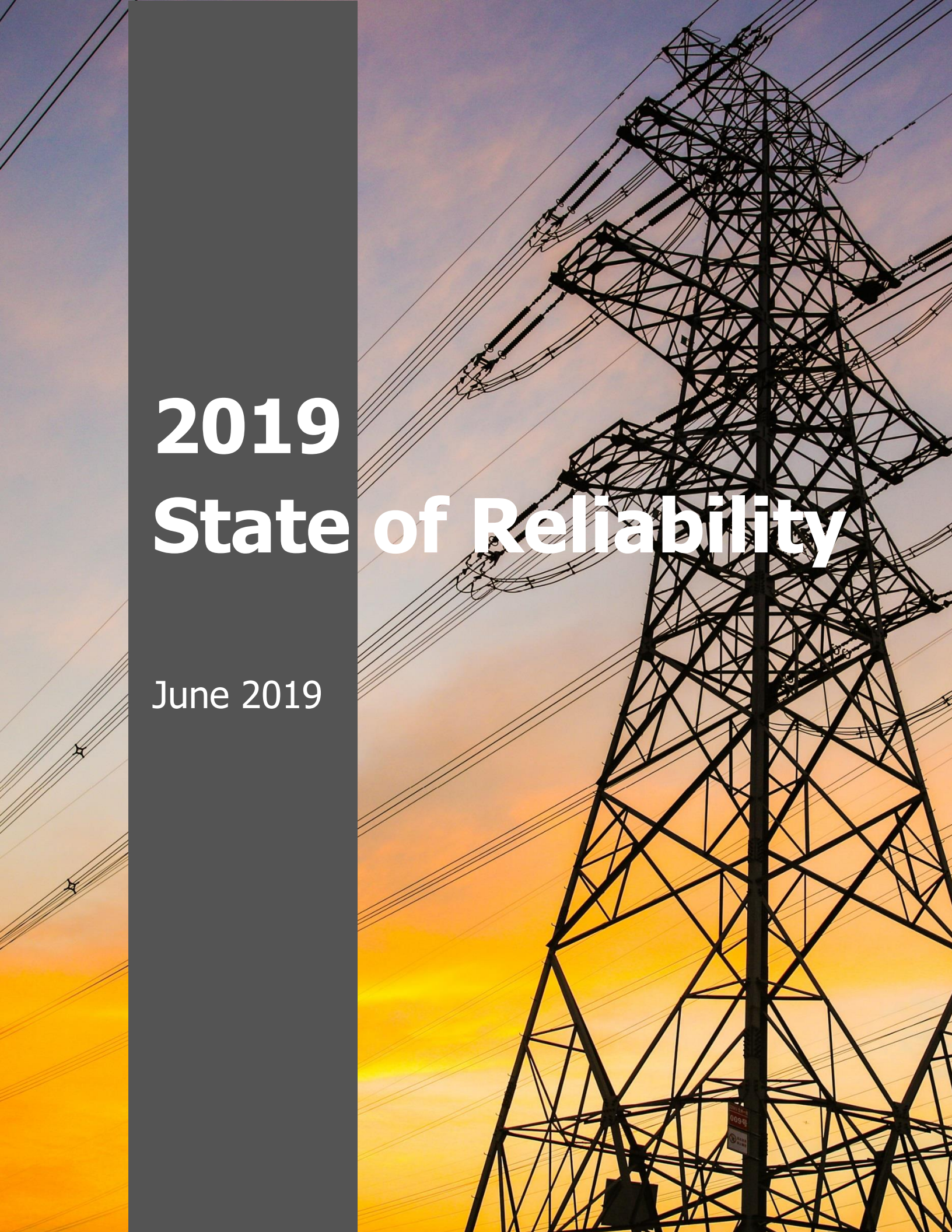


2019 State of Reliability

June 2019

Table of Contents

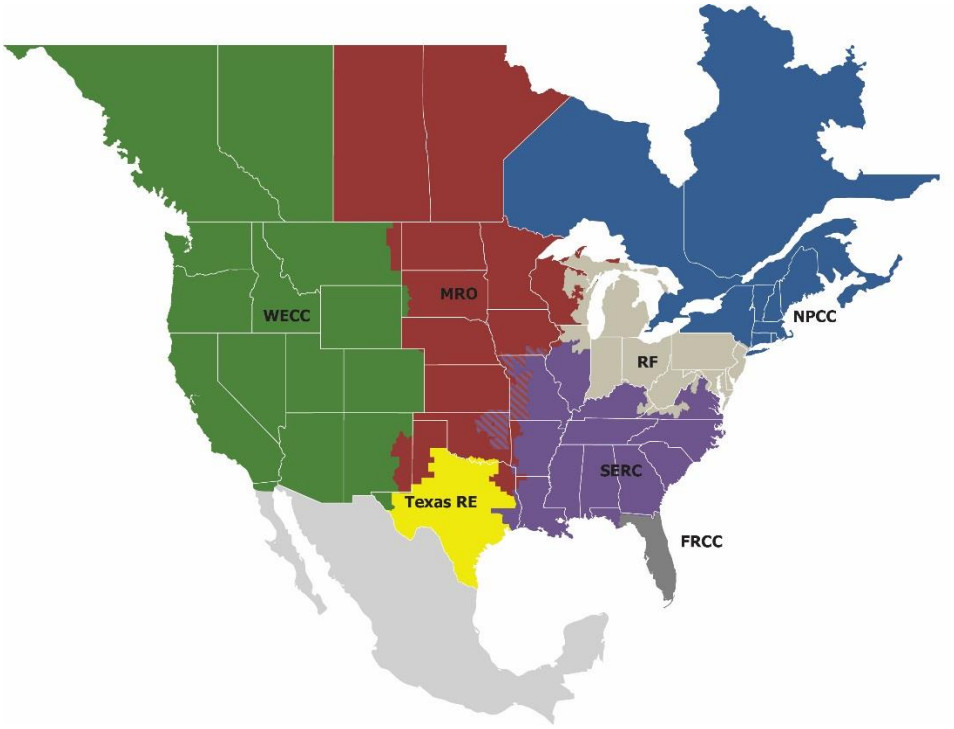
Preface iv
About This Report v
Objective v
Development Process v
Primary Data Sources v
Reading this Report vii
Executive Summary viii
Recommendations x
Chapter 1: The North American BPS—By the Numbers 1
Chapter 2: Event Analysis Review 3
Situation Awareness, Inputs, and Products 3
2018 Event Analysis Summary 4
Event Trends 6
Review of Major Events (Category 3, 4, and 5) 8
2018 Lessons Learned 9
NERC Alerts 11
Chapter 3: Reliability Indicators 12
Reliability Indicators and Trends 12
Energy Emergency Alerts 15
Planning Reserve Margin 16
Transmission-Related Events Resulting in Loss of Load 18
Automatic AC Transmission Outages 20
Automatic AC Transformer Outages 23
Element Unavailability 25
Weighted-Equivalent Generation Forced Outage Rate 28
Interconnection Frequency Response 30
Disturbance Control Standard Failures and Events Greater than MSSC 33
Protection System Misoperations 34
Interconnection Reliability Operating Limit Exceedances 36
Chapter 4: Severity Risk Index 40
2018 Severity Risk Index and Trends 42
Transmission Outage Severity 48
Chapter 5: Trends in Priority Reliability Issues 50
BPS Planning and Adapting to the Changing Resource Mix 50
Increasing Complexity in Protection and Control Systems 53
Human Performance and Skilled Workforce 57
Loss of Situation Awareness 61
Physical Security and Cyber Security 63
Resilience and Recovery from Extreme Natural Events 69
Appendix A: Contributions 73
Appendix B: Compilation of Recommendations 74

ERRATA, 1.1: June 25, 2019		
Page	**Section**	**Change**
Page 7	Event Trends, 2014–2018	Clarified 5-year average and annual load loss averages in Figure 2.6. Event counts revised to reflect corrections. Average load loss of was also revised downward from 167 MW to 116 MW.
Page 19	Transmission-Related Events Resulting in Loss of Load	"327 MW in 2014 to 166 MW" was revised to "316 MW in 2014 to 197 MW"

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the seven 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.

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



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

About This Report

Objective

The objective 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 reliability and security risks 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 (PAS). The *2019 State of Reliability* 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. The report is accepted by the Planning and Operating Committees and approved by the NERC Board of Trustees. The report is published annually, generally in June.

Primary Data Sources

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

Transmission Availability Data System (TADS)

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

Transmission
100kV and greater

Generation Availability Data System (GADS)

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

Conventional Generators
20 MW and larger

Misoperation Info Data Analysis System (MIDAS)

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

Transmission Owners,
Generator Owners,
Distribution Providers

The Event Analysis Management System (TEAMS)

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

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

Figure 1: NERC Reliability Performance and Event Information Systems

Reading this Report

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

Table 1: State of Reliability Major Parts	
The North American BPS: By the Numbers	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 of Trustees)

Additional Considerations

Additional considerations include the following:

- The data in this report represents the performance for the January–December 2018 operating year unless otherwise noted.
- Analysis in this report is based on 2014–2018 data and provides a basis to evaluate 2018 performance relative to performance over the last five years.
- This report is a review of industrywide trends, not of the performance of individual entities. Accordingly, information presented in this report is always aggregated 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, Quebec Interconnection is included in the Eastern Interconnection unless specific analysis for Quebec is shown.

Executive Summary

The *2019 State of Reliability* is NERC's independent assessment that focuses on BPS performance during 2018 as measured by a predetermined set of reliability indicators. This report, issued annually, 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 mitigations have led to positive improvements on the system.

The electricity sector is undergoing significant and rapid change, presenting new challenges and opportunities for reliability. With appropriate insight, careful planning, and continued support, the electricity sector will continue to navigate the associated challenges in a manner that maintains reliability. Year-over-year performance measures show generally positive trends in terms of generation, transmission, and protection and control performance. However, the evolving resource mix, along with persistent cyber and physical security threats, present critical challenges to BPS reliability that require the industry and the regulators to remain vigilant. As a key element of the ERO's mission, NERC remains focused on identifying emerging risks in order to maintain a proactive posture to ensure that the BPS remains highly reliable.

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

Key Finding 1

Extreme weather events continue to be leading contributors to transmission, generation, and load loss.

While extreme weather events continue to stress transmission, generation, and distribution systems, BPS reliability was maintained. Resilience to extreme weather was evidenced by adequate supply and strong transmission performance compared to the benchmark performance levels experienced during the 2014 polar vortex. There were two weather-related Category 3 events due to Hurricane Michael and Hurricane Florence. Transmission recovery during the extreme weather events in 2018 was evidenced by quick restoration times and statistically significant reductions in transmission outage severity. For more detailed information, refer to **Chapter 4: Severity Risk Index**.

Key Finding 2

There were no non-weather-related category 3, 4, or 5 events in 2018.

2018 was a year of high reliability with no non-weather related Category 3, 4, or 5 events and only one Energy Emergency Alert–Level 3 that led to firm load shedding (675 MW of load loss consisting of UFLS activation, manual firm load shedding action, and interruptible load curtailment actions in Nova Scotia on November 29, 2018, lasting just over seven hours due to extreme weather). Firm load was served 99.92% of time. This does not include inconsequential load loss or load loss due to distribution outages. For more detailed information, refer to **Chapter 2: Event Analysis Review**.

Key Finding 3

In Texas, there is still reliability risk in 2019 due to the projected capacity deficit, but better than expected performance from the generation fleet helped meet 2018 summer peak demand.

Texas continues to have insufficient resources to meet the Reference Margin Level, but still successfully met demand throughout the 2018 summer season. Despite having set a new system-wide peak demand record of 73,308 MW on July 19, 2018, higher than average peak availability from both wind and conventional generation (along with the use of demand response resources) helped serve peak demand and emergency operating procedures, such as firm load shedding, was not needed. For more detailed information, refer to **Chapter 3: Reliability Indicators**.

Key Finding 4

Despite continually evolving threats, no cyber or physical security incidents leading to unauthorized control actions or loss of load occurred in 2018.

In 2018, there were no reported cyber or physical security incidents that resulted in an unauthorized control action or loss of load. Nonetheless, grid security (particularly cyber security) is an area where NERC and industry must continually improve defenses as threats continue to rapidly evolve. While there were no NERC-reportable cyber security incidents during 2018, this does not mean that the risk of a cyber security incident is low, as the number of cyber security vulnerabilities are increasing. Both mandatory and voluntary reporting indicate that distribution-level events are more frequent than those affecting BES equipment. For more detailed information, refer to **Chapter 5: Trends in Priority Reliability Issues**.

Key Finding 5

Misoperations continue to be reduced.

Protection system misoperations exacerbate the severity of transmission outages. While the overall misoperations rate is slightly higher in 2018 than 2017 (8.0%, up from 7.4% in 2017), a statistically significant downward (positive) trend is shown over the past five-year period. The three largest causes of misoperations in 2018 were the same as in 2017: Incorrect Settings/Logic/Design Errors, Relay Failure/Malfunctions, and Communication Failures. For more detailed information, refer to **Chapter 3: Reliability Indicators**.

Key Finding 6

There were frequency response improvements 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 with statistical confidence in the arresting and/or settling periods. For more detailed information, refer to **Chapter 3: Reliability Indicators**.

Key Finding 7

As more inverter-based resources are added, solutions to emerging reliability challenges are being identified.

Inverter-based resources includes solar photovoltaic (PV), battery storage, and many forms of wind generation. A number of routine transmission line outages have led to the unplanned and wide-spread loss of significant amounts of predominately BPS-connected, inverter-based generation. In 2017, NERC established the Inverter-Based Resource Performance Task Force to study the issue and inform industry on the risks posed and options for mitigating them. In 2018, industry began implementation of the Inverter-Based Resource Performance Guideline. 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: Trends in Priority Reliability Issues**.

Recommendations

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

- 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
  - Resource adequacy with increasing energy constraints
- 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, and preparing for the next event) during the most extreme events and how system performance changes over time.
- 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.

In addition to these high-level recommendations, **Chapter 5: Trends in Priority Reliability Issues** includes more detailed and tactical recommendations for each of the six identified priorities issues:

- **BPS Planning and Adapting to the Changing Resource Mix**
- **Increasing Complexity in Protection and Control Systems**
- **Human Performance and Skilled Workforce**
- **Loss of Situation Awareness**
- **Physical Security and Cyber Security**
- **Resilience and Recovery from Extreme Natural Events**

Chapter 1: The North American BPS—By the Numbers

Figure 1.1 shows some numbers and facts about the North American BPS.

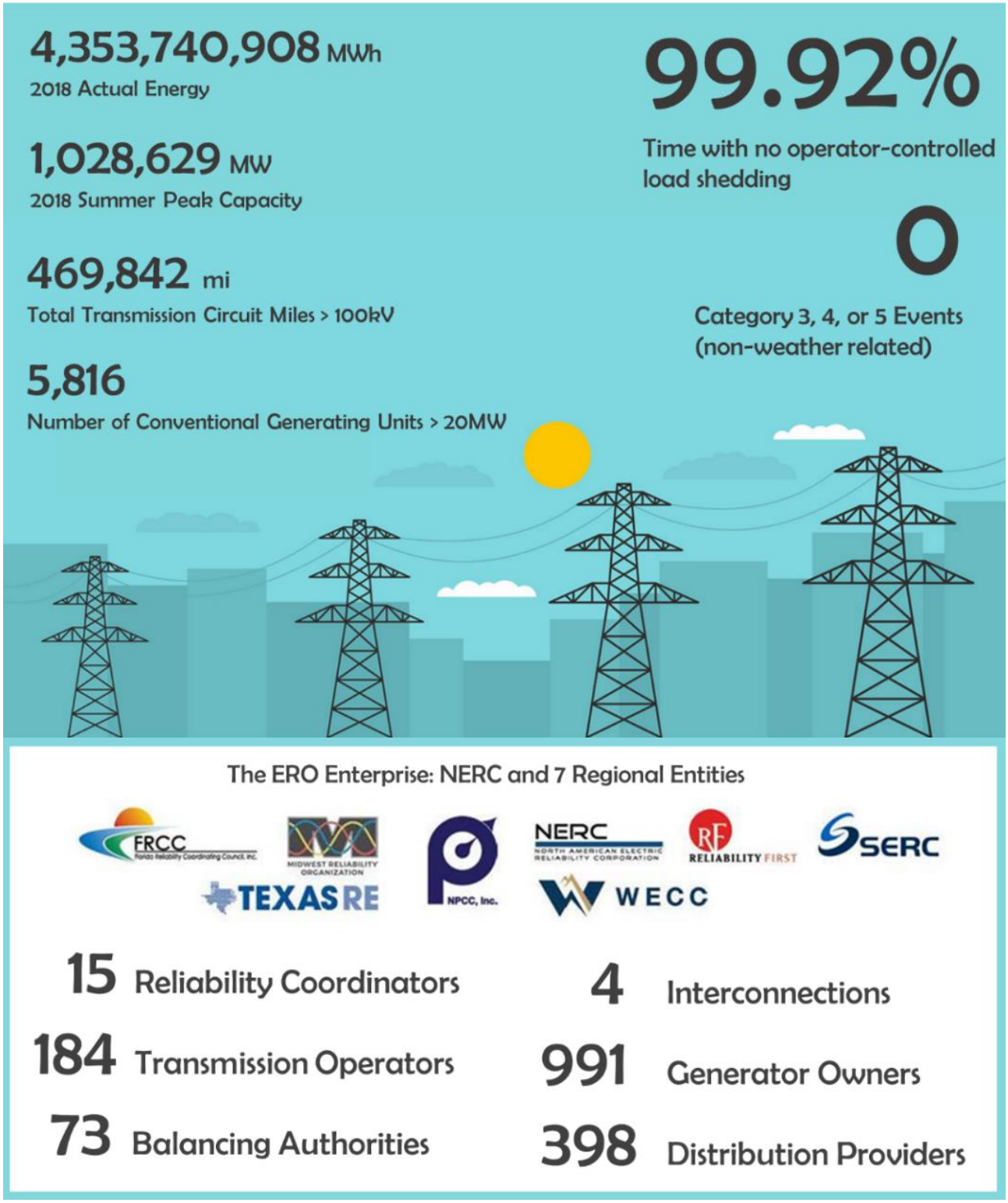


Figure 1.1: 2018 BPS Inventory and Performance Statistics, and Key Functional Organizations

How NERC Defines Bulk Power System Reliability

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

Adequacy: The ability of the electric system to supply the aggregate electric power and energy requirements of the 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%)
- For rotating blackouts, the term "rotating" is used because each set of distribution feeders is interrupted for a limited time, typically 20–30 minutes, and then those feeders are put back in service and another set is interrupted, and so on, rotating the outages among individual feeders

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 they spread over a wide area of the grid, they are referred to as "cascading blackouts," the 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 Bulk Electric System (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 collapse under normal operating conditions and/or voltage 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, and 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 these less probable severe events, 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. Less probable severe events would include, for example, 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.

Chapter 2: Event Analysis Review

The ERO's Event Analysis Process (EAP)[1] is used to conduct sequence and root cause analysis of disruption events occurring on the BPS (see **Figure 2.1**). The EAP begins with the ERO's Situational Awareness program to monitor real-time conditions and potential events on the BPS. Information is gathered for larger and more impactful events through the EAP. Review and analysis of this information helps identify potential reliability risks or emerging threats that can be addressed through a variety of solutions.

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 reoccurrence. Identification of the sequence of events answers the "what happened" question and determination of the root cause of an event answers the "why" question. It also allows for events to have cause codes or characteristics and attributes assigned that can then be used to identify trends. Trends may identify the need to take action, such as a NERC alert, or may initiate the need for the development of or revisions to Reliability Standards.

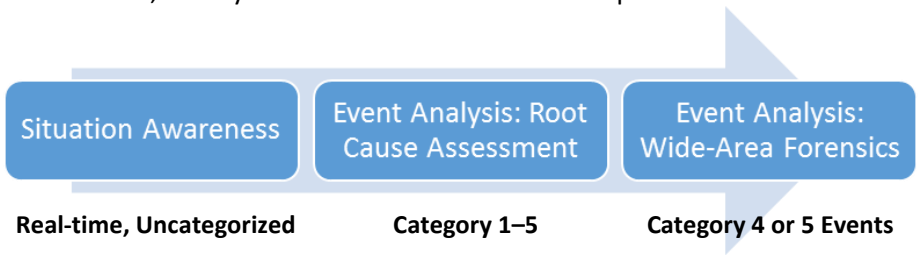


Figure 2.1: Event Analysis Process

Situation Awareness, Inputs, and Products

NERC Bulk Power System Awareness (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. See **Figure 2.2** for more information.

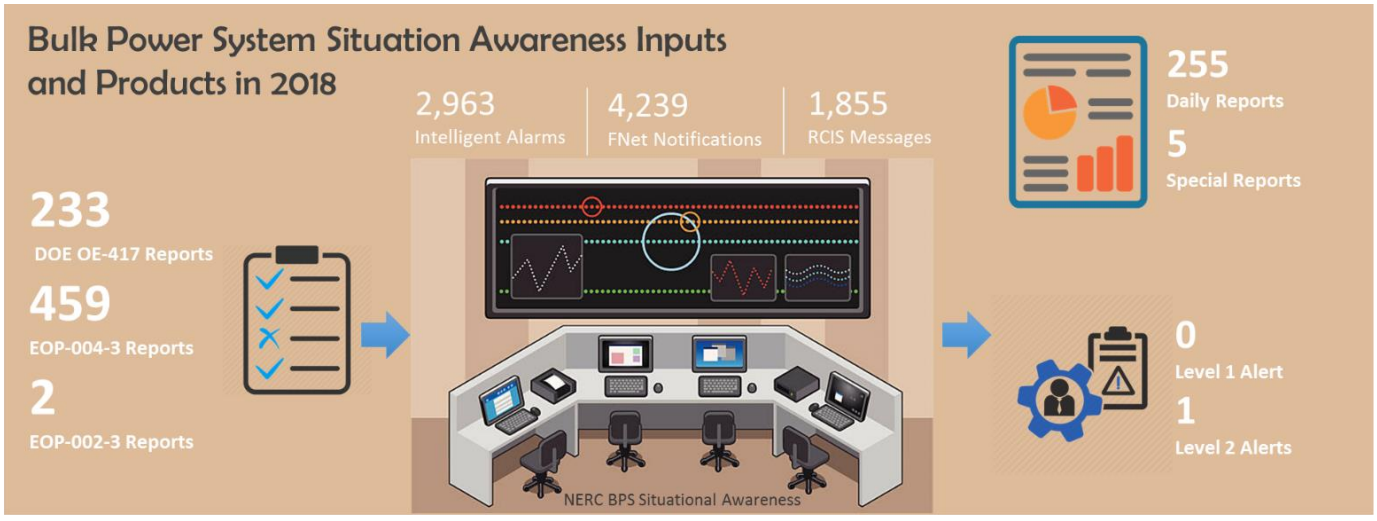


Figure 2.2: Bulk Power System Awareness by the Numbers

[1] EAP in effect as of January 1, 2017: http://www.nerc.com/pa/rrm/ea/ERO_EAP_Document/ERO_EAP_v3.1.pdf

2018 Event Analysis Summary

In 2018, industry reported 177 qualified events to the ERO Enterprise. The majority of the reports, 169 specifically, were Category 1 events. The top three most reported event categories in 2018 are Management and Organization, Design/Engineering, and Equipment/Materials. There were two weather-related Category 3 and no Category 4 or 5 events reported on the system for 2018. Hurricane Michael and Hurricane Florence occurred during 2018 and are Category 3 events based on the ERO EAP definitions. These weather-related events are being processed by FRCC and SERC to determine categorization, capture impacts, and identify high-level lessons learned and effective practices from the planning, preparation, and response to these storms. See **Figures 2.3–2.5** for a summary of events.

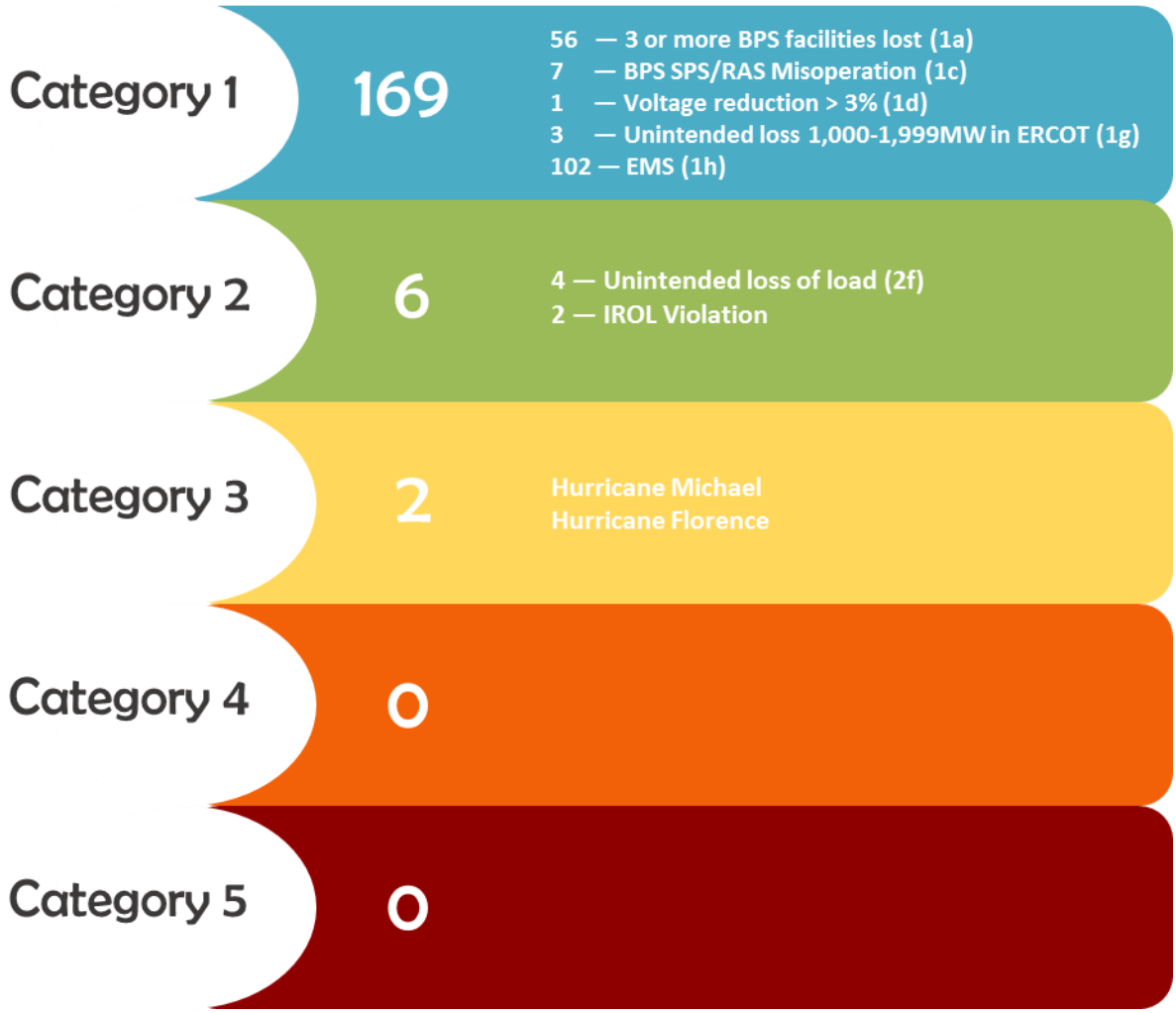


Figure 2.3: 2018 Qualified Events by Category

In addition to the categorized events listed above, significant generator outages during early January created an unusual operating condition in the South Central United States area. While not a categorized event, the operating condition led to the system being postured in a certain way that had the potential to cause an adverse reliability impact to the BPS. As a result, a joint NERC-FERC inquiry was conducted. At the time of publishing this report, the joint report has not yet been released.

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 TOP's 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 Tv

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

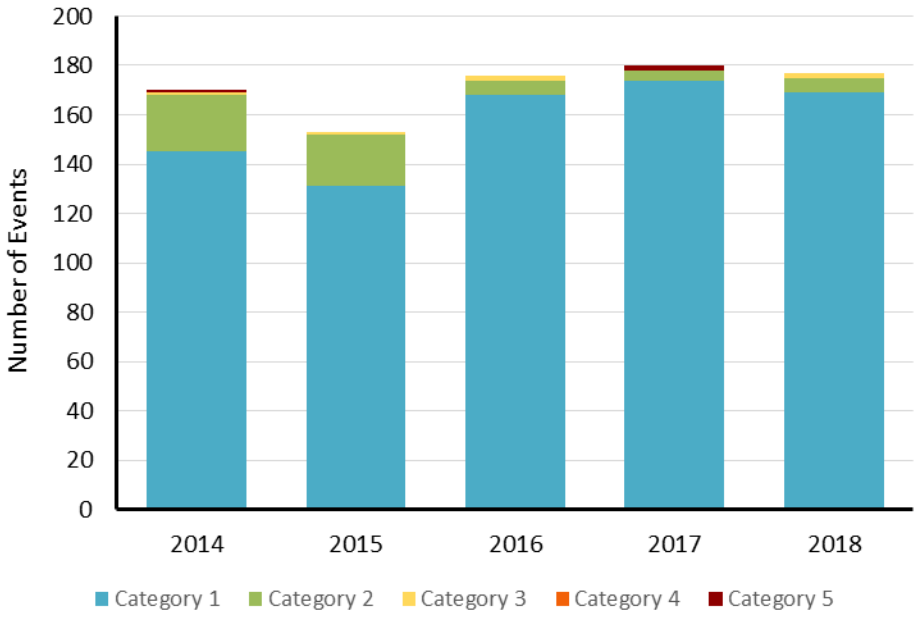


Figure 2.4: Number of Events per Category by Year

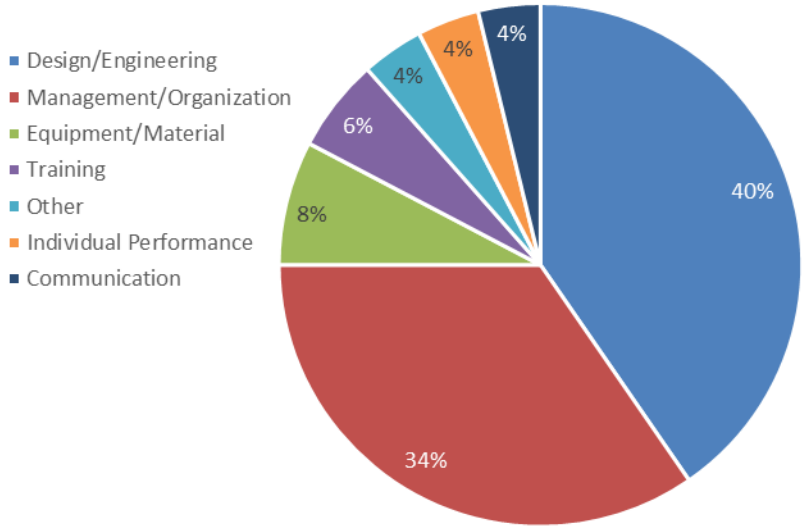


Figure 2.5: 2018 Identified Event Root Causes (processed to date)

Event Trends

There were 177 BPS events reported to NERC in 2018; this is comparable to the number of events reported per year in the preceding four-year period. In total, 856 events reports were submitted between 2014 and 2018. The largest portion of the cause coded events over the past five years was "Information to determine root cause less than adequate" (351). Of the 378 identified root causes, "Management/Organization" was identified as the leading root cause—146 events, or 39% of all identified root causes. "Design/Engineering" was second with 116 events, or 31%. See **Figure 2.6** for a summary of event trends.

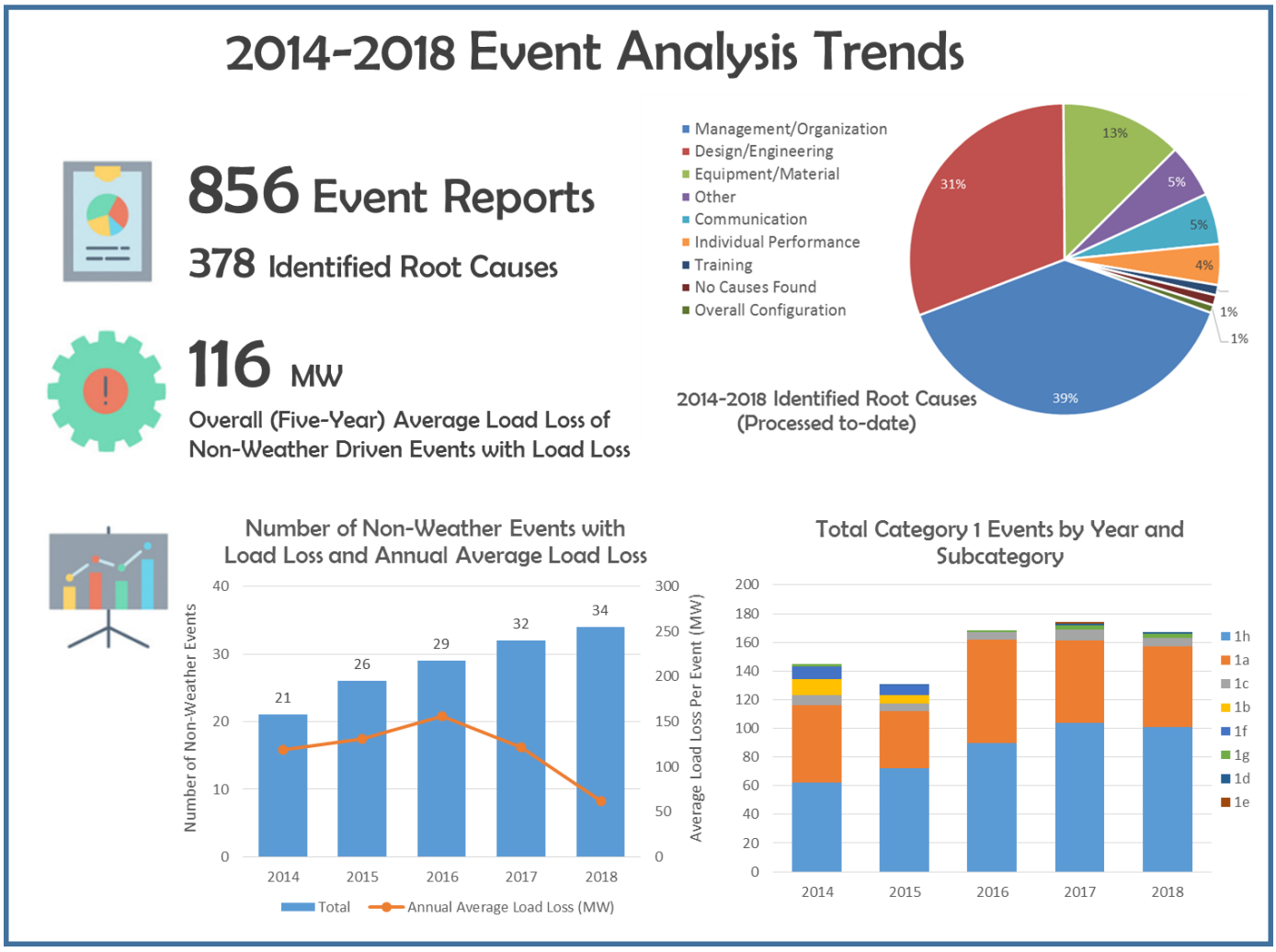


Figure 2.6: Summary of 2014–2018 Event Analysis Trends

The number of events with load loss has increased year-to-year as shown in **Figure 2.6**. The associated load loss averages by year remain effectively flat over the displayed periods. This demonstrates that, although there were more load lost events from year-to-year, the order of magnitude of loss remains relatively low and not statistically significant. Additionally, EAP reporting shows an increase in participating entities starting in 2015, potentially indicating an increase in the number of load loss events.

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. Additionally, the EAP saw a significant increase in participating entities from 2015 to 2016, indicating the maturation of the EAP as a potential contributor to the increase in event counts in general. This shift in future reporting resulted in a step-increase for the Category 1 total event count, which can be seen in **Figure 2.6**.

From a Regional perspective, RF had the largest group of events reported in 2018 with 41 events. FRCC, MRO, and SERC observed the largest total change of reported events from the previous year (see **Figure 2.7**).

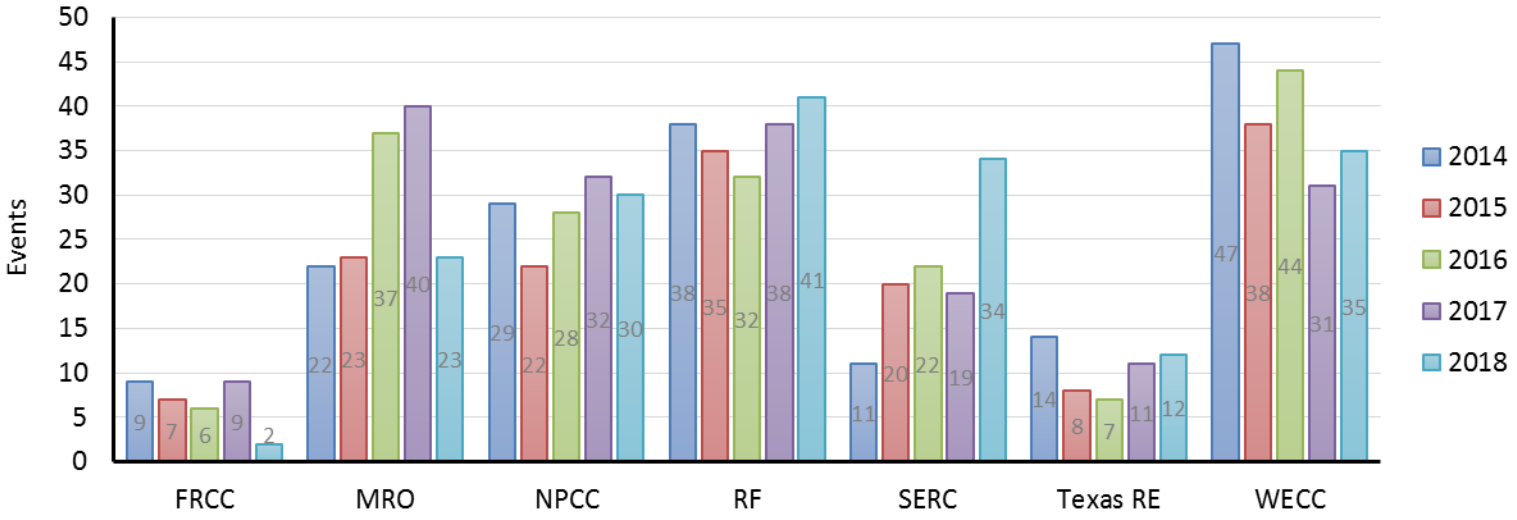


Figure 2.7: Total Events by Regional Entity (2014–2018)

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

While no Category 4 or 5 events were reported in 2018, Hurricane Florence and Hurricane Michael resulted in significant customer disruption and damage to the BPS, ultimately resulting in two Category 3 events.

Hurricane Florence made landfall as a NOAA-Category 1 storm on September 14, 2018, near Wrightsville Beach North Carolina (see **Figure 2.8**). The hurricane had 2,300 MW in forced outages/derates for the worst part of the storm as it tracked along portions of the North and South Carolina coasts. The total number of customer outages approached 1.4 million. As many as 50 BPS transmission assets sustained damage/outage, and flooding threatened several generation sites in the path of the storm. Generation capacity was sufficient for recovery, but damage and disruption to transmission assets posed a continued problem during the restoration period.

Hurricane Michael made landfall as a NOAA-Category 5 storm on October 10, 2018. Based on the event report, the hurricane had 575 MW in forced generation outages and wavered between 210 and 500 MW in restricted operation for one nuclear plant. The total number of customer outages was approximately 1.1 million, far exceeding the originally estimated 540,000 distribution customers. The storm's path was from Florida to Virginia, including Georgia and the Carolinas. The majority of the storm's damage to the electricity system was on the distribution side; however, the transmission system sustained outages to numerous 230 kV and 115 kV lines. Generation damage was limited mainly to renewable solar plants.

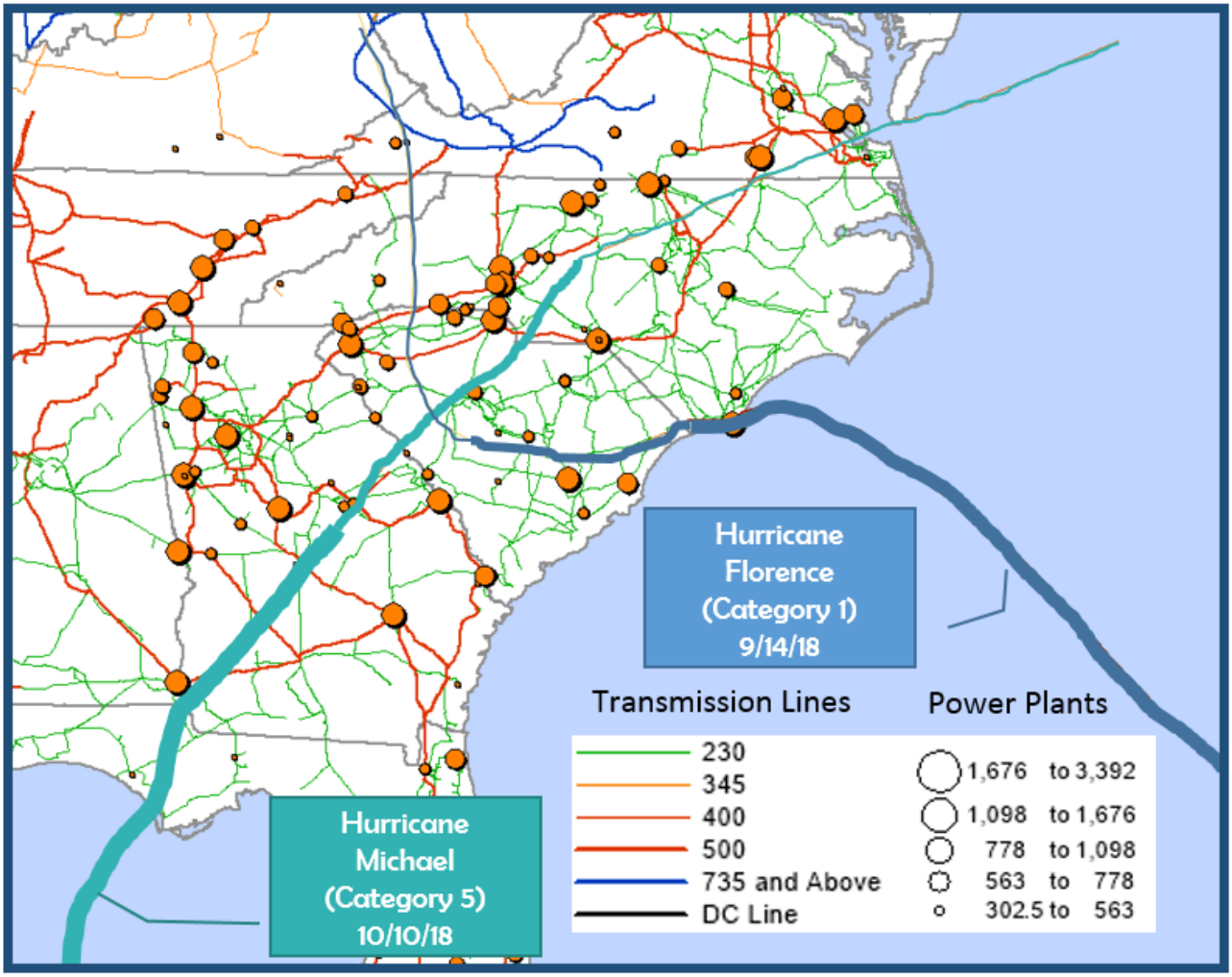


Figure 2.8: Path of 2018 Hurricane Michael and Hurricane Florence

2018 Lessons Learned

In support of the industry led EAP, one the ERO's primary objectives is to publish lessons learned. In 2018, a total of 15 lessons learned were published, up from 9 in 2017. The lifetime total for publication of lessons learned through 2018 is 149. Topics covered included operations, communications, transmission facilities, and relaying and protection systems. See **Table 2.1** for a list of lessons learned.

Table 2.1: Lessons Learned Published in 2018

LL #	Category	Title
LL20181203	Bulk-Power System Operations	Cascading Analysis Identifies Need for Pre-Contingent Load Shed[2]
LL20181202	Communications, Transmission Facilities	Avoiding IROL Exceedances with Rigorous Inspections during Commissioning, Consistent IROL Alarms, and Improved Training[3]
LL20181201	Relaying and Protection Systems	Initiatives to Address and Reduce Misoperations[4]

[2] Cascading Analysis Identifies Need for Pre-Contingent Load Shed
[3] Avoiding IROL Exceedances with Rigorous Inspections during Commissioning, Consistent IROL Alarms, and Improved Training
[4] Initiatives to Address and Reduce Misoperations

Table 2.1: Lessons Learned Published in 2018		
LL #	**Category**	**Title**
LL20181002	Transmission Facilities	Incorrect Field Modification and RAS Operation Lead to Partial System Collapse[5]
LL20181001	Communications	Networking Packet Broadcast Storms[6]
LL20180802	Transmission Facilities	Firewall Failure After Time Limit Exceeded[7]
LL20180801	Communications	Loss of Substation Data Circuits to SCADA[8]
LL20180702	Transmission Facilities	Preparing Circuit Breakers for Operation in Cold Weather[9]
LL20180701	Transmission Facilities	Risk of Internet Accessible Cyber Assets[10]
LL20180603	Communications	Back Office EMS Support Tools Impact Real-Time Situational Awareness[11]
LL20180602	Communications	External Model Data Causing State Estimator to Not Converge[12]
LL20180601	Transmission Facilities	Loss of Communication to Multiple SCADA RTUs at a Switching Center[13]
LL20180302	Transmission Facilities	Breaker Failure Due to Trip Coil Polarity[14]
LL20180301	Communications	State Estimator Outages Requiring Tuning/Calibrating EMS Settings[15]
LL20180101	Communications	Inadequate Battery Configuration Management Damaged a Generating Station and Tripped an HVDC Conversion Station[16]

[5] Incorrect Field Modification and RAS Operation Lead to Partial System Collapse
[6] Networking Packet Broadcast Storms
[7] Firewall Failure After Time Limit Exceeded
[8] Loss of Substation Data Circuits to SCADA
[9] Preparing Circuit Breakers for Operation in Cold Weather
[10] Risk of Internet Accessible Cyber Assets
[11] Back Office EMS Support Tools Impact Real-Time Situational Awareness
[12] External Model Data Causing State Estimator to Not Converge
[13] Loss of Communication to Multiple SCADA RTUs at a Switching Center
[14] Breaker Failure Due to Trip Coil Polarity
[15] State Estimator Outages Requiring Tuning/Calibrating EMS Settings
[16] Inadequate Battery Configuration Management Damaged a Generating Station and Tripped an HVDC Conversion Station

Event Analysis Principles

The information in this report is indicative of the analytical value of studying individual disturbances and events of various users, owners, and operators. These voluntary programs lead to the publication of lessons learned, technical alerts/recommendations, technical reports, and technical discourse between industry and the regulator that assist the bulk power industry as a whole. The following principals are core to the ERO's mission:

Promoting Reliability

The principal goal of the ERO is to promote the reliability of the BPS in North America. This goal is directly supported by evaluating qualifying BPS events, undertaking appropriate levels of analysis to determine the causes of the events, promptly assuring tracking of corrective actions to prevent recurrence, and providing lessons learned to the industry. The EAP also provides valuable input for training and education, reliability trend analysis efforts, and reliability standards development, all of which support continued reliability improvement.

Developing a Culture of Reliability Excellence

Through the EAP, the ERO strives to develop a culture of reliability excellence that promotes and rewards aggressive self-critical review and analysis of operations, planning, and critical infrastructure protection processes. This self-critical focus must be ongoing, and the industry must recognize that registered entities are linked together by their individual and collective performances. This focus is the root of understanding the underlying cause of events and avoiding similar or repeated events through the timely identification and correction of event causes and through the sharing of lessons learned.

Collaboration

Successful Event Analysis depends on a collaborative approach in which registered entities, REs, and NERC work together to achieve a common goal. The process requires clarity, certainty, and consistent adherence to reliability principles by BPS owners, operators, and users who perform a wide array of reliability functions.

Being a Learning Organization

As a learning organization, Event Analysis serves an integral function of providing insight and guidance by identifying and disseminating valuable information to owners, operators, and users of the BPS who enable improved and more reliable operation. As such, event analysis is one of the pillars of a strong ERO.

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 2018 concerning inverter performance.

NERC ALERT: Loss of Solar Resources during Transmission Disturbances due to Inverter Settings - II

As is well known from the past few years, inverter-based generating resources are becoming more prevalent. These resources are relatively new and provide new challenges to the inertia-dominated BPS. They require keen attention from the power system community in North America. In October 2017, a solar generation loss event in the WECC Region known as the Canyon 2 Wild Fire Event resulted in the publication of a disturbance report (Canyon 2 Fire Disturbance Report)[17] and a NERC alert.[18]

See the **BPS Planning and Adapting to the Changing Resource Mix** section for more analysis based on this alert.
Recommendations in the NERC alert included identification of the adverse characteristics of inverter-based performance during faults, the need for wide-area communication of the characteristics, and recommended actions concerning fault ride-through and restoration of current injection by all BPS inverter-based resources. The ongoing collaboration/discussion concerning inverters led to the Event Analysis Subcommittee of the NERC Operating Committee updating category definitions in the ERO EAP.

[17] https://www.nerc.com/pa/rrm/ea/Pages/October-9-2017-Canyon-2-Fire-Disturbance-Report.aspx
[18] https://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/NERC_Alert_Loss_of_Solar_Resources_during_Transmission_Disturbance-II_2018.pdf

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 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?
- Generation Performance and Availability: What are the energy limitations of the generation fleet?
- System Protection and Disturbance Performance: Can the system remain stable and withstand disturbances?

The reliability indicators presented in this report can precisely describe historical reliability performance; however, they cannot predict future reliability. 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:

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

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

Some of the reliability indicators require an extensive statistical analysis to determine whether statistically significant trends are being observed or whether numerical changes are unchanged within a band of confidence. Where statistically significant results are observed, NERC uses the following notation:

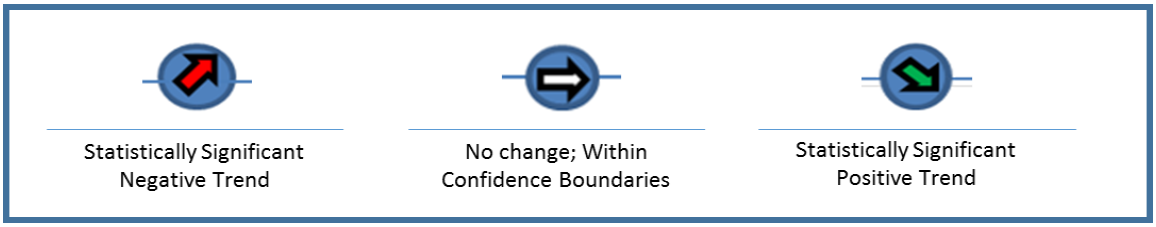


Table 3.1: Summary of Reliability Indicators			
Indicator Category	**Indicator Name**	**Brief Description**	**2018 Performance and Trend Results**
Resource Adequacy	BPS Planning and Adapting to the Changing Resource Mix	This metric counts the number of times EEA Level 3 Alerts are issued for BAs and when actual capacity and/or energy deficiencies occur.	Eastern Interconnection
			Western Interconnection
			Texas Interconnection
			Quebec Interconnection
	Planning Reserve Margin	This metric counts the number of areas reporting "marginal" or "inadequate" reserve margins for NERC's prior year Summer and Winter Reliability Assessment.	Texas RE-ERCOT Assessment Area
Transmission Performance and Availability	Transmission-Related Events Resulting in Loss of Load	This metric counts BPS transmission-related events resulting in the loss of load, excluding weather-related outages. Additional metrics measure the duration and magnitude of the load loss.	Transmission greater than 100kV
	Automatic AC Transmission Outages	This series of metrics measure the impacts of Failed Protection System, Human Error, Failed AC Substation Equipment, and Failed AC Element Equipment as factors in the performance of the transmission system.	Protection System
			Human Error
			AC Substation Equipment
			AC Circuit Equipment
	Automatic AC Transformer Outages	This series of metrics measure the impacts of Failed Protection System, Human Error, and Failed AC Substation Equipment as factors in the performance of the transformer fleet.	Protection System
			Human Error
			AC Substation Equipment
	Element Unavailability	This metric determines the percentage of BES ac transmission elements that are unavailable when outages due to automatic and nonautomatic events are considered. Planned outages are not included in the unavailability values.	AC Circuits
			Transformers

Table 3.1: Summary of Reliability Indicators			
Indicator Category	**Indicator Name**	**Brief Description**	**2018 Performance and Trend Results**
Generation Performance and Availability	**Weighted-Equivalent Generation Forced Outage Rate**	This metric measures the rated probability that a unit will not be available to deliver its full capacity at any given time due to forced outages and derates.	Conventional Generation greater than 20 MW
System Protection and Disturbance Performance	**Interconnection Frequency Response**	This metric determines 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.	Eastern Interconnection
			Western Interconnection
			Texas Interconnection
			Quebec Interconnection
	Disturbance Control Standard Failures and Events Greater than MSSC	This metric measures the ability of a balancing entity to balance resources and demand following reportable disturbances. The results help measure the risk the system is exposed to during extreme contingencies, how often they occur, and disturbance performance.	Disturbance Recovery Period
	Protection System Misoperations	This metric evaluates the performance of protection systems—both generator and transmission. The metric is the ratio of protection system misoperations to total system protection system operations.	BES Protection Systems
	Interconnection Reliability Operating Limit Exceedances	This metric measures the number and the duration an IROL is exceeded. An IROL is a system operating limit (SOL) that, if violated, could lead to instability, uncontrolled separation, or cascading outages.	Expanded Eastern Interconnection
			Western Interconnection
			Texas Interconnection

Energy Emergency Alerts

This metric counts the number of times Energy Emergency Alerts (EEA) Level 3 Alerts are issued for Balancing Authorities (BAs) and when actual capacity and/or energy deficiencies occur (see **Figures 3.1** and **3.2**).

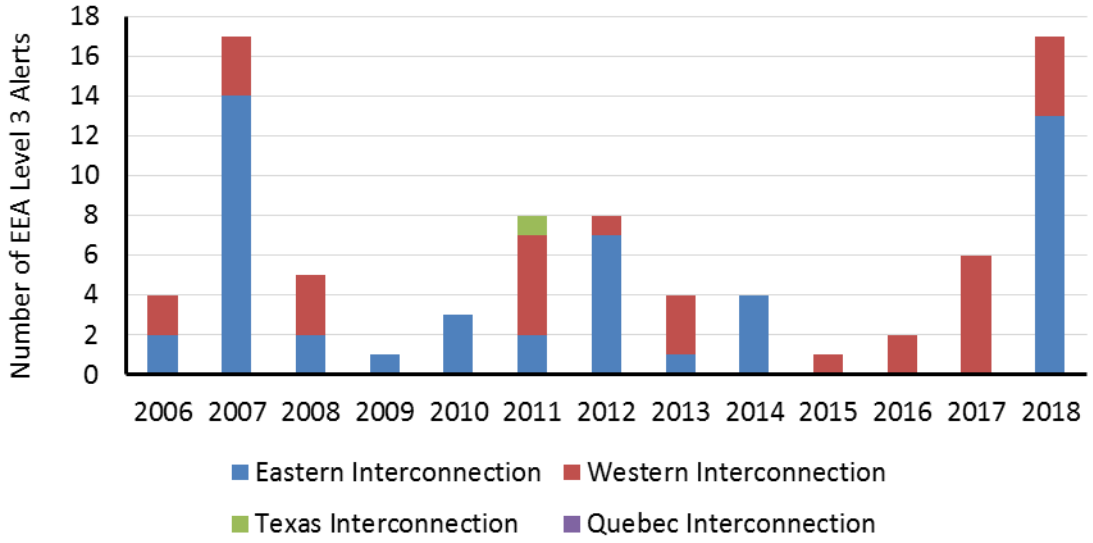


Figure 3.1: Number of EEA Level 3 Alerts by Interconnection, 2006–2018

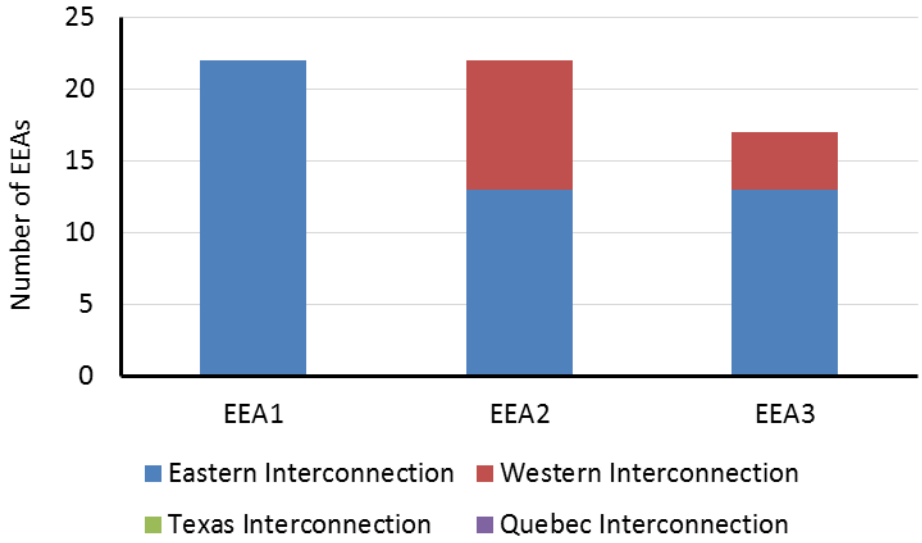


Figure 3.2: 2018 EEAs by Interconnection

2018 Performance and Trends

In 2018, 17 EEA Level 3 Alerts were declared, 11 more than the previous year. Some increase in EEA Level 3 Alerts can be attributed to the new EOP-011-1 that consolidated requirements from three standards: EOP-001-2.1b, EOP-002-3.1, and EOP-003-2. EOP-011-1 became effective April 4, 2017. For some Reliability Coordinators (RCs), the ability to access more resources from neighboring facilities now require an EEA to be initiated, which effectively has led to a lower activation threshold than what was in place historically. Therefore, more EEA Level 3 Alerts were expected.

The 17 EEA Level 3 Alerts declared lasted a total of 60.3 hours. The largest load loss associated with an EEA Level 3 was 675 MW and consisted of UFLS activation, manual firm load shedding action, and interruptible load curtailment

actions in Nova Scotia on November 11, 2018, over a seven-hour period. Of the 11 EEA Level 3 Alerts in the Eastern Interconnection, there were 9 in the SaskPower RC area, none of which led to firm load shedding. There have been no EEA Level 3 Alerts in the Quebec Interconnection, and only one in the Texas Interconnection in 2011.

Description
To ensure that all RCs clearly understand potential and actual energy emergencies in the Interconnection, NERC has established three levels of EEAs. 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.

Purpose
EEA trends may provide an indication of BPS capacity, energy, and transmission sufficiency. This metric may also provide benefits to the industry when considering correlations between EEA events and Planning Reserve Margins. When an EEA Level 3 alert is issued, firm-load interruptions are imminent or in progress. The issuance of an EEA Level 3 is due to a lack of available generation or when resources cannot be scheduled due to transmission constraints.

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?

Definition and Calculation
This metric counts the number of EEA Level 3 declarations.

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.

Source, Assumptions, and Limitations
NERC collects data from RCs when an EEA is declared.

- Metric Worksheet[19]
- NERC Reliability Standard EOP-011-1[20]

Planning Reserve Margin

This metric counts the number of areas reporting "marginal" or "inadequate" reserve margins for NERC's prior year Summer and Winter Reliability Assessment (see **Figure 3.3**).

Texas RE-ERCOT: Large Assessment Area
2018 Anticipated Reserve Margin: 10.53%
Amount Needed to Meet Reference Margin Level: 2,345 MW

[19] https://www.nerc.com/comm/PC/Performance%20Analysis%20Subcommittee%20PAS%202013/ALR6-2_clean.pdf
[20] https://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-011-1.pdf

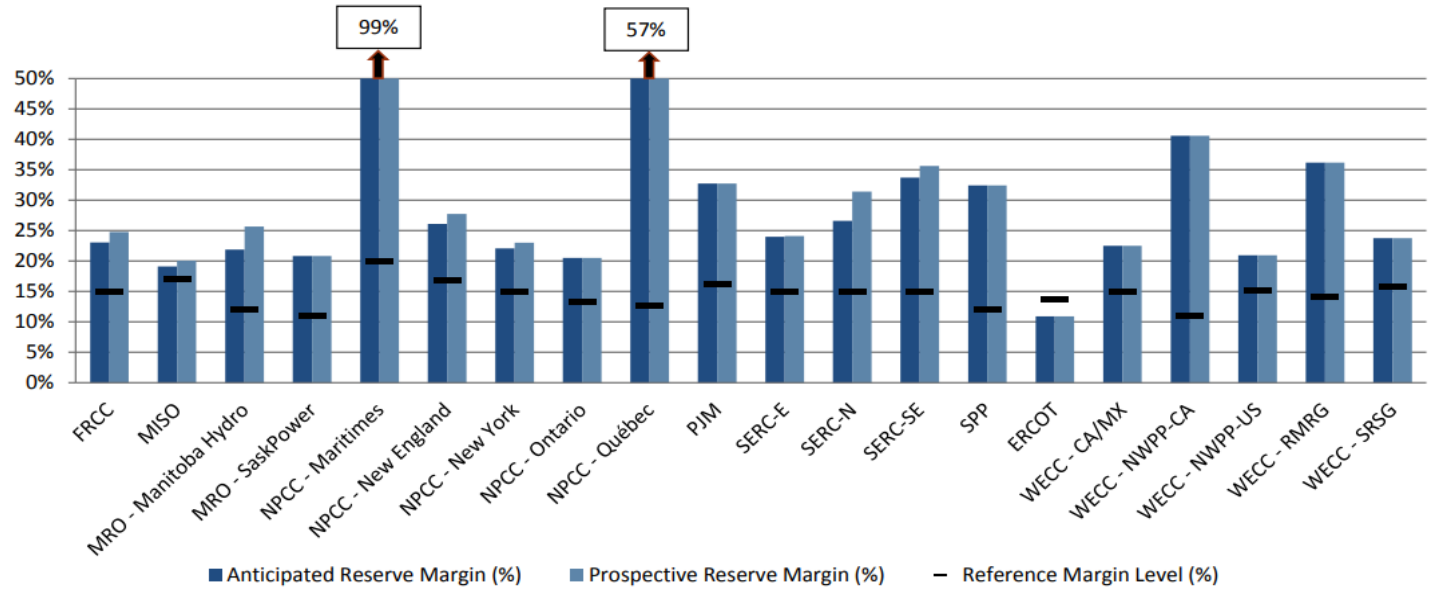


Figure 3.3: 2018 Summer Peak Planning Reserve Margins (Anticipated and Prospective Reserve Margins)

2018 Performance and Trends

In 2018, the Texas RE-ERCOT assessment area reported its reserve margin assessments to the ERO, and it was determined by the ERO's Reliability Assessment Process to be "Inadequate" for the 2018 summer peak.

Despite setting a new system-wide peak demand record of 73,308 MW on July 19, 2018, higher than average performance from wind generation contributed to high reliability performance and firm load shedding was not needed. This is more than 2,000 MW higher than the previous system-wide record set in August 2016.[21]

Description

This metric counts the number of areas reporting "adequate," "marginal," or "inadequate" Planning Reserve Margins for the 2018 summer and 2018/19 winter. NERC assesses resource adequacy by evaluating each assessment area's planning reserve margins relative to its Reference Margin Level. On the basis of the five-year projected reserves, NERC determines the risk associated 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.

Purpose

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.

[21] http://www.ercot.com/content/wcm/lists/144927/2018_Summer_Performance_One_Pager_FINAL.pdf

This Indicator Answers the Following Questions:

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

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 and Winter Reliability Assessments by class (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.
- **Green (good/improving)**: There are no marginal or inadequate assessments.

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 *2018 Summer Reliability Assessment*,[22] the *2018/2019 Winter Reliability Assessment*,[23] and the *2018 Long-Term Reliability Assessment*.[24]

Transmission-Related Events Resulting in Loss of Load

This metric counts BPS transmission-related events resulting in the loss of load, excluding weather-related outages. Additional metrics measure the duration and magnitude of the load loss (see **Figure 3.4**).

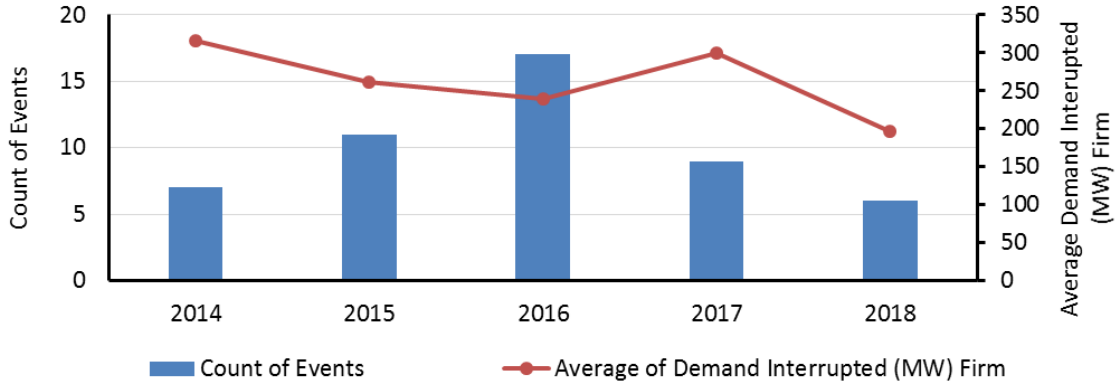


Figure 3.4: Transmission-Related Events Resulting in Loss of Load and Average Interrupted Demand, 2014—2018

[22] https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_SRA_05252018_Final.pdf

[23] https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_WRA_2018_2019_Draft.pdf

[24] https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_LTRA_2018_12202018.pdf

2018 Performance and Trends

In 2018, six events had transmission-related loss of load. This continues a mixed, but nonetheless improved, trend since 2014 in the number of events. A more notable trend is the reduced average demand interrupted during these events. The average has decreased just under 40% from 316MW in 2014 to 197MW in 2018.

Description

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

Purpose

To track transmission related events that resulted in firm load loss. This will allow 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 load loss?
- How much load loss occurred during these events?
- How reliable is the transmission system in serving firm load?

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 system demands. The reporting criteria for such events are as follows:[25]

- 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[26]
- 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), resulting in a firm load loss of 50 MW or more

Rating

- **Red (actionable)**: The count of events **and** MW load loss increased from year before **or** the count of events **or** MW 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 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 load loss for the year is less than the year before **and** below median value **or** count of events is zero

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

[26] https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf. This document defines SPS as a Special Protection Scheme and an RAS as a Remedial Action Scheme.

Source, Assumptions, and Limitations
NERC collects data from RCs when an EEA is declared.

- Reliability Standard EOP-004-3[27]
- NERC EAP
- Metric Worksheet[28]

Automatic AC Transmission Outages

This series of metrics measure the impacts of Failed Protection System, Human Error, Failed AC Substation Equipment, and Failed AC Element Equipment as factors in the performance of the transmission system (see **Figures 3.5–3.8**).

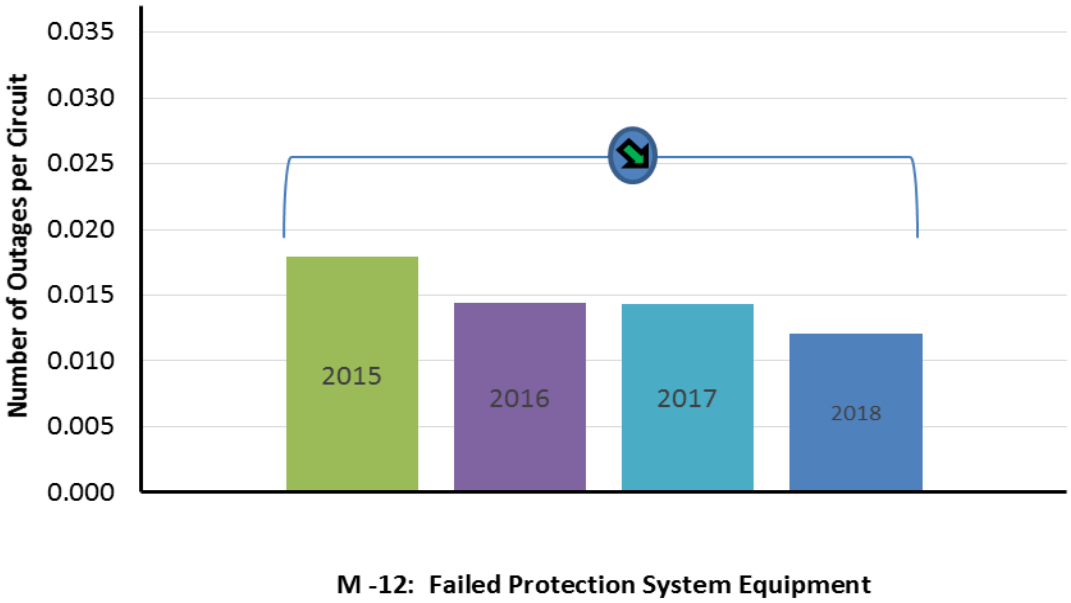


Figure 3.5: Number of Outages per Circuit due to Failed Protection System Equipment

[27] Reliability Standard EOP-004-3: https://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-004-3.pdf
[28] https://www.nerc.com/comm/PC/Performance%20Analysis%20Subcommittee%20PAS%202013/ALR1-4_Revised.pdf

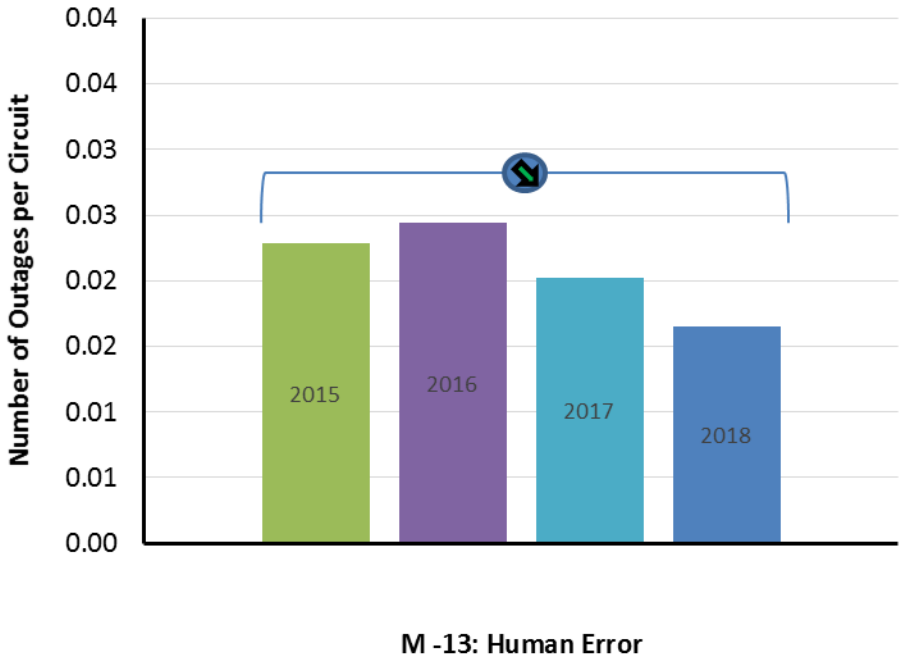


Figure 3.6: Number of Outages per Circuit due to Human Error

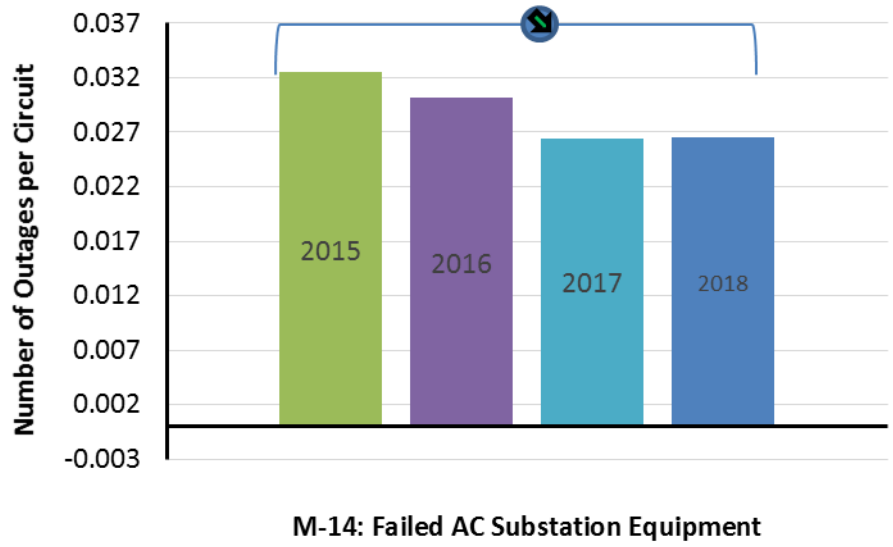


Figure 3.7: Number of Outages per Circuit due to Failed AC Substation Equipment

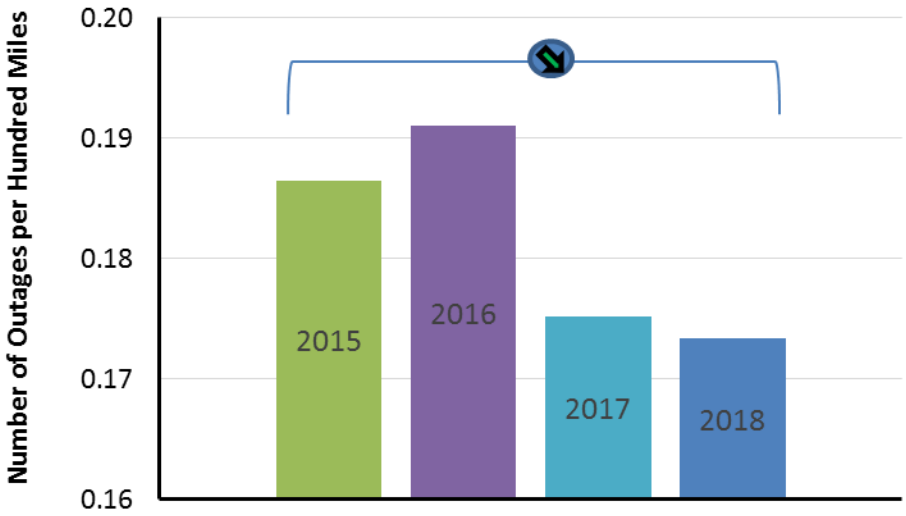


Figure 3.8: Number of Outages per Hundred Miles due to Failed AC Circuit Equipment

2018 Performance and Trends

In terms of availability, the performance of the transmission system in 2018 has improved over the last four years. Statistically significant reductions in Transmission Outages Due To Failed Protection System Equipment, Human Error, and Failed AC Substation Equipment were observed in 2018 leading to overall improvements in transmission availability.

Description

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.)

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 are the highest risk failure modes and what is their impact on transmission availability?
- How are active mitigation measures impacting transmission performance?
- What failure modes and associated transmission outages lead to the greatest reliability risk?

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.

Source, Assumptions, and Limitations

The Transmission Availability Data System (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

This series of metrics measure the impacts of Failed Protection System, Human Error, and Failed AC Substation Equipment as factors in the performance of the transformer fleet (see **Figures 3.9–3.11**).

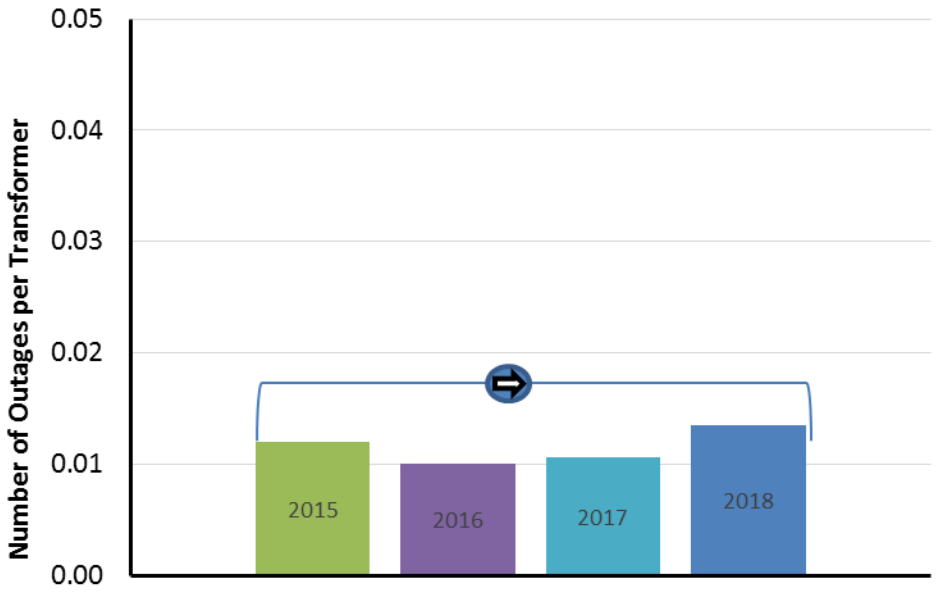


Figure 3.9: Number of Outages per Transformer Due to Failed Protection System Equipment

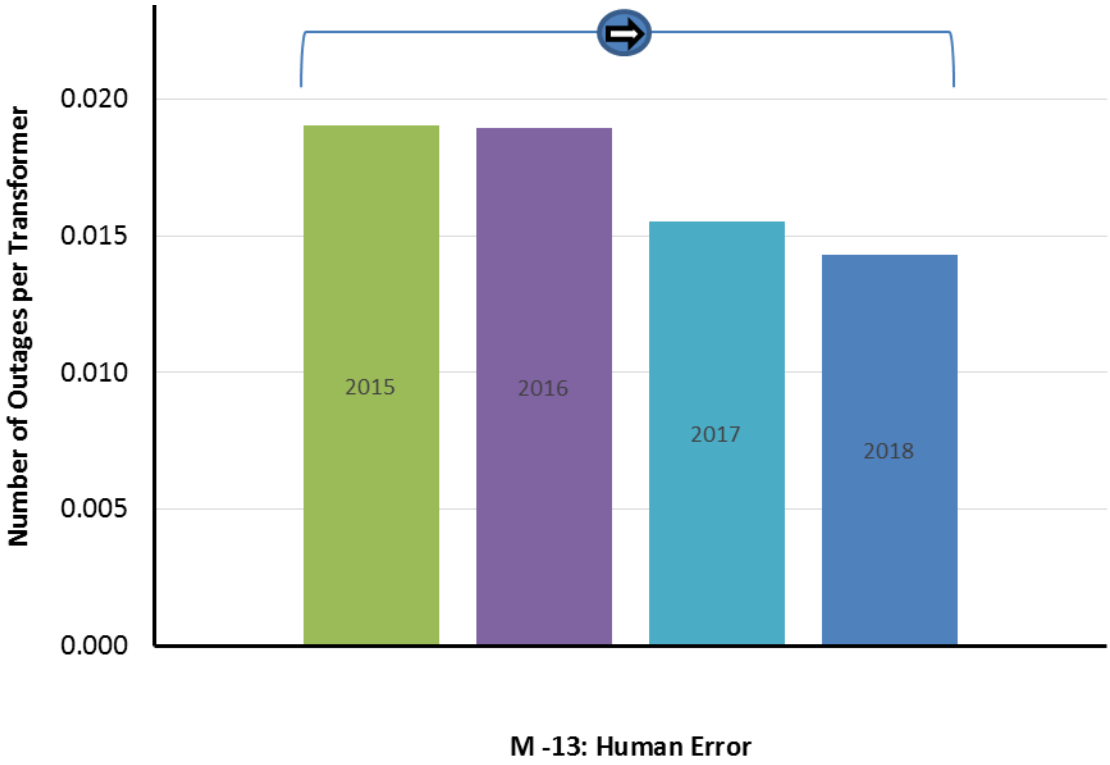


Figure 3.10: Number of Outages per Transformer due to Human Error

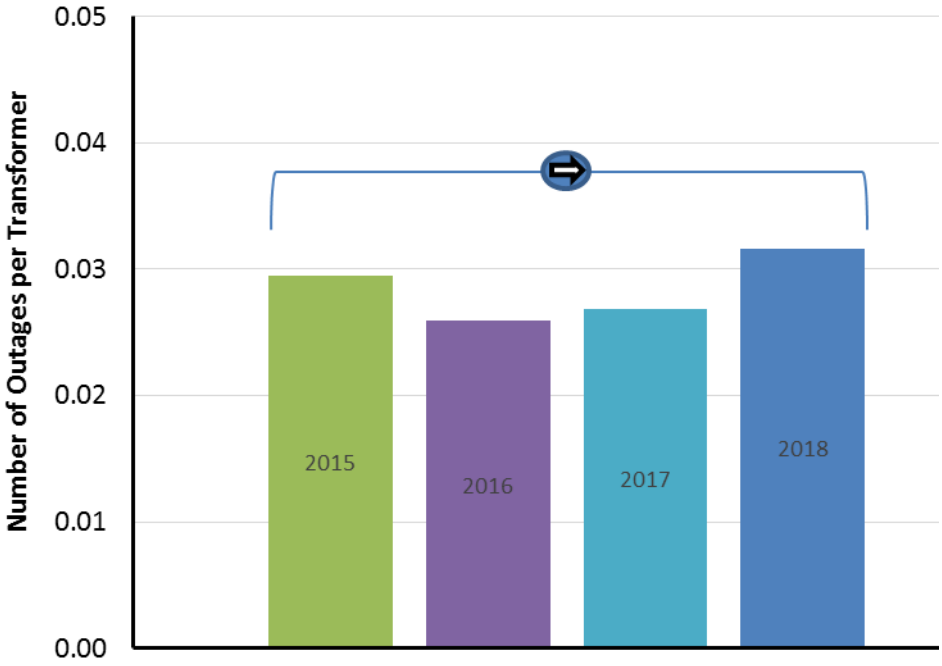


Figure 3.11: Number of Outages per Transformer due to Failed AC Substation Equipment

2018 Performance and Trends

From 2015 through 2018, the trend of automatic ac transformer outages caused by Failed Protection System Equipment, Human Error, and Failed AC Substation Equipment is stable and flat. A slight increase in the number of outages per transformer was observed in 2018 for outages caused by Failed Protection System Equipment and Failed AC Substation Equipment; however, these are within normal performance and not statistically significant.

Description
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.

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 Questions:

- What are the highest risk failure modes and what is their impact on transformer availability?
- How are active mitigation measures impacting transformer performance?
- What failure modes and associated transformer outages lead to the greatest reliability risk?

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.

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

Element Unavailability

This metric determines the percentage of BES ac transmission elements that are unavailable when outages due to automatic and nonautomatic events are considered. Planned outages are not included in the unavailability values (see **Figures 3.12** and **3.13**).

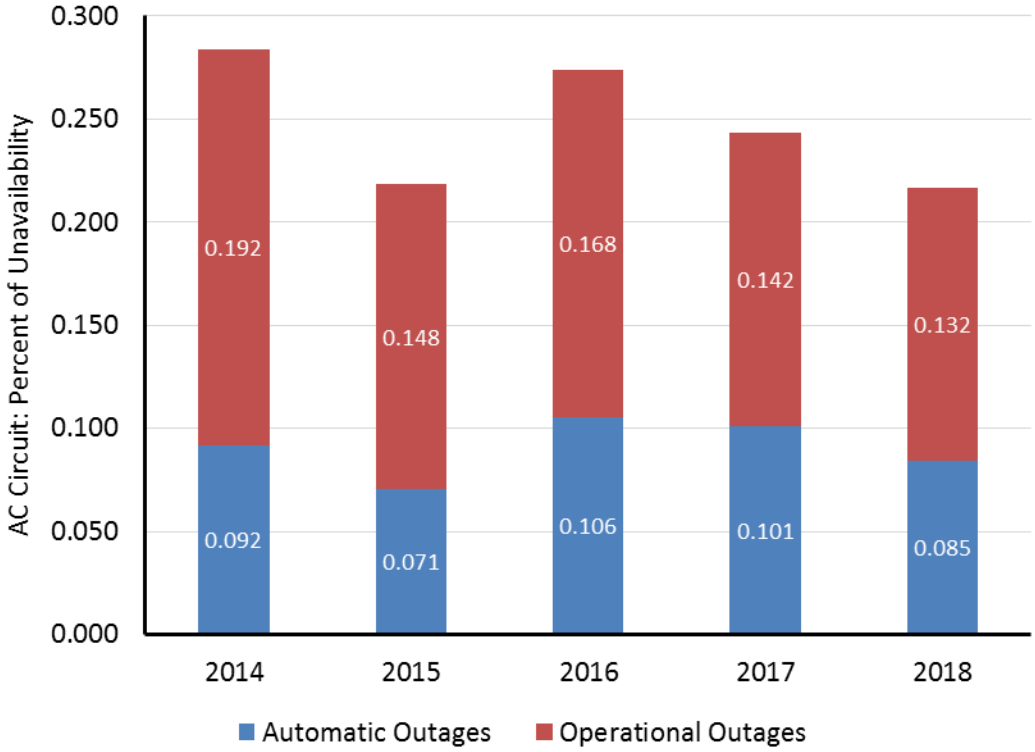


Figure 3.12: Transmission Unavailability

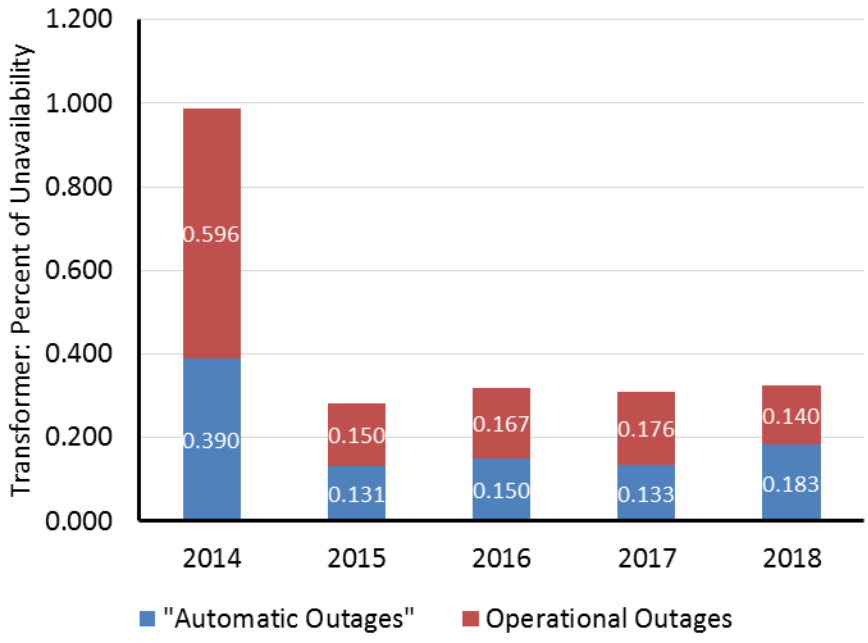


Figure 3.13: Transformer Unavailability

2018 Performance and Trends

In 2018, transmission over 200 kV across NERC had an unavailability rate of 0.22% (meaning, at any given time, there is a 0.22% chance that a transmission circuit is unavailable due to sustained automatic and operational outages). Transmission unavailability improved by 12% from the 2015–2017 average. Transformer unavailability, however, declined by 7% from the 2015–2017 average to 0.32%.

Description
This metric determines the percentage of BES ac transmission elements (transmission lines and transformers) that are unavailable when outages due to automatic and operational events are considered. Transmission and transformer outages can limit the performance of the transmission system and cause undesired consequences. More transmission outages can lead to poor transmission availability, and longer duration outages further strains transmission availability.

Purpose
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 Questions:

- How often are transmission lines and transformers unavailable?
- What is the probability of transmission line and transformer outages?
- How significant are transmission line and transformer outages to overall reliability?

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 nonautomatic outages. These outages are broken down into automatic (sustained) and nonautomatic (planned and 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.

Source, Assumptions, and Limitations
The NERC TADS provides the total number and duration of automatic and nonautomatic transmission system outages. Planned outages are not included in the unavailability values.

Weighted-Equivalent Generation Forced Outage Rate

This metric measures the rated probability that a unit will not be available to deliver its full capacity at any given time due to forced outages and derates (see **Figures 3.14** and **3.15**).

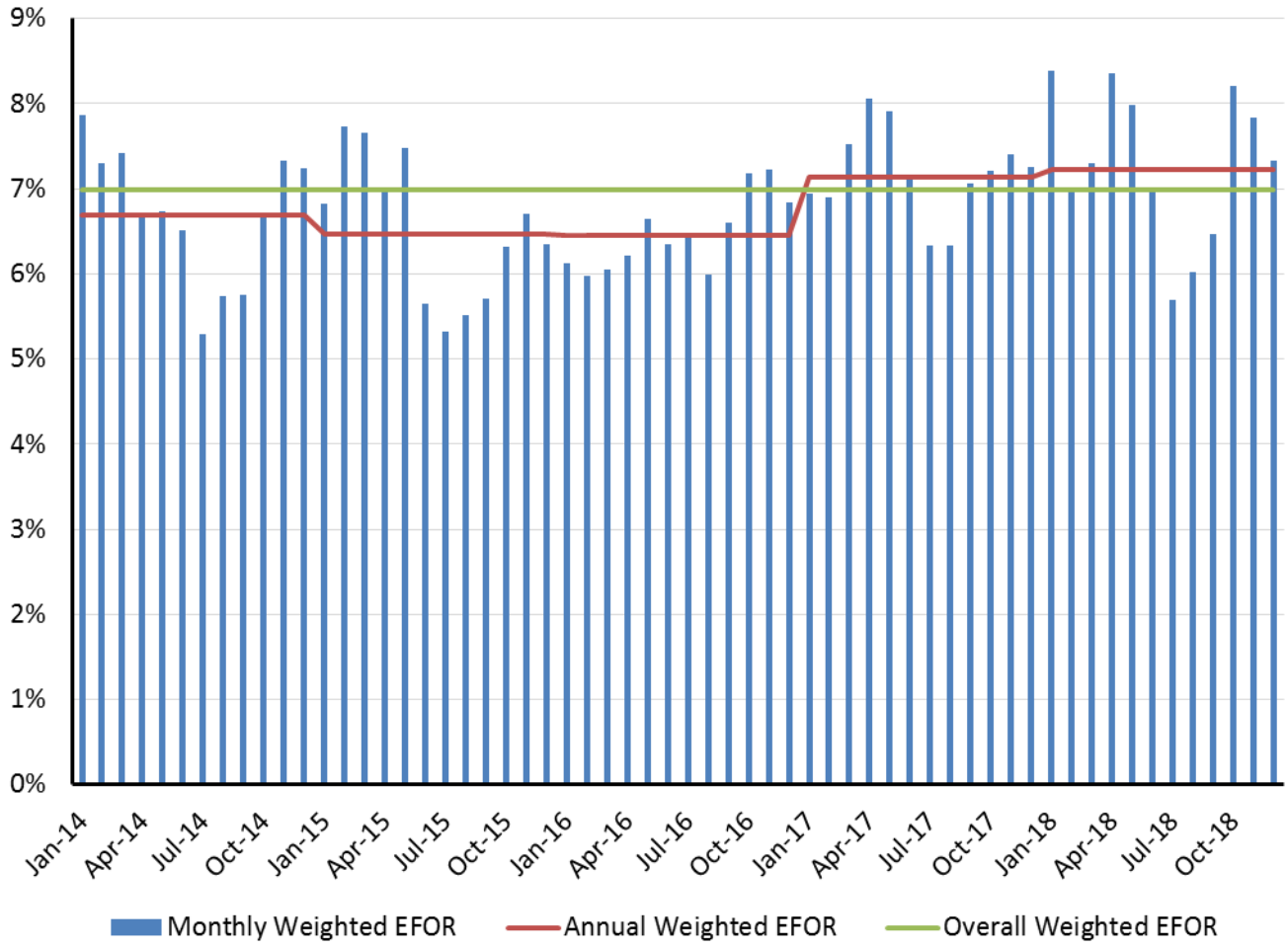


Figure 3.14: Monthly Capacity Weighted EFOR and Five-Year Rolling Average, 2014–2018

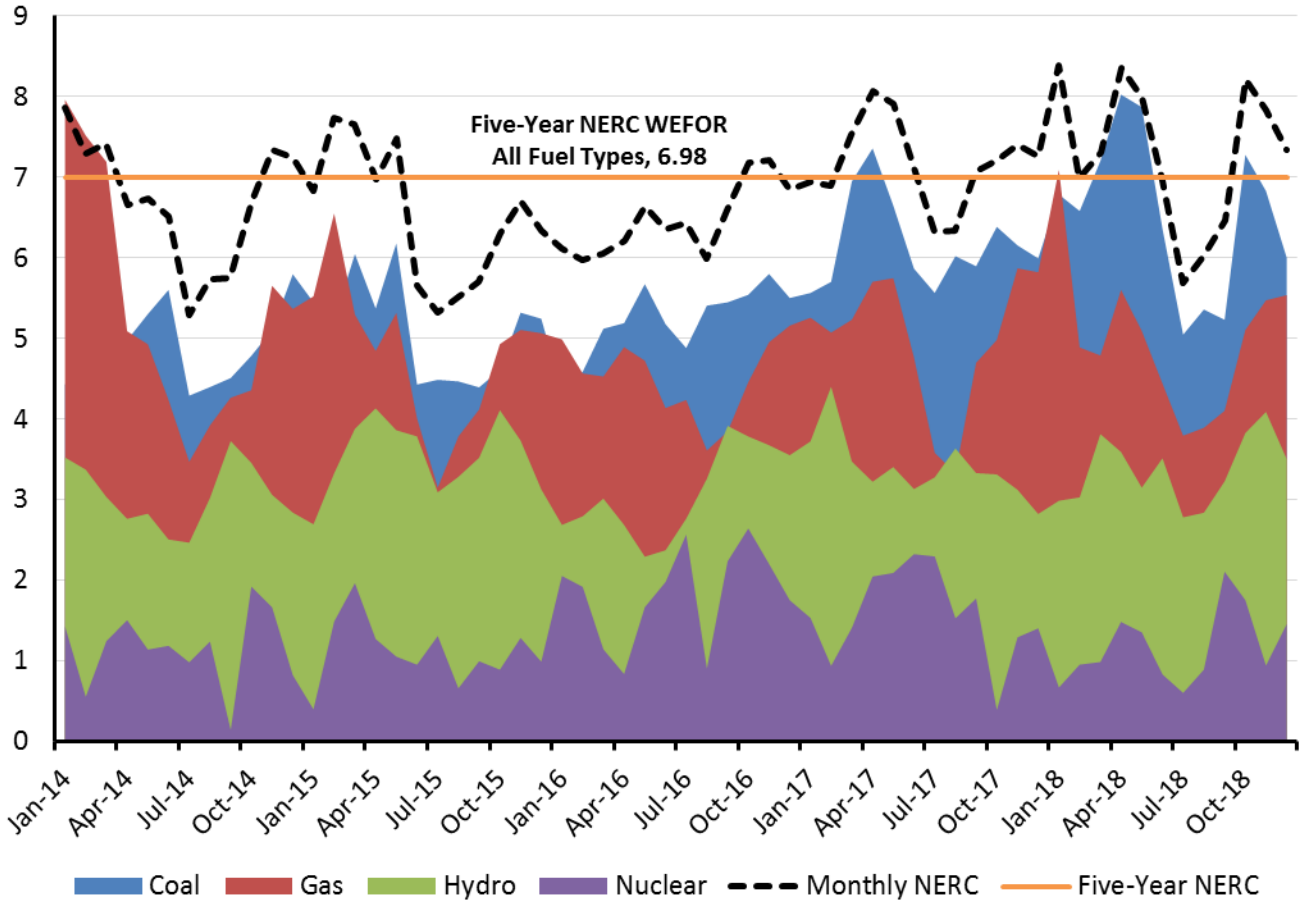


Figure 3.15: Overlaid Monthly Capacity Weighted EFOR by Fuel Type, 2014–2018

2018 Performance and Trends

The horizontal lines in **Figure 3.14** show the annual weighted equivalent forced outage rate (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% and only slightly lower than the 2018 annual WEFOR of 7.2%. The WEFOR has been fairly consistent and has a statistical distribution that is nearly an exact standard distribution. The 2018 annual WEFOR is above the five-year average for the second year in a row and has also increased since 2016.

Monthly WEFOR for select fuel types is shown in **Figure 3.15**. 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.

Description

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.

Purpose

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

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?

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 improvement and less than the five-year average **or** zero.

Source, Assumptions, and Limitations

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

Interconnection Frequency Response

This metric determines 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 (see **Table 3.1** and **Figure 3.16**).

Table 3.1: 2018 Frequency Response Performance Statistics and Trend Assessment

Interconnection	2018 OY Arresting Period Performance			2018 OY Stabilizing Period Performance		
	Mean UFLS Margin (Hz)	Lowest UFLS Margin (Hz)	2014–18 OY Trend	Mean $IFRM_{A-B}$ (MW/0.1 Hz)	Lowest $IFRM_{A-B}$ (MW/0.1 Hz)	2014–18 OY Trend
Eastern	0.458	0.404	Improving	2,411	1,141	Stable
Texas	0.594	0.498	Improving	940	562	Improving
Quebec	1.075	0.678	Improving	862	364	Improving
Western	0.405	0.246	Stable	1,789	890	Improving

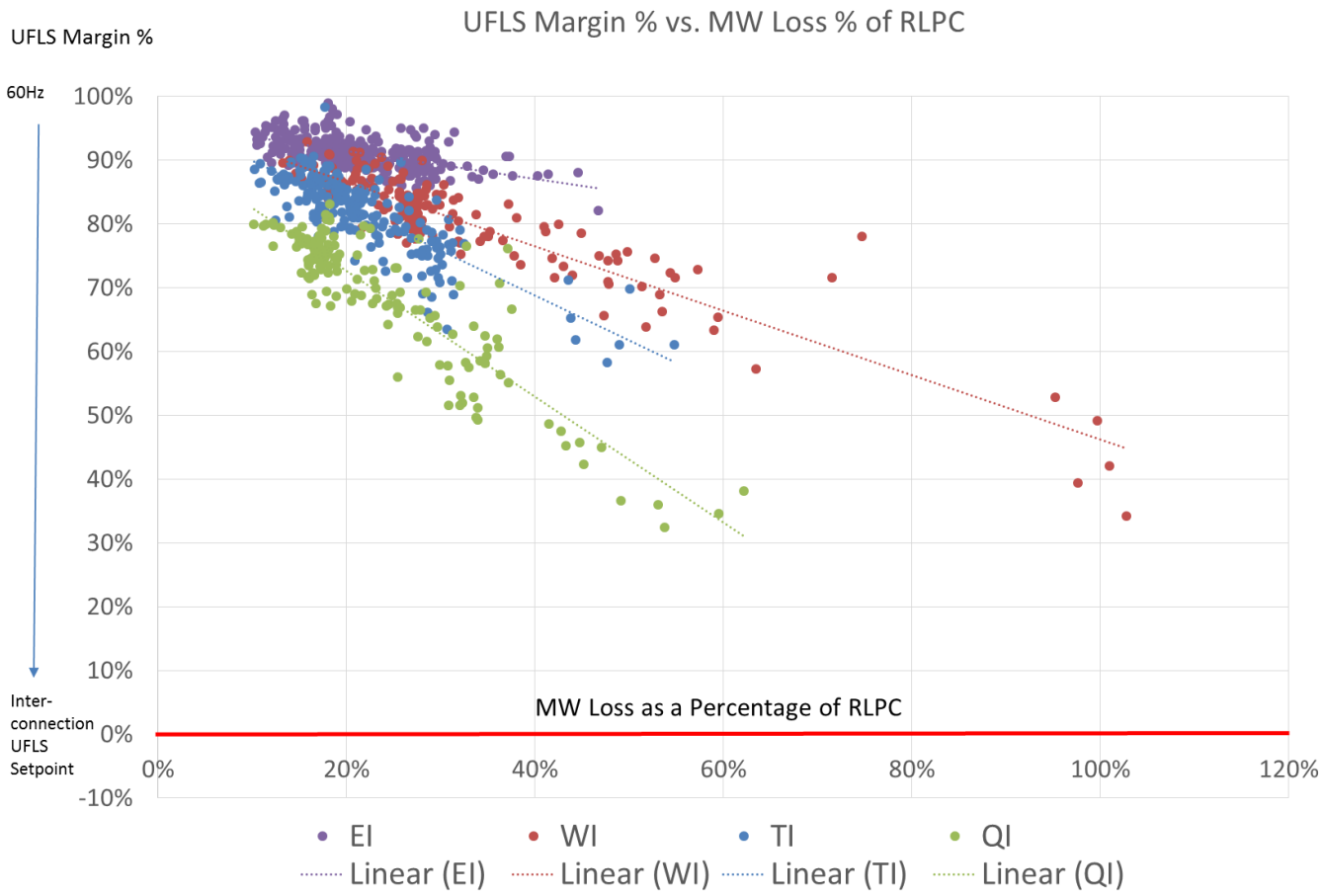


Figure 3.16: 2018 Qualified Frequency Disturbances and Remaining UFLS Margin

2018 Performance and Trends

Frequency response analysis for all of the Interconnections indicates acceptable and improving performance. The Eastern Interconnection (EI), the Texas Interconnection (TI), and the Quebec Interconnection (QI) showed statistically significant improvements in the arresting period from 2014 through 2018. The TI, QI, and WI exhibited statistically significant improvements during the stabilizing period from 2014 through 2018. In the 2018 operating year, the largest M-4 event occurred in the WI that was 2,741 MW (vs. an RLPC of 2,626 MW), resulting in a Point C of 59.746 Hz and UFLS margin of 0.246 Hz from a Value A starting frequency of 59.985 Hz. The event occurred in July 2018 during the HE 18:00 PDT.

During the arresting period, the goal is to arrest the frequency decline for credible contingencies before the onset of UFLS. The calculation for interconnection frequency response obligation (IFRO) under BAL-003 is based on arresting the Point C Nadir before the first step of UFLS, for contingencies at or above the resource loss protection criteria (RLPC) for the Interconnection. Measuring and tracking the margin between the first step UFLS setpoint and the Point C Nadir is an important indicator of risk for each Interconnection. **Figure 3.16** 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 setpoint 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 WI had three events at or near 100% of the RLPC and maintained sufficient UFLS margin. The largest events as measured by percentage of RLPC for the other Interconnections was between 50–60%. It is also interesting to note how the slope of the regression lines is representative of the relative strength (i.e., inertia) for the Interconnection.

Description

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 (Value A) to the time of the frequency nadir (Point C) 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.
- **Stabilizing period:** The time after the rebound period, once all primary frequency response is deployed and the system has entered a period of relative balance and the frequency is fairly stable. It is the average frequency occurring between 20 and 52 seconds after the start of resource loss event (Value B).

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?
- Are resource mix changes negatively impacting frequency response performance?
- How close has the system come to activating UFLS?

Definition and Calculation

This metric is based on methods defined in BAL-003-1.1 for developing a frequency response measure that is used to calculate an interconnection frequency response performance measure (IFRMA-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.

Source, Assumptions, and Limitations

The statistical analysis and data supporting these findings can be found in the supporting analysis that can be found on the Resources Subcommittee website.[29]

- 2018 Frequency Response Annual Analysis[30]

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

[30] https://www.nerc.com/comm/OC/Documents/2018_FRAA_Report_Final.pdf

- Essential Reliability Services Framework, Measures 1,2, and 4 – Historical Frequency Analysis[31]

Disturbance Control Standard Failures and Events Greater than MSSC

This metric measures the ability of a balancing entity to balance resources and demand following reportable disturbances. The results help measure the risk the system is exposed to during extreme contingencies, how often they occur, and disturbance performance (see **Figures 3.17** and **3.18)**.

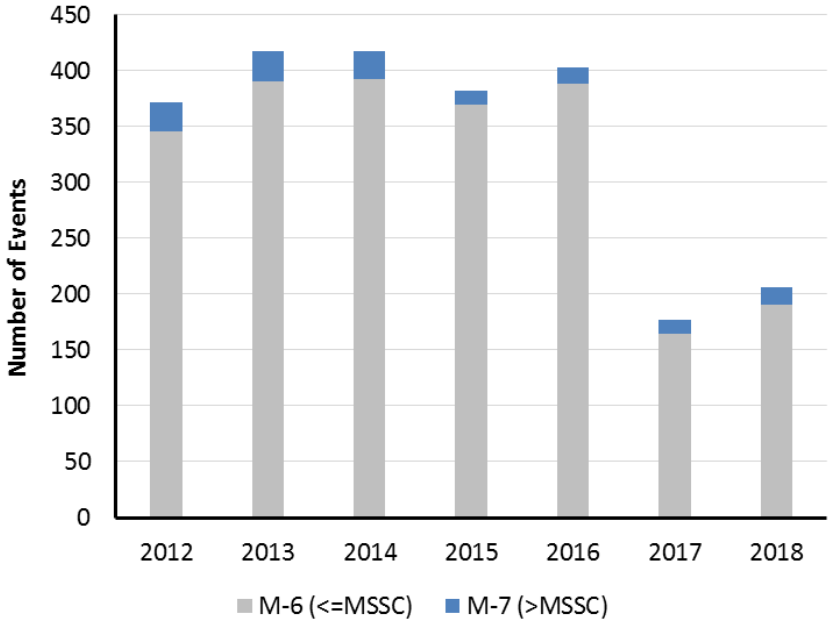


Figure 3.17: Number of Disturbance Control Standard Events

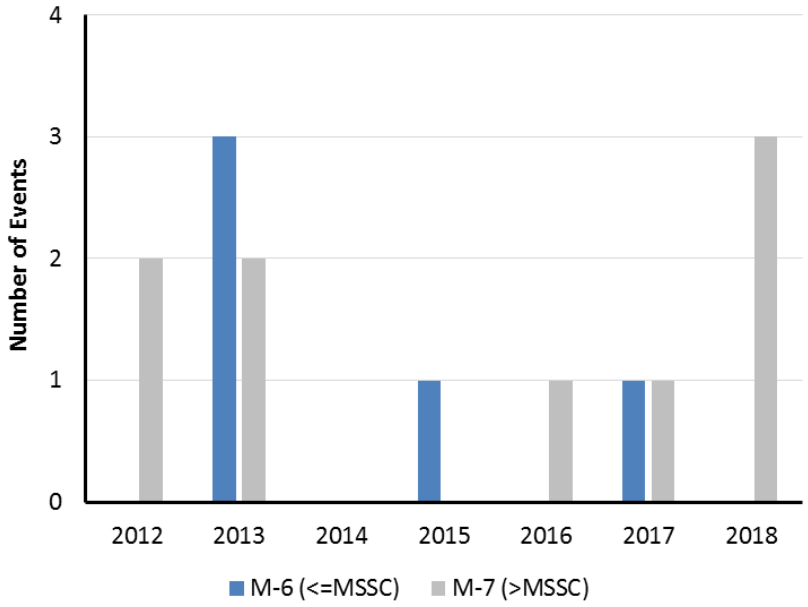


Figure 3.18: Number of Disturbance Control Standard Events with <100% Recovery

[31] https://www.nerc.com/comm/Other/essntlrlbltysrvcstskfrcDL/Item_6b.ii._ERS_Historical_%20Measures_124%20_Technical%20Brief_DRAFT_%2020171107.pdf

2018 Performance and Trends
Based on the similar annual results over the last five years, disturbance control recovery performance is stable, and there were no events that had less than 100% recovery. While there were three events that did not fully recover within the required time, these events were initiated by a contingency that was larger than the most severe single contingency (MSSC).

Description
This metric measures the ability of a BA or reserve sharing group (RSG) to balance resources and demand following reportable disturbances and those that are greater than the MSSC. NERC Reliability Standard BAL-002-3 requires that a BA or RSG maintain sufficient contingency reserves equal to or greater than its MSSC and to recover its reporting area control error within the contingency event recovery period for reportable balancing contingency events.

Purpose
Measure the BA or RSG's ability to utilize contingency reserve to balance resources and demand and return the Interconnection frequency within defined limits following a reportable disturbance. The results help measure the risk the system is exposed to during extreme contingencies, how often they occur, and disturbance performance.

This Indicator Answers the Following Questions:

- How successful are system operators at restoring the system to predisturbance levels?
- How often do reportable balancing contingency events occur?
- How often do reportable balancing contingency events greater than the MSSC occur?

Definition and Calculation
The metric is calculated as the percentage of the disturbance control standard recoveries divided by the number of disturbance control standard reportable events.

Rating

- **Red (actionable)**: <100% recovery increase **and** continues to be above the five-year average.
- **Yellow (monitor)**: <100% recovery increase for first year **and** it is above the five-year average.
- **White (stable)**: <100% recovery has no change **and** is less than five-year average.
- **Green (good/improving)**: <100% recovery shows improvement **and** is less than the five-year average **or** zero.

Source, Assumptions, and Limitations
NERC Reliability Standard BAL-002-2 requires that a BA or RSG report all disturbance control standard events and nonrecoveries to NERC.[32]

- Metric Worksheet[33]

Protection System Misoperations

This metric evaluates the performance of protection systems—both generator and transmission. The metric is the ratio of protection system misoperations to total system protection system operations (see **Figures 3.19** and **3.20**).

[32] https://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-002-2.pdf

[33] https://www.nerc.com/comm/PC/Performance%20Analysis%20Subcommittee%20PAS%202013/ALR%202-4DCS.pdf

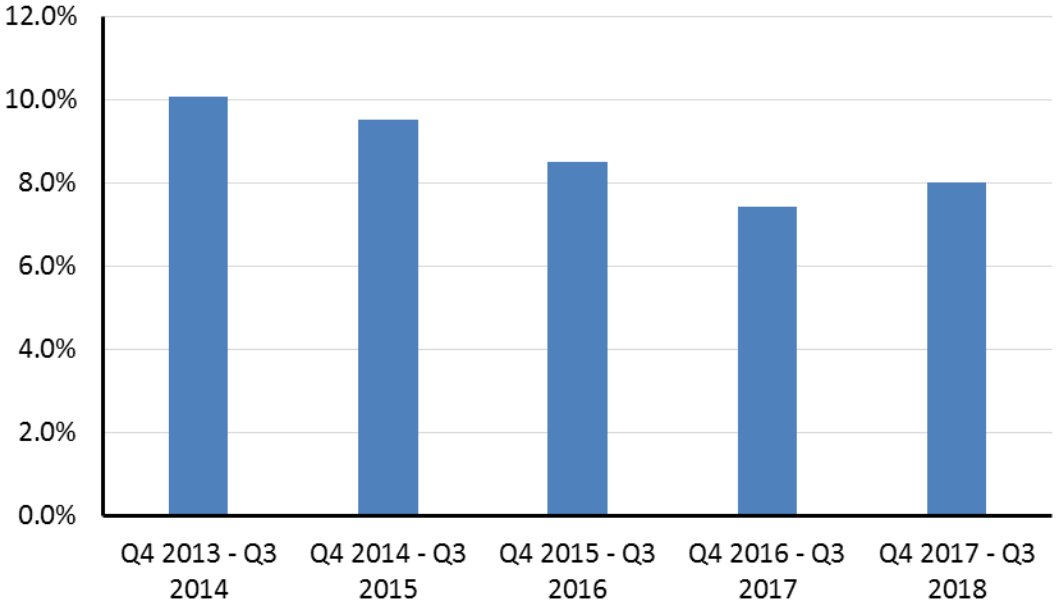


Figure 3.19: Annual Protection System Misoperation Rate Q4 2013 through Q3 2018

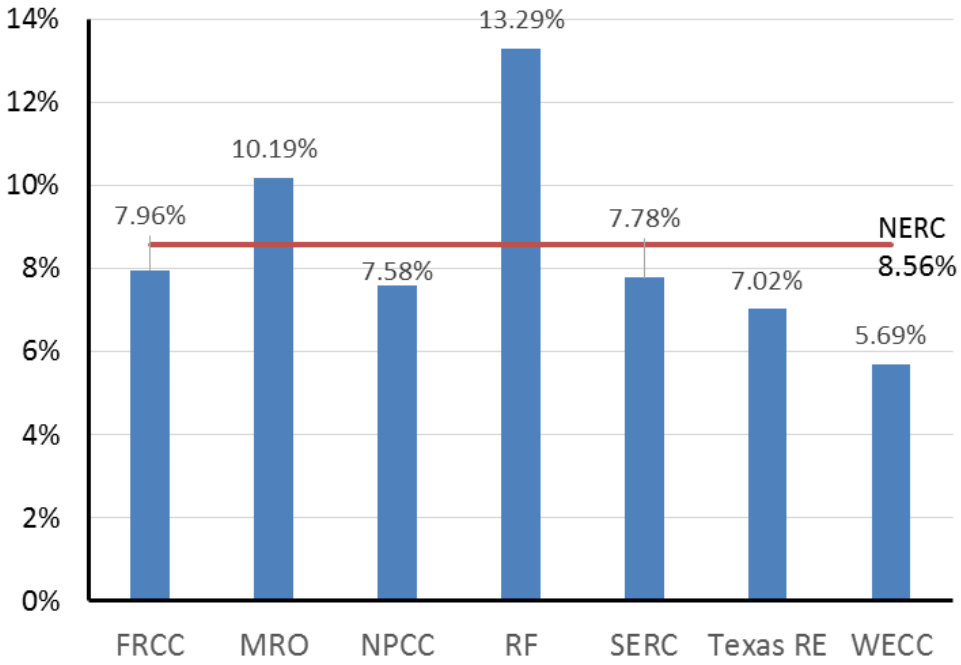


Figure 3.20: Five-Year Protection System Misoperation Rate by Region Q4 2013 through Q3 2018

2018 Performance and Trends

The overall NERC 2018 protection system misoperation rate is slightly higher than 2017, though a statistically significant downward and improving trend continues to be observed. The regional misoperations rate ranges from 5.7% to 13.3%.

Description

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. The data collection is granular and allows NERC to identify specific trends associated with certain geographies, technologies, human performance (HP), and management.

Purpose

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

This Indicator Answers the Following Questions:

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

Definition and Calculation

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

Rating

- **Red (actionable)**: Misoperation rate for NERC shows a statistically significant increase for more than one year.
- **Yellow (monitor)**: Misoperation rate for two Regions show a statistically significant increase **or** the NERC misoperation rate shows a statistically significant increase for one year.
- **White (stable)**: No statistically significant difference in the NERC misoperation rate (there may be a numerical change in the NERC misoperations rate).
- **Green (good/improving)**: Year over year statistical improvement and statistically significant decreasing trend in the NERC misoperation rate **or** zero.

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).[34]

Interconnection Reliability Operating Limit Exceedances

This metric measures the number and the duration an IROL is exceeded. An IROL is an SOL that, if violated, could lead to instability, uncontrolled separation, or cascading outages (see **Figures 3.21–3.23**).

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

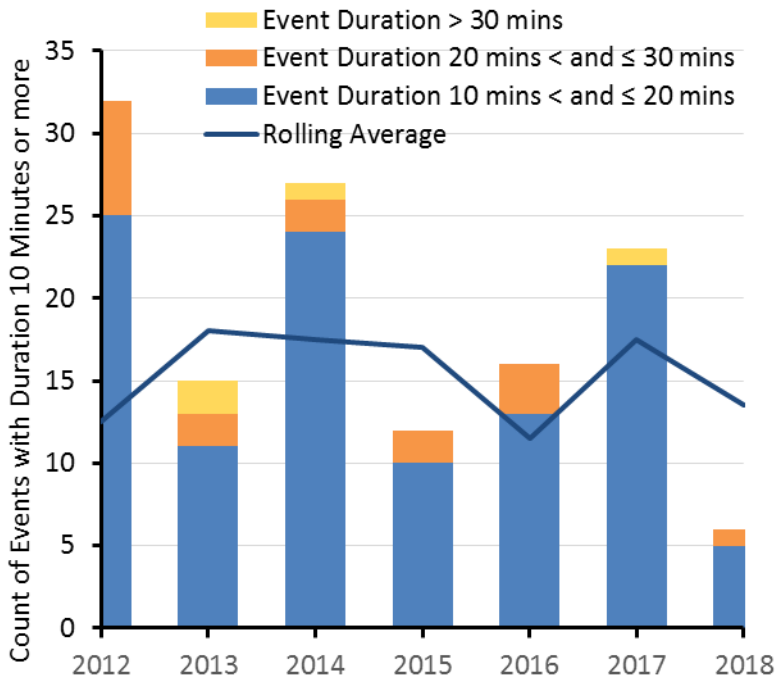


Figure 3.21: Expanded Eastern Interconnection IROL Exceedances

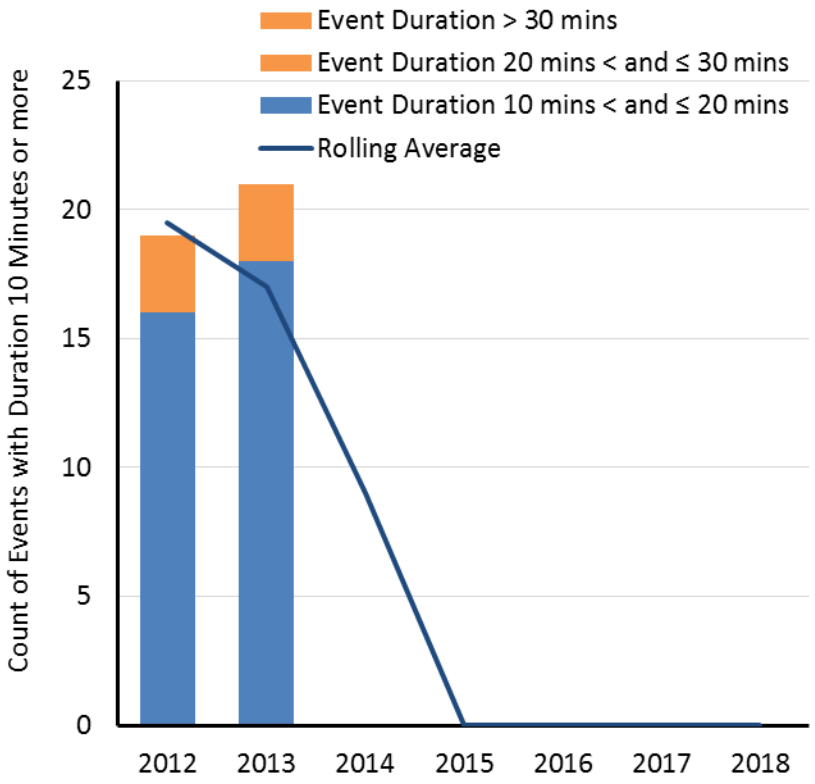


Figure 3.22: Western Interconnection IROL Exceedances

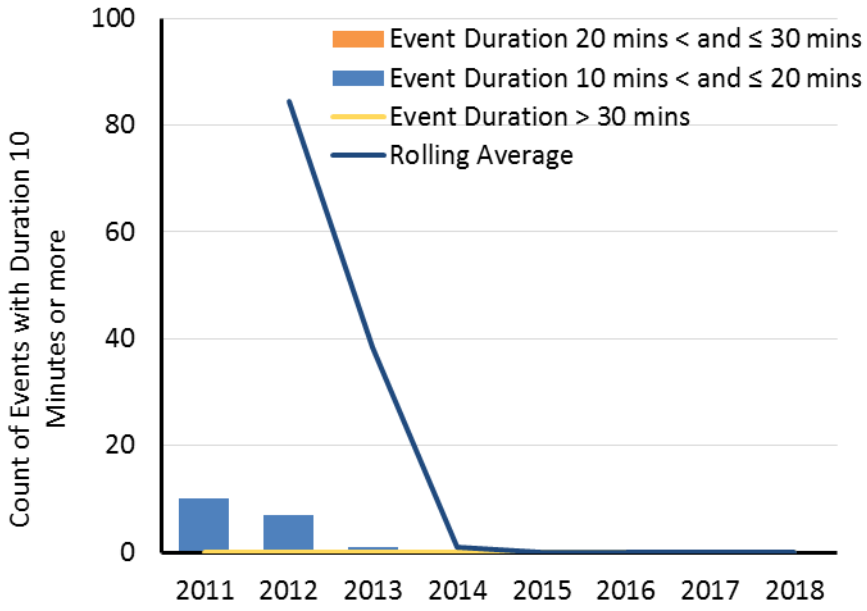


Figure 3.23: Texas Interconnection IROL Exceedances

2018 Performance and Trends

- **Expanded Eastern Interconnection:** In 2018, the two ranges that were impacted were the 10-second to the 10-minute range (not shown) and the 10-minute to the 20-minute range. Exceedance duration is below its five-year rolling average.
- **Western Interconnection:** Prior to 2014, only SOLs were reported. Since 2014, the trend has been stable with no IROL exceedances reported.
- **Texas Interconnection:** The trend has been stable at no exceedances since 2013.

Description

This metric measures the number of times and the duration that an IROL is exceeded. An IROL is an SOL 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.

Purpose

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.

This Indicator Answers the Following Questions:

- How often does the system exceed the established IROL?
- How quickly are IROL exceedances mitigated?
- How long is the system exposed to conditions beyond the established IROL?

Definition and Calculation

A simple number count of IROL (base case conditions or during a contingency) exceedances. Start and end times for IROL exceedance is recorded and the duration is grouped into three time segments as follows:

- 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 < 30+ minutes

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 greater than five-year average.
- **Yellow (monitor)**: Year-over-year count increase of IROL < 30 minutes **or** first year count of IROL < 20 minutes greater than five-year average.
- **White (stable)**: IROL < 20 minutes count is less than less than 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.

Source, Assumptions, and Limitations

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

Chapter 4: Severity Risk Index

The severity risk index (SRI) is calculated each year to measure the relative severity ranking of daily conditions based on performance rates and their impact on the BPS. Impacts are calculated and include load loss, loss of generation, and loss of transmission (see **2018** 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**).

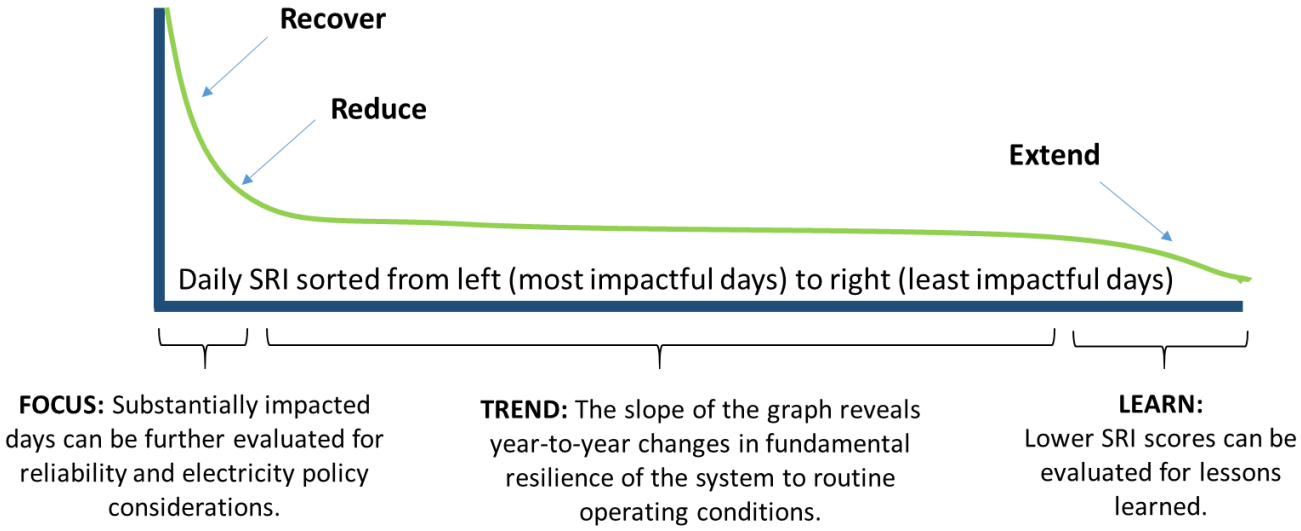


Figure 4.1: Severity Risk Index Concept

How the Severity Risk Index Is Calculated

The Severity Risk Index provides a daily measure of BPS performance. The metric is made of the following components **(Figure 4.2)**:

- **Weighting Transmission System Sustained 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 upon their voltage level and the daily outages divided by the total inventory's average capacity and factored at 30% of the SRI score.
- **Weighting 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.
- **Weighting Distribution Load Lost as a Result of Events Upstream of the Distribution System:** Load lost due to performance upstream of the distribution system is calculated based upon 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 then presented in several different 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 throughout the year.

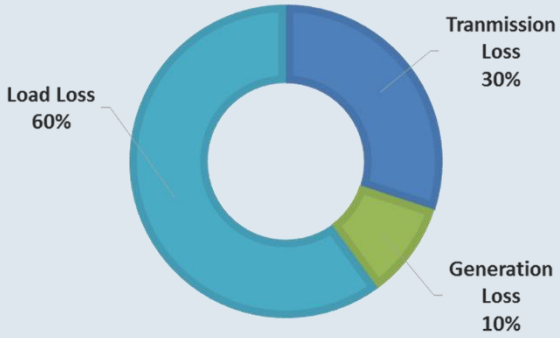


Figure 4.2: SRI Loss Components

2018 Severity Risk Index and Trends

Based on the historical trend and the SRI calculation, 2018 was shown to be the most reliable year compared to the prior five years. **Figure 4.3** sorts the highest SRI days to the lowest SRI days (from left to right). The thumbnail inset further illustrates that the moderate impacts measured during 2018's highest SRI days represented less stress to the BPS than were caused by the highest SRI days in any prior year on record.

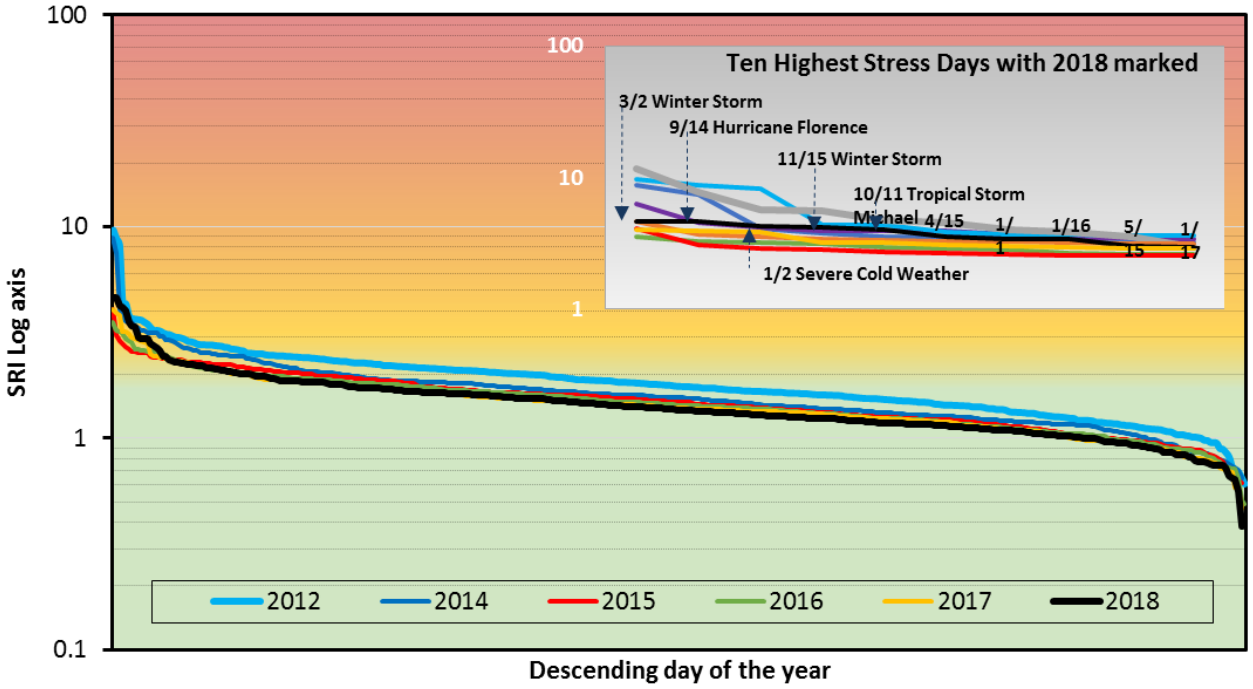


Figure 4.3: NERC Annual Daily Severity Risk Index Sorted Descending

Figure 4.4 shows the annual cumulative performance of the BPS. If a step change or inflection point occurs on the graph, it represents where a higher stress day (as measured by the SRI) occurred. The smoother the slope of the cumulative curve, the less volatile the day-to-day performance of the system through the evaluation period. The year 2018 began with relatively high SRI days and but continued with high performance through the end of the year. The cumulative SRI for 2018 was lower than any year during the prior five years, and it was roughly 30% lower than the 2012 cumulative SRI, which is the worst performing year since 2010 as measured by the SRI.

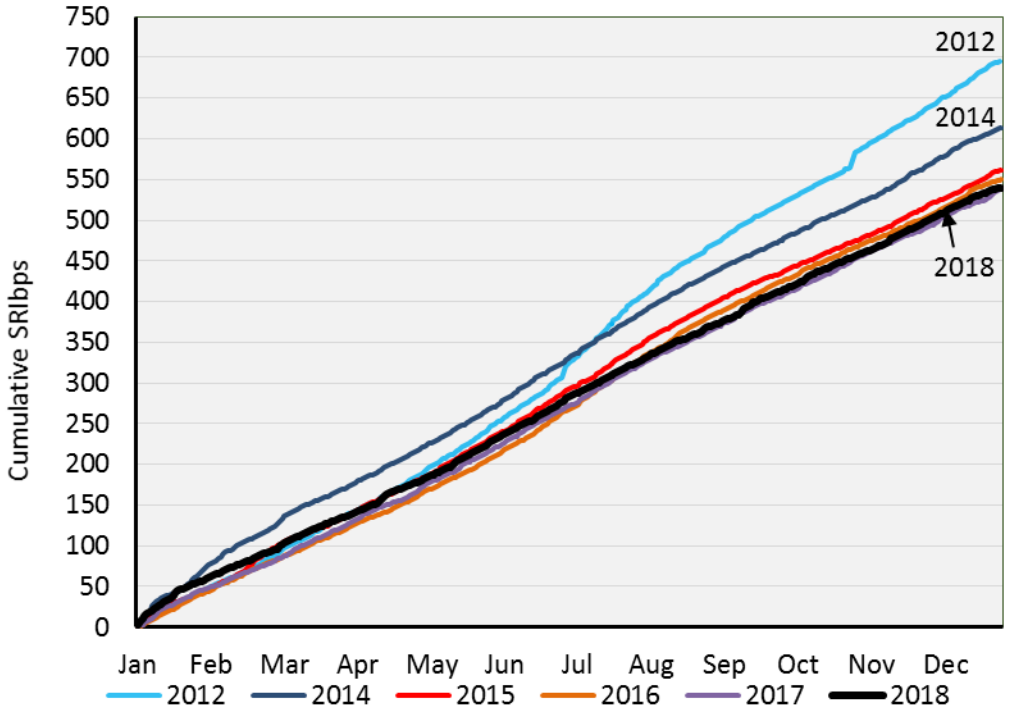


Figure 4.4: Cumulative SRI (2012 and 2014–2018)

Table 4.1 shows identifies the top-10 SRI days during 2018 and denotes the generation, transmission, and load loss components for each of these days. It further identifies whether a specific event contributed to a significant part of the SRI calculation, the type of event that occurred, and its general location. Many of the days dominated by generation loss were primarily driven by cold weather with more than half of the days experiencing winter storms—and two top days of winter storms occurring in November and March.

Table 4.1: 2018 Top 10 SRI Days

Rank	Date	NERC SRI and Weighted Components 2018				G/T/L	Weather Affected?*	Event Type	Region
		SRI	Weighted Generation	Weighted Transmission	Weighted Load Loss				
1	3/2/2018	4.63	0.90	0.43	3.30		√	Severe weather (winter storm Riley)	NPCC, RF
2	9/14/2018	4.63	1.32	0.56	2.75		√	Severe weather (hurricane Florence)	SERC
3	1/2/2018	4.23	3.87	0.26	0.10		√	Severe weather (load reduction)	SERC, NPCC
4	11/15/2018	4.15	1.69	0.29	2.16		√	Severe weather (winter storm Avery)	RF, SERC
5	10/11/2018	3.99	1.00	0.60	2.39		√	Severe weather (tropical storm Michael)	SERC
6	4/15/2018	3.51	1.07	0.41	2.02		√	Severe weather (late season snow, storm)	RF, SERC
7	1/1/2018	3.39	2.96	0.29	0.13		√	Severe weather (load reduction)	SERC, TRE
8	1/16/2018	3.36	2.31	0.77	0.28		√	Severe weather (severe cold weather)	SERC, TRE
9	5/15/2018	2.98	1.41	0.44	1.14		√	Severe weather (tornado, wind, hail)	NPCC, RF
10	1/17/2018	2.95	2.35	0.24	0.36		√	Severe weather (from 1/16/2018)	SERC

**Verified by OE-417*

Figure 4.5 reflects the data in the table above. It is a daily plot of the SRI score for 2018 (shown in blue) against control limits that were calculated using 2012–2018 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. Days of stress are identified by falling above the seasonal daily control limits.

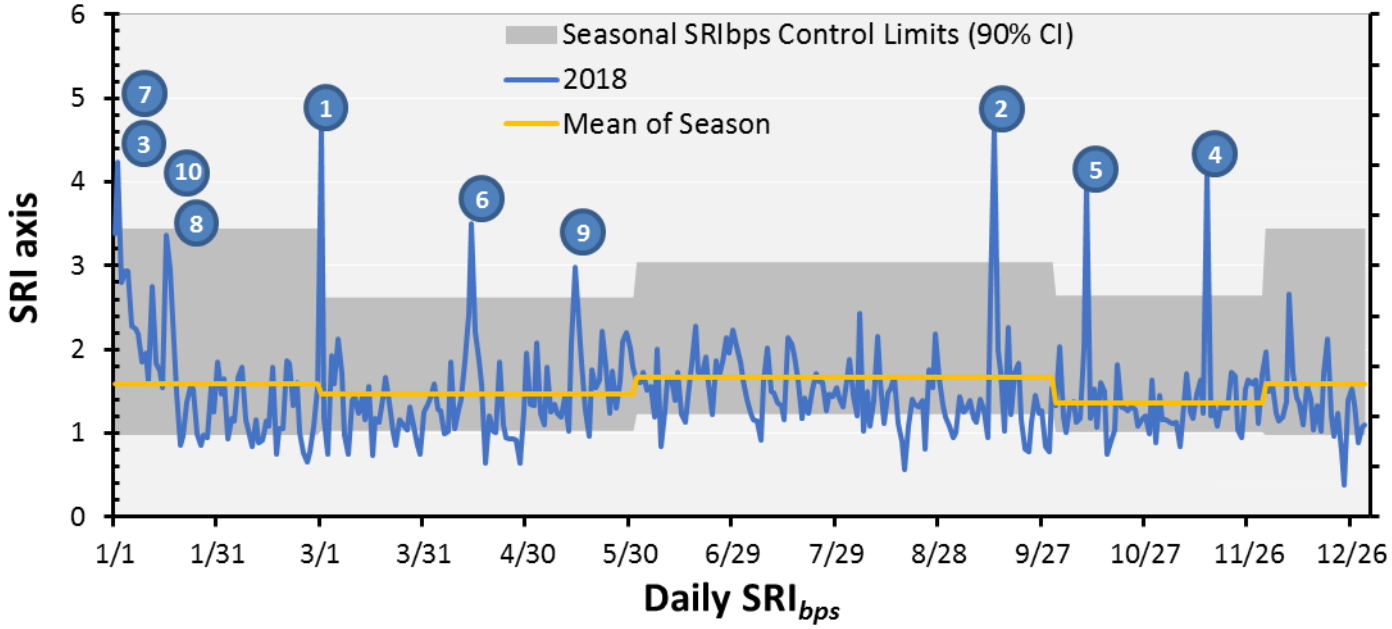


Figure 4.5: NERC 2018 Daily SRI with Top 10 Days Labeled, 90% Confidence Interval

Historical performance trends can be gathered by comparing the 2018 SRI to prior years. The top 10 SRI days for 2010 through 2018 are shown in Figure 4.6 and Table 4.2, none of which occurring since 2014.

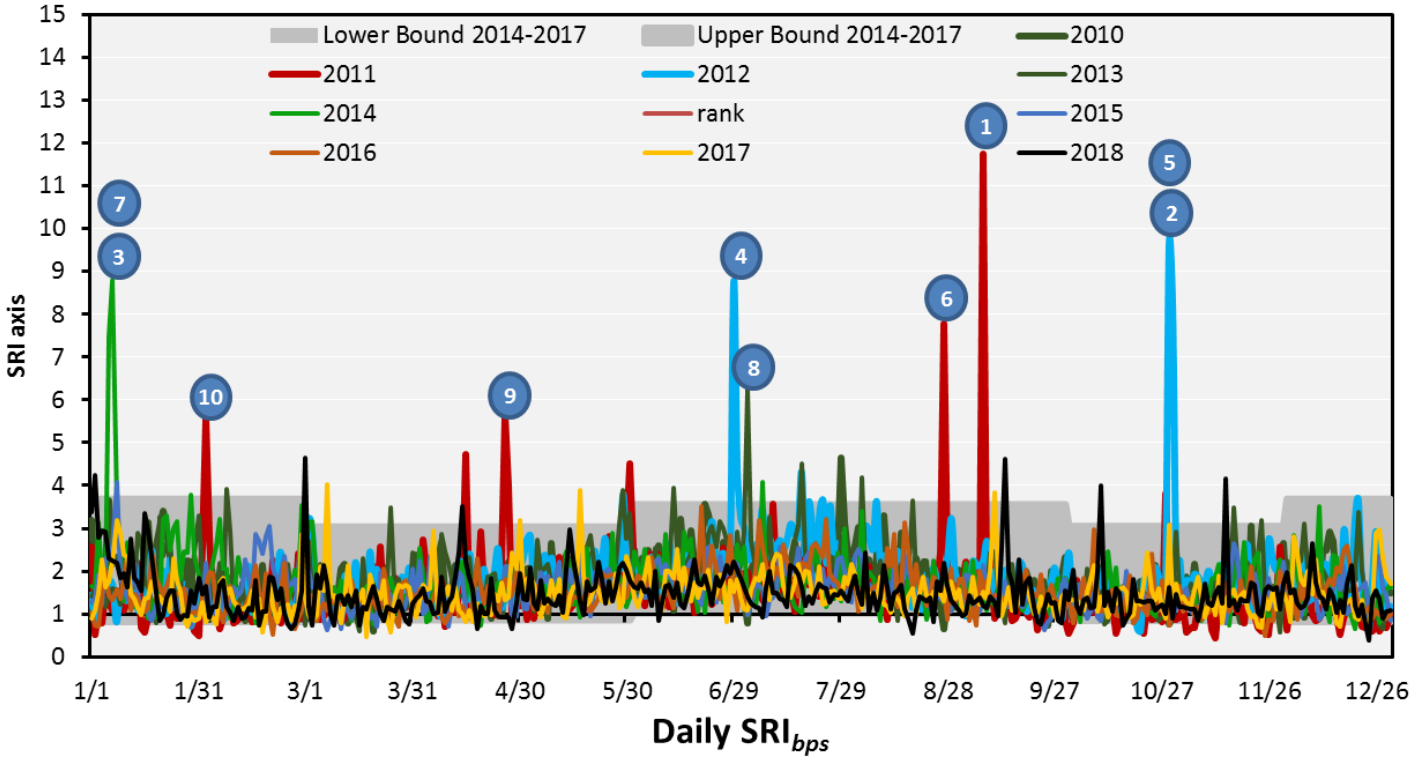


Figure 4.6: NERC 2010—2018 Daily SRI with Top 10 Days Labeled, 90% Confidence Interval

Table 4.2: Top 10 SRI Days (2008–2018)

Rank	Date	NERC SRI and Weighted Components					Weather Affected?*	Event Type	Region
		SRI	Weighted Generation	Weighted Transmission	Weighted Load Loss	G/T/L			
1	9/8/2011	11.8	1.2	0.8	9.8			Southwest Blackout	WECC
2	10/29/2012	9.6	2.2	1.8	5.6		√	Hurricane Sandy	NPCC, SERC
3	1/7/2014	8.8	7.6	0.7	0.5			Polar Vortex	RF, Texas RE, SERC
4	6/29/2012	8.8	2.8	1.4	4.6		√	Thunderstorm Derecho	RF, NPCC, MRO
5	10/30/2012	8.2	2.9	3.4	1.9		√	Hurricane Sandy	NPCC, SERC
6	8/28/2011	7.8	0.8	1.6	5.4		√	Hurricane Irene	NPCC, RF
7	1/6/2014	7.5	5.5	1.4	0.5			Polar Vortex	RF, Texas RE, SERC
8	9/14/2008	6.3	1.4	0.8	4.1		√	Hurricane Ike	Texas RE, SERC, RF, MRO, NPCC
9	7/4/2013	6.3	0.9	3.6	1.7			Heavy Rain and Flooding	FRCC, SERC
10	4/27/2011	5.6	1.9	3.5	0.2			Tornados, Severe Weather	SERC

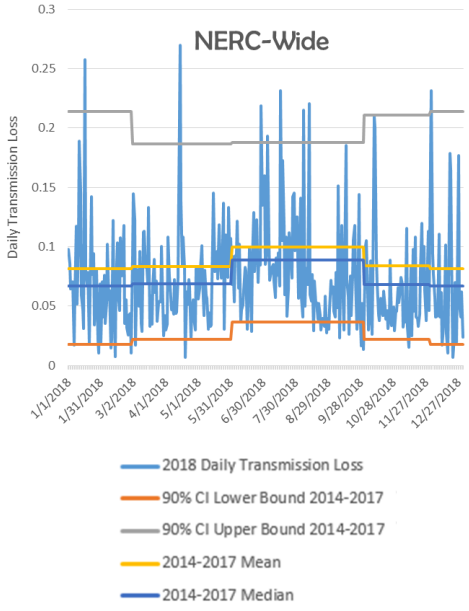
**Verified by OE-417*

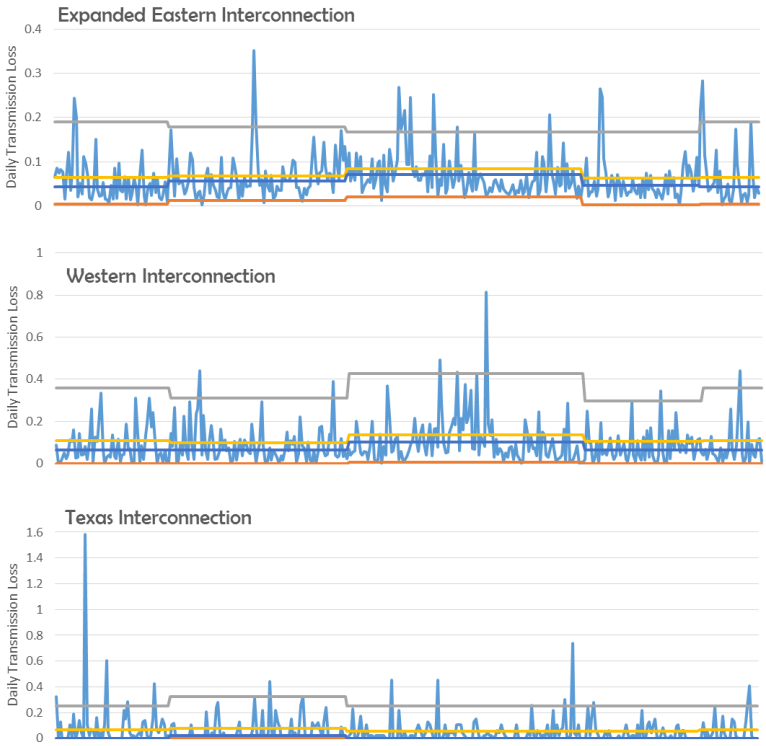
See **Figure 4.7** for information on transmission component of the SRI and **Figure 4.8** for information on generation component of the SRI.

2018 Daily Transmission Loss

90-percent Confidence Interval by Season

Daily Transmission Loss (DTL) is a share of the total MVA of the transmission system lost on a given day due to sustained automatic outages.





Transmission Performance and Availability Statistics

Descriptive Statistics of Daily Transmission Loss by Year (Share of Total Transmission MVA in TADS)						
Year	Days	Mean	Standard Deviation	Minimum	Maximum	Median
2014	365	0.108	0.09	0	0.754	0.084
2015	365	0.084	0.053	0.003	0.342	0.072
2016	366	0.081	0.051	0.002	0.515	0.072
2017	365	0.08	0.056	0.008	0.669	0.069
2018	365	0.073	0.043	0.007	0.269	0.065

Descriptive Statistics of Daily Transmission Loss by Season, 2014-2018 (Share of Total Transmission MVA in TADS)						
Season	Days	Mean	Standard Deviation	Minimum	Maximum	Median
Winter	305	0.080	0.069	0.002	0.000	0.064
Spring	461	0.081	0.059	0.000	0.754	0.069
Summer	610	0.096	0.058	0.012	0.669	0.085
Fall	450	0.079	0.063	0.000	0.472	0.064

Maximum Daily Transmission Loss for Last 5 years	
3/1/2014	0.75
Date	**Highest 2018 Daily Transmission Loss**
1/16/2018	0.26
4/14/2018	0.27
6/28/2018	0.22
7/16/2018	0.23
8/6/2018	0.21
8/11/2018	0.22
12/2/2018	0.23
1/16/2018	0.26

Trends 2014-2018

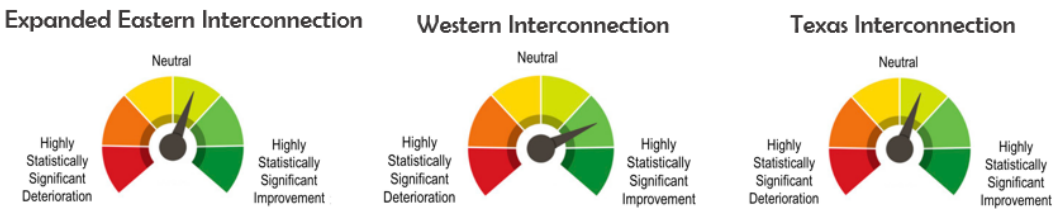
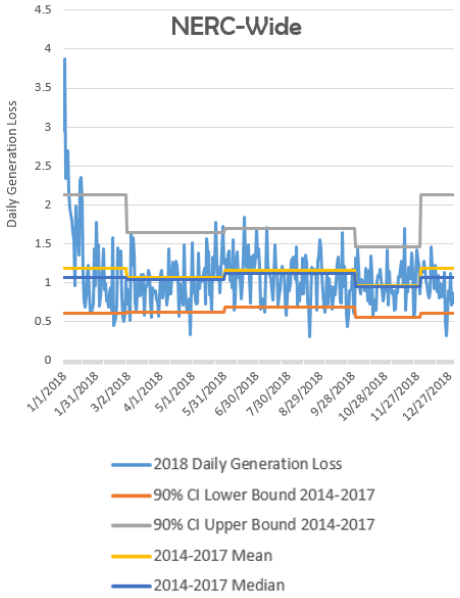


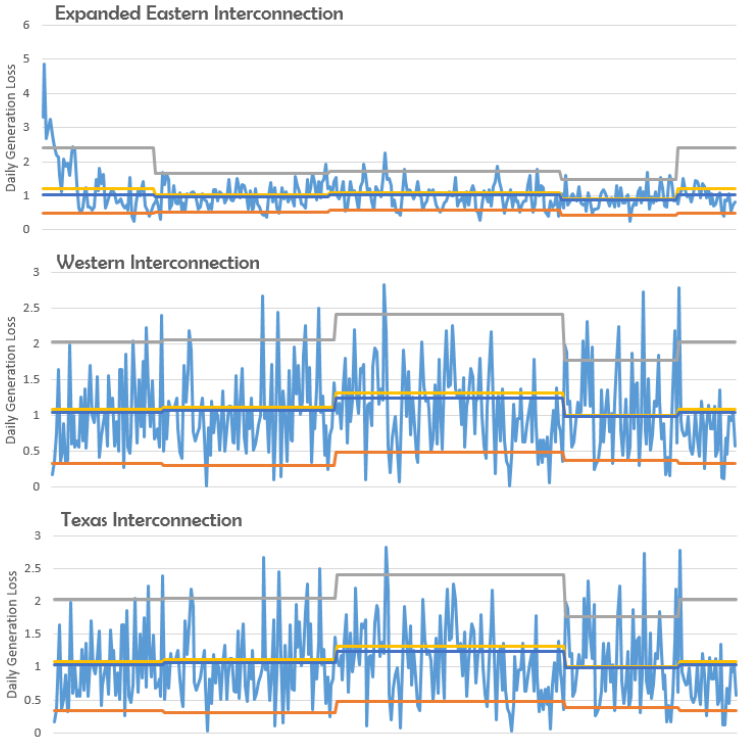
Figure 4.7: Transmission Performance and Availability Statistics

2018 Daily Generation Loss

90-percent Confidence Interval by Season

Daily Generation Loss (DGL) is a share of the total capacity of conventional generation reporting to GADS lost on a given day due to unplanned (forced) outages.





Generation Performance and Availability Statistics

Descriptive Statistics of Daily Generation Loss by Year
(Share of Total Conventional Generation in GADS)

Year	Days	Mean	Standard Deviation	Minimum	Maximum	Median
2014	365	1.18	0.58	0.43	7.56	1.09
2015	365	1.12	0.38	0.42	3.51	1.07
2016	366	1.09	0.34	0.38	2.61	1.07
2017	365	1.03	0.33	0.27	2.83	1.00
2018	365	1.06	0.39	0.3	3.87	1.01

Descriptive Statistics of Daily Generation Loss by Season, 2014-2018
(Share of Total Conventional Generation in GADS)

Season	Days	Mean	Standard Deviation	Minimum	Maximum	Median
Winter	305	0.96	0.27	0.42	2.07	0.95
Spring	461	1.05	0.32	0.27	2.58	1.02
Summer	610	1.13	0.32	0.30	2.61	1.11
Fall	450	1.18	0.63	0.31	7.56	1.04

Maximum Daily Generation Loss for Last 5 years (%)

1/7/2014	7.56

Date	Highest 2018 Daily Generation Loss
1/1/2018	2.97
1/2/2018	3.87
1/3/2018	2.34
1/4/2018	2.64
1/5/2018	2.69
1/6/2018	2.17
1/16/2018	2.31
1/17/2018	2.35

Trends
2014-2018

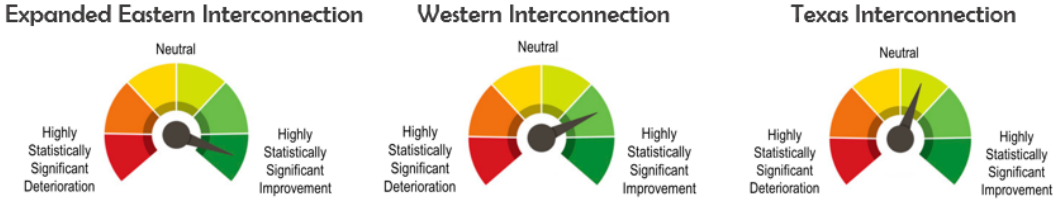


Figure 4.8: Generation Performance and Availability Statistics

Transmission Outage Severity

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. The impact of a TADS event to BPS reliability is called the transmission outage severity (TOS) of the event. A TADS event is a transmission incident that results in the automatic outage (sustained or momentary) of one or more elements. 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.

TADS inventory and outage data are used to study the ICCs of transmission outages. This analysis can shed light on prominent and underlying causes affecting the overall performance of the BPS. TOS determines which ICCs are most severe with respect to magnitude and duration of transmission events.[35]

TOS and outage duration for sustained transmission outages >100 kV from the 2015–2018 period are shown in **Figure 4.9**.

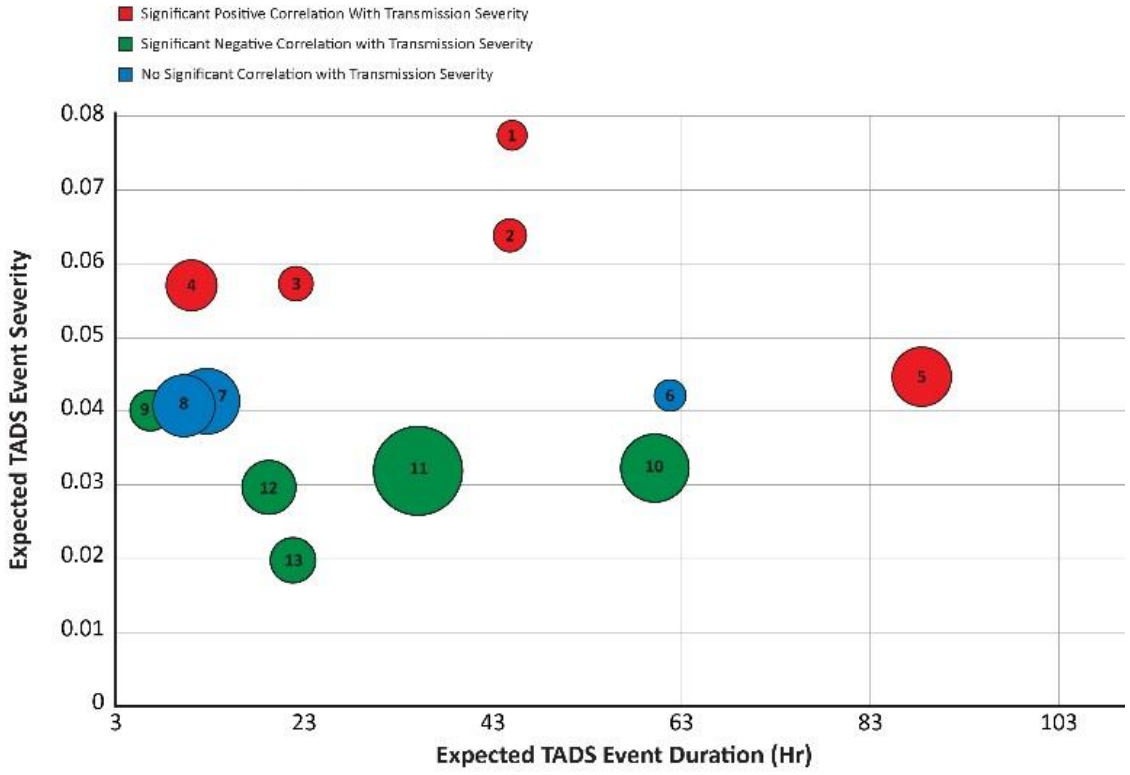


Figure 4.9: Transmission Outage Severity vs. Expected TADS Event Duration

[35] The equations are aligned to the definition of the transmission component in the SRI. The severity of a transmission outage is calculated based on its estimated contribution of power flow capacity through TADS transmission element based on voltage class. The average power flow MVA values or equivalent MVA values by Interconnection are used. The impact (in terms of MVA outages and duration) for each event are divided by the sum of the MVA inventory.

Total TOS has decreased year-over-year for the last four years (see **Figure 4.10**), a positive indication that transmission outages are leading to less severe reliability impacts.

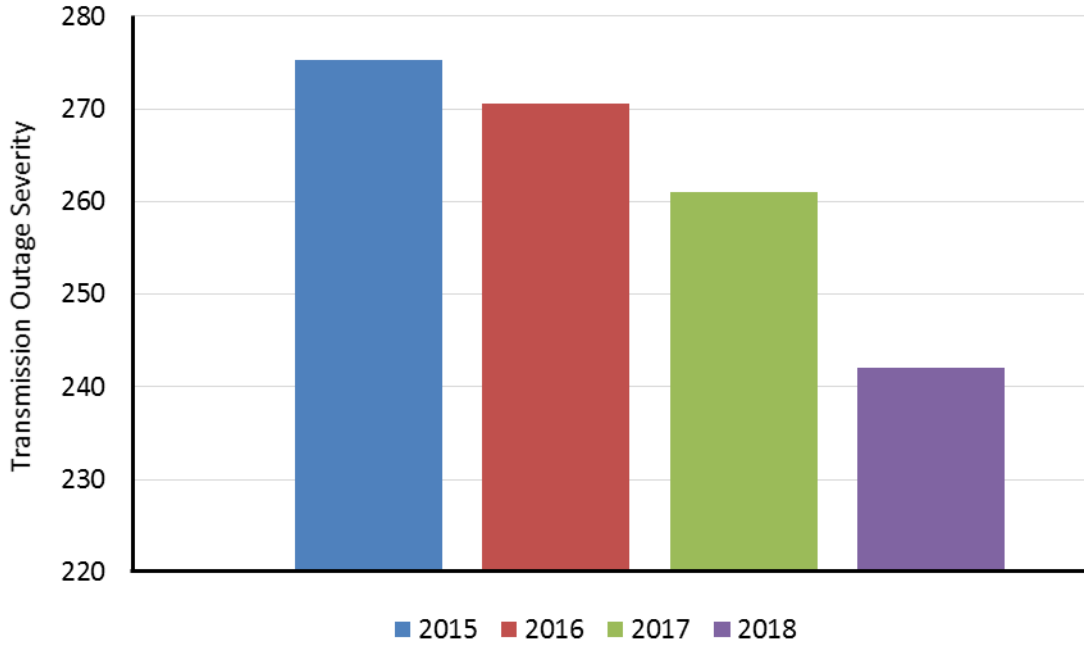


Figure 4.10: TOS of TADS Sustained Events of 100 kV+ AC Circuits and Transformers by Year

Chapter 5: Trends in Priority Reliability Issues

In addition to the core set of reliability indicators, this section of the report will highlight important observations and trends that pose specific reliability challenges. It is important that NERC use its data and analytical insights to establish priorities and expectations that commit both its and the industry's scarce resources. Data, information, and insights in this *State of Reliability* can shed light on key reliability issues, identify extent of conditions, and help determine what type of mitigation is most appropriate.

NERC routinely prioritizes emerging and known reliability issues. The Reliability Issues Steering Committee (RISC) is an advisory committee to the NERC Board of Trustees that triages and 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.

Based on an adapted set of priority issues identified in the most recent RISC report, this year's *State of Reliability* focuses on the risks described below:

- **BPS Planning and Adapting to the Changing Resource Mix**
- **Increasing Complexity in Protection and Control** Systems
- **Human Performance and Skilled Workforce**
- **Loss of Situation Awareness**
- **Physical Security and Cyber Security**
- **Resilience and Recovery from Extreme Natural** Events

BPS Planning and Adapting to the Changing Resource Mix

Today's resource mix has continued to evolve with the addition of emerging technologies, such as inverter-based generation resources; improving storage techniques; and federal, state, and provincial renewable favoring policies. Transmission Planners, BAs, Asset Owners, and System Operators of the BPS may not have sufficient time to develop and deploy plans in response to reliability considerations resulting from the new resource mix. Over time, regulatory initiatives, along with expected lower production costs and aging generation infrastructure, will likely alter the nature, investment needs, and dispatch of generation considering 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 to market design.

Changes in the Peak Resource Mix over the Past 10 years

The North American electric power system is undergoing a significant transformation with ongoing retirements of fossil-fired and nuclear capacity as well as growth in natural gas, wind, and solar resources.

Over the past 10 years 72 GW of conventional generation has retired, and 205 GW, 95 GW, and 22 GW of natural gas, wind and solar generation has been added, respectively; however, the on-peak value for wind and solar is significantly less (see **Figure 5.1**).

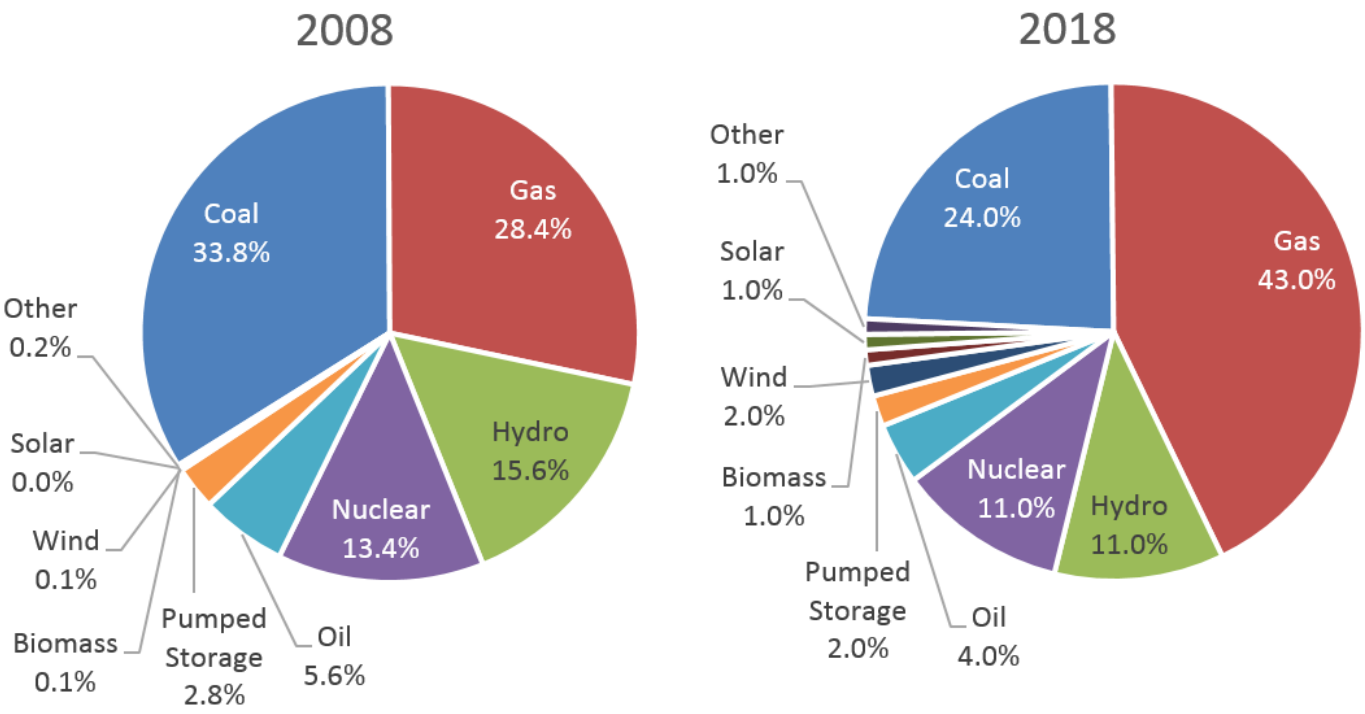


Figure 5.1: 2008 and 2018 NERC-Wide On-Peak Capacity Resource Mix

Distributed Energy Resource Installations

Increasing installations of distributed energy resources 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. Across the United States, approximately 25 GW of distributed solar generation has been installed since 2010 (see **Figure 5.2**). In Canada, Ontario has already installed just over 4 GW of DERs, and another 1 GW is expected in the coming years.

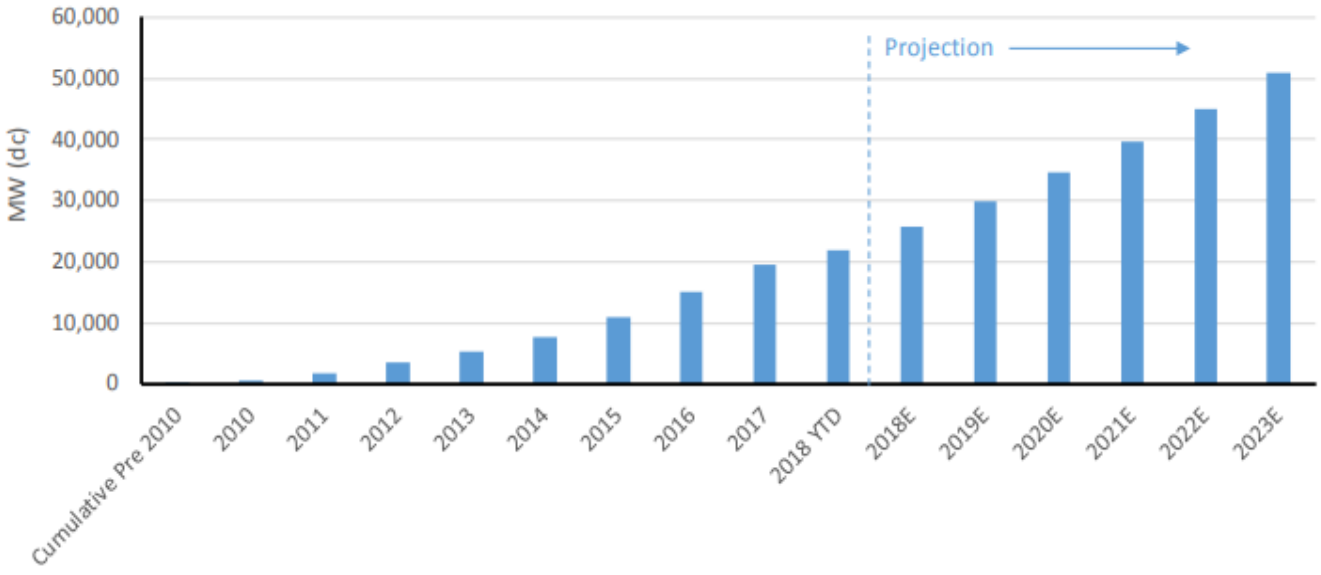


Figure 5.2: United States Cumulative Total Amount of Distributed Solar PV

Challenges and Solutions with Integrating Large Amounts of Inverters

Asynchronous resources (those that are not physically synchronized with the BPS) use inverters to connect and inject power into the grid. Because the system was largely designed around synchronous resources, technical challenges have begun to emerge. For example, a solar generation loss took place in the WECC Region in October 2017; the system experienced problems produced by wild-fire-related transmission line faults that triggered 900 MW of solar resource loss.

A major disturbance report was published in February 2018 and a second solar loss NERC alert was issued as a result of this analysis in May 2018 (see **Figure 5.3**). NERC collected a variety of data from solar Generator Owners and Operators to evaluate the extent of condition and potential mitigation strategies. WECC collaborated with NERC to conduct analysis resulting in publication of important operating guidance to the industry.

For more information, see the Inverter-Based Resource Performance Task Force website.[36]

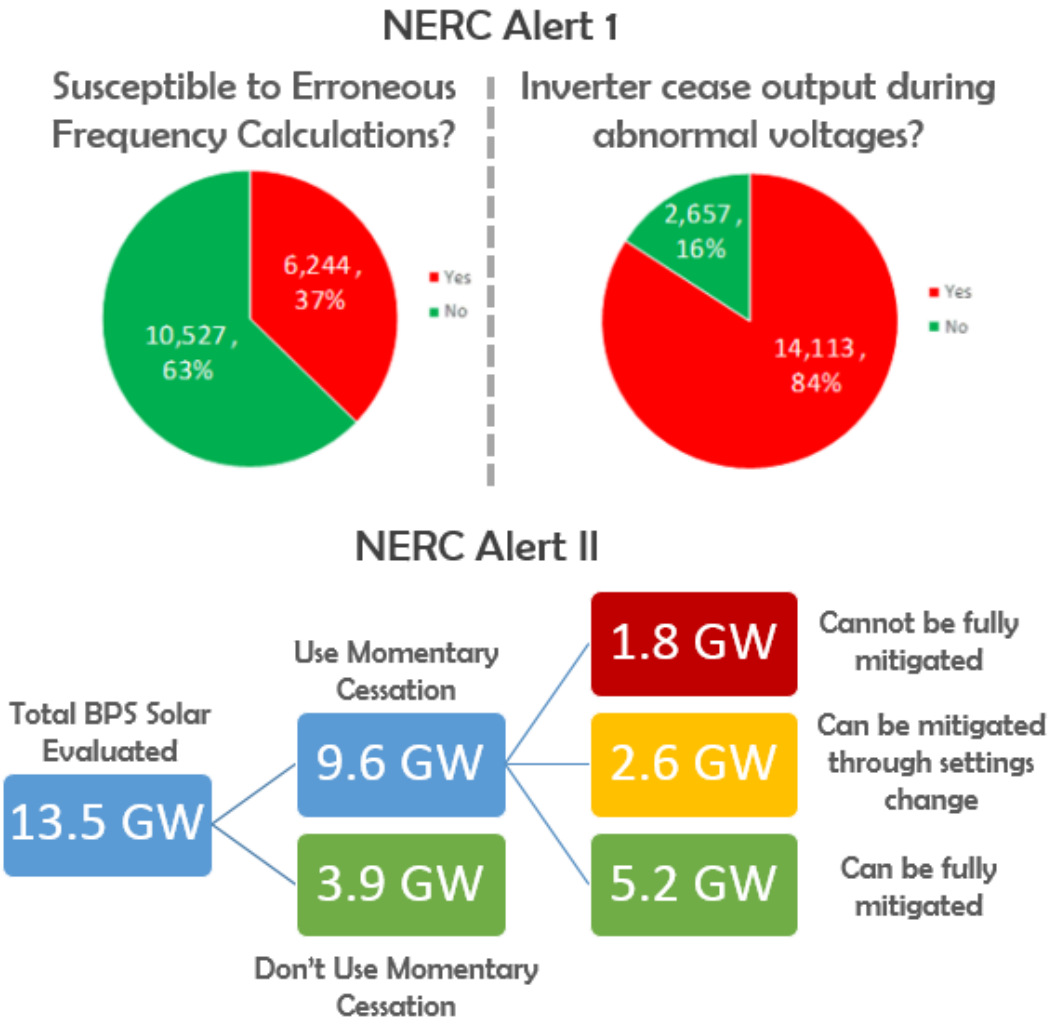


Figure 5.3: Understanding How Much Solar Capacity Is at Risk of Unexpected Behavior and Potential Mitigation

[36] https://www.nerc.com/comm/PC/Pages/Inverter-Based-Resource-Performance-Task-Force.aspx

Assessment

The electricity sector is undergoing significant and rapid change, presenting new challenges and opportunities for reliability. With appropriate insight, careful planning, and continued support, the electricity sector will continue to navigate the associated challenges in a manner that maintains reliability and resilience. As NERC has identified in recent assessments, retirements of conventional generation and the rapid addition of variable resources in some areas—primarily wind and solar—introduce different operating characteristics and require different considerations as the system continues to be planned for the future.

Actions in Progress

- NERC long-term, seasonal reliability assessments, and special assessments as needed
- Resources Subcommittee monitoring and analysis
- Inverter-Based Resource Performance Task Force
- Enhancements to NERC Protection and Control and Modeling Reliability Standards
- Development of requirements to collect GADS data for solar, wind, and energy storage installations

Recommendations

- The ERO Enterprise and industry should continue to expand the use of probabilistic approaches to develop resource adequacy measures that reflect variability and overall reliability characteristics of the resources and composite loads, including, but not limited to, energy and fuel constraints, energy storage, and DERs.
- NERC, working with the industry and forums, should develop guidelines and good industry practices for developing and maintaining accurate system and electromagnetic models that include the resources, load, and controllable devices that provide essential reliability services.

Increasing Complexity in Protection and Control Systems

Failure to properly design, coordinate, commission, operate, maintain, prudently replace, and upgrade BPS control system assets could negatively impact system resilience and result in more frequent and wider-spread outages initiated or exacerbated by protection and control system misoperations or failures. Resource mix changes can also impact wide-area protection largely due to the changing characteristics of generation and the need to coordinate with the distribution system. Asset management strategies are evolving to include greater amounts of digital-network-based controls for substation assets that introduce cybersecurity risks.

Regional Differences in Misoperations Rate

The NERC five-year misoperations rate can be broken down by RE (see **Figure 5.4**). Across seven REs, the misoperations rate ranges from 5.66% in WECC to 13.29% in RF.

Based on a statistical analysis, significant improvements have been observed in MRO, RF, SERC, and WECC. However, in FRCC, NPCC, and Texas RE, a statistically significant decline in performance has been observed. Statistically significant trends are highlighted by the connecting green and red arrow.

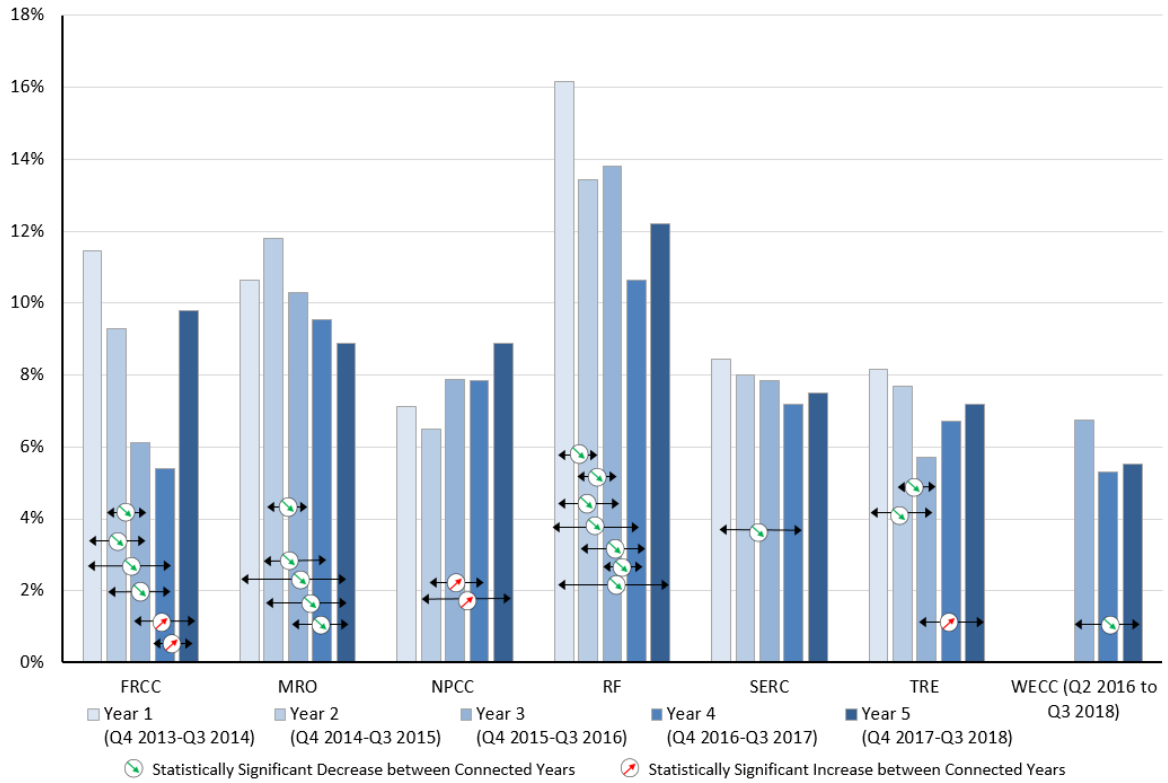


Figure 5.4: Year-Over-Year Changes and Trends in the Annual Misoperations Rate by Region

Leading Causes of Misoperations

The top three causes of misoperations are Incorrect Settings/Logic/Design Errors, Relay Failures/Malfunctions, and Communication Failures over the past five years (See **Figure 5.5**). These cause codes have consistently accounted for more than 60% of all misoperations since data collection started in 2011.

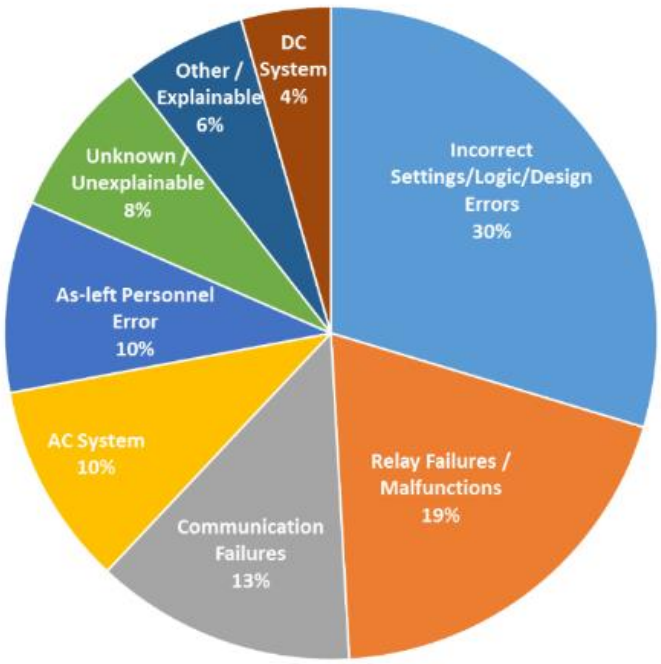


Figure 5.5: Misoperations by Cause Code (4Q 2013 through 3Q 2018)

Protection System Failures Leading to Transmission Outages

The calculated annual outage frequencies per ac circuit and per transformer were tested to identify significant year-to-year changes of the reliability metric (see **Figure 5.6**). Below is a summary of performance:

- There was no significant changes from 2015–2016.
- The 2017 outage frequency is significantly lower than in 2015–2016.
- Transformer outage frequency is improving.

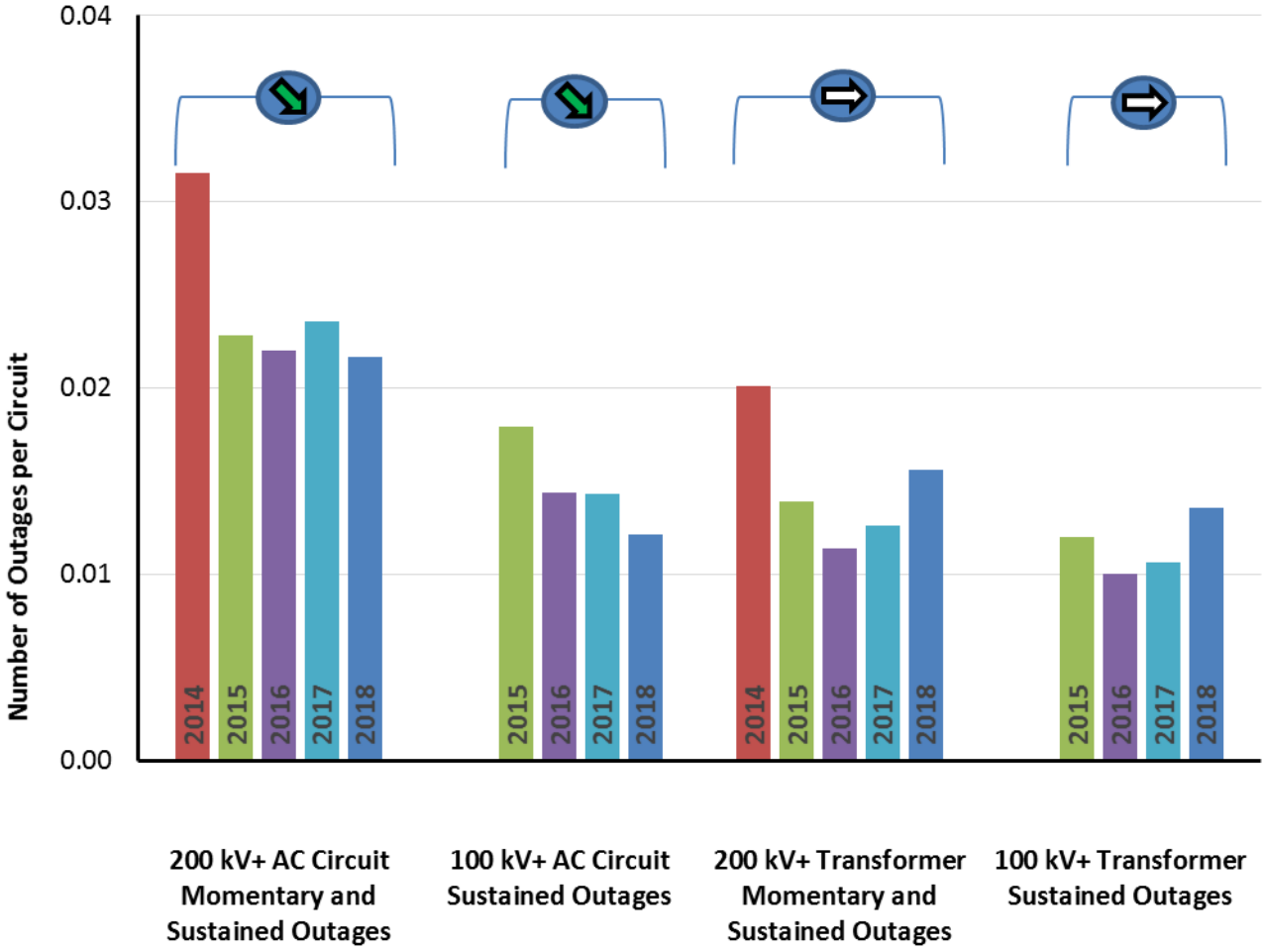


Figure 5.6: 100 kV+ AC Circuit Outages Initiated by Failed Protection System Equipment

Event-Related Misoperations

An analysis of misoperations data and events in the EAP found that, in 2015, there were 50 transmission-related system disturbances that resulted in a qualified event. Of those 50 events, a total of 34 events, or 68%, had associated misoperations. Of the 34 events, a total of 33 of them, or 97%, experienced misoperations that significantly increased the severity of the event. The number of misoperations due to breaker failure/bus differential was a significant portion of these misoperations. Since 2015, NERC and the Regional Entities formed various task forces, conducted more granular root cause analysis, and held workshops dedicated to reducing protection system misoperations. In 2018, the rate of misoperation-related events has decreased since 2016, but more significantly, the amount of breaker failure/bus differential misoperations has significantly decreased (see **Figure 5.7**). The interventions suggested by the ERO and deployed by the industry appear to have successfully reduced the number of events with misoperations, particularly those caused by breaker failure/bus differential.

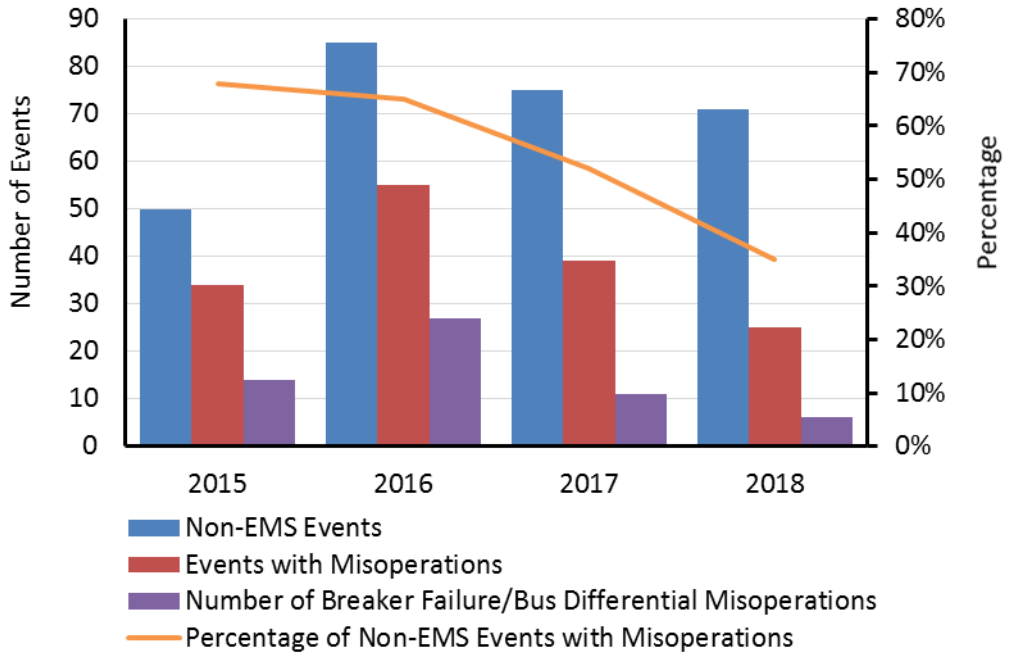


Figure 5.7: Events with Misoperations

Assessment

With more than 60% of all misoperations consistently accounted for by one of the aforementioned three causes of Incorrect Settings/Logic/Design Errors, Relay Failures/Malfunctions, and Communication, the ERO Enterprise is continuing to use Event Analysis data and industry and manufacturer expertise to focus on reducing these identified causes. Past sustained focus on education and outreach on settings regarding the instantaneous ground overcurrent protection function and on improving relay system commissioning tests has had a significant effect on reducing the rate. Additionally, specific regional efforts that targeted a reduction of communication failures resulted in a year-over-year measurable improvement. The regional specific efforts, such as the formation of focused technical teams and workshops, has been instrumental in helping the industry improve the misoperations rate. Continued focus by the ERO Enterprise and industry is merited, and the reduction of the misoperation rate remains a high priority in the sustainment of a reliable system.

Actions in Progress

- Conduct industry webinars on protection systems and document success stories on how GOs and TOs are achieving high levels of protection system performance.
- Collect and analyze protection system misoperations data and information through MIDAS.
- Report the quarterly protection system misoperations data on NERC's website.

Recommendations

- The ERO should work with industry experts and the forums 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 determine if there is an increasing reliability risk due to the different short-circuit contribution characteristics of inverter-based resources.
- The Misoperations Data Collection program should be enhanced by refining the data reporting instructions to improve overall data quality and consistency.

Human Performance and Skilled Workforce

The BPS is becoming more complex, and as the industry faces turnover in technical expertise, it will have difficulty staffing and maintaining necessary skilled workers. 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. In addition, inadequate human performance (HP) makes the grid more susceptible to both active and latent errors that negatively affect reliability. Weaknesses in HP may hamper an organization's ability to identify and address precursor conditions to promote effective mitigation and behavior management.

Transmission Outages Related to Human Performance

NERC TADS collects performance data on transmission outages due to Human Error.

> **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.

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. Operational outages caused by Human Error have a significantly increasing trend; however, the number of these events are very small (less than 0.01 outages per circuit) (see **Figure 5.8**).

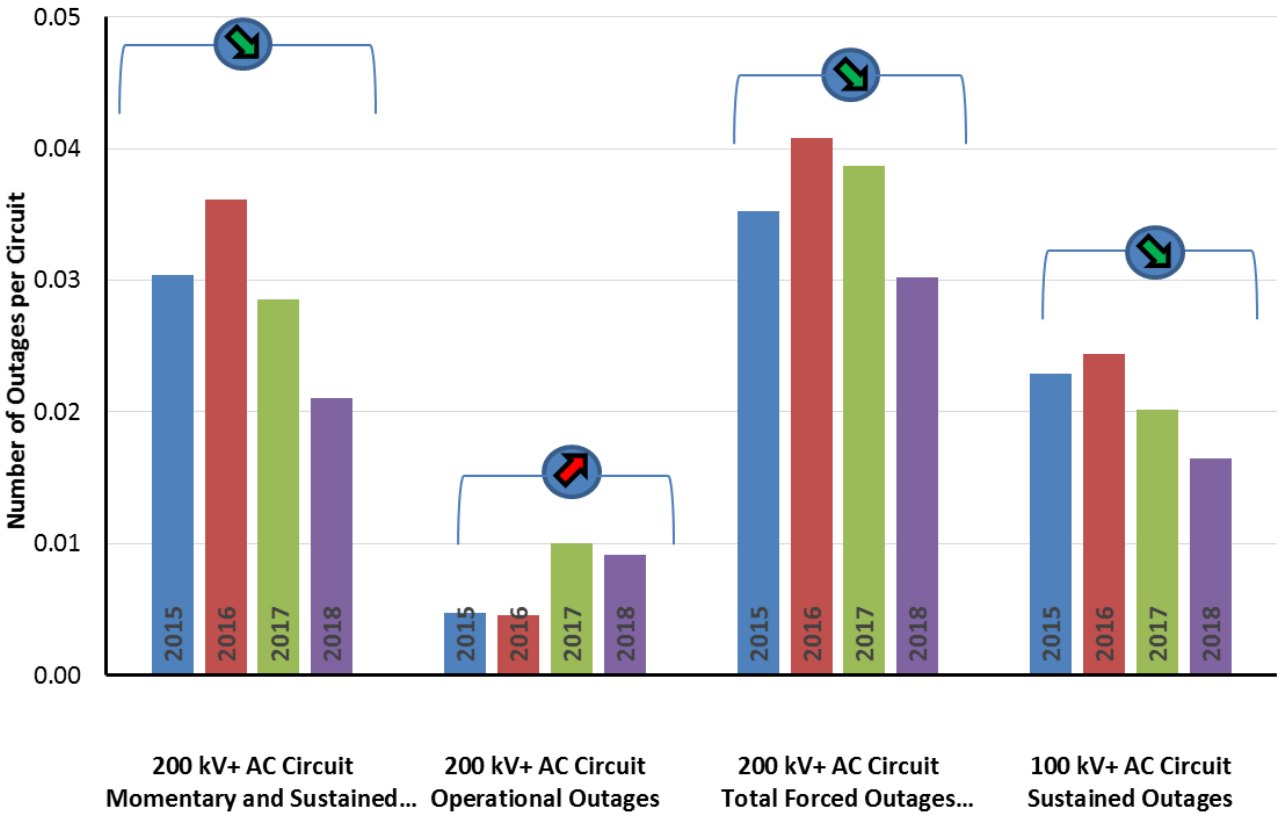


Figure 5.8: Transmission Outages Initiated by Human Error

Human Performance and Generation Outages

NERC GADS collects performance data generation outages due to Human Error (see **Figure 5.9**). GADS is able to calculate the amount of potential production lost due to any particular cause code. Over the past five years, total potential production loss has decreased for all fuel types and shows an improving performance trend. While the total potential electricity production loss is relatively small (21 TWH out of 4,300 TWH), the total reduction in Human Error-

related outages may be due to a decreasing coal-fired generation fleet. Staff shortage errors have greatly reduced over the analysis period and there has been a marked reduction in procedural human errors across all fuel types.

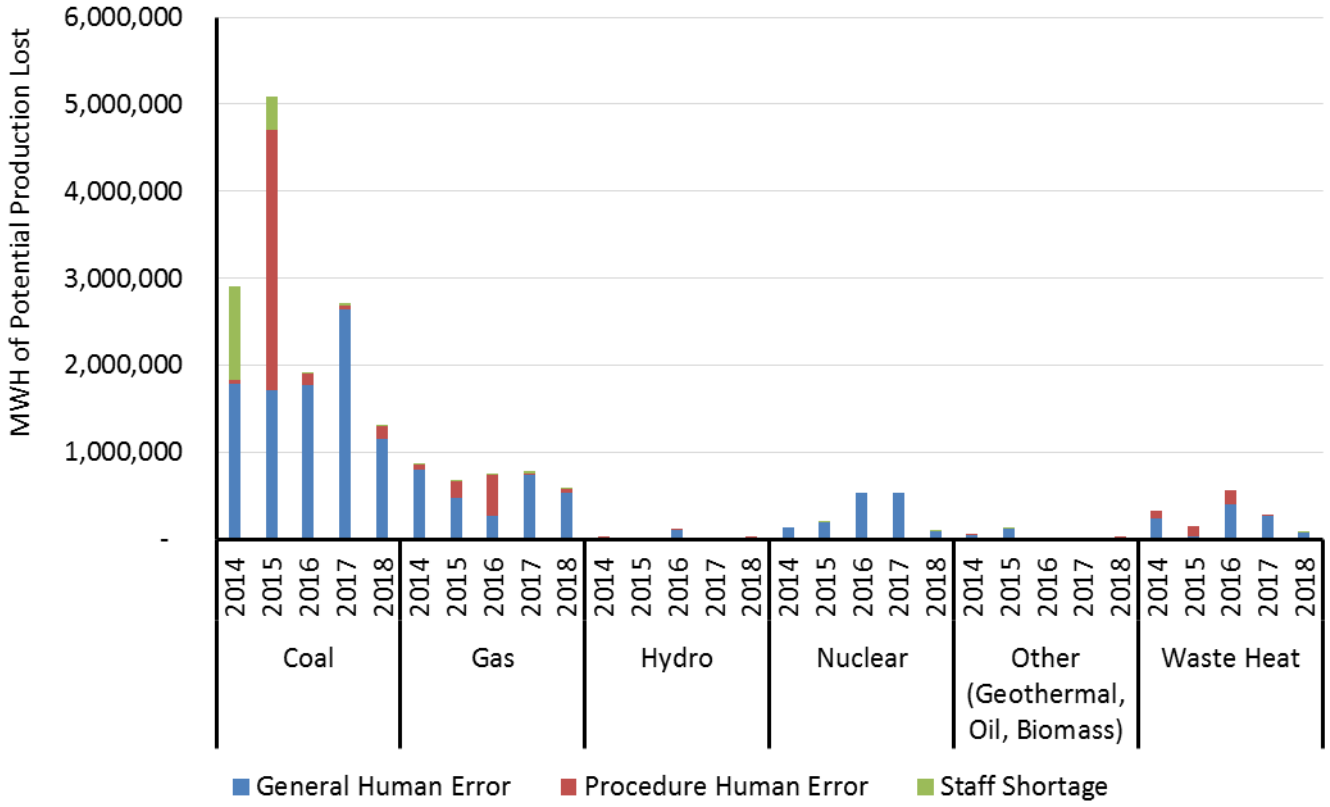


Figure 5.9: Potential Production Lost due to Forced Outages Caused by Human Error

Trends of Events Involving Human Performance as a Root or Contributing Cause

Management or Organization Challenges is an overarching set of event cause codes. Of all events in 2018, a total of 76 involved HP (see **Figure 5.10**). This is down from 113 in 2017, and as high as 174 in 2014. The top 5 detailed root cause codes for 2014–2018 time frame are the following:

- Job scoping did not identify special circumstances and/or conditions
- System interactions not considered or identified
- Risks/consequences associated with change not adequately reviewed/assessed
- Means/methods not provided for assuring adequate quality of contract services
- Inadequate work package preparation

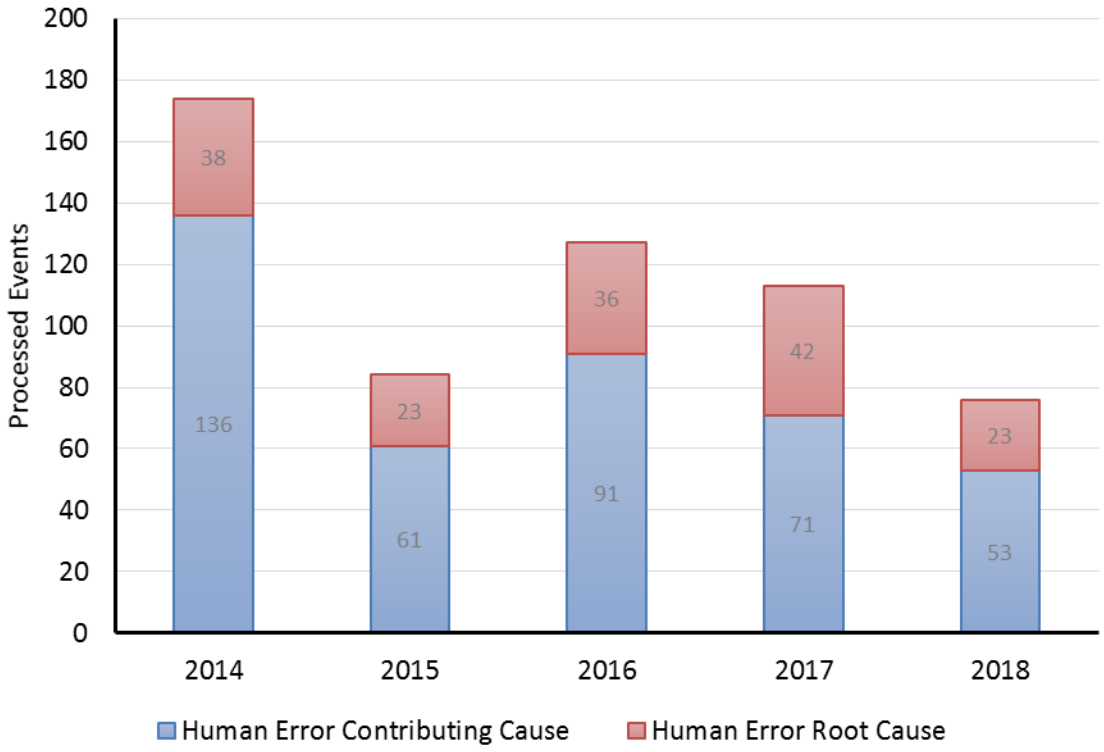


Figure 5.10: Human Error Root and Contributing Causes by Year, 2014–2018

Human Error and Protection System Misoperations

Figure 5.11 shows the number of misoperations due to the two different types of Human Error categorized by NERC: 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 setting, 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 setting 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.

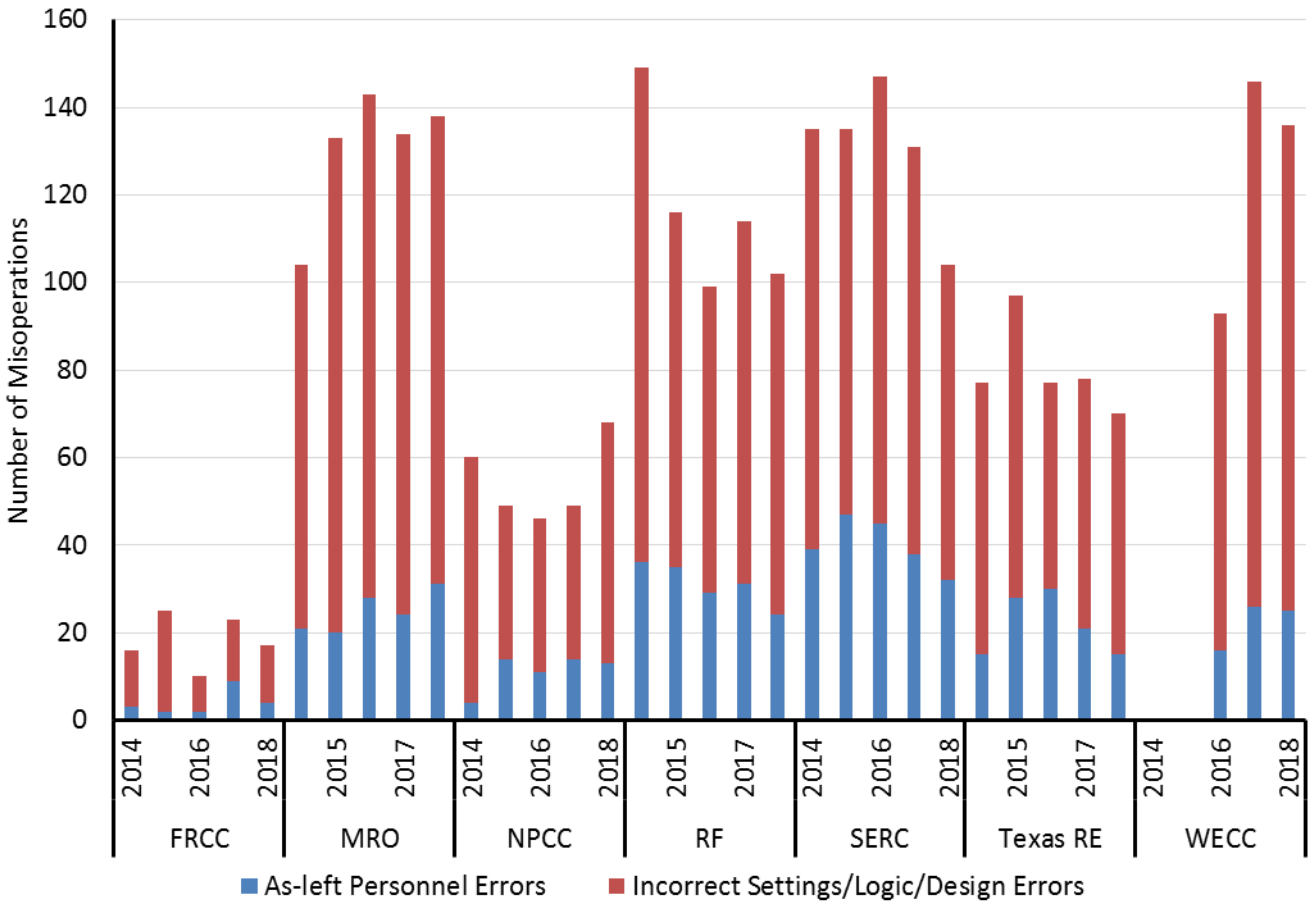


Figure 5.11: Protection System Misoperations Due to Human Error by Region, 2014–2018

Assessment

The ERO has identified work force capability and HP challenges as possible threats to reliability. Workforce capability and HP is a broad topic but can be divided into management, team, and individual levels.

NERC and the North American Transmission Forum (NATF) held the seventh annual HP conference in Atlanta, Georgia, improving Human Performance and Increasing Reliability on the BPS, at the end of March 2018. RF conducted a workshop specifically looking at Human Error and its relation to protection system misoperations.

Actions and Mitigations in Progress

- Annual NERC/NATF Human Performance Conference
- Event Cause Analysis training
- Monitoring and Situational Awareness Conference

Recommendations

The ERO and the forums should continue to focus on HP training and education through conferences and workshops that increase knowledge and provide information to further mitigate risk scenarios related to transmission and generation outages.

Loss of Situation Awareness

Situational awareness is necessary to maintain reliability, anticipate events, and respond appropriately when or before they occur. Without the appropriate tools and data, system operators may have degraded situational awareness for making decisions that ensure reliability for the given state of the BES. Certain essential functional capabilities must be in place with up-to-date information for staff to make informed decisions. An essential component of monitoring and situational awareness is the availability of information when needed. Unexpected outages of functions 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, energy management systems (EMSs) are an essential component of their situational awareness.

Impacts from the Loss of EMS

An EMS is a system of computer-aided tools 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, Real-Time Contingency Analysis, and/or Alarm Management.

While failure of a decision-support tool has not directly led to the loss of generation, transmission lines, or customer load, such failures may hinder the decision-making capabilities of the system operators 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.

The number of Category 1h events (loss of monitoring or control) has been stable for the last five years (see **Figure 5.12**).[37] Based on the 318 events reported by 130 registered entities from October 2013 to April 2017, the average outage time was 73 minutes, and the actual EMS availability was 99.99%.[38] Further, there were no reported EMS-related events that have caused loss of load.

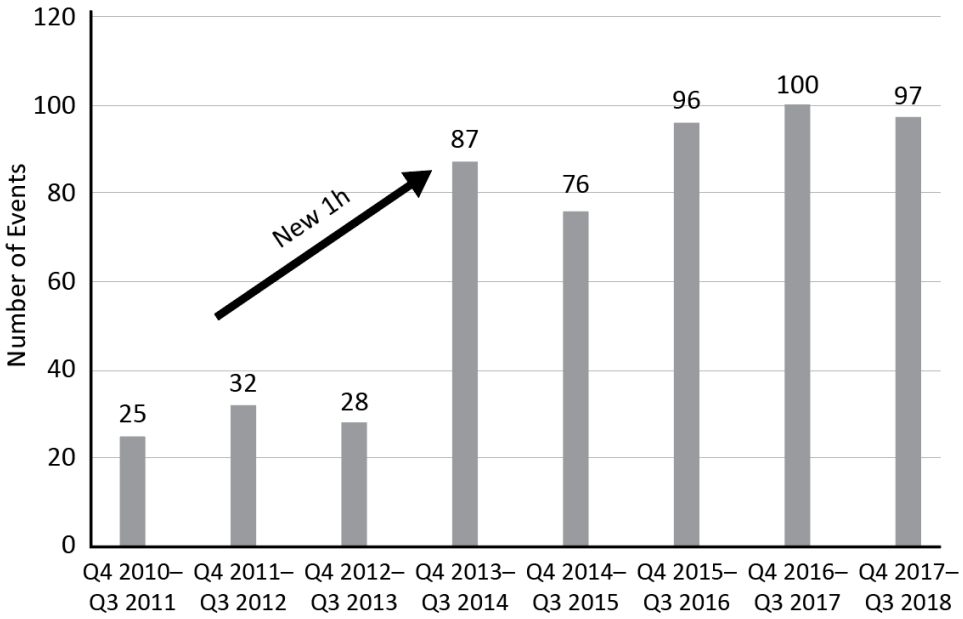


Figure 5.12: Number of EMS-related Events (Q4 2010 through Q3 2018)

[37] The significant increase of events between 2013 and 2014 was due to a new reporting criteria within the EAP for Category 1h events.

[38] Does not include all of 2018 due to data availability at time of publishing.

Failure Types Associated with Loss of EMS

Reliability risk varies (see **Figure 5.13**) depending on the function that is lost plus the duration of that outage, listed as follows:

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

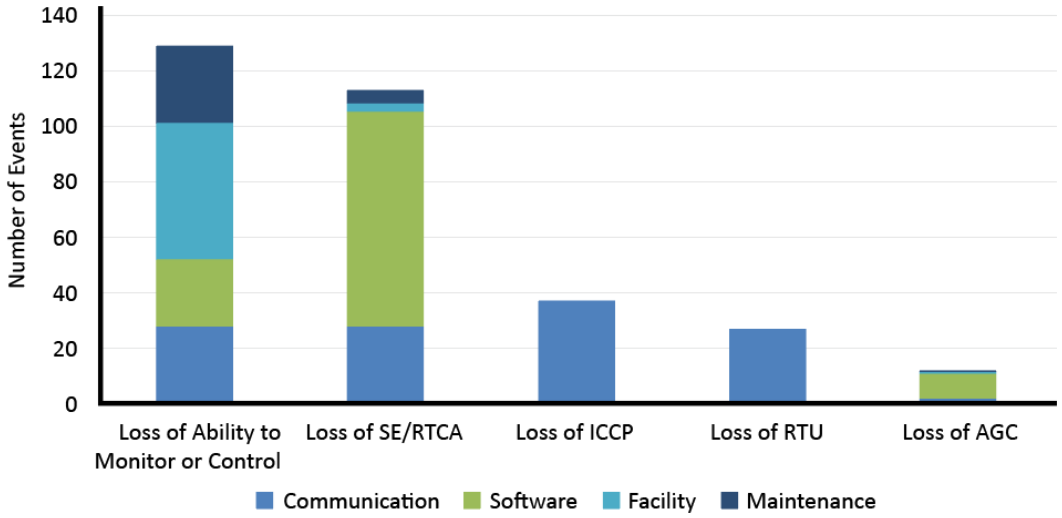


Figure 5.13: Number of EMS Events per Loss of EMS Functions (Q3 2013 through Q1 2017)

Largest Contributor to Loss of EMS

Reported EMS events can be grouped by the following attributes:

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

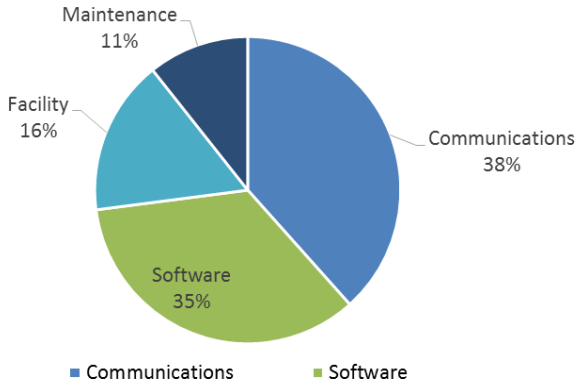


Figure 5.14: Contributors to Loss of EMS functions (Q3 2013 through Q1 2017)

Over the evaluation period from Q3 2013 through Q1 2017, outages associated with communications and software challenges contribute to the leading causes of EMS outages.

Assessment

In terms of EMS, software and telecommunications 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, such failures may hinder the decision-making capabilities of the system operators 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.

The Energy Management Working Group (EMSWG) published a reference document, *Risks and Mitigations for Losing EMS Functions Reference Document,*[39] 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 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. The continued active sharing of this group has reduced the residual risk associated with the potential loss of situation awareness and monitoring capability that comes with an EMS outage.

Actions and Mitigations in Progress

- The EAP allows 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.
- The NERC Monitoring and Situational Awareness Conference provides a forum to share knowledge.

Recommendations

- Electric utilities should develop and implement the system recovery and restoration plans, including drills and training on the procedures plus real-life practice implementing the procedures.
- Electric utilities should utilize offline tools (studies) to analyze contingencies plus other contingency-analysis, including day-ahead studies, seasonal and standing operating guides, and system operator training.
- 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.
- 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.

Physical Security and Cyber Security

Physical and cyber security issues remain a priority for NERC for the foreseeable future. Cyber threats are becoming more sophisticated and increasing in number. Exploitation of cyber vulnerabilities can result in loss of control or damage to utility voice communications, data, monitoring, protection and control systems, and tools. The potential for cyber or physical attack on natural gas infrastructure highlights the need for increased coordination among pertinent ISACs and the industry to improve response and recovery times due to the interdependency of the natural

[39] *Risks and Mitigations for Losing EMS Functions Reference Document*: http://www.nerc.com/comm/OC/ReferenceDocumentsDL/Risks_and_Mitigations_for_Losing_EMS_Functions_Reference_Document_20171212.pdf

gas and electricity system. Interdependency and increased reliance on third-party service providers, cloud-based services, and the supply chain expands the attack surface and associated risk for potential cyber vulnerabilities. The increasing digitization of the distribution system and internet-connected loads further expands the attack surface physically and logically, increasing risk to the BPS.

2018 Physical Security Events

In 2018, voluntary sharing with the E-ISAC of incident information, or additional details about an incident reported through mandatory reporting, occurred in 60% of the 207 incidents. The total number of incidents increased 5.3% from 2017 to 2018 (see **Figure 5.15**). Surveillance incidents included drone activity, overflights by airplane and helicopter, and unusual photography. Suspicious activity included incidents like trespassing, social engineering,[40] and suspicious objects. Theft incidents predominately targeted copper, but a significant amount of equipment and tool theft occurred as well. A total of 6 threat incidents were shared in 2018, consisting of bomb and activist threats. Some of these were targeted at the sector in general and not at specific members. No actual explosives were found in any of the reported incidents. There were 13 vandalism incidents in 2018, though it is worth noting that theft commonly involves some measure of vandalism as well. For the 2 "other" incidents, one saw a car crashing into a utility's front gates while fleeing from law enforcement, and in the other a tree cut with a chainsaw fell into a transmission line (this was considered to be an isolated event). A total of 41 gunfire incidents were reported, most commonly involving transmission lines and solar photovoltaic generation sites.

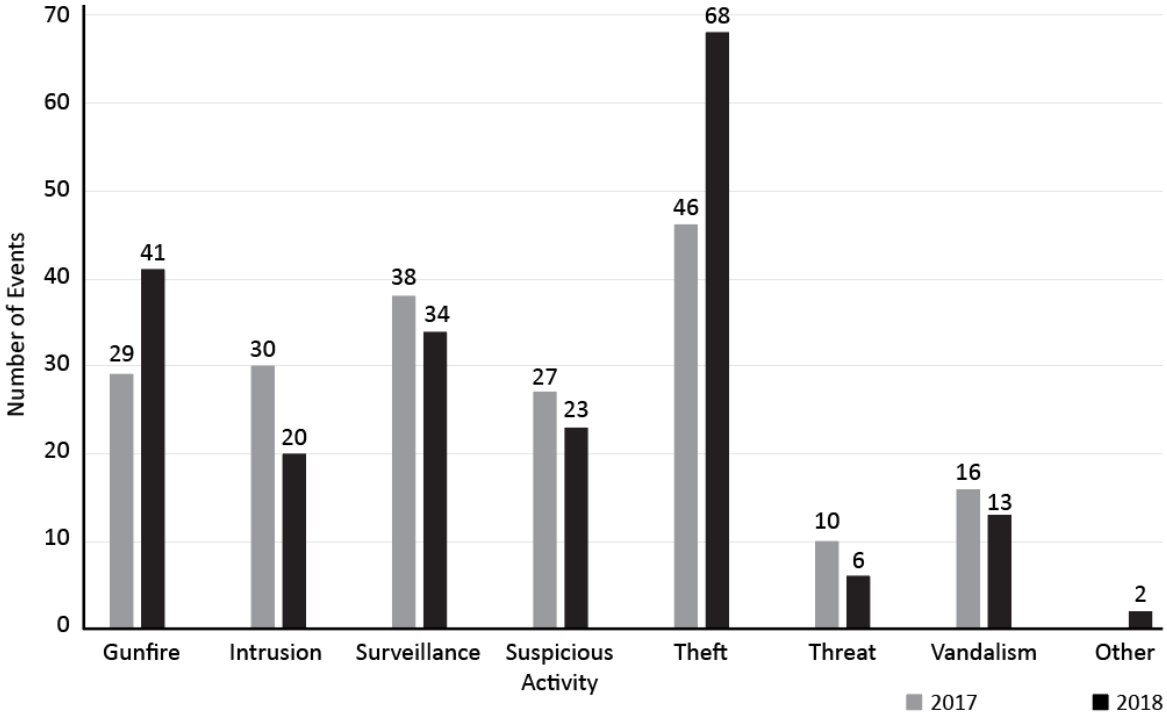


Figure 5.15: 2018 Physical Security Incidents

Regionally, the most incidents occurred in WECC and the least in Texas RE (see **Figure 5.16**). The number of incidents in the map add up to less than 207 because some incidents in 2018 involved the sector, and not a specific Region or lacked specific location data.

[40]Social Engineering is defined by NIST as the act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust. https://csrc.nist.gov/glossary/term/social-engineering

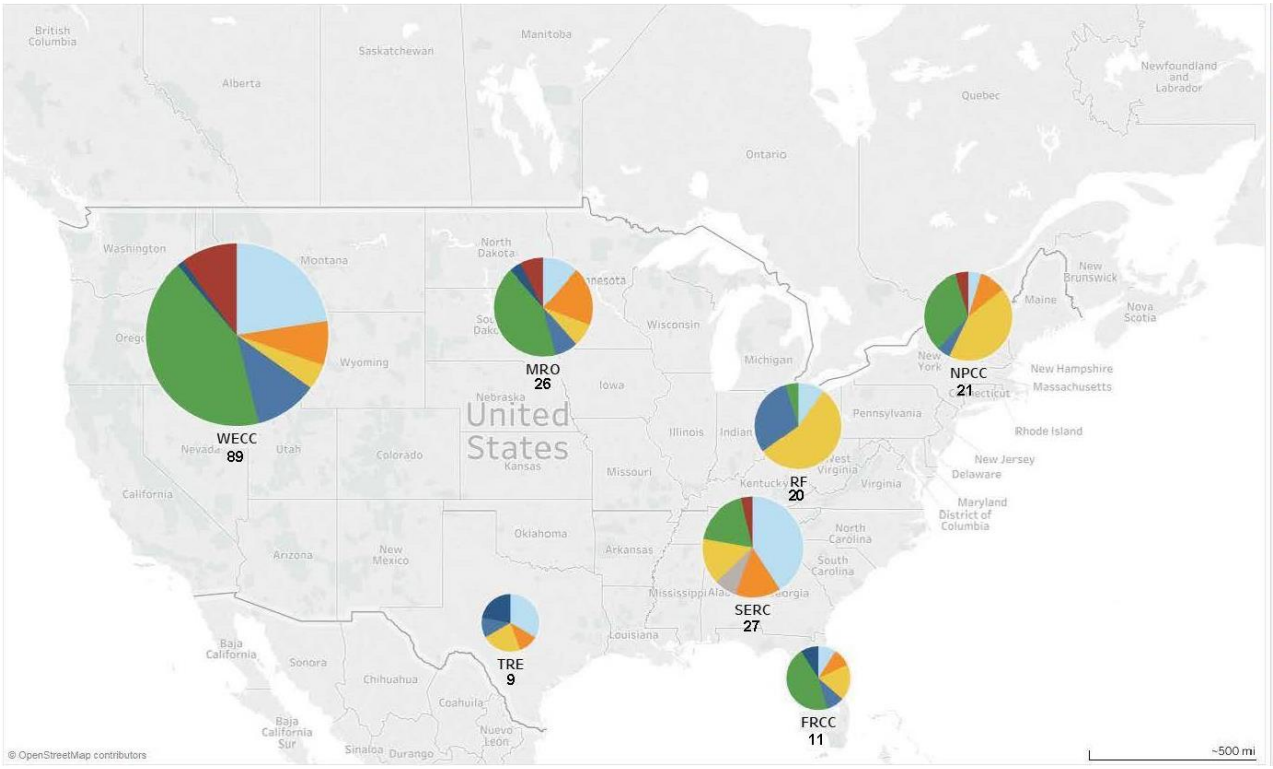


Figure 5.16: 2018 Physical Security Incidents by Region

Most Prominent Cyber Security Threats

This section covers the most prominent cyber security threats. **Figure 5.17** shows the reported cyber security incident by delivery mechanism.

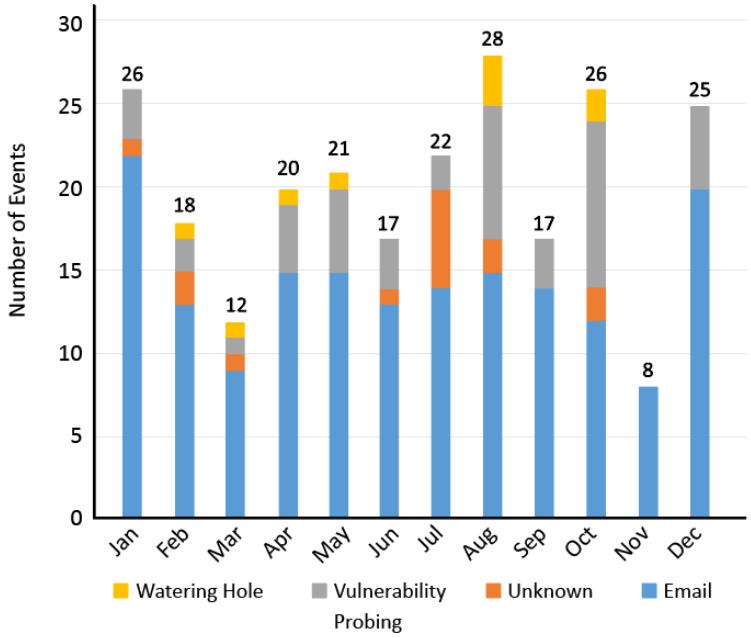


Figure 5.17: 2018 Cyber Security Incidents by Delivery Mechanism

Trusted Third-Party Phishing

One of the most common cyber attacks reported in 2018 was phishing emails received through trusted third parties (e.g., law firms, suppliers, solution providers) where the information technology (IT) networks were compromised.

The phishing emails are typically sent to the third-party victim's contact list or as a reply to the most recent conversations to increase the likelihood the recipient will believe the email came from a trusted source. Since the source is a seemingly legitimate organization, security solutions that perform anti-spoofing or spam filtering are less effective. While this type of phishing is prolific, it usually has little more sophistication than normal spam phishing.

Advanced threat actors continue to target third-party organizations with the intent to craft highly targeted phishing emails that are difficult to detect. This attack method was used to great effect during the campaign disclosed by the Department of Homeland Security and the FBI in 2017 and 2018, where Russian government-sponsored threat actors conducted network reconnaissance, gained access to IT networks, and collected information pertaining to industrial control systems in several energy sector organizations. This campaign involved stealing credentials through the Server Message Block (SMB) protocol to gain network access. While targeting SMBs has fallen out of favor for most threat actors—mostly due to many organizations monitoring outbound SMB traffic—credential harvesting remains one of the top attack methods.

Cryptojacking and Ransomware

Early 2018 saw the peak of many cryptocurrency prices that caused an explosion in cryptocurrency mining, including malicious cryptocurrency mining, which is referred to as cryptojacking. Around the same time, tools like CoinHive were developed to lower the barrier of entry to mining coins in a distributed manner. Although CoinHive was originally created as an alternative to online ads, malicious actors repurposed and embedded it into compromised websites.

Financially motivated criminals shifted focus from ransomware in 2017 to cryptojacking in 2018:

- Ransomware campaigns require staff support to guide victims through how to purchase cryptocurrency and send it to the malicious actors.
- Ransomware is quick and easy to detect due to its disruptive nature. To continue to bypass automated security systems, new ransomware variants have to be continually developed. Comparatively, cryptojacking incidents typically seek to avoid detection by using only a small portion of the victim's computer processing power to mine currency.

While most cryptojacking infections will not make the target system unusable, infected hosts are still negatively impacted. Prolonged operations of cryptominers can burn out components, requiring more frequent replacement, and some cryptojacking malware ignores stealth—by design or poor coding—and uses all available processing power, effectively causing a denial-of-service condition on the system.

Throughout 2018, many cryptocurrency prices have fallen drastically, to an eighth of their initial values in some cases. There is a distinct relationship between the price of popular cryptocurrencies and the level of detected cryptojacking activity. If the price and popularity of cryptocurrency continues to fall, financially motivated criminals will most likely shift their focus to other techniques, such as ransomware or banking Trojan malware.

Malware Frameworks

In 2018, many familiar malware families (e.g., Shamoon and GreyEnergy, the successor to BlackEnergy) saw new variants while other frameworks, like VPNFilter, first appeared. Each time a new malware framework is discovered, the E-ISAC works with a variety of government and private sector partners to deliver actionable and timely information to the industry. For example, in the case of VPNFilter, the E-ISAC leveraged its partnership with Dragos to quickly dispel concerns regarding the Modbus module's capabilities. The threat, however, is clear: advanced attackers continue to develop highly modular tools with the ability to greatly impact a targeted system.

Modular malware offers allows attackers faster development time and the ability to avoid analyst scrutiny. Instead of having to rewrite large swaths of code every time the malware's functionality needs to be changed or a new system

is targeted, the developers are compartmentalizing malware into functional pieces that can be easily swapped out. This also allows attackers to only deliver the final payload of the malware right before it is to be executed on the target system. If an entity discovers the malware before this time, defenders are left without the context behind the attack; likewise, unused modules remain viable for future use.

While modular malware is not new, it is becoming increasingly popular across all attacker skill levels. Criminal organizations are increasingly using common malwares like Emotet and Pony Loader to perform initial infections and then delivering the intended payload after establishing a foothold in a system. While highly specialized tools, like GreyEnergy and TRISIS, can allow advanced threat actors to impact specific systems, hiding behind common malware like Emotet can make differentiating hostile activity from standard operations more difficult.

Assessment

In 2018, as in previous years, there were no reported cyber or physical security incidents on BES facilities that resulted in a loss of load. This is the single most important security measure because it 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. Nonetheless, grid security (particularly cyber security) is an area where NERC and industry must continually improve defenses as threats and technologies continue to rapidly evolve.

The most prominent cyber and physical security threats affecting industry from January to December 2018 included gunfire, theft, cryptojacking, phishing, and malware. The cyber security threat landscape constantly changes, and members must be vigilant while staying informed about adversaries' latest tactics, techniques, and procedures. While many physical security threats and impacts remain similar from year-to-year, the threat from activist groups continues to evolve as they become more capable.

Continuing cyber threats include the following:

- **Supply Chain:** The supply chains for information and communications technology and industrial control systems may provide various opportunities for adversaries to initiate cyber attacks.
- **Credential Harvesting:** Tactics to acquire legitimate user credentials to gain initial access to targeted networks and establish persistence mechanisms will continue to be popular because they help actors evade detection. Sophisticated spear phishing activity to harvest credentials is the most common technique observed by members.
- **Exploitation of the Trust Relationship between Targeted Organizations and their Business Partners:** Recent incidents have demonstrated that nation-state adversaries are targeting the industry and other industries by compromising the networks of third-parties with which the intended targets have established business relationships. This tactic is a type of supply chain attack and increases the success rate of tactics used to initially compromise the intended target.
- **Network Device Targeting:** From the high-profile reports on VPNFilter to the state-sponsored actors targeting network devices in North America, switches and routes located on the edge of networks are a prime target for threat actors capable of intercepting and processing a large amount of information. Because these devices are placed at the boundary between internal networks and the internet and exist to allow controlled access to the internal network, these devices will most likely continue to be a target of reconnaissance.
- **Use of Native Tools:** Adversaries will likely continue to use tools and capabilities already present on a compromised network, such as PowerShell or Windows Management Infrastructure, to conduct reconnaissance, lateral movement, and privilege escalation. The presence or use of these tools on a targeted network is unlikely to raise alarm, so their inappropriate use helps evade detection.

Continuing physical threats include the following:

- **Gunfire Damage:** Vandalism due to gunfire damage in the southern and western regions 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.
- **Theft**: Theft is likely to continue at similar levels in 2019. This is particularly copper-related theft, but equipment and tool theft are also likely. The amount of theft can be influenced by the price of copper and local labor conditions.
- **Threats:** Activist group threats are likely to remain relatively constant this year. Lawful protests by activist groups targeting a utility can prove disruptive and costly and increase the likelihood of vandalism and sabotage. Activist-led social media campaigns dominated 2018; however, these campaigns have the potential to rapidly escalate to direct action and physical damage. 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 sector has been expressed by various ideological groups and should not be discounted, especially when undertaking facility construction or building transmission lines.
- **Unmanned Aerial Systems:** The proliferation and capabilities of unmanned aerial systems, often known as "drones," pose an increasing threat to the sector. Drone technology continues to improve, making drones cheaper, more capable, user-friendly, and of great benefit to the electricity industry, but they can be used to cause considerable harm, even by a nonmalicious user. 2018 saw an increase in the capability exhibited by malicious actors using drones as seen in the incidents at Gatwick and Heathrow airports in London in December 2018 and January 2019. Though these did not target the electricity industry, they do show an evolution in capability. They also highlight difficulties in response procedures under current law.

Actions and Mitigations in Progress

- The E-ISAC reduces cyber and physical security risk to the electricity industry by providing unique insights, leadership, and collaboration.
- The Cybersecurity Risk Information Sharing Program (CRISP) facilitates timely bidirectional exchange of cybersecurity information among industry, the E-ISAC, and the Department of Energy to enable owners and operators to better protect their systems from sophisticated cyber threats.
- NERC is publishing an Alert with regards to the use of certain foreign manufacturers of electronic equipment and software, including communications hardware and unmanned aerial systems.
- GridEx provides participants an opportunity to demonstrate, practice, and improve their responses to a combined cyber-physical attack.
- The NERC CIP Standards provide a common foundation of solid defenses for the BES.

Recommendations

- Revise the supply chain standards to address electronic access control or monitoring systems (EACMSs) that provide electronic access control (excluding monitoring and logging) to high and medium impact BES cyber systems.
- Revise the supply chain standards to address physical access control systems (PACSs) that provide physical access control (excluding alarming and logging) to high- and medium-impact BES cyber systems.
- Further studies are needed to determine whether new information supports modifying the standards to include low-impact BES cyber systems with external routable connectivity as follows: first, by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure; and second, by continued monitoring of the application of the criteria in CIP Reliability Standards that differentiate medium impact BES cyber systems from low impact.

- 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.
- E-ISAC should continue aggressive and detailed execution of its strategic plan, guided by the ESCC's Member Executive Committee.
- Public-private partnerships that pursue data exchanges used to increase security awareness to develop collaborative security analytics should be strengthened.
- 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 Department of Energy.

Resilience and Recovery from Extreme Natural Events

Resilience and recovery actions can mitigate exposure from multiple risks. This is particularly important as threats to electricity industry infrastructure from cyber and physical attacks are expected to increase, and customers and regulators have increasing expectations on the continuity of electric service. While this report addresses ways to address specific risks, not all possible risks can be anticipated or mitigated. Efforts and resources expended on resilience and recovery can address a wide range of risks and can also limit the extent of extreme or low-likelihood incidents. Resilience assessments in the planning and operating processes should be pursued to support BPS reliability.

Transmission Performance during Extreme Periods in 2018

"Extreme days" are based on the eight most impactful days determined by the daily transmission loss measure (found in the **Severity Risk Index** section). See **Figure 4.7** for a list of the most extreme days. **Figure 5.18** shows the top causes of transmission line outages during these extreme days.

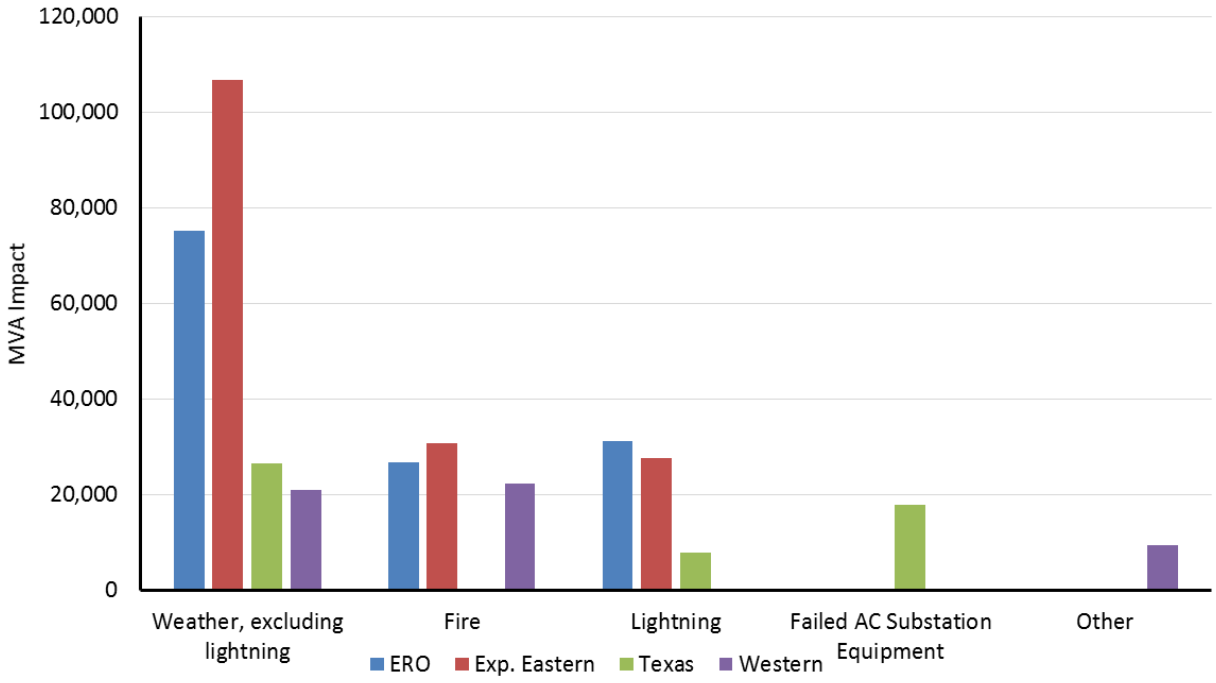


Figure 5.18: Top Transmission Outage Causes on Extreme Days in 2018

Conventional Generation Fleet Performance during Extreme Periods in 2018

"Extreme days" are based on the eight most impactful days determined by the daily generation loss measure (found in the **Severity Risk Index** section). See **Figure 4.8** for a list of the most extreme days. **Figure 5.19** shows the top causes of conventional generation outages during these extreme days.

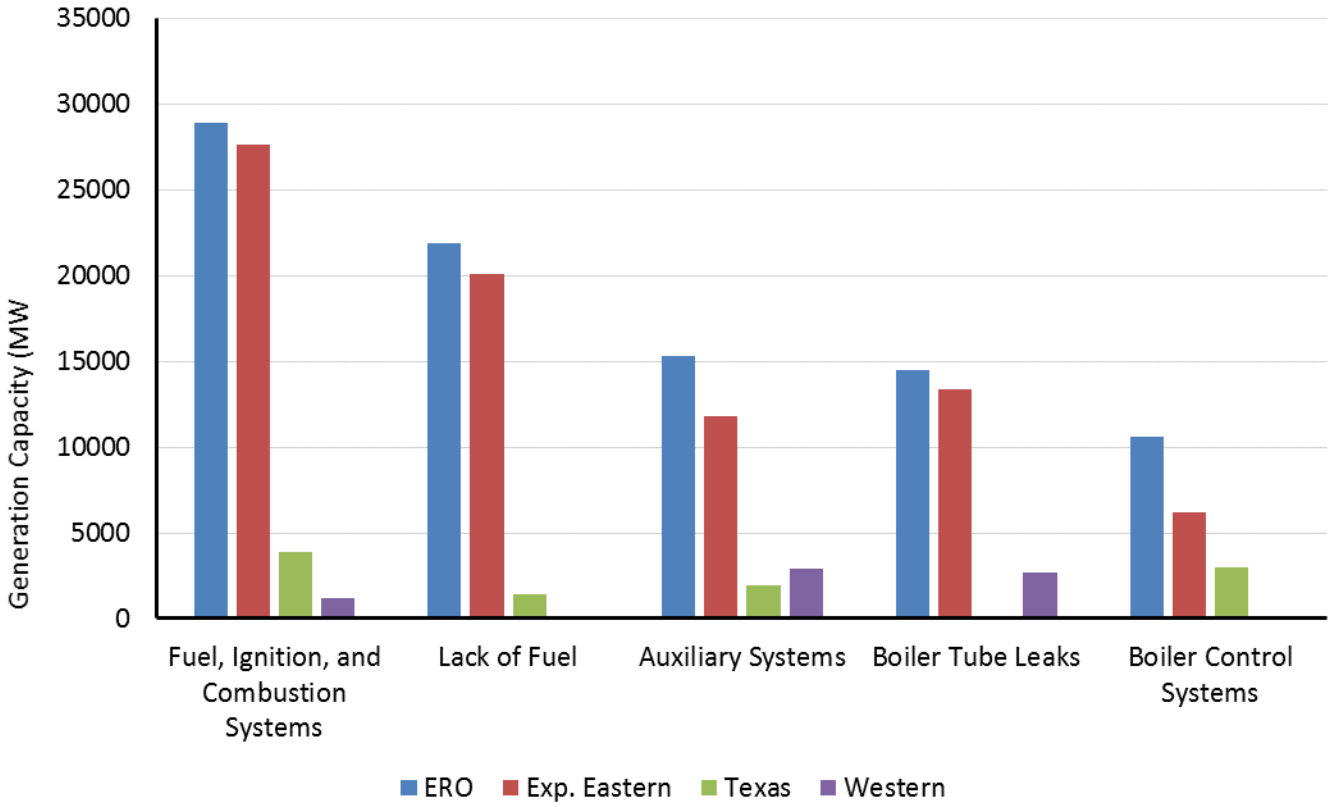


Figure 5.19: Top Generation Outage Causes on Extreme Days in 2018

Transmission Recovery during Extreme Periods Compared to Average Performance

Based on an analysis of TADS data, the duration of sustained transmission outages in each Interconnection is shorter than the average sustained outage event duration in their associated Interconnection (see **Figure 5.19**) and lower than the average sustained outage event duration for all of NERC (39 hours, not shown). This is evidence of extreme weather preparation, crew staging, mutual assistance, and recovery of in-service transmission. On an extreme day, there are many transmission outage events, but they are usually not long in durations. Recovery is quick and on average about 60% shorter than all other non-extreme days.

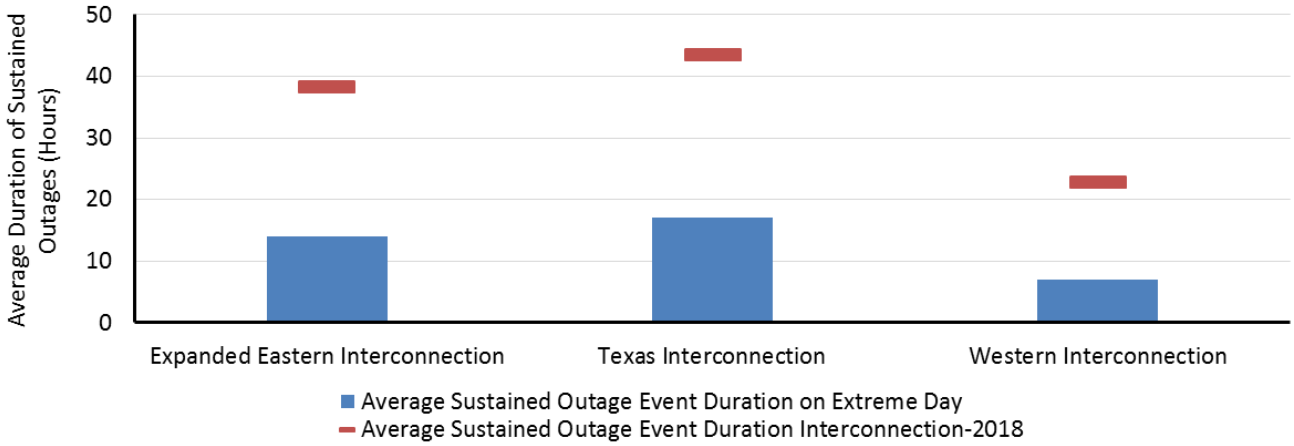


Figure 5.20: Average Sustained Transmission Outage Events for 2018 and Most Extreme Days

Table 5.1: 2018 Extreme Day Transmission Performance Compared to Average Performance

Interconnection	2018 Largest Transmission Loss (% share of total MVA)	Date	Number of Sustained Transmission Outage Events On Extreme Day	Leading Causes for Extreme Day	Average Sustained Outage Event Duration on Extreme Day	Longest Sustained Outage Event Duration on Extreme Day	Average Sustained Outage Event Duration 2018	Longest Sustained Outage Event Duration 2018
Expanded Eastern Interconnection	0.351	4/14	77	Weather	14 hours	111 hours	38 hours	8,760 hours
Texas Interconnection	1.586	1/16	46	Weather	17 hours	72 hours	44 hours	6,403 hours
Western Interconnection	0.815	8/11	34	Fire; Lightning	7 hours	23 hours	23 hours	2,184 hours

Assessment

Resilience and recovery actions can mitigate exposure from multiple risks. This is particularly important as threats to electricity industry infrastructure from cyber and physical attacks are expected to increase, and customers and regulators have increasing expectations on the continuity of electric service. Efforts and resources expended on resilience and recovery can address a wide range of risks and can also limit the extent of extreme or low-likelihood incidents. Resilience assessments in the planning and operating processes should be pursued to support BPS reliability.

Extreme conditions can push BPS equipment and resources to certain limits. It is important that these limits, such as fuel energy limitations or ambient temperatures, are well known and communicated with both system planners and operators.

Based on the SRI measures, 2018 had relatively high performance compared to prior years, and there has been an overall improve in generation and transmission performance.

Actions and Mitigations in Progress

- The NERC EAP emphasizes cold weather preparation on an annual basis in the late summer for the upcoming winter season.

- A cold weather preparation webinar is provided each year in addition to a standard online training package and other resources. In September 2018, the theme of the webinar was "Preparing Breakers for Cold Weather and Failure Modes and Mechanisms."

Recommendations

- Enhanced system restoration plans should be implemented, including drills and training on the procedures and real-life practice of procedure implementation.
- Mutual assistance agreements provide essential personnel, equipment, and material following extreme weather events. NERC encouraged participation with assistance from government and nongovernmental authorities where applicable.
- Coordination with government and first responders is critical for successful drone use. NERC, in collaboration with the industry, should publish a lesson learned to guide more effective drone use and inform government regulatory agencies that increased drone use can increase grid reliability.

Appendix A: 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: Noman Williams, GridLiance
Operating Committee	Chair: Lloyd Linke, WAPA Vice Chair: David Zwergel, MISO
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: Rich Hydzik, Avista Corporation Vice Chair: Vinit Gupta, ITC
Generation Availability Data System Working Group	Chair: Leeth DePriest, Southern Company Vice Chair: Steve Wenke, Avista Corporation
Transmission Availability Data System Working Group	Chair: Kurt Weisman, ATC Vice Chair: Brian Starling, Dominion
Resources Subcommittee	Chair: Tom Pruitt, Duke Energy Vice Chair: Sandip Sharma, ERCOT
Operating Reliability Subcommittee	Chair: Dave Devereaux, IESO Vice Chair: Chris Pilong, PJM
Frequency Working Group	Chair: Danielle Croop, PJM
Reliability Assessment Subcommittee	Chair: Tim Fryfogle, Reliability First Vice Chair: Lewis DeLarosa, Texas RE
System Protection and Control Subcommittee	Chair: Mark Gutzmann, Xcel Energy Vice Chair: Jeff Iler, AEP

NERC Staff	
Name	**Title**
Mark Lauby	Senior Vice President and Chief Reliability Officer
James Merlo	Vice President and Director, Reliability Risk Management
John Moura	Director, Reliability Assessment
David Till	Senior Manager, Advanced System Analysis and Modeling
Brad Gordon	Senior Manager, Power System Analysis
Svetlana Ekisheva	Senior Manager, Statistical Analysis and Outreach
Kwame Jones	Senior Data Analyst, Performance Analysis
Jack Norris	Engineer, Performance Analysis
Vivian Madu	Data Analyst, Performance Analysis
Margaret Pate	Program Liaison, Performance Analysis
Donna Pratt	Manager, Performance Analysis
Elsa Prince	Principal Advisor, Power System Analysis
Lee Thaubald	Technical Analyst, Performance Analysis
Matthew Varghese	Senior Engineer, Power System Analysis
Matthew Lewis	Manager of Event Analysis, Reliability Risk Management
Andy Slone	Senior Engineer of Event Analysis, Reliability Risk Management
Richard Hackman	Senior Event Analysis Advisor, Reliability Risk Management
Wei Qiu	Senior Engineer of Event Analysis, Reliability Risk Management
Rich Bauer	Associate Director, Event Analysis
Darrell Moore	Associate Director, Bulk Power System Analysis
Terry Campbell	Manager, Technical Publications
Alex Carlson	Senior Technical Publications Specialist
Sam Chanoski	Director, Threat Intelligence and Countermeasures
Bob Cummings	Senior Director, Engineering and Reliability Initiatives
Howard Gugel	Vice President and Director, Engineering and Standards
Kimberly Mielcarek	Senior Director, Communications
Ryan Quint	Senior Manager, System Analysis
Janet Sena	Senior Vice President, Policy and External Affairs
Sandy Shiflett	Senior Program Specialist
Jule Tate	Associate Director, Event and Performance Analysis

Appendix B: Compilation of Recommendations

Table B.1: 2018 State of Reliability Recommendations	
Long-Term and Strategic Recommendations	
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 • Resource adequacy with increasing energy constraints	
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, and preparing for the next event) during the most extreme events and how system performance changes over time.	
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.	
Recommendations to Address Priority Risks	
BPS Planning and Adapting to the Changing Resource Mix	The ERO Enterprise and industry should continue to expand the use of probabilistic approaches to develop resource adequacy measures that reflect variability and overall reliability characteristics of the resources and composite loads, including, but not limited to, energy and fuel constraints, energy storage, and DERs.
	NERC, working with the industry and forums, should develop guidelines and good industry practices for developing and maintaining accurate system and electromagnetic models, including resources, load, and controllable devices that provide essential reliability services.
Increasing Complexity in Protection and Control Systems	The ERO should work with industry experts and the forums 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 determine if there is an increasing reliability risk due to the different short-circuit contribution characteristics of inverter-based resources.
	The Misoperations Data Collection program should be enhanced by refining the data reporting instructions to improve overall data quality and consistency.
Human Performance and Skilled Workforce	The ERO and the forums should continue to focus on HP training and education through conferences and workshops that increase knowledge and provide information to further mitigate risk scenarios related to transmission and generation outages.

Table B.1: 2018 State of Reliability Recommendations	
Loss of Situation Awareness	Electric utilities should develop and implement the system recovery and restoration plans, including drills and training on the procedures plus real-life practice implementing the procedures.
	Electric utilities should utilize offline tools (studies) to analyze contingencies and other contingency-analysis, including day-ahead studies, seasonal and standing operating guides, and system operator training.
	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.
	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 on their facilities to maintain the reliability of the BES.
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 continue aggressive and detailed execution of its strategic plan, guided by the ESCC's Member Executive Committee.
	Public-private partnerships that pursue data exchanges used to increase security awareness to develop collaborative security analytics should be strengthened.
	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 Department of Energy.
Resilience and Recovery from Extreme Natural Events	Enhanced system restoration plans should be implemented, including drills and training on the procedures and real-life practice of procedure implementation.
	Mutual assistance agreements provide essential personnel, equipment, and material following extreme weather events. NERC encouraged participation with assistance from government and nongovernmental authorities where applicable.
	Coordination with government and first responders is critical for successful drone use. NERC, in collaboration with the industry, should publish a lesson learned to guide more effective drone use and inform government regulatory agencies that increased drone use can increase grid reliability.