mutual coupling or a protection system’s timer setting was not set to allow another action to complete prior to timing out. In many cases, there were usually processes, procedures, or other barriers that either were not sufficient to catch the error or were not in use. See **Figure 2.6** for a summary of event analysis trends.

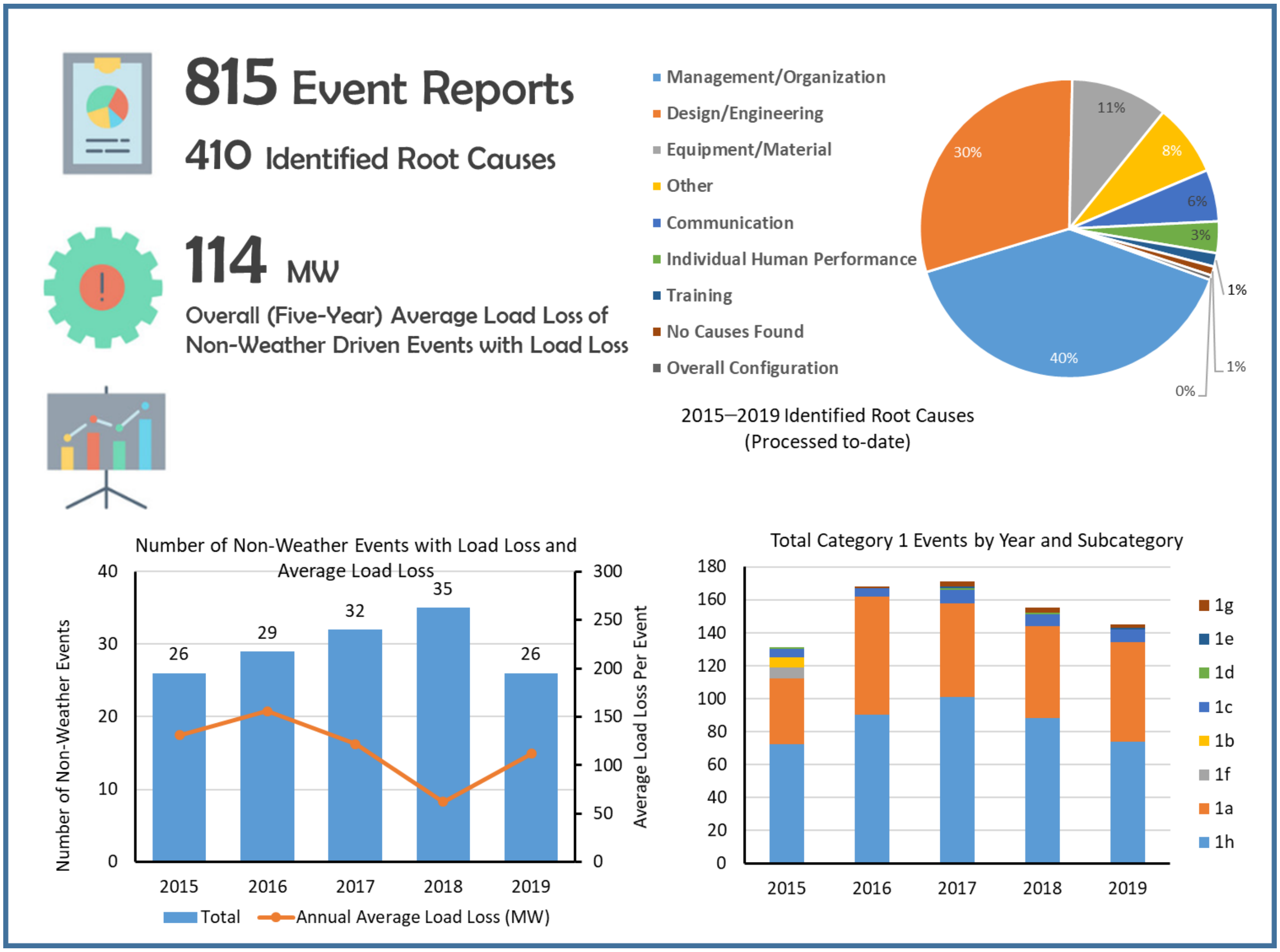


Figure 2.6: Summary of 2015–2019 Event Analysis Trends

The number of events with load loss steadily increased over the four years before returning to the first year's level of the current rolling data window (2015–2019) as shown in the lower left of **Figure 2.6**. The associated load loss averages trend remains effectively flat over the displayed periods; this demonstrates that, although there were more load loss events from year-to-year in 80% of the data period, the order of magnitude of loss remains relatively low, consistent, and not statistically significant.

The number of Category 1 events is stable over the last five years. Starting in 2016, Category 2b—Complete Loss of SCADA, Control or Monitoring Functionality for 30 Minutes or More—was retired. This resulted in future reporting of EMS-related events being shifted to Category 1h. This change in reporting resulted in a step-increase for the Category 1 total event count, shown in the lower right of **Figure 2.6**.

Review of Major Events (Category 3, 4, and 5)

No Category 3, 4, or 5 events occurred in 2019.

2019 Lessons Learned

In support of the industry led EAP, one the ERO's primary objectives is to publish lessons learned. In 2019, a total of 11 lessons learned were published. Topics covered included operations, communications, transmission facilities, and relaying and protection systems. See **Table 2.1** for a list of lessons learned published in 2019. The lifetime total for publication of lessons learned through 2019 is 160. Visit the Lesson Learned[11] page on the NERC website for a full list of lessons learned published to date.

Table 2.1: Lessons Learned Published in 2019

LL #	Category	Title
LL20191201	Generation Facilities, Transmission Facilities	Moisture Intrusion in Hermetically Sealed Metering Current Transformers
LL20190901	Communications	Risks Posed by Firewall Firmware Vulnerabilities
LL20190804	Transmission Facilities	Breaker Failure due to Multiple Reclose Attempts
LL20190803	Transmission Facilities	Inadvertent CVT Fuse Removal on a Live Circuit
LL20190802	Transmission Facilities	RAS Unexpected Operation
LL20190801	Communications	Loss of Monitoring or Control Capability due to Power Supply Failure
LL20190503	Communications	Telecom Provider Failure Induced Loss of ICCP from Regional Neighbors
LL20190502	Communications	Enhanced Alarming Can Help Detect State Estimator and Real-Time Contingency Analysis Issue
LL20190501	Transmission Facilities	Automatic Capacitor Operations along Radial Feed Result in Load Shed
LL20190202	Generation Facilities, Transmission Facilities	Substation Fires: Working with First Responders
LL20190201	Generation Facilities, Transmission Facilities	Current Drone Usage

[11] https://www.nerc.com/pa/rrm/ea/Pages/Lessons-Learned.aspx

Chapter 3: Reliability Indicators

This chapter provides a summary of the reliability indicators established by the ERO in concert with the Performance Analysis Subcommittee. Reliability indicators tie the performance of the BPS to a set of reliability performance objectives defined by NERC. Reliability performance objectives are established and defined using NERC's definition of adequate level of reliability (ALR). Each reliability indicator is mapped to a specific performance objective and is then evaluated to determine whether the actual performance of the system meets the expectations of ALR. Trending is also developed (typically, a prior five-year historical period), which helps determine whether certain aspects of reliability are improving, declining, or stable. A summary and additional details on methods and approaches follows.

Reliability Indicators and Trends

The reliability indicators below represent four core aspects to system performance that are measurable and quantifiable:

- **Resource Adequacy:** Does the system have enough capacity, energy, and ancillary services?
- **Transmission Performance and Availability:** Is the transmission system adequate to deliver electricity to all loads reliably?
- **Generation Performance and Availability:** Is the generation fleet energy limited?
- **System Protection and Disturbance Performance:** Will the system withstand disturbances and remain stable?

Reliability performance and trends of individual metrics should be evaluated within the context of the entire set of metrics.

Metrics are rated on a four-point color scale:

- **Red:** Actionable, may lead to key finding
- Yellow: Monitor
- **White:** Stable or no change
- **Green:** Improving

Table 3.1 summarizes the reliability indicators categories and names, the color scale applied, and links to each indicator's chapter of details.

Some of the reliability indicators have been evaluated to determine whether they exhibit statistically significant trends or whether the year-on-year changes all fall within a narrower band of confidence. Where statistically significant trends are observed, NERC uses the following notation:

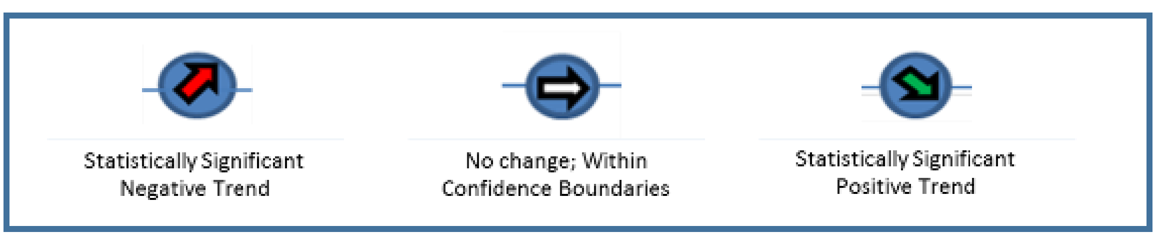


Table 3.1: Summary of Reliability Indicators		
Indicator Category	**Indicator Name**	**2019 Performance and Trend Results**
Resource Adequacy	Planning Reserve Margin	Texas RE-ERCOT Assessment Area
	Energy Emergency Alerts	Eastern Interconnection
		Western Interconnection
		Texas Interconnection
		Québec Interconnection
Transmission Performance and Unavailability	Transmission-Related Events Resulting in Loss of Load	Transmission greater than 100kV
	Automatic AC Transmission Outages	Protection System
		Human Error
		AC Substation Equipment
		AC Circuit Equipment
	Automatic AC Transformer Outages	Protection System
		Human Error
		AC Substation Equipment
	Transmission Element Unavailability	AC Circuits
		Transformers
Generation Performance and Availability	Weighted-Equivalent Generation Forced Outage Rate	Conventional Generation greater than 20 MW
System Protection and Disturbance Performance	Interconnection Frequency Response	Eastern Interconnection
		Western Interconnection
		Texas Interconnection
		Québec Interconnection
	Disturbance Control Standard Metric	Disturbance Recovery Period
	Protection System Misoperations	BES Protection Systems
	Interconnection Reliability Operating Limit Exceedances	Expanded Eastern Interconnection
		Western Interconnection
		Texas Interconnection

Resource Adequacy

For this report, two measures have been selected to indicate the status of resource adequacy for the BES: Planning Reserve Margin and EEAs. Planning Reserve Margin presents the forward-looking perspective on whether sufficient resources are expected to be available to meet demand. The EEAs provide real-time indication of potential and actual energy emergencies within an Interconnection.

Planning Reserve Margin

Planning Reserve Margin	Texas RE-ERCOT Assessment Area

This metric counts the number of areas reporting "adequate," "marginal," or "inadequate" Planning Reserve Margins for the 2019 summer and 2019/2020 winter. NERC assesses resource adequacy by evaluating each assessment area's Planning Reserve Margins relative to its Reference Margin Level. On the basis of projected reserves, NERC determines the associated risk by using the following framework:

- **Adequate:** Anticipated Reserve Margin is greater than Reference Margin Level, and there is a high degree of expectation in meeting all forecast parameters.
- **Marginal:** Anticipated Reserve Margin is greater than Reference Margin Level and there is a low degree of expectation in meeting all forecast parameters, or the Anticipated Reserve Margin is slightly below the Reference Margin Level and additional and sufficient Tier 2 resources are projected.
- **Inadequate:** Anticipated Reserve Margin is less than the Reference Margin Level; load interruption is likely.

Definition and Calculation

The Planning Reserve Margin determines the amount of committed capacity a given assessment area expects compared to the projected net internal demand. Each assessment area is evaluated annually through the long-term and seasonal assessment processes (21 assessment areas are currently evaluated). This metric counts the number of assessment areas reporting "marginal" or "inadequate" for NERC's prior year *Summer Reliability Assessment* and *Winter Reliability Assessment* according to the size of the assessment area (small <10,000 MW, medium 10,000–25,000 MW, and large >25,000 MW).

Rating

- **Red (actionable)**: There is at least one inadequate large assessment area.
- **Yellow (monitor)**: There is more than one small or medium inadequate assessment area.
- **White (stable)**: There is at least one marginal, no inadequate assessments.
- **Green (good/improving)**: There are no marginal or inadequate assessments.

Purpose

The purpose of the Planning Reserve Margin is to determine how many areas and to what extent capacity deficiencies can be expected. Planning Reserve Margins cannot precisely predict capacity deficiencies, but areas below the Reference Margin Level indicate a higher probability of a capacity deficiency occurring than the desired target of 1-day-in-10 years.

This indicator answers the following questions:

- What assessment areas are anticipating potential capacity deficiencies?
- How likely is a capacity deficiency?
- How significant is the potential capacity deficit?

2019 Performance and Trends

In 2019, the reserve margin assessment reported for Texas RE-ERCOT assessment area was determined by the ERO's reliability assessment process to be "inadequate" for the 2019 summer peak in comparison to the ERCOT Reference Margin Level of 13.75%. Between Summer 2018 and Summer 2019, ERCOT's Anticipated Reserve Margin decreased from 10.9% to 8.5% driven by higher load growth, a planned generator retirement, and delays in new generation. ERCOT anticipated that peak demand days could trigger EEAs and operating mitigations, such as increased imports into the area.

Texas RE-ERCOT: Large Assessment Area

2019 Anticipated Reserve Margin: 8.52%

Amount Needed to Meet Reference Margin Level: 3,802 MW

Figure 3.1 shows the 2019 summer peak Planning Reserve Margin by assessment area.

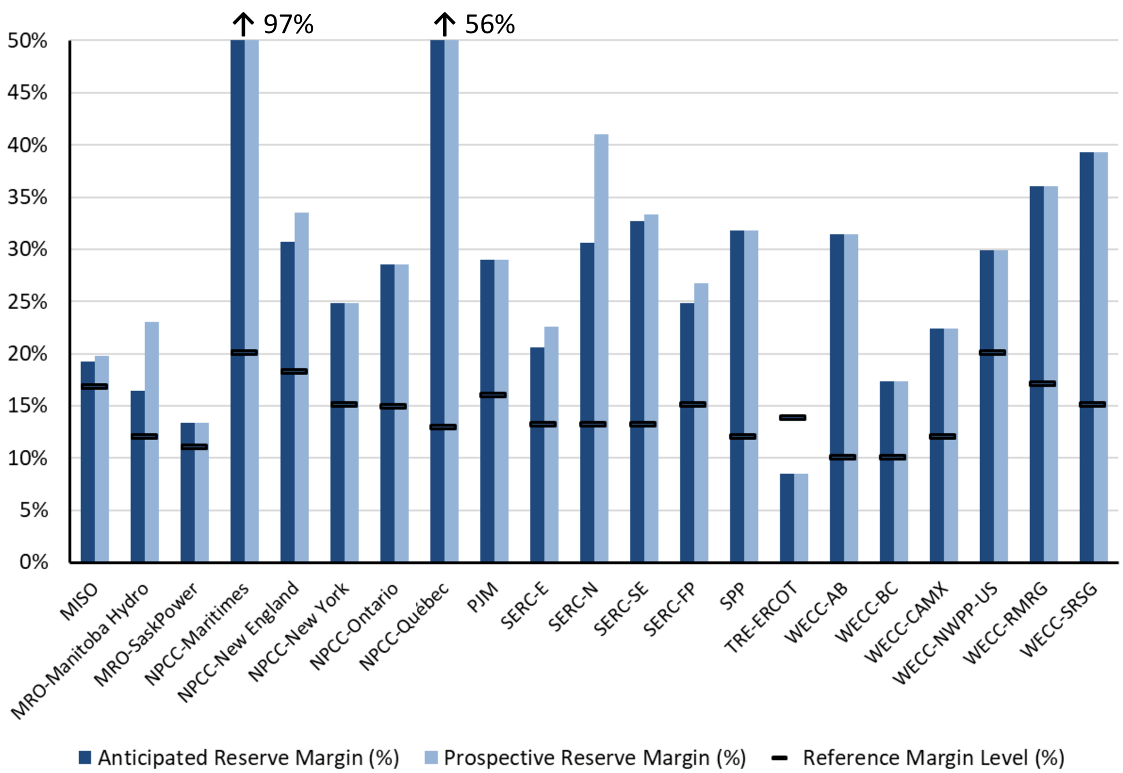


Figure 3.1: 2019 Summer Peak Planning Reserve Margins (Anticipated and Prospective Reserve Margins)

Planning Reserve Margins are NERC's primary long-term resource adequacy indicator. In order to provide more granular insight into the availability of resources to meet expected peak demand on a seasonal basis, NERC publishes an operational risk analysis for each assessment area in its seasonal reliability assessments. For example, the *2019 Summer Reliability Assessment* examined resource and demand scenarios and the potential impact that they could have on maintaining expected operating reserve requirements established by ERCOT.[12] The waterfall chart in **Figure 3.2** shows that typical generation outages during Summer 2019 could be expected to result in energy emergencies in

[12] ERCOT risk assessment developed by NERC using 2019 *Summer Reliability Assessment* data and additional data from Texas RE-ERCOT and the ERCOT 2019 *Preliminary SARA*

ERCOT on peak load days, and more severe load or generation outage scenarios had the potential to require load shedding for management. The scenario is based on historic ranges or expectations for generation maintenance outages, forced outages, and capacity derates as well as normal and extreme peak demand scenarios. NERC uses risk analysis such as this to enhance its resource adequacy assessments in each assessment area.

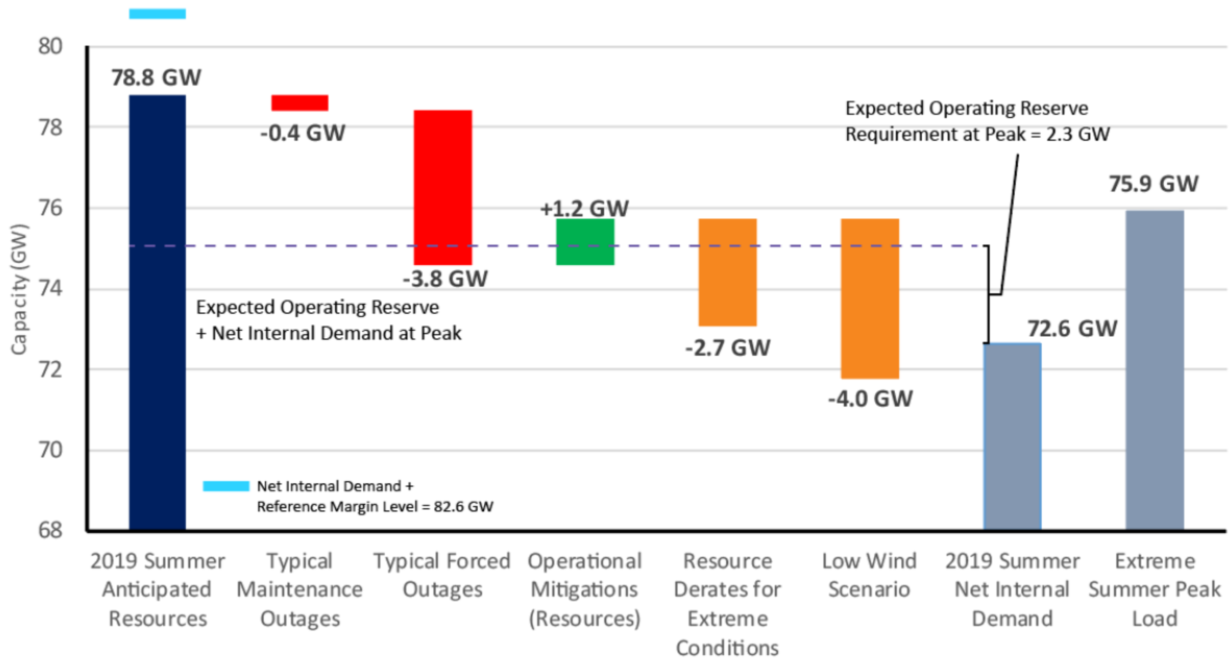


Figure 3.2: Texas RE-ERCOT Seasonal Risk Assessment

Operators in ERCOT faced challenging conditions during the 2019 summer but required minimal use of emergency alerts to maintain sufficient resources. After a cool start, Texas experienced very hot temperatures in August and September. EEAs were issued on two occasions in mid-August. ERCOT set a new system-wide peak demand record of 74.67 GW on August 12, 2019. Sufficient resources were available to remain above reserve requirements, primarily due to higher-than-average performance from wind generation resources and low total generator outages during the period of peak demand.[13]

ERCOT's energy-only wholesale electricity market relies on price signals to maintain reliability. Most generators are owned by merchant companies that compete in the market to serve ERCOT load. Prior to Summer 2019, ERCOT and the Public Utility Commission of Texas instituted designs for the Texas electricity market to support optimal performance, including expanding the triggering mechanism for scarcity pricing that provides maximum payouts to generators when supply is needed most. Price-responsive demand is also a component of the market that supports reliability. Operators in Texas use market drivers to incentivize generation, reduce outages, and manage demand during peak conditions.

Source, Assumptions, and Limitations

This data is gathered and reported annually as part of the NERC long-term and seasonal reliability assessments. The reports are the *2019 Summer Reliability Assessment*,[14] the *2019/2020 Winter Reliability Assessment*,[15] and the *2019 Long-Term Reliability Assessment*.[16]

---

[13] ERCOT review of Summer 2019: http://www.ercot.com/content/wcm/lists/172485/Review_of_ERCOT_Summer_2019_-_PUC_Workshop_-_FINAL_10-8-19.pdf

[14] https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_SRA_2019.pdf

[15] https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC%20WRA%202019_2020.pdf

[16] https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_LTRA_2019.pdf

Energy Emergency Alerts

Energy Emergency Alerts	Eastern Interconnection
	Western Interconnection
	Texas Interconnection
	Québec Interconnection

NERC has established three levels of EEAs that allow for communication of emerging energy emergencies among Balancing Authorities (BAs) and Reliability Coordinators (RCs) within an Interconnection. This metric measures the duration and number of times EEAs of all levels are issued and when firm load is interrupted due to an EEA Level 3 declaration. EEA Level 3 declarations indicate that firm load interruption is imminent or in progress due to the inability of meeting minimum contingency reserve requirements. However, not all EEA Level 3 alerts lead to an operator-controlled firm load interruption.

Rating

- **Red (actionable)**: Year over year count increase and continues to be above the five-year average.
- **Yellow (monitor)**: Year over year count increase and first year that it is above the five-year average.
- **White (stable)**: Reporting year over year count is no change and is less than five-year average.
- **Green (good/improving)**: Year over year count improvement and less than the five-year average or zero.

Definition and Calculation

These metrics track EEA declarations for BAs when actual capacity and/or energy deficiencies occur as defined by EOP-011-1.[17]

Purpose

The purpose of an EEA is to provide real-time indication of potential and actual energy emergencies within an Interconnection. EEA trends may provide an indication of BPS capacity, energy, and transmission insufficiency. This metric may also provide benefits to the industry when considering correlations between EEA events and Planning Reserve Margins.

This indicator answers the following questions:

- How often is the BPS in an energy emergency condition?
- What areas are experiencing the most energy emergency conditions?

[17] Copy of EOP-011-1: https://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-011-1.pdf

2019 Performance and Trends

In 2019, a total of 20 EEA Level 3 alerts were declared, this is three more than the previous year. Some increase in EEA Level 3 alerts can be attributed to change in resource mix and change in RCs. The most common reason for EEA Level 3 alert declaration was to recover reserves.

Figure 3.3 shows the year-over-year changes in EEA 3 by Interconnection. The 20 EEA Level 3 alerts declared in 2019 lasted a total of 27.65 hours. The largest load loss associated with an EEA Level 3 in 2019 was 150 MW. In 2019, there was one EEA Level 3 alert in the Québec Interconnection resulting in no firm load shedding and no EEA Level 3 events in the Texas Interconnection.

It is noteworthy that the Western Interconnection experienced significantly more EEA Level 3 events in 2019 that leads to a red rating. However, only two of the EEA Level 3 events in the Western Interconnection resulted in firm load shedding. The Eastern Interconnection experienced significantly fewer EEA Level 3 events in 2019, but this was still above the 5-year average that leads to a yellow rating. The Québec Interconnection experienced more EEA Level 3 events in 2019 and this is above the 5-year average that leads to a yellow rating. The Texas Interconnection has had no EEA Level 3 events in the past five years that leads to a green rating.

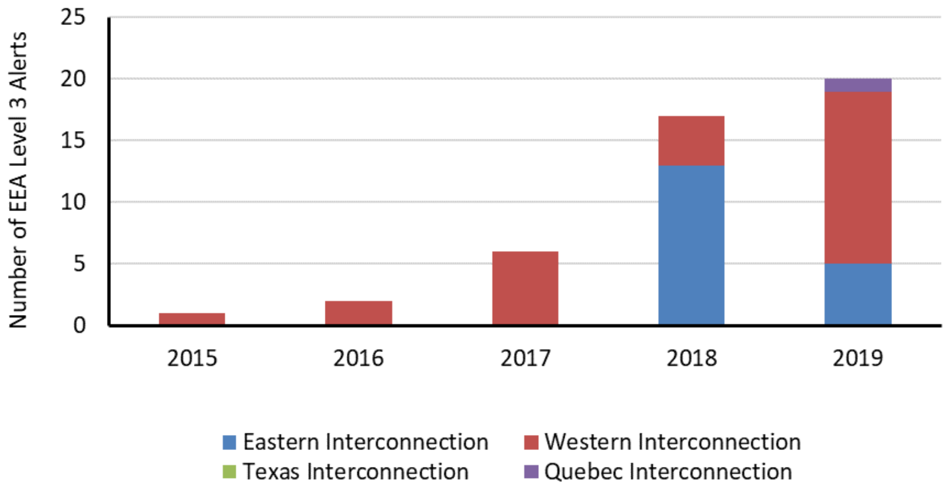


Figure 3.3: Number of EEA Level 3 Alerts by Interconnection, 2015–2019

Source, Assumptions, and Limitations

NERC collects data from RCs when an EEA is declared:

- Metric Worksheet[18]
- NERC Reliability Standard EOP-011-1[19]

[18] https://www.nerc.com/comm/PC/Performance%20Analysis%20Subcommittee%20PAS%202013/ALR6-2_clean.pdf

[19] https://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-011-1.pdf

Transmission Performance and Unavailability

When evaluating transmission reliability, an important concept is that transmission line outages have different impacts to BPS reliability. Some impacts could be very severe, such as impacting other transmission lines and load loss. Additionally, some outages are longer than others—long duration outages could leave the transmission system at risk for longer periods of time. A Transmission Availability Data System (TADS) event is an unplanned transmission incident that results in the automatic outage (sustained or momentary) of one or more elements.

TADS event information was analyzed for the following indicators in this section:

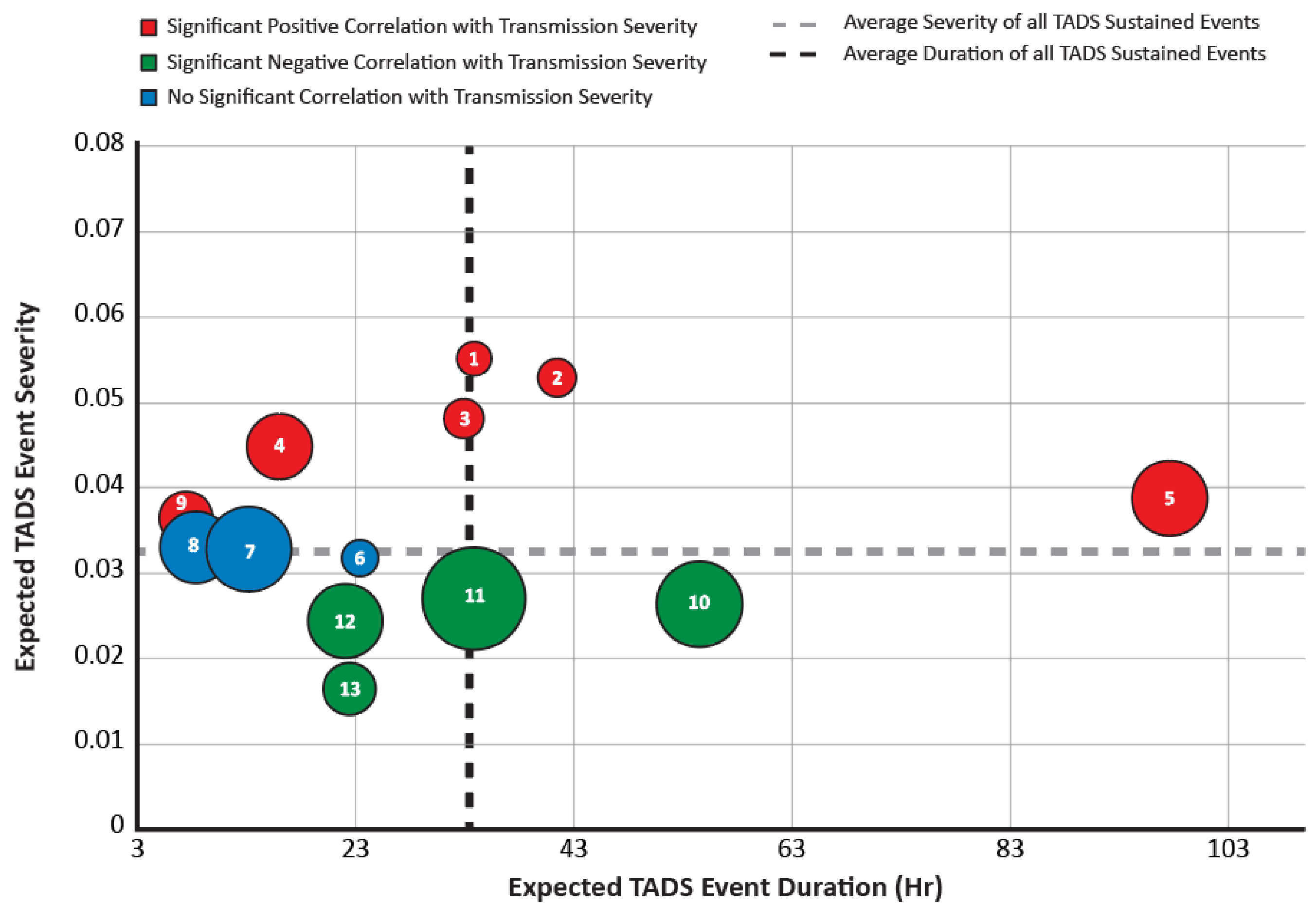
- Transmission Outage Severity
- Automatic AC Transmission Outages
- Automatic AC Transmission Outages
- Transmission Element Unavailability

The number of qualified events that include transmission outages not related to weather that resulted in firm load loss is also provided below.

Transmission Outage Severity

The impact of a TADS event to BPS reliability is called the transmission outage severity (TOS) of the event, which is defined by the number of outages in the event and by the type and voltage class of transmission elements involved in the event. TADS events are categorized by initiating cause codes (ICCs). These ICCs facilitate the study of cause-effect relationships between each event's ICC and event severity.

By examining the average TOS, duration, and frequency of occurrence for events with different ICCs (see **Figure 3.4**) it is possible to determine which ICCs contribute most to reliability performance for the time period considered. The average TOS for an ICC's events is displayed on the Y-axis. A higher TOS for an ICC indicates more outages or higher voltage elements were involved in an event. The average duration for a given ICC's events is displayed on the X-axis; events with a longer duration generally pose a greater risk to the BPS. The number of ICC occurrences is represented by the bubble size, larger bubbles indicate an ICC occurs more often. Lastly, the color represents statistical correlation, or lack thereof, relative to other ICCs.



1: Power System Condition
2: Fire
3: Combined Smaller ICC Groups
4: Misoperation
5: Failed AC Substation Equipment
6: Other
7: Unknown
8: Lightning
9: Human Error
10: Failed AC Circuit Equipment
11: Weather, Excluding Lightning
12: Foreign Interference
13: Vegetation

Figure 3.4: Transmission Outage Severity vs. Expected TADS Event Duration

An analysis of the total TOS by year indicates a statistically significantly improving trend for the last five years (see Figure 3.5), a positive indication that transmission outages are leading to less severe reliability impacts.

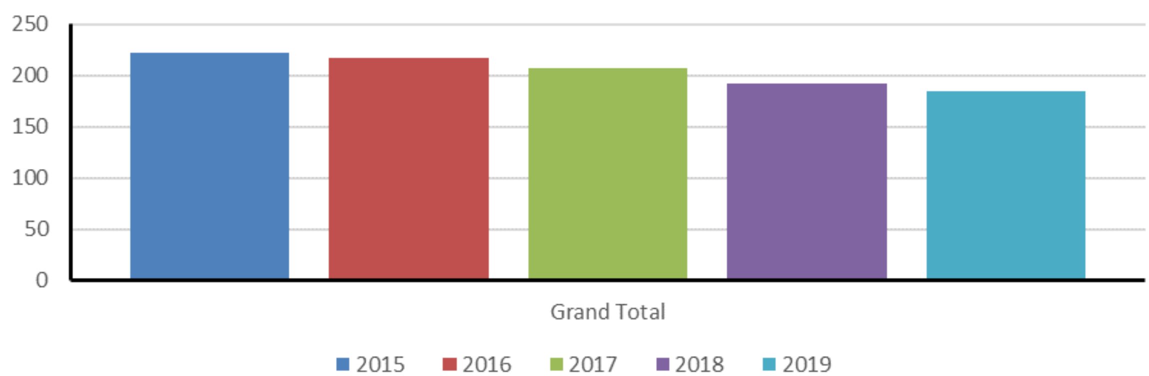


Figure 3.5: TOS of TADS Sustained Events of 100 kV+ AC Circuits and Transformers by Year

Transmission-Related Events Resulting in Loss of Load

Transmission-Related Events Resulting in Loss of Load	Transmission greater than 100kV

This metric counts BPS transmission-related events resulting in the loss of firm load, excluding weather-related outages. Additional metrics measure the duration and magnitude of the firm load loss.

Definition and Calculation

An "event" is an unplanned disturbance that produces an abnormal system condition due to equipment failures/system operational actions that result in the loss of firm load. The reporting criteria for such events are as follows:[20]

- The loss of firm load for 15 minutes or more:
  - 300 MW or more for entities with previous year's demand of 3,000 MW or more
  - 200 MW or more for all other entities
- A BES emergency that requires manual firm load shedding of 100 MW or more
- A BES emergency that resulted in automatic firm load shedding of 100 MW or more via automatic under-voltage or UFLS schemes or SPS/RAS[21]
- A transmission loss event with an unexpected loss within an entity's area, contrary to design, of three or more BES elements caused by a common disturbance (excluding successful automatic reclosing) that results in a firm loss of load of 50 MW or more
- Excludes weather related events

Rating

- **Red (actionable)**: The count of events and MW of load loss increased from the year before or the count of events or MW of load loss are greater than median value.
- **Yellow (monitor)**: MW load loss increased from year before or stable and greater than median value.
- **White (stable)**: The count of events or MW of load loss is slightly less than median value or the same as the year before and below the median value.
- **Green (good/improving)**: The count of events and MW of load loss for the year is less than the year before and below median value or count of events is zero.

Purpose

The purpose of this metric is to track transmission related events that result in loss of firm load. This allows planners and operators to validate their design and operating criteria, assuring acceptable performance of the system.

This indicator answers the following questions:

- How many transmission-related events occur on the BPS that lead to loss of firm load?
- How much firm load loss occurred during these events?

---

[20] ALR 1-4 Reporting Criteria: http://www.nerc.com/comm/PC/Performance%20Analysis%20Subcommittee%20PAS%202013/ALR1-4_Revised.pdf

[21] https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf. This document defines SPS as a special protection system and a RAS as a remedial action scheme.

2019 Performance and Trends

In 2019, seven distinct transmission events resulted in loss of firm load meeting the reporting threshold (see **Figure 3.6**); analysis indicates no discernable trend in the number of events. The median firm load loss over the past five years was 186 MW. In 2019, the median was 387 MW. This represents an increase in both the number and amount of firm load loss from 2018 levels. Although it is notable that the load loss level in 2019 is nearly twice the median in some previous years, no discernable trend in the number of events or amount of loss is identifiable.

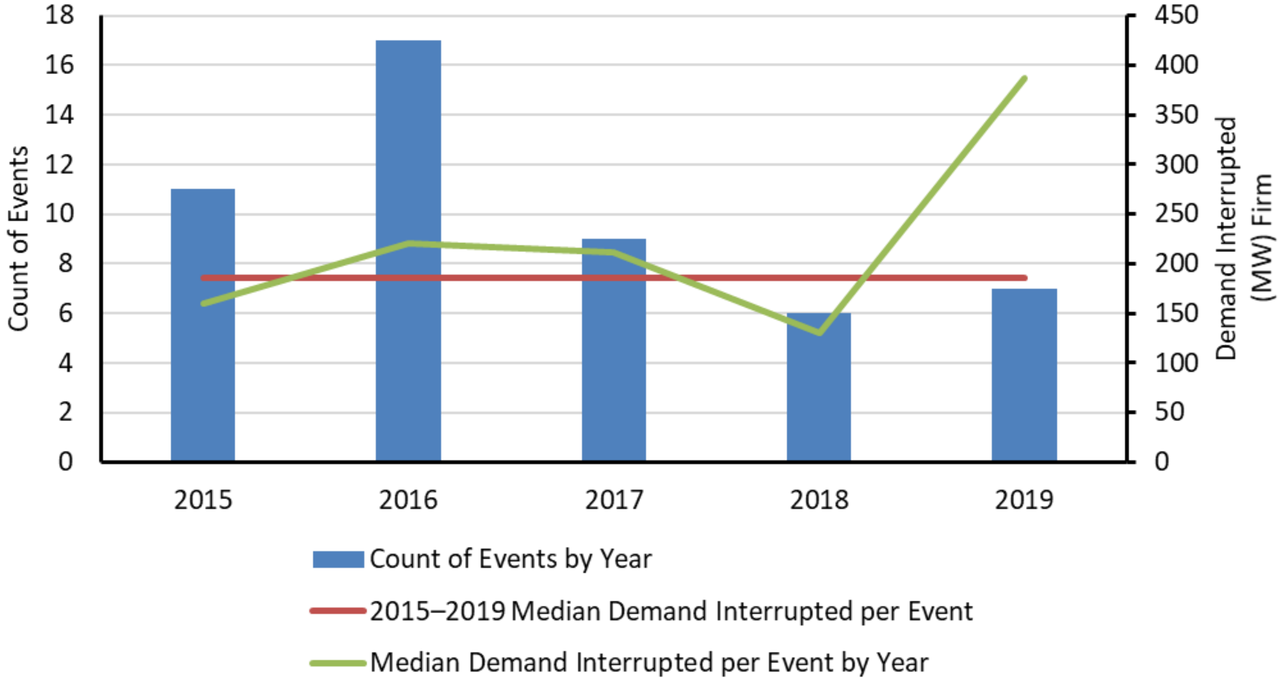


Figure 3.6: Transmission-Related Events Resulting in Loss of Firm Load and Median Amount of Firm Load Loss, 2015–2019

Source, Assumptions, and Limitations

NERC collects data from RCs when an EEA is declared:

- Reliability Standard EOP-004-3[22]
- NERC EAP
- Metric Worksheet[23]

[22] Reliability Standard EOP-004-3: https://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-004-3.pdf

[23] https://www.nerc.com/comm/PC/Performance%20Analysis%20Subcommittee%20PAS%202013/ALR1-4_Revised.pdf

Automatic AC Transmission Outages

Automatic AC Transmission Outages	Protection System
	Human Error
	AC Substation Equipment
	AC Circuit Equipment

This series of metrics measures the impacts of high-risk failure modes to transmission availability. The metrics include any BES ac transmission element outages that were initiated by the following:

- **Failed Protection System:** Misoperations or failure of protection system equipment, including relays and/or control misoperations except those caused by incorrect relay or control settings
- **Human Error:** Relative human factor performance, including any incorrect action traceable to employees and/or contractors to companies operating, maintaining, and/or assisting the TO
- **Failed AC Substation Equipment:** Equipment inside the substation perimeter, including transformers and circuit breakers but excluding protection system equipment
- **Failed AC Circuit Equipment:** Equipment like overhead or underground equipment outside the substation perimeter (This is the only metric based on outages per hundred miles.)

Definition and Calculation

Normalized count (on a per circuit basis, or per 100 miles for ac circuit equipment) of 100 kV and above ac transmission element outages (i.e., momentary and sustained automatic outages) initiated by each of the high-risk failure modes. Failed AC Element Equipment counts are normalized on a per 100-mile basis.

Rating

- **Red (actionable)**: The second year the outage rate has increased and a statistically significant increasing trend continues. For ac circuit equipment, the year-over-year count increases and continues to be above the five-year average.
- **Yellow (monitor)**: The first year the outage rate has increased and has a statistically significant increasing trend. For ac circuit equipment, the year-over-year count increases and first year that it is above the five-year average.
- **White (stable)**: No statistically significant difference in the outage frequency or a decline in the outage rate. For ac circuit equipment, no change in year-over-year count and is less than five-year average.
- **Green (good/improving)**: Statistical improvement and statistically significant decreasing trend or zero. For ac circuit equipment, year-over-year count is improved and less than the five-year average or zero.

Purpose

The purpose of this metric is to evaluate high-risk failure modes for transmission availability as a factor in the performance of the transmission system.

This indicator answers the following questions:

- What is the impact of these high risk failure modes on transmission availability?
- How are active mitigation measures impacting transmission performance?

2019 Performance and Trends

In terms of availability, the performance of the transmission system in 2019 has improved over the last four years (See **Figure 3.7** and **Figure 3.8**). Statistically significant reductions in 100 kV+ AC Circuit Transmission Outages Due To Failed Protection System Equipment, Human Error, and Failed AC Substation Equipment were observed in 2019 leading to overall improvements in transmission availability.

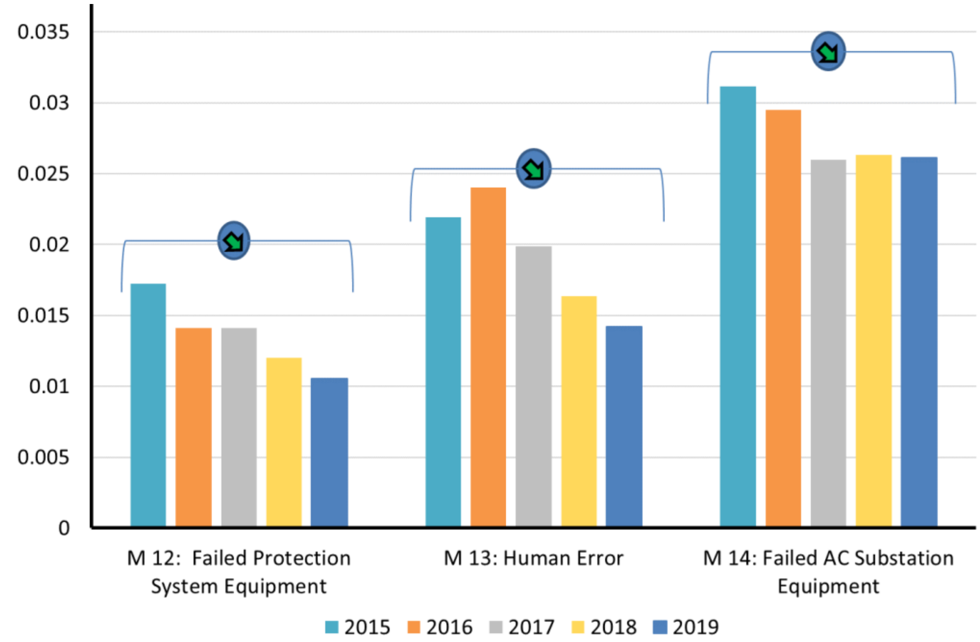


Figure 3.7: Number of Outages per Circuit due to Various Initiating Causes

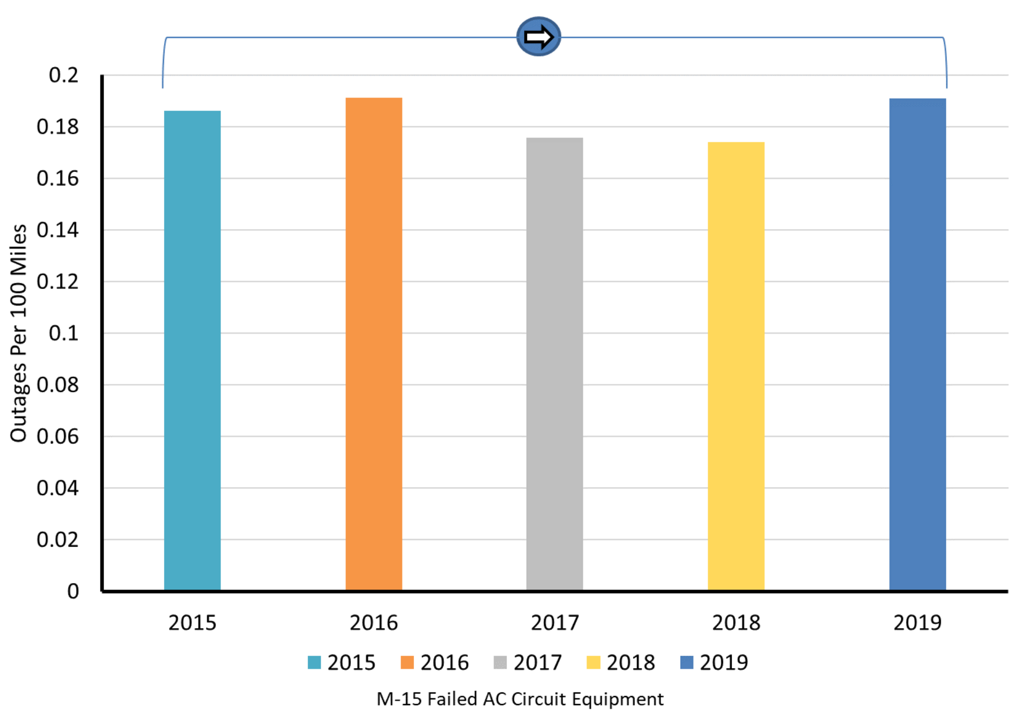


Figure 3.8: Number of Outages per Hundred Miles due to Failed AC Circuit Equipment

Source, Assumptions, and Limitations

TADS provides the total number and causes of automatic transmission system outages and for all transmission lines 100 kV and above.

Automatic AC Transformer Outages

Automatic AC Transformer Outages	Protection System
	Human Error
	AC Substation Equipment

This series of metrics measure the impacts of high risk failure modes to transformer availability. The metrics include any BES ac transformer outages that were initiated by the following:

- **Failed Protection System:** Misoperations or failure of protection system equipment, including relays and/or control misoperations except those caused by incorrect relay or control settings
- **Human Error:** Relative human factor performance, including any incorrect action traceable to employees and/or contractors to companies operating, maintaining, and/or assisting the TO
- **Failed AC Substation Equipment:** Equipment inside the substation perimeter, including transformers and circuit breakers but excluding protection system equipment

Definition and Calculation

Normalized count (on a per transformer basis) of 100 kV and above ac transformer outages (i.e., TADS momentary and sustained automatic outages) that were initiated by each of the high risk failure modes.

Rating

- **Red (actionable)**: The second year the outage rate has increased and a statistically significant increasing trend continues.
- **Yellow (monitor)**: The first year the outage rate has increased and has a statistically significant increasing trend.
- **White (stable)**: No statistically significant difference in the outage frequency or a decline in the outage rate.
- **Green (good/improving)**: Year-over-year statistical improvement and statistically significant decreasing trend or zero.

Purpose

The purpose of this metric is to evaluate high risk failure modes for transformer availability as a factor in the performance of the transmission system.

This indicator answers the following question:

What is the impact of these high risk failure modes on transformer availability?

2019 Performance and Trends

From 2015 through 2019, the trend of automatic ac transformer outages caused by Failed Protection System Equipment and Failed AC Substation Equipment is stable and flat. Human Error initiated outages saw a statistically significant decrease in 2019. A slight decrease in the number of overall outages per transformer was observed in 2019 for outages caused by Failed Protection System Equipment and Failed AC Substation Equipment; however, these are within normal performance and not statistically significant.

See **Figure 3.9** for the number of outages per transformer due to various initiating causes.

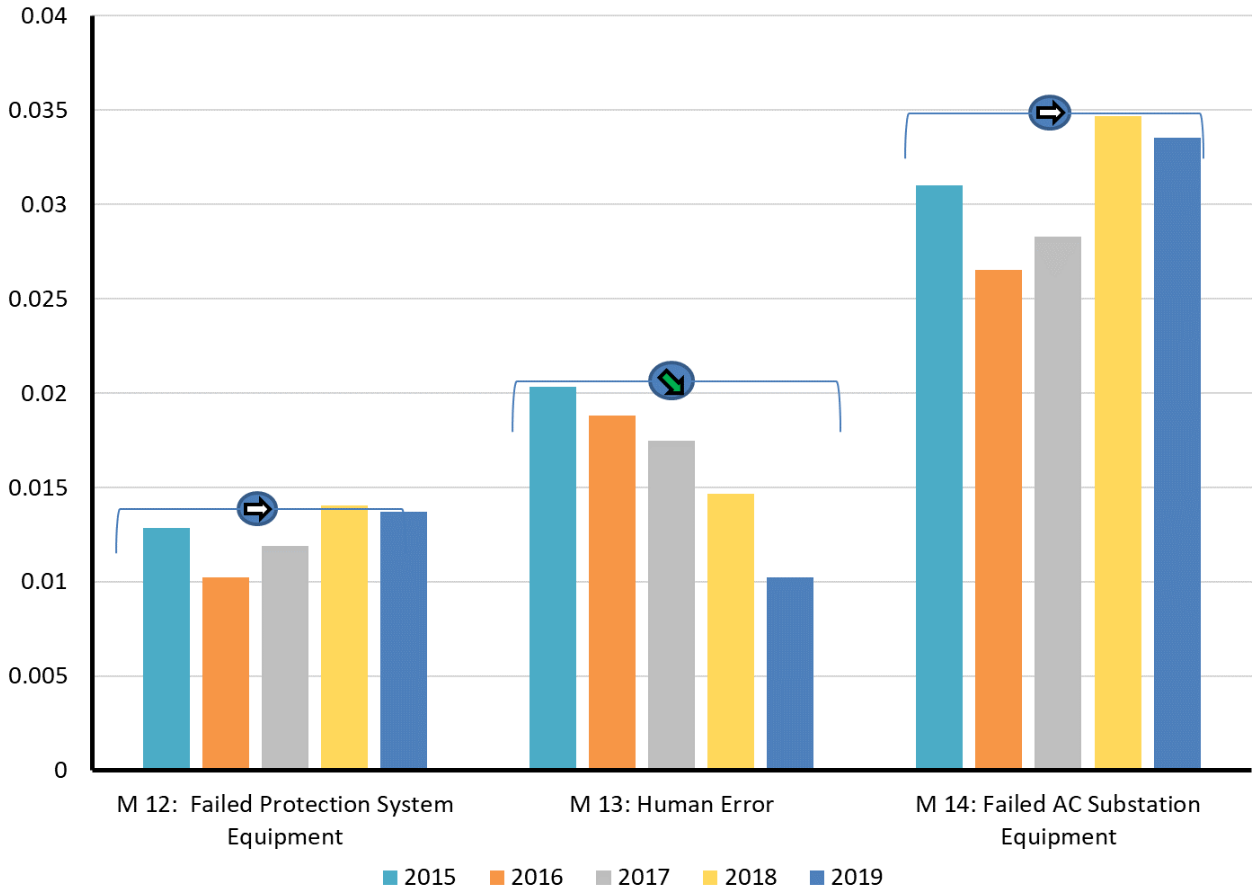


Figure 3.9: Number of Outages per Transformer Due to Various Initiating Causes

Source, Assumptions, and Limitations

The NERC TADS provides the total number and causes of automatic transformer outages for transformers 100 kV and above.

Transmission Element Unavailability

Transmission Element Unavailability	AC Circuits
	Transformers

This metric determines the percentage of BES ac transmission elements (i.e., transmission lines and transformers) that are unavailable when outages due to automatic and operational events are considered. Transmission and transformer outages can degrade the performance of the transmission system that can result in congestion, equipment overloads, and, in some instances, to cascading conditions and blackout. See **Figure 3.10** and **Figure 3.11**.

Definition and Calculation

This metric is calculated by determining the overall percent of transmission system elements (i.e., ac lines and transformers 200 kV and above) that are unavailable for service due to sustained automatic and non-automatic outages. These outages are broken down into automatic (sustained) and non-automatic (operational) outages. Momentary outages are not considered in this metric.

Rating

- **Red (actionable)**: Year-over-year count increase and continues to be above the five-year average.
- **Yellow (monitor)**: Year-over-year count increase and first year that it is above the five-year average.
- **White (stable)**: Year-over-year count is no change and is less than five-year average.
- **Green (good/improving)**: Year-over-year count improvement and less than the five-year average or zero.

Purpose

The purpose of the transmission element unavailability metric is to identify the availability of transmission elements and any availability trends, including geographic and causal that may need monitoring or mitigation. Unavailability is shown rather than availability in an effort to show why transmission was unavailable (e.g., automatic vs. operational outages).

This indicator answers the following question:

How often are transmission lines and transformers unavailable?

2019 Performance and Trends

In 2019, ac circuits over 200 kV across NERC had an unavailability rate of 0.27% (meaning, at any given time, there is a 0.27% chance that a transmission circuit is unavailable due to sustained automatic and operational outages). Transformers had an unavailability rate of 0.31% in 2019. **Figure 3.10** and **Figure 3.11** show very little variability in these metrics over five years, but 2019 was the second highest year of the five-year analysis period, slightly lower than 2016 in both ac circuit and transformer unavailability.

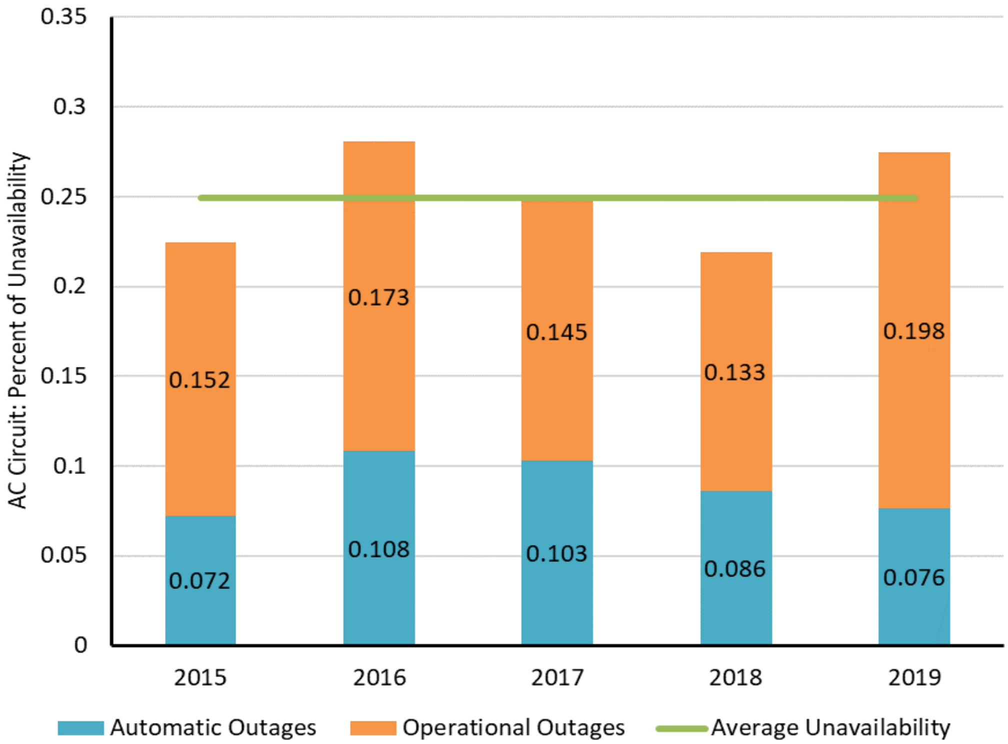


Figure 3.10: AC Circuit Unavailability

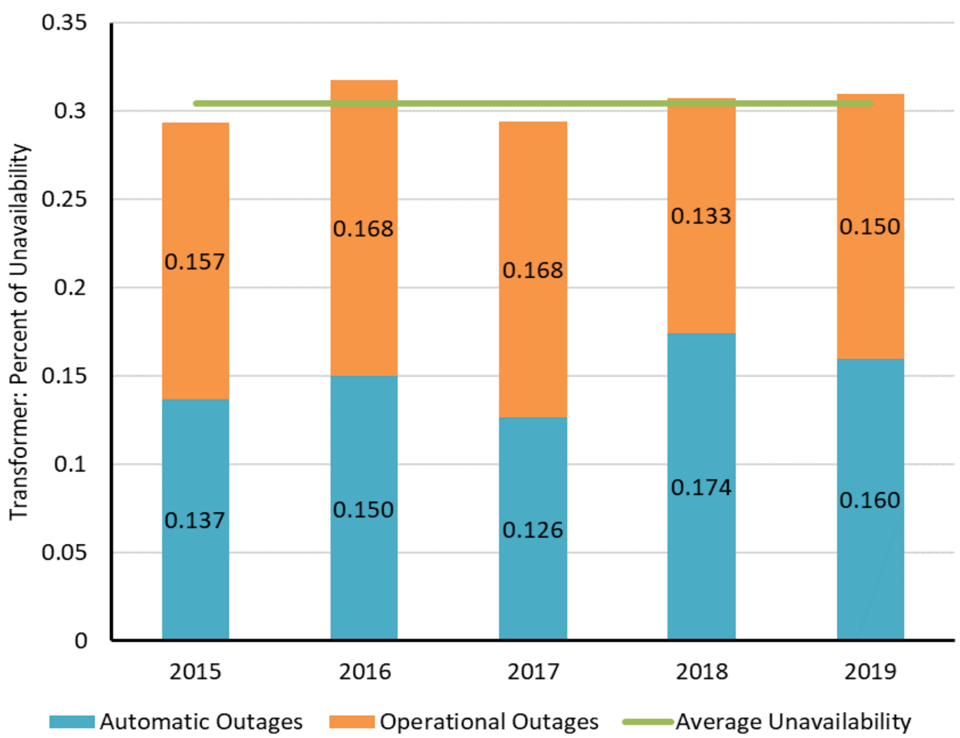


Figure 3.11: Transformer Unavailability

Source, Assumptions, and Limitations

The NERC TADS provides the total number and duration of automatic and non-automatic transmission system outages. Planned outages are not included in the unavailability values.

Generation Performance and Availability

Generating Availability Data Systems (GADS) contains information that can be used to compute reliability measures, such as megawatt-WEFOR. GADS collects and stores unit operating information. By pooling individual unit information, overall generating unit availability performance and metrics are calculated. The information supports equipment reliability, availability analyses, and risk-informed decision making to industry. Reports and information resulting from the data collected through GADS are used by industry for benchmarking and analyzing electric power plants.

Weighted-Equivalent Generation Forced Outage Rate

Weighted-Equivalent Generation Forced Outage Rate	**Conventional Generation greater than 20 MW**

The WEFOR measures the probability that a unit will not be available to deliver its full capacity at any given time while taking into consideration forced outages and derates. The mean Equivalent Forced Outage Rate (EFOR) over the five-year analysis period is 7.16%.

Definition and Calculation

WEFOR is a mean outage rate calculated by taking the sum of each unit's capacity weighted forced outage and derate hours divided by the sum of the total equivalent service, outage, and derate hours.

Rating

- **Red (actionable)**: Annual WEFOR has increased and continues to be above the five-year average.
- **Yellow (monitor)**: Annual WEFOR has increased and first year is above the five-year average.
- **White (stable)**: Annual WEFOR has no change and is less than five-year average.
- **Green (good/improving)**: Annual WEFOR has decreased and less than the five-year average or zero.

Purpose

WEFOR measures the probability that a unit will not be available to deliver its full capacity at any given time due to forced outages and derates. Individually, these statistics provide important information to plant owners in an effort to benchmark and improve the performance of their own generators. In aggregate, the statistics help inform system planners about how much generation, reserves, and transmission is needed to meet the reliability needs of the BPS, assuming a calculated amount of generation is unavailability.

This indicator answers the following questions:

- On average, how often are generators out of service?
- What is the trend of generation outages?
- How do generator outages differ between different fuel types?

2019 Performance and Trends

The horizontal lines in **Figure 3.12** show the annual WEFOR compared to the monthly WEFOR columns; the solid horizontal bar shows the mean outage rate over all years in the analysis period, which is 7.16% and only slightly higher than the 2019 annual WEFOR of 6.97%. The WEFOR has been fairly consistent and has a statistical distribution that is nearly an exact standard distribution. The 2019 annual WEFOR is below the five-year average, marking the first decrease since 2015.

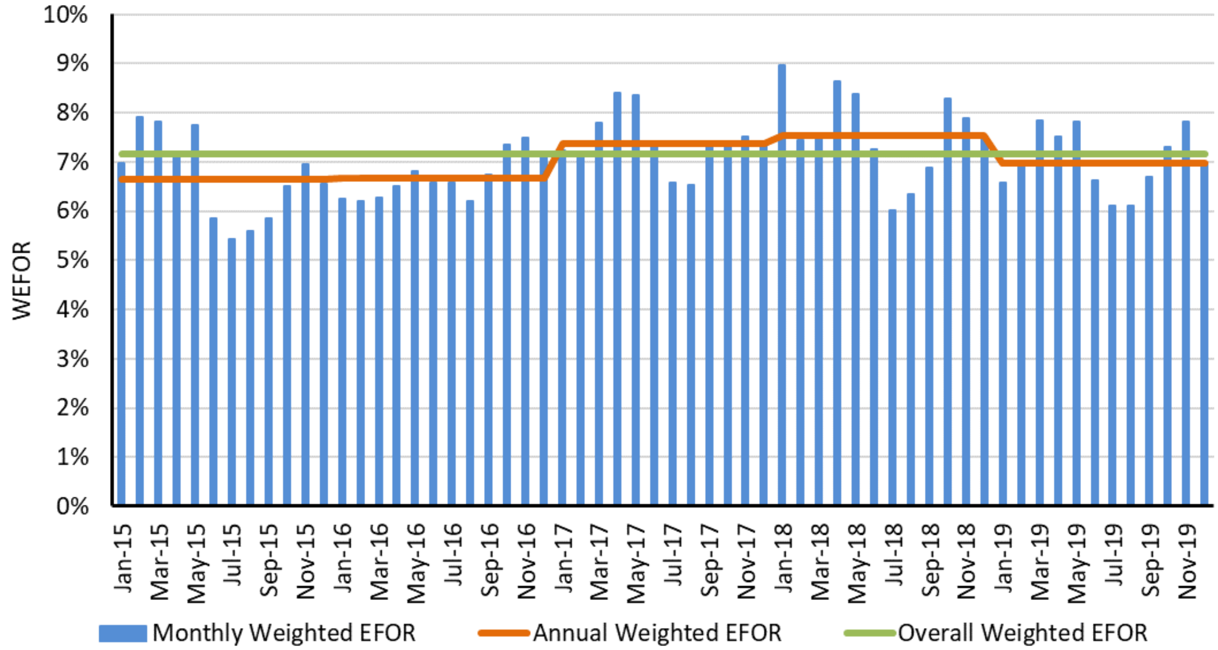


Figure 3.12: Monthly Capacity Weighted EFOR and Five-Year Rolling Average, 2015–2019

Monthly WEFOR for select fuel types is shown in **Figure 3.13**. The dashed line shows the monthly WEFOR of all fuel types, and the horizontal bar shows the mean outage rate of all fuel types over the five years in the analysis period. Coal-fired generation shows a slight increasing trend over the five-year period and represents the highest forced-outage rate of all conventional fuels except during extreme winter weather when natural-gas-fired generation outages spikes above coal.

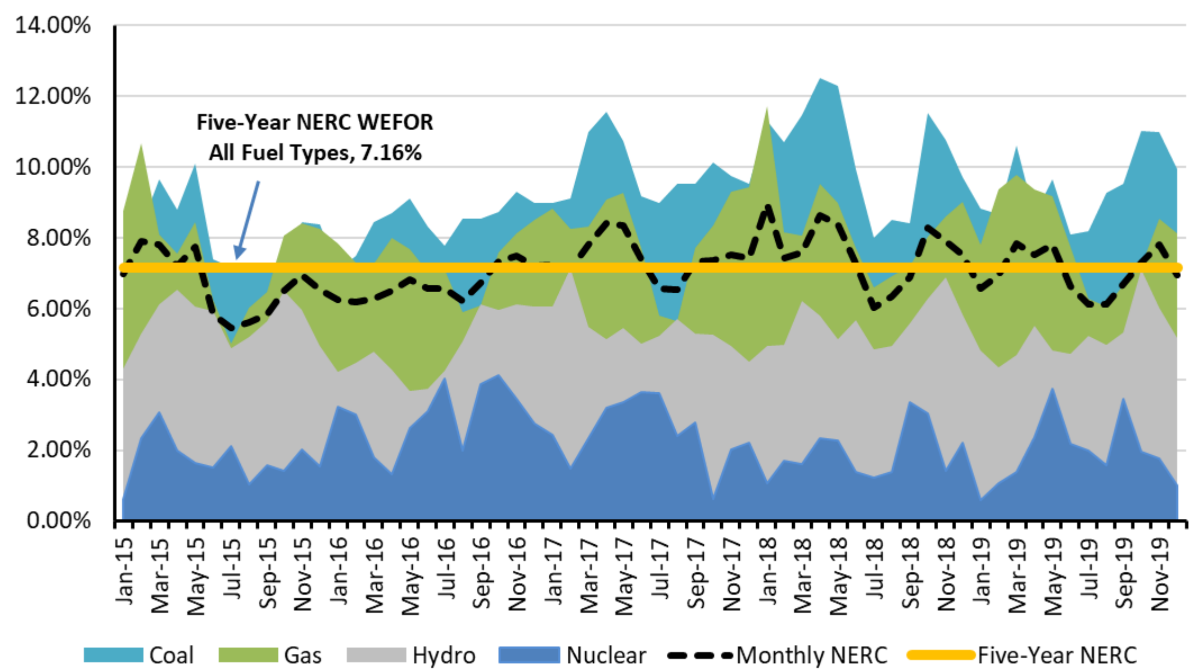


Figure 3.13: Overlaid Monthly Capacity Weighted EFOR by Fuel Type, 2015–2019

Source, Assumptions, and Limitations

NERC GADS provides the event and performance information necessary to calculate the WEFOR.

System Protection and Disturbance Performance

Reliability indicators selected to signal system protection and disturbance performance include the following:

- Interconnection Frequency Response
- Disturbance Control Standard Metric
- Protection System Misoperations
- Interconnection Reliability Operating Limit Exceedances

Interconnection Frequency Response

Interconnection Frequency Response	Eastern Interconnection
	Western Interconnection
	Texas Interconnection
	Québec Interconnection

Primary frequency response is essential for maintaining the reliability of the BPS. When there are disturbances due to the loss of generation or load, it is critical that large rapid changes in Interconnection frequency are arrested quickly and stabilized until frequency can be restored. The metric evaluates the following periods:

- **Arresting period:** The time from predisturbance frequency to the time of the frequency nadir that occurs within the first 12 seconds of the event. It is during the arresting period that the combination of system inertia, load damping, and primary frequency response provided by resources act together to limit the duration and magnitude of the frequency deviation. Loss of load events are excluded from arresting period analysis.
- **Stabilizing period:** The time after primary frequency response is deployed and the system has entered a period of relative balance and stable frequency. It is defined as the average frequency occurring between 20 and 52 seconds after the start of resource or load loss event.

Definition and Calculation

This metric is based on methods defined in the *ERS Framework Measure 1, 2, and 4 - Historical Frequency Analysis*[24] report used to calculate an interconnection frequency response performance measure ($IFRM_{A-B}$) as the ratio of the resource or load megawatt loss that initiated the event to the difference of predisturbance frequency (Value A) and the stabilizing period frequency (Value B). Measurement of frequency performance in that time period is a surrogate for the lowest frequency during the event (the nadir or Point C).

Rating

- **Red (actionable)**: Any statistical decline in the arresting period rolling five-year time trend or any instance of UFLS activation
- **Yellow (monitor)**: Statistical decline in the stabilizing period but not in the arresting period
- **White (stable)**: Improvement in arresting period or stabilizing period and no declining trend in the other period or no trend in arresting period or stabilizing period
- **Green (good/improving)**: Both arresting period and stabilizing period are statistically improving

[24] The BAL-003-1.1 standard defines PFR performance at the BA level: https://www.nerc.com/comm/Other/essntlrlbltysrvcstskfrcDL/Item_6b.ii._ERS_Historical_%20Measures_124%20_Technical%20Brief_DRAFT_%2020171107.pdf

Purpose

The purpose of this metric is to determine frequency response trends for each Interconnection so that adequate primary frequency control is provided to arrest and stabilize frequency during frequency excursions of a predefined magnitude.

This indicator answers the following questions:

- What is the performance trend for frequency response?
- How close has the system come to activating UFLS?

2019 Performance and Trends

Frequency response analysis for all of the Interconnections indicates acceptable and improving performance. The Eastern Interconnection and the Texas Interconnection showed statistically significant improvements during the arresting period from 2015 through 2019. The Texas and Western Interconnections exhibited statistically significant improvements during the stabilizing period from 2015 through 2019. In the 2019 operating year, the largest M-4 event occurred in the Québec Interconnection, which was 2,109 MW (vs. a resource loss protection criteria (RLPC)[25] of 1,700 MW), and resulted in a Point C of 58.932 Hz and a UFLS margin of 0.432 Hz from a Value A starting frequency of 60.019 Hz; the event occurred in March 2019 during the hour ending 4:00 p.m. Eastern time.

During the arresting period, the goal is to arrest frequency decline for credible contingencies before the activation of UFLS. The calculation for Interconnection frequency response obligation under BAL-003, Frequency Response and Frequency Bias Setting, is based on arresting the Point C Nadir before the first step of UFLS—for resource contingencies at or above the RLPC for the Interconnection. Measuring and tracking the margin between the first step UFLS set point and the Point C Nadir is an important indicator of risk for each Interconnection. **Figure 3.14** represents an analysis of the arresting period of M-4 events. The y-axis shows the percent UFLS margin from 100% (60 Hz) to 0% (first step UFLS set point for the Interconnection). The x-axis represents the MW loss for the event, expressed as a percentage of the RLPC for the Interconnection. Analysis for each of the Interconnections indicates an adequate level of reliability. The Western Interconnection had four events at or greater than 100% of the RLPC and maintained sufficient UFLS margin. The Québec Interconnection had five events greater than 80% of the RLPC and maintained sufficient UFLS margin. The largest events as measured by percentage of RLPC for the Eastern Interconnection and Texas Interconnection were 45% and 55%, respectively.

Frequency response for all of the Interconnections indicates stable and improving performance as shown in **Table 3.2**.

Table 3.2: 2019 Frequency Response Performance Statistics and Trend Assessment

Interconnection	2019 OY Arresting Period Performance			2019 OY Stabilizing Period Performance		
	Mean UFLS Margin (Hz)	Lowest UFLS Margin (Hz)	2015–19 OY[26] Trend	Mean $IFRM_{A\text{-}B}$ (MW/0.1 Hz)	Lowest $IFRM_{A\text{-}B}$ (MW/0.1 Hz)	2015–19 OY Trend
Eastern	0.459	0.434	Improving	2,358	1,188	Stable
Texas	0.579	0.473	Improving	909	512	Improving
Québec	1.017	0.432	Stable	688	293	Stable
Western	0.418	0.357	Stable	1,895	909	Improving

[25] The RLPC is the predetermined contingency in each Interconnection used to determine the respective Interconnection frequency response obligation.

[26] The operating year for frequency events begins on December 1 and ends on November 30 the following year in accordance with the NERC Reliability Standard BAL-003-1.

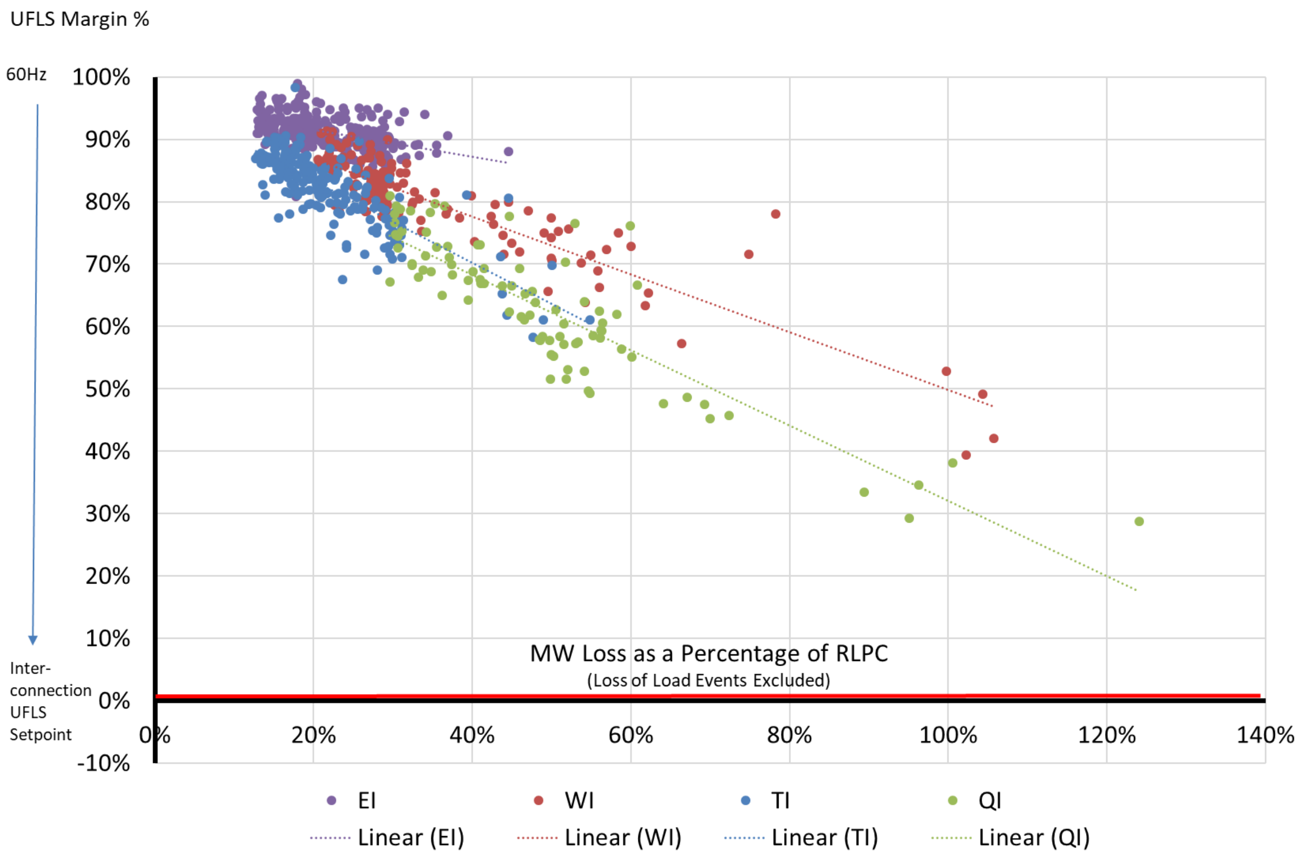


Figure 3.14: Operating Year (OY) 2015–2019 Qualified Frequency Disturbances and Remaining UFLS Margin

Source, Assumptions, and Limitations

The data supporting these findings can be found on the NERC Resources Subcommittee website.[27]

[27] https://www.nerc.com/comm/OC/Pages/Resources-Subcommittee.aspx

Disturbance Control Standard Metric

Overall Rating

Disturbance Control Standard Metric	Disturbance Recovery Period

This metric measures the ability of a BA or reserve sharing group (RSG) to balance resources and demand following reportable disturbances. NERC Reliability Standard BAL-002-3, contingency reserve, requires that a BA or RSG maintain sufficient contingency reserves equal to its most severe single contingency and recover their balance of resources and demand within the contingency event recovery period[28] for reportable balancing contingency events (RBCEs).

Definition and Calculation

The metric is calculated as a percentage of the RBCE recoveries divided by the total number of RBCEs.

Rating

- **Red (actionable)**: The recovery percentage decreased year-over-year and continues to be below the five-year average.
- **Yellow (monitor)**: The recovery percentage decreased year-over-year and is below the five-year average.
- **White (stable)**: The recovery percentage is ≥ year-over-year and is ≤ five-year average.
- **Green (good/improving)**: The recovery percentage is > year-over-year or 100% and is ≥ the five-year average.

Purpose

The purpose is to measure the ability of the BA or RSG to use contingency reserves to restore the balance of resources and demand within the system following a reportable disturbance. The results help measure the risk the system is exposed to during contingencies, the annual trend in reportable events, and how the BA or RSG's system performs when they occur.

This indicator answers the following questions:

How successful are BAs at restoring their system to predisturbance levels following RBCEs?

2019 Performance and Trends

In 2019, the total number of RBCEs was lower than each of the four previous years. Over the last five years, the average percent recovery was 99.7%. In 2019, there was only one event in which the BA did not restore its system to predisturbance levels within the contingency event recovery period. See **Figure 3.15** and **Figure 3.16**.

[28] A period that begins at the time that the resource output begins to decline within the first one-minute interval of a RBCE and extends for 15 minutes thereafter.

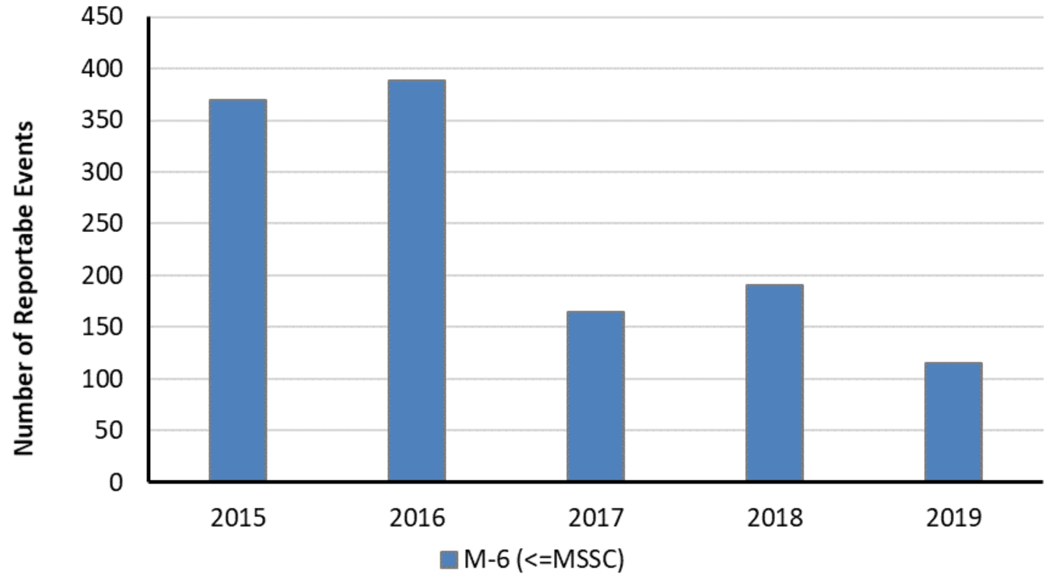


Figure 3.15: Number of Reportable Balancing Contingency Events

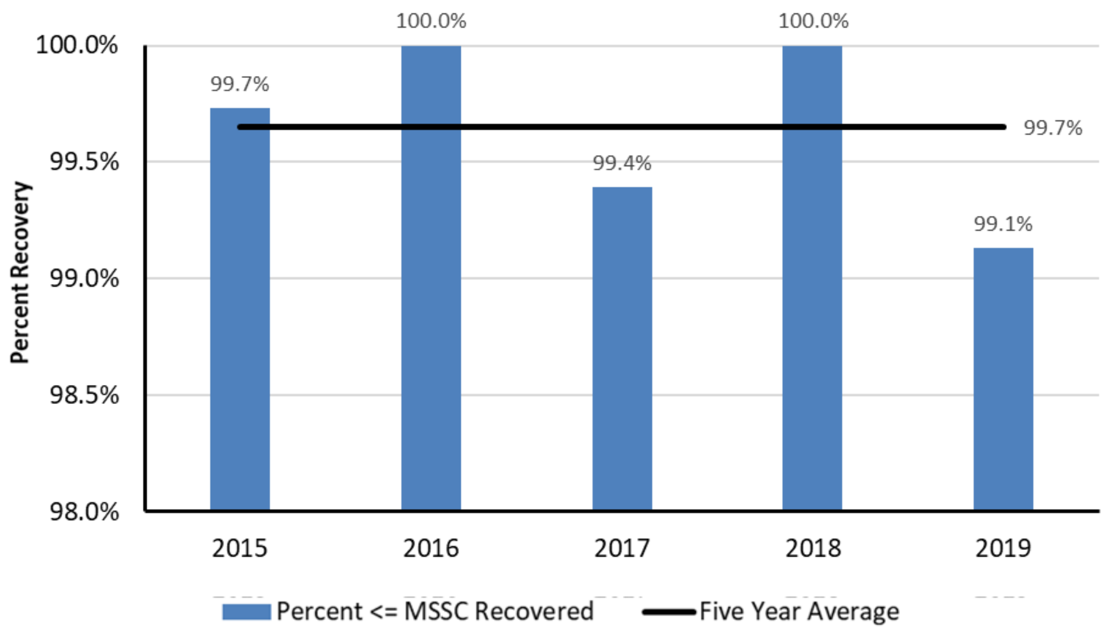


Figure 3.16: Percent of Reportable Balancing Contingency Events with 100% Recovery

Source, Assumptions, and Limitations

Prior to December 31, 2017, NERC Reliability Standard BAL-002-1[29] required that a BA or RSG report all disturbance control standard events and nonrecoveries to NERC. On January 1, 2018, NERC Reliability Standard BAL-002-2[30] became effective, which required a BA or RSG to document all RBCEs and their recoveries but no longer requires them to be reported to NERC. The disturbance control standard data used for 2018 and 2019 is from voluntary submissions from the BAs and RSGs.

[29] https://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-001-1.pdf
[30] https://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-002-2(i).pdf

Protection System Misoperations

Protection System Misoperations	BES Protection Systems

The Protection System Misoperations metric evaluates the performance of protection systems—both generator and transmission. Protection system misoperations have been identified as a major area of concern as stated in previous *State of Reliability* reports because misoperations exacerbate event impacts for the BPS.

Definition and Calculation

The metric is the ratio of protection system misoperations to total protection system operations.

Rating

- **Red (actionable)**: The misoperations rate for NERC shows a statistically significant increase compared to the past four years for more than one year.
- **Yellow (monitor)**: The misoperations rate for two REs show a statistically significant increase **or** the NERC misoperations rate shows a statistically significant increase compared to the past four years for one year.
- **White (stable)**: There is no statistically significant difference in the NERC misoperations rate compared to the past four years (there may be a numerical change in the NERC misoperations rate).
- **Green (good/improving)**: There is a statistically significant decreasing trend in the NERC misoperations rate **or** zero compared to the past four years.

Purpose

The purpose of the Protection System Misoperations metric is to calculate a misoperations rate to determine the relative performance of protection system operations and allow NERC to identify concerning or improving trends. The misoperations rate provides a consistent way to trend misoperations and to normalize for weather and other factors that can influence the count.

See **Figure 3.17** for the year-over-year changes and trends in the annual misoperations rate by RE.

This indicator answers the following questions:

- How do protection system misoperations counts compare to correct operations?
- Do protection system misoperations happen more frequently?

2019 Performance and Trends

By breaking NERC and each RE's misoperations rate out annually over the last five years then comparing the first four years with the most recent year (see **Figure 3.18**), a statistically significant decreasing trend can be observed in the misoperations rate for MRO, SERC, and NERC as a whole. No statistically significant trend is observed for NPCC, RF, Texas RE, or WECC.

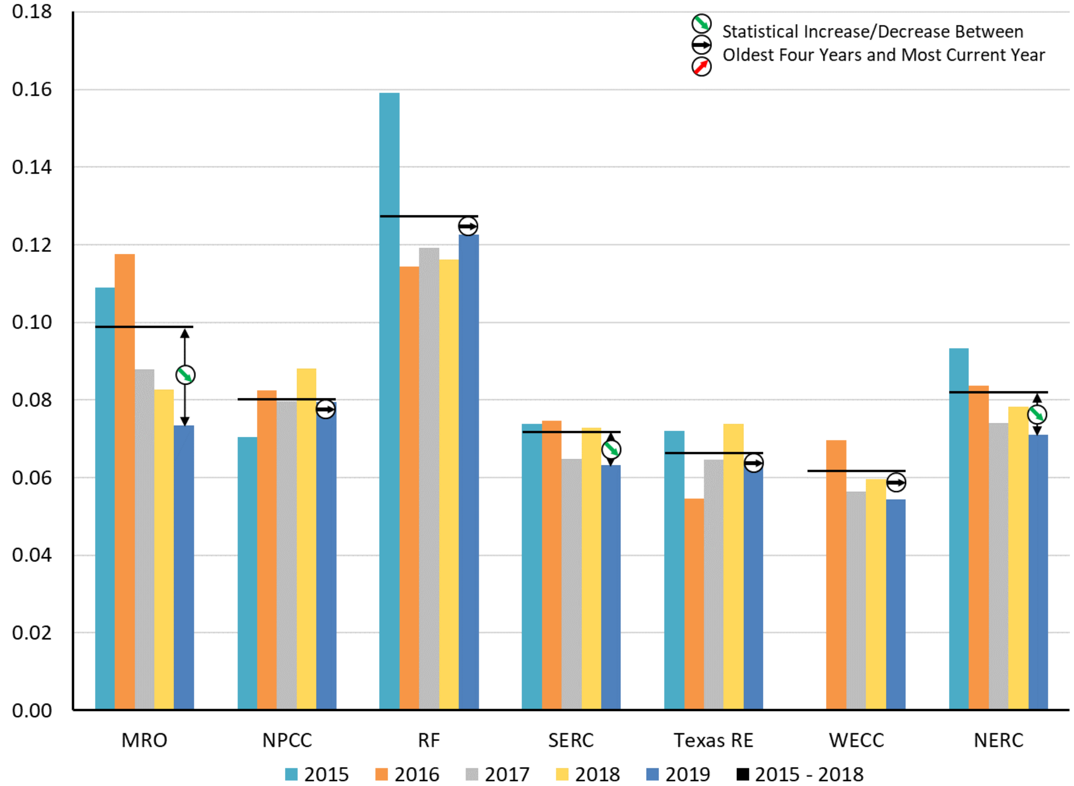


Figure 3.17: Year-Over-Year Changes and Trends in the Annual Misoperations Rate by Regional Entity

The overall NERC 2019 protection system misoperations rate is lower than the previous five years and a statistically significant downward and improving trend continues to be observed. The five-year RE protection system misoperations rate ranges from 5.96% to 12.61%.

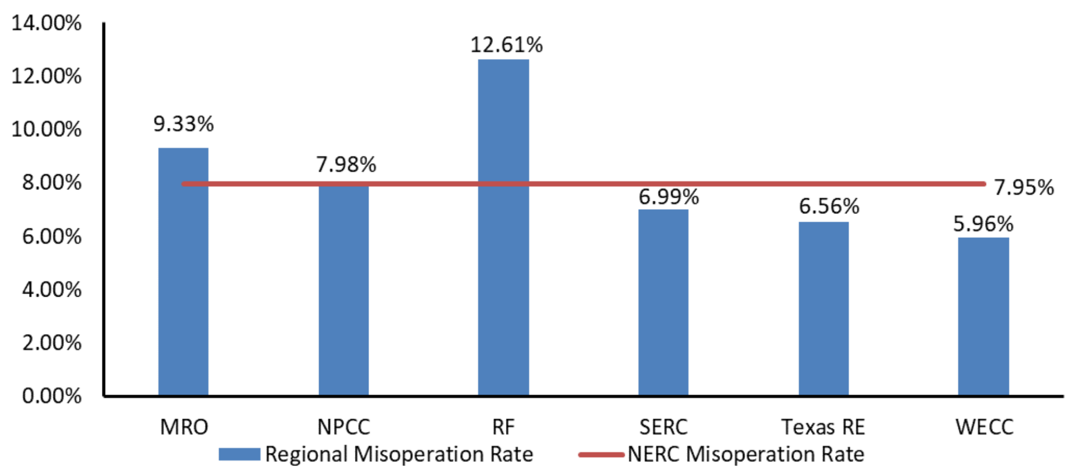


Figure 3.18: Five-Year Protection System Misoperations Rate by Regional Entity 2015 through 2019

Source, Assumptions, and Limitations

Protection system operations and misoperations are reported by TOs, Generator Owners (GOs), and Distribution Providers (DPs) via the Misoperations Information Data System (MIDAS).[31]

[31] https://www.nerc.com/pa/RAPA/Pages/Misoperations.aspx

Interconnection Reliability Operating Limit Exceedances

Interconnection Reliability Operating Limit Exceedances	Expanded Eastern Interconnection
	Western Interconnection
	Texas Interconnection

This metric measures the number of times and the duration that an IROL is exceeded. An IROL is a system operating limit that, if violated, could lead to instability, uncontrolled separation, or cascading outages. Each RC is required to operate within the IROL limits and minimize the duration of such exceedances. IROL exceedance data are reported per quarter and uses four duration intervals between 10 seconds and greater than 30 minutes. The data is presented at the Interconnection level.

Definition and Calculation

A simple number count of IROL (real-time or post-contingent) exceedances. Start and end times for IROL exceedance are recorded and the duration is grouped into four time segments as follows:

- 10 seconds ≤ time IROL has been exceeded < 10 minutes (excluded from metric)
- 10 minutes ≤ time IROL has been exceeded < 20 minutes
- 20 minutes ≤ time IROL has been exceeded < 30 minutes
- 30 minutes ≤ time IROL has been exceeded

Rating

- **Red (actionable)**: One IROL > 30 minutes or continued count of IROL< 20 minutes greater than five-year average for more than one year or continued count of IROL < 20 minutes is greater than five-year average.
- **Yellow (monitor)**: Year-over-year count increase of IROL < 30 minutes or first year count of IROL < 20 minutes is greater than five-year average.
- **White (stable)**: IROL < 20 minutes count is less than the five-year average.
- **Green (good/improving)**: Year-over-year count decrease of IROL < 30 minutes or zero, and IROL < 20 minutes is less than the five-year average or zero.

Purpose

The purpose of measuring IROL exceedances is to provide an indication of frequency and duration of IROL mitigation. Exceeding an IROL could cause widespread outages if prompt operating control actions are not taken to return the system to within normal IROL limits (see **Figure 3.19**).

This indicator answers the following questions:

- How often does the system exceed an established IROL?
- How quickly are IROL exceedances mitigated?

2019 Performance and Trends

- **Expanded Eastern Interconnection:**[32] In 2019, there were exceedances in three of the four ranges of the metric. The largest number of exceedances were in the 10-second to the 10-minute range (not shown), but the 10-minute to 20-minute range also had significantly more exceedances in 2019, with 32 this year, which is greater than those reported in previous years. There were also more exceedances in the 20-minute to 30-minute range in 2019 with 6. This totaled 38 exceedances lasting more than 10 minutes, doubling the rolling five-year average. There were no IROL exceedances reported that lasted more than 30 minutes. Some of the increase is due to the following:
  - One entity performed a review where it determined there was a need to update how they tracked and identified IROLs exceedances in real time. They found it was not clear to the operators when something was flagged as an IROL for certain equipment-related thermal exceedances. The entity then upgraded its systems and tools to address the identified issues. As a result of these changes, there was a significant increase in the number of reported IROL exceedances by this entity.
  - The aforementioned improvements were implemented in late 2018 that now provide automatic identification and tracking of IROL exceedances. The resultant increase in IROL exceedances in 2019 is attributed to water level conditions, a maintenance situation, and the improved situational awareness and tracking of IROL exceedances.
- **Western Interconnection:** Prior to 2014, only system operating limits were reported. Since 2014, the trend has been stable with no IROL exceedances reported.
- **Texas Interconnection:** The trend has been stable with no exceedances since 2013.

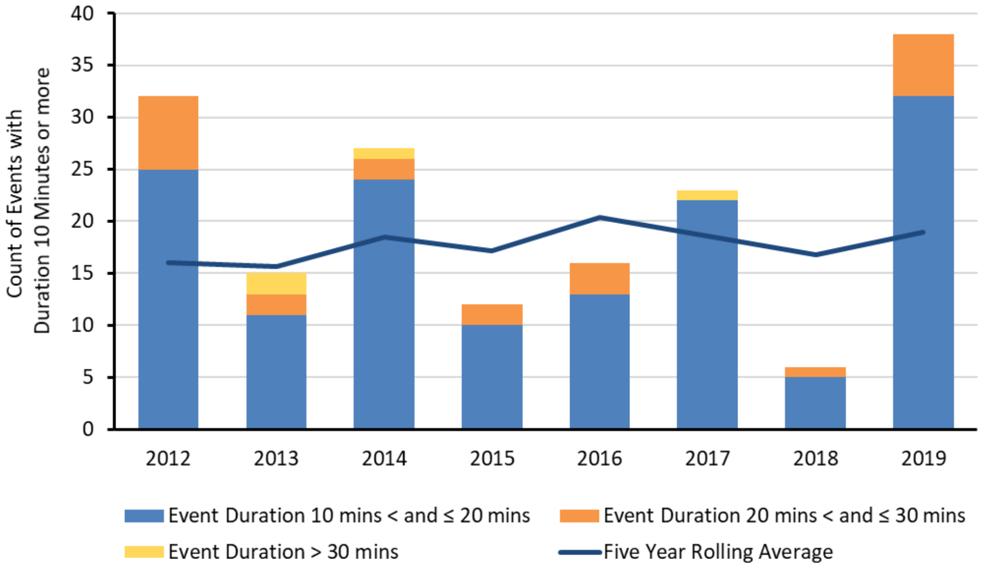


Figure 3.19: Expanded Eastern Interconnection IROL Exceedances

Each RC has a different methodology to determine IROLs based on the make-up of their area and what constitutes an operating condition that is less than desirable. The discussion of performance on an Interconnection basis is for clarity, not for comparison.

Source, Assumptions, and Limitations

RCs provide this data to NERC. Each RC currently collects and records IROL data as required by IRO-009.

[32] Expanded Eastern Interconnection includes the Eastern Interconnection and Québec Interconnection

Chapter 4: Severity Risk Index

The severity risk index (SRI) is calculated (see the following **text box**) to measure the relative severity ranking of daily conditions based on the impact on the BPS from load loss, loss of generation, and loss of transmission (see **Severity Risk Index and Trends**). This measure provides a quantitative approach to determine which days throughout a given year had more relative impact on BPS reliability. In other words, the index provides a broad picture of system performance, reliability, and resilience and allows NERC to measure and develop year-on-year trends of the relative conditions (see **Figure 4.1**).

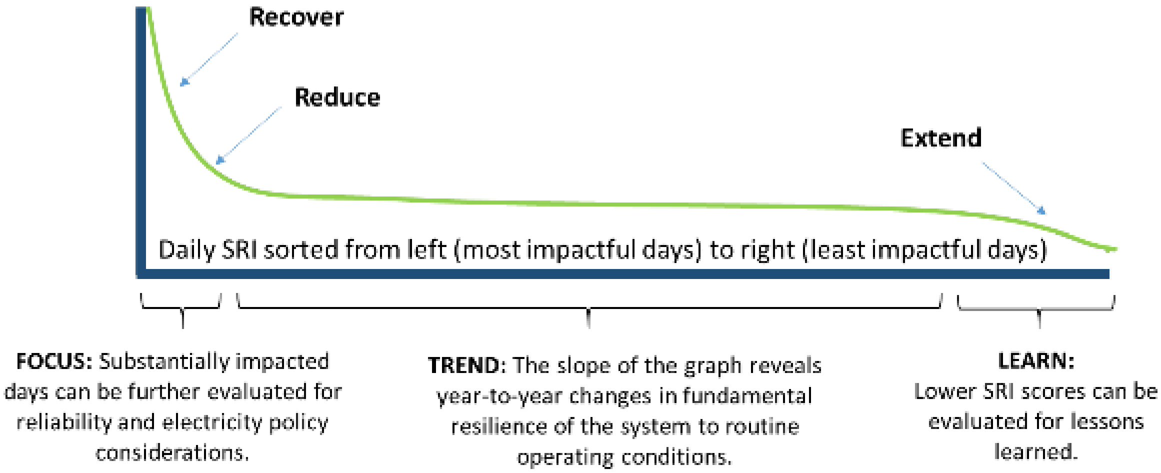


Figure 4.1: Severity Risk Index Concept

How the SRI Is Calculated

The SRI provides a daily measure of BPS performance. The metric includes the following components (**Figure 4.2**):

- **Weighted Transmission System Sustained Unplanned or Operational Outages for AC Circuits, DC Circuits, and Transformers with Voltages Greater than 100 kV:** Transmission line outages are weighted with an assumed average capacity based on their voltage level and the daily outages divided by the total inventory's average capacity and factored at 30% of the SRI score.
- **Weighted Generation System Unplanned Outages:** Generation capacity lost is divided by the monthly capacity of the generation fleet for the year being evaluated and factored at 10% of the SRI score.
- **Weighted Distribution Load Lost as a Result of Events Upstream of the Distribution System:** Distribution load lost due to performance upstream of the distribution system is calculated based on outage frequency for the day divided by system peak loading and factored at 60% of the SRI score.

With these weighted components, the SRI becomes an indicator of performance for the BPS from capacity loss, transmission outages, and load loss. This daily data is presented in various ways to demonstrate performance throughout the year, performance of the best and poorest days within the year, and the contributions of each of the components of the SRI on those key days.

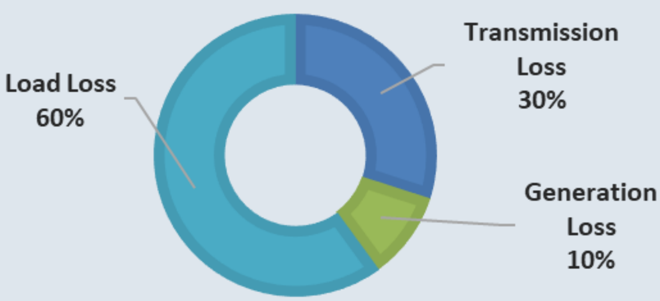


Figure 4.2: SRI Loss Components

Severity Risk Index and Trends

Figure 4.1 shows the annual cumulative performance of the BPS over the five-year period of 2015–2019, grouped by seasons within each year. Overall, 2019 had the lowest annual cumulative SRI. Seasonally, only the cumulative SRI for Fall 2015 was slightly lower than 2019.

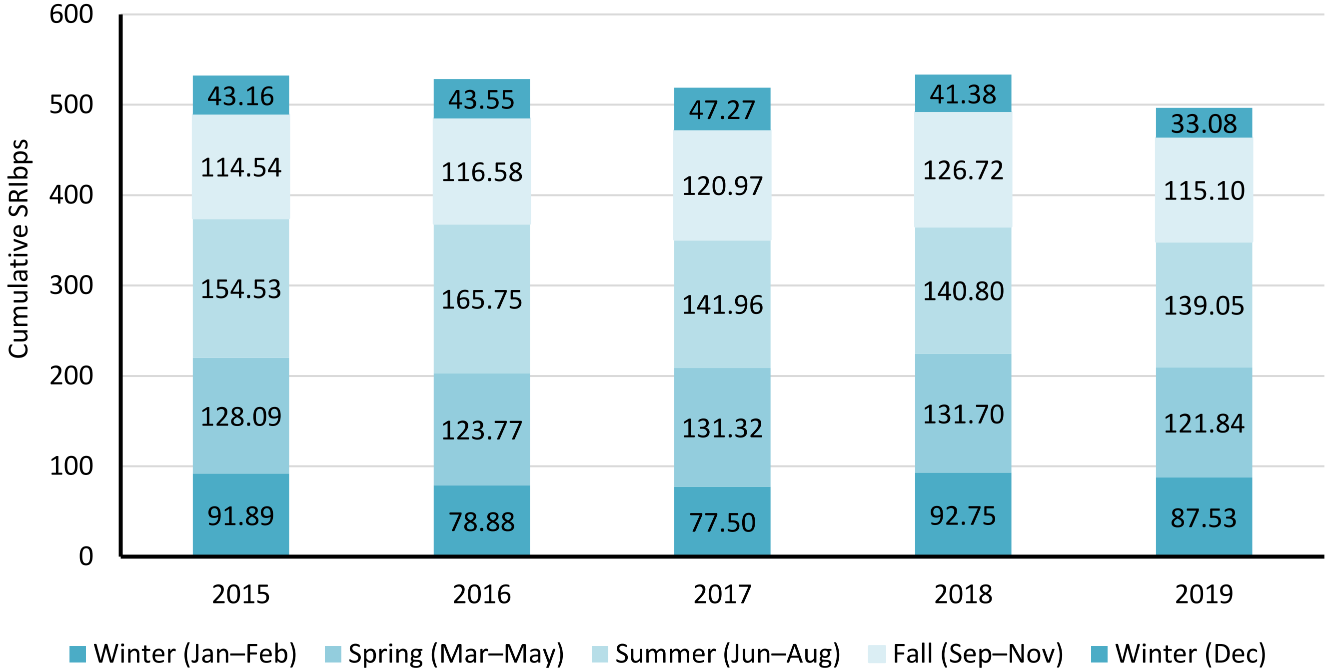


Figure 4.1: Cumulative SRI (2015–2019)

Compared to the prior cumulative SRI values over the five-year analysis period, 2019 was shown to be the most reliable. Figure 4.2 displays the SRI for each of the days in the year in descending order (from left to right); 2019 had the lowest peak SRI day and the majority of daily values were lower than all other years in the analysis period.

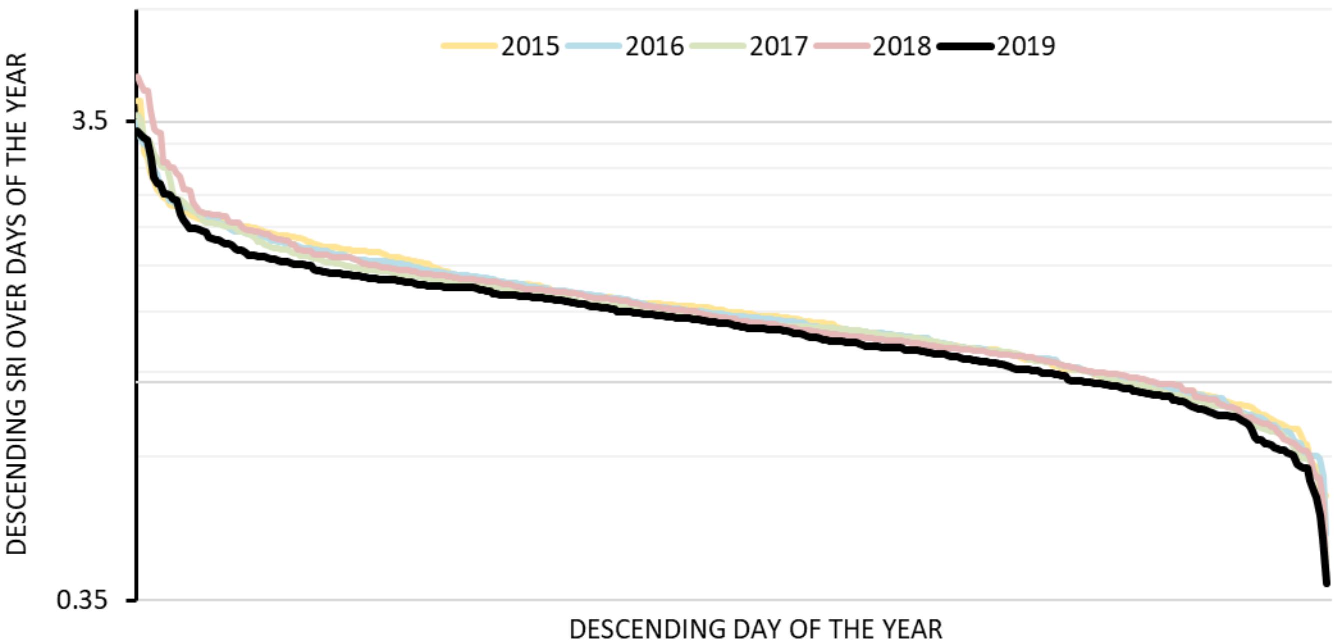


Figure 4.2: NERC Annual Daily Severity Risk Index 2015–2019

Figure 4.3 plots the daily SRI scores for 2019 against control limits that were calculated using 2015–2018 seasonal daily performance. On a daily basis, a general normal range of performance exists, which is visible by the gray colored band or within the daily seasonal 90% control limits.[33] Days of stress are identified by those that extend above the seasonal daily control limits.

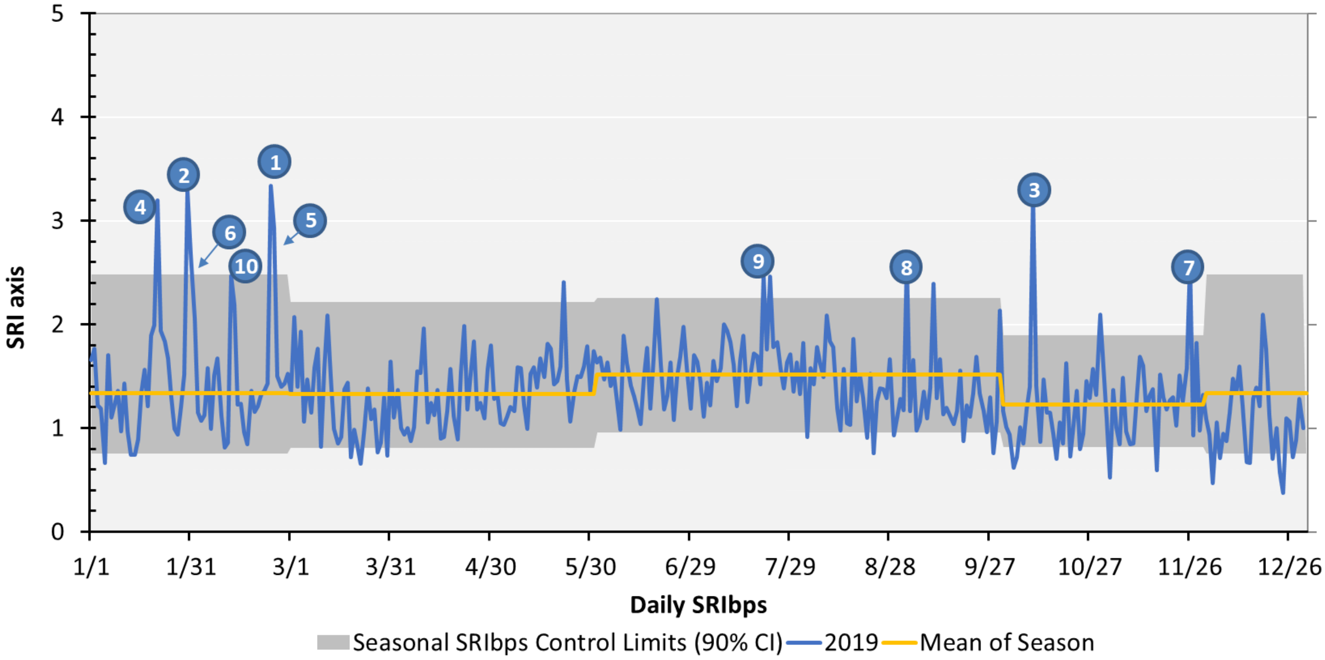


Figure 4.3: NERC 2019 Daily SRI with Top 10 Days Labeled, 90% Confidence Interval

Table 4.1 provides details on the generation, transmission, and load loss components for the top 10 SRI days during 2019. For each top SRI day, the table includes whether a specific event was a contributing factor, the type of event that occurred, and its general location by NERC RE. Of the top 10 SRI days in 2019, a total of 6 were contributed to cold weather events, only 1 was contributed to a fire event, and the remaining 3 were due to coincidental generator outages with no correlating factors.

Table 4.1: 2019 Top 10 SRI Days

Rank	Date	NERC SRI and Weighted Components 2019				Event Type (*Weather Influenced)	Regional Entity
		SRI	Weighted Generation	Weighted Transmission	Weighted Load Loss		
1	February 24	3.34	0.59	0.18	2.57	Wind Storm*	RF
2	January 30	3.29	2.83	0.33	0.13	Winter Storm Jayden*	RF, SERC, MRO
3	October 11	3.25	0.94	1.58	0.73	Saddleridge Fire	WECC
4	January 21	3.20	2.79	0.31	0.10	Winter Storm Indra*	RF, SERC, NPCC
5	February 25	2.93	1.30	0.46	1.17	Winter Storms Quiana and Ryan*	RF
6	January 31	2.68	2.53	0.13	0.03	Winter Storm Jayden*	RF, SERC, NPCC, MRO

[33] The 90% confidence interval (CI) of the historic values is between 5th percentile and 95th percentile.

Table 4.1: 2019 Top 10 SRI Days							
Rank	Date	NERC SRI and Weighted Components 2019				Event Type (*Weather Influenced)	Regional Entity
		SRI	Weighted Generation	Weighted Transmission	Weighted Load Loss		
7	November 27	2.60	1.16	0.50	0.94	Coincidental Generator Outages	SERC, WECC
8	September 3	2.60	2.01	0.41	0.18	Coincidental Generator Outages	SERC, WECC, RF
9	July 22	2.47	1.33	0.15	1.00	Coincidental Generator Outages	SERC, WECC, RF
10	February 12	2.47	1.08	0.68	0.71	Winter Storms Maya and Nadya*	RF, WECC

SRI Performance Trends

Historical performance trends can be gathered by comparing the top 2019 SRI days to those of prior years. Figure 4.4 shows the top 10 SRI days for each of the past five years in descending rank order. The moderate impacts measured during 2019's highest SRI days generally represented less stress to the BPS than were caused by the highest SRI days in the four prior years.

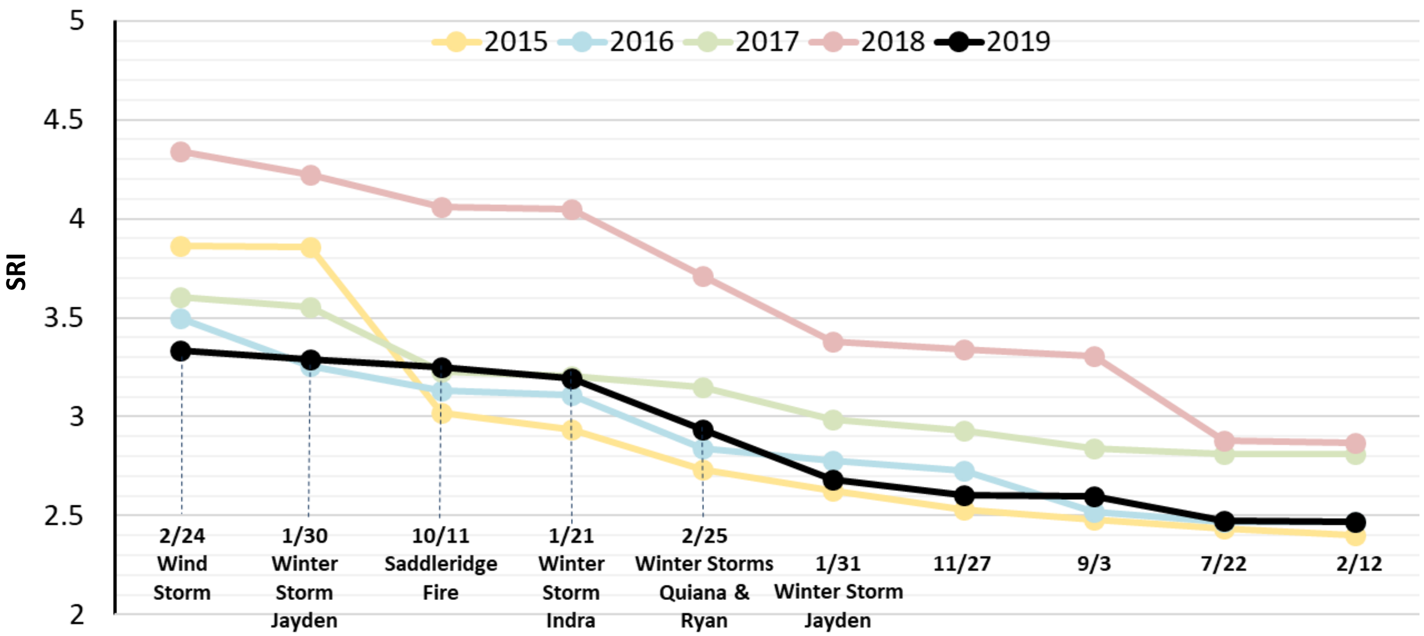


Figure 4.4: NERC Annual Daily Severity Risk Index Sorted Descending

When comparing the SRI of the top 10 SRI days of the past five years to the top 10 SRI days of 2019 in Figure 4.5, the highest SRI days of 2019 fall below the top 10 SRI days that occurred between 2015 and 2018. Details of the top 10 SRI days that occurred 2015–2018 are provided in Table 4.2.

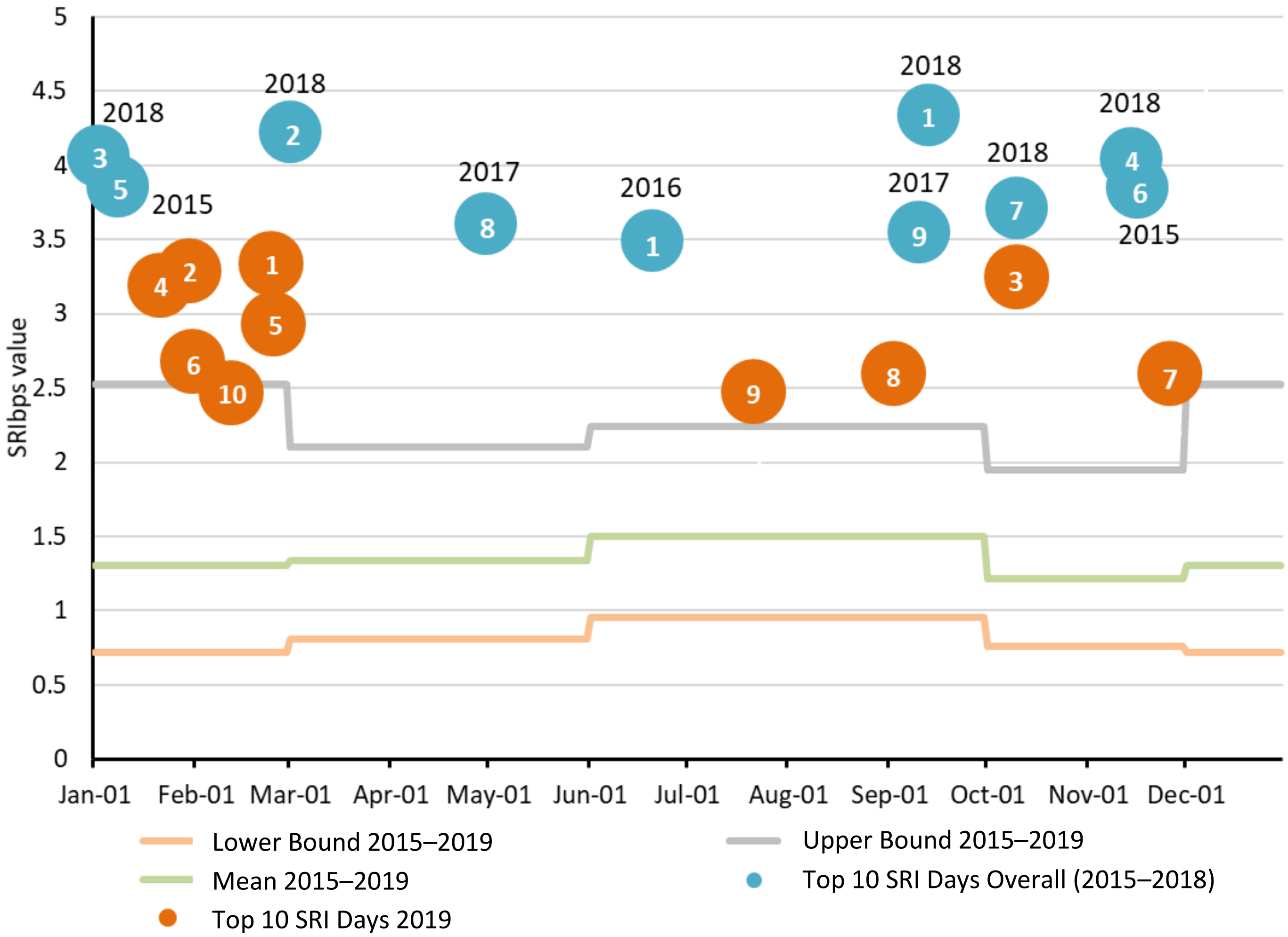


Figure 4.5: NERC 2015–2019 Daily SRI with Top 10 Days Labeled, 90% Confidence Interval

Table 4.2 identifies the top 10 SRI days occurring between 2015 to 2019 with the contribution of the generation, transmission, and load loss components to the SRI for each day as well as contributing event information and REs impacted by the event.

Table 4.2: Top 10 SRI Days 2015–2019

Rank	Date	NERC SRI and Weighted Components				Event Type (*Weather Influenced)	Regional Entities
		SRI	Weighted Generation	Weighted Transmission	Weighted Load Loss		
1	September 14, 2018	4.34	1.34	0.47	2.53	Hurricane Florence*	SERC
2	March 2, 2018	4.22	0.90	0.42	2.90	Winter Storm Riley*	NPCC
3	January 2, 2018	4.06	3.81	0.16	0.10	Winter Storm Grayson*	SERC, RF, MRO, NPCC, Texas RE
4	November 15, 2018	4.05	1.84	0.26	1.95	Winter Storm Avery*	RF, NPCC

Table 4.2: Top 10 SRI Days 2015–2019							
Rank	Date	NERC SRI and Weighted Components				Event Type (*Weather Influenced)	Regional Entities
		SRI	Weighted Generation	Weighted Transmission	Weighted Load Loss		
5	January 8, 2015	3.86	3.33	0.23	0.30	Winter Storm Juno*	SERC, NPCC
6	November 17, 2015	3.85	1.03	1.02	1.80	Weather Conditions across Northwest*	WECC
7	October 11, 2018	3.71	0.98	0.54	2.19	Hurricane Michael*	SERC
8	May 1, 2017	3.61	1.76	0.32	1.53	Coincidental Generator Outages	SERC, RF
9	September 11, 2017	3.55	1.61	1.74	0.20	Hurricane Irma*	SERC
10	June 20, 2016	3.49	1.86	0.29	1.35	Coincidental Generator Outages	WECC, RF, SERC, MRO

Chapter 5: Trends in Priority Reliability Issues

NERC routinely prioritizes emerging and known reliability issues. The Reliability Issues Steering Committee (RISC) is an advisory committee to the NERC Board that provides front-end, high-level leadership and accountability for these emerging and known issues of strategic importance to BPS reliability. The RISC provides a framework for prioritizing reliability issues and offers recommendations to help NERC and industry effectively focus their resources on the critical issues needed to best improve the reliability of the BPS. This section integrates data, information, and insights from across prior sections of this report and other NERC sources to shed light on the key reliability issues that the RISC identified. The discussion of each issue is followed by a summary of actions under way and recommendations to address the topic.

Emerging Risk Areas

In 2019, the RISC identified four high level risks: Grid Transformation, Extreme Natural Events, Security Risks, and Critical Infrastructure Interdependencies. This year's *State of Reliability* report focuses on the aspects of these risks, as listed below:

- **BPS Planning and Adapting to the Changing Resource Mix**
- **Impacts of Inverter-Based and Distributed Energy Resources on the BPS**
- **Increasing Complexity in Protection and Control Systems**
- **Human Performance and Skilled Workforce**
- **Loss of Situation Awareness**
- **Bulk Electric System Impact of Extreme Event Days**
- **Cyber and Physical Security**
- **Critical Infrastructure Interdependencies: Electric-Gas Working Group**

BPS Planning and Adapting to the Changing Resource Mix

Today's resource mix has continued to evolve with the retirement of traditional baseload generators, their replacement with natural gas generators, and the introduction of emerging technologies (e.g., inverter-based generation resources supported by federal, state, and provincial policies that favor renewable generation). Transmission Planners, BAs, asset owners, and system operators of the BPS require sufficient time to develop and deploy plans in response to reliability considerations that result from the new resource mix. Over time, regulatory initiatives, expected lower production costs, and aging generation infrastructure will likely alter the nature, investment needs, and dispatch of generation regarding the replacement of large rotating synchronous central-station generators with natural-gas-fired generation, renewable forms of asynchronous generation, demand response, storage, smart- and micro-grids, and other technologies. Planners and operators may be challenged to integrate these inputs and will need to make necessary changes, such as revising operational practices and procedures, enhancing NERC Reliability Standards, or changing market designs.

Changes in the Peak Resource Mix over the Past 10 years

Over the past 10 years, more than 100 GW of conventional generation[34] capacity has retired, and 246 GW, 91 GW, and 30 GW of new natural gas, wind, and solar generation capacity has been added to the BPS, respectively.[35] Variable generation from renewable wind and solar resources contribute to resource adequacy but often do not provide the same contribution to capacity at the peak demand hour (i.e., on-peak) as conventional generation resources. **Table 5.1** and **Figure 5.1** show the changing capacity composition of generating resources in North America over the past 10 years, including both installed and on-peak capacity in 2019. Installed capacity indicates what the resource is capable of producing at its maximum potential output. However, the on-peak capacity value may differ from installed capacity because it accounts for only that capacity contribution that the resource type provides at times of peak demand. As shown, the share of wind and solar resources has grown in terms of installed capacity additions over the past decade, but the growth has been less substantial at times of peak demand.

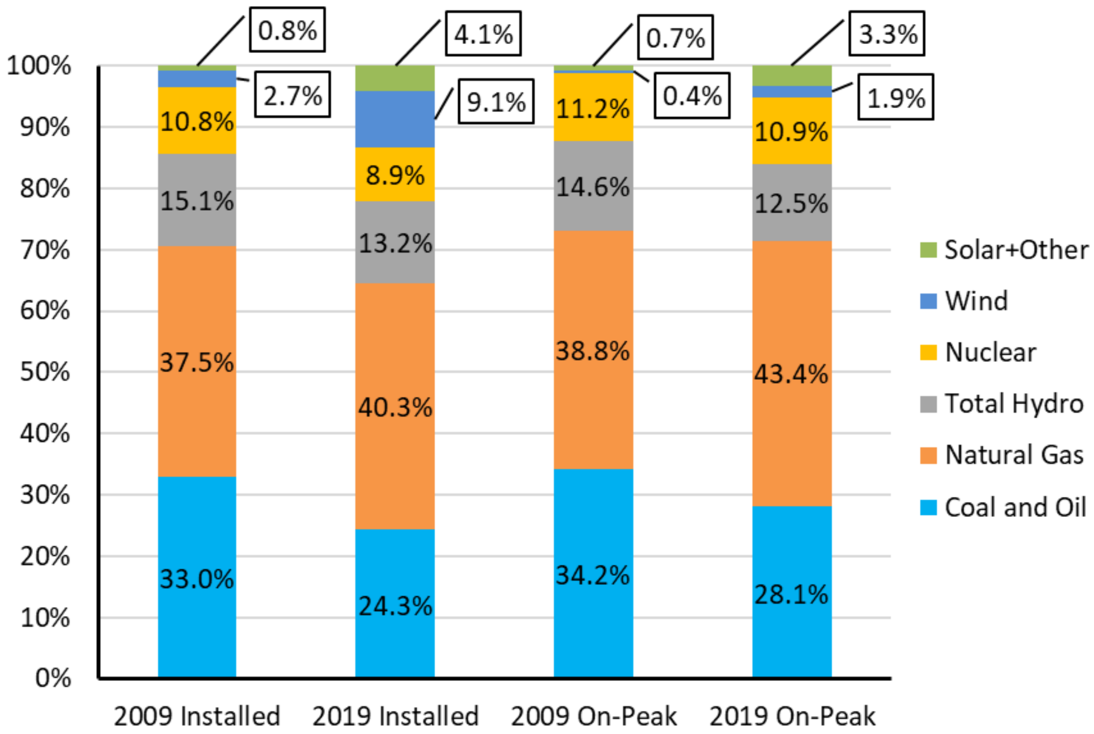


Figure 5.1: 2009 and 2019 NERC-Wide Capacity Resource Mix

[34] Conventional generation is generally understood to be baseload thermal (i.e., nuclear, coal, oil, hydro, and natural gas).

[35] Data obtained from Energy Information Administration (EIA) and NERC *Long-Term Reliability Assessments*.

Table 5.1: Generation Resource Capacity by Fuel Type								
Generation Fuel Type	2009 Installed		2019 Installed		2009 On-Peak		2019 On-Peak	
	GW	Percent	GW	Percent	GW	Percent	GW	Percent
Coal	307.8	29.5%	269.6	20.6%	307.8	30.7%	246.8	24.0%
Natural Gas	391.7	37.5%	526.8	40.3%	391.7	39.1%	445.8	43.4%
Hydro	158.0	15.1%	173.1	13.2%	147.7	14.7%	128.0	12.5%
Nuclear	113.1	10.8%	116.2	8.9%	113.1	11.3%	111.4	12.1%
Oil	37.0	3.5%	48.4	3.7%	37.0	3.7%	41.5	4.0%
Wind	27.9	2.7%	119.6	9.1%	4.4	0.4%	19.5	1.9%
Solar	0.5	0.1%	31.1	2.4%	0.0	0.0%	17.4	1.7%
Other	7.8	0.7%	22.9	1.8%	0.0	0.0%	16.0	1.6%
Total:	**1,043.7**	**100%**	**1,307.7**	**100%**	**1001.6**	**100.0%**	**1,026.4**	**100%**

The resource mix and speed at which is changing varies considerably across different parts of the North American power system. Figure 5.2 provides an Interconnection-level view of the generation resource mix since 2009. NERC's *Long-Term Reliability Assessment* reports on both the current generation resource mix and projections for the next 10 years for each of the 21 assessment areas that encompass the North American BPS.

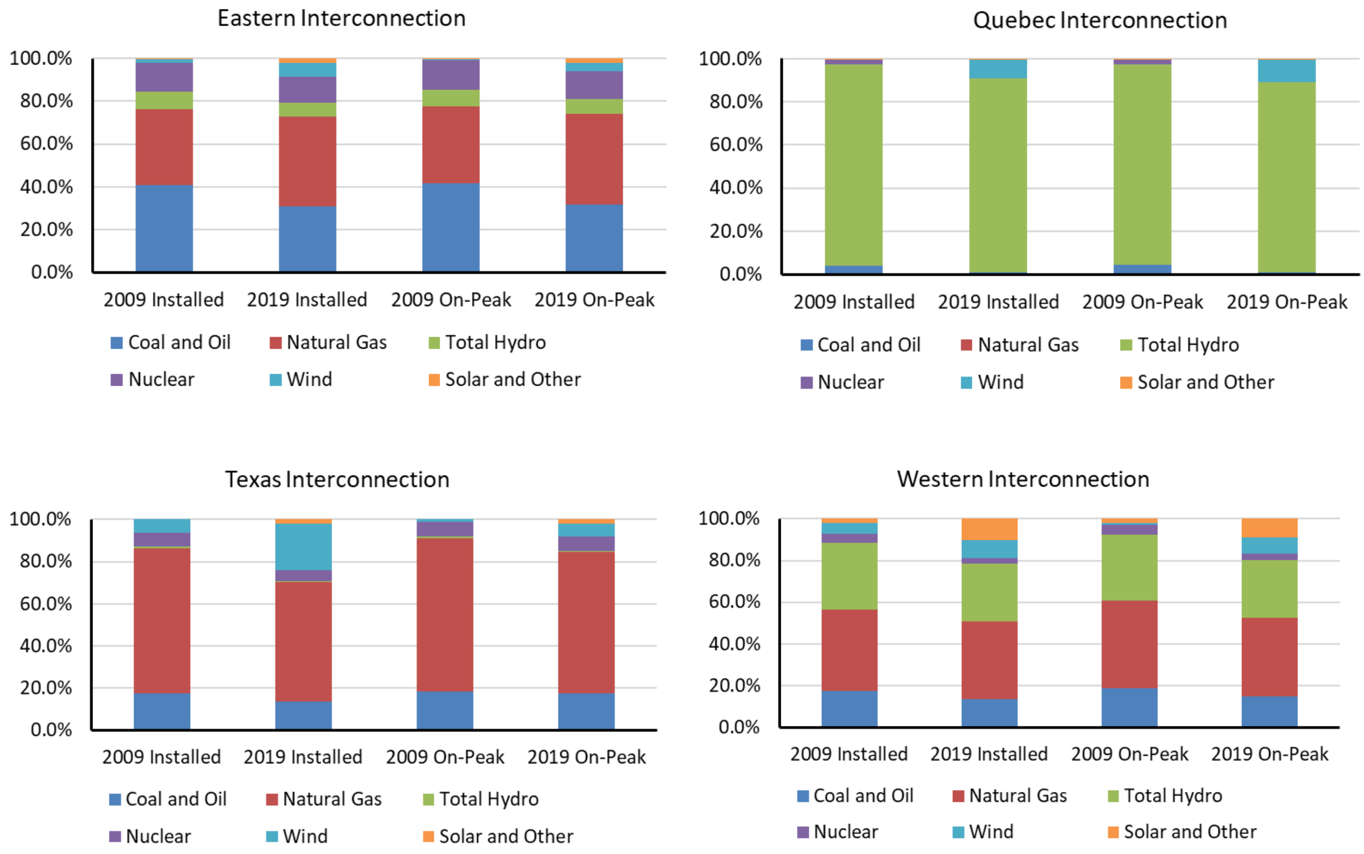


Figure 5.2: 2009 and 2019 Capacity Resource Mix By Interconnection

The ERO and its technical committees, along with industry stakeholders, continue to give priority to managing grid transformation to ensure reliability. Integrating new types of generating resources and harnessing the changing composition to serve load that is now also more dynamic than ever presents growing challenges for today's Transmission Planners and Operators.[36] The subsections that follow discuss these trends and industry's activities that occurred in 2019.

[36] See NERC *ERO Reliability Risk Priorities Report*, November 2019

Growth in Distributed Energy Resources

The generation resource mix is also changing through continued growth in solar PV installations on the distribution network. Increasing installations of distributed energy resources (DERs) modify how distribution and transmission systems interact with each other. Transmission Planners and Operators may not have complete visibility and control of these resources, but as growth becomes considerable, their contributions must be considered in system planning, forecasting, and modeling. In North America, there is approximately 21 GW of distributed solar generation capacity, and NERC projects the amount will more than double to over 45 GW by 2029.[37]

Maintaining Fuel Assurance

Growing reliance on natural gas for electricity generation is driving a variety of actions within the industry and across interdependent infrastructure sectors to manage risks to natural gas fuel supply. Most areas are reliant on natural gas to meet on-peak electricity demand. Unlike generation with on-site fuel storage, natural-gas-fired generators depend on the natural gas pipeline system to deliver just-in-time fuel for electricity production. Growth in the use of natural gas as a fuel for electricity generation and other applications can stress the natural gas supply infrastructure when necessary expansions do not keep pace.

Managing fuel-related risks to electricity generation is a complex but critically important task for reliability. Throughout 2019, electric industry experts collaborated with counterparts and stakeholders in the natural gas supply and delivery chains through the NERC Electric-Gas Working Group (EGWG) to develop guidelines for the electric industry's efforts in promoting fuel assurance. The new guidelines, published in early 2020, help electric system operators and planners enhance their planning approaches to address fuel assurance and fuel disruption risk to the reliable operation of the BPS.[38] The EGWG is engaging industry to support implementation of the guidelines and the development of metrics for evaluating effectiveness.

---

[37] Ref: 2019 LTRA, p. 28

[38] See the Reliability Guideline: *Fuel Assurance and Fuel-Related Reliability Risk Analysis for the Bulk Power System*: https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Fuel_Assurance_and_Fuel-Related_Reliability_Risk_Analysis_for_the_Bulk_Power_System.pdf

Impacts of Inverter-Based and Distributed Energy Resources on the BPS

The capacity of DERs is increasing across areas of the North American BPS. The increasing penetration of DERs may bring potential benefits for future BPS operations; however, with those benefits will come greater challenges for BPS planning and operations.

The NERC System Planning Impacts from Distributed Energy Resources Working Group (SPIDERWG) has been addressing planning-related challenges for a system with increasing penetrations of DERs. Specifically, the group has focused on four key aspects: aggregate DER modeling, model verification, reliability studies that incorporate DER performance, and coordinating DER activities with industry stakeholders. NERC SPIDERWG recently published a reliability guideline that highlights the potential reliability benefits that IEEE 1547-2018 can provide and BPS perspectives that should be considered during its adoption.[39] The guideline recommends that the authorities governing interconnection requirements, which are the state regulatory agencies in many cases, ensure proper coordination of industry stakeholders and consideration for future BPS reliability needs. NERC has been coordinating with the National Association of Regulatory Utility Commissioners on the development of this guideline and other activities such that increasing amounts of DERs can be reliably integrated. More information can be found on the SPIDERWG webpage.[40]

Challenges and Solutions with Integrating Large Amounts of Inverter-Based Resources

Asynchronous resources (those that are not physically synchronized with the BPS) use a power electronic interface (i.e., inverters) to connect to the ac power grid. The system was largely designed around synchronous generating resources, and technical challenges and innovative solutions have emerged as the penetrations of inverter-based resources has continued to increase across many areas of North America. Some inverter-based resource performance issues have been significant enough to result in grid disturbances that affect the reliability of the BPS, such as the tripping of a number of BPS-connected solar PV generation units that occurred during the 2016 Blue Cut fire and 2017 Canyon 2 fire disturbances in California. The ERO continues to focus resources on addressing potential reliability issues associated with the ever-increasing penetration of inverter-based resources.[41]

A major disturbance report was published in February 2018 following the Canyon 2 Fire disturbance,[42] and NERC issued a second solar loss NERC alert as a result of this analysis in May 2018.[43] NERC collected data from GOs of BES solar PV resources regarding their protection and controls response to grid disturbances and provided recommendations to improve performance to mitigate any potential reliability issues. The NERC IRPTF has published two NERC reliability guidelines related to the performance of BPS-connected inverter-based resources and recommended improvements to transmission service provider interconnection requirements to bring clarity and consistency to interconnection studies and requirements for inverter-based resources.[44, 45] NERC IRPTF is also in the process of publishing a technical report that highlights the modeling and studies activities the group has undertaken, documenting existing and future challenges that should be addressed by industry related to modeling and studies of inverter-based resources. For more information, see the IRPTF website.[46]

[39] https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Guideline_IEEE_1547-2018_BPS_Perspectives.pdf
[40] https://www.nerc.com/comm/PC/Pages/System-Planning-Impacts-from-Distributed-Energy-Resources-Subcommittee-(SPIDERWG).aspx
[41] In 2019, NERC published a summary of ERO activities to maintain reliability of the BPS through the growth of inverter-based resources in the resource mix. A discussion of significant grid disturbances, NERC alerts, and mitigating activities is included in the summary located here: https://www.nerc.com/comm/PC/Documents/Summary_of_Activities_BPS-Connected_IBR_and_DER.pdf
[42] https://www.nerc.com/pa/rrm/ea/1200_MW_Fault_Induced_Solar_Photovoltaic_Resource_/1200_MW_Fault_Induced_Solar_Photovoltaic_Resource_Interruption_Final.pdf
[43] https://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/NERC_Alert_Loss_of_Solar_Resources_during_Transmission_Disturbance-II_2018.pdf
[44] https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Inverter-Based_Resource_Performance_Guideline.pdf
[45] https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Reliability_Guideline_IBR_Interconnection_Requirements_Improvements.pdf
[46] https://www.nerc.com/comm/PC/Pages/Inverter-Based-Resource-Performance-Task-Force.aspx

Ensuring Sufficient Flexible Resources

With increasing levels of variable renewable generation in the resource mix, there is a growing need to have resources available that can be reliably called upon on short notice to balance electricity supply and demand if shortfall conditions occur. Flexible resources that can include responsive generators with assured fuel or energy and demand response are necessary in some areas today to ensure resource adequacy and meet ramping needs. ERCOT and California rely on the output from wind and solar generation to meet projected peak demand as shown in **Figure 5.3**. Should solar and wind output fall below expectations during peak conditions, these areas may need to draw on unanticipated resources or additional imports from outside of the area to maintain balance between load and generation.[47] Additionally, the high levels of solar PV resources in these areas cause the daily load shape to change such that greater amounts of flexible resources are needed to match steep ramping conditions during times when the change in wind or solar output changes rapidly. See the **text box** on the next page for more information.

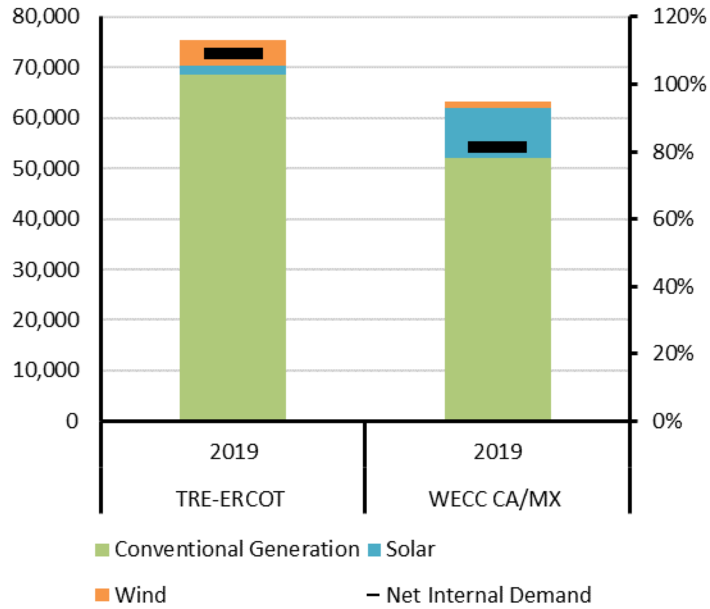


Figure 5.3: Wind and Solar Contribution to Resource Mix and Meeting Net Internal Demand in Texas RE-ERCOT and WECC CA/MX Assessment Areas

The **2019 Saddleridge Fire** demonstrated the value of local, flexible generation to reliability during an extreme event. However, as increasing amounts of thermal generators retire, some areas may be losing local flexible resources. Some generation retirements may limit flexible resource options for operators when extreme events impact the transmission system and local conventional or variable generation is unavailable.

NERC assesses the resource adequacy of the BPS and analyzes emerging issues, such as flexible resource needs, in its seasonal and long-term reliability assessments and is obligated to report on reliability periodically. Various planning and operating entities as well as regional, state, provincial, and local regulatory organizations are responsible for resource planning and procurement. In addition to the annual and seasonal assessments, NERC conducts biennial probabilistic assessments of resource adequacy that can provide insights into system needs as variable generation resources increase. NERC is in the process of conducting its next probabilistic assessment.

[47] See *2019 LTRA* for additional information, including future trends based on 10-year projections, p. 25–27

Flexible Resources for Ramping

In areas with significant amounts of solar PV resources, balancing electricity supply and demand can be especially challenging when the sun is setting and load is increasing. As the sun recedes, the collective contributions of solar PV resources rapidly diminish leading to a steep ramp-up from dispatchable resources to meet electricity demand. **Figure 5.4** is an illustration of ramping needs for a simulated system under three levels of solar resource capacity (not an actual system).

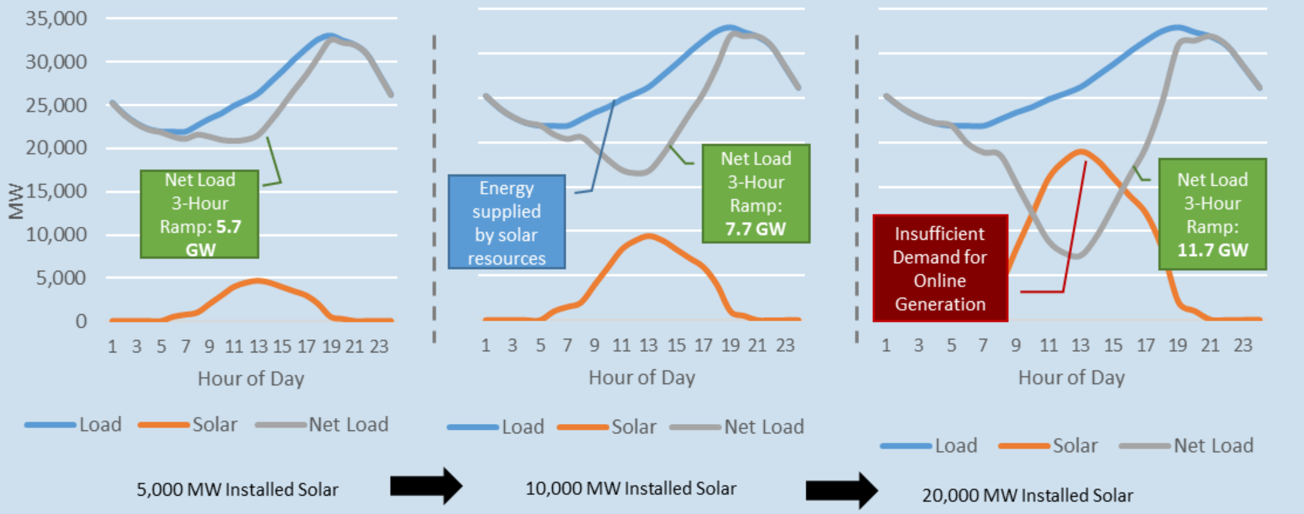


Figure 5.4: Illustration of Changing Ramping Needs as Solar Resources Increase

Areas can address concerns with ramping by ensuring there are sufficient flexible resources available to meet anticipated conditions. In California, the Independent System Operator (CAISO) annually assesses the flexible capacity needs to meet reliability criteria so that sufficient resources can be procured.

Figure 5.5 shows the actual three-hour ramp requirements by month for the CAISO area since 2016. The need for increasing amounts of flexible ramping resources is consistent with historical year-on-year trends.[48]

In areas where increases in intermittent resources is still anticipated, the availability of flexible resources should be considered to keep pace with the ramping needs and the need to serve load when the variable generation is not available.

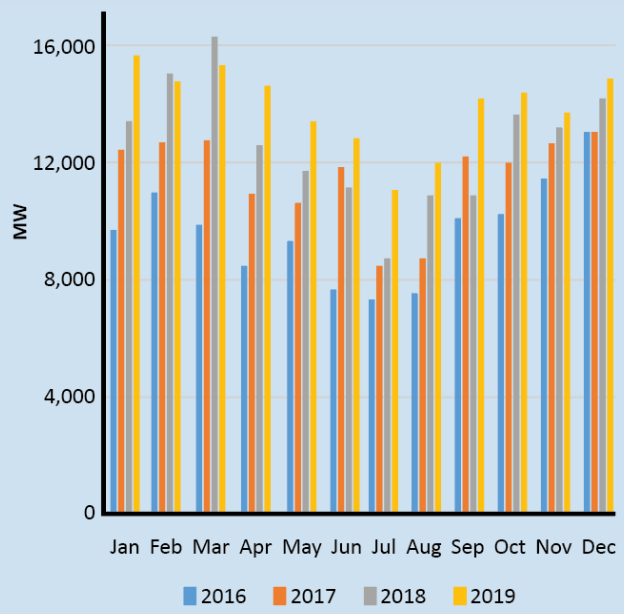


Figure 5.5: Maximum Three-Hour Ramps in CAISO 2016–2019

[48] See CAISO flexible capacity needs assessment process: **Figure 5.5** is based on historical three-hour ramp data reported in the draft *Flexible Capacity Needs Assessment for 2021,* April 2020: http://www.caiso.com/informed/Pages/StakeholderProcesses/FlexibleCapacityNeedsAssessmentProcess.aspx

Actions in Progress

- Assess resource adequacy, operating reliability, and emerging reliability issues through NERC's long-term, seasonal, and probabilistic reliability assessments
- Conduct technical analysis and develop guidelines and recommendations as specified in the work plans for the IRPTF, SPIDERWG, and the Resources Subcommittee
- Develop requirements to collect GADS data for solar, wind, and energy storage installations
- Adopt and implement guidelines for assessing fuel assurance and fuel-related reliability risk by registered entities

Recommendations

The ERO, its technical committees, and industry stakeholders should continue to address reliability risks associated with grid transformation and the changing resource mix as detailed in the *2019 RISC Report* and the *2019 Long-Term Reliability Assessment*. Key recommendations are summarized as follows:[49]

- The ERO Enterprise and industry should work with manufacturers, vendors, and standards groups to continue mitigation efforts regarding momentary cessation as identified in the 2018 NERC alert.
- The ERO Enterprise should enhance the reliability assessment process by incorporating energy adequacy metrics and evaluating scenarios posing the greatest risk in NERC reliability assessments. This includes expanding the use of probabilistic approaches to assess resource adequacy with energy-limited or uncertain resources.
- The ERO Enterprise should develop updated data and modeling capabilities and requirements to ensure valid and accurate results given resource and grid transformation (ongoing effort). Efforts initiated by the SPIDERWG to support collection of aggregated DER data for planning studies and the development of guidance for reliability studies that account for increasing amounts of DERs should be continued.
- Industry should identify, design, and commit flexible resources needed to meet increasing ramping and variability requirements through improved recognition of the capabilities of these types of resources. Presently, concerns associated with ramping are confined to certain parts of North America; however, as variable generation increases, system planners will need to ensure that sufficient flexible resources are available. The ERO Enterprise should continue to evaluate flexible resource needs in future long-term reliability assessments.

[49] Additional details on recommendations and action plans for addressing risks associated with changing resource mix, BPS planning, and resource adequacy and performance are included in the *2019 RISC Report* and the *2019 Long-Term Reliability Assessment*.

Increasing Complexity in Protection and Control Systems

Failure to properly design, coordinate, commission, operate, maintain, prudently replace, and upgrade BPS control system assets causes misoperation of protection and control systems. Misoperations can initiate more frequent and/or more wide-spread outages. Resource mix changes involving growth in inverter-based generation sources can also impact wide-area protection and increase the need to coordinate protection with the distribution system.

Leading Causes of Misoperations

The top three causes of misoperations over the past five years are Incorrect Settings/Logic/Design Errors, Relay Failures/Malfunctions, and Communication Failures (See **Figure 5.6**). For each five-year period analyzed since data collection started, these three causes have consistently accounted for more than 60% of all misoperations.

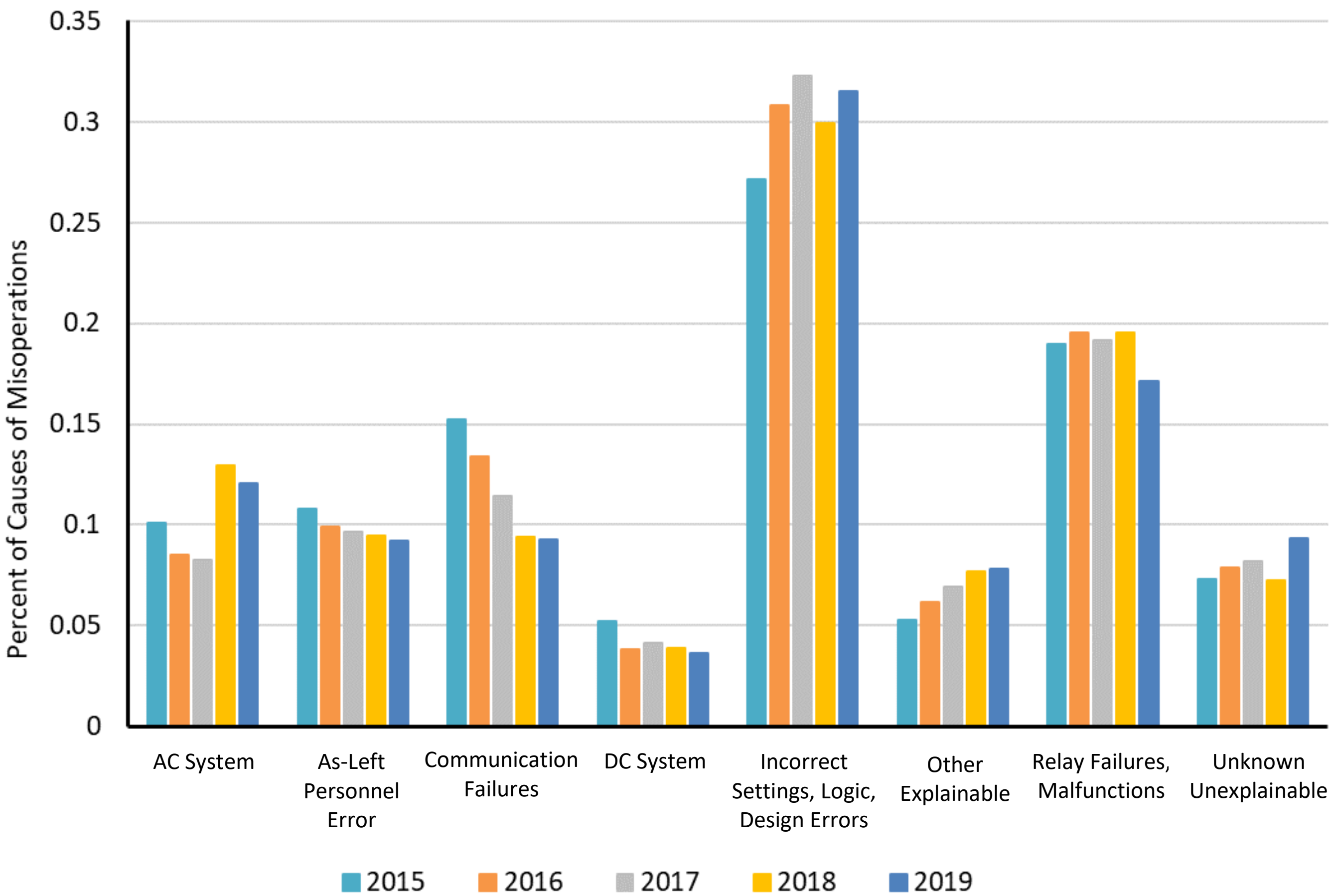


Figure 5.6: Misoperations by Cause Code (2015–2019)

Protection System Failures Leading to Transmission Outages

AC circuits saw a statistically significant decrease in the number of outages per circuit. While there was a slight decrease in the number of outages per transformer, it was not statistically significant (see **Figure 3.7** and **Figure 3.9**).

Event-Related Misoperations

An analysis of misoperations data and events reported through NERC's EAP found that, in 2015, there were 50 transmission-related system disturbances that resulted in a qualified event.[50] Of those 50 events, a total of 34 events (68%) had associated misoperations. Since 2015, the ERO and stakeholders formed various task forces, conducted more granular root cause analysis, and held workshops dedicated to reducing protection system misoperations. In

[50] For a list of definitions of qualified events, see the Categories and Subcategories for Qualifying Events text box.

2019, there were 74 transmission-related qualified events. Of those 74 events, 36 events, or 49% of them, involved misoperations (see **Figure 5.7**). The efforts taken by the ERO and implemented by the industry appear to have successfully reduced the number of events with misoperations.

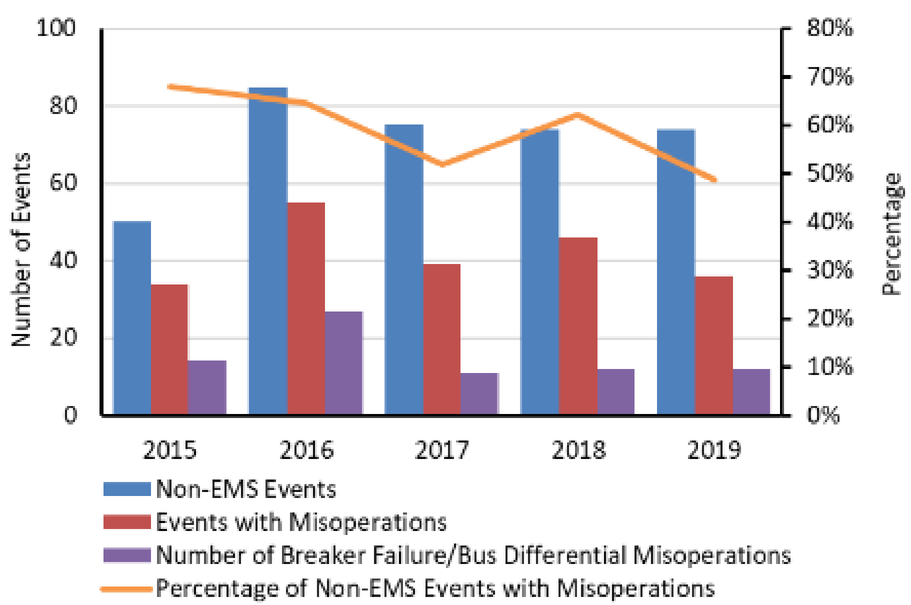


Figure 5.7: Events with Misoperations

Actions in Progress

- NERC, REs, and stakeholders continue to conduct industry webinars on protection systems and document success stories on how GOs and TOs are achieving high levels of protection system performance.
- The MIDASWG will collect and analyze protection system misoperations data and information through MIDAS and provide training to ensure consistency of operations and misoperations reporting.
- NERC will report the quarterly protection system misoperations data on NERC's website.

Recommendations

- The ERO should work with industry experts to promote the development of industry guidelines on protection and control system management to improve performance.
- As more inverter-based generation is added to the BPS, the ERO should work with stakeholders to determine if there is an increasing reliability risk due to the different short-circuit contribution characteristics of inverter-based resources.

Human Performance and Skilled Workforce

The evolving BPS is becoming more complex, requiring industry to hire and maintain a workforce with the appropriate skillsets. The addition of significant internal procedural controls needed to maintain compliance with NERC Reliability Standards requirements has brought additional complexity to many skilled worker positions. The effective use of human performance (HP) will help trap, catch, reduce, and mitigate the active and latent errors that negatively affect reliability. Weaknesses in HP hamper an organization's ability to identify and address precursor conditions that degrade effective mitigation and behavior management.

Transmission Outages Related to Human Performance

NERC TADS collects transmission outage data with a variety of causes, including human error. The definition of human error as a cause of transmission outage is defined in the TADS Data Reporting Instructions (DRI).[51]

The calculated annual outage frequencies per ac circuit and per transformer were tested to identify statistically significant year-to-year changes of the reliability metric. For ac circuits, automatic outages caused by human error have seen a statistically significant decrease in frequency. For both ac circuits and transformers, operational outages caused by human error have seen a statistically significant increase in frequency. The overall frequency of forced outages due to human error, which represents automatic and operational outages combined, has seen no statistically significant change for either ac circuits or transformers (see **Figure 5.8**). For operational outages, that is those that are non-automatic and required for the purpose of avoiding an emergency or to maintain the system within operational limits, the outages related to human error appear to be consistently increasing. Although they are a small portion of the overall outages, this is a concerning trend.

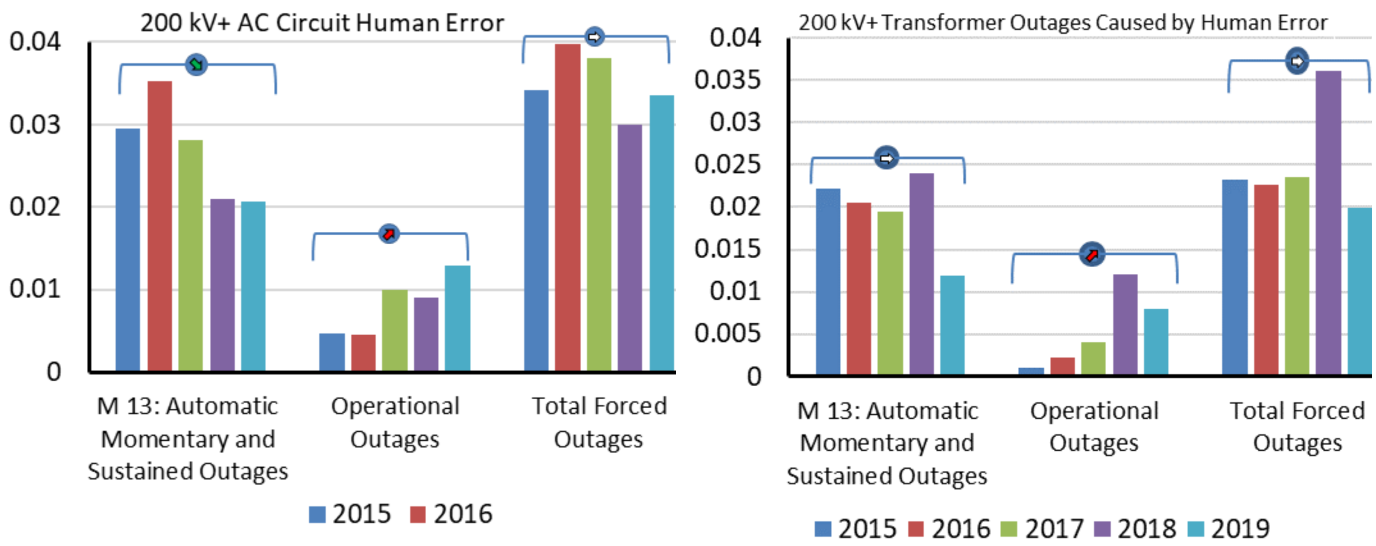


Figure 5.8: AC Circuit and Transformer Outages Initiated by Human Error

Human Performance and Generation Outages

NERC GADS collects generation outage data associated with a variety of causes, including human error. **Figure 5.9** shows the annual forced generation outages on a per-unit basis caused by human error. The causes reported have been grouped into three categories: general human error, procedural human error, and staff shortage. Of the fuel types, only nuclear generation shows a notable increase in human-error-caused events in 2019; the sub causes of staff shortage and procedure human error were present for nuclear generators in 2018 and 2019. Over the past five years, forced outages attributed to human error have averaged 1% of all forced generator outage events.

[51] **Human Error:** Relative human factor performance including any incorrect action traceable to employees and/or contractors to companies operating, maintaining, and/or assisting the TO.

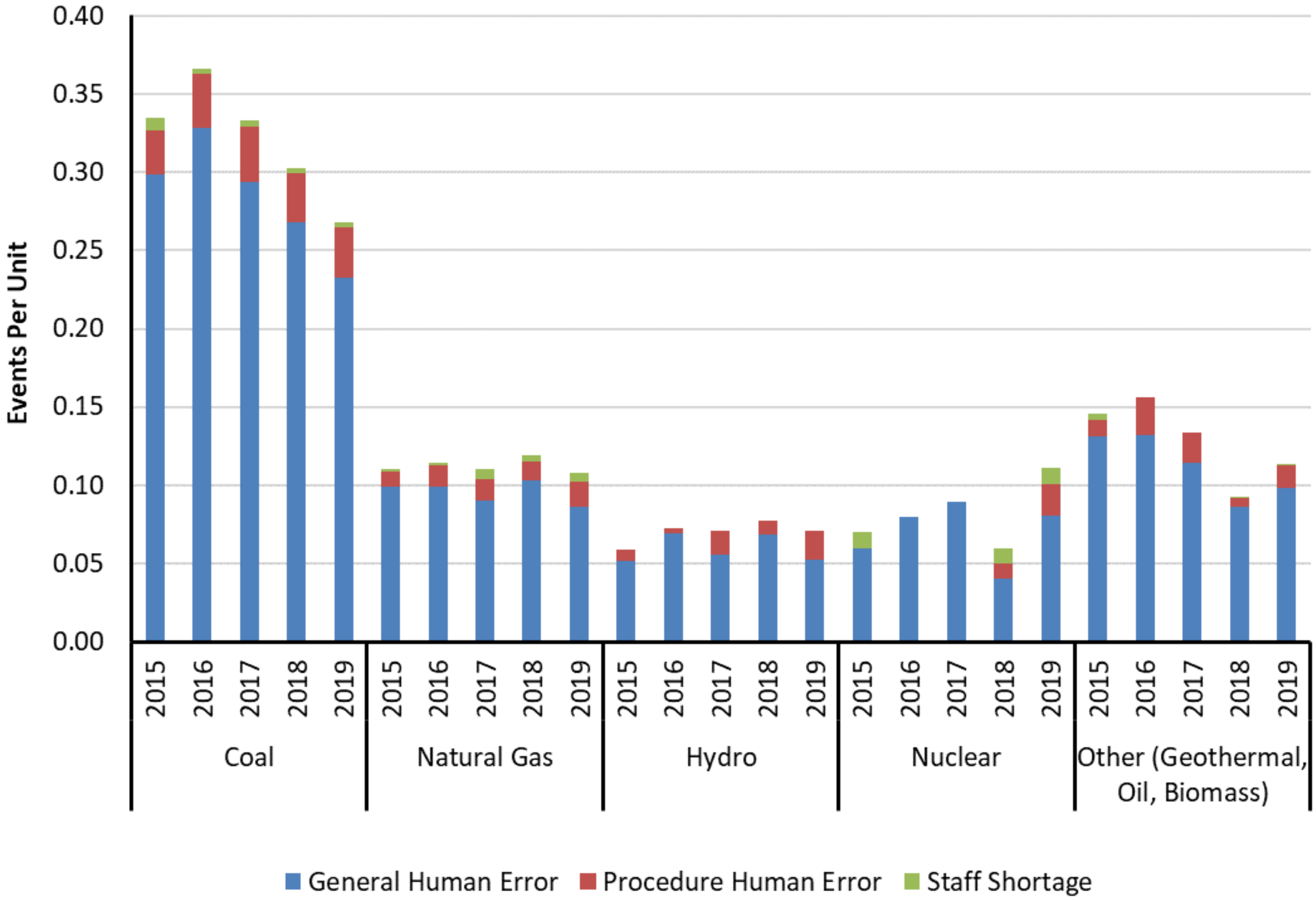


Figure 5.9: Generation Forced Outage Events per Unit Caused by Human Error

Trends of Events Involving Human Error as a Root Cause

In the ERO Event Analysis trending process, the management or organization and individual human error cause sets are overarching descriptions for human error. Of all processed events in 2019, these occurred a total of 34 times as a root cause (see **Figure 5.10**). This is down from 35 in 2018 and a high of 49 in 2017. However, analysis of the processed events year-over-year resulting in human error as a root cause is currently moving in an upward direction for the 2015–2019 time period (see **Figure 5.10**). The top five detailed root cause codes for the same period are members of the management or organization set and are listed below:

- Job scoping did not identify special circumstances and/or conditions
- System interactions not considered or identified
- Inadequate work package preparation
- Risks/consequences associated with change not adequately reviewed/assessed
- Management policy guidance or expectations are not well-defined, understood, or enforced

Event processing during 2019 saw a shift in the top five root causes with the emergence of "management policy…" as listed above (see the **text box** on the next page for more information). The top five detailed root causes, coupled with the apparent underlying trend shown in **Figure 5.10**, suggests a need for industry to focus on improving on the management and organization areas within their companies in an effort to modify the trend toward a flatter or downward sloping curve.

Management and organizational challenges comprise a range of possible contributing and root causes in the ERO trending process. It is comprised of the following sub-categories where methods, actions, and/or practices are less than adequate:

- Management methods
- Resource management
- Work organization and planning
- Supervisory methods
- Change management

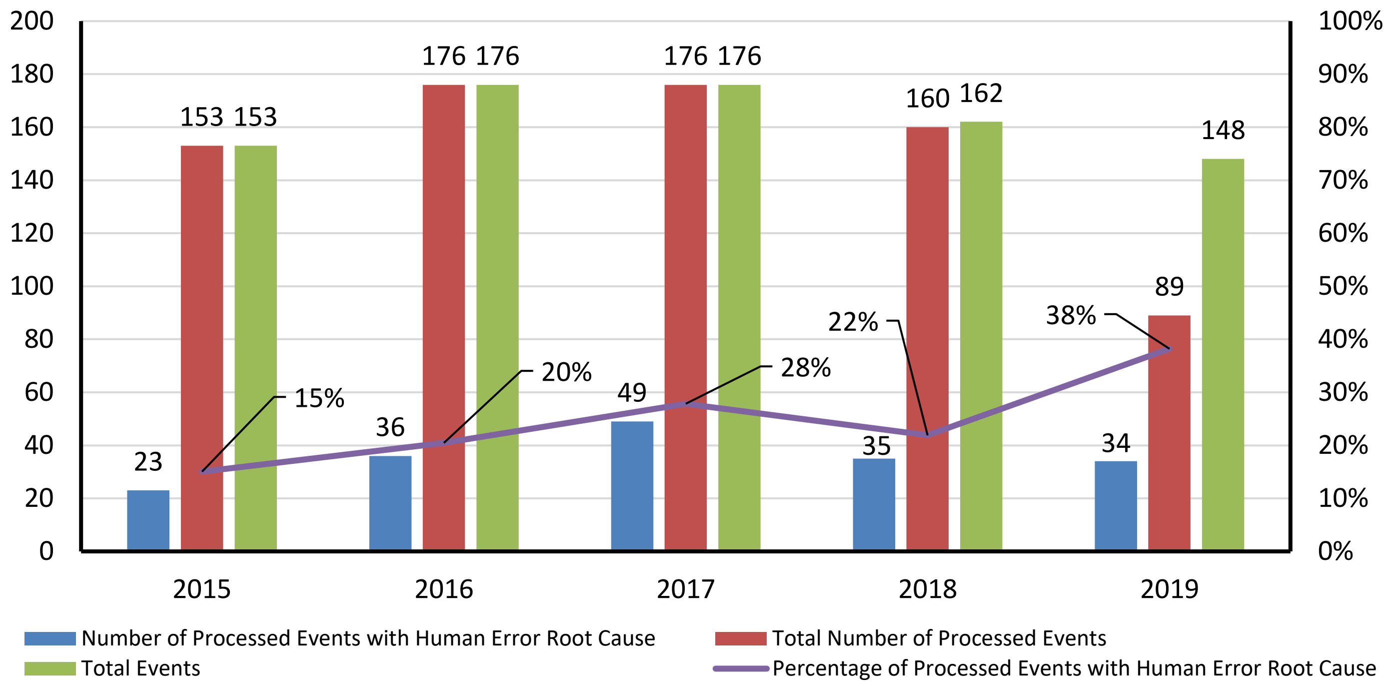


Figure 5.10: Human Error Root Cause by Year, 2015–2019

Human Error and Protection System Misoperations

Protection system misoperations remain an important indicator of the reliability of the BPS. Human error is one of the potential causes for misoperations to occur. Figure 5.11 shows the number of misoperations due to human error by RE for the past five years. There are two different causes of human error misoperations reported in MIDAS: As-left Personnel Errors and Incorrect Settings/Logic/Design Errors. Together, these account for roughly 40% of misoperations over the last five years, described in more detail as follows:

- **As-left Personnel Errors:** These are misoperations that are due to the as-left condition of the composite protection system following maintenance or construction procedures. These include test switches left open, wiring errors not associated with incorrect drawings, carrier grounds left in place, settings places in the wrong relay, or settings left in the relay that do not match engineering intended and approved settings. This includes personnel activation of an incorrect settings group.
- **Incorrect Settings/Logic/Design Errors:** These are misoperations due to errors in the following:
  - **Incorrect Settings:** This includes errors in issued settings, including those associated with electromechanical or solid-state relays and the protection element settings in microprocessor-based relays, excluding logic errors discussed in the Logic Error cause code. This includes setting errors caused by inaccurate modeling.

- **Logic:** This includes errors in issued logic settings and errors associated with programming microprocessor relay inputs, outputs, custom user logic, or protection function mapping to communication or physical output points.
- **Design:** This involves incorrect physical design. Examples include incorrect configuration on ac or dc schematic or wiring drawings or incorrectly applied protective equipment.

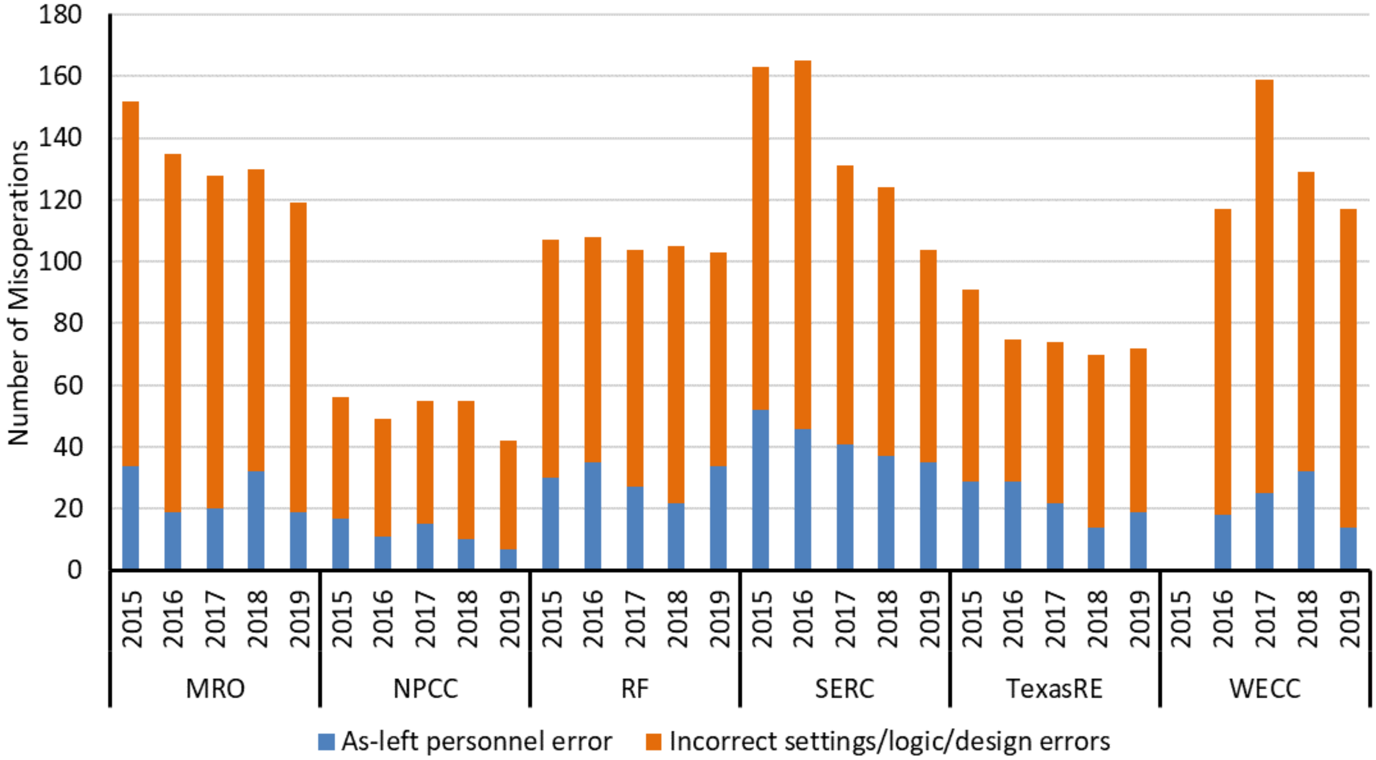


Figure 5.11: Protection System Misoperations Due to Human Error by Regional Entity, 2015–2019[52]

In **Figure 5.11**, it is notable that Incorrect Settings/Logic/Design Errors greatly outweigh As-left personnel error for overall number of misoperations that occur. While the number of misoperations varies among REs, the five-year trends generally show a stable or downward trend in misoperations with causes attributed to human error.

Actions and Mitigations in Progress

- The ERO has identified work force capability and human error as possible threats to the reliability of the BPS. These broad topics are generally categorized for analysis by the ERO under management, organization, and individual contributions. The reported occurrences in **Figure 5.11** illustrate two areas of focus that will help improve the misoperations rate on the BPS. The data suggests a need for focus on both individual actions and organizational processes/procedures pertaining to protective systems.
- The ERO Enterprise provides educational opportunities annually to assist industry in understanding and focusing on reducing human error through human performance concepts, methods, techniques, and procedures. NERC, the North American Transmission Forum (NATF) and the DOE sponsored their eighth annual HP conference in Atlanta, Georgia, Improving Human Performance on the Grid, in March 2019.

[52] MIDAS data collection for WECC began in Q2 2016.

- The RE have been working with local industry working groups to review and aid in addressing reported misoperations and other human performance issues.
- The ERO/NATF-led human performance awareness and education event is scheduled annually.
- The ERO Event Analysis program continues.
- The NERC cause analysis course is offered periodically.
- RE-specific human-performance-related activities continue to occur.

Recommendations

- Industry must focus on human and organizational performance improvement. The ERO Enterprise, the NATF, and the North American Generation Forum (NAGF) need to continue assisting industry through training and education events and workshops that increase knowledge and provide information to help industry modify and strengthen procedural and organizational structures to more effectively mitigate risk scenarios related to transmission and generation outages.

Loss of Situation Awareness

Situation awareness is necessary to maintain reliability, anticipate events, and respond appropriately when or before events occur. Without the appropriate tools and data, system operators may have degraded situation awareness that impacts their ability to make decisions that ensure reliability for the given state of the BES. Certain essential capabilities must be in place with up-to-date information for staff to make informed decisions. An essential component of monitoring and situation awareness is the availability of information when needed. Unexpected outages of systems needed for communications, monitoring and control of equipment, or planned outages without appropriate coordination or oversight can leave system operators with impaired visibility. Additionally, insufficient communication and data regarding neighboring entity's operations is a risk as operators may act on incomplete information. For system operators, EMSs are an essential component of situation awareness and are addressed in the following subsections.

Impacts from the Loss of EMS

An EMS is a computer-aided environment used by system operators to monitor and control BPS elements. The EMS provides situational awareness and allows system operators to monitor and control the frequency; the status (open or closed) of switching devices plus real and reactive power flows on the BES tie-lines and transmission facilities within the control area; and the status of applicable EMS applications, such as State Estimator (SE), Real-Time Contingency Analysis (RTCA), and/or Alarm Management.

The number of Category 1h events (loss of monitoring or control) has been stable for the last five years (see **Figure 5.12**). Based on the 441 events reported by 135 registered entities from 2015 to 2019, the average outage time (see **Figure 5.13**) was 69 minutes, and the actual EMS availability was 99.99%. Furthermore, there were no reported EMS-related events that have caused loss of load.

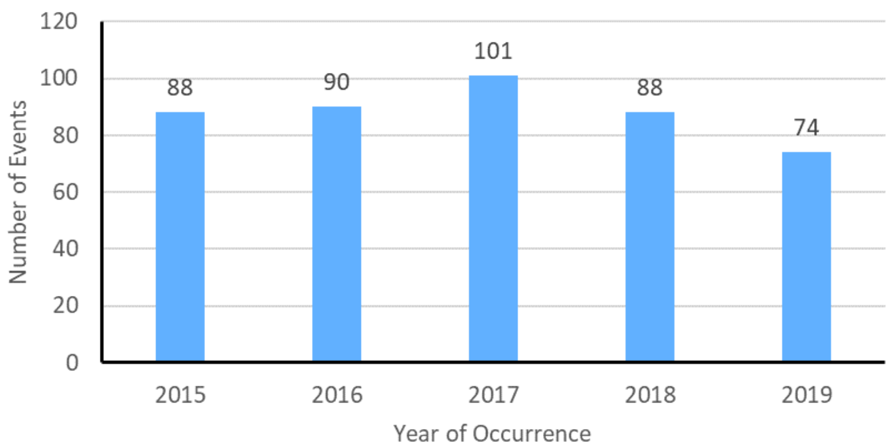


Figure 5.12: Number of EMS-Related Events (Q1 2015 through Q4 2019)

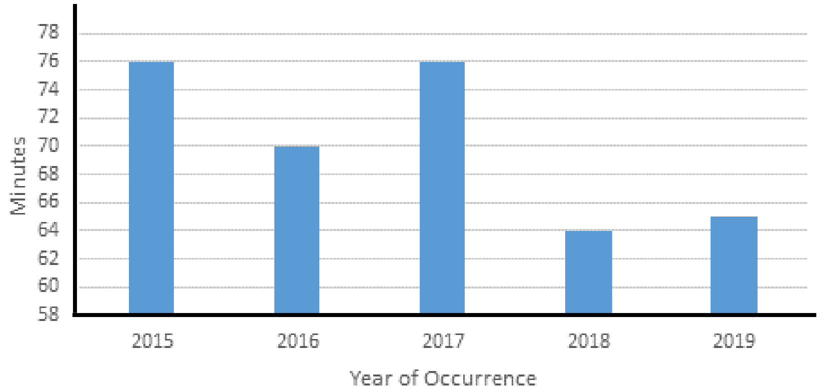


Figure 5.13: Average Outage Time (Q1 2015 through Q4 2019)

Failure Types Associated with Loss of EMS

Reliability risk varies (see **Figure 5.14**) depending on the function that is lost plus the duration of that outage, listed as follows:

- **Loss of SE/RTCA:** The dominant EMS failure mode, disrupts the real-time assessment and predictive analysis that the EMS provides
- **Loss of Ability to Monitor or Control**: Operator loss of status of devices/switching
- **Loss of ICCP:** Disrupts the information shared between operators
- **Loss of RTU:** Loss of communications from SCADA
- **Loss of Automatic Generation Control (AGC):** Loss of the ability to remotely monitor and control generating units

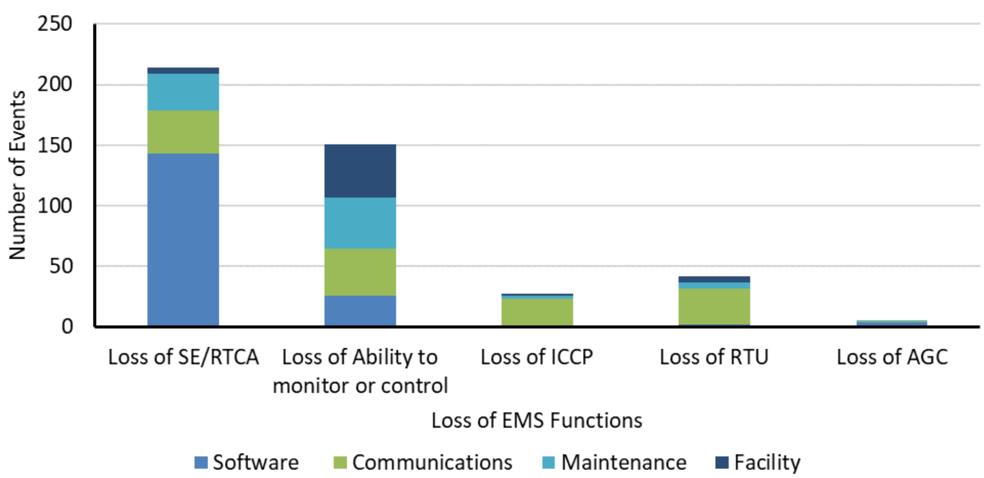


Figure 5.14: Number of EMS Events per Loss of EMS Functions (Q1 2015–Q4 2019)

Largest Contributor to Loss of EMS

Figure 5.15 shows that over the evaluation period from 2015–2019, outages associated with software and communications challenges contribute to the leading causes of EMS outages. Reported EMS events can be grouped by the following attributes:

- **Software**: Software defects, modeling issues, database corruption, memory issues, etc.
- **Communications**: Devices issues, less than adequate system interactions, etc.
- **Facility:** Loss of power to the control center or data center, fire alarm, ac failure, etc.
- **Maintenance:** System upgrades, job-scoping, change-management, software configuration, or settings failure, etc.

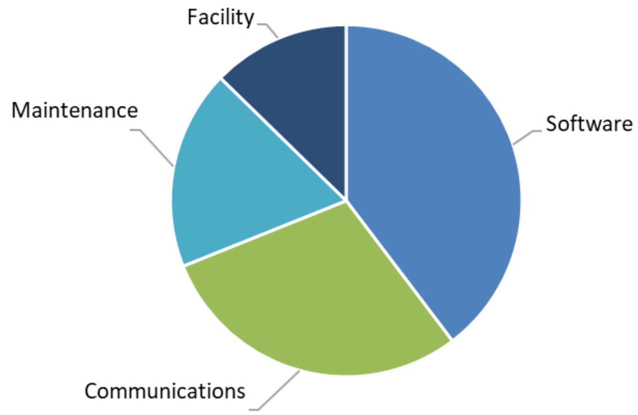


Figure 5.15: Contributors to Loss of EMS functions (Q1 2015–Q4 2019)

Loss of SE/RTCA

Over the evaluation period from 2015–2019, the loss of SE/RTCA is the most prevalent EMS failure. Figure 5.16 shows how EMS software, communications, maintenance, and facilities contributed to loss of SE/RTCA events each year (2015–2019). EMS software is the major contributor to the loss of SE/RTCA in all years studied.

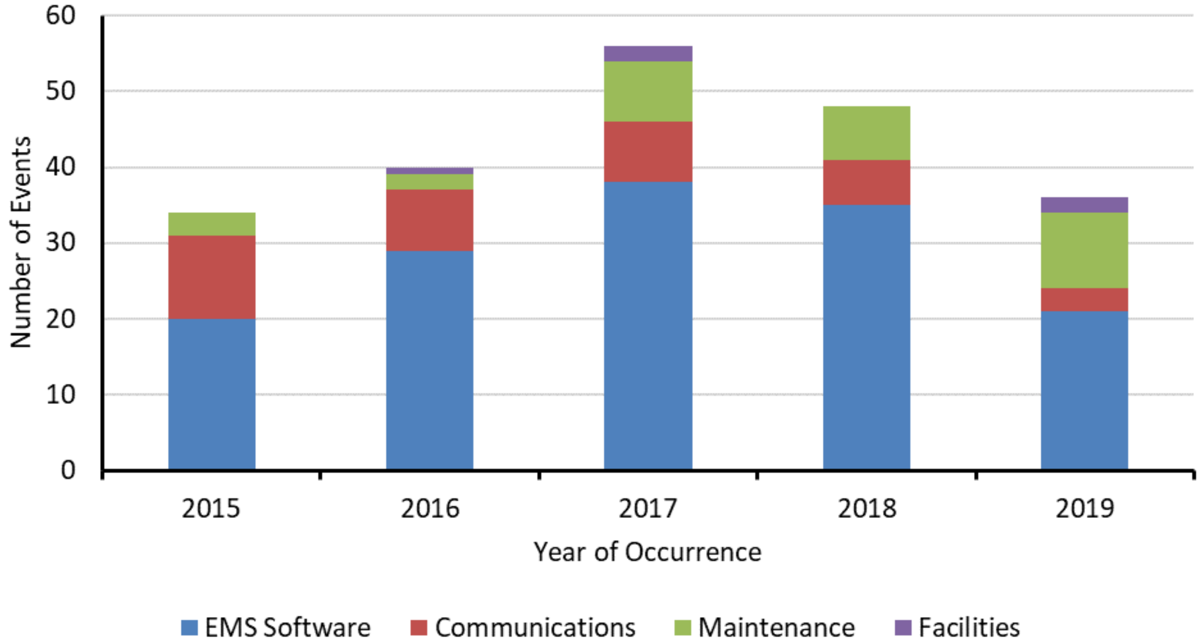


Figure 5.16: Contributors to Loss of SE/RTCA by Year

The following are lessons learned or best practices that should be considered to manage the risks caused by software for loss of SE/RTCA:

- Work with the vendor, consider developing an inventory of key EMS settings that need to be tuned or calibrated
- Develop dedicated in-house expertise with real-time tools. More skilled in-house personnel who can troubleshoot and correct these issues can lead to shorter SE/RTCA outage durations; this may include additional knowledge transfer from the vendor to the in-house personnel
- Conduct periodic reviews of SE/RTCA settings and parameters to ensure that the SE/RTCA continues to converge and produce a quality solution. The frequency of these reviews will vary, but consider reviewing the settings and parameters following model changes, generation retirements, software upgrades, and any other significant changes made to the EMS system or the model
- Share models between the RC and its TOPs using standardized formats, such as the common information model
- Consider standardizing on model names for facilities. Due to different EMS vendors and platforms, different data points may be called different cryptic names (often truncated due to space limitations). Standardization of these model names could help reduce confusion and lead to fewer SE/RTCA outages

Assessment

In terms of EMS, software and communications failure are major contributors to the loss of EMS. While failure of a decision-support tool has not directly led to the loss of generation, transmission lines, or customer load, EMS failures may hinder the decision-making capabilities of the system operators during normal operations or more importantly during a disturbance. NERC has analyzed data and identified that short-term outages of tools and monitoring systems are not uncommon, and the industry is committed to reducing the frequency and duration of these types of events.

Actions and Mitigations in Progress

- The Energy Management System Working Group (EMSWG) analyzes the events and data that are being collected on EMS outages and challenges. From Event Analysis reports, NERC published multiple lessons learned specifically about EMS outages. See the communications category for all EMS-related lessons learned in **Table 2.1**. The continued active sharing of this group has reduced the residual risk associated with the potential loss of situational awareness and monitoring capability that comes with an EMS outage.
- The EMSWG published a reference document, *Risks and Mitigations for Losing EMS Functions Reference Document,*[53] to identify and discuss the risk(s) of losing EMS functions, analyze the causes of EMS events, and share mitigation strategies to reduce the risks.
- The EAP enables the ERO to continue to analyze, track, and trend these EMS-related outages.
- Lessons learned and best practices will continue to be shared with industry to improve overall EMS performance. For 2019, four lessons learned were developed for EMS systems. See the communications category for all EMS-related lessons learned in **Table 2.1**.
- The annual NERC Monitoring and Situational Awareness Conference provides a forum to share knowledge.

---

[53] *Risks and Mitigations for Losing EMS Functions Reference Document*: https://www.nerc.com/comm/OC/ReferenceDocumentsDL/Risks_and_Mitigations_for_Losing_EMS_Functions_v2.pdf

Recommendations

- Electric utilities should develop and implement the system recovery and restoration plans, including scenarios in which the EMS and decision-support tools are unavailable. These plans should also include drills and training on the procedures plus real-life practice implementing the procedures.
- Electric utilities should use offline tools (studies) in addition to the real-time analysis tools in EMSs to analyze contingencies plus other contingency-analysis tools, including day-ahead studies as well as seasonal and standing operating guides; these contingency-analysis tools will provide a backup when the primary real-time analysis tools fail.
- Electric utilities should have backup tools and functionality ready and test them periodically. Backup tools and functionality include backup EMS systems, backup control centers, and other additional redundancy. The testing and use of these tools should be documented in emergency plans. System operators should be aware of these procedures and trained in using backup tools.
- Working with the ERO, electric utilities should develop and implement communication and response processes between RCs, BAs, and TOPs to improve overlapping coverage of situational awareness. The RCs, BAs, and TOPs should coordinate actions with their facilities to maintain the reliability of the BES.

Bulk Electric System Impact of Extreme Event Days

Extreme event days are identified as events that fall above of the 95th percentile upper bound relative to historical severity measures for a given season within NERC or a specified Interconnection.[54] This analysis expands on the transmission and generation components that contribute to the SRI reported in **Chapter 4**.

The response to extreme days is characterized by the amount of transmission or generation reporting immediate outages or derates on a given day. By analyzing the impact and causes of extreme event days it is possible to identify which conditions pose the highest risk to the BES. Resilience and recovery actions can mitigate exposure from these risks. While this analysis cannot address every potential scenario, learning from performance during extreme events helps provide insight into how the system may respond to a range of conditions and events.

Extreme day outages for transmission and generation are presented for NERC and by Interconnection.[55] The analysis listed below is reported separately for transmission and generation in **Table 5.2**, arranged with NERC first and followed by each Interconnection. The figures listed in **Table 5.2** show the following:

- The daily loss chart illustrates on a time line where extreme days exceed the seasonal bounds.
- The table shows the maximum daily loss in the last five years and details of each of the days in 2019 that exceed seasonal bounds. The worst day for each section is highlighted in red. The average is bold.
- The chart illustrates the major causes of outages occurring on the extreme outage days.

Table 5.2: Reference for Extreme Day Tables and Figures

Interconnection	Transmission		Generation	
	Impact of Daily Transmission Losses	Maximum Daily Transmission Loss Impact, 2019 Daily Detail of Transmission Loss, and Top Outage Causes	Impact of Daily Generation Losses	Maximum Daily Generation Loss Impact, 2019 Daily Detail of Generation Loss, and Top Outage Causes
NERC	Figure 5.17	Figure 5.18	Figure 5.19	Figure 5.20
Expanded Eastern	Figure 5.21	Figure 5.22	Figure 5.23	Figure 5.24
Texas	Figure 5.25	Figure 5.26	Figure 5.27	Figure 5.28
Western	Figure 5.29	Figure 5.30	Figure 5.31	Figure 5.32

Transmission Impacted: NERC

In 2019, seven days qualified as extreme transmission days for the BPS in North America. On these days, the aggregated potential MVA capacity impacted due to automatic transmission outages was 2.5–8 times as high as the average day across NERC. These outages were initiated by a variety of causes, primarily weather (excluding lightning) and fire. 2019's most extreme transmission-impacting day was caused due to the Saddleridge Fire event in the Western Interconnection that resulted in repeated outages on two 500 kV ac transmission lines. Despite the extreme conditions, reliability was maintained due to operator action and availability of local thermal generation.

Generation Impacted: NERC

Based on analysis of GADS data, five days in 2019 qualified as extreme for the BPS in North America. On these days, the generation portion of the BES experienced outages that were 2–3 times as severe as the average day. These outages were initiated by a variety of causes with fuel, ignition, and combustion systems being the main contributor, primarily within the Eastern Interconnection. Additionally, lack of fuel continues to appear as an issue for natural gas and oil units within the Eastern Interconnection during cold weather events.

---

[54] The 90% confidence interval of the historic values is between 5th percentile and 95th percentile.

[55] For extreme day Interconnection analysis, the Québec Interconnection is included in the analysis labeled as Expanded Eastern Interconnection.

NERC-Wide: Transmission Impacts during Extreme Days

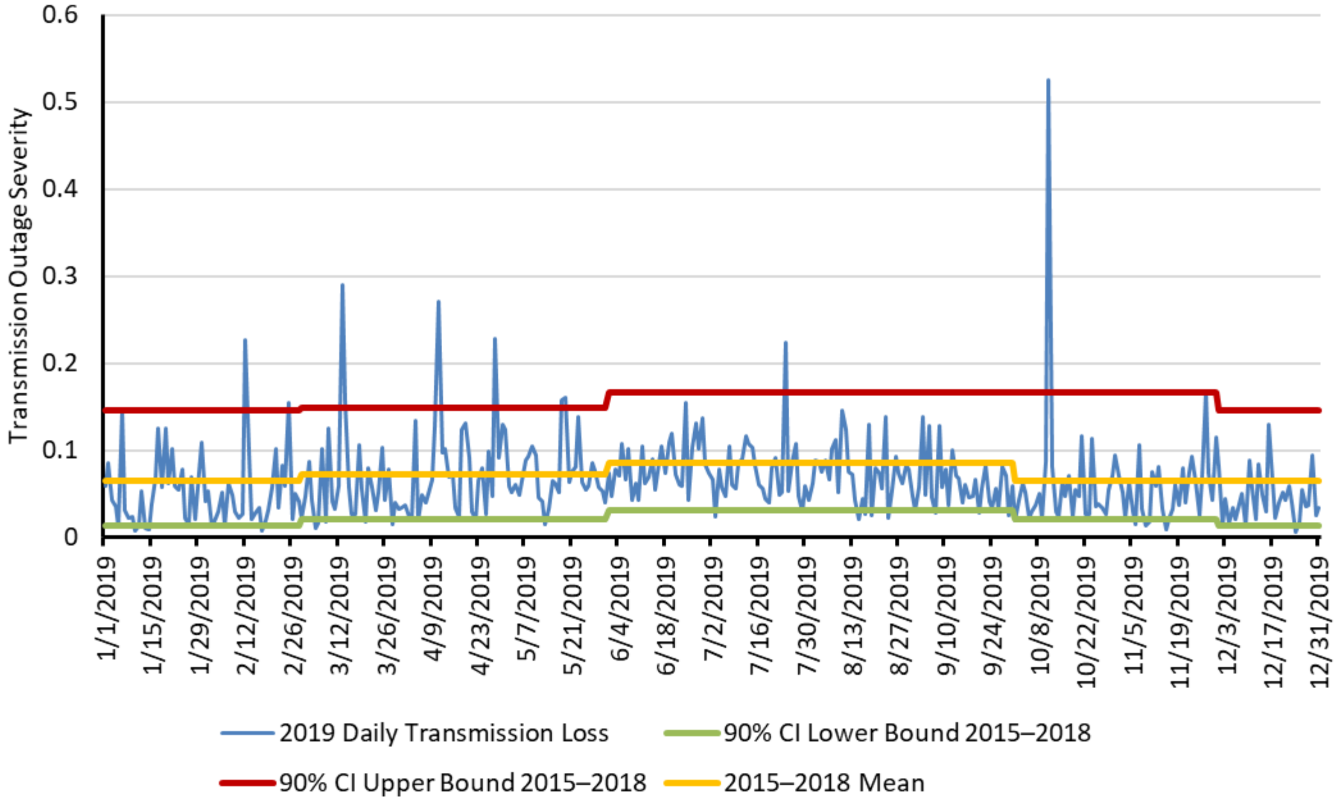


Figure 5.17: Transmission Impacted during Extreme Event Days—NERC

Maximum Daily Transmission Loss in Last Five Years (%)
NERC

Date	Daily Transmission Loss
Sep 11, 2017	0.581
Oct 11, 2019	0.526
Mar 13, 2019	0.290
Apr 11, 2019	0.270
Apr 28, 2019	0.228
Feb 12, 2019	0.228
Aug 24, 2019	0.225
Nov 27, 2019	0.168
2019 Average	**0.065**

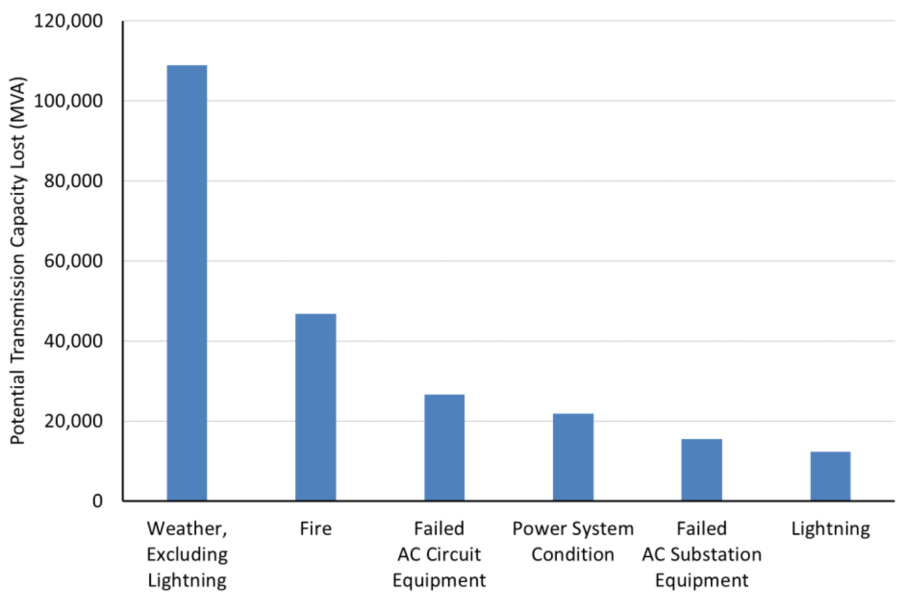


Figure 5.18: Leading Causes of Transmission Outages during Extreme Event Days—NERC

NERC-Wide: Generation Impacts during Extreme Days

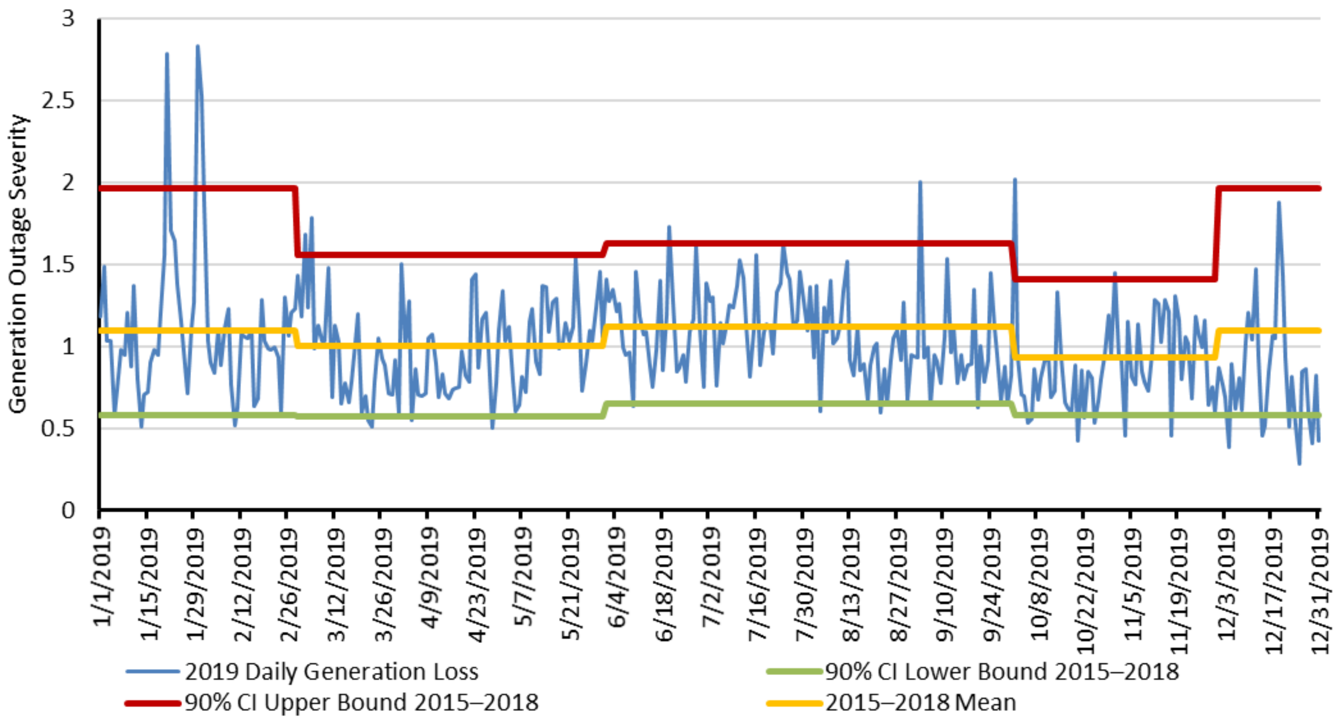


Figure 5.19: Generation Impacted during Extreme Event Days—NERC

Maximum Daily Generation Loss in Last Five Years (%) NERC	
Date	Daily Generation Loss
Jan 2, 2018	3.807
Jan 30, 2019	2.831
Jan 21, 2019	2.789
Jan 31, 2019	2.531
Oct 3, 2019	2.021
Sep 3, 2019	2.006
2019 Average	**1.010**

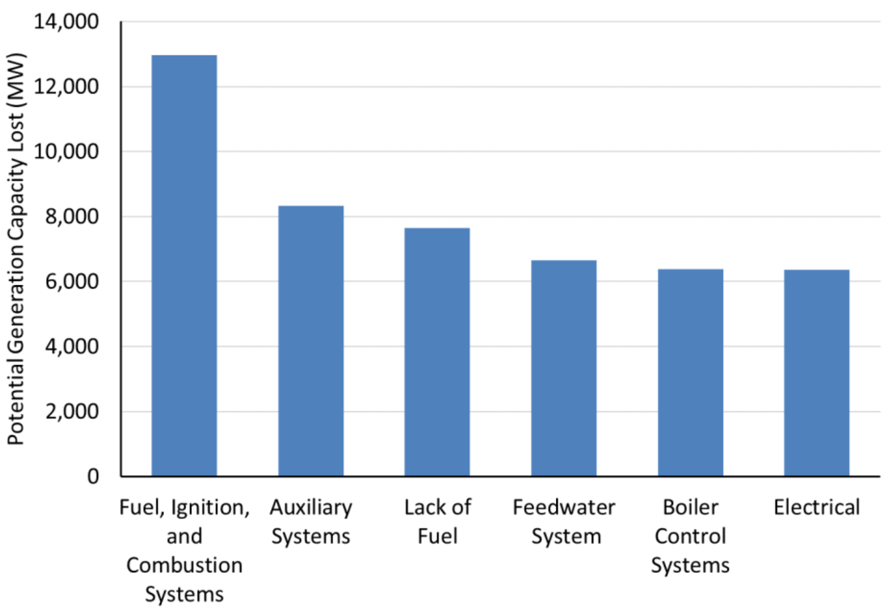


Figure 5.20: Leading Causes of Generation Forced Outages during Extreme Event Days—NERC

Expanded Eastern Interconnection: Transmission Impacts during Extreme Days

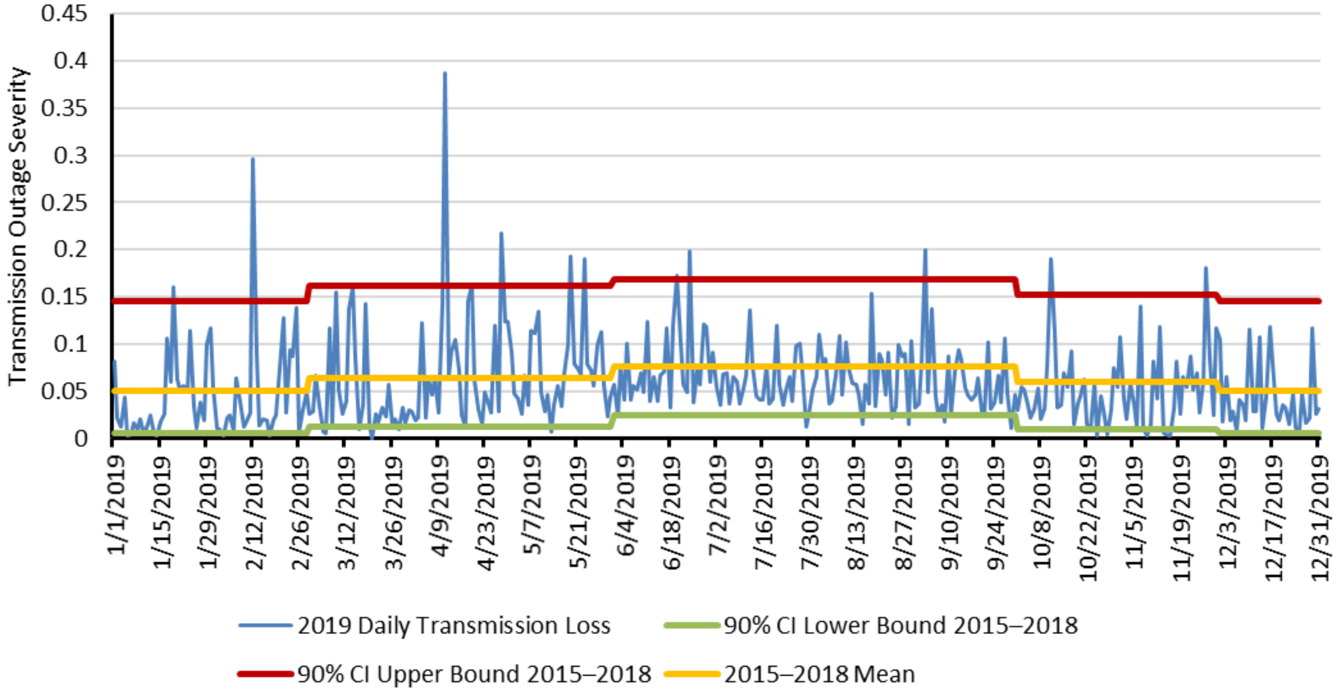


Figure 5.21: Transmission Impacted during Extreme Event Days—Expanded Eastern Interconnection

Maximum Daily Transmission Loss in Last Five Years (%)
Expanded Eastern Interconnection

Date	Daily Transmission Loss
Sep 11, 2017	0.840
Apr 11, 2019	0.388
Feb 12, 2019	0.296
Apr 28, 2019	0.217
Sep 3, 2019	0.200
Jun 24, 2019	0.199
May 19, 2019	0.193
May 23, 2019	0.190
Oct 11, 2019	0.190
Nov 27, 2019	0.180
Jun 29, 2019	0.173
2019 Average	**0.058**

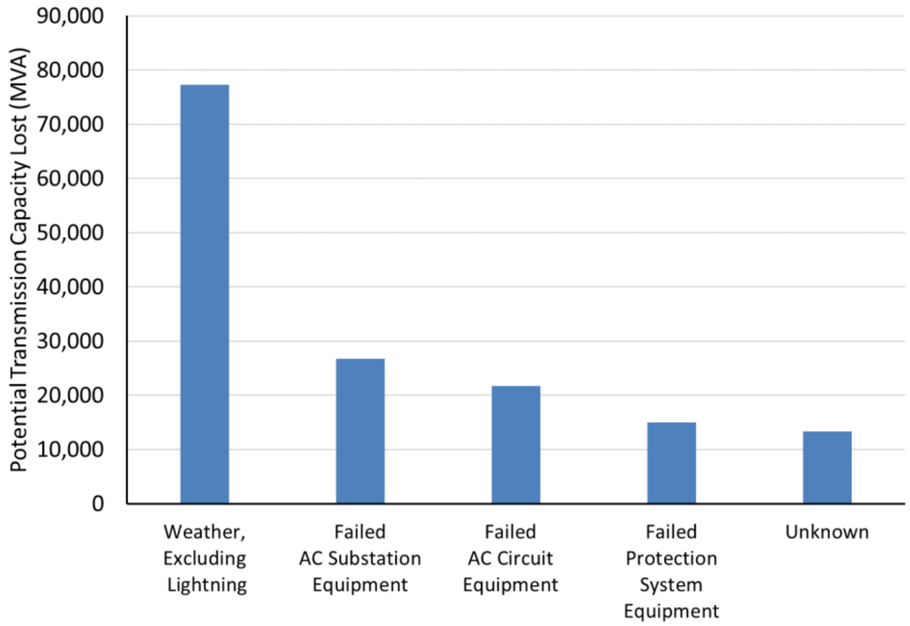


Figure 5.22: Leading Causes of Transmission Outages during Extreme Event Days—Expanded Eastern Interconnection

Expanded Eastern Interconnection: Generation Impacts during Extreme Days

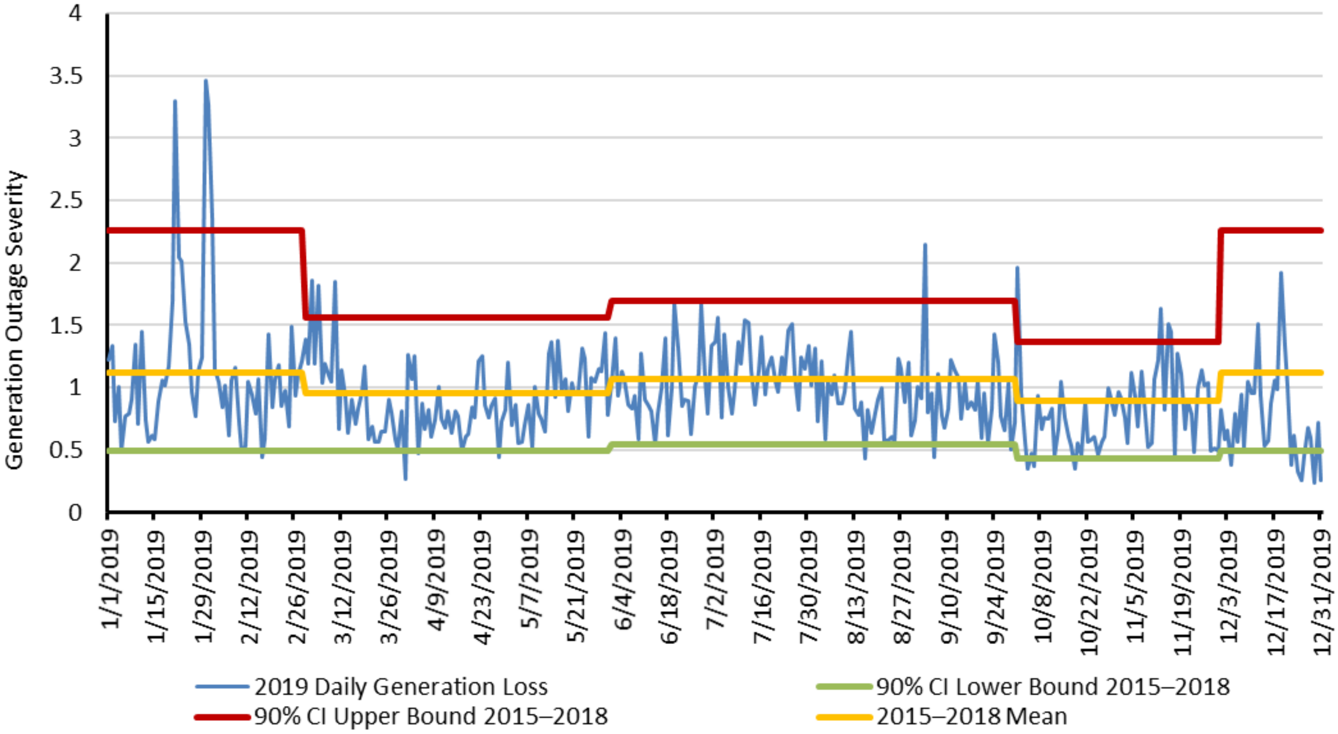


Figure 5.23: Generation Impacted during Extreme Event Days—Expanded Eastern Interconnection

Generation Loss in Last Five Years (%) Expanded Eastern Interconnection	
Date	Daily Generation Loss
Jan 2, 2018	4.795
Jan 30, 2019	3.463
Jan 21, 2019	3.293
Jan 31, 2019	3.264
Feb 1, 2019	2.362
2019 Average	**0.946**

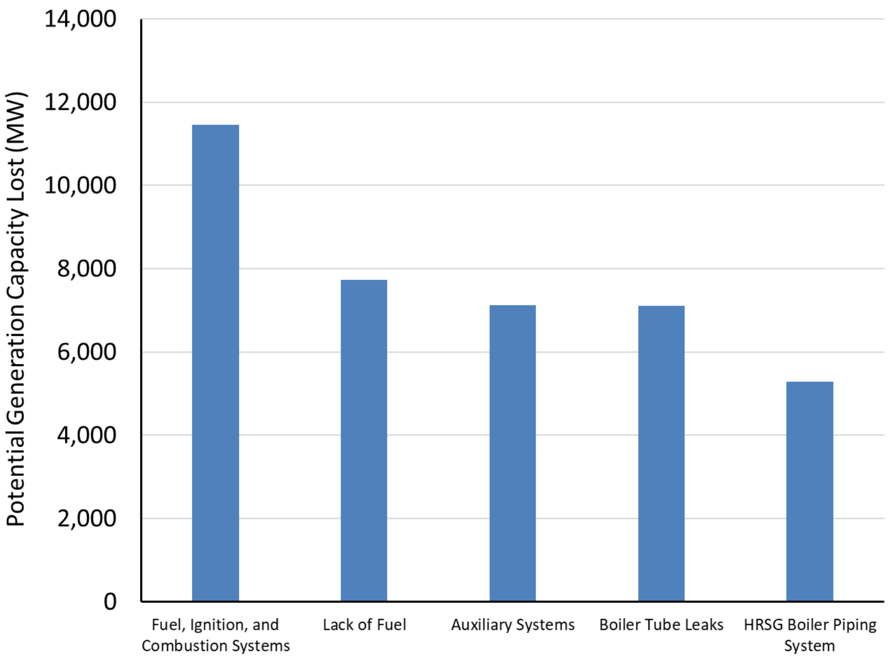


Figure 5.24: Leading Causes of Generation Forced Outages during Extreme Event Day—Expanded Eastern Interconnection

ERCOT Interconnection: Transmission Impacts during Extreme Days

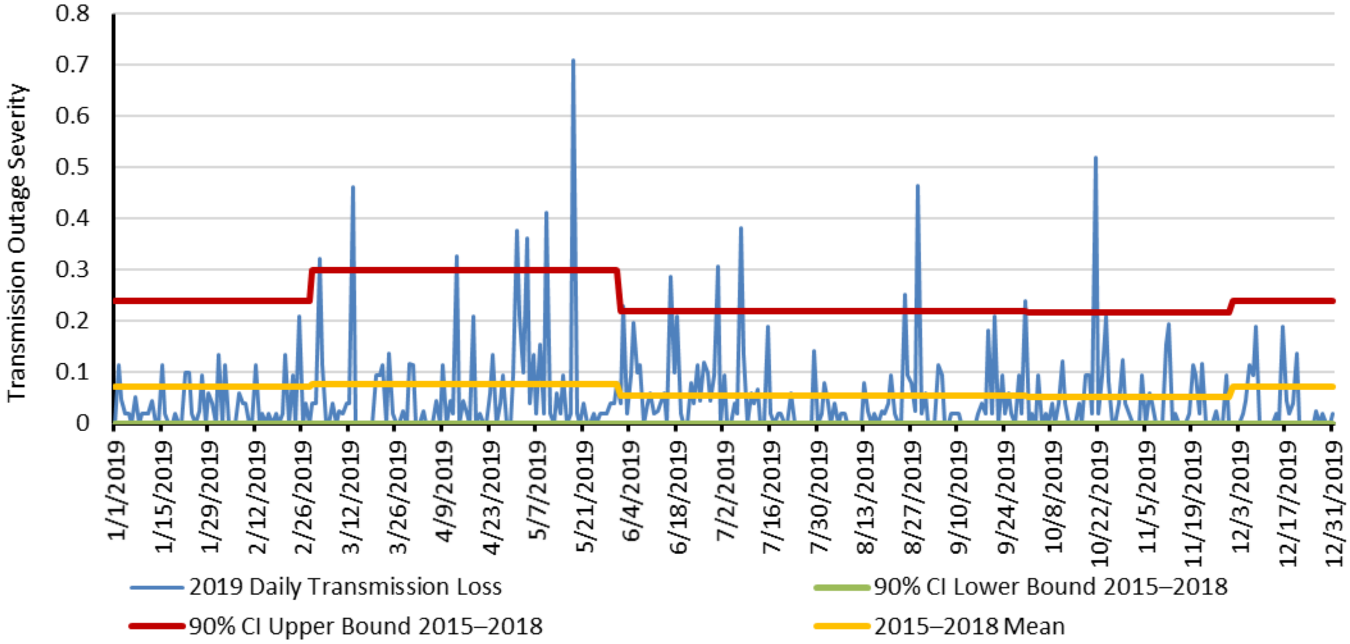


Figure 5.25: Transmission Impacted during Extreme Event Days—ERCOT Interconnection

Maximum Daily Transmission Loss in Last Five Years (%)
ERCOT Interconnection

Date	Daily Transmission Loss
Dec 27, 2015	1.733
May 18, 2019	0.708
Oct 21, 2019	0.519
Aug 29, 2019	0.463
Mar 13, 2019	0.461
May 10, 2019	0.413
Jul 7, 2019	0.382
May 1, 2019	0.378
May 4, 2019	0.362
Apr 13, 2019	0.327
Mar 3, 2019	0.323
Jun 30, 2019	0.306
2019 Average	**0.051**

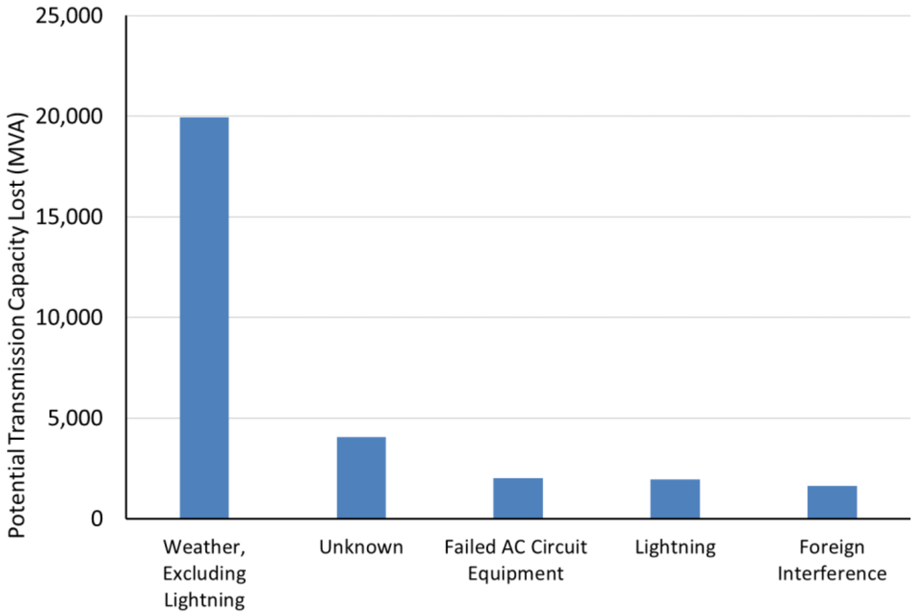


Figure 5.26: Leading Causes of Transmission Outages during Extreme Event Days—ERCOT Interconnection

ERCOT Interconnection: Generation Impacts during Extreme Days

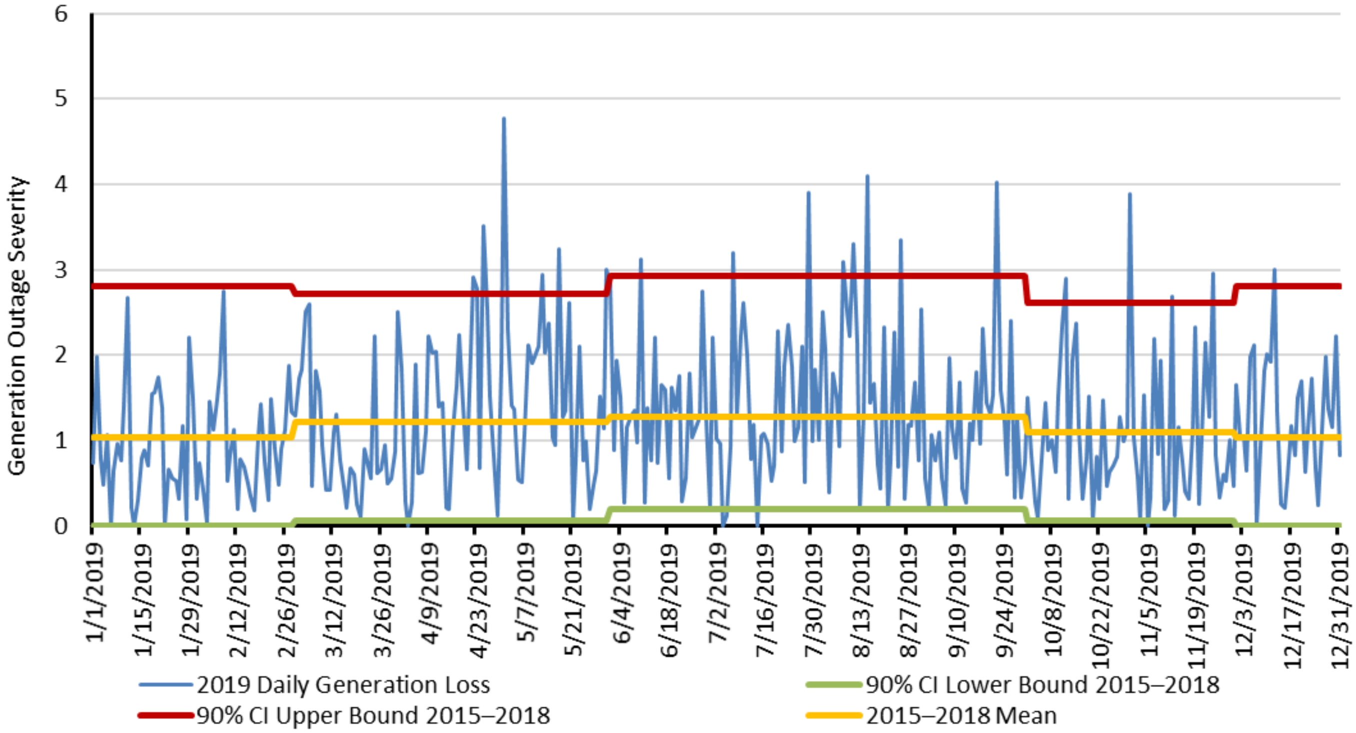


Figure 5.27: Generation Impacted during Extreme Event Days—ERCOT Interconnection

Maximum Daily Generation Loss in Last Five Years (%)
ERCOT Interconnection

Date	Daily Generation Loss
Dec 18, 2016	7.877
May 1, 2019	4.775
Aug 15, 2019	4.103
Sep 22, 2019	4.029
Jul 29, 2019	3.901
Oct 31, 2019	3.892
Apr 25, 2019	3.507
Aug 25, 2019	3.343
Aug 11, 2019	3.299
May 17, 2019	3.242
Jul 7, 2019	3.202
Jun 10, 2019	3.125
Aug 8, 2019	3.098
2019 Average	**1.232**

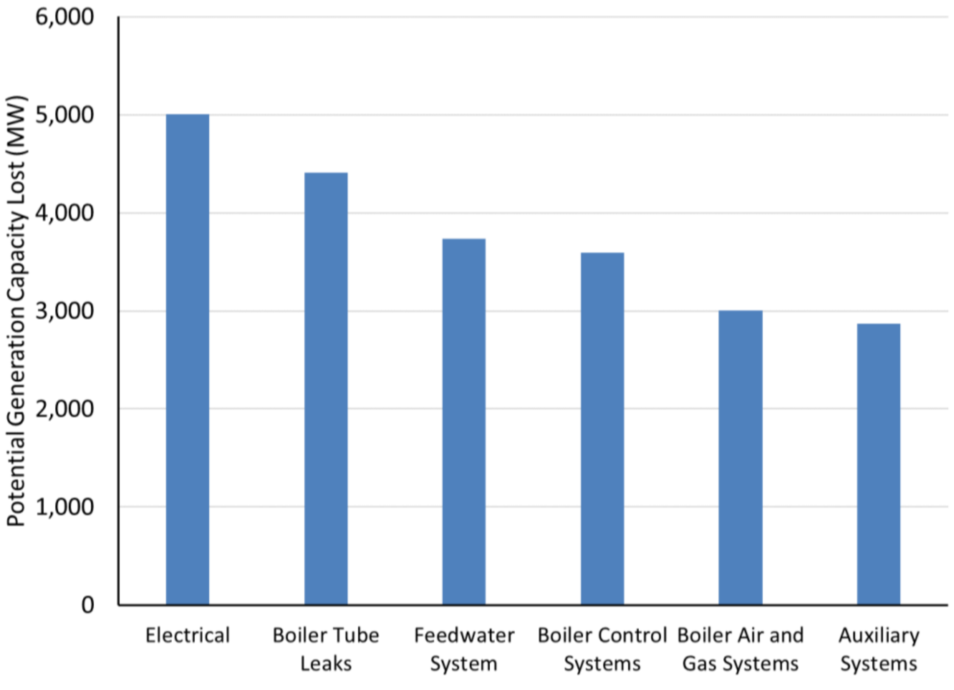


Figure 5.28: Leading Causes of Generation Forced Outages during Extreme Event Days—ERCOT Interconnection

Western Interconnection: Transmission Impacts during Extreme Days

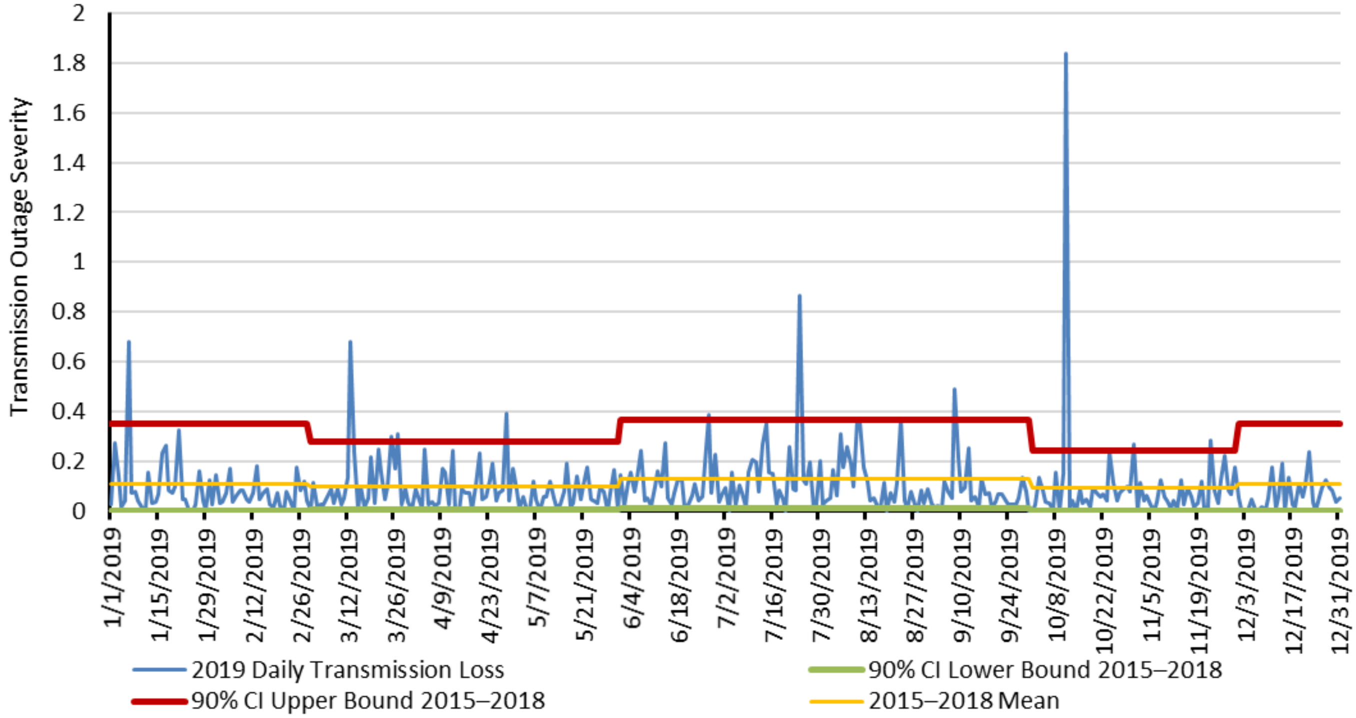


Figure 5.29: Transmission Impacted during Extreme Event Days—Western Interconnection

Maximum Daily Transmission Loss in Last Five Years (%)
Western Interconnection

Date	Daily Transmission Lost
Oct 11, 2019	1.836
Jul 24, 2019	0.866
Mar 13, 2019	0.682
Jan 6, 2019	0.681
Sep 8, 2019	0.489
Apr 28, 2019	0.393
Jun 27, 2019	0.388
Aug 23, 2019	0.370
Aug 10, 2019	0.369
2019 Average	**0.096**

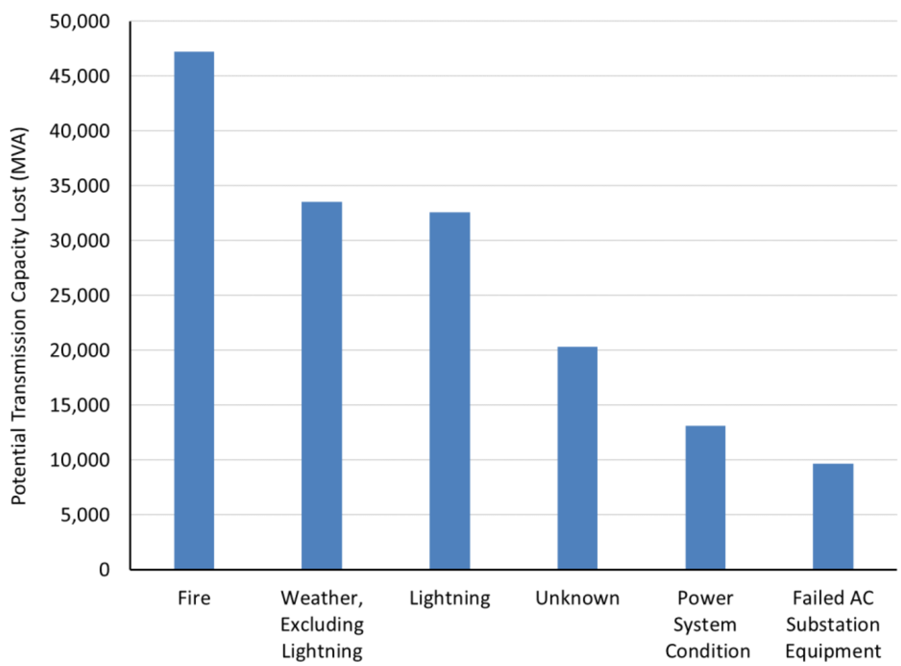


Figure 5.30: Leading Causes of Transmission Outages during Extreme Event Days—Western Interconnection

Western Interconnection: Generation Impacts during Extreme Days

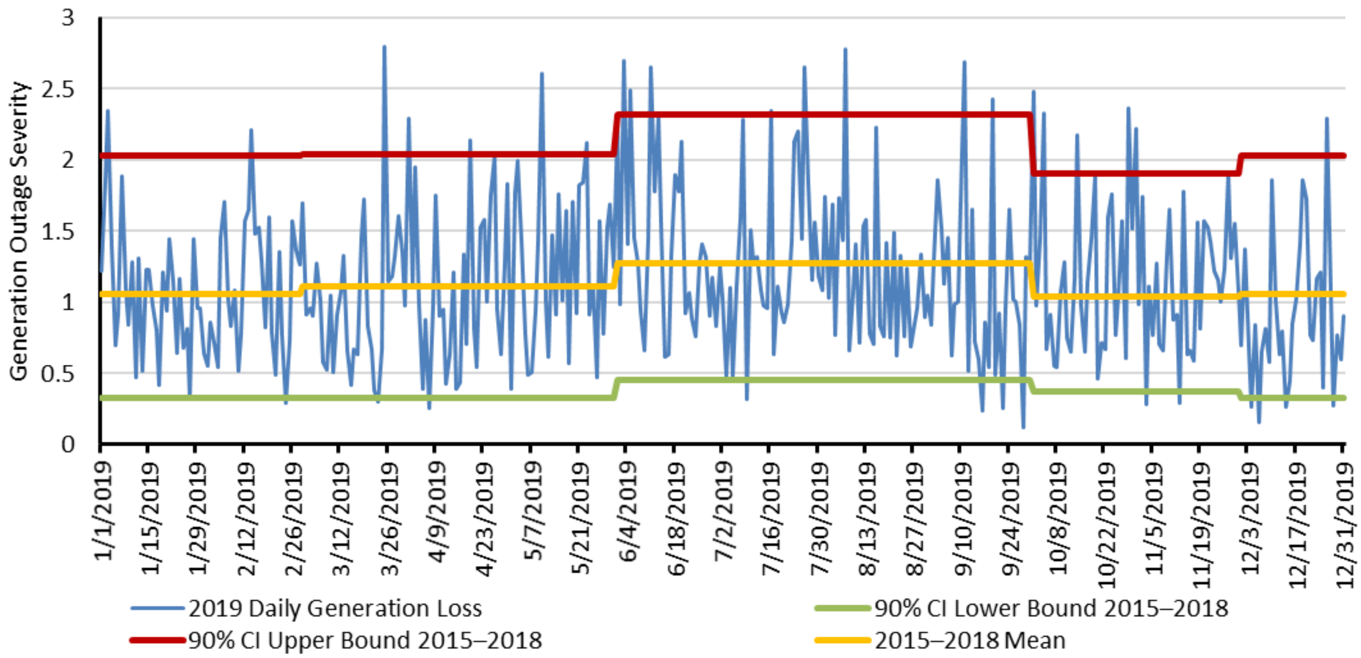


Figure 5.31: Generation Impacted during Extreme Event Days—Western Interconnection

Maximum Daily Generation Loss in Last Five Years (%) Western Interconnection

Date	Daily Generation Lost
Apr 28, 2015	3.722
Mar 25, 2019	2.801
Aug 7, 2019	2.782
Jun 3, 2019	2.702
Sep 11, 2019	2.688
Jun 11, 2019	2.657
Jul 26, 2019	2.650
May 10, 2019	2.609
Jun 5, 2019	2.494
Oct 1, 2019	2.480
Sep 19, 2019	2.429
Oct 29, 2019	2.365
Jan 31, 2019	2.351
Jul 16, 2019	2.351
Oct 4, 2019	2.327
2019 Average	**1.153**

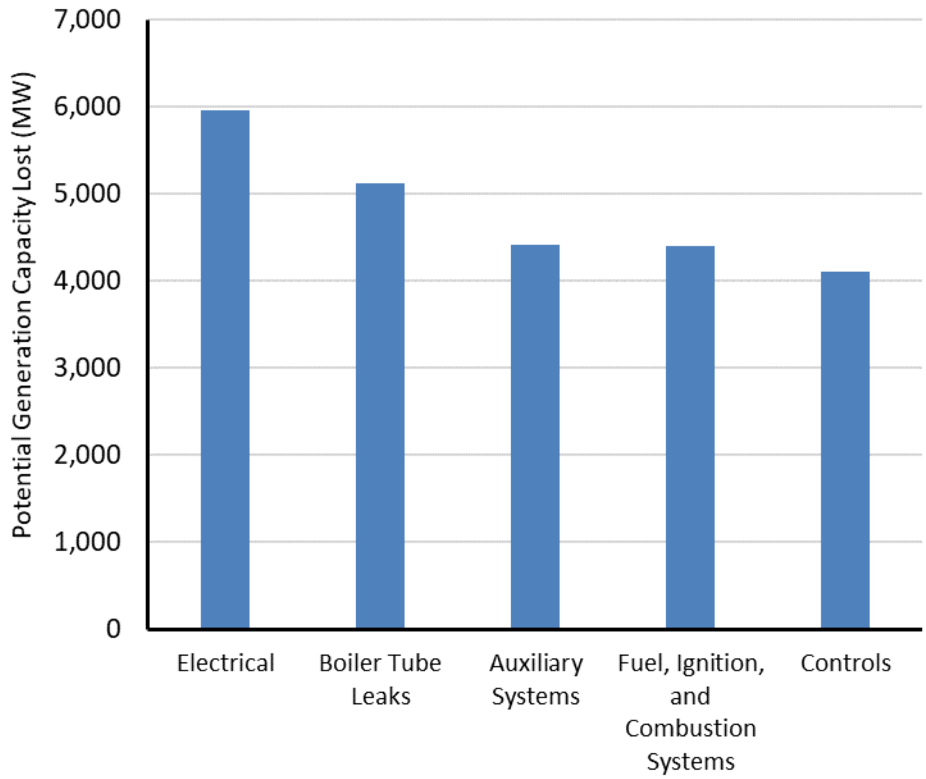


Figure 5.32: Leading Causes of Generation Forced Outages during Extreme Event Days—Western Interconnection

Actions and Mitigations in Progress

- Mutual assistance agreements provide essential personnel, equipment, and material following extreme weather events. NERC continues to encourage participation with assistance from government and nongovernmental authorities where applicable.
- Standards around equipment winterization are under development.
- Entities are developing energy forecasts, such as ISO New *England's 21-day Energy Assessment Forecast and Report*, which compares forecasted and expected conditions against established thresholds to trigger the declaration of energy alerts (declared in day 6–21 time frame) or energy emergencies (declared in Day 1–5 time frame).[56]
- Studies assessing single points of failure for pipeline disruptions that affect number of generators are being done at the regional, market, or utility level to understand the impact of limitations on gas supply.
- NERC continues to emphasize cold weather preparation. An annual cold weather preparation webinar is provided in addition to a standard online training package and other resources.
- Training on reporting for GADS and TADS is offered annually to ensure the continuous improvement of data integrity and quality related to equipment outages and causes.

Recommendations

- Hardening of critical systems to reduce the impacts of weather should remain a key consideration for entities owning transmission assets.
- Implement recommendations outlined in the NERC *Fuel Assurance and Fuel-Related Reliability Risk Analysis for the Bulk Power System* reliability guideline recently published.[57]
- Planning for extreme conditions remains an important tool to promote understanding of the impact of scenarios on system behavior. The efforts of the planning and modelling groups at NERC are improving models and methods utilized to assess future performance. The ERO, REs, and stakeholders should continue to work together to identify extreme scenarios to be studied and prioritize those study efforts going forward.

[56] https://www.iso-ne.com/isoexpress/web/reports/operations/-/tree/21-Day-Energy-Assessment-Forecast-and-Report-Results
[57] https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Fuel_Assurance_and_Fuel-Related_Reliability_Risk_Analysis_for_the_Bulk_Power_System.pdf

Cyber and Physical Security

Cyber and physical security remains a priority for NERC, and the distinctions between cyber and physical security continue to blur. While the majority of actual occurrences can still be neatly categorized as cyber or physical security related, the realization of more severe potential reliability impacts frequently requires compromise of both cyber and physical security defenses. Entities are targeted by criminals because entities are organizations with valuable resources and by nation-state adversaries due to the importance of the critical services they provide to national security, public welfare, and the economy. Utilities are now on the front lines of an escalating conflict that they did not choose to engage in; they are opposed by nation-state adversaries that they are ill equipped to compete with alone. The reality of today’s threat environment is that every organization is a target, and adversaries can employ extremely sophisticated capabilities backed by significant resources to accomplish their objectives. NERC works closely with public and private partners to address these concerns even as threats continuously evolve. As the digitization of the electricity industry and of society continues to grow in scale and in complexity, exploitable vulnerabilities increase in number regardless of remediation efforts. Taken together, these trajectories create increasing risk to the BPS.

2019 Physical Security Environment

Three threat sources dominated the physical security environment throughout 2019, listed here:

- **Unmanned Aerial Systems:** UAS threats to industry increased through 2019. Drone technology continues to improve, making a variety of platforms cheaper and more capable with lower barriers to access. Relevant UAS incidents in 2019 include attacks on Saudi Arabian energy infrastructure, interference with two major airports in England, and a mock attack on a nuclear facility in France. UAS supply chain risks were addressed in a U.S. Department of Homeland Security alert on Chinese-manufactured UASs. The alert highlighted the potential exposure of sensitive data linked to equipment designed, manufactured, or supplied abroad. Together, these demonstrate the increasing flexibility of UAS use for malicious purposes across the physical, cyber, and informational environments.
- **Activist Group Threats:** Activist group threats increased slightly over the past year. Social media campaigns tied to environmental, social, and political causes dominated 2019 and occasionally targeted the electricity industry; while these campaigns rarely escalated to direct action, the potential for associated physical security threats remains. Lawful protests by activist groups targeting a utility can be disruptive to operations but also present an elevated risk of vandalism and sabotage activities from the protesting group or from opportunists. Therefore, while the electricity industry is not targeted as frequently as other sectors, such as oil and natural gas, the aspiration to cause damage to the electricity industry has been expressed by various ideological groups and should not be discounted.
- **Untargeted Criminal Activity:** Gunfire damage, particularly in the Southern and Western United States, will likely continue at current levels. This type of activity often peaks around hunting seasons in the spring and fall and is much more prevalent in rural areas. Throughout 2019, theft and other untargeted and mischief vandalism continued at similar levels to previous years. Copper-related theft is most common, but tools, other equipment, and material of value are also likely. The level of this activity can be influenced by local economic conditions and the market price of scrap copper.

2019 saw a significant increase (+536%) in physical security incidents (see **Table 5.3**) that were driven by a significantly higher number of incidents voluntarily shared with the E-ISAC from two organizations. Voluntary information sharing from all entities accounted for 79% of the 1,318 total incidents in 2019. While this created a large increase in the overall count of incidents known and analyzed, qualitative trend analysis confidently asserts that the 2019 physical security environment was relatively similar to prior years as opposed to an actual increase in the number or severity of incidents.

Table 5.3: Types of Physical Security Incidents Reported to the E-ISAC	
Theft	Theft incidents were predominately copper theft but also included electronic equipment, materials, vehicles, keys, and other items. A majority of thefts took place at substations.
Intrusion	A total of 42% of intrusions took place at substations and over half included break-in damage only. A total of 15 incidents included tampering of some type, all of which were assessed to be mischief rather than intentional attempts to impact the BPS.
Suspicious Activity	A majority of suspicious activity reports took place at administrative buildings, such as commercial sites or office buildings, and generally included suspicious objects or packages, impersonation of company employees, social engineering attempts, and a variety of unexplained behavior.
Vandalism	Most vandalism incidents in 2019 involved transmission and distribution systems, but it is worth noting that theft incidents commonly involve some measure of vandalism as well. Of note, one entity reported a series of apparently related instances of vandalism on pad-mount transformers by cutting or drilling holes into the bases of transformers, leading to equipment failure and customer outages.
Surveillance	Photography and UASs accounted for a majority of surveillance incidents. UAS incidents were typically fly-overs where the UAS's intent could not be determined, the discovery of drones on entity properties or facilities, or drones being used to conduct surveillance. In one case, an entity reported several UASs flying in a stack formation over their property for over three hours two nights in a row. Visually interesting sites, such as generation plants, substations, administrative buildings, and communication sites, were popular targets of surveillance.
Threat	Threat incidents targeting specific companies or employees were mostly bomb related, mostly from disgruntled customers or members of the public. Other threats targeting the industry in general typically came from various activist groups.
Gunfire	Gunfire incidents are primarily discovered during routine inspections or transmission line maintenance. Most incidents are assessed as accidental or nonmalicious vandalism (target practice).
Sabotage	An entity characterized a series of cuts to fiber optic cables associated with a coal analyzer system as potential sabotage.
Other	Other physical security incidents included activist activity on entity properties, arson, apparent accidental crashes, and a small plane becoming entangled in power lines in one case.

Regionally, the most incidents occurred in WECC and the least in Texas RE (see **Figure 5.33**). The number of incidents in the map add up to less than 1,318 because some incidents in 2019 involved a specific sector and not a RE or the report lacked specific location data. **Figure 5.33** also breaks the RE incidents into types. The types that appear to occur in greatest numbers in all REs appear to be gunfire and intrusions.

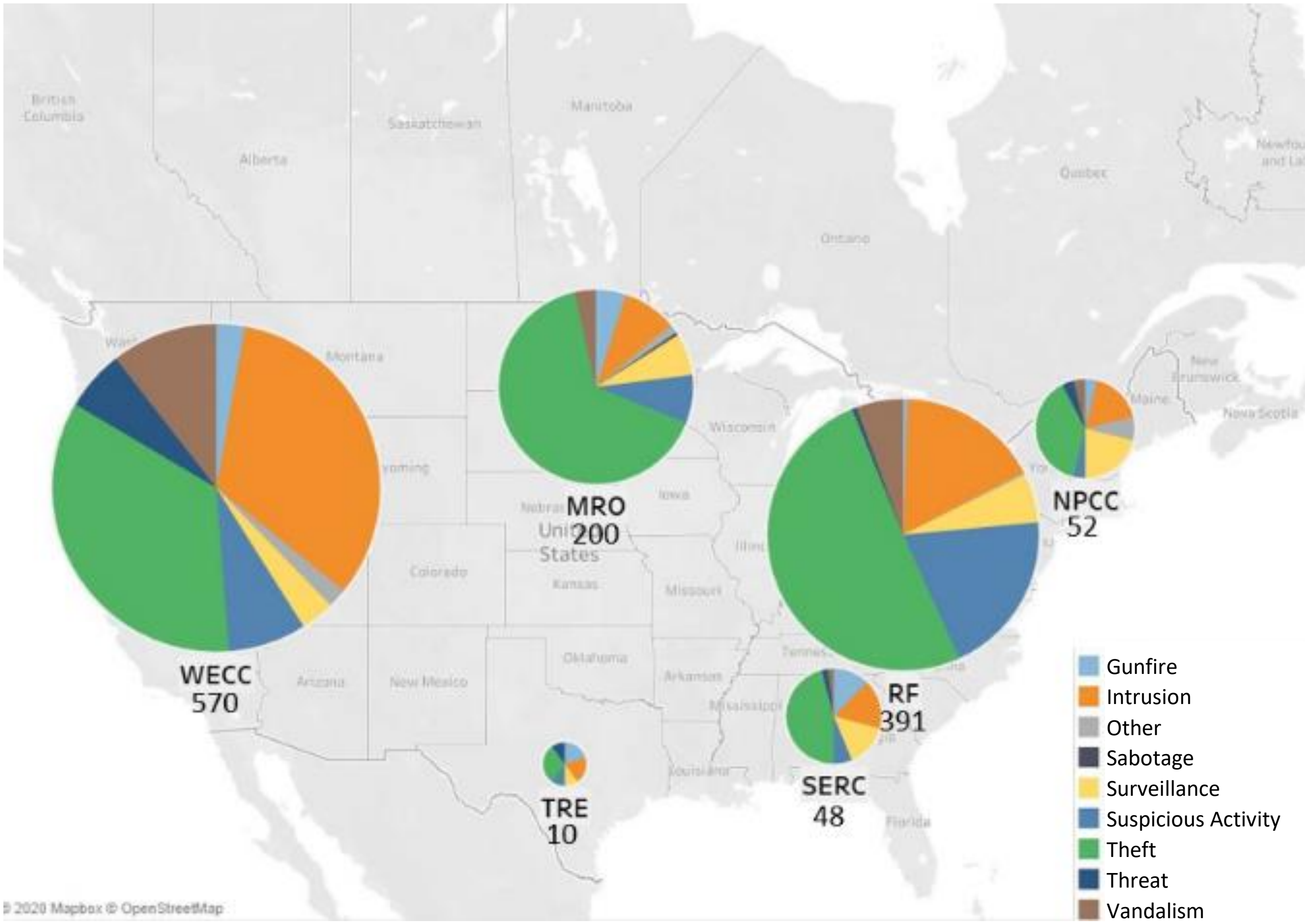


Figure 5.33: 2019 Physical Security Incidents by Regional Entity

For 2019, prior years' improvements in data collection and analytical capability allow longitudinal analysis of quarterly physical security incident trends against a consistent three year (2016–2018) baseline (see **Figure 5.34**)

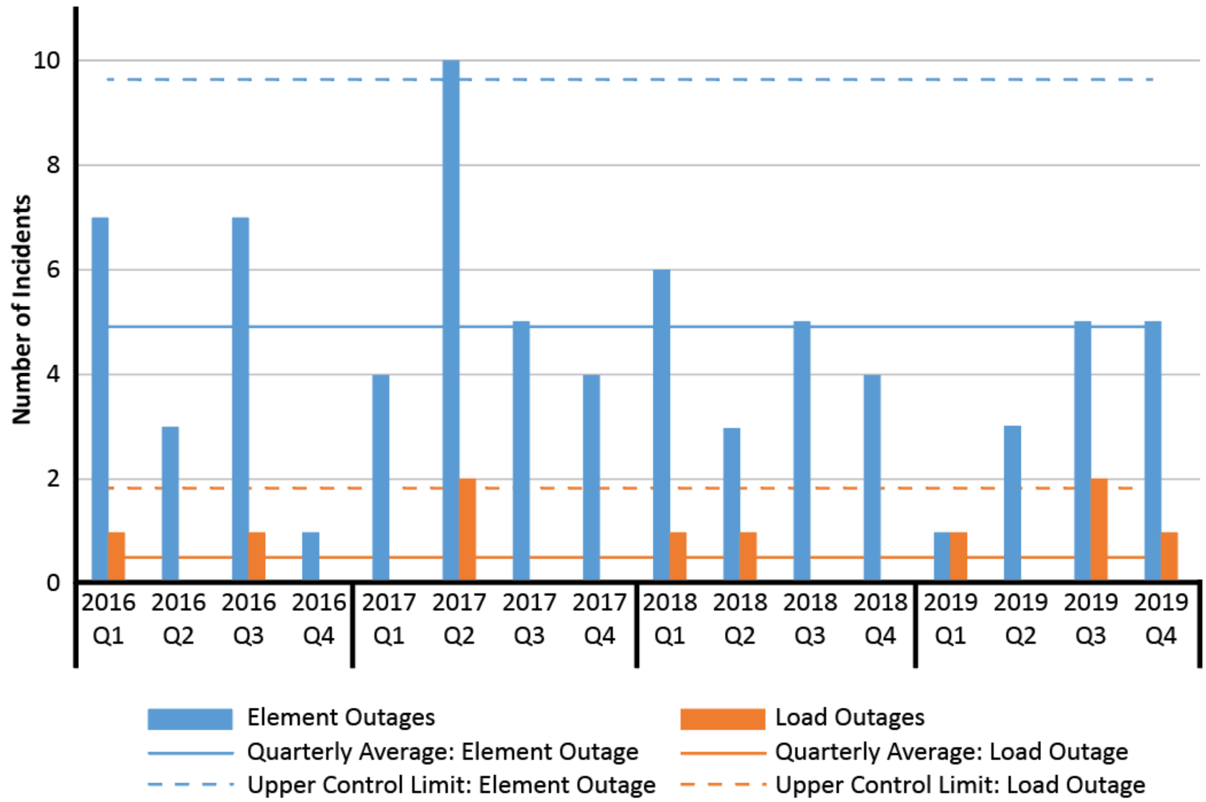


Figure 5.34: 2016–2019 Impactful Physical Security Incident Quarterly Trends

There were 14 physical security incidents in 2019 that resulted in a BES element outage, 4 of which also involved consequential loss of load. Details of the 4 incidents with load outages were as follows:

- A transmission line tripped to lockout during a storm due to gunshot damage to five of six bells on a single insulator string; system topology at the time of the incident also forced 40 MW of generation across three facilities offline and caused a sustained outage to 5 MW of load after the line sectionalized automatically by design.
- A looped transmission line tripped due to a conductor failure from apparent recent gunshot damage, causing an outage to industrial loads from four connected substations for approximately 16 hours.
- A transmission substation was de-energized to safely make repairs following discovery of copper ground theft, resulting in an unplanned outage to 4 MW of load for over four hours.
- A transmission line tripped to lockout due to a fault caused by vandalism to a switch. This resulted in damage to the line switch and burned open jumpers, causing 35 MW of load to be interrupted for over 13 hours.

2019 Cyber Security Environment

In 2019, as in previous years, there were no known NERC-reportable cyber security incidents that resulted in a loss of load. This shows that the combined efforts of industry, NERC, the E-ISAC, and government partners have so far been successful in protecting the BPS's reliability. Positive results for the most important measure notwithstanding, NERC and industry must maintain a continued focus on improving defenses and resilience capabilities because adversaries constantly learn and adopt new tactics, new vulnerabilities are introduced and discovered, and the duration and magnitude of potential impacts change as the grid and cross-sector interdependencies evolve.

While specific techniques and indicators of compromise change frequently, certain underlying tactics observed across the broad cyber security industry continued through 2019. Applying these insights from other industries and countries provides context to electricity industry-sourced observations, information sharing, and reports of how similar tactics may be employed against the electricity industry. In increasing order of potential impact to utilities, these tactics are as follows:

- **Cyber Hygiene:** Adversaries will find and exploit weaknesses in basic cyber hygiene, such as known and unremediated vulnerabilities in popular software, inappropriately configured internet-facing devices, and reuse of credentials that were exposed in prior breaches of other organizations.
- **Social Engineering:** Targeted phishing and other forms of social engineering exploit human fallibility and trust to gain an initial foothold into targeted systems. Phishing continues to be widely used because it continues to deliver results for adversaries, and the most advanced examples of targeted spear phishing are practically indistinguishable from legitimate email traffic.
- **Insider Threats:** Recruiting a willing or coerced insider to facilitate access is a highly effective (but riskier to the adversary) tactic. Employees, subcontractors, and other business affiliates have good access to the targeted organization and are often knowledgeable about sensitive, non-public systems of particular value. Insider threats are unwittingly facilitated by lax organizational security cultures.
- **Supply Chain Compromise:** An adversary's goal in supply chain compromise is getting a specific organization or industry to acquire and use equipment that has unknown exploitable features. While there are many methods, supply chain vectors are resource intensive; certain vendors can introduce their goods into locations of strategic interest through insurmountable competitiveness on cost likely subsidized by the host vendor's host nation. Deliberately opaque and convoluted networks of largely unknown resellers and brokers with bids deliberately crafted to exploit the acquisition rules of the target customer are sometimes used to mask these activities. For power system and telecommunications facilities, turnkey engineering-procurement-construction management contracts are an enduring risk throughout the entire lifecycle of the infrastructure, increasing exposure to the threat. In the most extreme cases, simply acquiring the target organization or a connected entity is a feasible option for the most well-resourced adversaries. While legal and regulatory controls in the United States and Canada may prevent direct use of this tactic, these defenses would not necessarily preclude the adversary from locking down strategic portions of a broader value chain.

Cyber security is a dynamic and multifaceted discipline that constantly evolves on both the offensive and defensive sides, challenging longer-term trend analyses seen elsewhere in State of Reliability reports. In 2019, the number of cyber security events shared with the E-ISAC from all sources nearly tripled, to 684. In cyber security, different from other sections of this report, an event is a change in the normal behavior of a system, process, or environment. The typical organization experiences thousands or millions of events every day, and very few of these events are incidents (incidents are events that negatively impact the organization). Therefore, while the significant increase in available information in 2019 has improved our understanding of the environment, it does not necessarily mean that there were more (or more impactful) incidents in 2019 compared to prior years. **Figure 5.35** shows monthly cyber security events by type. Suspicious Activity and Phishing attempts were by large the most frequent event types reported in 2019.

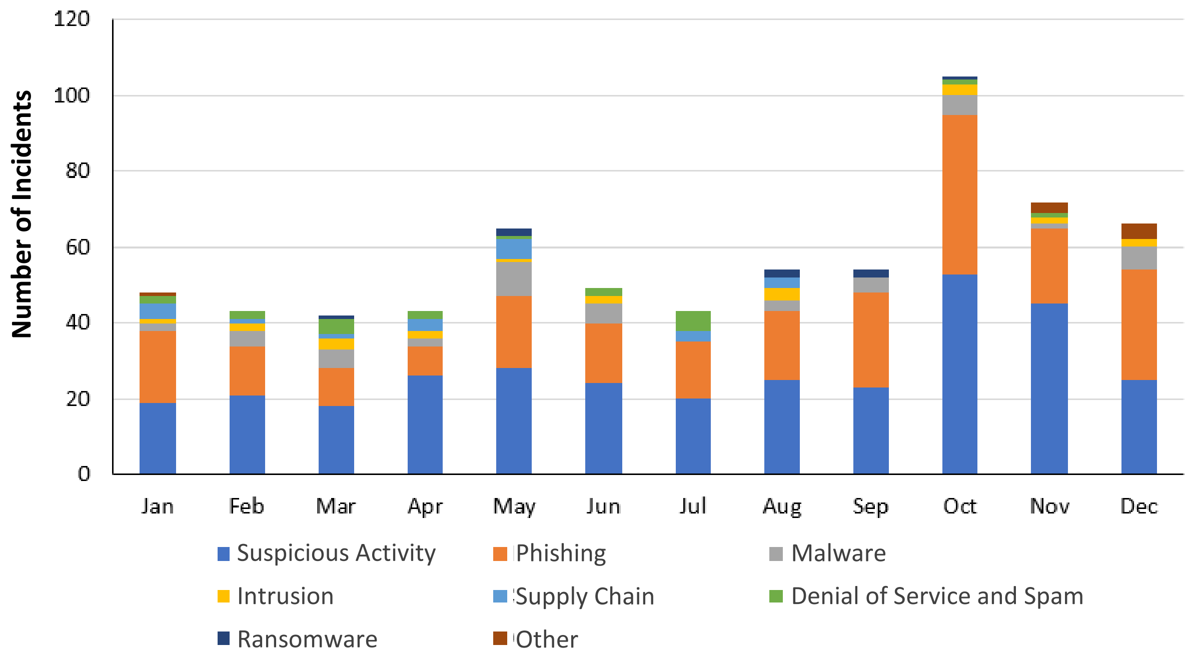


Figure 5.35: 2018 Cyber Security Events by Delivery Mechanism

XENOTIME

Targeted and prolonged malicious cyber activity is often tracked by using distinctive names to denote a particular related set of activities or organization. XENOTIME is a sophisticated threat actor group behind the TRISIS malware attack in 2017 that caused a disruption at an oil and natural gas facility in Saudi Arabia. The joint Dragos-E-ISAC report on XENOTIME outlines an expansion in targeting to include the electricity industry in North America. Dragos emphasized the fact that this is an expansion, not a shift, in activity as the group continues to target oil and natural gas organizations.

Supply Chain

The complex nature of the supply chains for information technology poses a significant security concern to the electricity industry. In 2019, NERC and the E-ISAC released a Level 2 NERC alert that addressed issues raised by the use of certain telecommunications and video surveillance equipment from certain Chinese technology suppliers. The E-ISAC has urged members to view the U.S. prohibitions on these Chinese suppliers in the context of the U.S. Department of Homeland Security's Binding Operational Directive 17-01, which compelled U.S. federal agencies to remove Kaspersky-branded products.

Geopolitical Tension

Geopolitical tensions between the United States and Iran in 2019 heightened concern over potential retaliatory cyber offensive activities against critical infrastructure. Cyber operations are an important part of Iran's tool kit to pursue domestic, regional, and international interests. Iran has historically leveraged asymmetrical tactics in order to extend their capabilities. Cyber operations act as a force multiplier for Iran to exercise influence, suppress dissent, and harm regional and international adversaries. Iranian cyber threat actors continuously develop and improve their capabilities. Open-source information has attributed several offensive cyber operations that targeted a variety of industries, including energy, to Iranian actors. For some of these high-profile attacks, the U.S. government identified Iranian threat actors as the perpetrators and issued several indictments.

Ransomware

Ransomware remains a threat with tactics constantly evolving and threat actors becoming more sophisticated and creative. Although the E-ISAC has not observed ransomware targeting electricity industrial control systems (ICSs), ransomware continues to affect ICS environments around the world. Much of the ransomware that impacted industrial or manufacturing organizations around the world was more targeted in nature. These ransomware incidents were typically not spread inadvertently by self-propagating malware but occurred due to threat actors compromising domain administrators' accounts and propagating the malware to all systems in the network. Even when the affected systems are only IT networks, the operational and business impact to affected organizations can be severe.

Critical Vulnerabilities

The E-ISAC shared information on a number of critical vulnerabilities found in information technology and ICSs that presented a significant risk to asset owners and operators. These vulnerabilities include BlueKeep, a vulnerability in Microsoft's Remote Desktop Services that could allow for the spread of malware in a worm-able manner, and the 11 vulnerabilities in VxWorks real-time operating system announced in July. While none of these threats focus specifically on the electricity industry, organizations must maintain vigilant as attackers have begun to target these vulnerabilities. The E-ISAC shared mitigation methods and lists of affected systems in multiple all-points bulletins released for each significant vulnerability.

Actions and Mitigations in Progress

- The E-ISAC reduces cyber and physical security risk by continually improving the quality, timeliness, and actionability of information sharing to drive entity action to defend the BPS and improve their resilience.
- The Cybersecurity Risk Information Sharing Program (CRISP) facilitates timely bidirectional exchange of cyber security information among industry, the E-ISAC, and the DOE to enable owners and operators to better protect their systems from sophisticated cyber threats.
- The E-ISAC and Ontario's Independent Electricity System Operator (IESO) are partnering to combine analytic insights from CRISP and from the IESO's Project Lighthouse to improve shared understanding of the cyber security threat environment on a continent-wide basis.
- NERC's GridEx, and other federal, regional, and entity-level exercises and drills provide participants an opportunity to demonstrate, practice, and improve their responses to different attack scenarios.
- The NERC critical infrastructure protection standards provide a common foundation of solid defenses for the BES.

Recommendations

- The industry should continue to drive improvements in its security posture through technological hardening, growing a culture of security, and effective information exchange between entities, the E-ISAC, and trusted partner organizations.
- The E-ISAC should update its long-term strategic plan to incorporate developments over the last two years and continue aggressive and detailed execution of the plan that is guided by the ESCC's Member Executive Committee.
- Industry and the E-ISAC should continue to actively participate in public-private partnership opportunities coming from the National Infrastructure Advisory Council's 2019 *Transforming the U.S. Cyber Threat Partnership*[58] report and the 2020 *Cyberspace Solarium Commission* report, available on the Solarium website.[59]
- CRISP capabilities and participation should be expanded, and the CRISP model should be leveraged to incorporate new data sources for analysis coordinated with the ESCC and the DOE.

---

[58] https://www.cisa.gov/sites/default/files/publications/NIAC-Transforming-US-Cyber-Threat-PartnershipReport-FINAL-508.pdf
[59] https://www.solarium.gov/

Critical Infrastructure Interdependencies: Electric-Gas Working Group

NERC has been working with industry to mitigate the potential effects of some of the emerging critical infrastructure interdependencies, including addressing the continued reliance on natural gas deliverability and infrastructure. In 2019, NERC formed the EGWG for the purpose of analyzing the interoperability between natural gas and electricity and developing mitigation plans to address the increased interdependency of the two industries.

Key activities of the EGWG include, but are not limited to, the following:

- Author guidelines, white papers, compliance guidance, etc. in support of natural gas disruption considerations and risks that are applicable to all REs and could extend to be inclusive of all fuel sources
- Develop educational materials that can be used for a range of audiences that describe any potential emerging risks and possible solutions to address these risks
- Provide technical assistance in support for assessing fuel-related concerns in other NERC program areas
- Provide assistance to NERC Event Analysis evaluations of BPS disturbances when fuel disruptions are involved in the disturbance as necessary

In 2019 the EGWG developed a guideline directed toward industry on potential action plans and contingency plans that industry should develop to address these interdependencies. The *Fuel Assurance and Fuel-Related Reliability Risk Analysis for the Bulk Power System*[60] reliability guideline was developed in 2019 and approved by NERC's Planning Committee in March of 2020.

[60] https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Fuel_Assurance_and_Fuel-Related_Reliability_Risk_Analysis_for_the_Bulk_Power_System.pdf

Appendix A: Compilation of Recommendations

<table>
<tr><th colspan="2">Table A.1: 2020 State of Reliability Recommendations</th></tr>
<tr><th colspan="2">Long-Term and Strategic Recommendations</th></tr>
<tr><td colspan="2">The ERO and industry should continue improving their ability to understand, model, and plan for a system with a significantly different resource mix. Priority should be given to understanding the implications of the following:
Frequency response under low inertia conditions
Contributions of inverter-based resources to essential reliability services
Increasing protection system and restoration complexities with increased inverter-based resources</td></tr>
<tr><td colspan="2">The ERO and industry should develop comparative measurements and metrics to understand the different dimensions of resilience (e.g., withstanding the direct impact, managing through the event, recovering from the events, preparing for the next event) during the most extreme events and how system performance varies with changing conditions.</td></tr>
<tr><td colspan="2">The ERO and industry should continue to work closely together to understand and share information on cyber and physical security threats and mitigate the risks posed by these threats through a variety of approaches, including resilient system design, consequence-informed planning and operation, and practicing response and recovery processes.</td></tr>
<tr><th colspan="2">Recommendations to Address Priority Risks</th></tr>
<tr><td rowspan="4">BPS Planning and Adapting to the Changing Resource Mix</td><td>The ERO Enterprise and industry should work with manufacturers, vendors, and standards groups to continue mitigation efforts regarding momentary cessation as identified in the 2018 NERC alert.</td></tr>
<tr><td>The ERO Enterprise should enhance the reliability assessment process by incorporating energy adequacy metrics and evaluating scenarios that pose the greatest risk in NERC reliability assessments: this includes expanding the use of probabilistic approaches to assess resource adequacy with energy-limited or uncertain resources.</td></tr>
<tr><td>The ERO Enterprise should develop updated data and modeling capabilities and requirements to ensure valid and accurate results given resource and grid transformation (ongoing effort). Efforts initiated by the SPIDERWG to support collection of aggregated DER data for planning studies and the development of guidance for reliability studies that account for increasing amounts of DERs should be continued.</td></tr>
<tr><td>Industry should identify, design, and commit flexible resources needed to meet increasing ramping and variability requirements through improved recognition of the capabilities of these types of resources. Presently, concerns associated with ramping are confined to certain parts of North America; however, as variable generation increases system planners will need to ensure that sufficient flexible resources are available. The ERO Enterprise should continue to evaluate flexible resource needs in future long-term reliability assessments.</td></tr>
</table>

Table A.1: 2020 State of Reliability Recommendations	
Increasing Complexity in Protection and Control Systems	The ERO should work with industry experts to promote the development of industry guidelines on protection and control system management to improve performance.
	As more inverter-based generation is added to the BPS, the ERO should work with stakeholders to determine if there is an increasing reliability risk due to the different short-circuit contribution characteristics of inverter-based resources.
Human Performance and Skilled Workforce	Industry must focus on human and organizational performance improvement. The ERO Enterprise, the NATF, and the North American Generation Forum (NAGF) need to continue assisting industry through training and education events and workshops that increase knowledge and provide information to help industry modify and strengthen procedural and organizational structures to more effectively mitigate risk scenarios related to transmission and generation outages.
Loss of Situation Awareness	Electric utilities should develop and implement the system recovery and restoration plans, including scenarios in which the EMS and its decision-support tools are unavailable. These plans should also include drills and training on the procedures plus real-life practice implementing the procedures.
	Electric utilities should use offline tools (studies) in addition to the real-time analysis tools in EMSs to analyze contingencies plus other contingency-analysis, including day-ahead studies and seasonal and standing operating guides. This will provide a backup when the primary real-time analysis tools fail.
	Electric utilities should have backup tools and functionality ready and test them periodically. Backup tools and functionality include backup EMS systems, backup control centers, and other additional redundancy. The testing and use of these tools should be documented in emergency plans. System operators should be aware of these procedures and trained in using backup tools.
	Working with the ERO, electric utilities should develop and implement communication and response processes between RCs, BAs, and TOPs to improve overlapping coverage of situational awareness. The RCs, BAs, and TOPs should coordinate actions with their facilities to maintain the reliability of the BES.

Bulk Electric System Impact of Extreme Event Days	Hardening of critical systems to reduce the impacts of weather should remain a key consideration for entities owning transmission assets.
	Implementing the recommendations outlined in the NERC *Fuel Assurance and Fuel-Related Reliability Risk Analysis for the Bulk Power System* reliability guideline recently published should remain a key consideration.
	Planning for extreme conditions remains an important tool to promote understanding of the impact of scenarios on system behavior. The efforts of the planning and modeling groups at NERC are improving models and methods utilized to assess future performance. The ERO, the REs, and stakeholders should continue to work together to identify extreme scenarios to be studied and prioritize those study efforts going forward.
Physical Security and Cyber Security	The industry should continue to drive improvements in its security posture through technological hardening, growing a culture of security, and effective information exchange between entities, the E-ISAC, and trusted partner organizations.
	The E-ISAC should update its long-term strategic plan to incorporate developments over the last two years and continue aggressive and detailed execution of the plan—guided by the ESCC's Member Executive Committee.
	Industry and the E-ISAC should prepare to take advantage of public-private partnership opportunities coming from the National Infrastructure Advisory Council's *2019 Transforming the U.S. Cyber Threat Partnership* report and the *2020 Cyberspace Solarium Commission* report.
	CRISP capabilities and participation should be expanded, and the CRISP model should be leveraged to incorporate new data sources for analysis coordinated with the ESCC and the DOE.

Appendix B: Contributions

NERC would like to express its appreciation to the many people who provided technical support and identified areas for improvement as well as all the people across the industry who work tirelessly to keep the lights on each and every day.

NERC Industry Group Acknowledgements	
Group	**Officers**
Planning Committee	Chair: Brian Evans-Mongeon, Utility Services, Inc. Vice Chair: Joseph Sowell, Georgia Transmission Co.
Operating Committee	Chair: David Zwergel, MISO Vice Chair: Doug Hils, Duke Energy
Critical Infrastructure Protection Committee	Chair: Marc Child, Great River Energy Vice Chair: David Revill, GTC and David Grubbs, City of Garland
Performance Analysis Subcommittee	Chair: Maggie Peacock, SERC Vice Chair: Brantley Tillis, Duke Energy
Events Analysis Subcommittee	Chair: Vinit Gupta, ITC Vice Chair: Ralph Rufrano, NPCC
Generation Availability Data System Working Group	Chair: Leeth DePriest, Southern Company Vice Chair: Steve Wenke, Avista Corporation
Misoperations Information Data Analysis System Working Group	Chair: Brian Kasmarzik Vice Chair: Thomas Teafatiller, Reliability First
Transmission Availability Data System Working Group	Chair: Dan King, Ameren Vice Chair: John Idzior, Reliability First
Resources Subcommittee	Chair: Sandip Sharma, ERCOT Vice Chair: Greg Park, NWPP
Operating Reliability Subcommittee	Chair: Chris Pilong, PJM Vice Chair: Jimmy Hartmann, ERCOT
Frequency Working Group	Chair: Danielle Croop, PJM
Reliability Assessment Subcommittee	Chair: Lewis De La Rosa, Texas RE Vice Chair: Anna Lafoyiannis, IESO
System Protection and Control Subcommittee	Chair: Jeff Iler, AEP Vice Chair: Bill Crossland, RF

NERC Staff	
Name	**Title**
Mark Lauby	Senior Vice President and Chief Engineer
John Moura	Director, Reliability Assessment and Performance Analysis
Terry Campbell	Manager and Editor, Technical Publications
Alex Carlson	Senior Technical Publications Specialist
Tom Coleman	Director, Power Risk Issues and Strategic Management
Svetlana Ekisheva	Principal Data Science Advisor
Brad Gordon	Senior Engineer
Ara Johns	Senior Analyst
Kwame Jones	Senior Data Analyst
Matthew Lewis	Manager of Event Analysis
Kimberly Mielcarek	Senior Director, Communications
Darrell Moore	Director, Situation Awareness

NERC Staff	
Name	**Title**
Jack Norris	Engineer II
Mark Olson	Manager, Reliability Assessments
Margaret Pate	Program Liaison
Donna Pratt	Manager, Performance Analysis
Wei Qiu	Senior Engineer
Ryan Quint	Lead Engineer
Darrel Richardson	Principal Tech Advisor
Ed Ruck	Senior Engineer
Janet Sena	Senior Vice President, Policy and External Affairs
Sandy Shiflett	Senior Program Specialist
John Paul “JP” Skeath	Engineer II
Lee Thaubald	Technical Analyst