

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

State of Reliability 2017

June 2017

RELIABILITY | ACCOUNTABILITY



**3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com**

Table of Contents

Preface.....	v
Executive Summary	vi
Chapter 1: Key Findings and Recommendations.....	1
Chapter 2: 2016 Reliability Highlights	7
Essential Reliability Services	7
Single Point of Disruption	8
Renewable Penetration and Distributed Energy Resources.....	9
Grid Security	10
Electricity Information Sharing and Analysis Center	11
Chapter 3: Severity Risk Assessment and Availability Data Systems	12
Overview of Severity Risk Analysis	12
Overview of TADS Analysis	20
Overview of Generation Availability Data System (GADS) Data Analysis.....	23
Overview of Demand Response Availability Data System (DADS) Analysis.....	24
Chapter 4: Reliability Indicator Trends.....	26
Summary.....	26
M-2 BPS Transmission-Related Events Resulting in Loss of Load	27
M-9 Correct Protection System Operations	31
M-12 through M-14 Automatic AC Transmission Outages.....	35
M-15 Automatic AC Transmission Outages Initiated by Failed AC Circuit Equipment.....	40
M-16 Element Availability Percentage and Unavailability Percentage	41
Chapter 5: Enforcement Metrics for Risk and Reliability Impact	43
CP-1: Risk Metric.....	43
CP-2: Impact Metric	46
Chapter 6: Event Analysis.....	49
Background	49
Analysis and Reporting of Events.....	49
Major Initiatives in Event Analysis.....	54
Summary.....	57
Chapter 7: BES Security Metrics	58
Background	58
Measuring Security Risks	58
Beyond Standards and Compliance: The E-ISAC.....	59

Table of Contents

Cyber Security Risk.....	60
E-ISAC Member Engagement.....	62
Outlook for 2017 and Recommendations	63
Chapter 8: Actions to Address Recommendations in Prior State of Reliability Reports	65
Completed Recommendations	66
Ongoing Recommendations	69
Appendix A: Statistical Analysis of SRI Assessment.....	73
SRI Performance by Year	73
Performance of SRI Components by Year.....	75
Seasonal Performance of SRI	79
Appendix B: Statistical Analysis of Transmission Data	81
Study Method	81
Study 1: TADS Sustained and Momentary Events for 200 kV+ AC Circuits (2012–2016).....	86
Study 2: TADS CDM Events for 200 kV+ AC Circuits	92
Study 3: Regional Entity Transmission Analysis.....	95
Study 4: TADS Sustained Events of 100 kV+ AC Circuits (2015–2016).....	97
Study 5: Sustained Events for 100 kV+ AC Circuits and Transformers (2016).....	104
Study 6: Sustained Cause Code Study for Sustained Outages of 100 kV+ AC Circuits (2015–2016).....	110
Summary of TADS Data Analysis.....	113
Appendix C: Analysis of Generation Data.....	115
Generator Fleet Reliability	116
Forced Outage Causes	117
Appendix D: Analysis of Demand Response Data	122
Overview	122
Demand Response Programs.....	122
Demand Response: Reliability Events.....	125
DADS Metrics	130
Looking Ahead	136
Appendix E: Reliability Indicator Trends.....	137
M-1 Planning Reserve Margin.....	137
M-3 System Voltage Performance	138
M-4 Interconnection Frequency Response.....	138
M-6 Disturbance Control Standard Failures	169
M-7 Disturbance Control Events Greater than Most Severe Single Contingency (MSSC).....	169
M-8 Interconnection Reliability Operating Limit Exceedances	170

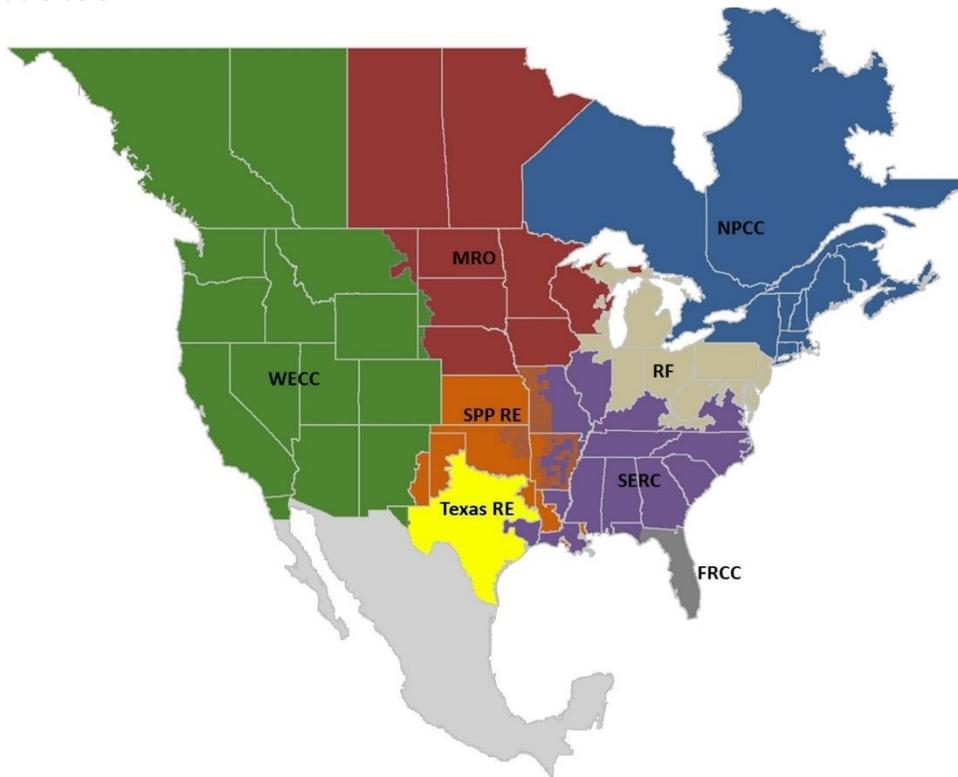
Table of Contents

M-9 Correct Protection System Operations	173
M-10 Transmission Constraint Mitigation	179
M-11 Energy Emergency Alerts	179
Appendix F: Statistical Significance Whitepaper	181
Theoretical Background	181
Examples from Performance Analysis	184
Reliability Indicator M-14: Outages Initiated by Failed Substation Equipment	184
Conclusion.....	185
Common Statistical Tests.....	186
References	186
Appendix G: Security Performance Metrics	187
Background	187
Purpose	187
NERC Alert Process and Security Incidents During 2016	187
Security Performance Metrics and Results.....	188
Roadmap for Future Metrics Development.....	194
Appendix H: Abbreviations Used in This Report	195
Appendix I: Contributions.....	199
Acknowledgements	199
NERC Industry Gr	199

Preface

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the reliability of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC’s area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the Electric Reliability Organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC’s jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

The North American BPS is divided into eight Regional Entity (RE) boundaries, as shown in the map and corresponding table below.



The Regional boundaries in this map are approximate. The highlighted area between SPP and SERC denotes overlap as some load-serving entities participate in one Region while associated transmission owners/operators participate in another.

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

Executive Summary

NERC, as the ERO of North America, is tasked with the mission of assuring the reliability of the North American BPS. This is accomplished in a variety of ways, including through independent assessments of BPS reliability and the documentation of results in a periodic report. The *State of Reliability 2017* focuses on the performance of the BPS during 2016 as measured by an established set of reliability indicators (metrics) for comparison to previous years to identify trends.

Based on this report, the BPS provided an adequate level of reliability (ALR)¹ during 2016. In addition, risks to reliability, key areas for improvement, and highlights of ongoing work by industry to improve system reliability and resiliency were identified. This report summarizes the results from ongoing activities to promote reliability across multiple fronts, including reliability assessments and system performance analyses. Analysis of system performance enables NERC to examine trends and identify potential risks to reliability, establish priorities, and develop effective mitigation strategies to control reliability risks. Analysis of system performance data and trends are translated into the key findings below. The corresponding recommendations in [Chapter 1](#) promote further risk assessment and mitigation efforts and help to focus the work and resources of the ERO and the industry.

2016 Key Findings:

1. No Category 4 or 5 events² in 2016
2. Protection system misoperation rate continues to decline, but remains a priority
3. Frequency response shows improvement, but requires continued focus
4. Cyber and physical security risk increases despite no loss of load events
5. Transmission outages caused by human error show a slight increase
6. BPS resiliency to severe weather continues to improve

The *State of Reliability 2017* is an independent report developed by NERC with support from industry. The report builds upon several existing NERC activities and deliverables, including those developed by task forces or working groups under the direction of NERC's Planning, Operating, and Critical Infrastructure Protection Committees. These industry groups support NERC in developing recommendations and mitigation strategies for reliability issues, often prompted by specific findings in this and other NERC reports. Specific BPS incidents in 2016 also served as leading indicators or "faint signals"³ of reliability risks. For example, the California drought-like conditions contributed to the Blue Cut fire transmission line outages, resulting in the cessation of power injection by inverters for a number of solar facilities. Early and ongoing investigation by the ERO contributed to mitigation efforts. These efforts are further detailed in [Chapter 2](#).

Topics in this report are centered on the ERO's Reliability Risk Priorities⁴ that were identified by NERC's Reliability Issues Steering Committee (RISC) and accepted by NERC's Board of Trustees in November 2016. Specifically, Cybersecurity Vulnerabilities and Changing Resource Mix were identified as two high-risk profiles that are evolving and maintaining a high likelihood of impact to the reliability of the BPS with mitigation strategies that are often

¹ Definition of "Adequate Level of Reliability,"

[http://www.nerc.com/pa/Stand/Resources/Documents/Adequate_Level_of_Reliability_Definition_\(Informational_Filing\).pdf](http://www.nerc.com/pa/Stand/Resources/Documents/Adequate_Level_of_Reliability_Definition_(Informational_Filing).pdf)

² Events on the Bulk Electric System (BES) are categorized sequentially from 1 to 5 with 5 being the highest in severity, as detailed in <http://www.nerc.com/pa/rrm/ea/Pages/EA-Program.aspx>.

³ Seeing the Invisible: National Security Intelligence in an Uncertain Age. Thomas Quiggin, World Scientific, 2007

⁴

http://www.nerc.com/comm/RISC/Related%20Files%20DL/ERO_Reliability_Risk_Priorities_RISC_Recommendations_Board_Approved_Nov_2016.pdf

less certain than lower risk profiles. These risks are further explained in [Chapter 1: Key Findings](#), [Chapter 2: 2016 Reliability Highlights](#), and [Chapter 7: BES Security Metrics](#). In addition, [Chapter 4: Reliability Indicator Trends](#) presents a list of the original 16 reliability metrics with trending results that show changes to BPS reliability observed in 2016 when compared to previous years. Supporting information for the complete set of metrics is included in [Appendix E](#), while [Appendix F](#) explains the relevance of the term “statistically significant,” which is used widely throughout this report.

There were no reportable cyber security incidents in 2016 and, therefore, no events that caused loss of load. While this indicates NERC’s efforts with industry have been successful in isolating and protecting operational systems from various adversaries, this does not suggest that cyber security risk is low. Recognizing that risk management and determining appropriate and meaningful security metrics is difficult, the NERC Critical Infrastructure Protection Committee (CIPC) and NERC’s Electricity Information Sharing and Analysis Center (E-ISAC) have developed a roadmap for future metrics development, including refining the initial set of metrics that are based on operational experience. The roadmap addresses consideration of the challenges associated with collecting security-related data:

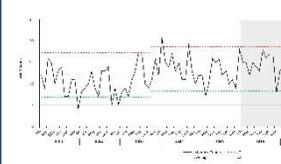
- Historically, NERC and the E-ISAC have limited data related to cyber and physical security incidents as these incidents have been relatively rare and have had little or no impact on BPS reliability.
- The magnitude or number of constantly changing security threats and vulnerabilities is not known with any degree of certainty, particularly as they relate to BPS reliability.
- The number and type of cyber systems and equipment used by the industry is vast, making it difficult to develop metrics that are meaningful to individual entities across the industry.
- Data that details security threats, vulnerabilities, and real incidents is highly sensitive. Handled inappropriately, vulnerabilities could be exposed and new and more sophisticated exploits developed.

The CIPC has researched security metrics developed by leading experts outside the electricity industry and examined more than 150 of these to assess their applicability from a BPS reliability perspective. The CIPC concluded that about 30 of the 150 would be relevant. This assessment underscores the challenges associated with developing relevant and useful security metrics that rely on data willingly and ably provided by individual entities. The NERC E-ISAC and CIPC continue to investigate potential new physical and cyber security metrics.

While the key findings, data, and information in this report are presented independently, they are cross-cutting and demonstrate interdependencies between many of the issues that present unique challenges to the electricity industry. These risks must be strategically monitored and mitigated in order to preserve the reliability of the BPS. NERC’s *State of Reliability 2017* report provides a basis for understanding and prioritizing these risks and, more importantly, how these interdependent challenges require ERO-wide coordination to effectively mitigate these risks.

Chapter 1: Key Findings and Recommendations

This chapter presents key findings extracted from the analyses and insights in the body of this report. The key findings and recommendations also include suggestions for additional data collection or analyses for future State of Reliability reports.



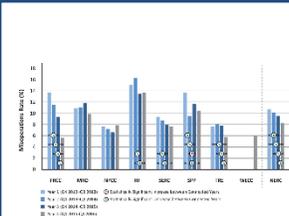
Key Finding 1: No Category 4 or 5 Events in 2016

While the number of lower category events did not significantly decline, there were no Category 4 or 5 events and only two Category 3 events for the second consecutive year. Events on the Bulk Electric System (BES) are categorized sequentially from 1 to 5 with 5 being the highest in severity.

Reviews of these events and those of lower severity resulted in the publishing of 13 lessons learned that shared actionable information with the industry to mitigate risks to BES reliability. For example, the Blue Cut wildfire in California caused transmission faults that cleared as designed, but a number of dispersed solar generation facilities were lost due to erroneous calculations of system frequency. The NERC Event Analysis (EA) Process scans beyond just qualified events to identify and analyze “faint signal” events that are not at mandatory reporting thresholds.

Recommendations

- 1-1: **Emphasize participation in the NERC EA Process:**⁵ NERC should continue to review events and occurrences to identify reliability risks, measure the success of mitigation efforts, and share valuable lessons learned with the continued support and input from industry.
- 1-2: **Expand lessons learned:**⁶ Expand the use of outreach beyond published lessons learned and webinars by using interventions, such as multimedia products and better event data analysis sharing. Continue collaborative efforts with the North American Generator and Transmission Forums and others to share reliability information and seek new venues for increased sharing.
- 1-3: **Include vendors and manufacturers in analyses when possible:** As the grid continues to rapidly transform, NERC must continue to track and trend occurrences and events to identify, analyze, and provide recommendations for risk mitigation. Augment collaboration with industry thorough the NERC technical committees by including vendors and manufacturers in the technical analysis of equipment performance and specifications.



Key Finding 2: Protection System Misoperation Rate Continues to Decline, but Remains a Priority

The overall NERC misoperation rate is lower in 2016 than last year (8.7 percent, down from 9.5 percent), continuing a four-year trend of declining rates across North America. The three largest causes of misoperations in 2016 remained the same as in 2015: Incorrect Settings/Logic/Design Errors, Relay Failure/Malfunctions, and Communication Failures.

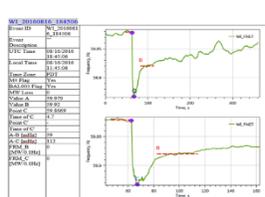
⁵ <http://www.nerc.com/pa/rrm/ea/Pages/EA-Program.aspx>

⁶ <http://www.nerc.com/pa/rrm/ea/Pages/Lessons-Learned.aspx>

While the misoperation rates for some Regions increased in 2016, the overall NERC 2016 misoperation rate is lower than last year (from 9.5 percent⁷ to 8.7 percent), continuing a four-year declining trend across North America. For the first time, the WECC Region's overall operation count was collected, enabling the WECC misoperation rate to be developed for the last two quarters of 2016 (calculated to be 6.0 percent). Using this newly acquired WECC data results in the collective NERC misoperation rate's reduction to 8.3 percent for the measured 2016 year.

Recommendations

- 2-1: Identify protection system misoperations as a primary focus for industry: Protection system misoperations should remain an area of focus as it continues to be one of the largest contributors to the severity of transmission outages.
- 2-2: Expand seminars on protection misoperations topic: Continue with and expand upon Regional efforts on education, outreach, and training with industry and stakeholders to reduce protection system misoperations and continue the downward trend.
- 2-3: Form partnerships to broaden message on misoperations: Continue collaboration with the North American Transmission Forum, vendors, manufacturers, and others to understand, mitigate, and reduce the protection system misoperation rate and impact on the BES. Seek new venues for understanding the challenges associated with the top causes of misoperations and broaden data sharing and information outreach where possible.



Key Finding 3: Frequency Response Shows Improvement, but Requires Continued Focus

Three of the four interconnections showed overall improvement while the Québec Interconnection frequency trend moved from “declining” to “stable.” No interconnection experienced frequency response performance below its interconnection frequency response obligation (IFRO).

Frequency response for all four interconnections improved during the 2012–2016 time frame. Adequate frequency response arrests and stabilizes frequency during system disturbances. The addition of a large number of variable energy resources (VERs) onto the BPS has resulted in the need for operational flexibility to accommodate demand while also effectively managing the resource portfolio. This metric should continue to be monitored as the rapidly changing resource mix presents a potential challenge to frequency response,⁸ one of the essential reliability services (ERSs). ERSs are comprised of primary frequency response (PFR), voltage support, and ramping capability, all needed for the continued reliable operation of the BPS. As VERs are becoming more significant, NERC is developing sufficiency guidelines in order to establish requisite levels of ERSs, frequency response being most notable in this case.

Additionally, increasing installations of distributed energy resources (DERs) modify how distribution and transmission systems interact with each other. Many system operators currently lack sufficient visibility and operational control of these resources, increasing the risk to BPS reliability. This visibility is a crucial aspect of

⁷ The 2016 *State of Reliability* stated the 2015 rate as 9.4 percent. Further analysis resulted in corrections to data which increased the 2015 rate by 0.1 percent, not significantly impacting the conclusions on protection system performance.

⁸ <http://www.nerc.com/comm/Other/essntlrbltysrvscstskfrcdL/ERSTF%20Framework%20Report%20-%20Final.pdf>

power system planning, forecasting, and modeling that requires adequate data and information exchanges across the transmission and distribution interface. The most significant growth in DER penetration is occurring in NPCC and WECC. NERC's Distributed Energy Resources Task Force (DERTF) released their initial report in February of 2017.⁹

Recommendations

- 3-1: Enhance measurement of frequency response and voltage to quantify the effects from the changing resource mix: NERC should continue to measure the effects of the changing resource mix on frequency response and voltage support, including any effects related to DERs. Many system operators currently lack sufficient visibility and operational control of these resources, which is a crucial aspect of power system planning, forecasting, and modeling that requires adequate data and information exchanges across the transmission and distribution interface.
- 3-2: Continue modifications to generator interconnection agreements: Regulators and markets should continue to support modifications and improvements to generator interconnection agreements to ensure frequency response capabilities for new generation resources.
- 3-3: Increase awareness of frequency response challenges: Continued collaboration with the North American Generator Forum and others to increase frequency response awareness and capabilities is required. Continued and expanded efforts on education, outreach, and training to improve awareness of the challenges associated with frequency response are needed to inform all levels of both industry and policy makers.



Key Finding 4: Cyber and Physical Security Risk Increases, Despite No Loss-Of-Load Events

In 2016, there were no reported cyber or physical security incidents that resulted in a loss of load. Nonetheless, grid security, particularly cyber security, is an area where past performance does not predict future risk. Threats continue to increase and are becoming more serious.

Responsible entities report cyber security incidents to the E-ISAC as required by the NERC Reliability Standard CIP-008-5 Incident Reporting and Response Planning. The above finding reports the total number of reportable cyber security incidents¹⁰ that occurred in 2016 and identifies how many of these incidents have resulted in a loss of load. While there were no reportable cyber security incidents during 2016 and therefore none that caused a loss of load, this does not necessarily suggest that the risk of a cyber security incident is low. In fact, the number of cyber security vulnerabilities continues to increase as does the number of threat groups.¹¹ There were a few nonmandatory reports of cyber incidents in 2016, such as phishing and malicious software, found on enterprise (noncontrol) computers. While none of these incidents resulted in load loss, they are a reminder that cyber security risks are ever present.

⁹ http://www.nerc.com/comm/Other/essntlrbltysrvctskfrcl/Distributed_Energy_Resources_Report.pdf

¹⁰ Ref. NERC Glossary of Terms: "A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity."

¹¹ Security Metric 7, Appendix G

Responsible entities also report physical security events to the Electricity Information Sharing and Analysis Center (E-ISAC) as required by the NERC EOP-004-2 Event Reporting Reliability Standard. The above finding is a result of the total number of physical security reportable events¹² that occur in 2016 and identifies how many of these events have resulted in a loss of load. This finding does not include physical security events that affect equipment at the distribution level (i.e., non-BES equipment). Both mandatory and voluntary reporting indicate that distribution-level events are more frequent than those affecting BES equipment.

The mandatory reporting process does not create an accurate picture of cyber security risk since most of the cyber threats detected by the electricity industry manifest themselves in the enterprise environment (email, websites, smart phone applications, etc.), rather than the control system environment where impacts could cause loss of load and result in a mandatory report. Occasionally, the E-ISAC receives voluntary notifications from entities that malicious code was found on an employee's workstation or that an attack was detected against the entity's public-facing website.

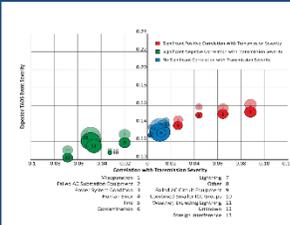
NERC, in collaboration with the Department of Energy and its national laboratories, is exploring ways control system traffic could be directly captured in a passive and nondisruptive manner in addition to the large data sets of information flowing from the corporate or business systems. Once the Cyber Automated Information Sharing System (CAISS)—which is currently a pilot program—becomes more widespread, the system will allow indicators of compromise (IOC) that may be seen on enterprise information technology systems via the Cybersecurity Risk Information Sharing Program (CRISP) to be compared to any potential intrusions or malicious data collected from control systems, further refining risk metrics to grid operations. These initiatives will assist in developing a better picture of the BPS' security state.

Recommendations

NERC and industry should be guided by the following recommendations in maturing existing metrics and developing new metrics to enhance industry's view of evolving security risks.

- 4-1: Redefine incidents in more granular form: Redefine reportable incidents to be more granular and include zero-consequence incidents that might be precursors to something more serious.
- 4-2: Run malware signature comparisons to create benchmarks: Use CRISP data to run malware signature comparisons to see how many hits occur on a benchmark set of entities and if any have serious implications for the grid. This metric could be used to provide a percent change from a benchmark year-over-year.
- 4-3: Characterize type and frequency of cyber threats reported through CAISS data: Use data obtained from CAISS and other similar capabilities to characterize the type and frequency of various cyber threats reported through the year.
- 4-4: Expand outreach to public and private sector data resources: Include other data sources such as the FBI, SANS Institute, Verizon, etc., as input for understanding the broader security landscape surrounding critical infrastructures.
- 4-5: Strengthen situational awareness for cyber and physical security: NERC should actively maintain, create, and support collaborative efforts to strengthen situational awareness for cyber and physical security while providing timely and coordinated information to industry. In addition, industry should continue to review its planning and operational practices to mitigate potential vulnerabilities to the BPS.

¹² Reportable events are defined in Reliability Standard EOP-004-2 Event Reporting, Attachment 1.



Key Finding 5: Transmission Outage Rates Caused by Human Error Show a Slight Increase, but no Increase in Outage Severity

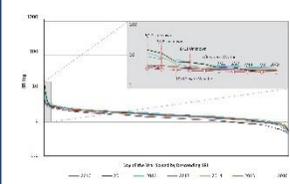
The number of automatic (momentary and sustained) transmission outages from Human Error significantly reduced from 2014 to 2015. Year-end 2016 data demonstrates a return to 2014 levels. While no increase in outage severity was discovered, Human Error remains a major contributor to transmission outage severity and will remain an area of focus.

Industry’s increased efforts to lower the number of outages defined as “unknown in cause” has resulted in a marked improvement of causal identification, thus less use of the “unknown” descriptor in Transmission Availability Data System (TADS) reporting. It is not clear whether some portion of the increase in Human Error for 2016 may be a result of more deliberate cause coding, thereby reducing outages with an unknown cause, but increasing the rate of outages caused by Human Error. It is important to note that the while the outage rate has increased, the overall correlation with transmission line outage severity has not markedly increased from past years.

Additionally, outages from Failed Alternating Current Circuit Equipment (insulators, conductors, etc.) have increased from past trends, potentially for the same reason as mentioned previously. Transmission line outages caused by Failed AC Substation Equipment (breakers, transformers, etc.) have remained flat as a trend with neither an increase nor a decrease in the rate of occurrence.

Recommendations

- 5-1: Increase human performance training and education: NERC should continue to provide focus on human performance training and education through conferences and workshops that increase knowledge and mitigation from possible risk scenarios.
- 5-2: Increase awareness of human performance issues with industry and policymakers: Explore increased collaboration with the NAGF, NATF, and other groups. Continue to expand efforts on education, outreach, and training to improve awareness of the challenges associated with human performance to inform all levels of both industry and policy makers.
- 5-3: Initiate focused data collection and assessment: Industry should investigate the possible value of increased granularity of data collection for transmission outages collected in the Transmission Availability Data System caused by Failed AC Circuit Equipment, Failed AC Substation Equipment, and Human Performance.



Key Finding 6: BPS Resiliency to Severe Weather Continues to Improve

In 2016 for the second consecutive year, there were no days that the daily severity risk index (SRI) was part of the top-10 most severe list of days between 2008 and 2015, despite days with extreme weather conditions across North America.

Performance outcomes were determined using the SRI, which is a measure of stress to the BPS in any day resulting from the combination of generation, transmission, and load loss components. In 2016, there were no days that made the daily SRI top-10 most severe list of days between 2008 and 2015; this is despite days with extreme

weather conditions across North America. Improvements in the 2016 SRI demonstrate that industry preparedness continues to have a positive influence on BPS resiliency.

Recommendations

- 6-1: Update the severe weather collaboration process with industry: NERC should continue to expand outreach with industry to improve grid resilience before, during, and after extreme weather events.

- 6-2: Develop the SRI on interconnection or regional basis: The ERO Enterprise should continue to explore the possibility of developing the SRI on an interconnection or regional basis to provide greater insight into targeted weather mitigation.

- 6-3: Update the winter weather reliability guideline: In coordination with the NAGF, the NERC Operating Committee (OC) should review and update the Generator Unit Winter Weather Readiness Reliability Guideline¹³ to capture lessons learned from previous winters.

¹³http://www.nerc.com/comm/OC/Reliability%20Guideline%20DL/Generating_Unit_Winter_Weather_Readiness_final.pdf

Chapter 2: 2016 Reliability Highlights

This chapter describes actions taken to mitigate strategic reliability risks and events that occurred to offer further insight into the risks. This insight provided context for the analytical conclusions drawn from the metric data found in [Chapter 4](#) and [Appendix E](#) and produced richer conclusions from and key findings for the *State of Reliability 2017* than would have otherwise been possible. In some cases, topics covered in the previous *State of Reliability* reports are re-examined as NERC's understanding has deepened and mitigation efforts have refined. In these cases, some background information will be reintroduced that is accompanied with new insights.

The topics examined in this chapter are closely related to the following high-risk reliability profiles that were identified in the RISC's ERO Reliability Risk Priorities:¹⁴

- Changing Resource Mix
- Bulk Power System Planning
- Resource Adequacy Performance
- Cyber Security Vulnerabilities

The RISC profile Changing Resource Mix is closely related to BPS Planning and Resource Adequacy Performance. NERC has collaborated with industry to address all three with a focus on ERSs, which are foundational for understanding and mitigating the risks' potential negative impacts on the system. Single points of disruption have also become a greater risk as the resource mix continues to rapidly change. Specifically, increased dependence on natural-gas-fired capacity can lead to greater reliability risks due to the loss of natural gas or other fuel contingencies. Grid security issues and related cyber security vulnerabilities are also examined in this chapter.

Essential Reliability Services

Attention to the changing resource mix in 2016 primarily targeted establishing approaches for measuring ERSs, especially as the penetration of inverter-based generation continues to increase (e.g., solar and wind turbine technologies). NERC's Essential Reliability Services Working Group (ERSWG) is a group of industry subject matter experts that have supported NERC in its effort to inform policy makers on the importance of ERSs.

The ERSWG's support includes the release of multiple deliverables. Among these deliverables are an ERS concept paper,¹⁵ a framework report,¹⁶ and several videos¹⁷ that explain frequency support, ramping, and voltage support. Regulators and industry have since taken additional actions in 2016 to address frequency response and voltage support.

Primary Frequency Response

Increased industry focus on frequency response in recent years ([Appendix E: Metric M-4](#)) has paralleled improved system performance. The United States interconnections all demonstrated improved trends 2012–2016 as seen in [Table 4.1](#) and the detailed analysis in [Appendix E](#). Previous frequency response performance in 2012–2015 was inconclusive in the Eastern and Western Interconnections since inconsistent data did not allow for accurate trending. The Québec Interconnection showed similar improvement from declining performance over 2012–2015 to a stable trend 2012–2016.

¹⁴

http://www.nerc.com/comm/RISC/Related%20Files%20DL/ERO_Reliability_Risk_Priorities_RISC_Recommendations_Board_Approved_Nov_2016.pdf

¹⁵ http://www.nerc.com/comm/Other/essntlrbltysrvcskfrcdl/ERSTF_Concept_Paper.pdf

¹⁶ <http://www.nerc.com/comm/Other/essntlrbltysrvcskfrcdl/ERSTF%20Framework%20Report%20-%20Final.pdf>

¹⁷ <https://vimeo.com/nerclearning/erstf-1>

NERC has collaborated with the NAGF to conduct the NAGF Primary Frequency Workshop in 2016, which was attended by NERC, NAGF, and FERC staff in addition to vendors. The NERC Resources Subcommittee (RS) conducted interconnection-level, web-based training sessions on implementation of Reliability Standard BAL-003-1 (R1),¹⁸ and on frequency response and frequency bias setting for industry Balancing Authorities (BAs). The RS also conducted a web-based instruction, Frequency Response Initiative – Generator Event Survey, for Generator Owners (GOs) and Generator Operators (GOPs). Additionally, the RS worked on enhanced frequency response measures as assigned by the ERSWG in its framework report. FERC issued a notice of proposed rulemaking (NOPR) to require new generators connecting to the BES to have the capability to provide frequency response. FERC also modified the *pro forma* Small Generator Interconnection Agreement to require newly interconnecting small generating facilities to ride through abnormal frequency events. These distinct, yet coordinated actions demonstrate a need for these efforts to continue in order to have an effective impact on improvements to interconnection frequency response.

Voltage Support

PAS and System Analysis and Modeling Subcommittee (SAMS) groups, at the direction of NERC’s Planning Committee (PC), have worked in 2016 to advance Measure 7–Reactive Capability on the System—from the ERSWG’s framework document. PAS completed the related tasks of determining a methodology for data collection to support Measure 7 and used it to solicit a voluntary industry data submission from the identified BAs. PAS submitted the data to the SAMS for further evaluation that is expected in 2017. Similar to its frequency requirement, FERC modified the *pro forma* Small Generator Interconnection Agreement¹⁹ to require newly interconnecting small generating facilities to ride through abnormal voltage events.

Single Point of Disruption

NERC continues to assess the increasing risk of fuel disruption impacts on generator availability from the dependency of electric generation and natural gas infrastructure as a single point of disruption (SPOD). In the past, NERC conducted two special assessments on gas-electric interdependencies; a primer highlighting key considerations in 2011²⁰ and a detailed framework for incorporating risks into reliability assessments in 2013.²¹ As highlighted in previously released NERC *Long-Term Reliability Assessments* (LTRAs), substantial progress has been made in the last five years to improve coordination between natural gas pipelines, gas distribution companies, and electric industries. Even so, there are remaining concerns and opportunities to address on this subject.²² NERC published its *Short-Term Special Assessment: Operational Risk Assessment with High Penetration of Natural Gas-Fired Generation*²³ in May 2016. In the document, NERC recommended incorporating fuel availability into national and regional assessments.

Until recently, natural gas interdependency challenges were most experienced during extreme winter conditions and focused almost exclusively on gas delivery through pipelines. However, the recent outage of an operationally-critical natural gas storage facility in Southern California—Aliso Canyon—demonstrates the potential risks to BPS reliability of increased reliance on natural gas without increased coordination between the two industries. In October 2015, a gas leak was detected in a well at Aliso Canyon. The facility is owned by Southern California Gas Company (SoCalGas) and is one of the largest natural gas storage facilities in the United States. It is a critical component of the natural gas system in the Los Angeles Basin, which serves 11 million core natural gas customers and provides gas to 18 power plants with approximately 9,800 MW of capacity in the L.A. basin. Through November and December 2015 as SoCalGas worked to stop the leak, it reduced the amount of working gas stored

¹⁸ BAL-003-1(R1) compliance was effective in December, 2016.

¹⁹ <https://www.ferc.gov/industries/electric/indus-act/gi/SGIA.pdf>

²⁰ http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/Gas_Electric_Interdependencies_Phase_I.pdf

²¹ http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_PhaseII_FINAL.pdf

²² <http://www.nerc.com/pa/RAPA/ra/Pages/default.aspx>

²³ http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC%20Short-Term%20Special%20Assessment%20Gas%20Electric_Final.pdf

in Aliso Canyon from 86 Bcf to 15 Bcf. The leak was sealed in February 2016; however, additional injection of gas into the facility was prohibited pending a comprehensive inspection of the 114 storage wells at the facility. The BPS reliability risk of potentially controlled load shedding persisted through the 2016 summer season.

While the situation at Aliso Canyon did not meet the criteria/threshold of an EA Process qualified event, NERC Bulk Power System Awareness (BPSA) began closely monitoring the situation at its onset. NERC BPSA has coordinated with WECC SA to remain informed of the activities surrounding the issue and will continue to collaborate with WECC SA as they determine what, if any, ongoing reliability concerns there may be.

Renewable Penetration and Distributed Energy Resources

California provides a leading indicator of BES performance given the high penetration of renewable and distributed energy resources in the state. It has established a renewables portfolio standard (RPS) of 33 percent by 2020 and 50 percent by 2030. CAISO 2020 (33 percent) studies indicate that, in times of low load and high renewable generation, as much as 60 percent of its energy production would come from renewable generators that displace conventional generation and frequency response capability.²⁴ Net load is the difference between forecast load and expected production from variable generation resources (renewable generation). The difference is an imbalance between peak demand and renewable generation that strains the grid. Net load is illustrated using what is commonly known as the “duck curve” since the load shape across a day resembles the profile of a duck (see **Figure 2.1**). California’s duck curve is already meeting projections for the year 2020. ERO SA and EA have worked to ensure that they are able to detect and mitigate “faint signals” of potential future reliability threats.

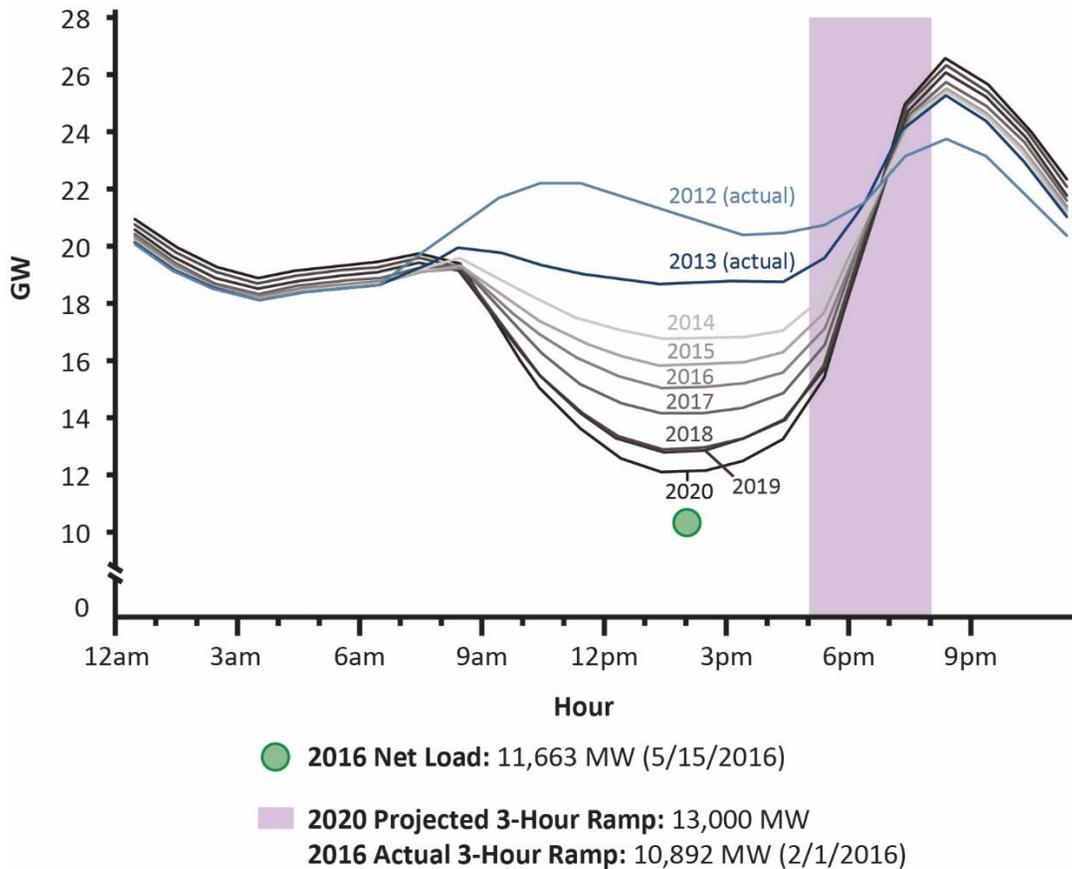


Figure 2.1: CAISO Duck Curve

²⁴ http://www.caiso.com/Documents/FlexibleResourcesHelpRenewables_FastFacts.pdf

Unplanned Loss of Renewable Generation

On August 16, 2016, smoke from the Blue Cut wildfire in San Luis Obispo County, CA, resulted in the tripping of two 500 kV lines in the active fire area. There was a noticeable frequency excursion with Peak RC reporting the loss of more than 1,000 MW across multiple renewable resources in the CAISO BA following these line outages. CAISO, SCE, and Peak confirmed that no conventional generators tripped and that all the resources that were lost practically instantaneously were utility-scale renewables, primarily solar.

While not a qualifying event in the ERO EA Process, the occurrence was significant and unusual enough that the ERO requested an event report and worked with the engineers and planners at CAISO and Southern California Edison to better understand this first known major loss of renewable resources due to a transmission system disturbance.

The tripping of the first 500 kV line was due to smoke from the fire creating a fault and the line clearing as designed. The second 500 kV line tripped as a result of a smoke induced fault, again by design, and cleared within three cycles. Before that fault cleared, the transient caused by the fault was experienced at the 26 nearby solar farms (thus the aggregate over 1,000 MWs of generation) and subsequently caused the inverters to quit injecting ac current (within two cycles).

- Many of the inverters stopped outputting power before the fault cleared, indicating that the faulted condition alone created the condition that caused the response as opposed to post-fault system response (transient stability).
- Many inverters calculated frequencies at the inverter terminals which are well outside of the values that would be expected for a normally cleared fault. Many inverters calculated a system frequency in the range of 57 Hz during the fault.
- A thorough analysis of the event and the operating characteristics of the related equipment is underway.

There were also multiple instances of unplanned loss of wind generation observed in 2015–2016 in Electric Reliability Council of Texas (ERCOT), the most severe resulting in the temporary loss of 475 MW. The generation loss events occurred as a result of BES voltage disturbances. These were typically also not qualifying events under the ERO EA Process criteria. Texas RE, in conjunction with ERCOT, gathered information from each event to determine the cause of individual wind turbine loss based on wind turbine type and manufacturer. These analyses were hampered by the lack of high-speed data recording capability that is necessary to determine the magnitude of voltage disturbances at the individual wind plant locations. Preliminary data analytics indicate possible issues with voltage ride-through capability as well as other turbine control system parameters. These events provide insight to challenges discussed in the Essential Reliability Services Task Force Measures Framework Report.²⁵

Grid Security

Cyber Security Vulnerabilities remains a high-risk profile relative to BPS reliability. Chapter 7 and Appendix G of this report detail the evolving nature of the risk and progress in the endeavor to measure it. Specifically, the data NERC received in 2016 from OE-417s and EOP-004s show low numbers of cyber penetrations of grid operating systems in North America and few reports of physical intrusions.²⁶ These low numbers indicate that NERC's efforts with industry have been successful in isolating and protecting operational systems from various adversaries. The numbers are also an indication that the electricity industry's record of breaches is much lower than many other sectors and government agencies that have been victims of numerous data breaches.²⁷

²⁵ <http://www.nerc.com/comm/Other/essntlrbltysrvscstskfrcdl/ERSTF%20Framework%20Report%20-%20Final.pdf>

²⁶ See Appendix G for the BESSMWG metrics.

²⁷ <http://www.nydailynews.com/news/national/hacker-dumps-info-thousands-homeland-security-workers-article-1.2524440>; <https://www.scmagazine.com/anonsec-claims-credit-for-nasa-drone-hack/article/528448/>; <http://www.cbsnews.com/news/irs-identity-theft-online-hackers-social-security-number-get-transcript/>.

Electricity Information Sharing and Analysis Center

The E-ISAC's mission is to be a leading, trusted source that analyzes and shares electricity industry security information. The E-ISAC gathers security information, coordinates incident management, and communicates mitigation strategies with stakeholders within the electricity industry across interdependent sectors and with government partners.

Most of the E-ISAC's communications with electricity industry members are via a secure internet portal that was significantly upgraded at the end of 2015. In 2016, the E-ISAC added 1,512 new users to the portal, a growth of 19.5 percent over 2015. As the E-ISAC continues to collect portal activity data, the information will assist the E-ISAC in recruiting new members to the portal and determining how the E-ISAC can best serve members' interests and needs.

Increased physical security and cyber security information sharing will enable the E-ISAC to conduct more complete analysis. Robust data collection over time helps identify important trends and patterns. By providing unique insight and analysis on physical and cyber security risks, the E-ISAC's aim is to add value for its members and assist with overall risk reduction across the ERO Enterprise.

NERC and the electricity industry have taken actions to address cyber and physical security risks to the reliable operation of the BPS as a result of potential and real threats, vulnerabilities, and events. The E-ISAC has started hosting unclassified threat workshops biannually. These threat workshops bring together security experts from government and industry to discuss threats facing the electricity industry. The discussions include a focus on past threats, incidents and lessons learned, current threats that may impact industry, or views on emerging threats. The E-ISAC held its first threat workshop on December 6, 2016, in Washington, D.C. and has future workshops planned.

CRISP

CRISP is a public-private partnership cofounded by the Department of Energy (DOE) and NERC and managed by the E-ISAC that facilitates the exchange of detailed cyber security information among industry, the E-ISAC, DOE, and Pacific Northwest National Laboratory. The program facilitates information sharing and enables owners and operators to better protect their networks from sophisticated cyber threats.

Participation in the program is voluntary and enables owners and operators to better protect their networks from sophisticated cyber threats. The purpose of CRISP is to collaborate with industry partners to facilitate the timely bidirectional sharing of unclassified and classified threat information. CRISP information helps support development of situational awareness tools to enhance the industry's ability to identify, prioritize, and coordinate the protection of its critical infrastructure and key resources.

Chapter 3: Severity Risk Assessment and Availability Data Systems

The severity risk index (SRI) metric quantifies the performance of the BPS on a daily basis. It was designed to provide comparative context for evaluating current and historical performance of the system. Interchangeable use of terms, such as high-risk, high-stress, and high-impact for BPS days, is allowed since the terms are only descriptive of measured SRI within this context. This chapter gives an overview of the metric, its calculation, and the BPS performance in 2016 relative to previous years. It further details the role of the metric's component parts in the determination of the 2016 performance. The three component parts are daily generation loss, transmission element loss, and load loss.

Overview of Severity Risk Analysis

Observations

The 2016 daily SRI has shown solid performance from prior years as expressed by the mean and standard deviation detailed in [Appendix A](#). For each component of the SRI, the following observations can be made:

- **Generation Component:** The generation loss component of the SRI indicates 2011 was the benchmark year for the generation fleet; however, this time period predates the mandatory generation reporting requirements, so it is inconclusive whether that year should be the measure against which subsequent years should be compared.
- **Transmission Component:** With regard to the transmission component of the SRI, 2016 compared to 2015²⁸ had a higher median and maximum transmission day, but overall less volatility as measured by a lower standard deviation.
- **Load Loss Component:** The load loss component of the SRI in 2016 exhibits the best year of performance demonstrated by smaller values of the descriptive statistics such as mean, maximum, standard deviation, etc. (outlined in [Appendix A Table A.5](#)) when compared to prior years.

Calculation for the SRI Metric

Since the inception of the *State of Reliability Report*, the industry has developed the SRI metric, which serves to daily measure the effect of BPS performance. The metric is made of the following weighted components:

- Transmission system automatic outages for voltages 200 kV+
- Generation system unplanned outages
- Distribution load lost as a result of events upstream of the distribution system

Each of the components of the calculation for the SRI metric are weighted at a level recommended by the OC and Planning Committee (PC) as follows:²⁹

- Generation capacity lost is divided by the total generation fleet for the year being evaluated and factored at 10 percent of the SRI score.
- 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 percent of the SRI score.

²⁸ The scope of TADS data collection prior to 2015 applied to momentary and sustained outages of BES elements rated 200kV+. In 2015 it expanded to include sustained outages for elements below 200 kV. This change significantly affected the SRI transmission component. Therefore, comparisons of SRI transmission components are limited to years 2010–2014 for the former collection scope and years 2015-present for the current collection scope.

²⁹ http://www.nerc.com/docs/pc/rmwg/SRI_Equation_Refinement_May6_2011.pdf

- Load lost due to performance upstream of the distribution system is calculated based upon outage frequency for the day, which is divided by system peak loading and is factored at 60 percent of the SRI score.

With these weighted components, the SRI becomes an indicator of the stress on 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.

Interpreting the Yearly Descending SRI Curve

The SRI descending curve shown in [Figure 3.1](#) demonstrates several components that are valuable for analysis:

- First, the left side of the graph, where the system has been substantially stressed, should be compared to the high-stress days of prior years. This section of the graph is highlighted in a call out box in [Figure 3.1](#).
- Second, the slope of the central part of the graph reveals year-to-year changes in fundamental resilience of the system to routine operating conditions.
- Finally, the right section of the curve provides information about how many days with lower SRI scores occurred during any year compared to other years.

2016 Year in Review

The chart shown in [Figure 3.1](#) outlines that the year's highest impacting days did not significantly stress the BPS as would have been expected. The thumbnail inset further illustrates that the moderate impacts measured during 2016's highest SRI days represented less stress to the BPS than were caused by the highest SRI days in any prior year on record. For example, the maximum SRI value for 2016 was 3.6; the next lowest maximum value of 4.06 occurred in 2013. Additional information on the descriptive statistics (mean, standard deviation, minimum, maximum, and median) of the daily SRI can be found in [Appendix A](#). Based on prior years' analyses of the SRI, a high-stress day³⁰ has been determined to be a day where the day's SRI score exceeded 5.0. During 2016, no days exceeded this benchmark value; thus, even the more challenging days in the year demonstrated better resilience than in prior years.

³⁰ High-stress days are days during which BPS performance has experienced noteworthy impacts to any or all of its generation, transmission, or load SRI components. Based on past analyses, days that exceed an SRI rating of 5.0 (on a scale of 0 to 1000) are often memorable and may provide lessons learned opportunities. If no days exceed five, the highest 10 days for the year are generally reviewed for their initiating causes.

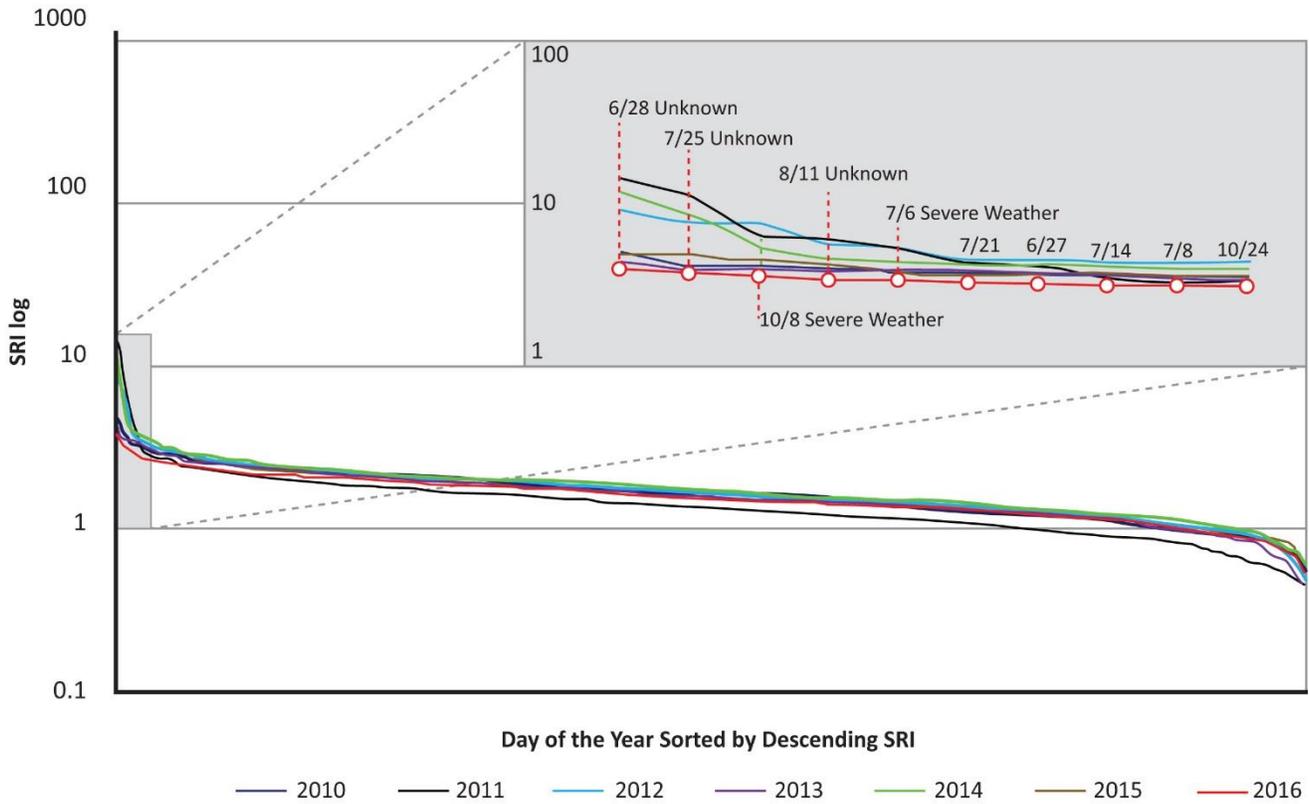


Figure 3.1: NERC Annual Daily Severity Risk Index Sorted Descending

Table 3.1 identifies the top 10 SRI days during 2016 and denotes the weighted generation, transmission, and load loss components for each of these days. It further identifies the significance of each component’s contribution to the total SRI calculation, the type of event that occurred, and its general location. General observations include that many of the days were dominated by generation loss and were minimally driven by cold weather with more than half of the days occurring in June, July, and August. PAS separately reviewed DOE OE-417³¹ reports to determine any reported event correlations to weather influenced events. In past years, most top SRI days had an associated report indicating that the performance was influenced by weather; however, analysis suggests that the top SRI days are not driven by large reaching weather events in 2016. Instead, the 2016 top SRI days were a combination of many smaller local events, indicating that BPS resilience to the events during the year was high.

³¹ <https://www.oe.netl.doe.gov/oe417.aspx>

Table 3.1: 2016 Top 10 SRI Days									
Date	NERC SRI and Weighted Components 2016				G/T/L	Weather Influenced (Verified by OE-417)?	Rank	Event Type	Region
	SRI	Weighted Generation	Weighted Transmission	Weighted Load Loss					
6/28/2016	3.57	2.64	0.88	0.09			1		
7/25/2016	3.38	2.61	0.64	0.07			2		
10/8/2016	3.14	0.77	2.33	0.13		✓	3	Severe Weather	SERC
8/11/2016	3.06	2.39	0.53	0.08		✓	4	Severe Weather	RFC
7/6/2016	2.99	2.33	0.59	0.01			5		
7/21/2016	2.90	1.92	0.89	0.29			6		
6/27/2016	2.82	1.84	0.82	0.08			7		
7/14/2016	2.79	1.49	0.83	0.06		✓	8	Severe Weather	SERC
7/08/2016	2.73	1.64	0.89	0.14			9		
10/24/2016	2.71	2.18	0.37	0.23			10		

Figure 3.2 reflects a new way of providing insight into the SRI and its evaluation of the BPS performance. It is a daily plot of the SRI score for 2016 (shown in blue) against control limits that were calculated using 2010–2016 seasonal daily performance. On a daily basis, a general normal range of performance exists. This is visible in the gray colored band or within the daily seasonal 90 percent control limits. Days of stress rise above the seasonal daily control limits. Figure 3.2 indicates that the BPS performance in 2016, as measured by the SRI, was stable with only five days having an SRI value above the seasonal control limits.

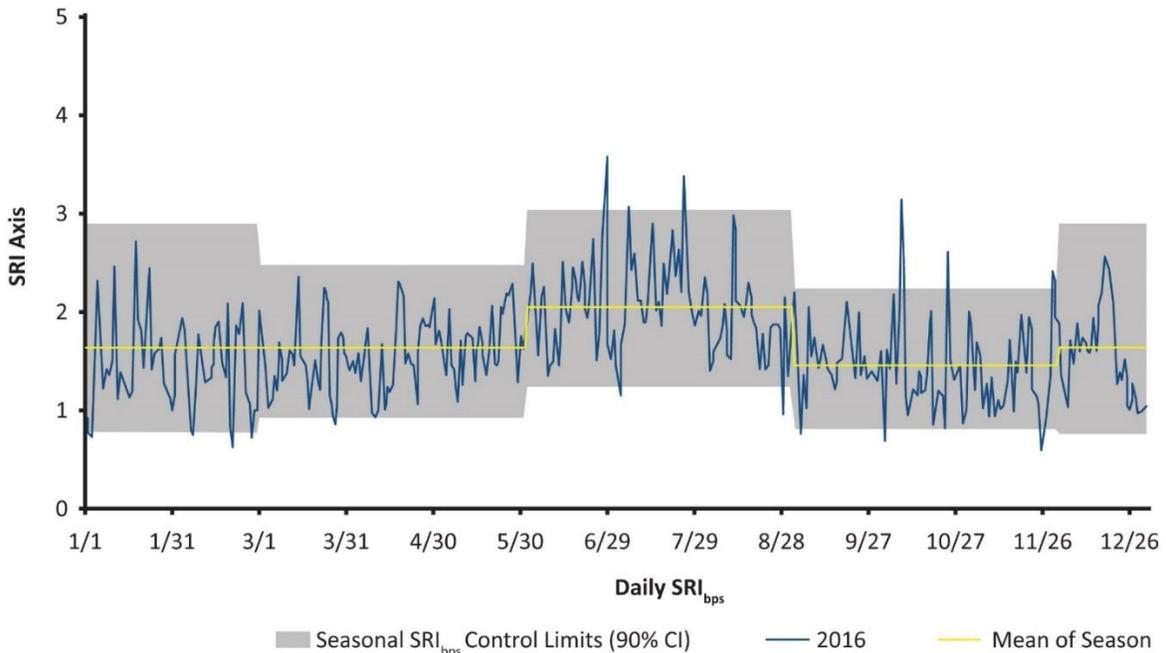


Figure 3.2: NERC 2016 Daily SRI with Top 10 Days Labeled

Table 3.2 identifies the top 10 SRI days for years 2008–2016. These are distinctly different than the 2016 days in Table 3.1, in that they are dominated by extreme weather events, and the weighted load loss contributes significantly to the SRI for most of the days.

Table 3.2: Top 10 SRI Days (2008–2016)									
Date	NERC SRI and Weighted Components				G/T/L	Weather Influenced (Verified by OE-417)?	Rank	Event Type	Region
	SRI	Weighted Generation	Weighted Transmission	Weighted Load Loss					
9/8/2011	14.0	1.2	0.8	12.0		No	1	Southwest Blackout	WECC
1/7/2014	11.1	9.8	0.9	0.4		Yes	2	Polar Vortex	RF, Texas RE, SERC
2/2/2011	10.8	3.0	0.5	7.3		Yes	3	Cold Weather Event	Texas RE
6/29/2012	8.9	2.6	1.4	4.9		Yes	4	Thunderstorm Derecho	RF, NPCC, MRO
1/6/2014	8.0	6.7	1.2	0.2		Yes	5	Polar Vortex	RF, Texas RE, SERC
10/30/2012	7.2	2.9	3.4	0.9		Yes	6	Hurricane Sandy	NPCC, SERC
10/29/2012	7.0	2.0	1.8	3.2		Yes	7	Hurricane Sandy	NPCC, SERC
4/27/2011	5.8	1.9	3.5	0.4		Yes	8	Tornadoes Severe Storm	SERC
8/28/2011	5.6	0.8	1.6	3.2		Yes	9	Hurricane Irene	NPCC, RF
1/4/2008	5.3	1.2	0.8	3.2		Yes	10	Pacific Coast Storm	WECC

Figure 3.3 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 2016 began with relatively low SRI days and continued this best performance through June. After June, slight escalation occurred, and this moved the cumulative SRI to just slightly poorer than 2011, which stands as the best year on record when comparing annual cumulative SRI_{bps}. There were a few step changes on the curve for the remainder of the year, but a slight increase in the slope occurs at year-end reflecting the minor impact of the beginning of winter weather.

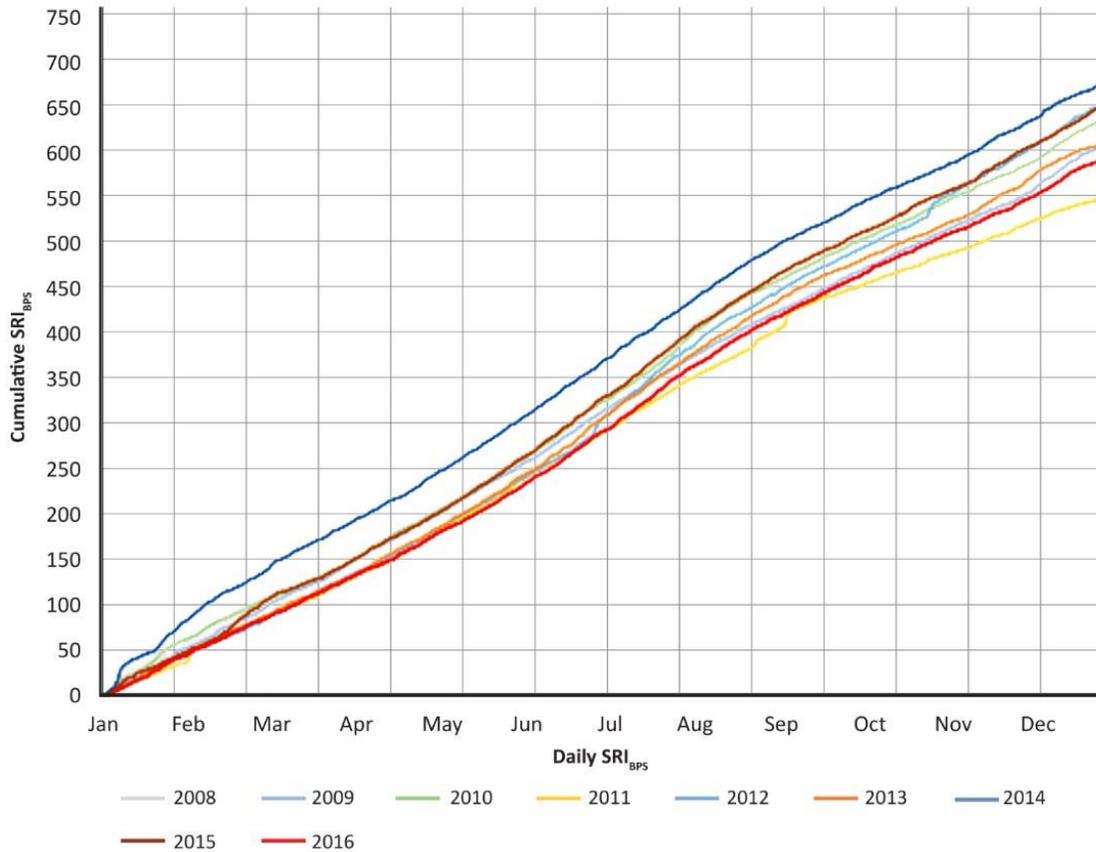


Figure 3.3: BPS Cumulative SRI (2008–2016)

Figure 3.4 breaks down the 2015 cumulative performance by BPS segment. The components are generation, transmission, and load loss in that order. During the year, no single component shows a significant step change for any given day, rather the performance within each segment proves to be very stable. Through the winter and spring, the slopes of each segment are fairly constant, and the generation component does not appear to have any visible deviation to the slope. In the transmission segment, it appears that a slight elevation in its contribution occurs through the summer. The load loss component also reflects a slight increase through the summer season, but also reflects no unusual increase from an individual day. The unplanned generation unavailability component is typically the largest contributor to cumulative SRI.

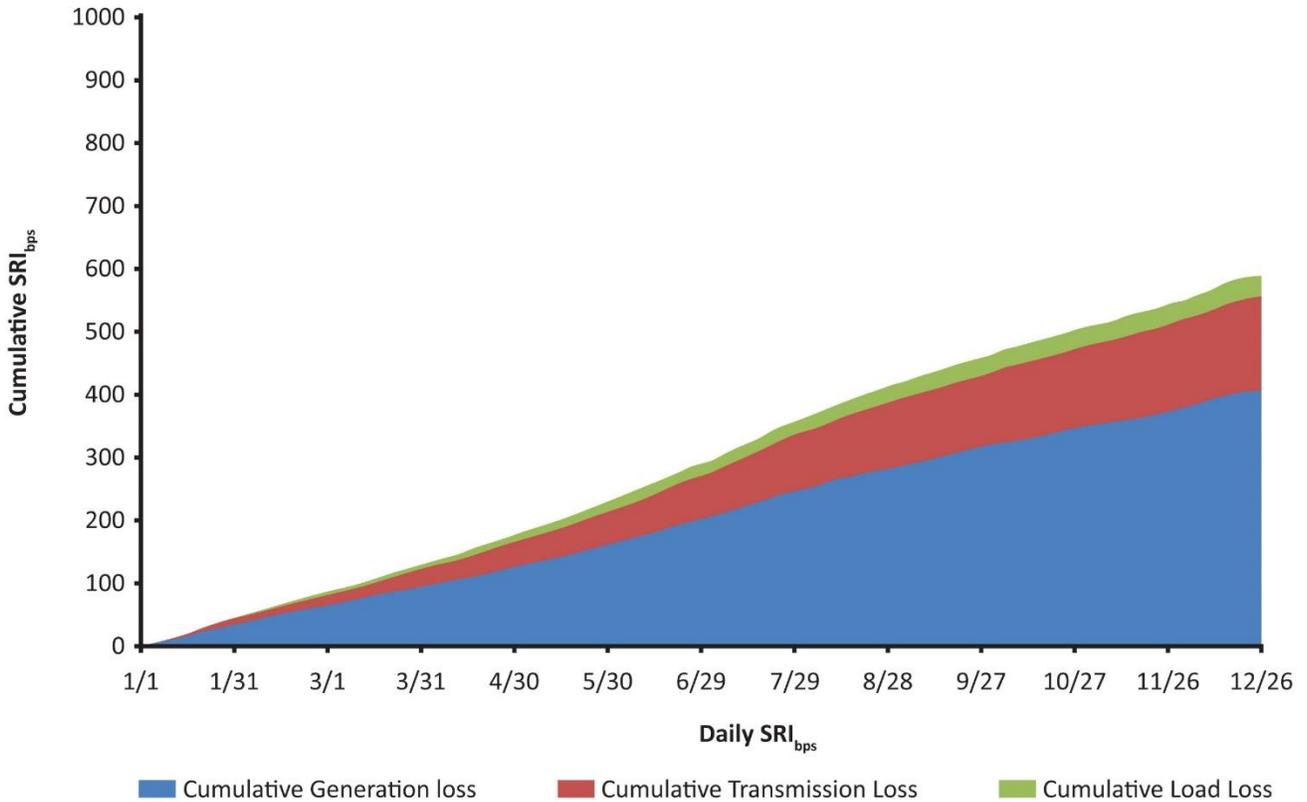


Figure 3.4: NERC Cumulative SRI by Component for 2016

Figure 3.5 provides the history of 365-days of rolling SRI accumulated performance such that each data point represents the value compared to a single year’s BPS performance. For example, the point at 12/31/2008 represents the accumulated SRI values of 1/1/2008 through 12/31/2008. The next point on the graph 1/1/2009 would shift the values forward such that it would represent the accumulated SRI values of 1/2/2008 through 1/1/2009.

The trend for performance demonstrates that the best performance has occurred toward the end of 2011 and the beginning of 2012. Since then, SRI performance elevated slightly and generally stayed at that level until the end of 2014, followed by the SRI falling to a fairly stable level in 2015 with improvements reflected through 2016.

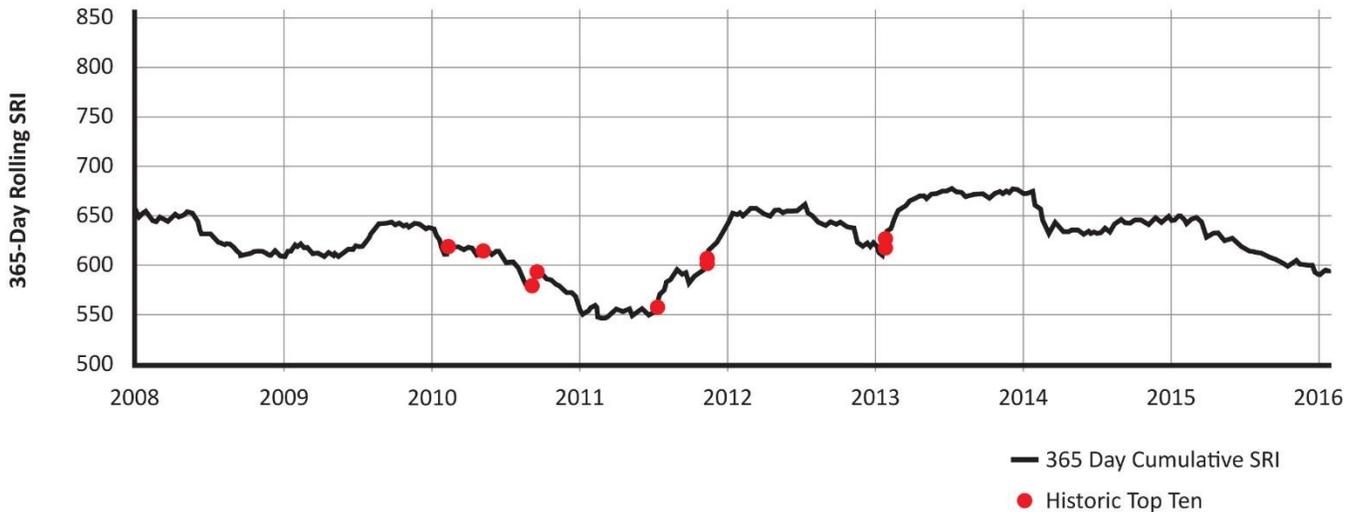


Figure 3.5: 365-day Cumulative SRI 2009-2016

Figure 3.6 further demonstrates the 365-day rolling history that segments the performance by each component. The top chart, in **Figure 3.6**, shows generation loss, which elevated after 2011 and topped out during late 2014. Some improvement occurred during 2015 and appeared to persist through 2016, and this carried through into the composite performance shown in **Figure 3.5**. The transmission component indicates consistent performance through 2009, elevated SRI through 2010, and slight deterioration through 2015 with subsequent slight improvements in the latter half of 2016. The load loss component indicates improvement through 2009 with 2011 and 2012 having several individual step-change days (large load loss events) followed by gradual but continual improvement.

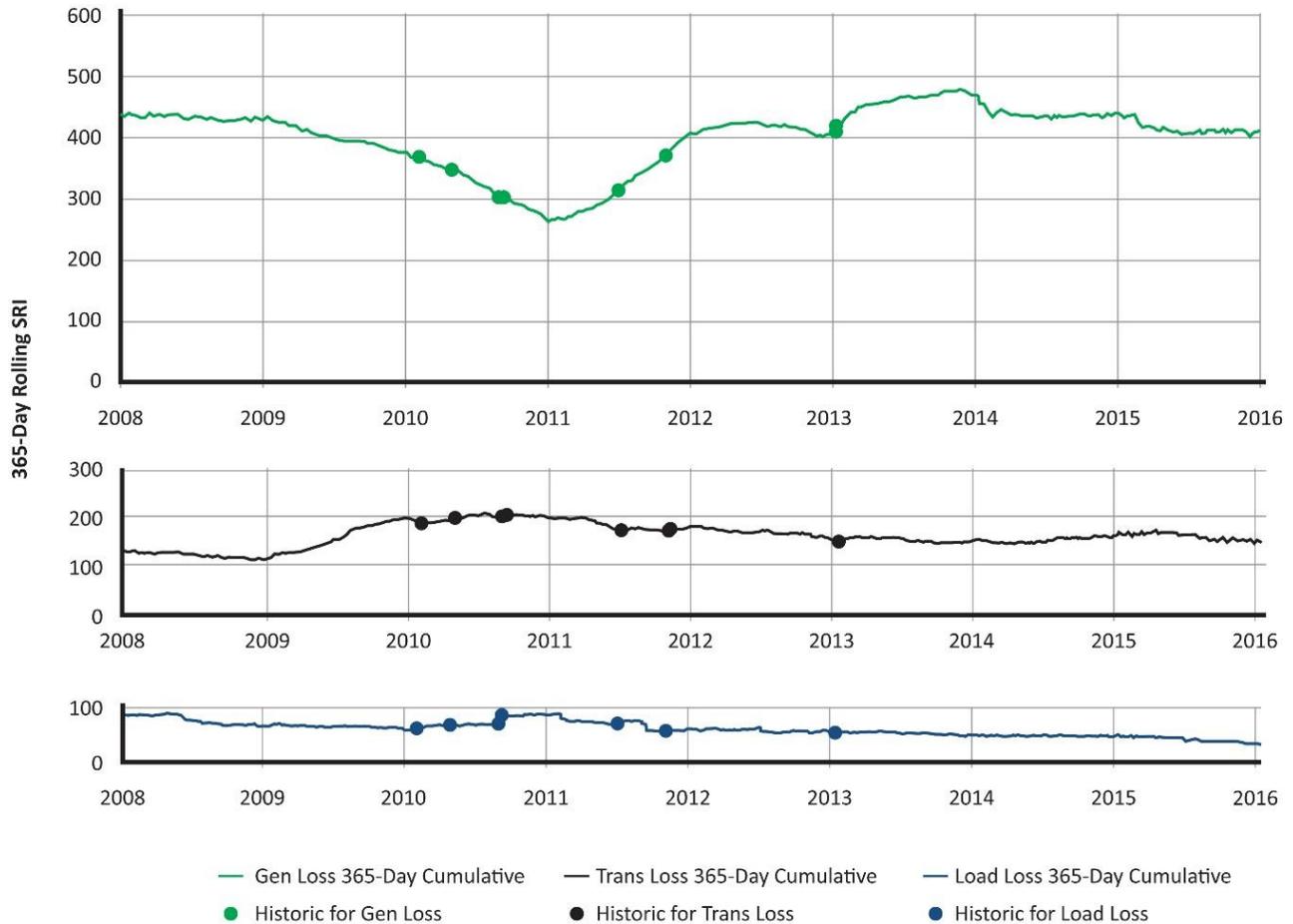


Figure 3.6: 365-day Cumulative SRI 2009–2016 by Component

Overview of TADS Analysis

TADS outage data is used to populate the transmission outage impact component of the SRI. Since transmission outages are a significant contributor to the SRI, the study of their initiating cause codes (ICCs) and sustained cause codes (SCCs) can shed light on prominent and underlying causes affecting the overall performance of the BPS. A complete analysis of TADS data is presented in [Appendix B](#).

NERC performed six focused analytical studies of TADS data from the period 2012–2016 as follows:

1. An ICC analysis of 2012–2016 TADS outage events (momentary and sustained) for ac circuits 200 kV+
2. An ICC analysis of a subset of outage events from Study 1 that included only common/dependent mode (CDM) events with multiple transmission element outages
3. An ICC analysis of 2012–2016 TADS outage events (momentary and sustained) for ac circuits 200 kV+ by Region
4. An ICC analysis of 100 kV+ ac circuit outage events that lasted for more than a minute (defined as a sustained outage event) from 2015–2016
5. For the first time NERC analyzed by ICC 100 kV+ ac circuit and transformer sustained outage events that occurred in 2016
6. The 2015–2016 sustained ac circuit outages were analyzed by SCC

The results of these studies can be summarized with the following observations:

- The ICC Weather (excluding lightning) was a top contributor to transmission outage severity (TOS) of the 2016 sustained events for ac circuits and transformers (Study 5). From 2015 to 2016, the number of the weather-initiated momentary and sustained events of 200 kV+ ac circuits increased by 28 percent (Study 1), and the number of weather-initiated sustained events of 100 kV+ ac circuits increased by 15 percent (Study 4) while the respective TADS inventory increases were below 0.6 percent. Additionally, Weather (excluding lightning) ranks 3rd among sustained causes of ac circuit outages (Study 6).
- The ICC Unknown initiated fewer TADS events in 2016 compared with 2015: the number of Unknown momentary and sustained events of 200 kV+ ac circuits and the number of Unknown sustained events of 100 kV+ ac circuits both reduced. Moreover, from 2015 to 2016, the average transmission severity of sustained events with ICC Unknown statistically significantly reduced while the relative transmission outage risk of this ICC decreased from 16.5 percent to 12.2 percent.
- The number of combined momentary and sustained events of 200 kV+ ac circuits and sustained events of 100 kV+ circuits initiated by Misoperation increased in 2016 (Study 1 and Study 4, respectively). Relative risk of the ICC Misoperation also increased for these two datasets (Studies 1 and 4). For 2012–2016 CDM events), Misoperation is the biggest group and the top contributor to the TOS (Study 2).
- The number of TADS events initiated by Failed AC Circuit Equipment increased significantly in 2016. This was by 43 percent for combined momentary and sustained events of 200 kV+ ac circuits (Study 1) and by 23 percent for sustained events of 100 kV+ ac circuits (Study 4). Events with this ICC, on average, have a smaller TOS, but because of their high frequency of occurrence, they rank as the 3rd contributor of the TOS of sustained events of ac circuits (Study 4). Sustained outages with sustained cause code Failed AC Circuit Equipment are the largest group of ac circuit sustained outages; moreover, they have the longest duration among all sustained outages on average (Study 6).
- The number of combined momentary and sustained events of 200 kV+ ac circuits and of sustained events of 100 kV+ ac circuits both increased from 2015 to 2016, but the average TOS of an event statistically significantly decreased for both datasets (Studies 1 and 4).
- The addition of TADS transformer outages and inventory to the data for sustained events of 100 kV+ ac circuits did not significantly increase the number of events and did not lead to big changes in the ranking of ICCs by size and by relative risk, or other results of the analyses (Studies 4 and 5).

Figures 3.7 and **Figure 3.8** provide a graphic summary of Studies 1 and 4, respectively.

Figure 3.7 represents an analysis of the TOS risk of the 2012–2016 TADS events for the 200 kV+ ac circuits. The x-axis is the magnitude of the correlation of a given ICC with TOS. The y-axis represents the expected TOS of an event when it occurs. The color of the marker indicates if there is a correlation of TOS with the given ICC (positive correlation: red, negative correlation: green, or no significant correlation: blue). The size/area of the marker indicates the probability of an event initiating in any hour with a given ICC and is proportional to the number of events initiated by a given cause. For example, location and size of the Misoperation bubble in **Figure 3.7** indicates that TADS events with an ICC of Misoperation have a significant correlation between how often they will occur and their severity.

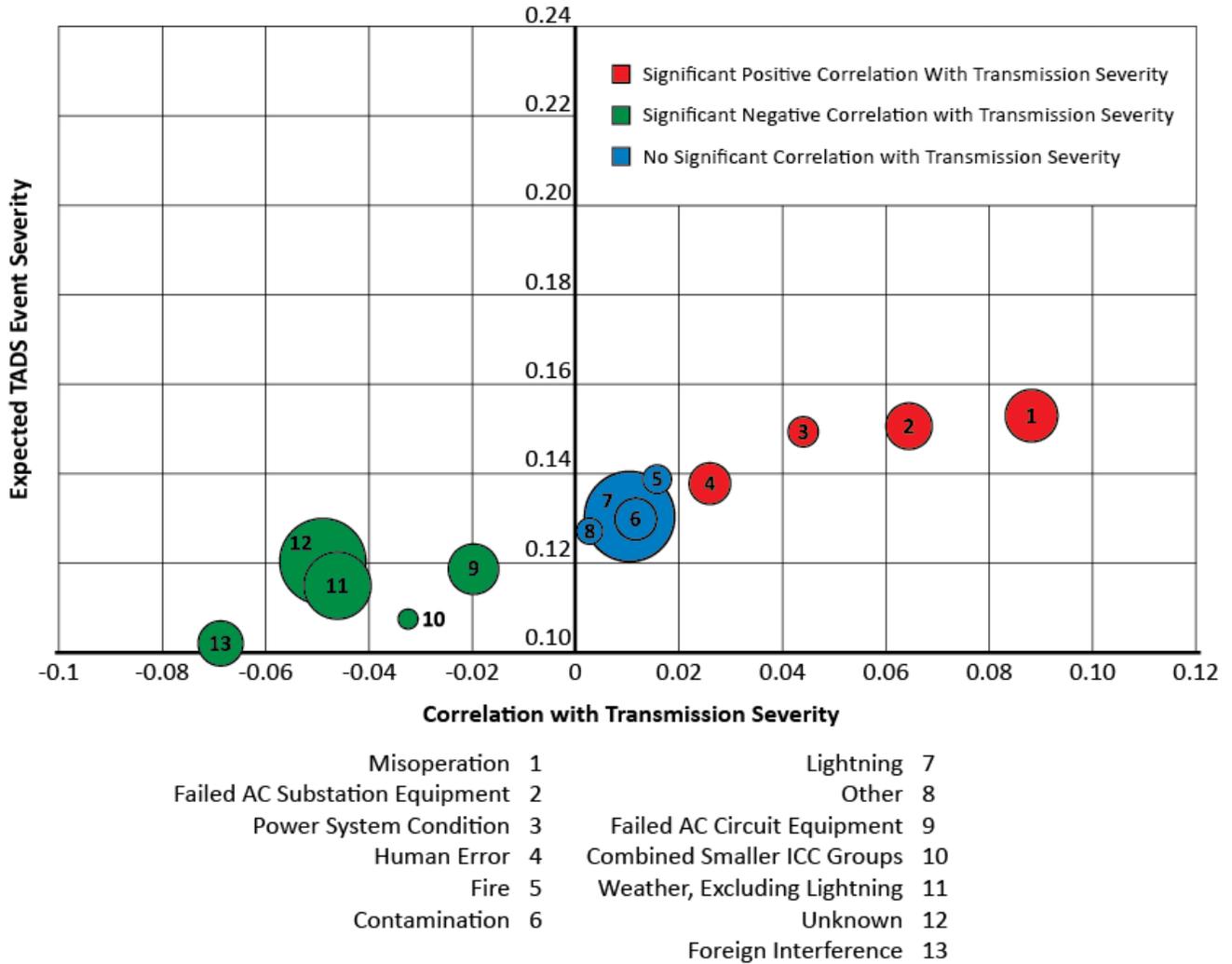


Figure 3.7: Risk Profile of 2012–2016 TADS 200 kV+ AC Circuit Events by ICC

The Misoperation ICC (which represents the TADS ICCs of Failed Protection System Equipment and Human Error associated with Misoperation) and Failed AC Substation Equipment ICC both show a statistically significant positive correlation with TOS and a higher relative transmission risk. Power System Condition, while showing a positive correlation with TOS, has a lower relative transmission risk based on the frequency of these TADS events and their expected TOS. The biggest marker (Lightning) corresponds to the biggest ICC group, which has no significant correlation with TOS but shows a high relative transmission risk because of the high probability of events initiated by lightning. The next two biggest ICC groups, Unknown, and Weather (excluding lightning), have a statistically significant negative correlation with the TOS.

Figure 3.8 represents an analysis of the TOS risk of the 2015–2016 ICC study of sustained events of 100 kV+ ac circuits in the same format. When comparing **Figure 3.7** to **Figure 3.8** (e.g., 2012–2016 TADS 200 kV+ ac circuit momentary and sustained events vs 2015–2016 100 kV+ ac circuits sustained events), 100 kV+ ac circuit sustained events with an ICC of Misoperation have decreased (while still positively correlated) in both occurrence and severity while events with an ICC of unknown have shifted from a negatively correlation between occurrence and severity to positive correlation. Misoperation, Failed AC Substation Equipment, Human Error, and Unknown show a statistically significant positive correlation with TOS and a higher relative transmission risk. Power System Condition, Contamination, and Combined Smaller ICC groups (while showing a positive correlation with TOS) have a lower relative transmission risk based on the small frequency of these events. In contrast, the biggest marker

for Weather (excluding lightning) indicates the highest frequency of weather-initiated events. This leads to the highest relative risk of this group despite a lower TOS of its events.

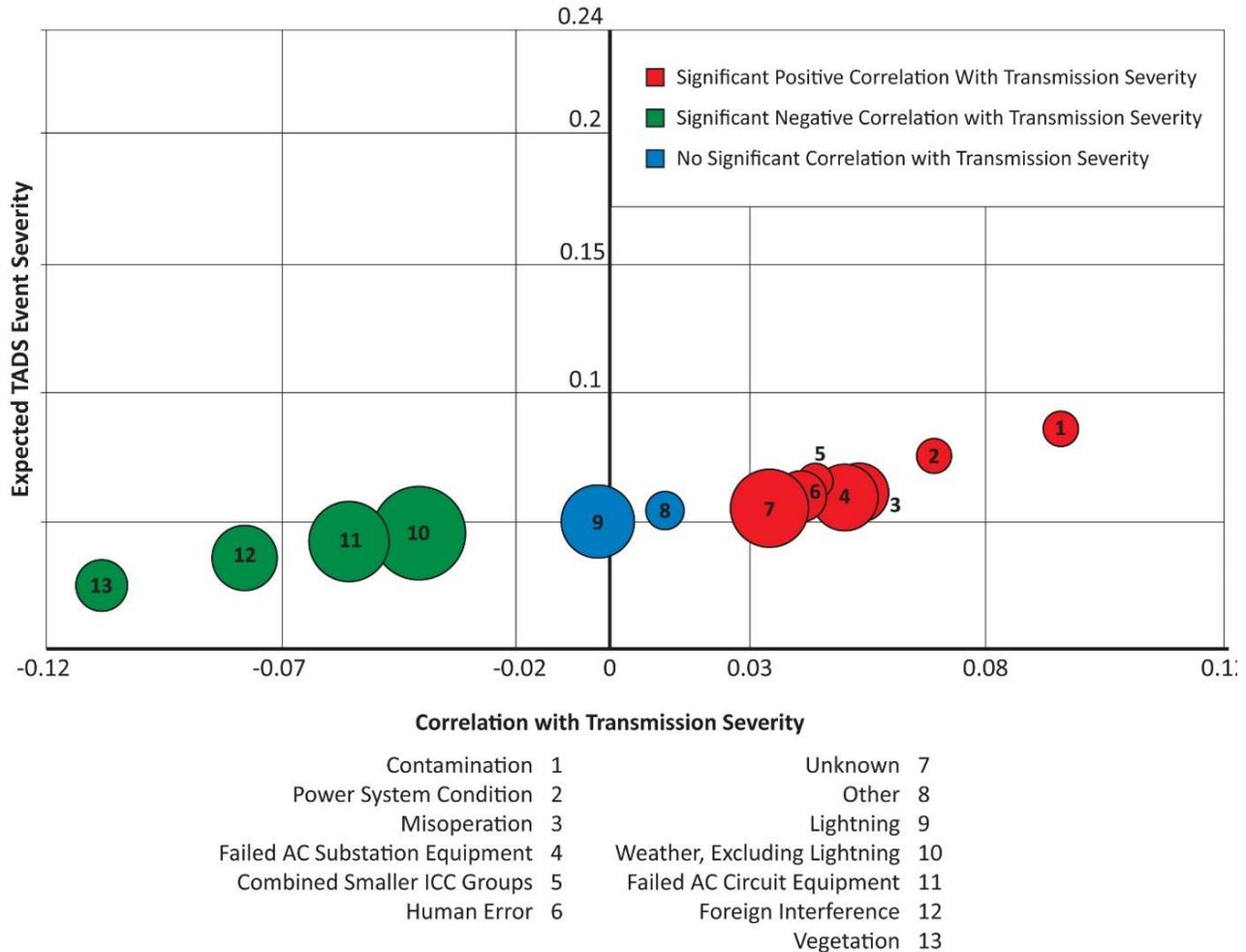


Figure 3.8: Risk Profile of the 2015–2016 Sustained Events of 100 kV+ AC Circuits by ICC

Overview of Generation Availability Data System (GADS) Data Analysis

An analysis of GADS data for calendar years 2012–2016 is presented in [Appendix C](#). GADS outage data is used to populate the generation outage impact component of the SRI. Generation outages are a significant contributor to the 2016 SRI despite the low weighting factor assigned to the generation component. The study of their initiating causes can shed light on prominent and underlying causes affecting the overall performance of the BPS.

An analysis of the age of the existing fleet shows the following:

- An age bubble exists around 37–46 years by a population, consisting of coal and some gas units.
- A significant age bubble around 12–20 years is comprised almost exclusively of gas units.

The data set shows a clear shift toward gas-fired unit additions with the overall age of that fleet across North America being almost 10 years younger than the age of the coal-fired base-load plants that have been the backbone of power supply for many years. This trend is projected to continue given current forecasts around price and availability of natural gas as a power generation fuel as well as regulatory impetus.

GADS contains information used to compute several reliability measures, such as the weighted equivalent forced

outage rate (WEFOR). WEFOR is a metric that measures the probability a unit will not be available to deliver its full capacity at any given time while taking into consideration forced outages and derates. The mean equivalent forced outage rate (EFOR) over the analysis period is 7.1 percent. EFOR has been consistent with a near-exact standard distribution.

To understand generator performance, NERC reviewed the top 10 causes of unit forced outages for the summer and winter seasons³² as well as the annual causes for the 2012–2015 period. The analysis focused on the top causes of forced outages measured in terms of Net MWh of potential production lost. Thus, both the amount of capacity affected and the duration of the forced outages are captured.

Based on the five years of available data since GADS reporting became mandatory, the following observations can be made (as seen in [Table 3.3](#)):

- Severe storms in the last quarter of 2012, such as Hurricane Sandy, caused an increase in the forced outage Net MWh reported for Winter 2013.³³
- The shoulder months of spring/fall in 2014 and 2016 have higher Net MWh attributed to forced outages than the corresponding summer or winter periods.

NERC	Total Annual MWh	Summer MWh	Winter MWh	Spring/Fall MWh
2012	293,475,653	75,914,722	112,989,119	104,571,812
2013	309,011,065	83,422,362	131,422,688	94,166,015
2014	278,987,876	73,610,732	97,782,322	107,594,822
2015	251,795,168	76,955,351	88,651,639	86,188,178
2016	253,530,864	86,112,430	74,256,269	93,162,171

Overview of Demand Response Availability Data System (DADS) Analysis

In 2016, the DADS Working Group (DADSWG) continued efforts to improve data collection and reporting through outreach and development of training materials. Future DADSWG efforts are focused on improving data collection, updating existing materials and developing additional guidance documents, maintaining data quality, and providing observations of possible demand response contributions to reliability.

An analysis of DADS data from 2013 through 2016 provides the following observations:

- Over the 2013–2016 period, the total registered capacity of demand response increased slightly year-over-year in the summer reporting period (2 percent to 10 percent as reflected in [Figure D.1](#)).
- Increases in demand response enrollment in the winter reporting periods continue with a 12.7 percent increase between 2015 and 2016 ([Figure D.1](#)). This increase is due to changes in program rules and the implementation of new wholesale market demand response programs in a single Region.³⁴ The DADS Working Group will continue to monitor and report on trends in enrollment.

³² Winter includes the months of December, January, and February. When analysis is performed on a calendar year basis, as for this report, these three months are included from the same calendar year. Summer includes May through September; all other months are categorized as Spring/Fall.

³³ For this analysis, the season of a forced outage is associated with the season in which the start date of the event was reported in that year; when an event continues into the next year, a new event record is created in January. This results in the event being categorized as occurring in the winter for the continuation event.

³⁴ This conclusion was reached through analysis of data at a nonpublic level that cannot be included in the report. The Region is not identified in the interest of assuring the protection of any reporting entity’s confidentiality.

- With the exception of the summer of 2013, DADS Metric 4 reflects that the realized demand reduction rate continues to be well above 90 percent during both summer and winter periods (see [Figure D.12](#) and [Figure D.13](#)).
- In 2016, the DADSWG did not identify any additional metrics for the data available in DADS.
- The variability at which demand response is deployed may be a function of the demand response programs’ designs rather than an indication of extensive reliability issues within a Region as the SERC Region illustrates.

In [Figure 3.9](#), which shows demand response events reported into DADS from January 2013 through September 2016 (grouped by month for the four years of event data), the black diamond in each column indicates the number of calendar days in a month when demand response was deployed for a reliability event. The stacked bars show the number of days that demand response events occurred in each NERC Region.³⁵ Note that in the SERC Region, demand response was deployed nearly every month during the analysis period, which was a function of a demand response program’s design.

A complete analysis of the DADS data is presented in [Appendix D](#).

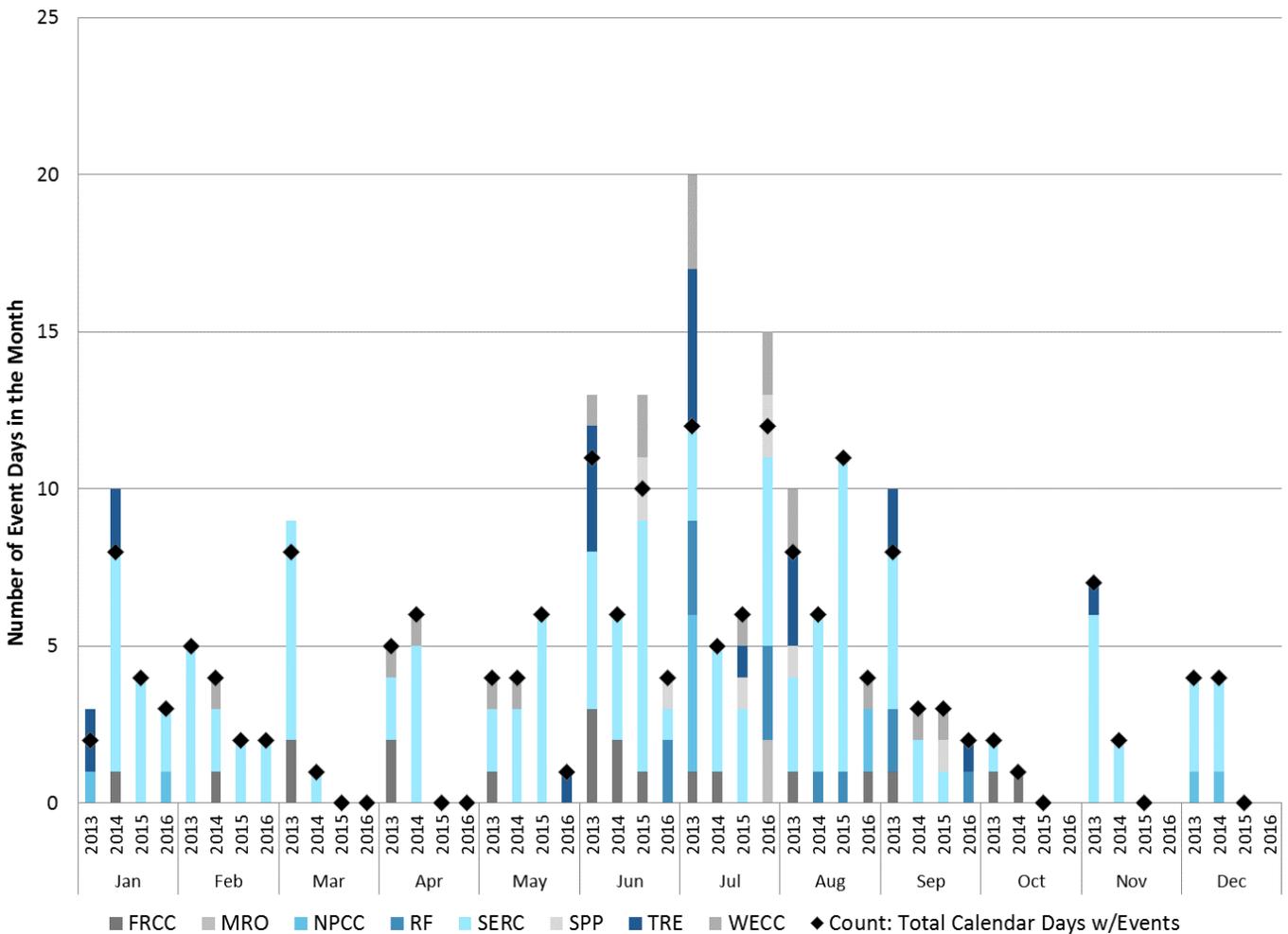


Figure 3.9: Demand Response Events by Month and Region, 2013–2016

³⁵ Event data for October 2016 through December 2016 is not reported until after the publication of this report.

Chapter 4: Reliability Indicator Trends

This chapter provides a summary of the reliability indicators (**Table 4.1**) and follows with a section on select metrics determined to best communicate the state of reliability in 2016, including its most challenging and improving trends and those supporting the key findings detailed in Chapter 1. Other metrics and any supporting material can be found in Appendix E. One particular metric (metric M-4, Interconnection Frequency Response) is discussed in [Chapter 2](#) while details are explored in [Appendix E](#).

NERC reliability indicators tie the performance of the BPS to a set of reliability performance objectives included in the approved 2012 Adequate Level of Reliability (ALR) definition.³⁶ This set of seven NERC reliability performance objectives are mapped to the current reliability indicators,³⁷ denoted as M-X, and are then evaluated to determine whether the BPS meets the ALR definition and whether overall reliability is improving or worsening. **Table 4.1** provides a summary of the trends over the past five years by providing a performance rating of improving, declining, stable, or inconclusive based on analysis of available data. “Inconclusive” is the term used when mixed results prevent determination of a trend over the analysis period.

Summary

When reviewing the reliability indicators it is important to note the following:

- **Table 4.1** lists each reliability indicator with its metric trend rating(s). Additional information for each metric can be found later in this chapter and in [Appendix E](#).
- PAS annually reviews the reliability indicators to identify gaps in performance or data collection. Over time, PAS has implemented changes, added new indicators, and retired some indicators to keep the others relevant. An example of a recent change would be the alignment of M-12 through M-16 to the BES definition. Future developments may include the adoption of ERSWG measures³⁸ with near-term focus on Measure 7: Reactive Capability on the System. PAS has solicited voluntary industry data submission to support the measure, and SAMS is using this data to evaluate the measure’s value.
- Metrics are evaluated over different periods of time. This can be attributed to the period established with the approved metric definition, the duration for what data is available, or other data limitations. For example, M-4 Interconnection Frequency Response has a period defined as “1999 or when data is first available,” and M-12 has a time frame defined as “a rolling five-year average.”
- Metrics may be defined to be NERC-wide, for a specific Region, or on interconnection-level basis.
- The ALR defines the state of the BES to meet performance objectives. Reliability performance and trends of individual metrics should be evaluated within the context of the entire set of metrics.
- It is important to retain the anonymity of individual reporting entities when compiling the data necessary to evaluate metric performance. Details presented in this report are aggregated to maintain the anonymity of individual reporting organizations.

³⁶ Definition of “Adequate Level of Reliability”:

http://www.nerc.com/comm/Other/Adequate%20Level%20of%20Reliability%20Task%20Force%20%20ALR%20Final%20Documents%20Posted%20for%20Stakeholders%20and%20Board%20of%20Trustee%20Review/2013_03_26_ALR_Definition_clean.pdf

³⁷ http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2014_SOR_Final.pdf

³⁸ <http://www.nerc.com/comm/Other/essntlrbltysrvkstskfrDL/ERSTF%20Framework%20Report%20-%20Final.pdf>

Table 4.1: Metric Trends		
Metric	Description	Trend Rating
M-1	Planning Reserve Margin	Stable— Appendix E
M-2	BPS Transmission-Related Events Resulting in Loss of Load (modified in early 2014)	Improving
M-3	System Voltage Performance (discontinued in 2014)	Retired— Appendix E
M-4	Interconnection Frequency Response	Eastern—Improving— Appendix E
		ERCOT—Improving— Appendix E
		Western—Improving— Appendix E
		Québec—Stable— Appendix E
M-5	Activation of Underfrequency Load Shedding (discontinued in 2014)	Retired
M-6	Average Percent Nonrecovery Disturbance Control Standard Events	Stable
M-7	Disturbance Control Events Greater than Most Severe Single Contingency	Stable
M-8	Interconnected Reliability Operating Limit/System Operating Limit (IROL/SOL) Exceedances (modified in 2013)	Eastern—Inconclusive— Appendix E
		ERCOT—Stable— Appendix E
		Western—Stable— Appendix E
		Québec—Retired— Appendix E
M-9	Correct Protection System Operations	Improving
M-10	Transmission Constraint Mitigation (discontinued in 2016)	Retired
M-11	Energy Emergency Alerts (modified in 2013)	Inconclusive
M-12	Automatic AC Transmission Outages Initiated by Failed Protection System Equipment (modified in late 2014)	Circuits—Improving
		Transformers—Improving
M-13	Automatic AC Transmission Outages Initiated by Human Error (modified in late 2014)	Circuits—Inconclusive
		Transformers—Improving
M-14	Automatic AC Transmission Outages Initiated by Failed AC Substation Equipment (modified in late 2014)	Circuits—Stable
		Transformer—Improving
M-15	Automatic AC Transmission Outages Initiated by Failed AC Circuit Equipment (modified in late 2014; normalized by line length)	Declining
M-16	Element Availability Percentage (APC) and Unavailability Percentage (modified in 2013)	Circuits—Inconclusive
		Transformers—Improving

M-2 BPS Transmission-Related Events Resulting in Loss of Load

Background

This metric measures BPS transmission-related events that result in the loss of load, excluding weather-related outages. The underlying data that is used for this metric is important for operators and planners in assessing how effective their design and operating criteria are.

Consistent with the revised metric approved by the OC and PC in March 2014, an “event” is an unplanned disturbance that produces an abnormal system condition due to equipment failures/system operational actions (either intentional or unintentional) that result in the loss of firm system demands. This is identified by using the subset of data provided in accordance with Reliability Standard EOP-004-2.³⁹ The reporting criteria for such events, beginning with data for events occurring in 2013, are as follows:⁴⁰

1. 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
2. A BES emergency that requires manual firm load shedding of 100 MW or more
3. A BES emergency that resulted in automatic firm load shedding of 100 MW or more (via automatic undervoltage or underfrequency load shedding schemes, or special protection systems (SPSs)/remedial action schemes (RASs))
4. 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

PAS reviewed this M-2 metric in 2013 and made changes to its criteria to increase consistency with EOP-004-2 criteria for reporting transmission-related events that result in loss of load. The criteria presented above were approved for implementation in the first quarter of 2014. Changes in the annual measurement between 2012 and 2013 therefore reflect the addition of Criteria 4, which has been applied to the data since 2013. For the first part of the analysis below, shown in [Figure 4.1](#) and [Figure 4.2](#), historical data back to 2002 was used and the new Criteria 4 was not included to allow trending of the other aspects of the metric over time. [Figure 4.3](#) includes all of the criteria, so it was only evaluated for 2013–2016: the time period for which data collection associated with the new criteria was available. The performance trend is continuing to improve.

Assessment

[Figure 4.1](#) shows the number of BPS transmission-related events that resulted in the loss of firm load from 2002–2016. On average, just under eight events were experienced per year. The BPS experienced four transmission load loss events in 2016. This continues a mixed but improved trend since 2012 in the number of events.

[Figure 4.2](#) indicates that the top three years in terms of load loss remain 2003, 2008, and 2011 due to the major loss-of-load events that occurred. In 2003 and 2011, one event accounted for over two-thirds of the total load loss, while in 2008, a single event accounted for over one-third of the total load loss.

Load loss excluding Criteria 4 is less for 2016 than for any year since 2002 inclusive. Load loss over the last four years remains below the median value. This also continues a mixed, but improved, trend since 2011 in the total annual load loss from these events.

³⁹ <http://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-004-2.pdf>

⁴⁰ http://www.nerc.com/comm/PC/Performance%20Analysis%20Subcommittee%20PAS%202013/ALR1-4_Revised.pdf

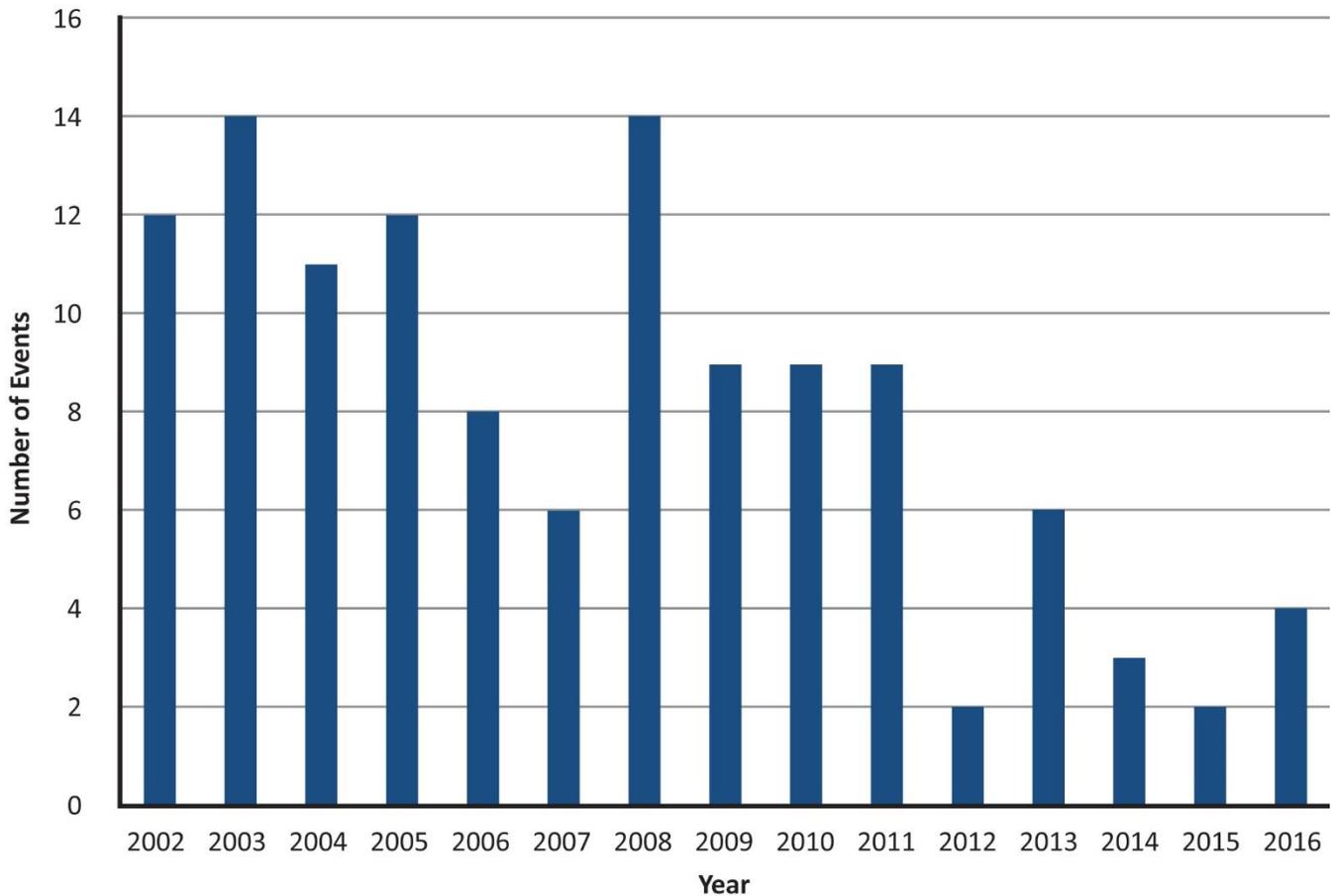
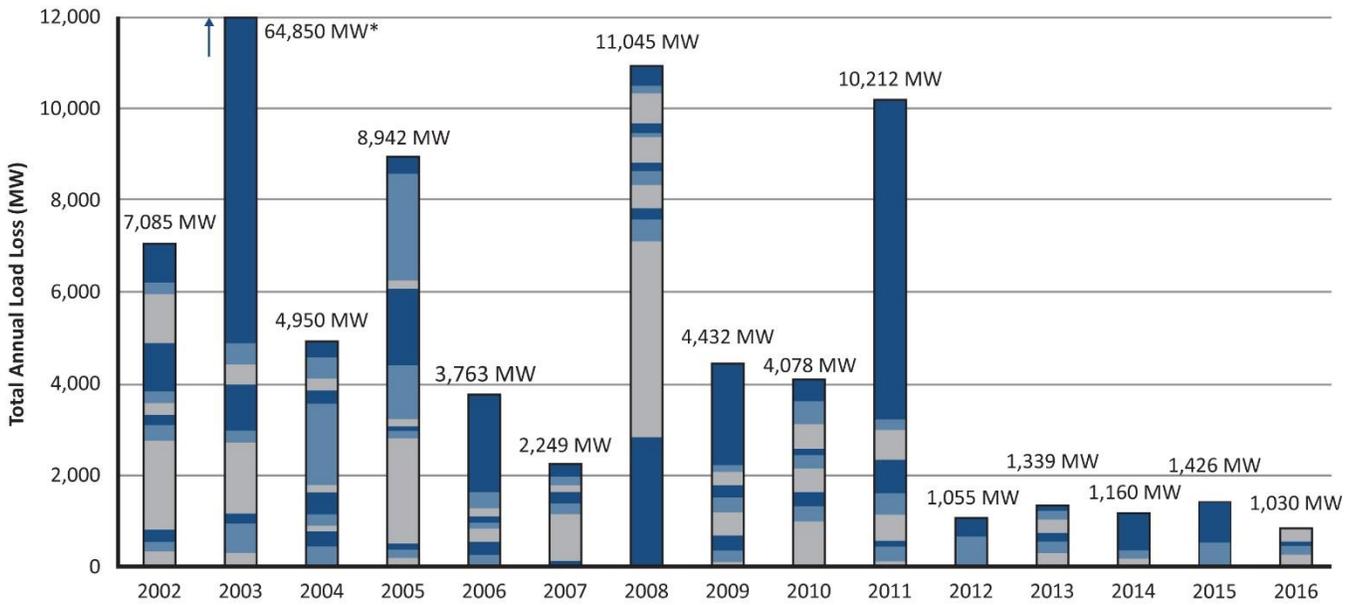


Figure 4.1: M-2 BPS Transmission Related Events Resulting in Load Loss (Excluding Criteria 4)



Each band of color represents a different event.

*Vertical axis scale has been reduced due to large value of 2003 NE blackout event.

Figure 4.2: M-2 BPS Transmission-Related Events Resulting in Load Loss (Excluding Criteria 4)

Figure 4.3 shows the number of events resulting in firm load loss of 50 MW or greater from 2013–2016 and their durations. The metric was modified in 2013 to include Criteria 4 events. There were 14 events during 2016 (10 under Criteria 4. See Figure 4.2) with load loss of ≥ 50 MW. For 2016 the largest number of load loss events was once again in the category of less than one hour in duration.

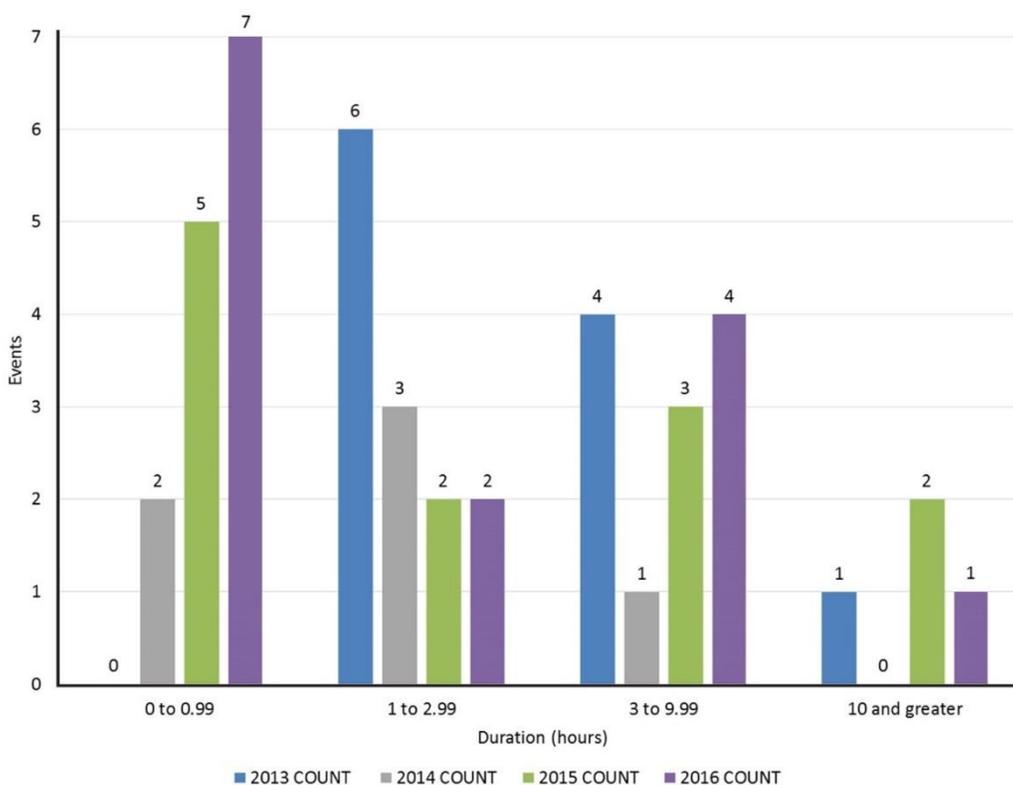


Figure 4.3: Outage Duration vs. Events

The major significance of this metric is found in the detailed data that supports the Criteria 4 events captured in Figure 4.3 that cannot be shared in this report in an attributable form due to confidentiality requirements. The initiating cause and, where applicable, the contributing factor(s) of these 10 events support the message of the other metrics in this chapter and validate the approaches in use by NERC and the entire ERO Enterprise. These are listed in Table 4.2.

Event Number	Initiating Cause	Contributing Factor(s)
1	Circuit Equipment Failure	
2	Protection System Misoperation	
3	Circuit Equipment Failure	
4	Protection system Misoperation	
5	Human Error	Misoperation

Table 4.2: 2016 Criteria 4 Initiating Cause and Contributing Cause(s)		
Event Number	Initiating Cause	Contributing Factor(s)
6	Circuit Equipment Failure	
7	Circuit Equipment Failure	Misoperation
8	Protection System Misoperation	Circuit Equipment Failure
9	Circuit Equipment Failure	Protection System Misoperation
10	Circuit Equipment Failure	Protection System Misoperation

Of the 10 events, six have the initiating cause of Circuit Equipment Failure, three with the contributing factor of Misoperation; three have the initiating cause of Protection System Misoperation, one of these with the contributing factor of Circuit Equipment Failure; and one of these has the initiating cause of Human Error with the contributing factor of Misoperation.

M-9 Correct Protection System Operations

Background

The correct protection system operations metric demonstrates the performance of protection systems (both generator and transmission) on the BPS. The metric is the ratio of correct protection system operations to total system protection system operations.

Protection system misoperations have been identified as a major area of concern as stated in previous *State of Reliability* reports. Improvements to data collection that the System Protection Control Subcommittee (SPCS) proposed were implemented as a result.⁴¹ NERC coordinates with each Region as well as these groups to continue the focus on improvements. Both correct operations and misoperations are including in the reporting below.

Assessment

Figure 4.4 shows the total correct operations rate for NERC through the first three reporting quarters of 2016.

⁴¹http://www.nerc.com/comm/PC/Protection%20System%20Misoperations%20Task%20Force%20PSMTF%202/PSMTF_Report.pdf

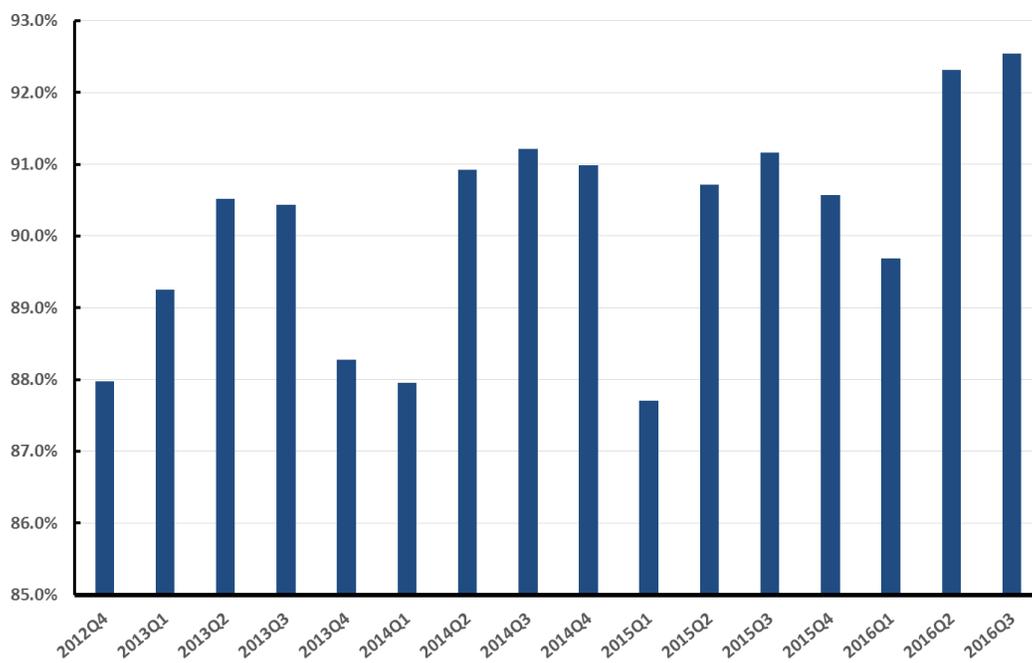


Figure 4.4: Correct Protection System Operations Rate

Figure 4.5 shows the regional misoperation rates and summarizes results of the statistical tests⁴² on misoperation rate comparisons. The dark blue bars show the rates that are statistically significantly higher than NERC’s rate of 9.5 percent, as shown in Table E.24, and the light blue bars correspond to the rates significantly lower than NERC’s rate. NPCC’s rate was calculated based on the Q1 2013–Q3 2016 data. WECC’s rate was calculated based on Q2 and Q3 2016 data when they became available.

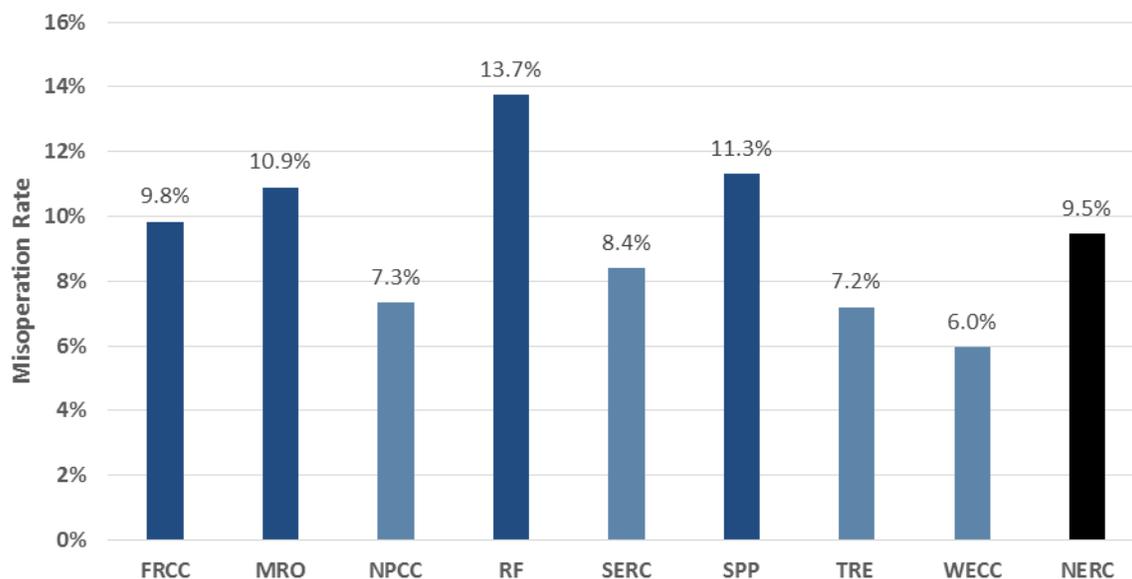


Figure 4.5: Four-Year Misoperation Rate by Region (Q4 2012–Q3 2016)

⁴² Large sample test on population proportions at the 0.05 significance level

Year-Over-Year Changes by Region

Changes from the first four quarters (Q4 2012–Q3 2013, Year 1) to the second four quarters (Q4 2013–Q3 2014, Year 2) to the third four quarters (Q4 2014–Q3 2015, Year 3) to the fourth four quarters (Q4 2015–Q3 2016, Year 4) were studied to compare time periods with similar composition of seasons.⁴³ For Year 4, the misoperation rate is calculated in two ways: 1) with all Regions (excluding WECC) and 2) with WECC misoperation and operation counts included for Q2 and Q3 2016. The changes are shown in **Figure 4.6**.

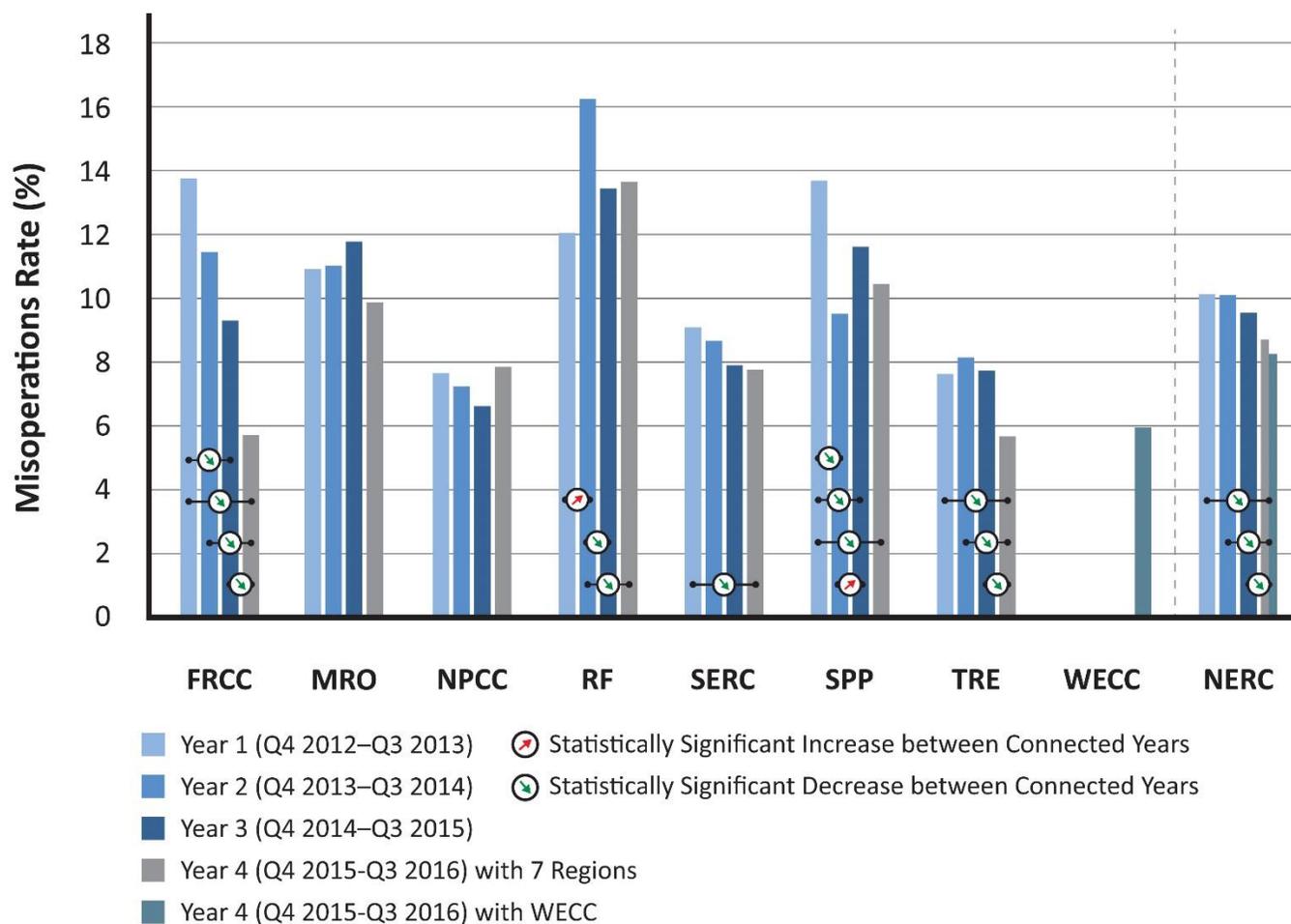


Figure 4.6 Year-Over-Year Changes in Misoperation Rate by Region and NERC

In **Figure 4.6**, Regions are listed alphabetically from left to right with the total misoperation rate for NERC on the far right. Tests⁴⁴ on misoperation rates found the statistically significant year-to-year changes shown in **Figure 4.6** by arrows. Red arrows signify increased rates and green arrows signify decreased rates.

Table 4.3 lists the Regional misoperation rates that are shown graphically in **Figure 4.6**.

⁴³ Year-over-year changes in historical rates shown in this report reflect improvements in data quality resulting from the standardization and automation of the collection of protection system operations and misoperations data in 2016.

⁴⁴ Large sample test on population proportions at the 0.05 significance level

Table 4.3: Misoperation Rate by Region and NERC—by Year					
Region	Year 1 (Q4 2012-Q3 2013)	Year 2 (Q4 2013-Q3 2014)	Year 3 (Q4 2014-Q3 2015)	Year 4 (Q4 2015-Q3 2016, 7 Regions)	Year 4 (Q4 2015-Q3 2016, Last 2 Quarters with WECC)
FRCC	13.7%	11.4%	9.3%	5.7%	5.7%
MRO	10.9%	11.0%	11.8%	9.9%	9.9%
NPCC (Q1 2013 to Q3 2016)	7.7%	7.2%	6.6%	7.9%	7.9%
RF	12.1%	16.2%	13.4%	13.6%	13.6%
SERC	9.1%	8.7%	7.9%	7.8%	7.8%
SPP	13.7%	9.5%	11.6%	10.4%	10.4%
TRE	7.6%	8.2%	7.7%	5.7%	5.7%
WECC (Q2 and Q3 2016 only)					6.0%
NERC	10.2%	10.1%	9.5%	8.7%	8.3%

In **Figure 4.7**, Regions are listed alphabetically from left to right with the total NERC rate on the far right of the combined misoperation rate of the top three causes of misoperations (Incorrect Settings/Logic/Design Errors, Relay Failures/Malfunctions, and Communication Failures) for the four years.

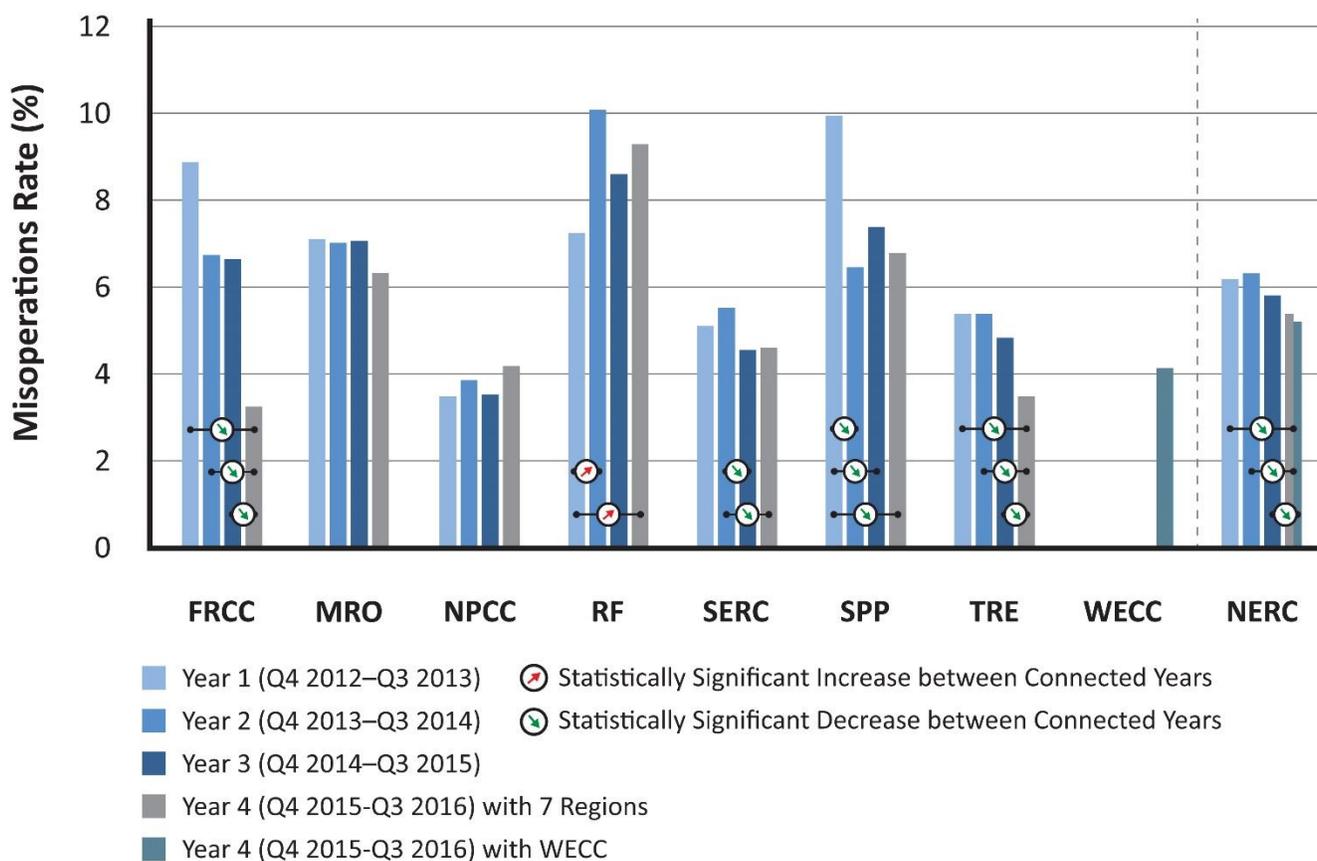


Figure 4.7: Year-Over-Year Changes in Misoperation Rate for Top Three Causes by Region and NERC

Tests⁴⁵ on misoperation rates for the top three causes combined found the statistically significant year-to-year changes shown in **Figure 4.7** by arrows. Red arrows signify increased rates and green arrows signify decreased rates. These observations confirm an improving performance of M-9.

Actions to Address Misoperations

NERC is revising a number of Reliability Standards that involve protection systems.⁴⁶ To increase awareness and transparency, NERC will continue to conduct industry webinars⁴⁷ on protection systems and document success stories on how entities achieve higher levels of protection system performance. The quarterly protection system misoperation trends of NERC and the REs can be viewed on NERC's website.⁴⁸

In addition, NERC and Regional staff have again analyzed the top three protection system misoperation cause codes reported by the Regions and NERC through compliance with Reliability Standard PRC-004-2.1a to identify RE trends and provide guidance to protection system owners that experience a high number of misoperations.⁴⁹ Incorrect Setting/Logic/Design Errors was found to still be the largest source of misoperations in almost every Region. This supports the focus on setting/logic/design controls, and REs are also pursuing targets specific to [each Region's own results](#). NERC and Regional staff also updated the reporting template to separate the "Incorrect Setting/Logic/Design Errors" into "Incorrect Settings," "Logic Errors," and "Design Errors" to provide more granular information for their mitigation. NERC and industry actions identified in the report are expected to result in a statistically significant reduction in the rate of misoperations due to these causes by the end of 2017.

The ERO Enterprise determined from EA data and from industry expertise that a sustained focus on education regarding the instantaneous ground overcurrent protection function and on improving relay system commissioning tests were actionable and could have a significant effect. The relay ground function accounted for 11 misoperations in 2014, causing events that were analyzed due to voluntary entity reporting and cooperation. That was reduced to six event-related misoperations in 2015, and further reduced to one event-related operation in 2016. Similarly, one Region experienced a statistical improvement in relay misoperations from 2013–2014 and maintained this performance through 2016. This performance followed Regional efforts that targeted a reduction of communication failures.

Based on the statistically significant increase in the total correct operation rate and the reduction in NERC's misoperation rate from 9.5 percent in 2015 to 8.7 percent in 2016, the performance trend for this metric is considered to be improving. Further statistical analysis can be found in [Appendix E](#).

M-12 through M-14 Automatic AC Transmission Outages

Background

These metrics measure the impacts of Failed Protection System, Human Error, and Failed AC Substation Equipment respectively as factors in the performance of the ac transmission system. The metrics use the TADS data and definitions. The metrics were enhanced in 2014 and 2015 to be consistent with the collection of BES data in TADS and to align with the definition of the BES and include some equipment to 100 kV.⁵⁰ With the revisions, the metrics include any BES ac transmission element outages that were initiated by the following:

- M-12: TADS Initiating Cause Code (ICC) of Failed Protection System Equipment
- M-13: TADS Initiating Cause Code (ICC) of Human Error

⁴⁵ Large sample test on population proportions at the 0.05 significance level

⁴⁶ <http://www.nerc.com/pa/Stand/Standards-Under-Development.aspx>

⁴⁷ http://www.nerc.com/files/misoperations_webinar_master_deck_final.pdf

⁴⁸ <http://www.nerc.com/pa/RAPA/ri/Pages/ProtectionSystemMisoperations.aspx>

⁴⁹ [http://www.nerc.com/pa/RAPA/PA/Performance Analysis DL/NERC Staff Analysis of Reported Misoperations - Final.pdf](http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC%20Staff%20Analysis%20of%20Reported%20Misoperations%20-%20Final.pdf)

⁵⁰ <http://www.nerc.com/pa/RAPA/Pages/BES.aspx>

- M-14: TADS Initiating Cause Code (ICC) of Failed AC Substation Equipment

Each metric is calculated for ac circuits and transformers separately in sub-metrics as follows:

- The continued normalized count (on a per circuit basis) of 200 kV+ AC transmission element outages (i.e., TADS momentary and sustained automatic outages) that were initiated by Failed Protection System Equipment, Human Error, or Failed AC Substation Equipment.
- Beginning January 1, 2015, the normalized count (on a per circuit basis) of 100 kV+ AC transmission element outages (i.e., TADS sustained automatic outages) that were initiated by Failed Protection System Equipment, Human Error, or Failed AC Substation Equipment.

Assessment M-12 through M-14 AC Circuit Outages

Changes of the metrics by year are shown in [Figures 4.8](#) through [Figure 4.10](#) which present the ac circuit outages two sub-metrics: 1) the annual frequency of automatic outages per 200 kV+ ac circuit, for the time period 2012–2016, and 2) the annual frequency of sustained automatic outages per 100 kV+ ac circuit, for the time period 2015–2016.

Overall, the performance of M-12 through M-14 ac circuit outages is inconsistent. There is improved performance of M-12 in ac circuits Failed Protection System Equipment; however, M-12 had no significant change from 2015–2016. Performance of M-13 for ac circuits Human Errors was inconsistent. M-13 had a significant increase from 2015–2016. M-14 for ac circuits Failed Protection System Equipment had stable performance, yet M-14 had no significant change from 2015–2016.

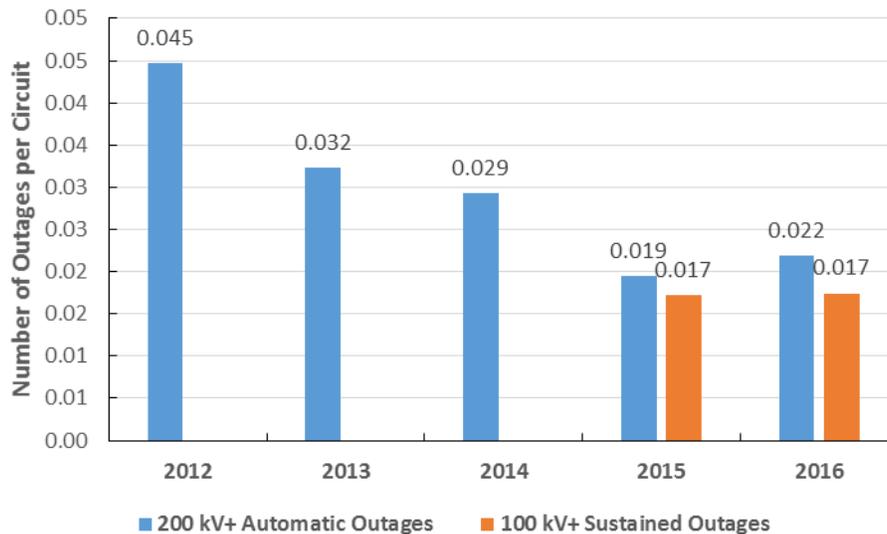


Figure 4.8: AC Circuit Outages Initiated by Failed Protection System Equipment (M-12)

The calculated annual outage frequencies, per ac circuit, were tested to identify significant year-to-year changes of the reliability metric. Below is a summary of M-12 performance for the five years:

- Statistically significant decrease from 2012–2013 and from 2014–2015
- No significant changes from 2013–2014 and from 2015–2016
- The 2016 outage frequency is significantly lower than in each year from 2012–2014

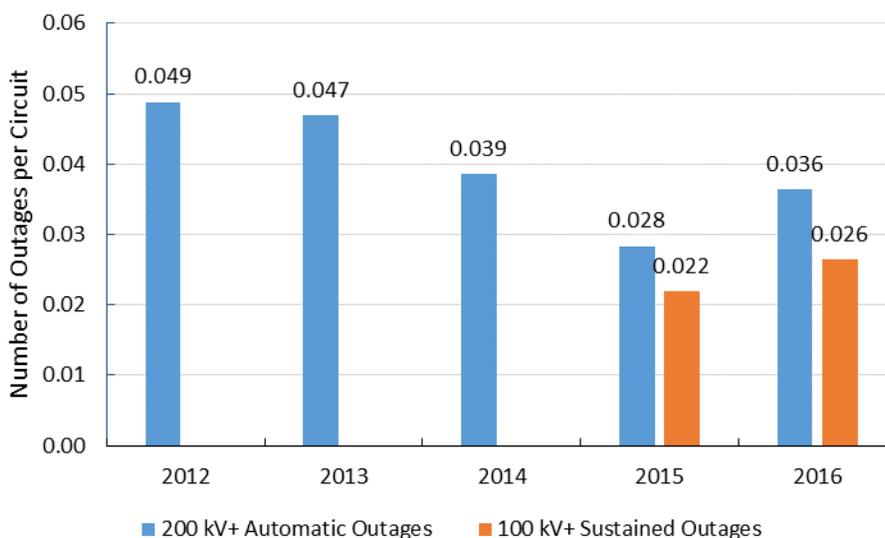


Figure 4.9: AC Circuit Outages Initiated by Human Error (M-13)

The calculated annual outage frequencies per ac circuit were tested to identify significant year-to-year changes of the reliability metric. Below is a summary of M-13 performance for the five years:

- Year-to-year decreases from 2012–2014 with no statistically significant changes from 2012–2013 and from 2013–2014
- Statistically significant decrease from 2014–2015
- Statistically significant increase from 2015–2016
- The 2016 outage frequency is statistically significantly lower than in each year from 2012–2013

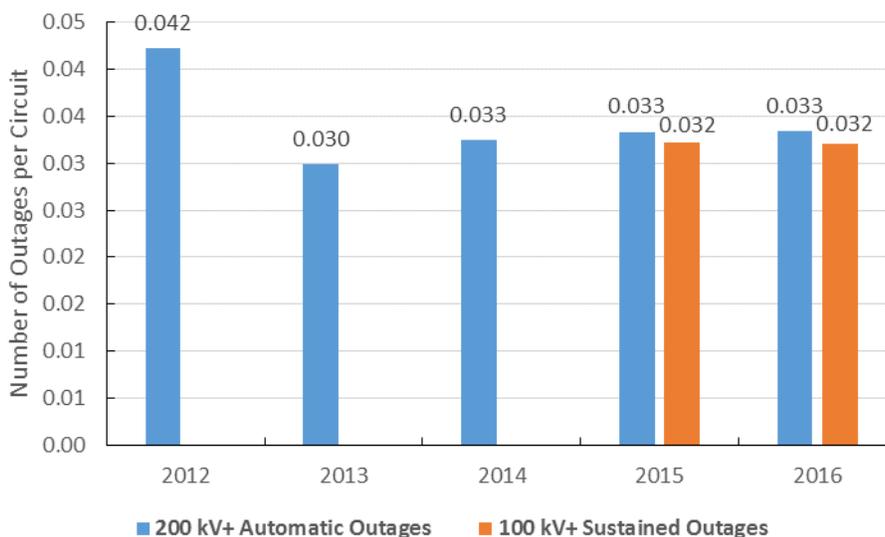


Figure 4.10: AC Circuit Outages Initiated by Failed AC Substation Equipment (M-14)

The calculated annual outage frequencies per ac circuit were tested to identify statistically significant year-to-year changes of the reliability metric. Below is a summary of M-14 performance for the five years:

- Statistically significant decrease from 2012–2013

- No statistically significant changes from 2013–2014, from 2014–2015, and from 2015–2016
- The 2016 outage frequency is significantly lower than in 2012

Assessment M-12 through M-14 Transformer Outages

Changes of the metrics by year are shown in **Figures 4.11** through **Figure 4.13** which present the transformer outages sub-metrics as follows: 1) the annual frequency of automatic outages per 200 kV+ transformer for the time period 2012–2016, and 2) the annual frequency of sustained automatic outages per 100 kV+ transformer for the time period 2015–2016.

Overall, the performance of M-12 through M-14 transformer outages is improving. Performance of M-12 for Transformers Failed Protection Equipment is improving while M-12 had no significant change from 2015–2016. Observations confirm a stable performance for the five years and an improved performance since 2013 of M-13 for Transformer Human Error, and M-13 had no significant change from 2015–2016. Performance of M-14 for Transformer Failed AC Substation Equipment has improved, and M-14 had no significant change from 2015–2016.

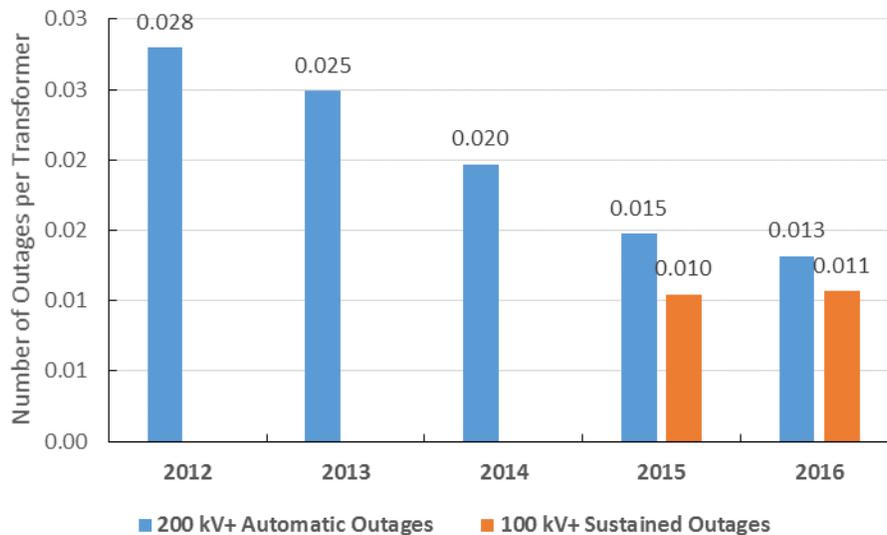


Figure 4.11: Transformer Outages Initiated by Failed Protection System Equipment (M-12)

The calculated annual outage frequencies per transformer were tested to identify significant year-to-year changes of the reliability metric. Below is a summary of M-12 performance for the five years:

- Year-to-year decreases from 2012–2015 with no statistically significant changes for any pair of consecutive years
- The 2016 outage frequency is lower than in each year from 2012–2015 and statistically significantly lower than in 2012–2013

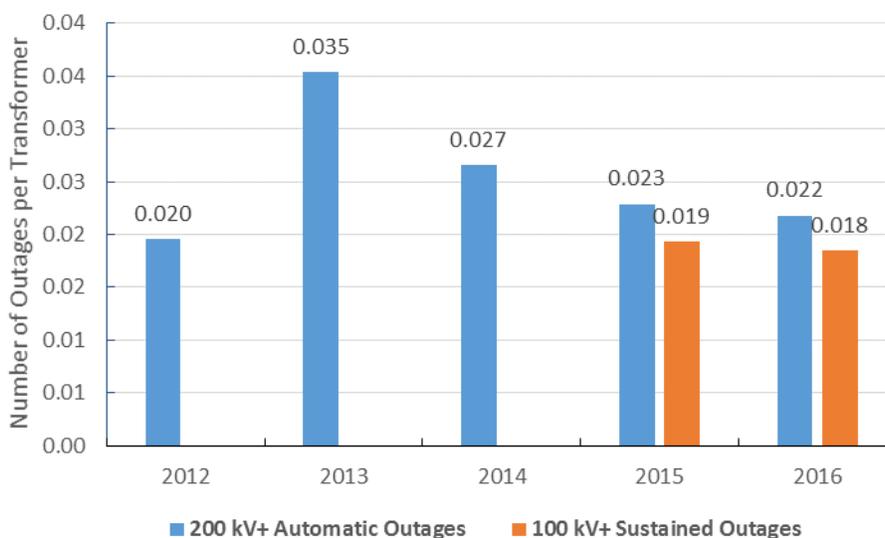


Figure 4.12: Transformer Outages Initiated by Human Error (M-13)

The calculated annual outage frequencies per transformer were tested to identify statistically significant year-to-year changes of the reliability metric. Below is a summary of M-13 performance for the five years:

- Annual decreases from 2013–2016
- Statistically significant decrease from 2013–2015
- The 2016 outage frequency is lower than in 2013, 2014, and 2015 and statistically significantly lower than in 2013

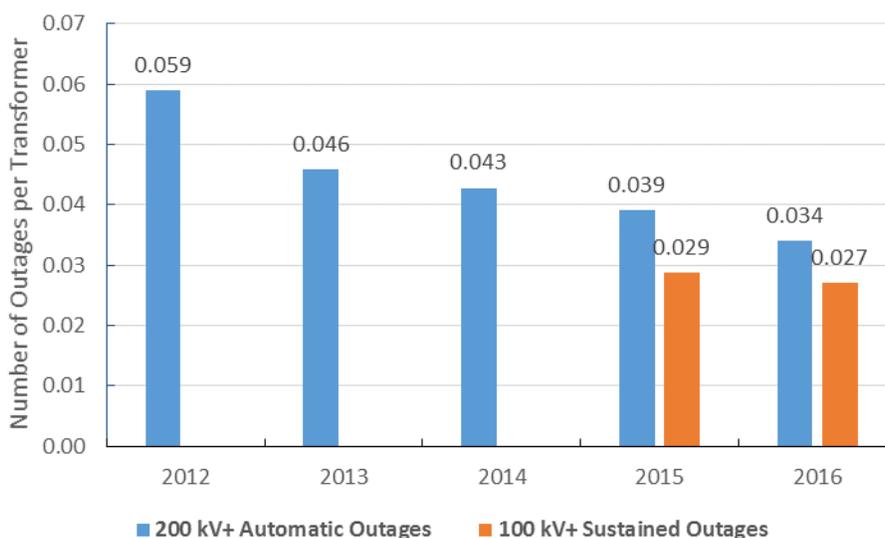


Figure 4.13: Transformer Outages Initiated by Failed AC Substation Equipment (M-14)

The calculated annual outage frequencies per transformer were tested to identify significant year-to-year changes of the reliability metric. Below is a summary of M-14 performance for the five years:

- Year-to-year decreases from 2012–2016 with no significant changes between any two consecutive years
- The 2016 outage frequency is lower than in any other year and statistically significantly lower than in 2012

M-15 Automatic AC Transmission Outages Initiated by Failed AC Circuit Equipment

Background

This metric measures the impact of Failed AC Circuit Equipment as one of many factors in the performance of ac transmission systems. Metric M-15 follows the same methodology described for M-12 through M-14 except that it uses a normalization based on a line length and is defined for ac circuits only. As with M-12 through M-14 the sub-metrics are calculated as follows:

- The continued normalized count (on a per 100 circuit-mile basis) of 200 kV+ ac transmission circuit outages (i.e., TADS momentary and sustained automatic outages) initiated by Failed AC Circuit Equipment
- Beginning January 1, 2015, the normalized count (on a 100 per circuit-mile basis) of 100 kV+ ac transmission circuit outages (i.e., TADS sustained automatic outages) initiated by Failed AC Circuit Equipment

Assessment

Changes of M-15 by year are shown in [Figure 4.14](#). [Figure 4.14](#) presents M-15 (blue), the annual frequency of automatic outages per hundred miles for ac circuits of 200 kV+, for the time period 2012–2016 and M-15 (orange), the annual frequency of sustained automatic outages per hundred miles for ac circuits of 100 kV+, for the time period 2015–2016.

For the years 2012–2016, M-15 performance was declining, demonstrated by an increase in outage frequency. This is also seen in M-15 from 2015–2016.

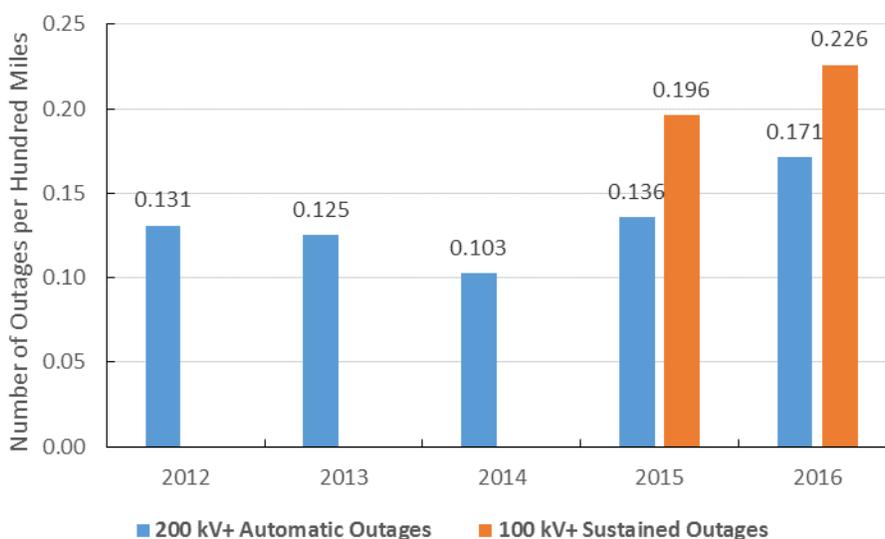


Figure 4.14: AC Circuit Outages Initiated by Failed AC Circuit Equipment

The observed changes in the calculated frequencies cannot be statistically analyzed due to a mile-based normalization (these numbers do not represent observations in a statistical sample) and can be only compared numerically. The annual outage frequencies per hundred-mile ac circuit decreased every year from 2012–2014 and then increased in 2015 and again in 2016. The 2016 frequency was the largest after 2011.

M-16 Element Availability Percentage and Unavailability Percentage

Background

The element availability percentage (APC) and unavailability percentage metric determines the percentage of BES ac transmission elements that are available or unavailable when outages due to automatic and nonautomatic events are considered.

Originally, there were two metrics: one to calculate availability and one to calculate unavailability, but these were combined into one metric in 2013. This metric continues to focus on availability of elements at 200 kV+ because the components of the calculation included planned outages (these are no longer collected in TADS since 2015), unplanned outages (these are collected in TADS for all BES elements), and operational outages (these are only collected in TADS for 200 kV+). Therefore, the reporting voltage levels for this metric did not change.

Assessment

For both transmission element types, ac circuits, and transformers, only charts for unavailability are shown because annual unavailability can be broken down by outage type (unlike availability). This is important since a part of unavailability due to planned outages is shown for 2012–2014 and removed for 2015–2016 due to changes in TADS data collection.

Figure 4.15 presents 200 kV+ ac circuit unavailability as a percentage for the time period 2012–2016. Note that in 2015–2016 unavailability due to planned outages is removed from the definition and calculation. In 2012–2013, this portion of unavailability was the largest of the three.

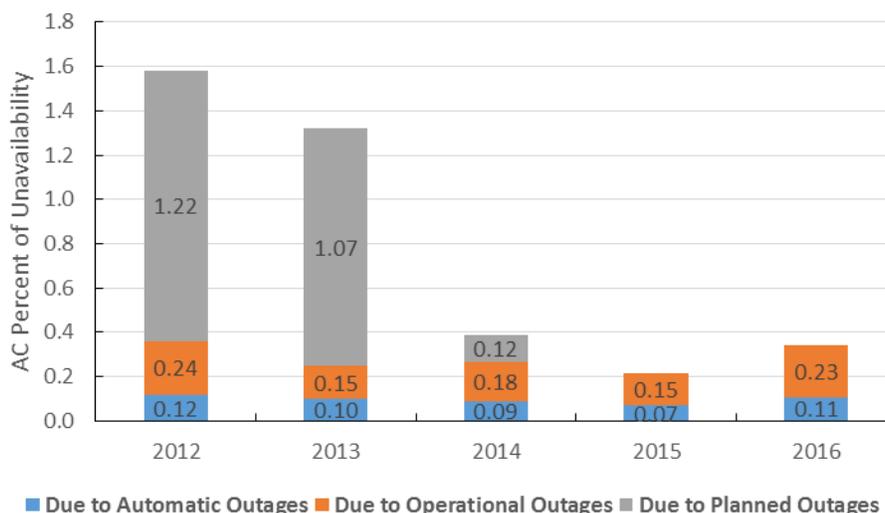


Figure 4.15: AC Circuit Unavailability by Year and Outage Type

The ac circuit combined unavailability, due to operational and automatic outages in 2016, was the second largest from 2012–2016.

Figure 4.16 presents 200 kV+ TADS transformer unavailability as a percentage for the time period 2012–2016. Since 2015, unavailability due to planned outages has been removed from the definition and calculation. In 2012–2014, this portion of unavailability was the largest of the three.

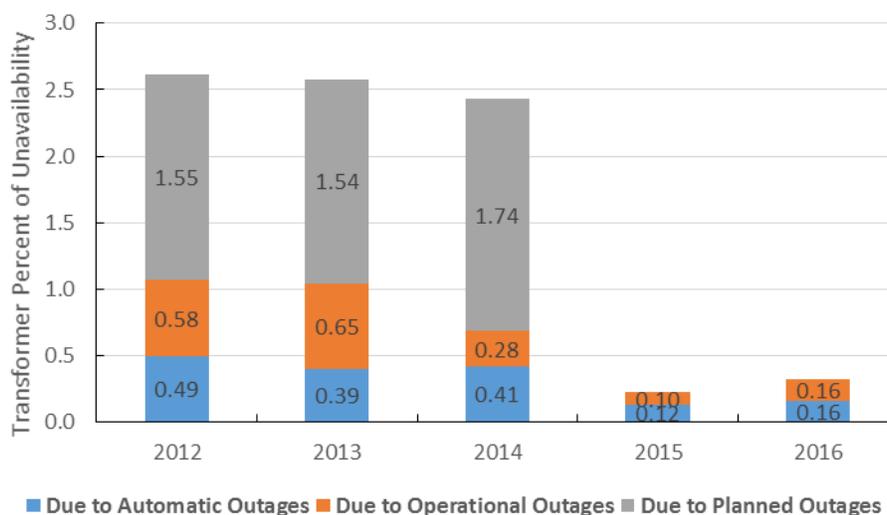


Figure 4.16: Transformer Unavailability by Year and Outage Type

Transformer unavailability due to operational and automatic outages in 2016 was the second lowest from 2012 to 2016.

The performance trend of M-16 for ac circuits is inconclusive and for transformers is considered to be improving. It is worth noting that a sizable change in transformer inventory occurred in 2015 due to changes in TADS reporting and that additional year-over-year data will be needed before drawing definite conclusions.

Chapter 5: Enforcement Metrics for Risk and Reliability Impact

The Compliance and Certification Committee (CCC) and PAS developed two compliance-based metrics with a focus on compliance violation's risk to and impact upon the BPS. When reviewing the enforcement metrics, it is important to keep the following considerations in mind:

- A violation that could create a potentially serious risk to reliability may not have an actual impact on reliability.
- A violation that results in some adverse impact to the BPS may not have created a serious risk to reliability.
- Not all incidents on the BPS are the results of violations of a Reliability Standard.

The ERO Enterprise assesses and handles violations as the noncompliance is identified by registered entities and RE compliance monitoring activities. With the RE's implementation of risk-based compliance monitoring and enforcement, the REs can focus their review on serious-risk violations. Some serious-risk violations occurring prior to 2016 are yet to be fully investigated and filed with FERC. As the REs conclude the investigation and mitigation of those serious-risk violations and NERC files notices of penalty (NOPs) with FERC, the counts of serious-risk violations reported in this chapter may increase.

CP-1: Risk Metric

Compliance Process-1 (CP-1) is a quarterly count of violations⁵¹ determined to have posed a serious risk to the reliability of the BPS.⁵² This metric tracks serious-risk violations based on the quarter when the violations occurred.

Figure 5.1 depicts the number of and the trend in serious-risk violations that have completed the enforcement process since the start of mandatory compliance with Reliability Standards in 2007. The rolling average provides an indicator of whether the rate of serious-risk violations is increasing, decreasing, or remaining steady.

⁵¹ NERC provides this information on a quarterly basis at: <http://www.nerc.com/pa/comp/CE/Pages/Compliance-Violation-Statistics.aspx>

⁵² Information on risk assessment of noncompliance is available at:

[http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO%20Self-Report%20User%20Guide%20\(April%202014\).pdf](http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO%20Self-Report%20User%20Guide%20(April%202014).pdf)

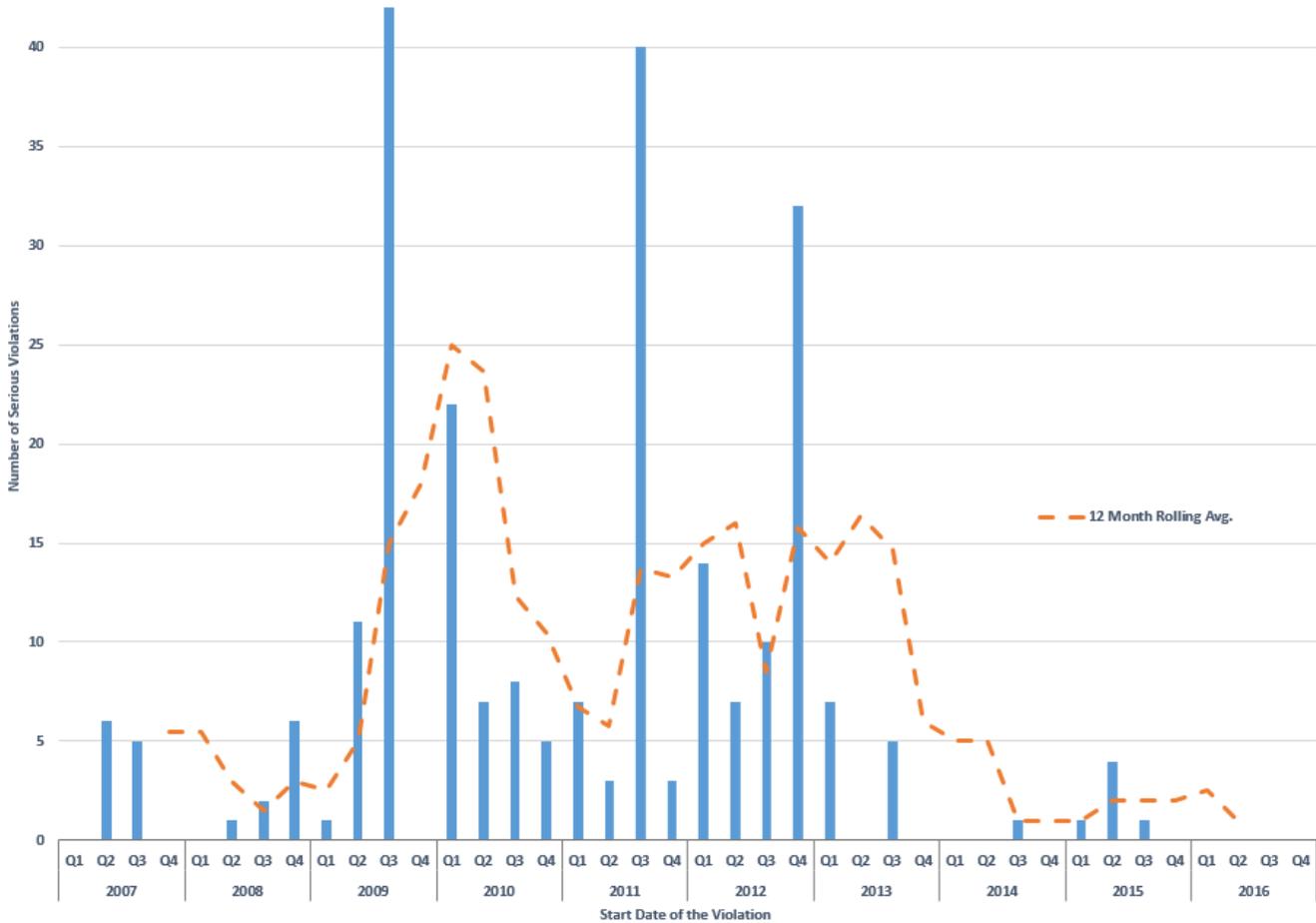


Figure 5.1: Serious-Risk Violations (CP-1)

Serious-risk-based violations have remained below the rolling average except in four instances as follows: The spikes in the third quarter of 2009 and the first quarter of 2010 are largely attributable to the implementation of the Critical Infrastructure Protection (CIP) Reliability Standards as they became applicable to additional registered entities. The spike in the third quarter of 2011 is largely attributable to the September 8, 2011, Southwest Outage and the resulting violations resolved through FERC/NERC investigations. The last spike in the fourth quarter of 2012 is related to a large number of serious CIP violations.

While it appears that there is a decreasing trend in the 12 month rolling average of serious risk violations, it is important to remember that there is time required to fully understand serious risk violations and reach disposition, which may include the filing of a full NOP. NERC and RE representatives have analyzed serious risk violations from 2012 through the end of 2015. In the future, there may be additional serious risk violation added to the count of this metric as reported violations are fully analyzed and reach disposition.

Figure 5.2 depicts the top 10 standards and requirements that were filed at FERC as serious-risk violations since 2012.⁵³ NERC posts all NOP on its website to provide information to industry about how to reduce the frequency of noncompliance and its associated risk.⁵⁴

⁵³ With CIP Version 5 and revisions to the IRO/TOP Standards, the requirement numbers have changed, but most of the substantive requirements remain.

⁵⁴ The Enforcement page is here: <http://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx> The Searchable Notice of Penalty Spreadsheet available on that page indicates the risk assessments for all violations included in Notices of Penalty.

The serious risk issues addressed in NOPs in 2016 included the following:

- A lack of commitment to NERC compliance regarding CIP Reliability Standards
- Vegetation contacts
- Repeat conduct
- Ineffective change management including employee turnover
- Lack of preparedness for the interconnection of new facilities and the enforceability of new requirements and
- Inadequate training of personnel on tools and processes

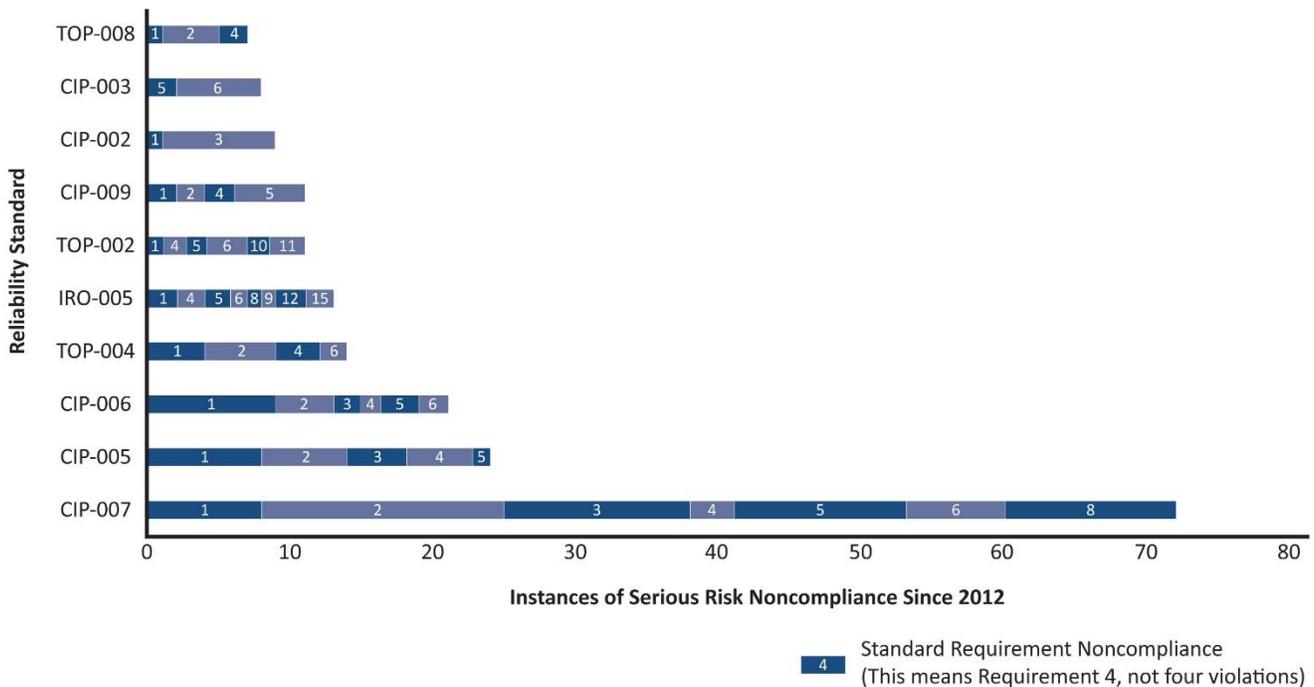


Figure 5.2: Standards and Requirements with Most Occurrences of Serious-Risk Violations

Figure 5.3 shows the risk breakdown of violations processed from 2013 to 2016. A small percentage of violations were deemed to have the potential to create a serious risk. Risk assessments result from evaluation of the possible impact of a noncompliance and the likelihood of occurrence of that impact. CP-1 is a measure of potential risk and not of actual impact. CP-2 considers the impact of an occurrence of noncompliance.

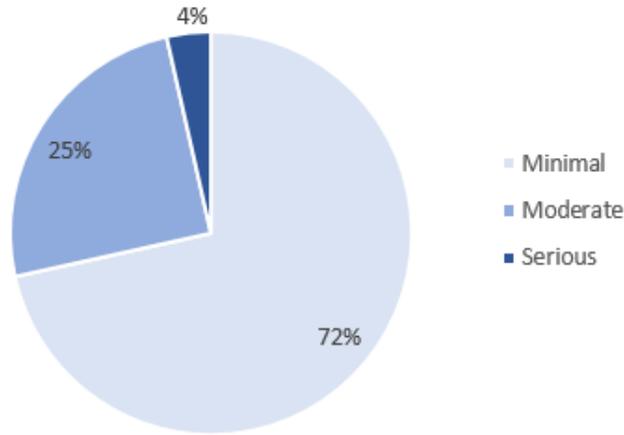


Figure 5.3: Final Risk Assessments (2013–2016)

CP-2: Impact Metric

In addition to analysis of noncompliance occurrences that have a potential for serious risk to the BPS, NERC also evaluates whether these instance have an actual impact on reliability as a result and looks for trends in what requirements are being violated that produce negative reliability impacts. Compliance Process-2 (CP-2) is a quarterly count of the number of noncompliance incidents with observed reliability impact regardless of the risk assessment. This metric is based on what happened because of a specific instance of noncompliance. **Figure 5.4** maps the four data tiers that define the impacts used for CP-2 with Tier 3 being the most serious.

There was a violation or PV and it led to:

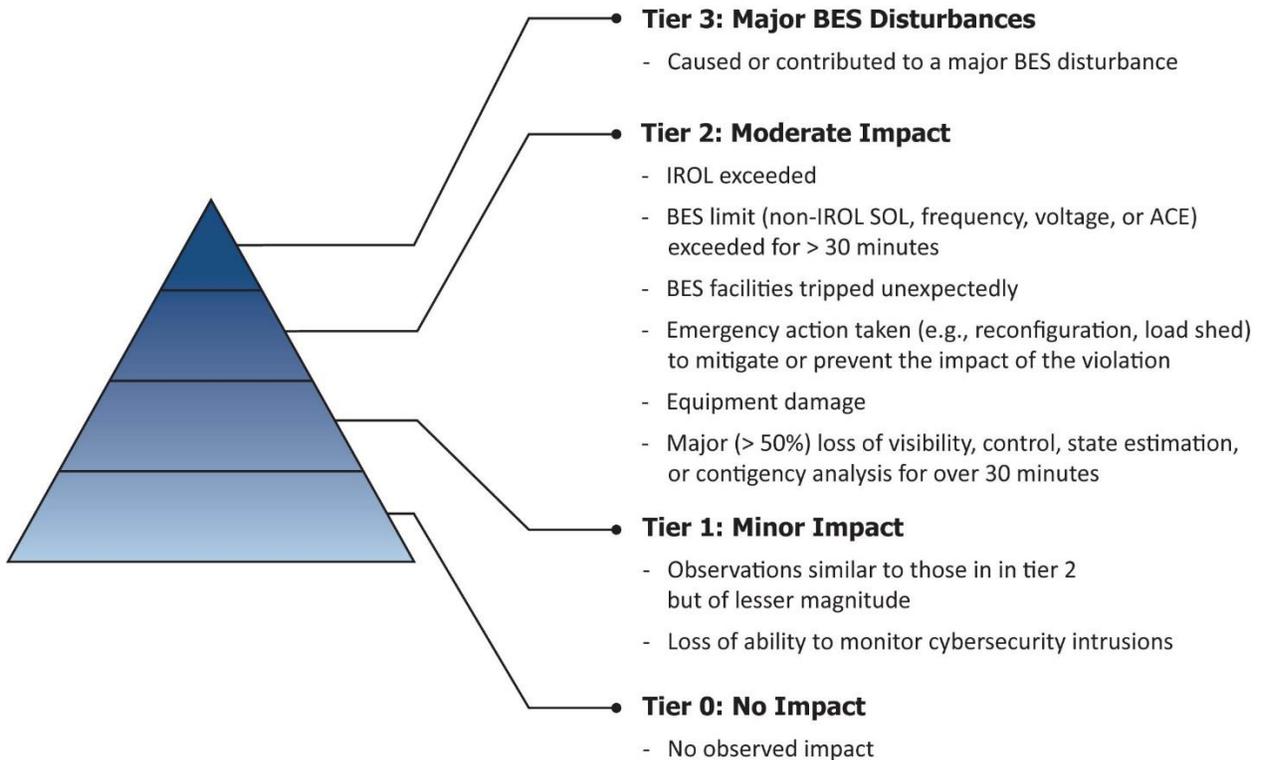


Figure 5.4: Impact Observations Mapped to the Impact Pyramid Tiers

Tier 0 observations represent the largest number of violations with no observable impact to BPS reliability.

Figure 5.5 represents the occurrence dates of the violations filed since 2014 that had some observed impact on reliability.⁵⁵ Tier 0 observations (no observed impact) are not depicted. The moving averages provide an indicator of whether the rate of impactful violations is increasing, decreasing, or remaining steady.

As in the CP-1 graph, **Figure 5.5** displays a spike in violations with impact in the third quarter of 2011 because of the Southwest Outage that occurred on September 8, 2011. The spike in the third quarter of 2012 is attributable to violations by WECC RC, now Peak Reliability, that are described in a March 31, 2014, NOP filing with FERC.⁵⁶ As with the trend in CP-1, the number of violations with impact remains constant at a relatively low level. However, as not all reported noncompliances have reached final disposition, this metric is also subject to change.

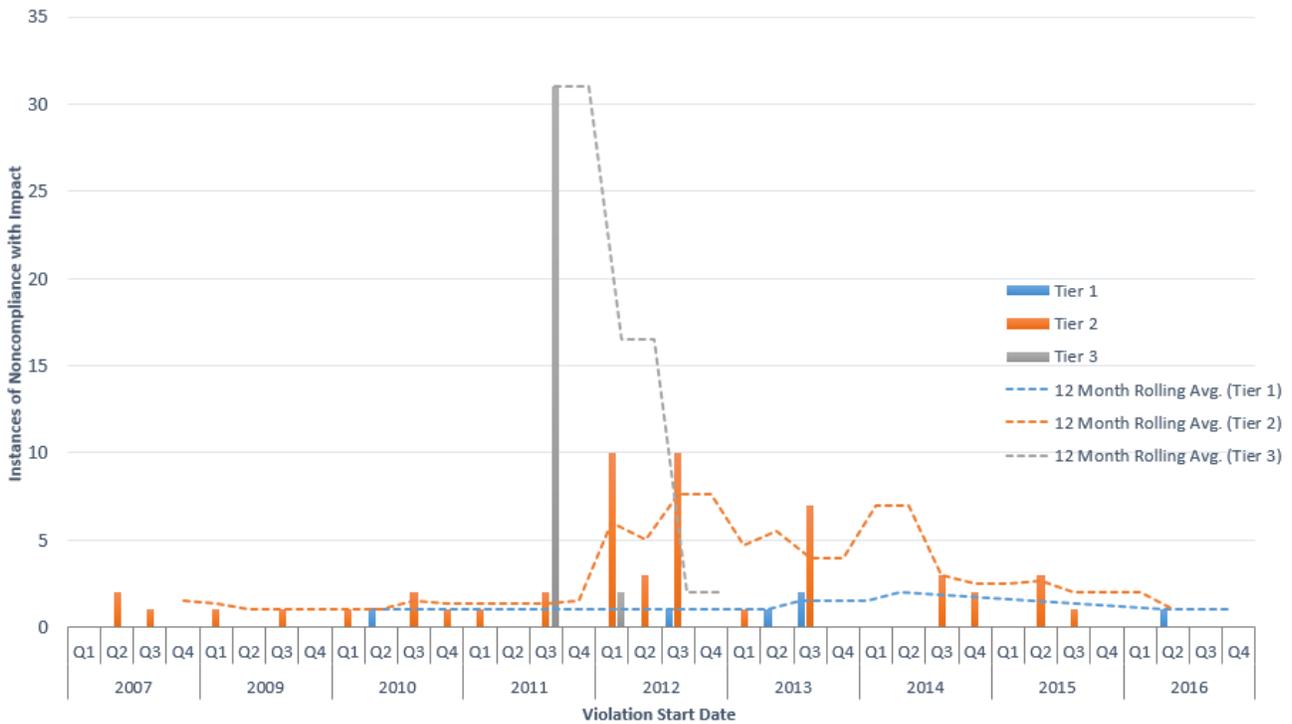


Figure 5.5: CP-2 Occurrences (2014–2016 Data)

Figure 5.6 shows the breakdown by requirement of the most frequently impactful noncompliance filed in 2014 through 2016.

The IRO and Transmission Operator (TOP) requirements represented in **Figure 5.6** correspond to the serious-risk violations associated with the Southwest Outage and the WECC RC NOP referenced previously.

⁵⁵ NERC provides this information on a quarterly basis at: <http://www.nerc.com/pa/comp/CE/Pages/Compliance-Violation-Statistics.aspx>

⁵⁶ http://www.nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/Public_FinalFiled_NOP_NOC-2268.pdf

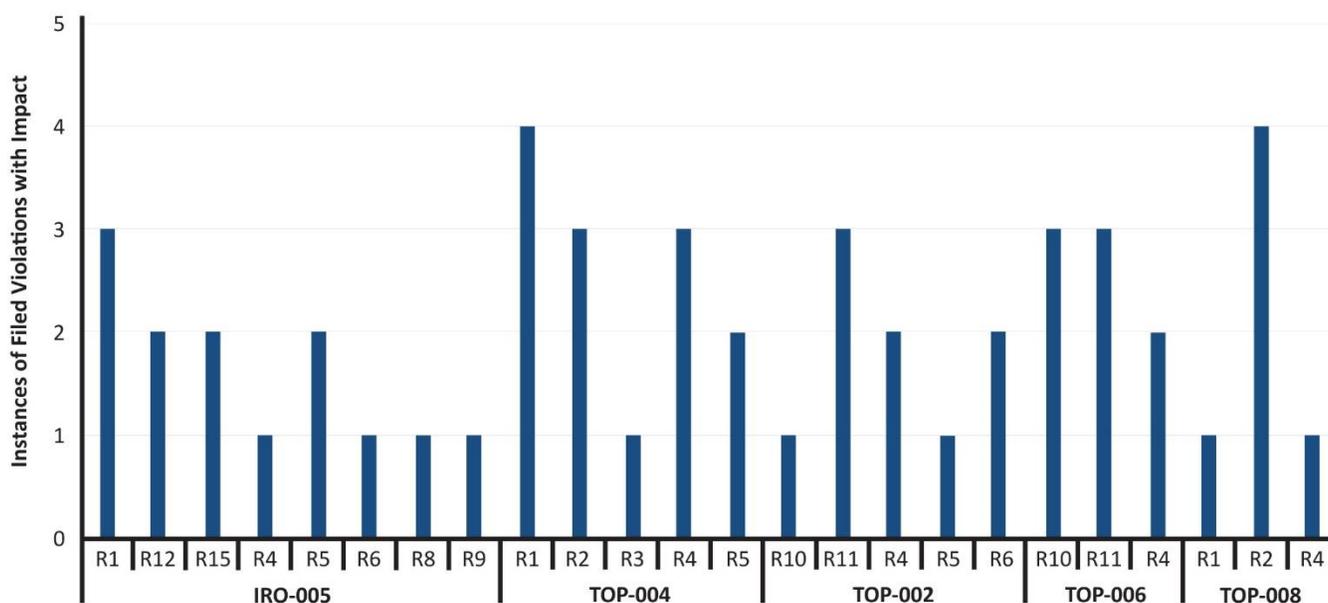


Figure 5.6: Most Frequently Filed Standards and Requirements (2014–2016 Data)

NERC provides quarterly updates on trends in the Compliance Monitoring and Enforcement Program⁵⁷ and will continue to update CP-1 and CP-2 during 2017. NERC also analyzed and reported on the causal trends associated with the violations depicted in CP-1 and CP-2 metrics. The additional analysis with conclusions and recommendations can be found on the NERC website.⁵⁸ At a high level, the key issues observed included the following:

- Monitoring and situational awareness
- Planning and system analysis
- Human performance

While the CP-1 and CP-2 metrics have only been included in two *State of Reliability* reports since their adoption, they provide beneficial information about which standards and requirements, when violated, have the potential for serious risk to the BPS and which ones have been observed to result in reliability impact. The analysis of these two metrics provide the registered entities with information to focus on improving processes, procedures, and controls in those areas where the most risk or impact has been determined to exist.

⁵⁷ <http://www.nerc.com/pa/comp/CE/Pages/Compliance-Violation-Statistics.aspx>

⁵⁸ <http://www.nerc.com/pa/comp/CE/Compliance%20Violation%20Statistics/Analysis%20of%20Serious%20Risk%20Violations%20with%20an%20Impact.pdf>

Chapter 6: Event Analysis

The industry’s voluntary ERO EA Process provides information to the ERO and industry on the categories and causes of qualifying events. Review and analysis of this information can identify potential reliability risks or vulnerabilities to the BPS that need to be mitigated. Significant incidents have occurred that do not meet threshold criteria for inclusion in the EA Process; these are addressed in [Chapter 2, Reliability Highlights](#).

Background

Since its initial implementation in October of 2010, the EA Process has collected 896 qualified events and yielded 125 lessons learned, including 13 published in 2016.⁵⁹

The first step in the ERO EA Process is BPS awareness and the monitoring of the BPS for reliability incidents. BPS conditions provide recognizable signatures through automated tools, mandatory reports, voluntary information sharing, and third-party publicly available sources. The majority of these signatures represents conditions and occurrences that have little or no reliability impact. The ERO Enterprise monitors these signatures for significant occurrences and emerging risks and threats across North America.

Registered entities continue to share information and collaborate with the ERO well beyond any mandatory reporting in order to maintain and improve the overall reliability of the grid. Only a small subset of the reported occurrences rise to the level of a reportable event. **Table 6.1** provides details on the 2016 information, mandatory reports, and other information that is translated into products that address reportable events.

Table 6.1: Situational Awareness Inputs and Products for 2016

Information Received	Products
Mandatory reports	229 daily reports
339 DOE OE-417 Reports	28 special reports for significant occurrences
325 EOP-004-2 Reports	
2 EOP-002-3 Reports	1 reliability-related NERC Advisory (Level 1) Alert
Other information⁶⁰	646 new Event Analysis entries (known as “Notifications” and associated with the 171 qualified events and the 267 nonqualified occurrences)
3,403 Intelligent Alarms Notifications	2 reliability-related NERC Recommendation (Level 2) Alert
4,238 FNet/Genscape Notifications and 946 Daily Summaries	
2,049 WECCnet Messages	
2,121 RCIS Messages	
2,393 Space Weather Predictive Center Alerts	
1,123 Assorted US Government Products	
5,260 Assorted Confidential, Proprietary, or Nonpublic Products	
2,235 Reliability Coordinator and ISO/RTO Notifications	

Analysis and Reporting of Events

Using automated tools, mandatory reports, voluntary information sharing and third-party publicly available sources, disturbances on the grid are categorized by the severity of their impact on the BPS. Table 6.2 contains a

⁵⁹ The link to the NERC Lessons Learned page: <http://www.nerc.com/pa/rrm/ea/Pages/Lessons-Learned.aspx>

⁶⁰ Information sources listed in no particular order or priority, and not limited to these resources

consolidated chart of the reportable events since the program's inception (October 2010). Additional information on the EA Process can be found on the NERC website.⁶¹ As of January 1, 2017, a new EA Process version will go into effect.⁶²

Table 6.2: Events Analysis Event Summary			
Event Category	Count (Total)	Count (2016)	Comments (2016 Events)
CAT 1	712	163	71 - Three or more BPS facilities lost (1a) 5 - BPS SPS/RAS Misoperation (1c) 1 – Unintended loss 1,000-1,399MW generation in ERCOT (1g) 86 - Partial EMS (1h)
CAT 2	161	6	2 – Loss of Offsite Power (2d) 4 – Unintended loss of load (2f)
CAT 3	18	2	Loss of 1,400+ MW generation in ERCOT Loss of 2,000+ MW generation in other Interconnections
CAT 4	3	0	
CAT 5	2	0	
Total CAT 1-5 Events	896	171	
Nonqualified Occurrences Reported	2,532	267	

In 2016, there were 85 non Energy Management System (EMS) brief reports submitted to the ERO. This was a substantial increase when compared to 50 non-EMS reports submitted to the ERO in 2015. Of these 85 events, 77 were Category 1 events, six were Category 2 events, and two were Category 3.a events in ERCOT. Subsequent to January 1, 2017, the two Category 3.a events in ERCOT would have been classified as a Category 1.g events to more accurately reflect the risk associated with them.

Out of the 85 non-EMS events in 2016, there were 55 of these events (65 percent) that experienced one or more misoperations. In all 55 of these events, the misoperations exacerbated the severity of the event. Of these 55 events with misoperations involved, 27 events (49 percent) experienced a breaker failure scheme misoperation or bus differential misoperation. These types of misoperations typically have a high impact on the BPS, particularly when they clear a straight bus with multiple facilities. The 2016 percentage of events with misoperations compares closely to the 2013–2015 results.

⁶¹ EAP process in effect through the end of 2016: http://www.nerc.com/pa/rrm/ea/EAPProgramDocumentLibrary/ERO_EAP_V3_final.pdf

⁶² EAP Process in effect as of January 1, 2017: http://www.nerc.com/pa/rrm/ea/ERO_EAP_Document/ERO_EAP_v3.1.pdf

There were 86 EMS events in 2016. Common themes for the EMS events were the following:

- Change management
- Testing procedures
- Vendor relationships
- Network infrastructure

Loss of situational awareness was identified as a moderate priority risk by the RISC. Loss of EMS events will continue to be a high priority for the ERO, as loss of situational awareness can be a precursor or contributor to a BES event.

The EMS Working Group (EMSWG) analyzes the events and data that are being collected about EMS outages and challenges. From the EA reports and the work of the Event Analysis Subcommittee (EAS), NERC published multiple lessons learned specifically about EMS outages and worked to build and support an industry-led EMS Task Force (EMSTF) to support the EAS. The hard work and active sharing of this group has reduced some of the residual risk associated with this potential loss of situation awareness and monitoring capability that comes with this type of event, and they will continue to provide valuable information to the industry. NERC hosted its fourth annual Monitoring and Situational Awareness Conference on September 27–28, 2016, with the theme of EMS Resiliency.

For trending of the number of events, NERC uses a standard Statistical Process Control methodology, resulting in control charts. The control chart provides control limits that are calculated by using an Individuals-Moving Range calculation. In this way, there is no unnecessary reaction to what would be considered normal variation in the numbers of events reported. This also helps determine what “normal” looks like when determining if any anomalies have occurred.

Figure 6.1 is the control chart for the 897 Qualified Events through 2016. In October 2013, when Version 2 of the EA Process introduced a new category of events, collectively known as Category 1h: Partial Loss of the EMS, occurrences that were not previously reported became visible and a shift in the control limits occurred. The control chart of events in 2016 shows the numbers of events were stable and predictable.

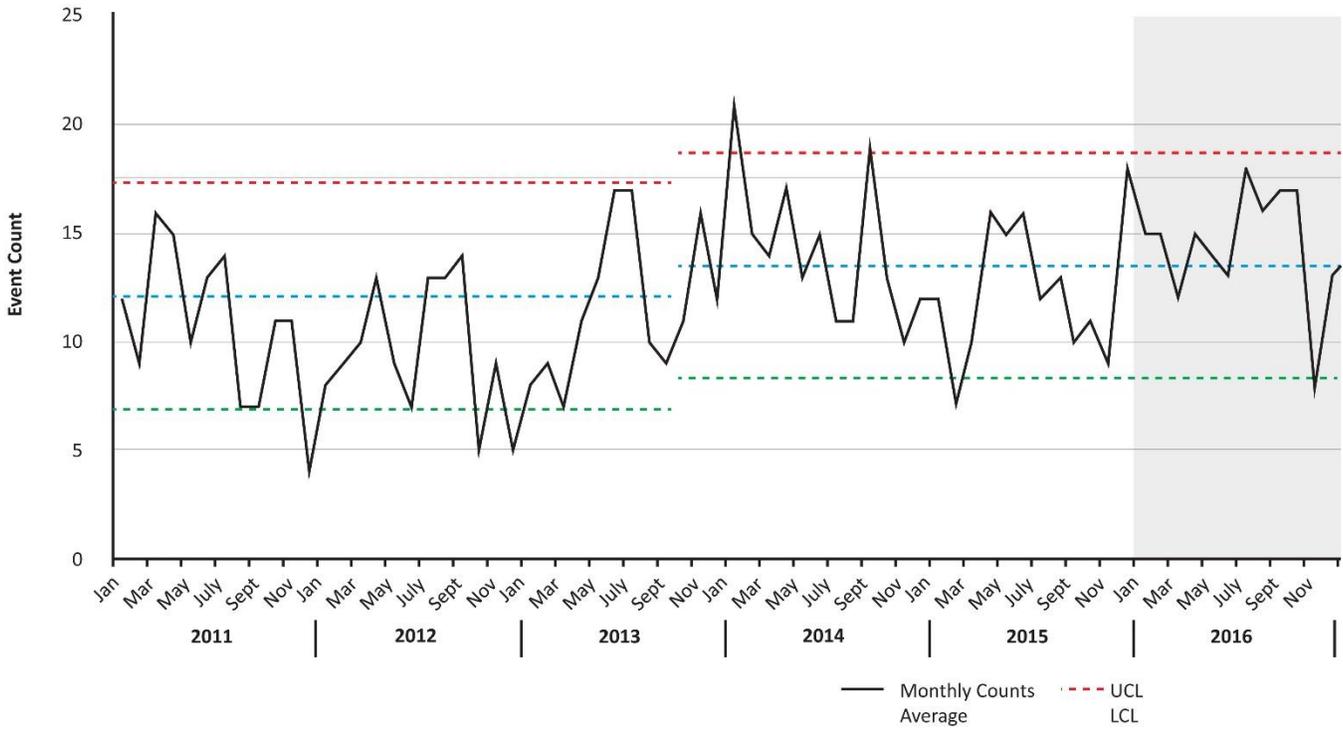
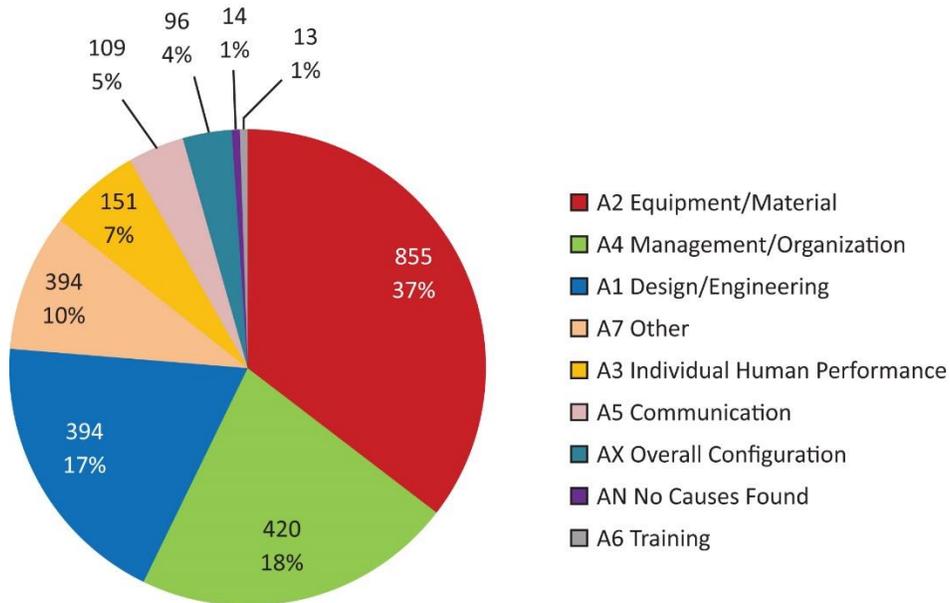


Figure 6.1: Control Chart for the Number Events (Per Month) Over Time

Through the EA Process, cause codes were assigned to 674 of the 896 events, leading to 2,279 root or contributing cause codes being identified. The root cause of every event cannot be determined, though many of the contributing causes or failed defenses can be established. **Figure 6.2** shows the overall breakdown of the identified cause codes of events.



674 events have been cause coded with 2279 identified causes

Figure 6.2: The Percentage of Contributing Causes by Major Category

Identification of these areas of concern allows for the prioritization and search for actionable threats to reliability. When this data was shared with the AC Substation Equipment Task Force (ACSETF) it was determined that, while the initial data pointed to the potential problem areas, the data was not detailed enough to analyze any specific problem areas. Following recommendations from the ACSETF report, an addendum was developed for the types of information needed to support the EA Process when failed equipment is identified.⁶³

Out of the 85 transmission-related events in 2016, a total of 29 events (34 percent) experienced substation equipment failures. In total, 27 of these 29 substation equipment failures were either the initiating cause of the event or they subsequently increased the severity of the event. The substation equipment failures were as follows:

- 10 internal breaker failures
- 8 stuck/slow breakers
- 1 breaker bushing failure
- 2 shunt capacitor failures
- 2 lightning arrester failures
- 3 circuit Switcher/disconnect failures
- 1 free standing CT failure
- 1 potential transformer failure
- 1 bus insulator failure
- 1 SF6 bus leak/failure
- 1 battery/charger failure

The top two causes of substation equipment failures were related to circuit breakers. As noted in their report of March 2015, the ACSETF⁶⁴ concluded that 1) circuit breaker failures have the highest percentage of failures; 2) the top four subcomponents are interrupter, mechanism, trip coil, and bushing; and 3) inherent in circuit breaker failure is an increased probability that additional BPS elements will also be forced out of service. NERC EA has created a template to collect additional information for substation equipment failures and will continue to analyze the data for common themes. NERC also published a lessons learned in March 2017, “Slow Circuit Breaker Operation Due to Lubrication Issues.”

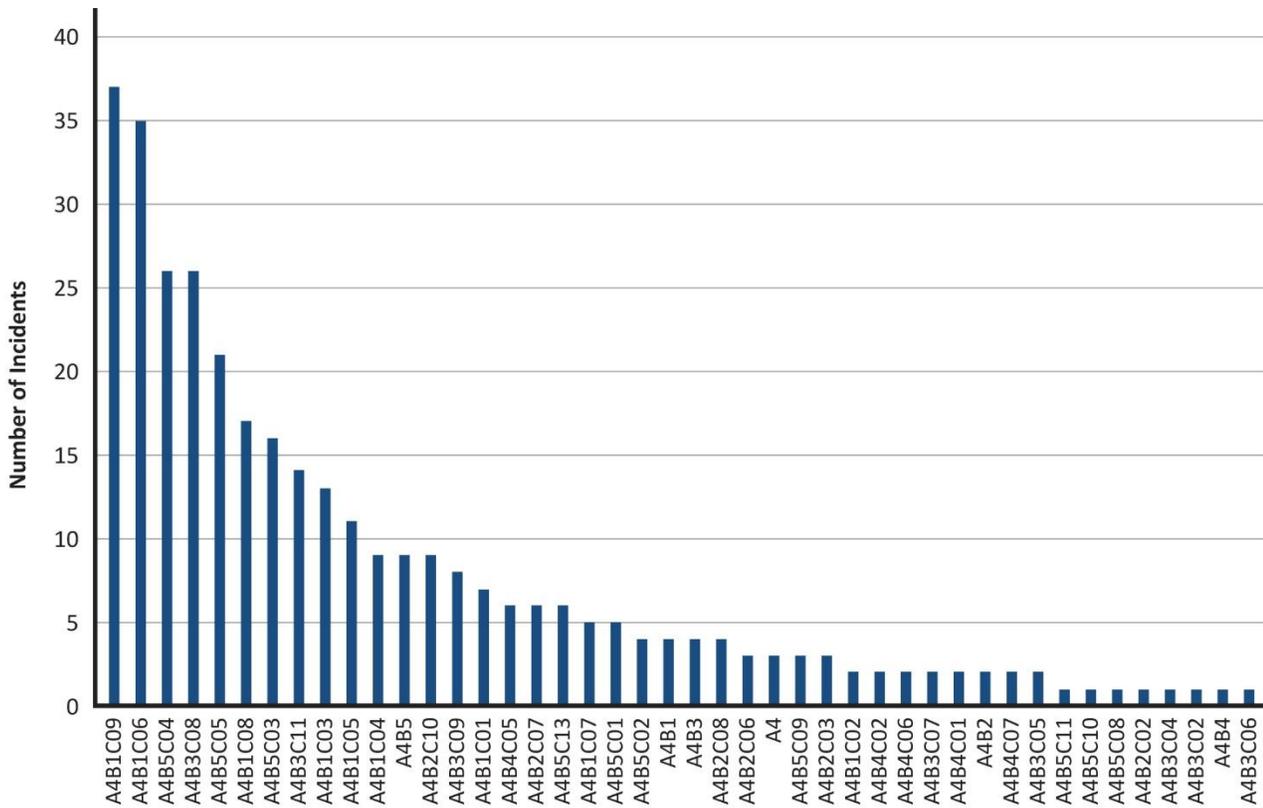
Asset management and maintenance was identified as a low-priority risk by the RISC.⁶⁵ Low-priority risks do not mean that possible reliability impact is small, but rather the profiles are understood with clearly identifiable steps that can be taken to manage risk. The failure to properly commission, operate, maintain, and upgrade BES assets could result in more frequent or more severe outages as equipment failures initiate or exacerbate events.

A similar identification of trends can be observed in the large contribution of “less than adequate” or “needs improvement” cause factors in management and organizational practices that contribute to events. Many of these threats can be identified and shared with the industry for awareness. For example, in **Figure 6.3**, the identification of some of the challenges to organization and management effectiveness are identified.

⁶³ <http://www.nerc.com/pa/rrm/ea/Pages/EA-Program.aspx>

⁶⁴ http://www.nerc.com/comm/PC/AC%20Substation%20Equipment%20Task%20Force%20ACSETF/Final_ACSETF_Report.pdf

⁶⁵ http://www.nerc.com/comm/RISC/Related%20Files%20DL/ERO_Reliability_Risk_Priorities_RISC_Recommendations_Board_Approved_Nov_2016.pdf



A4B1C09 = Corrective actions for previously identified problem were not adequate to prevent recurrence
 A4B1C06 = Previous industry or in-house experience was not effectively used to prevent recurrence
 A4B5C04 = Risks/consequences associate with change not adequately reviewed/assessed
 A4B3C08 = Job scoping did not identify special circumstances and/or conditions
 A4B5C05 = System interactions not considered or identified
 A4B1C08 = Corrective actions to a known or repetitive problem were untimely
 A4B5C03 = Inadequate vendor support of change
 A4B3C11 = Inadequate work package preparation
 A4B1C03 = Management direction created insufficient awareness of impact of actions on reliability

Figure 6.3: Management or Organization Challenges Contributing to an Event

Major Initiatives in Event Analysis

Human Performance

EA has identified work force capability and human performance (HP) challenges as possible threats to reliability. HP and a skilled workforce was also identified as a priority by the RISC. Workforce capability and HP is a broad topic but can be divided into management, team, and individual levels. NERC held its fifth annual HP conference in Atlanta, Improving Human Performance on the Grid, at the end of March 2016.⁶⁶ Its sixth annual HP conference, Improving Human Performance and Increasing Reliability on the Bulk Power System, was held jointly with NATF in Atlanta in March 2017.

NERC continues to conduct cause analysis training with staff from the Regions and registered entities. As of December 2016, personnel from all eight Regions, and approximately 1,380 people from 250 different registered entities have received cause analysis training, roughly 11,000 hours of training.

⁶⁶ http://www.nerc.com/pa/rrm/hp/2016_Human_Performance_Conference/Forms/AllItems.aspx

NERC held its fourth annual Monitoring & Situational Awareness Conference at the California ISO offices in September 2016. This conference continues to focus on issues related to EMS events, situational awareness, and EMS resiliency.

2016 Winter Weather Review

On September 1, 2016, a webinar and preparedness training was provided to the industry to prepare for Winter 2016–2017. The objective of the “Winter Preparation for Severe Cold Weather” webinar was to remind industry of the need to continue to appropriately prepare for the upcoming winter weather forecasts. The webinar was well attended by industry with over 200 users, owners, and operators of the BPS participating in the webinar. The webinar provided an overview of current reference materials and updated training packages. Information was shared from the *Short-Term Special Assessment, Operational Risk Assessment with High Penetration of Natural Gas-Fired Generation*⁶⁷ and the preliminary 2016–2017 North America Winter Outlook. The winter preparation materials can be found on NERC’s website.⁶⁸

Event Severity Risk Index

NERC EA staff calculates an event severity risk index (eSRI) for all qualified events (as defined in the EA Process). This calculation is based on the methodology used by NERC for the standard SRI as described in [Chapter 3](#), and it considers the loss of transmission, the loss of generation, and the loss of firm load (along with load-loss duration).

The formula used is:

$$eSRI = RPL * W_L * (MW_L) + W_T * (N_T) + W_G * (N_G), \text{ where}$$

RPL = Load Restoration Promptness Level

W_L = Weighting of load loss (60 percent)

MW_L = normalized weighting of load loss

W_T = weighting of transmission lines lost (30 percent)

N_T = normalized number of ac transmission lines lost, in percent

W_G = weighting of loss generation (10 percent)

N_G = normalized Net Dependable Capacity of generation lost

The value of this calculation results in a number between zero and one; thus, for easier use in analysis, this small number is multiplied by 1000.

Every event reported through the EA Process has its eSRI calculated, but for the purposes of trending, certain event groups are excluded. The excluded groups are the following:

- Weather-driven events: The purpose of excluding the weather-driven events is because they are outside of the control of the BES entities, thus not considered when studying impact over which there is control. A weather-driven event is an event whose root cause is determined to be weather (or other force of nature); examples would include the Hurricane Sandy event, an earthquake, or a string of tornadoes knocking down transmission towers, among others. There have been 14 of these events since October 2010.

⁶⁷ http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC%20Short-Term%20Special%20Assessment%20Gas%20Electric_Final.pdf

⁶⁸ <http://www.nerc.com/pa/rrm/ea/Pages/Cold-Weather-Training-Materials.aspx>

- AESO islanding events: As AESO designed islanding events as an intentional act in their SPS schemes, these are also excluded.
- Category 4 and 5 events: The purpose of excluding Category 4 and 5 events is that they are monitored and tracked in a distinct manner, so counting them in this trending would be duplicative.
- Events prior to 2011: For the purposes of trending, it has been decided that the 18 events in 2010 would not be included as this was such a small sample from a limited time frame.

Total Qualified events reported is 897.

- Excluded 2010 events: 20 which leaves 877 events.
- Excluded Category 4 and 5 events: five, which leaves 872 events.
- Excluded Weather-driven events (root cause is weather): 10, which leaves 862 events.
- Excluded AESO Islanding: 35, which leaves 827 events.

Number of events used for eSRI trending: is 827 events.

Once this number is calculated for each event and is plotted in chronological sequence, the slope of the trend line is calculated and plotted. In this way, the trend can be visually identified (as well as numerically calculated using statistical software). Every day has its eSRI calculated (meaning a day with no events has an eSRI = 0.000). For any days with multiple events, the eSRIs are additive.

The eSRI calculations are shown in [Figure 6.4](#) and [Figure 6.5](#).

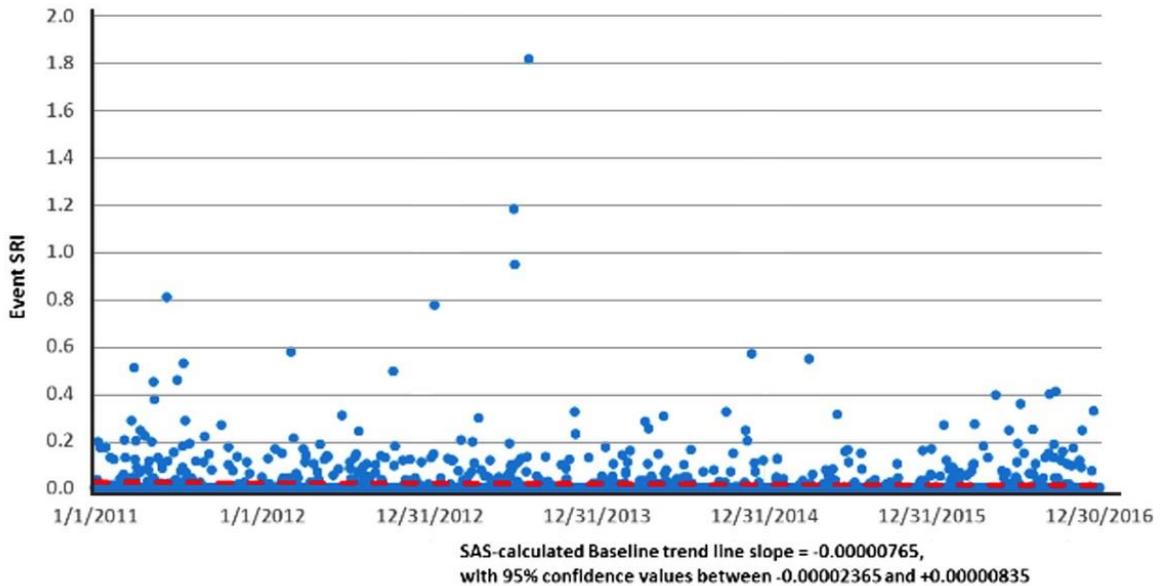


Figure 6.4: Trend line of eSRI

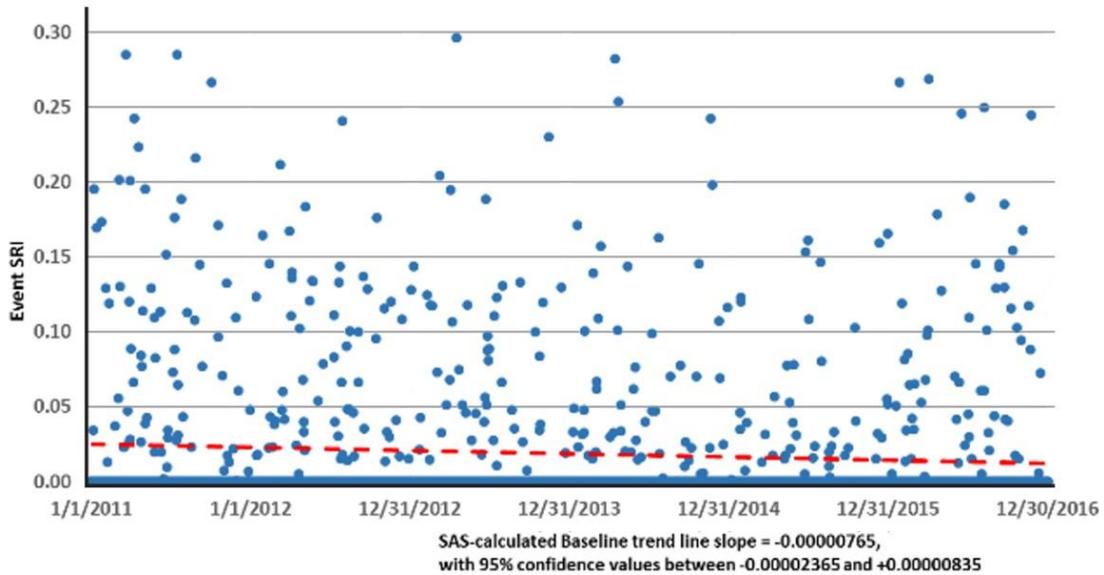


Figure 6.5: Expanded View of eSRI Trend Line Y axis 0 to 0.3

As can be seen from the expanded view (included to address the scale limit visibility), the eSRI is approximately zero within the statistical confidence interval. Furthermore, as indicated in [Figures 6.4](#) and [Figure 6.5](#), the trend line is relatively flat.

Summary

The EA Process continues to provide valuable information for the industry to address potential threats or vulnerabilities to the reliability of the BPS. The ability to identify specific pieces of equipment that are potential threats, as well as emerging trends that increase risk to the system, illustrates the value of the EA Process. These outcomes, coupled with the ability to actively share the information through lessons learned, webinars, technical conferences, and related venues, remain critical to the sustainment of high reliability.

Chapter 7: BES Security Metrics

Background

One of the most complex endeavors that NERC undertakes is assessing security risks to the BPS. Capturing metrics on physical and cyber security is equally complex. A great deal of data is available regarding cyber incidents, but not all incidents may cause loss of load or impact grid operations. Specifically, the data NERC received in 2016 from OE-417s and EOP-004s show low numbers of cyber penetrations of grid operating systems in North America and few reports of physical intrusions.⁶⁹ These low numbers indicate that NERC's efforts with industry have been successful in isolating and protecting operational systems from various adversaries. The numbers are also an indication that the electricity industry's record of breaches is much lower than many other sector (including government agencies) that have been victims of numerous data breaches.⁷⁰

The number of reportable cyber security incidents affecting customers resulting in loss of load remains at zero, and the number of reportable cyber incidents affecting grid operations was also at zero for the last two years. During 2015 and 2016, no physical security events occurred that caused a loss of load.⁷¹

NERC takes all cyber incidents seriously. Although significant risks to the grid still exist, the low numbers show that the electricity industry has seen exceptional performance in protecting the grid from security incidents to date.

Measuring Security Risks

Internet-facing corporate systems at utilities are probed hundreds of thousands of times per day. Once in a while, a laptop might become infected. These incidents may occur a few times a month for a typical company and up to several dozen times per month for the larger utilities. No clear line exists on what to report on these routine cyber issues, near-misses, or possible attempts that are difficult to measure and do not cause loss of load or impact grid operations.

On the control systems side, the number of incidents reported affecting grid operations was zero throughout 2015 and 2016. NERC currently has superior reporting and ethics on disclosure in place, and companies are seeing and fixing issues within their own information technology (IT) departments. However, NERC cannot solely rely on an incident reporting metric as a sign of risk; this kind of reporting would be misleading as a result of the difference between the numbers of incidents reported on the corporate versus control systems side.

Another way to measure cyber risk that does not depend on self-reporting is to use the analytic data gathered from the CRISP and the CAISS to calculate risk indices based on the number of cyber incidents discovered. This measurement would be more reliable than self-reporting incidents but could somewhat overstate BPS concerns because the collected data is only from the corporate interfaces to the internet and not from control systems at this point, assuming that the two systems are air gapped.

NERC, in collaboration with the DOE and the National Laboratories, is exploring ways operational traffic could also be captured, in addition to the large data sets of information flowing from the corporate or business systems. Once CAISS—which is currently a pilot program—becomes more widespread, it will allow indicators of compromise (IOC) that may be seen on enterprise IT systems via CRISP to be compared to any potential intrusions or malicious data collected from control systems, further refining risk metrics to grid operations.

⁶⁹ See Appendix G for the BESSMWG metrics.

⁷⁰ <http://www.nydailynews.com/news/national/hacker-dumps-info-thousands-homeland-security-workers-article-1.2524440>; <https://www.scmagazine.com/anonsec-claims-credit-for-nasa-drone-hack/article/528448/>; <http://www.cbsnews.com/news/irs-identity-theft-online-hackers-social-security-number-get-transcript/>

⁷¹ In late 2014, a physical security event occurred that resulted in loss of load; however, this event was not officially reported until January 2015. See *(enter corresponding EO-417 for citation)*.

And finally, the most important cyber risk faced on the grid is more existential: the capability of nation-states or other capable adversaries to launch a massive cyberattack to disrupt electricity operations. The chances of this happening are extremely low; however, the consequences could be significant for this worst case scenario. Currently, no method exists to determine a true quantitative measure of this sort of risk. What NERC can measure is that no major cyber- and few physical-related load losses have happened to date; that extremely low numbers of incidents have occurred on the operating side, and that attention to security performance has been excellent on the corporate side.

The BESSMWG, under the direction of the Critical Information Protection Committee (CIPC), chose to measure the existential risk by adopting Metric 6, based on the NIST Global Cyber Security Vulnerabilities Index and Metric 7 as PWC's Global State of Information Security index.⁷² Both of these reports chart cyber risk year-over-year on a global basis across all sectors from credible sources. With a global outlook towards cyber and physical attacks on grid infrastructure, these reports recognize that other utilities around the world have been successfully attacked by capable adversaries with some attacks resulting in loss of control and shutdown of operational electric loads.

Cyber Security Incident Case Study: Ukraine

In December 2015, Ukraine fell victim to a cyber attack that included spear phishing, credential harvesting and lateral movement, unauthorized remote access, telephony denial-of-service, and sustaining persistent access. In February 2016, NERC's E-ISAC provided subject matter expertise to develop the NERC alert, *Mitigating Adversarial Manipulation of Industrial Control Systems as Evidenced by Recent International Events*, which shared techniques observed in the Ukraine cyber attacks. Most of these same tactics and techniques were used in a subsequent series of attacks against Ukraine in December 2016, when Ukraine's state-owned national power company, Ukrenergo, experienced an outage at an electrical substation in the capital city of Kyiv. Service was restored as a result of manual operator intervention. Researchers confirmed that the outage was the result of a cyber attack that occurred during the end of a protracted campaign.

In addition to the 2016 NERC alert, the E-ISAC worked with the SANS Institute to publish a Ukraine Defense Use Case (DUC).⁷³ This 29-page report "summarizes important learning points and presents several mitigation ideas based on publicly available information on Industrial Control Systems (ICS) incidents in Ukraine."

The techniques used against Ukraine have several options for remediation and prevention. NERC, through standards and compliance; and the E-ISAC, through information sharing, industry collaboration, and publications like the NERC alert and DUC; often stresses and shares these remediation and prevention tips with the electricity industry.

The events in Ukraine underscore the importance of grid security and provide a real-world example of consequences of a cyber attack on the electrical grid. The events abroad also highlight the importance of user training and information sharing in order to prevent a similar attack on the North American power grid. Similar tactics are woven into the North America-wide grid security exercise (GridEx) series.

Beyond Standards and Compliance: The E-ISAC

The E-ISAC's mission is to be a leading and trusted source that analyzes and shares electricity industry security information. The E-ISAC gathers security information, coordinates incident management, and communicates mitigation strategies with stakeholders within the electricity industry across interdependent sectors and with government partners.

⁷² PWC did not provide the data for 2016; the BESSMWG is working to determine if this information will be available in future. If not, the BESSMWG will seek alternate sources for similar data.

⁷³ https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Most of the E-ISAC's communications with electricity industry members are via an internet portal that was significantly upgraded at the end of 2015. In 2016, the E-ISAC added 1,512 new users to the portal, a growth of 19.5 percent over 2015. The most popular views by members were documents, including weekly reports and analytical assessments posted by the E-ISAC. In 2016, 1,525 unique users downloaded 713 different documents 18,555 times. The top downloaded document of 2016 was the E-ISAC/SANS Ukraine Defense Use Case previously mentioned.⁷⁴ As the E-ISAC continues to collect portal activity data, the information will assist the E-ISAC in recruiting new members to the portal and determining how the E-ISAC can best serve members' interests and needs.

Increased physical security and cyber security information sharing will enable the E-ISAC to conduct more complete analysis. Robust data collection over time helps identify important trends and patterns. By providing unique insight and analysis on physical and cyber security risks, the E-ISAC's aim is to add value for its members and assist with overall risk reduction across the ERO Enterprise.

Cyber Security Risk

In 2016, there were 241 cyber bulletins posted to the E-ISAC portal.⁷⁵ Of the 241 cyber bulletins, 210 were posted based on information provided by members or posted by members themselves. This trend is consistent with the 218 cyber bulletins in 2015. The E-ISAC expects this number to increase in 2017 as member participation increases. The E-ISAC also posted several bulletins based on information obtained from government partners and trusted open source partners. Like 2015, the second quarter (Q2) of 2016 saw the most portal posts based on information provided by members.

Just under half of the reports from members involved phishing incidents. Other important trends and analysis conducted throughout the year focused on the Dridex campaign, ransomware, and the Internet of Things (IoT). The E-ISAC also monitored several important cyber events in 2016, including malicious cyber activities by the Russians and a power outage in Ukraine.

Several key topics and takeaways from the analysis of reports include the following:

Phishing: In 2016, over 40 percent of cyber bulletins posted were about phishing; this trend is consistent with what the E-ISAC observed in 2015. These phishing emails contained information relating to the Dridex campaign, html credential harvesting, Gh0st RAT, Locky, typosquatting, whaling, and vawtrak attempts.

Ransomware: Since the beginning of 2016, the E-ISAC reporting and media coverage pointed to a significant increase in ransomware-specific cyber extortion activity. Ransomware is a special class of disruptive, malicious software designed to deny access to data and files until the victim meets payment demands. Once compromised, the victim may have to restore systems from back-up tapes or pay the ransom with the hope of regaining access to the data and files. In response to the prevalence of ransomware across all critical sectors and its destructive capabilities, the E-ISAC provided subject matter expertise in a NERC alert that was issued in June 2016⁷⁶. The E-ISAC also released a detailed assessment in May 2016 outlining the evolution of ransomware tactics.⁷⁷

Internet of Things (IoT): Serious concerns surround the security of devices designed to be used as part of the IoT. Cyber security practitioners generally agree that most IoT devices connected to the Internet are likely to be a target because they generally do not have security as an important part of their design process. Due to the highly

⁷⁴ <https://www.eisac.com/Collaboration#/document/4185>

⁷⁵ Bulletins describe physical and cyber security incidents and provide timely, relevant, and actionable information of broad interest to the electricity industry.

⁷⁶ http://www.nerc.com/pa/rrm/bpsa/Facility%20Ratings%20Alert%20DL/NERC_Alert_A-2016-06-07-01_Ransomware_Extortion_Poses_Increasing_Risk.pdf

⁷⁷ This document is not publicly available.

interconnected and unauthenticated state of the IoT, the lack of sufficient security design in IoT products and toys can be leveraged against critical systems accessible from the internet.

The use of a large number of IoT devices can be harnessed from all areas of the Internet rather than a small number of networks. This massive scale of the IoT devices has successfully generated attack throughput rates on the order of several hundred megabits-per-second to one terabit-per-second (tbps) or more.

The October 21, 2016, distributed denial-of-service (DDoS) attack against the Dyn-managed domain name system (DNS) infrastructure resulted in 1.2 tbps of network throughput (also referred to as bandwidth) being used against the DNS address provider's infrastructure. Malware, such as Mirai, will continue to grow as the overall throughput of internet providers' infrastructure will be the ultimate limiting factor.

A level 2 NERC alert, published on October 11, 2016, was concerned with issues with IoT devices that are connected to the public Internet. In conjunction with the alert, on October 24, 2016, the E-ISAC released its *Internet of Things DDoS White Paper*.⁷⁸

GRIZZLY STEPPE: On December 29, 2016, The Department of Homeland Security (DHS) and the FBI released a Joint Analysis Report (JAR) titled, "GRIZZLY STEPPE - Russian Malicious Cyber Activity"⁷⁹, that provided details of the tools used by Russian intelligence services to compromise and exploit networks and endpoints associated with a range of U.S. government, political, and private sector entities. The JAR also included recommended mitigations and information on how to report such incidents to the U.S. government. The E-ISAC analyzed the indicators of compromise (IOC) provided by government intelligence for potential malicious network traffic that may affect the electricity industry.

Burlington Electric Department (utility) received this information from DHS and found a potentially compromised laptop. The utility conducted further analysis and investigation determining the laptop had not been connected to the grid and that the incident was not linked to any effort by the Russian government to target or hack the utility. Based on information currently available, the E-ISAC believes that neither the electricity industry nor this particular utility were targeted by this cyber attack. The information points to this activity as part of a broader, untargeted campaign searching for vulnerable computers to exploit. Both the wide range in age of indicators in question and the fact that addresses belonged to content providers, cloud computing providers, and internet service providers, in addition to private companies and individuals made the connection of any activity difficult to substantiate as belonging to a particular actor.

CRISP

CRISP is a public-private partnership, cofounded by the DOE and NERC, and managed by the E-ISAC, that facilitates the exchange of detailed cyber security information among industry (i.e., E-ISAC, DOE, and Pacific Northwest National Laboratory). This partnership facilitates information sharing and enables owners and operators to better protect their networks from sophisticated cyber threats.

Participation in the program is voluntary and enables owners and operators to better protect their networks from sophisticated cyber threats. The purpose of CRISP is to collaborate with industry partners to facilitate the timely bidirectional sharing of unclassified and classified threat information. CRISP information helps support development of situational awareness tools to enhance the industry's ability to identify, prioritize, and coordinate the protection of its critical infrastructure and key resources.

⁷⁸ This document is not publicly available.

⁷⁹ https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

CRISP participant companies serve approximately 75 percent of electricity consumers in the United States. The quantity, quality, and timeliness of the CRISP information exchange allows the industry to better protect and defend itself against cyber threats and to make the BPS more resilient.

E-ISAC Member Engagement

In 2016, the E-ISAC completed its first full year working with the Member Executive Committee (MEC), a subcommittee of the Electricity Subsector Coordinating Council (ESCC) that consists of three chief executive officers and eight chief information officers or chief security officers. This group provides strategic guidance to improve and enhance the E-ISAC, particularly in the areas of the products and services the E-ISAC offers to its members. The MEC has two working groups: the Member Engagement, Products, and Services (MEPS) Working Group and the Operations, Tools, and Technologies (OTT) Working Group.

While enhancing the E-ISAC's products and services will be an ongoing activity, the E-ISAC, MEPS, and the OTT made great progress in 2016 to address and implement the MEC recommendations and work plan items. These products and services and continued member engagement will enhance information sharing and as a result the overall security of the grid.

E-ISAC Threat Workshop

As a result of planning and discussions with representatives from the MEPS, the E-ISAC has started hosting unclassified threat workshops biannually. These threat workshops bring together security experts from government and industry to discuss threats facing the electricity industry. The discussions include a focus on past threats, incidents and lessons learned, current threats that may impact industry, or views on emerging threats. The E-ISAC held its first threat workshop on December 6, 2016, in Washington, DC; the second workshop is scheduled for June 20, 2017, in Irwindale, CA.

To maximize information sharing with asset owners and operators (AOO), the workshops include discussions between presenters and attendees during each briefing with E-ISAC analysis of the topics raised and dedicate time to industry discussion after the briefings. These discussions and added analysis by the E-ISAC better enable AOOs to mitigate threats and incorporate best practices.

E-ISAC Monthly Briefing Series Update

The E-ISAC continues to host its monthly briefing series for AOOs, covering timely, CIP topics for participants. The briefings involved federal and technical partners, including DHS staff from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the Office of Intelligence and Analysis, and the National Cybersecurity and Communications Integration Center (NCCIC), as well as FireEye and iSIGHT Partners. The monthly briefing series also includes special guest presentations.

Participation in the monthly briefings during 2016 ranged from 180 to over 400 attendees. This was the first full year that the series included a physical security section (added April 2015), and full replays were available for member download (added December 2015). Based on polling feedback, 70 to 96 percent of attendees consider the meetings to be of "Considerable Value" or "Great Value." The E-ISAC will continue to encourage industry to share security best practices and lessons learned on topics relevant to the industry by inviting more industry AOOs as guest presenters.

Grid Security Exercise (GridEx)

NERC conducted its third biennial grid security and emergency response exercise, GridEx III, on November 18–19, 2015. NERC's mission is to assure the reliability of the BPS, and GridEx III provided an opportunity for industry and other stakeholders to respond to simulated cyber and physical attacks affecting the reliable operation of the grid. Led by the E-ISAC, GridEx III was the largest geographically distributed grid security exercise to date. GridEx III consisted of a two-day distributed play exercise and a separate executive tabletop on the second day. More than

4,400 individuals from 364 organizations across North America participated in GridEx III, including industry, law enforcement, and government agencies.

In March 2016, the E-ISAC released three reports (one available to the public and two restricted to industry and government stakeholders) regarding the lessons learned on GridEx III. The reports summarize the exercise and provide recommendations that the E-ISAC has integrated into its internal crisis action plan and standard operating procedures.⁸⁰ In addition, the ESCC has adopted many of the recommendations into its playbook and used the GridEx III exercise to spur action on cyber mutual assistance, increase spares of critical equipment, and provide cross-sector support during crisis situations. Finally, all participating organizations were able to improve internal and external communications and relationships with important stakeholders and exercise crisis response procedures against an advanced attack scenario that identified potential gaps and improvements to improve security, resilience, and reliability.

Grid Security Conference (GridSecCon)

The E-ISAC hosted over 400 electricity cyber and physical security professionals in Quebec City, Canada, October 17–23, 2016. GridSecCon 2016 provided free training on physical and cyber security issues and technologies, such as Ukraine, Grassmarlin, and Cyber Attack Defense Training Exercise for the Grid. The conference included speaker sessions discussing industry’s work with government partners, space weather, hunting and killing on networks, and advanced research and development in the industry.

Cross-sector Activities

The E-ISAC engages with the government at all levels, including international, federal, state, local, territorial, tribal, and provincial governments. It also includes close international allies with critical infrastructure protection sector partners and other ISACs.

During 2016, the E-ISAC’s federal partners were active in response to Presidential Policy Directive 41: *United States Cyber Incident Coordination* and created projects covering cyber mutual assistance, high profile exercises, cyber incident response plans, learning opportunities for the E-ISAC staff, and power outage incident technical reference products.⁸¹ The E-ISAC worked closely with our federal partners in support of their activities and provided feedback where appropriate, such as with the recently updated National Cyber Incident Response Plan (NCIRP)⁸². The E-ISAC has also maintained participation with the NCCIC, the National Integration Center, and the National Operations Center.

Through the National Council of ISACs (NCI), the E-ISAC is able to collaborate with all critical infrastructure-specific ISACs. The E-ISAC assisted the NCI in establishing new information sharing procedures and collaborative analytical approaches. This partnership helped lead to additional threat briefing opportunities and increased information sharing. Furthermore, this partnership allowed the E-ISAC to provide additional insight and analysis on key topics, such as the Ukraine events and the IoT emerging issue.

Outlook for 2017 and Recommendations

NERC and the electricity industry have taken actions to address cyber and physical security risks to the reliable operation of the BPS as a result of potential and real threats, vulnerabilities, and events. NERC and the BESSMWG, under the direction of CIPC, will continue to do this in 2017 with the development of metrics that provide a global and industry-level view of how security risks are evolving and indicate the extent to which the electricity industry is successfully managing these risks.

⁸⁰ <http://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf>.

⁸¹ <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>.

⁸² <https://www.us-cert.gov/ncirp>

The following recommendations will guide NERC and the BESSMWG in maturing existing and developing new metrics to enhance industry's view of evolving security risks:

- Redefine reportable incidents to be more granular, and include zero consequence incidents that might be precursors to something more serious.
- Use CRISP data to run malware signature comparisons to see how many hits occur on a benchmark set of entities and if any have serious implications for the grid. This metric could be used to provide a percent change from a benchmark year-over-year.
- Use data obtained from CAISS and similar capabilities to characterize the type and frequency of various cyber threats reported through the year.
- Include other data sources such as the FBI, SANS Institute, Verizon, etc., as input for understanding the broader security landscape surrounding critical infrastructures.

Chapter 8: Actions to Address Recommendations in Prior State of Reliability Reports

The *State of Reliability Report* identifies key findings, and many of these findings contain recommended actions for NERC or the larger ERO Enterprise, PAS, and other subcommittees and working groups. **Table 8.1** shows the number of past recommendations and includes whether the item was completed as of the *2016 State of Reliability Report*; was ongoing in 2016, but has since been closed out as a completed recommendation; or is still an ongoing recommendation. Actions completed through the 2016 report are considered archived, and details about their completion are available in this chapter of the report.⁸³

Key Finding Action Status	2011	2012	2013	2014	2015	2016	Total
Completed Status Through 2016 Report	4	6	6	5	8	0	29
Completed During 2016	0	0	1	0	1	3	5
Ongoing as of 2017 Report	0	0	0	0	3	4	7
Total Actions from All Reports	4	6	7	5	12	7	41

Table 8.1 shows that, over the six years of reports, 41 recommendations have been considered actionable. Actions to address those specific items have been completed for 34 recommendations. These actions are understood to have improved the reliability of the BPS. In this report, additional key findings and recommendations are identified and will be reported in future *State of Reliability Reports*.

Table 8.2 outlines actions that have addressed the recommendations completed during 2016, and **Table 8.3** outlines recommendations where actions are currently ongoing and will be included in future reports.

⁸³ Prior *State of Reliability* reports can be found at the following locations:
[http://www.nerc.com/comm/PC/Performance Analysis Subcommittee PAS DL/2011 RARPR FINAL.pdf](http://www.nerc.com/comm/PC/Performance%20Analysis%20Subcommittee%20PAS%20DL/2011%20RARPR%20FINAL.pdf).
[http://www.nerc.com/pa/RAPA/PA/Performance Analysis DL/2012 SOR.pdf](http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2012%20SOR.pdf).
[http://www.nerc.com/pa/RAPA/PA/Performance Analysis DL/2013 SOR May 15.pdf](http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2013%20SOR%20May%2015.pdf).
[http://www.nerc.com/pa/RAPA/PA/Performance Analysis DL/2014 SOR Final.pdf](http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2014%20SOR%20Final.pdf).
<http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2015%20State%20of%20Reliability.pdf>

Completed Recommendations

Table 8.2: Completed Recommendations				
Item Reference	Finding SOR Report Year	Key Finding SOR Reference	Recommendations	Actions Taken to Date
1	2013	Page 17 Paragraph 1	A small subject matter expert technical group should be formed to further study the data collection assumptions when assigning the “Unknown” cause code.	<p>The TADSWG analyzed outages with the “Unknown” cause code; they focused on sustained outages greater than ten minutes. NERC provided blind (nonattributable) results of statistical analyses of entities submitting the highest numbers of outages with Unknown cause code normalized alternatively by number of circuits and by 100 circuit miles. A further list grouped statistically similar entities for submission of Unknowns (from the group with the most to the group with the least submissions of outages with an Unknown cause code). The lists were made available to representatives of the Regions to assist in their discussions with member Transmission Owners (TOs). No Owner can view other Owners’ rankings, but each Owner can view its own ranking and in which statistical group it resides.</p> <p>REs have worked with TOs to improve data that was collected and to reduce unknown sustained outage causes. This effort serves as a model for subsequent investigative analysis. Additional detailed analysis of these cause-coded outages that are consistent with analysis performed by other transmission analytical groups, like the NATF, are being reviewed and will further inform the process. Industry awareness of these cause codes is being elevated by TADSWG and REs. <i>The State of Reliability 2017</i> details a reduction in outages with the cause code of Unknown in calendar year 2016.</p> <p>Efforts will continue, but the recommendation is now complete.</p>

Table 8.2: Completed Recommendations

Item Reference	Finding SOR Report Year	Key Finding SOR Reference	Recommendations	Actions Taken to Date
2	2015	Page 9 Paragraph 5	<p>NERC, working with the NATF, should evaluate the failure rate of circuit breakers and determine the impact of bus configuration on ac transmission circuit outages. NERC, working with IEEE and other applicable industry forums, should develop a consistent method for the collection and distribution of ac substation equipment failure data.</p>	<p>NERC and NATF analyses have confirmed that circuit breaker failure remains the highest probability failure within the Substation Equipment Failure cause code. NERC’s analysis has confirmed that the failure of a circuit breaker to operate properly increases the probability that additional BPS elements will also be forced out of service, increasing the TOS of the event. Bus configuration has the single largest impact on this severity increase. From greatest to least increase, the top three bus configurations are: 1) straight bus, also known as main and transfer bus, 2) ring bus, and 3) breaker and a half bus.</p> <p>Three actions are ongoing based on the completed recommendation:</p> <ul style="list-style-type: none"> • TADSWG is pursuing a multi-pronged approach to obtain more granular data for the AC Substation Equipment Failure cause code. TADSWG is first working with NATF seeking blind data analysis regarding sub-cause codes to determine what insights this might provide. • NERC’s EA group is continuing its analysis of voluntary and mandatory event submissions through the EA Process in order to issue lessons learned but using much more detailed failure cause codes for substation equipment. • The EA group is also participating in and utilizing statistical and trending failure data from outside sources such as the Electric Power Research Institute (EPRI) and the Centre for Energy Advancement through Technical Innovation (CEATI). Collaboration and coordination with these outside organizations are expected to assist in benchmarking

Table 8.2: Completed Recommendations

Item Reference	Finding SOR Report Year	Key Finding SOR Reference	Recommendations	Actions Taken to Date
				<p>and validating equipment failure trends, including further development of possible corrective actions.</p>
3	2016	Page 1 Key finding 1	<p>Results indicate that targeting the top three causes of misoperations should remain an effective mitigation strategy. NERC should, in collaboration with industry, improve knowledge of risk scenarios by focusing education on the instantaneous ground overcurrent protection function and on improving relay system commissioning tests.</p>	<p>The ERO Enterprise, in collaboration with industry and IEEE, is developing and delivering education focused on the instantaneous ground overcurrent function and commissioning tests.</p> <p>For example, RF conducted its <i>Protection System Workshop for Field Personnel</i> on August 16–17, 2016. It focused on commissioning tests.</p> <p>Texas RE working with ERCOT’s System Protection Working Group developed, “A Review of Ground Fault Protection Methods for Transmission Lines⁸⁴” a white paper aimed at reducing protection system misoperations and focused on the instantaneous ground overcurrent function. This document published in Spring 2017.</p> <p>NERC and the SPCS are collaborating with the IEEE Protection System Relaying Committee and an I25 drafting team to release an IEEE Guideline for commissioning testing for use by the industry.</p> <p>The details and results of each of these efforts are being shared across the ERO Enterprise and with each Region’s members to improve protection operational performance.</p> <p>These actions all focus on the two areas addressed in the recommendation, and while NERC always strives for continuous</p>

84

http://www.ercot.com/content/wcm/key_documents_lists/27278/ERCOT_SPWG_Review_of_Ground_Fault_Protection_Methods_For_Transmission_Lines.pdf

Table 8.2: Completed Recommendations

Item Reference	Finding SOR Report Year	Key Finding SOR Reference	Recommendations	Actions Taken to Date
				improvement, this recommendation is now complete.
4	2016	Page 2 Key Finding 4	Through the efforts of the EAS and participation of registered entities, NERC should continue to develop and publish lessons learned from qualifying system events.	Part of the EA Process is to publish lessons learned from system events. EAS will continue to develop and publish lessons learned for the registered entities.
5	2016	Page 4 Key Finding 7	NERC should actively maintain, create, and support collaborative efforts to strengthen situational awareness for cyber and physical security while providing timely and coordinated information to industry. In addition, industry should review its planning and operational practices to mitigate potential vulnerabilities to the BPS.	Through the E-ISAC, NERC continues to monitor and disseminate timely cyber and physical security information for its members. NERC also collaborates to strengthen situational awareness through an agreement with the European Union (EU) to share lessons learned and the hosting and participation in situational awareness and grid security conferences in addition to the biennial GridEx exercise.

Ongoing Recommendations

Table 8.3: Ongoing Recommendations

Item Reference	Finding SOR Report Year	Key Finding SOR Reference	Recommendations	Actions Taken to Date
6	2015	Page 31 Paragraph 2	The collected data (transmission related events resulting in load loss) does not indicate whether load loss during an event occurred as designed. Data collection will be refined in the future for this metric to allow enable data grouping into categories, such as separating load	NERC, PAS, and the TADSWG are currently evaluating data collection and methods that may be enhanced to provide increased awareness of year-over-year trends when load loss occurs during transmission events. These efforts may include collaboration with IEEE and industry forums. This is included in PAS annual reliability metrics review process.

Table 8.3: Ongoing Recommendations

Item Reference	Finding SOR Report Year	Key Finding SOR Reference	Recommendations	Actions Taken to Date
			loss as designed from unexpected firm load loss. Also, differentiating between load losses as a direct consequence of an outage compared to load loss as a result of an operator-controlled action to mitigate an IROL/SOL exceedance should be considered.	
7	2015	Page 32 Paragraph 1	The ERSWG has recommended a measure that was approved by the OC and PC for data collection and testing. This may support development of new voltage and reactive support metrics going forward.	<p>The ERSWG Measures Framework Report contained a proposed measure 7, which was assigned to PAS to develop the necessary data collection processes to allow a test of measure 7 as a potential future voltage and reactive metric.</p> <p>During 2016, PAS developed and conducted a voluntary data collection and released the data for analysis to the SAMS.</p>
8	2015	Page 43 Paragraph 4	Since monitoring the changes that occurred in 2014 versus prior years, the time range categories for IROL exceedances may need to be reviewed. Based on this anticipated result (that monitoring granularity has increased, which may result in a variance over history) the parameters for reporting on Time Range 1 should be examined to ensure that the correct information is being captured.	<p>The TADSWG is currently evaluating data collection and methods that may be enhanced to provide increased awareness of year-over-year trends when load loss occurs during transmission events.</p> <p>Also, the Methods for Establishing IROLs Task Force (MEITF) is currently reviewing consistency of IROL exceedance criteria and may be recommending changes to the IROL exceedance metric.</p>

Table 8.3: Ongoing Recommendations

Item Reference	Finding SOR Report Year	Key Finding SOR Reference	Recommendations	Actions Taken to Date
9	2016	Page 1 Key Finding 2	NERC should consider performing daily SRI calculations on a regional basis to investigate the feasibility of correlating performance with regional weather data.	NERC and PAS are examining interconnection level daily SRI calculations prior to developing possible daily SRI calculations on the regional level.
10	2016	Page 1 Key Finding 3	NERC should provide focus on HP training and education through conferences and workshops that increase knowledge of possible risk scenarios.	NERC continues to host HP workshops to enhance awareness of the HP impact on system risk.
11	2016	Page 2 Key Finding 5	NERC should provide leadership in collaborative efforts to improve system model validation, particularly dynamic models, including the use of synchrophasor and other advanced technology.	Several modeling improvement initiatives have begun. The Synchronized Measurement Subcommittee and the Power Plant Modeling & Verification Task Force have been created to implement and monitor several modeling initiatives. There have also been a number of reliability guidelines and technical reference documents prepared to enhance modeling efforts.
12	2016	Page 2 Key Finding 6	<p>The ERO should lead efforts to monitor the impacts of resource mix changes with concentration on the following:</p> <ul style="list-style-type: none"> • ERS measures for frequency and voltage support that have been developed and adopted • Methods to increase the population and capability of resources providing frequency response, especially under the scenario that conventional generation continues 	The ERSWG continues to develop implementation plans for various essential reliability service measures.

Table 8.3: Ongoing Recommendations

Item Reference	Finding SOR Report Year	Key Finding SOR Reference	Recommendations	Actions Taken to Date
			<p>to be replaced with variable energy resources</p> <ul style="list-style-type: none"> • Reliability of reactive power generators, such as static var compensators(SVCs), FACTS devices, and synchronous condensers when applied to replace the voltage support function of retiring conventional generators, such as low-voltage ride-through • Protection for these devices, as well as compatibility and coordination with other BPS protection and controls 	

Appendix A: Statistical Analysis of SRI Assessment

This appendix contains detailed data analysis supporting the SRI assessment in Chapter 3. NERC staff has statistically analyzed the daily SRI for 2010–2016 to compare total SRI year-over-year differences as well as differences within the individual generation, transmission, and load loss components. Differences by season have also been investigated.

SRI Performance by Year

Tests indicate statistically significant changes among annual distributions of SRI. ANOVA analysis found that 2011 performance was the best SRI since 2010. Moreover, the difference with all other years was statistically significant.⁸⁵ The 2016 SRI performance was statistically similar to 2013 and 2015; statistically better than in 2010, 2012, and 2014, but worse than 2011. The descriptive statistics of the annual distributions of SRI are listed in [Table A.1](#).

Year	N	Mean	Standard Deviation	Minimum	Maximum	Median
2010	365	1.74	0.61	0.59	4.64	1.7
2011	365	1.5	1.04	0.48	13.97	1.34
2012	366	1.78	0.81	0.55	8.87	1.65
2013	365	1.67	0.60	0.46	4.06	1.57
2014	365	1.85	0.87	0.68	11.14	1.72
2015	365	1.67	0.56	0.69	4.47	1.57
2016	366	1.62	0.50	0.57	3.60	1.55

The relative SRI performance by year is further visible in the boxplot representations of [Figure A.1](#). The year 2011 was the best as measured by median as well as mean. This is in spite of the relatively large standard deviation with outliers that included the September 8, 2011, load shed event and the February 2, 2011, cold weather load loss event.

⁸⁵ ANOVA with Fisher's Least Significant Difference test at the significance level of 0.05.

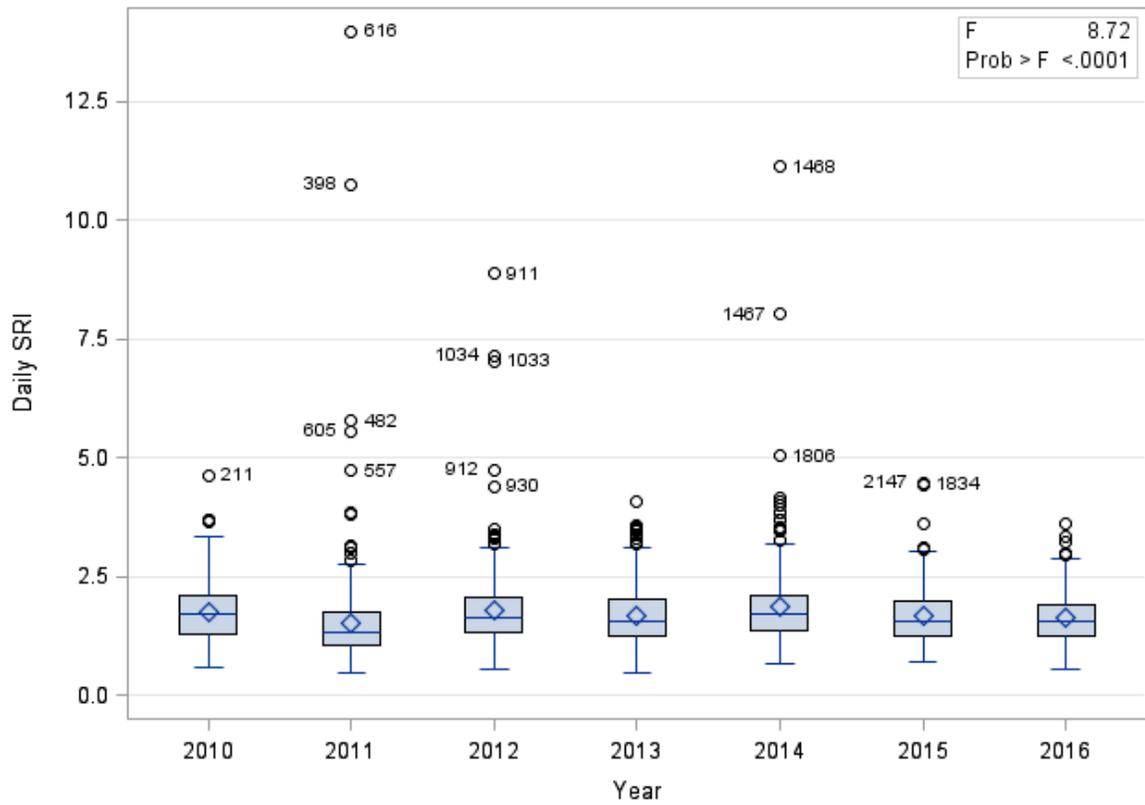


Figure A.1: Boxplot of SRI Distribution by Year

The performance of each year statistically compared to every other year is depicted in [Table A.2](#) below. If no reference to statistical significance is made within the table, it is assumed to be statistically significant.⁸⁶

⁸⁶ At significance level 0.05.

Table A.2: Pairwise Comparison of SRI by Year

Base Year	Compared to Year					
	2011	2012	2013	2014	2015	2016
2010	2011 Better	No Statistically Significant Difference	No Statistically Significant Difference	2010 Better	No Statistically Significant Difference	2016 Better
2011		2011 Better				
2012			2013 Better	No Statistically Significant Difference	2015 Better	2016 Better
2013				2013 Better	No Statistically Significant Difference	No Statistically Significant Difference
2014					2015 Better	2016 Better
2015						No Statistically Significant Difference

Performance of SRI Components by Year

The descriptive statistics of the annual distributions of the weighted generation component of the daily SRI are listed in [Table A.3](#).

Table A.3: Descriptive Statistics of Weighted Generation SRI Component by Year						
Year	N	Mean	Standard Deviation	Minimum	Maximum	Median
2010	365	1.03	0.34	0.29	2.67	1.01
2011	365	0.72	0.29	0.12	3.00	0.69
2012	366	1.12	0.36	0.30	2.92	1.08
2013	365	1.10	0.33	0.29	2.11	1.08
2014	365	1.29	0.72	0.43	9.80	1.16
2015	365	1.14	0.41	0.43	3.97	1.09
2016	366	1.12	0.36	0.38	2.64	1.11

Tests indicate statistically significant changes among annual distributions of the generation component of the daily SRI. ANOVA analysis shows that all pairwise annual differences in the average generation component values are statistically significant except between years 2012 and 2013, 2012 and 2015, 2012 and 2016, 2013 and 2015, 2013 and 2016, and 2015 and 2016. The relative performance of the generation component by year is further displayed in [Figure A.2](#), where 2011 was the best as measured by median as well as mean, and 2014 was the worst with the largest average, median, and standard deviation of the generation component.

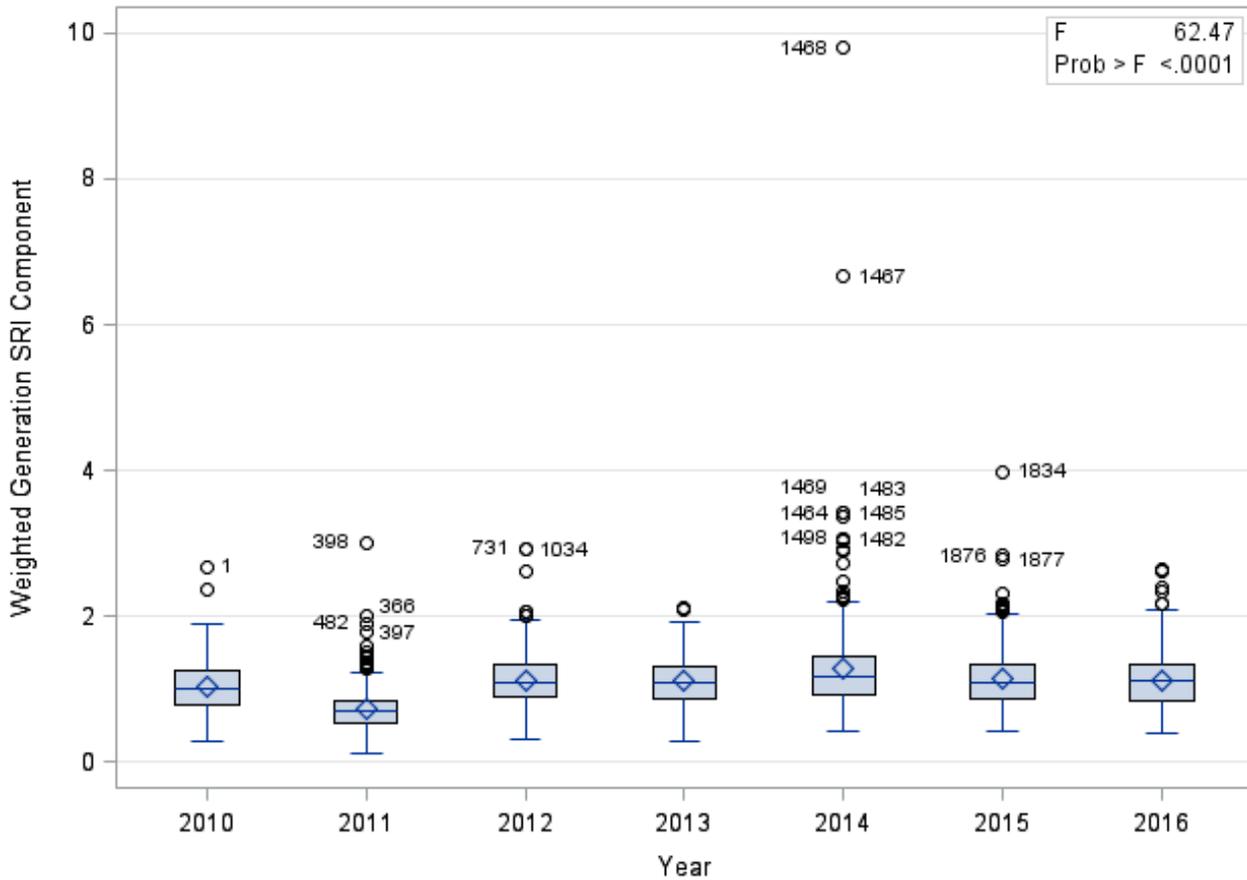


Figure A.2: Boxplot of Distribution of Generation SRI Component by Year

The descriptive statistics of the annual distributions of the transmission component of the daily SRI are listed in [Table A.4](#).

Table A.4: Descriptive Statistics of Weighted Transmission SRI Component by Year						
Year	N	Mean	Standard Deviation	Minimum	Maximum	Median
2010	365	0.55	0.39	0.06	3.17	0.48
2011	365	0.55	0.38	0.03	3.53	0.46
2012	366	0.50	0.38	0.00	3.35	0.43
2013	365	0.42	0.32	0.00	2.20	0.33
2014	365	0.42	0.27	0.05	1.85	0.37
2015	365	0.40	0.26	0.03	1.78	0.33
2016	366	0.40	0.23	0.04	2.33	0.37

Tests indicate statistically significant changes among annual distribution of the transmission component of the daily SRI. ANOVA analysis shows that the years 2010, 2011, and 2012 were worse than the years 2013, 2014, 2015, 2016 (all pairwise differences between the groups are statistically significant). The first three years had not only

statistically larger averages but also larger medians and standard deviations than the most recent three years. It is important to remember that TADS data collection changed in 2015 to include sustained outages for BPS elements below 200 kV; this change significantly affected both the daily numerator and the denominator of the transmission component from 2015 forward. Therefore, comparisons of the transmission components should be limited to those for the years 2010–2014 or those for the years 2015–present in order to avoid introduction of error. The relative performance of the transmission component by year is further illustrated by **Figure A.3**.

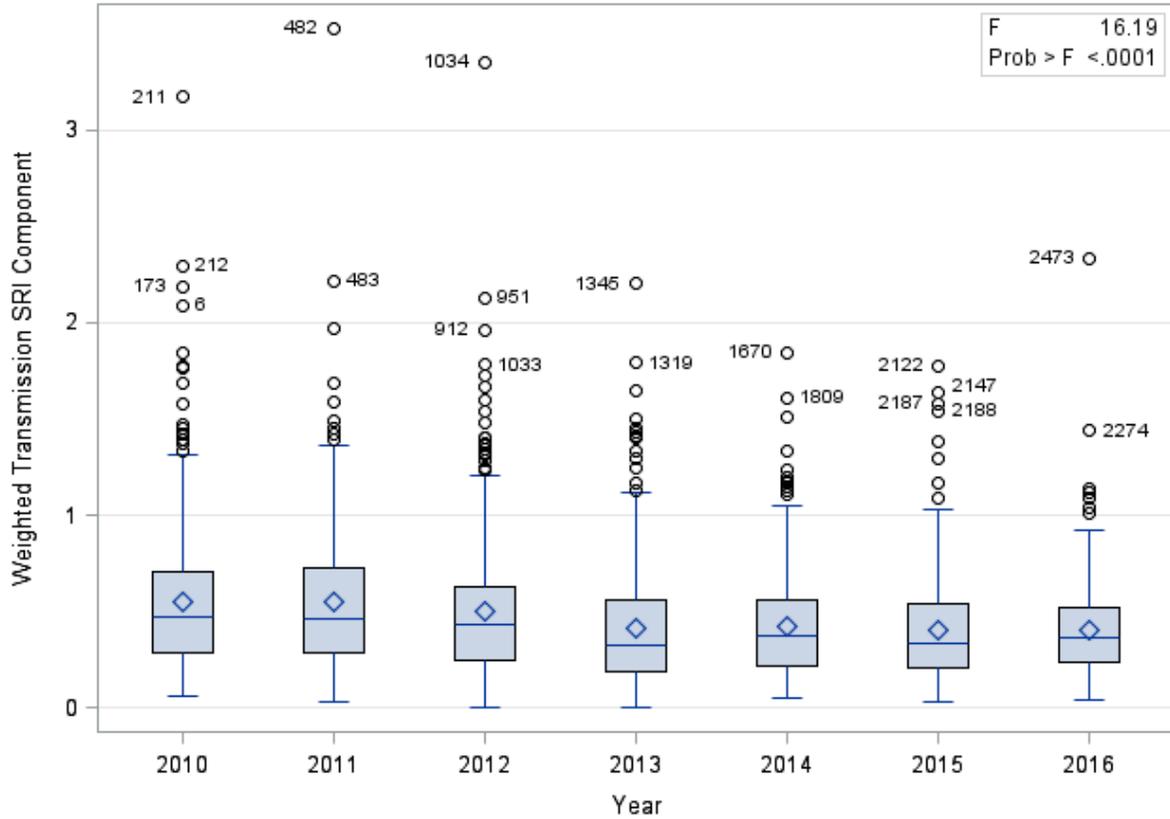


Figure A.3: Boxplot of Distribution of Transmission SRI Component by Year

The descriptive statistics of the annual distribution of the load loss component of the daily SRI are listed in **Table A.5**.

Table A.5: Descriptive Statistics of Weighted Load Loss SRI Component by Year						
Year	N	Mean	Standard Deviation	Minimum	Maximum	Median
2010	365	0.16	0.18	0.00	1.62	0.11
2011	365	0.23	0.77	0.00	11.98	0.11
2012	366	0.17	0.35	0.00	4.88	0.08
2013	365	0.15	0.24	0.00	2.32	0.08
2014	365	0.14	0.25	0.00	3.59	0.07
2015	365	0.13	0.15	0.00	1.72	0.09
2016	366	0.09	0.10	0.00	0.84	0.07

Tests indicated statistically significant changes among annual distribution of the load loss component of the daily SRI. ANOVA analysis showed that the year 2011 was the worst year with a statistically significantly larger average daily load loss component than any other year. 2016 was the best year with the smallest median and variance and statistically better mean than in 2010, 2011, 2012, and 2013. The relative performance of the load loss component by year is further illustrated by [Figure A.4](#).

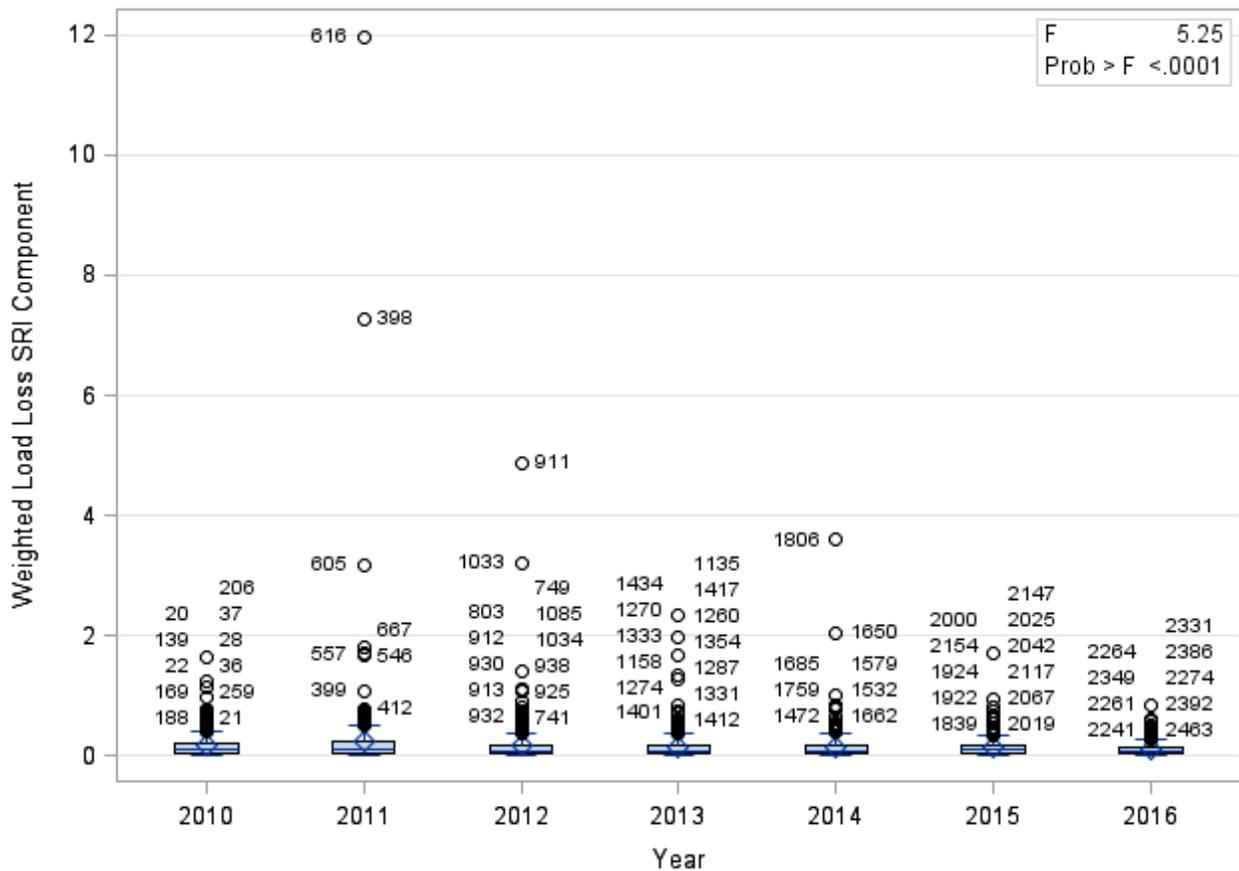


Figure A.4: Boxplot of Distribution of Load Loss Component of SRI by Year

Seasonal Performance of SRI

In **Figure A.5**, the daily performance of SRI is shown over the seven-year history along with a time trend line.

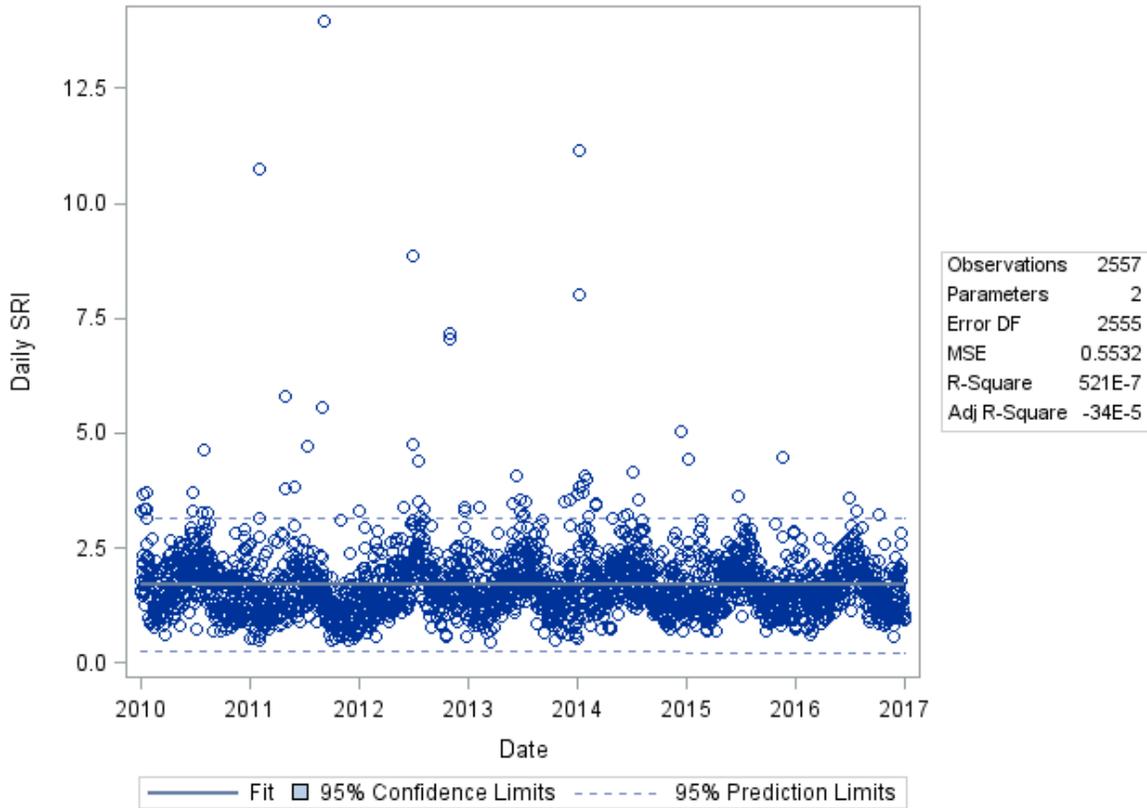


Figure A.5: Scatter Plot for SRI 2010–2016

The time trend line has a negative slope that is not statistically significant ($p = 0.72$). The same result can be drawn for the correlations analysis: on average, daily SRI has been flat from 2010–2016.

Analysis of the seasonal performance reveals statistically significant differences in SRI by season. The fall SRI has the best performance, the summer SRI has the worst, and spring and winter SRIs are statistically similar. **Table A.6** shows the statistics by season based on the 2010–2016 data.

Table A.6: Descriptive Statistics of SRI by Season						
Season	N	SRI				
		Mean	Standard Deviation	Minimum	Maximum	Median
Winter	633	1.63	0.87	0.49	11.14	1.49
Spring	644	1.63	0.52	0.46	5.78	1.57
Summer	642	2.04	0.66	0.69	8.87	1.96
Fall	638	1.45	0.75	0.48	13.97	1.37

Tests⁸⁷ indicate that all differences in the seasonal, expected SRI are statistically significant except those for winter and spring, which are illustrated in **Figure A.6**.

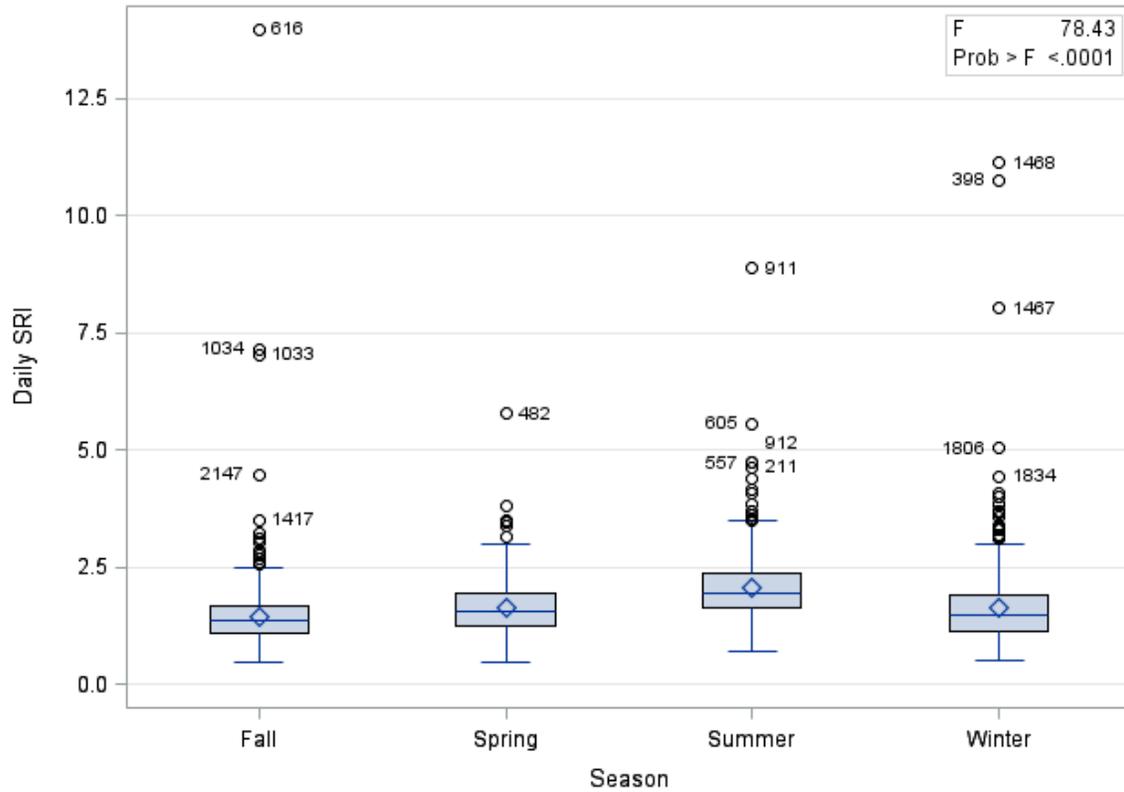


Figure A.6: Boxplot for SRI by Season 2010–2016

⁸⁷ANOVA with Fisher’s Least Significant Difference test at the significance level of 0.05.

Appendix B: Statistical Analysis of Transmission Data

The SRI presented in [Chapter 3](#) consists of several weighted risk impact components: generation, transmission, and load loss.⁸⁸ The transmission component of the SRI is a weighted factor of the impact of a given day's transmission outages (as reported in TADS) on the BPS. This appendix provides an analysis of TADS outage events based on their TADS outage initiating or sustained cause(s).

Study Method

The following four sections provide a description of the data analysis methodology used in the appendix to rank transmission outage causes by risk to the transmission system and track TADS data changes by year.

Defining BPS Impact from Transmission Risk

An impact of a TADS event to the BPS reliability is called the Transmission Outage Severity (TOS) of the event. A TADS event TOS is defined by Equations B.1 and B.2, which are aligned to the definition of transmission component of the SRI. Equation B.1 is used for TADS studies involving ac circuit outage events; Equation B.2 is applied to TADS studies involving both ac circuit and transformer outage events. 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 megavolt ampere (MVA) values, or equivalent MVA values, are shown in [Table B.1](#). These equivalent MVA values are also applied to the denominator of the TOS equation to normalize the function. For normalization, the denominator in Equation B.1 is defined as the sum of the equivalent MVA's of TADS ac circuit inventory for the same year as the event; similarly, the denominator in Equation B.2 is defined as the sum of the equivalent MVA's of TADS ac circuit and transformer inventory for the same year as the event. This allows comparison of TADS events across years while taking into account the changing number of ac circuits and transformers within the BPS.

$$\text{Transmission Outage Severity (TADS AC circuit outage event)} = \frac{\sum(\text{Equivalent MVA of AC Circuits with automatic outages in this event})}{\sum(\text{Equivalent MVA of ALL AC Circuits in TADS inventory})} \cdot 1000$$

Equation B.1

$$\text{Transmission Outage Severity (TADS AC circuit or Transformer outage event)} = \frac{\sum(\text{Equivalent MVA of AC Circuits and Transformers with automatic outages in this event})}{\sum(\text{Equivalent MVA of ALL AC Circuits and Transformers in TADS inventory})} \cdot 1000$$

Equation B.2

⁸⁸ http://www.nerc.com/docs/pc/rmwg/pas/index_team/sri_equation_refinement_may6_2011.pdf, pp. 2-3.

Table B.1: Equivalent MVA Values of TADS Elements		
Voltage Class	AC Circuits	Transformers
100–199 kV	200	100
200–299 kV	700	259
300–399 kV	1,300	518
400–599 kV	2,000	1,034
600–799 kV	3,000	1,441

Impact of the TADS Data Collection Changes

Beginning in 2015, the reporting changed through the *NERC Rules of Procedure 1600 Data Request* so that TADS data collection would align with the implementation of the FERC approved BES definition.⁸⁹ Two additional voltage classes were amended, namely, less than 100 kV and 100–199 kV.

Changes to TADS data collection had an impact on existing metrics and provides for expanded analysis. **Table B.2** illustrates the ac circuit data collected at the various voltage classes available to support outage metrics. For example, discontinuation of the nonautomatic planned outage data no longer supports a total outage availability (or unavailability) metric. Sustained outages are the only common outages collected at all voltage classes above and below 200 kV.

Table B.2: TADS BES Outage Data Collection by AC Voltage Class (Effective Jan 1, 2015)				
AC Voltage Class	Automatic Outages		Nonautomatic Outages	
	Sustained	Momentary	Planned	Operational
Below 100 kV	Yes	No	No	No
100–199 kV	Yes	No	No	No
200–299 kV	Yes	Yes	No	Yes
300–399 kV	Yes	Yes	No	Yes
400–599 kV	Yes	Yes	No	Yes
600–799 kV	Yes	Yes	No	Yes

Legend	
Yes	Outage data collected for this type of outage and voltage class
No	Outage data <u>not</u> collected for this type of outage and voltage class

⁸⁹ <http://www.nerc.com/pa/RAPA/Pages/BES.aspx>

The following six study cases were analyzed for TADS data sets described above. The results of the six ICC studies follow in this Appendix:

1. 200 kV+ TADS ac circuit events (momentary and sustained) from 2012–2016
2. 200 kV+ ac circuit common or dependent-mode (CDM) events, which resulted in multiple transmission element outages from 2012–2016
3. 200 kV+ TADS ac circuit events (momentary and sustained) by Region from 2012–2016
4. 100 kV+ TADS ac circuit sustained events from 2015–2016
5. 100 kV+ TADS ac circuit and transformer 2016 sustained events
6. 100 kV+ sustained 2015–2016 outages analyzed by sustained cause code.

The less than 200 kV sustained automatic outage data set was not included in study cases 1–3 to allow for a valid year-over-year comparative analysis of the 200 kV+ data set for the years 2012–2016. In Studies 1–4 and 6, the TOS of TADS events is calculated by using [Equation B.1](#). In Study 5 it is by using [Equation B.2](#).

Determining Initiating Causes and Modification Method

TADS collects automatic outages⁹⁰ and operational outages.⁹¹ 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 ICC. These ICCs facilitate the study of cause-effect relationships between each event's ICC and event severity. The procedure illustrated in [Figure B.1](#) is used to determine a TADS event's ICCs. The procedure that defines ICCs for a TADS event allows ICC assignment to a majority of transmission outage events recorded in TADS.

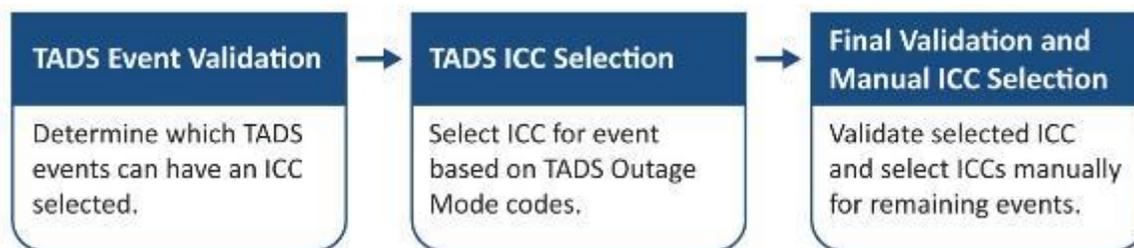


Figure B.1: TADS Event Initiating Cause Code Selection Procedure

Prior to *State of Reliability 2017*, reports have analyzed the TADS data set and TADS-defined ICCs. The *State of Reliability 2013–2016* reports also included analysis based on an augmented data set that defined changes in ICCs to further distinguish normal clearing events from abnormal clearing events. Two TADS ICCs are impacted: Human Error and Failed Protection System Equipment.

- TADS Human Error ICC is subdivided by type codes, which first became available in 2012. Using the type codes in the consequent *State of Reliability* reports, data for two specific type codes related to protection system misoperations have been removed from the Human Error ICC and added to the Failed Protection

⁹⁰ An outage that results from the automatic operation of a switching device, causing an element to change from an in-service state to a not in-service state. Single-pole tripping followed by successful ac single-pole (phase) reclosing is not an Automatic Outage.

⁹¹ A Non-Automatic Outage for the purpose of avoiding an emergency (i.e., risk to human life, damage to equipment, damage to property) or to maintain the system within operational limits and that cannot be deferred. Includes Non-Automatic Outages resulting from manual switching errors.

System Equipment ICC. Those type codes are 61 dependability⁹² (failure to operate) and 62 security⁹³ (unintended operation).

- TADS Failed Protection System Equipment ICC, plus the Human Error type code 61 and 62 data, are added together in a new or augmented ICC labeled “Misoperation” in each *State of Reliability* report.

The *State of Reliability 2013–2014* reports have revealed that analyzing data based on both data sets (TADS ICCs and TADS augmented ICCs to include the Misoperation cause code) has not provided additional information. Therefore, starting with the 2015 report, the TADS data and analyses have been based on the augmented ICC data set, which currently contains five years of data. In the 2017 report, references to ICC mean the augmented ICC as described above.

Determining Relative Risk

The process of the statistical analysis (performed to identify top causes to transmission risk) is demonstrated in **Figure B.2**. After completing Step 1 (quantifying an event impact by TOS) and Step 2 (assigning ICC’s to TADS events), NERC staff determined in Step 3 the correlation between each ICC and TOS. Statistically significant relationships between several ICC’s and TOS were then determined. Sample distributions were also studied to determine any statistically significant pair-wise differences in expected TOS between ICCs. At Step 4, the relative risk was calculated for each ICC group and then ranked by risk to the transmission system. Where applicable, year-to-year changes in TOS and relative risk are evaluated.

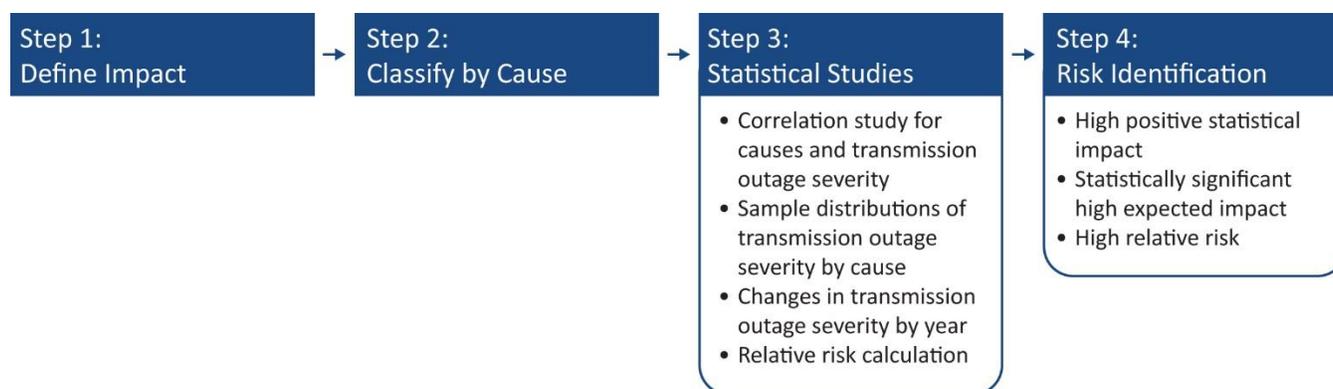


Figure B.2: Risk Identification Method

To study the relationship between ICCs and the TOS for TADS events, NERC investigated the statistical significance of the correlation between TOS and the indicator function⁹⁴ of a given ICC.⁹⁵ The test is able to determine a statistically significant positive or negative correlation between ICC and TOS.

⁹² Event Type 61 Dependability (failure to operate): one or more automatic outages with delayed fault clearing due to failure of a single protection system (primary or secondary backup) under either of these conditions:

- Failure to initiate the isolation of a faulted power system element as designed, or within its designed operating time, or
- In the absence of a fault, failure to operate as intended within its designed operating time.

⁹³ Event Type 62 Security (unintended operation): one or more automatic outages caused by improper operation (e.g., overtrip) of a protection system resulting in isolating one or more TADS elements it is not intended to isolate, either during a fault or in the absence of a fault.

⁹⁴ The indicator function of a given ICC assigns value 1 to an event with this ICC and value 0 to the rest of the events.

⁹⁵ For each ICC, a null statistical hypothesis on zero correlation at significance level 0.05 was tested. If the test resulted in rejection of the hypothesis, it is concluded that a statistically significant positive or negative correlation between an ICC and transmission severity exists; the failure to reject the null hypothesis indicates no significant correlation between ICC and transmission severity.

Distributions of TOS for the entire dataset were examined separately for events with a given ICC. A series of t-tests⁹⁶ were performed to compare the expected TOS of a given ICC with the expected outage severity of the rest of the events at significance level of 0.05. Then the Fisher’s Least Square Difference⁹⁷ method was applied to determine statistically significant⁹⁸ differences in the expected TOS for all pairs of ICCs.

Statistically significant differences in the expected TOS for each ICC group were analyzed for each year of data. This showed if the average TOS for a given ICC group had changed over time.

The relative risk was calculated for each ICC group. The impact of an outage event was defined as the expected TOS associated with a particular ICC group. The probability that an event from a given group initiates during a given hour is estimated from the frequency of the events of each type without taking into account the event duration. The risk per hour of a given ICC was calculated as the product of the probability per hour and the expected severity (impact) of an event from this group. The relative risk was then defined as the percentage of the risk associated with each ICC out of the total (combined for all ICC events) risk per hour. The risk profiles of TADS events initiated by common causes are visualized in [Figure 3.7](#) and [Figure 3.8](#), which summarize the results of correlational, distributional, and risk ranking analyses.

AC Circuit Event Statistics by Year

There are 27,405 TADS ac circuit events with ICCs assigned, comprising 99.9 percent of the total number of TADS events for the years 2012–2016. These events contribute 99.5 percent of the total calculated TOS of the database calculated by [Equation B.1](#) without taking into account transformer outages. [Table B.3](#) provides the corresponding event statistics by year.

Table B.3: TADS AC Circuit Outage Events Summary (2012–2016)						
Summary	2012	2013	2014	2015	2016	2012–2016
Number of TADS Events	3,753	3,557	3,477	7,936	8,721	27,444
Number of Events with ICC Assigned	3,724	3,557	3,467	7,936	8,721	27,405
Percentage of Events with ICC Assigned	99.2%	100.0%	99.7%	100.0%	100.0%	99.9%
TOS all TADS Events	612.4	506	448.2	468.8	489.9	2,525
TOS of TADS Events with ICC Assigned	602.1	506	445	468.8	489.9	2,512
Percentage of TOS of Events with TADS ICC Assigned	98.3%	100%	99.3%	100%	100%	99.5%

⁹⁶ For t-test, see D. C. Montgomery and G. C. Runger, Applied Statistics and Probability for Engineers. Fifth Edition. 2011. John Wiley & Sons. Pp. 361-369.

⁹⁷ For Fisher’s Least Significance Difference (LSD) method or test, see D. C. Montgomery and G. C. Runger, Applied Statistics and Probability for Engineers. Fifth Edition. 2011. John Wiley & Sons. Pp. 524-526.

⁹⁸ At significance level of 0.05.

The increased number of events from 2015 reflects the changes in TADS data collection and includes sustained outages of the 100–199 kV ac circuits. For comparison, in 2012–2014, a TADS ac circuit event in North America started, on average, every two hours and 26 minutes, while in 2015–2016 a TADS ac circuit event started, on average, every one hour and three minutes because more events have become reportable. However, the total TOS of all TADS ac circuit events did not increase dramatically in 2015. This is because of the denominator in [Equation B.1](#) increased due to the 2015 inventory increase and events on 100–199 kV ac circuits have a smaller TOS contribution when compared with other events (as reflected by equivalent MVA values in [Table B.1](#)).

Study 1: TADS Sustained and Momentary Events for 200 kV+ AC Circuits (2012–2016)

Events with Common ICC by Year and Estimates of Event Probability

[Table B.4](#) lists annual counts and hourly event probability of TADS events by ICC. The six largest ICC groups combined amount to 76 percent of TADS events for 200 kV+ for the most recent five years. With the addition of 2016 data, the ICC of Foreign Interference replaced Failed AC Substation Equipment in the top six ICCs.

Almost all TADS ICC groups have sufficient data available to be used in a statistical year-to-year analysis. Only three ICCs (Vegetation; Vandalism, Terrorism, or Malicious Acts; and Environmental) do not have sufficient size for reliable statistical inferences. Therefore, these ICC groups are combined into a new group, named “Combined Smaller ICC Groups Study 1-3,” that can be statistically compared to every other group and also studied with respect to annual changes of TOS.

Using the TOS measure and TADS event ICCs, it is possible to statistically analyze the most recent five years of TADS data (2012–2016). For TADS events initiated by a common cause, the probability⁹⁹ of observing the initiation of an event during a given hour is estimated using the corresponding historical event occurrences reported in TADS. Namely, the event occurrence probability is the total number of occurrences for a given type of event observed during the historical data period divided by the total number of hours in the same period. Therefore, the sum of the estimated probabilities for all events is equal to the estimated probability of any event during a given hour.

Table B.4: TADS 200 kV+ AC Circuit Outage Events and Hourly Event Probability by ICC (2012–2016)

Initiating Cause Code	2012	2013	2014	2015	2016	2012–2016	Event Initiation Probability/Hour
Lightning	852	813	709	783	733	3,890	0.089
Unknown	710	712	779	830	773	3,804	0.087
Weather (excluding lightning)	446	433	441	498	638	2,456	0.056
Failed AC Circuit Equipment	261	248	224	255	362	1,350	0.031
Misoperation	321	281	314	165	249	1,330	0.030
Foreign Interference	170	181	226	274	258	1,109	0.025
Failed AC Substation Equipment	248	191	223	221	214	1,097	0.025
Contamination	160	151	149	154	289	903	0.021

⁹⁹ Probability is estimated using event occurrence frequency of each ICC type without taking into account the event duration.

Table B.4: TADS 200 kV+ AC Circuit Outage Events and Hourly Event Probability by ICC (2012–2016)

Initiating Cause Code	2012	2013	2014	2015	2016	2012–2016	Event Initiation Probability/Hour
Human Error (w/o Type 61 OR Type 62)	212	191	149	132	153	837	0.019
Power System Condition	77	109	83	96	81	446	0.010
Fire	106	130	44	65	72	417	0.010
Other	104	64	77	77	78	400	0.009
Combined Smaller ICC Groups Study 1-3	57	53	49	37	47	196	0.006
<i>Vegetation</i>	43	36	39	32	34	184	0.004
<i>Vandalism, Terrorism, or Malicious Acts</i>	10	9	8	1	7	35	0.001
<i>Environmental</i>	4	8	2	4	6	24	0.001
All with ICC Assigned	3,724	3,557	3,467	3,587	3,947	18,282	0.417
All TADS Events	3,753	3,557	3,477	3,587	3,947	18,321	0.418

In 2016, there was a significant increase in the number of events initiated by Weather (excluding lightning), Failed AC Circuit Equipment, Misoperation, and Contamination. This drove an overall increase in the number of outage events. However, the two biggest ICC groups, Lightning and Unknown, had noticeable decreases in the number of events from 2015 to 2016.

Correlation between ICC and TOS

To study a relationship between ICC and TOS of TADS events, the statistical significance of the correlation between TOS and the indicator function¹⁰⁰ of a given ICC was investigated.¹⁰¹ A statistically significant positive or negative correlation between ICC and TOS could be determined by the statistical test. There were three key outcomes of all tests as stated here:

- A statistically significant positive correlation of ICC to TOS indicates a greater likelihood that an event with this ICC would result in a higher TOS.
- A significant negative correlation indicates the contrary; in this case, a lower TOS would be likely.
- If no significant correlation is found, it indicates the absence of a linear relationship between ICC and the TOS and that the events with this ICC have an expected TOS similar to all other events from the database.

Figure B.3 shows the correlations between calculated TOS and the given ICC. A red bar corresponds to an ICC with statistically significant positive correlation with TOS, a green bar corresponds to an ICC with statistically significant negative correlation, and a blue bar indicates no significant correlation.

¹⁰⁰ The indicator function of a given ICC assigns value 1 to an event with this ICC and value 0 to the rest of the events.

¹⁰¹ For each ICC, a null statistical hypothesis on zero correlation at significance level 0.05 was tested. If the test resulted in rejection of the hypothesis, it is concluded that a statistically significant positive or negative correlation between an ICC and transmission outage severity exists; the failure to reject the null hypothesis indicates no significant correlation between ICC and transmission outage severity.

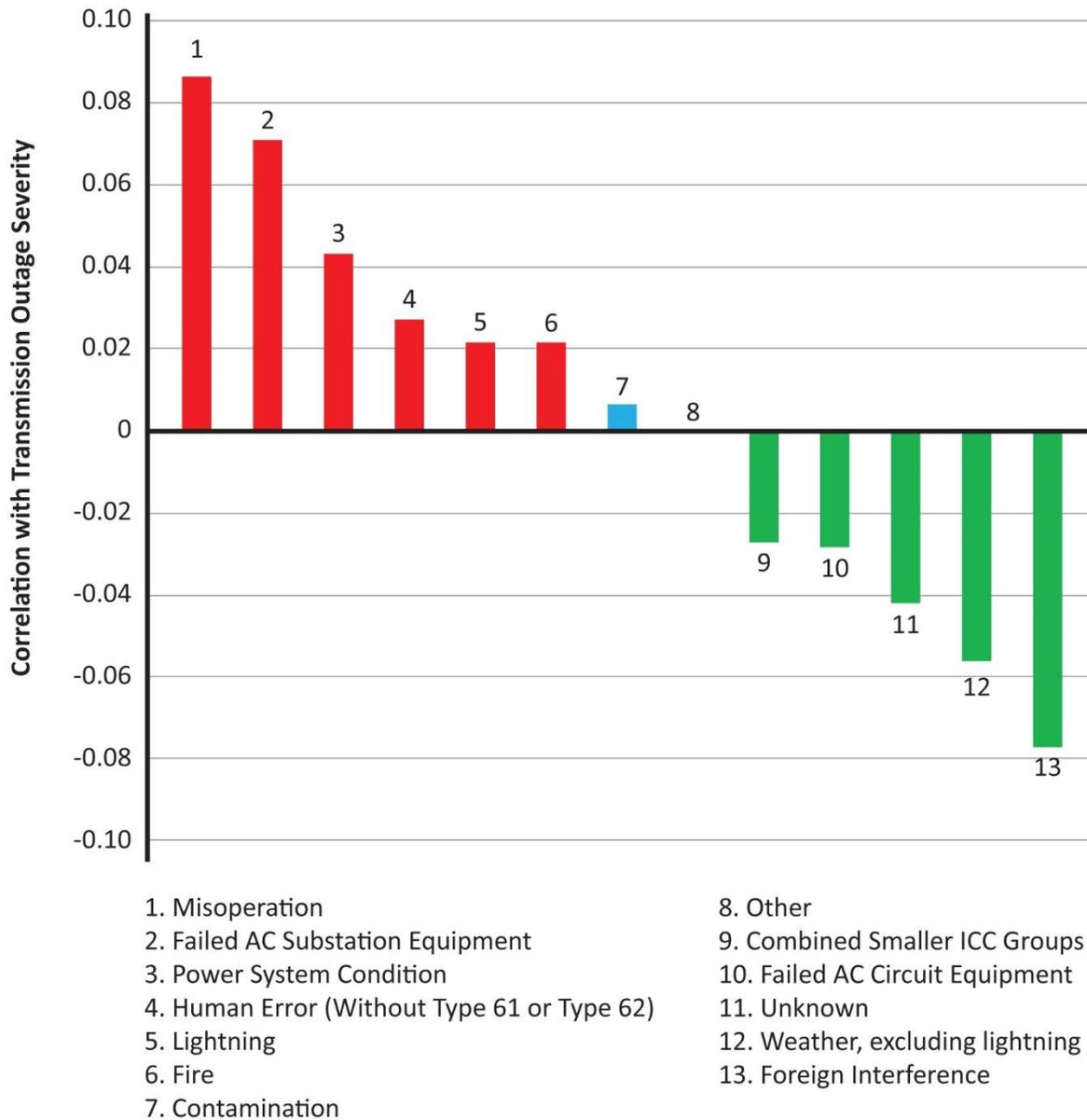


Figure B.3: Correlation between ICC and TOS of 200 kV+ AC Circuit Outage Events (2012–2016)

Distribution of TOS by ICC

The distribution of TOS was studied separately for events with a given ICC and the complete dataset for the five years combined. The sample statistics for TOS are listed in [Table B.5](#) with the ICCs ordered from the largest average TOS to the smallest.

A series of the Fisher’s Least Square Difference tests confirms that the groups of events initiated by Misoperation, Failed AC Substation Equipment, Power System Condition, Fire, Human Error, and Lightning have statistically¹⁰² greater expected severity than other events. It means that when an event initiated by one of these causes occurs, it has a greater impact and a higher risk to the transmission system on average. The tests on homogeneity of variances highlights statistically greater variances (and the standard deviations) for the top three ICC groups and

¹⁰² At significance level 0.05

Human Error as compared with other events. The greater variance can signify additional risk since it implies more frequent occurrences of events with high TOS.

Table B.5 also provides a column that lists ICCs with TOS statistically smaller than for a given ICC referenced by the table's initial column index. For example, Misoperation and Failed AC Substation Equipment initiate events with statistically larger TOS than any other ICC, starting with Fire (indices 4-13). However, differences between the top three groups are not significant, meaning that an individual impact of events from these groups are similar.

Table B.5: Distribution of TOS of 200 kV+ AC Circuit Outage Events by ICC (2012–2016)					
Index No.	ICC	Average TOS	Is Expected TOS Statistically Significantly Different than for other Events?	ICC with Statistically Significantly Smaller Average TOS	Standard Deviation of TOS
1	Misoperation	0.153	Larger	4,5,6,7,8,9,10,11,12,13	0.126
2	Failed AC Substation Equipment	0.151	Larger	4,5,6,7,8,9,10,11,12,13	0.110
3	Power System Condition	0.150	Larger	5,6,7,8,9,10,11,12,13	0.133
4	Fire	0.139	Larger	8,9,10,11,12,13	0.082
5	Human Error (w/o Type 61 OR Type 62)	0.137	Larger	6,8,10,11,12,13	0.093
6	Lightning	0.131	Larger	9,10,11,12,13	0.078
7	Contamination	0.130	No	9,10,11,12,13	0.068
	All events	0.128	N/A	N/A	0.084
8	Other	0.127	No	11,12,13	0.094
	All with ICC assigned	0.127	N/A	N/A	0.083
9	Unknown	0.120	Smaller	11,12,13	0.064
10	Failed AC Circuit Equipment	0.119	Smaller	12,13	0.074
11	Weather (excluding lightning)	0.115	Smaller	13	0.069
12	Combined Smaller ICC Groups Study 1-3	0.108	Smaller	none	0.058
13	Foreign Interference	0.102	Smaller	none	0.056

Average TOS by ICC: Annual Changes

Year-over-year changes in calculated TOS for 200 kV+ ac circuit events by ICC are reviewed next. **Figure B.4** shows changes in the average TOS for each ICC for the 2012–2016 dataset. The groups of ICC events are listed from left to right by descending average TOS for the five years combined. The largest average TOS over the data period was observed for events initiated by Misoperation.

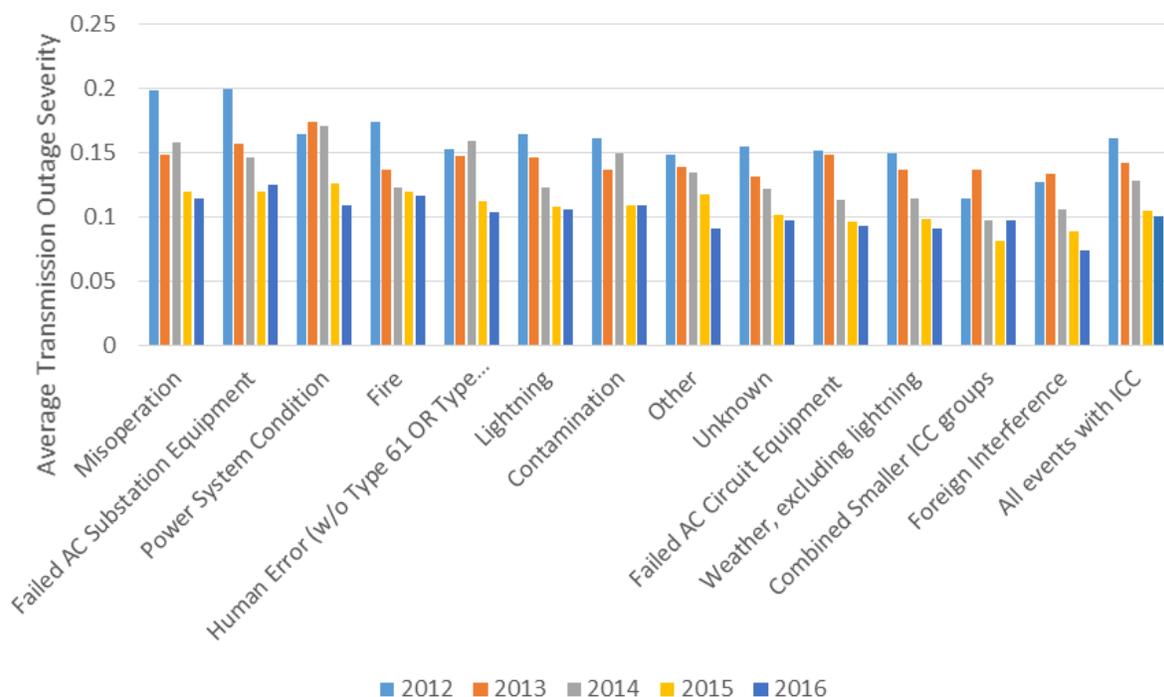


Figure B.4: Average TOS of 200 kV+ AC Circuit Events by ICC and Year (2012–2016)

The noticeable decrease in the average TOS in 2015 for all ICC groups (shown in [Figure B.4](#)) was due to a larger ac circuit inventory and therefore to a larger total MVA of the ac circuit inventory that is a denominator in the formula for the TOS of a TADS event ([Equation B.1](#)). A fair comparison and a valid year-to-year analysis can be performed separately among the 2012–2014 data and between the 2015–2016 data. Compared to 2015, only the ICC group Foreign Interference had a significant change (decrease) in the 2016 average TOS. Overall, the average transmission severity for all events also decreased statistically significantly 2015–2016.

ICC Misoperation has the highest average TOS over the five-year period, but in 2015 and 2016 it ranks third. Another noticeable change in ranking is for the ICC Power System Condition with respect to the average TOS;¹⁰³ in 2015, it ranked the first and in 2016 became the fifth.

TOS Risk and Relative Risk of 200 kV+ AC Circuit Outage Events by ICC

The risk of each ICC group can be defined as the total TOS associated with this group. Its relative risk is equal to the percentage of the group TOS in the 2012–2016 database. Equivalently, the risk of a given ICC per hour can be defined as the product of the probability that an event with this ICC initiates during an hour and the expected TOS (impact) of an event from this group. For any ICC group, the relative risk per hour is the same as the relative risk for a year (or any other time period) if estimated from the same dataset.

Relative risk of the 2012–2016 TADS ac circuit events by ICC is listed in [Table B.6](#). The probability that an event from a given ICC group initiates during a given hour is estimated from the frequency of the events of each type without taking into account the event duration. Excluding weather-related events and events with unknown ICCs, events initiated by Misoperation, by Failed AC Substation Equipment, and by Failed AC Circuit Equipment had the

¹⁰³ Power System Condition is defined as “automatic outages caused by power system conditions such as instability, overload trip, out-of-step, abnormal voltage, abnormal frequency, or unique system configurations (e.g., an abnormal terminal configuration due to existing condition with one breaker already out of service).”

largest shares in the total TOS and contributed 8.7 percent, 7.1 percent, and 6.9 percent respectively to TOS relative risk for the most recent five years.

Power System Condition has a low rank despite having the third largest average TOS of an individual event. This is because there are a small number of events with this ICC, and the occurrences of these events are rare (as reflected by their small probability).

Table B.6: Relative Risk of TADS 200 kV+ AC Circuit Outage Events by ICC (2012–2016)

Group of TADS Events	Probability that an Event from a Group Starts During a Given Hour	Expected Impact (Expected TOS of an Event)	Risk Associated with a Group Per Hour	Relative Risk by Group
All TADS events 200 kV+	0.418	0.128	0.0534	100%
All 200 kV+ with ICC assigned	0.417	0.127	0.0530	99.4%
Lightning	0.089	0.131	0.0116	21.7%
Unknown	0.087	0.120	0.0104	19.6%
Weather (excluding lightning)	0.056	0.115	0.0065	12.1%
Misoperation	0.030	0.153	0.0046	8.7%
Failed AC Substation Equipment	0.025	0.151	0.0038	7.1%
Failed AC Circuit Equipment	0.031	0.119	0.0037	6.9%
Contamination	0.021	0.130	0.0027	5.0%
Human Error (w/o Type 61 OR Type 62)	0.019	0.137	0.0026	4.9%
Foreign Interference	0.025	0.102	0.0026	4.8%
Power System Condition	0.010	0.150	0.0015	2.9%
Fire	0.010	0.139	0.0013	2.5%
Other	0.009	0.127	0.0012	2.2%
Combined Smaller ICC Groups Study 1-3	0.006	0.108	0.0006	1.1%

Figure B.5 shows year-over-year changes in the relative risk of TADS events by ICC. The groups of ICC events are listed from left to right by descending relative risk for the most recent five years combined. The top two contributors to transmission risk—Lightning and Unknown—had a decrease in relative risk in 2016 due to a decrease in the number (and the frequency) of events as reflected in Table B.4. In contrast, Weather (excluding lightning) had an increase due to a significant (28 percent) increase in the number of the weather-initiated events in 2016.

The relative risk of Misoperation increased from 5.3 percent in 2015 to 7.2 percent in 2016 due to an increase in the number of outage events initiated by Misoperation, still being the second smallest relative risk for the group over the five years. Also, there was a significant increase in the relative risk for the ICCs Failed AC Circuit Equipment and Contamination due to increases in the frequency of these events in 2016.

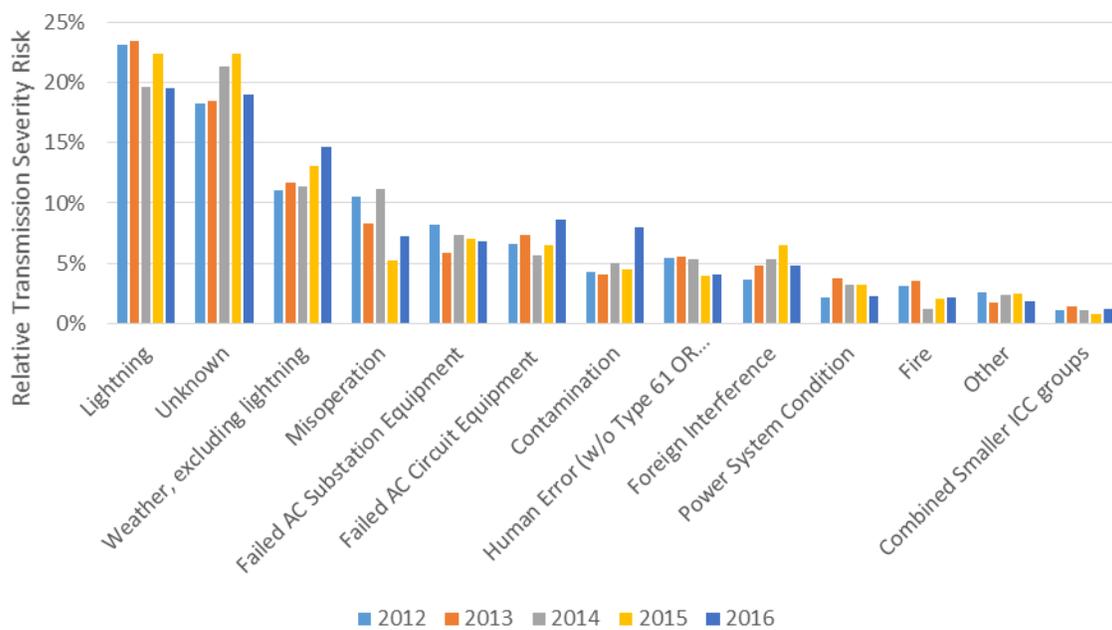


Figure B.5: Relative TOS Risk 200 kV+ AC Circuit Outage Events by ICC and Year (2012–2016)

Study 2: TADS CDM Events for 200 kV+ AC Circuits

Common/Dependent Mode Event ICC Analysis (2012–2016)

TADS also provides information to classify outages as Single Mode or CDM events. A Single-Mode event is defined as a TADS event with a single-element outage. CDM events result in multiple transmission element outages where all outages have one of the mode codes (other than Single Mode) as described in [Table B.7](#). These TADS events have a higher TOS than TADS events with a Single-Mode outage. It is important to monitor and investigate CDM events due to their increased potential risk to system reliability.

Table B.7: Outage Mode Codes	
Outage Mode Code	Automatic Outage Description
Single Mode	A single-element outage that occurs independently of another automatic outage
Dependent Mode Initiating	A single-element outage that initiates at least one subsequent element automatic outage
Dependent Mode	An automatic outage of an element that occurred as a result of an initiating outage, whether the initiating outage was an element outage or a nonelement outage
Common Mode	One of at least two automatic outages with the same initiating cause code where the outages are not consequences of each other and occur nearly simultaneously
Common Mode Initiating	A common-mode outage that initiates one or more subsequent automatic outages

TADS event are categorized as either a Single Mode event or a CDM event where possible. Some TADS events were entered as a combination of Single Mode outages and other outage modes. These events were manually

examined to determine if the event was Single Mode or CDM. For some events, it was not possible to determine whether the event was Single Mode or CDM, nor was it possible to tell the ICC for the event. These events, approximately 0.2 percent of all TADS 200 kV+ events, were removed from the study.

Table B.8 lists numbers of CDM events of 200 kV+ ac circuits by ICC for 2012–2016. There was a total of 2,701 CDM events with 2,664 of these assigned to one of the 15 ICCs. CDM events comprise 14.7 percent of all TADS 200 kV+ events from 2012–2016. The reciprocal of the CDM probability per hour of 0.062 predicts that in NERC’s defined BES system of 200 kV+ ac circuits that a CDM event started, on average, every 16 hours and 14 minutes.

Table B.8 provides the population percentage of CDM events in the different ICC groups. These percentages vary greatly. There are only 3.4 percent of CDM events among events initiated by Contamination while the 42.6 percent of events initiated by Power System Condition are CDM events.

Table B.8: CDM Events of 200 kV+ AC Circuits and Hourly Event Probability by ICC (2012–2016)				
Initiating Cause Code	CDM events	TADS events 200 kV+	CDM as % of ALL	CDM Event Initiation Probability/Hour
Misoperation	446	1,330	33.5%	0.010
Failed AC Substation Equipment	425	1,097	38.7%	0.010
Lightning	421	3,890	10.8%	0.010
Unknown	238	3,804	6.3%	0.005
Weather (excluding lightning)	213	2,456	8.7%	0.005
Human Error (w/o Type 61 OR Type 62)	190	837	22.7%	0.004
Power System Condition	190	446	42.6%	0.004
Failed AC Circuit Equipment	179	1,350	13.3%	0.004
Foreign Interference	128	1,109	11.5%	0.003
Other	106	400	26.5%	0.002
Fire	70	417	16.8%	0.002
Contamination	31	903	3.4%	0.001
Combined Smaller ICC Groups Study 1-3	27	243	11.1%	0.001
<i>Vegetation</i>	13	184	7.1%	0.0003
<i>Environmental</i>	7	24	29.2%	0.0002
<i>Vandalism, Terrorism, or Malicious Acts</i>	7	35	20.0%	0.0002
With ICC Assigned	2,664	18,282	14.6%	0.061
TADS Events	2701	18321	14.7%	0.062

Annual datasets of CDM events do not have enough observations to track statistically significant year-over-year changes in TOS. Upon combining the three smallest ICC groups (Vegetation; Environmental; and Vandalism, Terrorism, or Malicious Acts) into a new group (Combined Smaller ICC groups), the five-year ICC groups are used for the correlation analysis. Out of all ICCs, only Foreign Interference has a statistically significant (negative) correlation with the indicator of TOS.

The TOS by ICC is analyzed and the distributions of TOS by ICC are statistically compared. The sample statistics for TOS by ICC are listed in Table B.9 (same format as [Table B.5](#)). The TOS of the 2012–2016 CDM events of the 200 kV+ ac circuits has a sample mean of 0.191 and a sample deviation of 0.152 shown in the highlighted row. The mean TOS is greater than the 0.128 for all 200 kV+ TADS events in [Table B.5](#) which is not surprising since CDM events involve multiple outages.

Statistical tests determined few statistically significant differences in the average TOS between ICC groups. These results reflect less variability between ICC groups for CDM events than for all events partially due to their smaller sizes. Only three ICC groups have statistically different expected outage severity; events initiated by Lightning have the higher expected severity than the other CDM events while events initiated by Foreign Interference, and events from smaller groups combined have the smaller expected TOS than the other CDM events.

Table B.9 also provides a column that lists ICCs with TOS statistically smaller than for a given ICC referenced by the table’s initial column index. For example, Contamination initiates events with statistically larger TOS than ICC Foreign Interference or Combined Smaller ICC groups.

Table B.9: Distribution of TOS of CDM 200 kV+ AC Circuit Outage Events by ICC (2012–2016)					
Index No.	ICC	Average TOS	Is Expected TOS Statistically Significantly Different than for Other Events?	ICC With Statistically Significantly Smaller Average TOS	Standard Deviation of TOS
1	Contamination	0.233	No	12, 13	0.186
2	Lightning	0.202	Larger	13	0.139
3	Human Error (w/o Type 61 OR Type 62)	0.195	No	13	0.152
4	Failed AC Circuit Equipment	0.193	No	13	0.134
5	Misoperation	0.192	No	13	0.185
	CDM events	0.191	N/A	N/A	0.152
6	Unknown	0.191	No	13	0.137
7	Power System Condition	0.190	No	13	0.180
	CDM with ICC assigned	0.189	N/A	N/A	0.151
8	Failed AC Substation Equipment	0.189	N/A	13	0.145
9	Weather (excluding lightning)	0.187	No	13	0.136
10	Fire	0.184	No	13	0.124
11	Other	0.174	No	none	0.145
12	Combined Smaller ICC groups	0.152	Smaller	none	0.086
13	Foreign Interference	0.135	Smaller	none	0.094

The overall transmission risk and relative risk by ICC group for CDM events were calculated and ranked. Table B.10 provides a breakdown of relative risk of CDM events by ICC group.

Table B.10: Relative Risk of 200 kV+ AC Circuit CDM Events by ICC (2012–2016)

Group of TADS events	Probability that an Event from a Group Starts During a Given Hour	Expected Impact (Expected TOS of an Event)	Risk Associated with a Group Per Hour	Relative Risk by Group
All TADS 200 kV+	0.418	0.128	0.0534	100%
CDM events	0.062	0.191	0.0118	22.1%
CDM with ICC assigned	0.061	0.189	0.0115	21.5%
Misoperation	0.010	0.192	0.0020	3.7%
Lightning	0.010	0.202	0.0019	3.6%
Failed AC Substation Equipment	0.010	0.189	0.0018	3.4%
Unknown	0.005	0.191	0.0010	1.9%
Weather (excluding lightning)	0.005	0.187	0.0009	1.7%
Human Error (w/o Type 61 OR Type 62)	0.004	0.195	0.0008	1.6%
Power System Condition	0.004	0.190	0.0008	1.5%
Failed AC Circuit Equipment	0.004	0.193	0.0008	1.5%
Other	0.002	0.174	0.0004	0.8%
Foreign Interference	0.003	0.135	0.0004	0.7%
Fire	0.002	0.184	0.0003	0.6%
Contamination	0.001	0.233	0.0002	0.3%
Combined Smaller ICC groups	0.001	0.152	0.0001	0.2%

Analysis of TADS CDM events indicated that events with ICCs of Misoperation, Lightning, and Failed AC Substation Equipment are the three largest contributors to TOS of the 200 kV+ ac circuit events with multiple outages.

Study 3: Regional Entity Transmission Analysis

The following is a study of the TOS of TADS events by Region. This analysis is based on the 2012–2016 TADS data for the 200 kV+ ac circuits and utilizes the general methodology described in the previous sections. Here, a summary of this analysis is introduced and similarities and differences in transmission risk profiles by Region are examined. [Figure B.6](#) shows the breakdown of NERC-wide inventory, TADS ac circuit events and TOS risk by Region. The breakdown of the number of outage events and total TOS is similar to breakdown of the NERC inventory by ac circuit counts and by ac circuit miles.

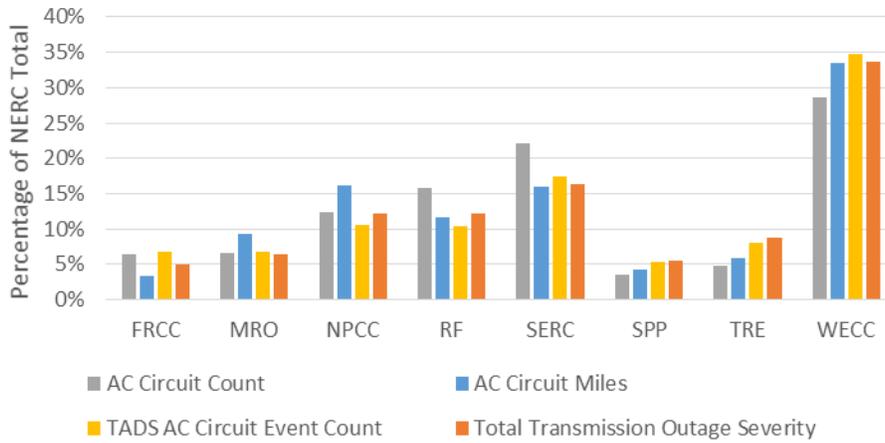


Figure B.6: NERC 200 kV+ AC Circuit Inventory, TADS Events and Breakdown by Region (2012–2016)

The Regional ac circuit inventories differ by count (number of circuits or circuit miles) and by voltage class mix. This may contribute to the significant differences in the average TOS of TADS events between Regions. Since the ac circuit voltage determines the TOS ([Equation B.1](#)), outages on systems with higher voltages would have a greater impact.

The TOS by ICC was studied for each Region. A comparative analysis of RE relative risks by ICC is summarized in [Figure B.7](#). ICCs are listed from left to right by decreasing relative risk for NERC data.

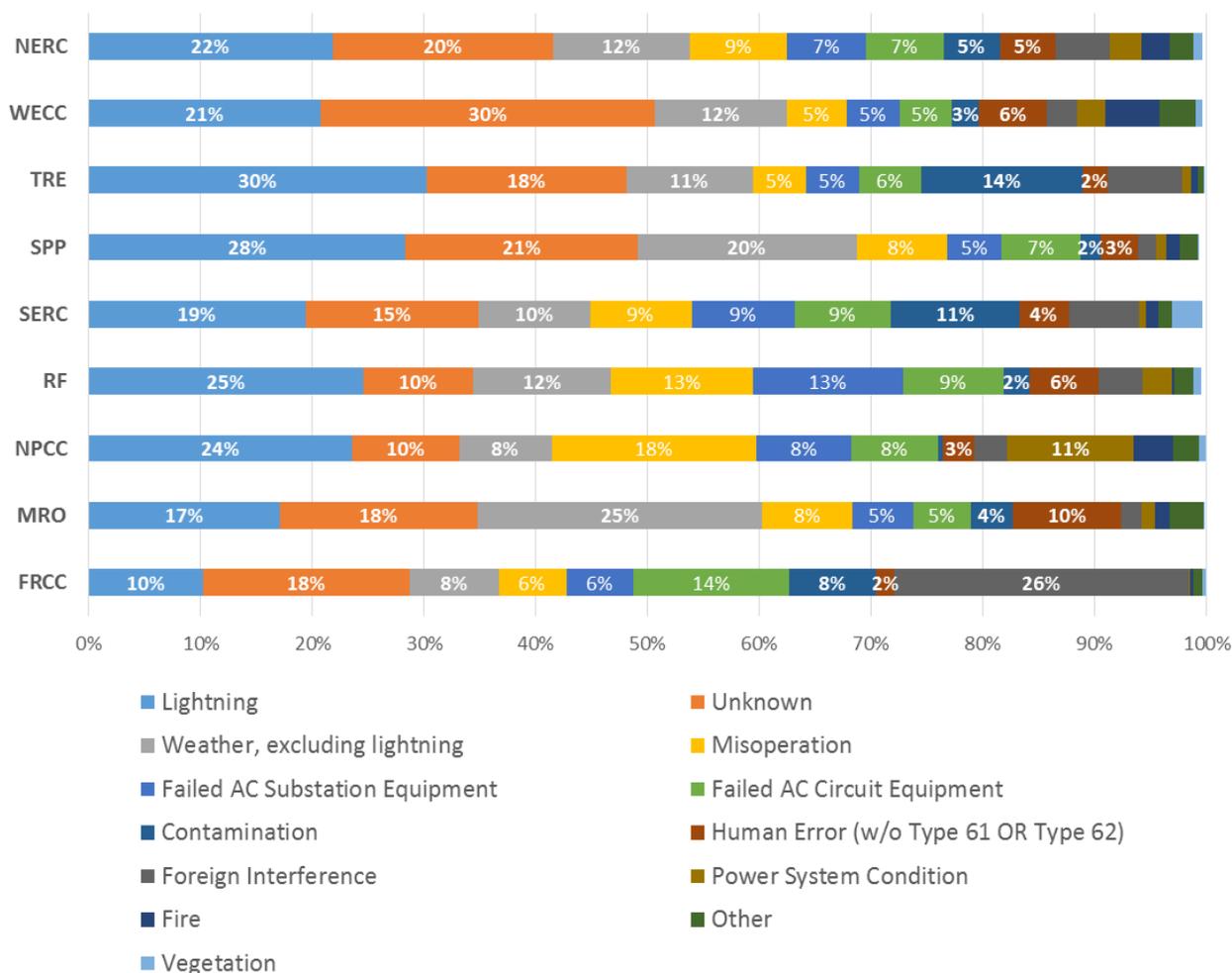


Figure B.7: Relative Transmission Risk of 200 kV+ AC Circuit Outage Events by ICC and Region (2012–2016)

The ICC contributions vary dramatically among Regions for the top NERC ICCs. For example, Misoperation has the highest relative risk in NPCC (18 percent) and the lowest in TRE and WECC (five percent) with other Regions’ numbers closer to the NERC average of nine percent. For MRO, SPP, TRE, and WECC, AC Substation Equipment failures resulted in five percent of the total TOS while they contributed 13 percent in RF.

FRCC has a very distinctive profile with a unique risk breakdown. First, the top three ICCs for North America (the two weather-related ICCs and Unknown) comprise only 37 percent of the TOS in FRCC versus 54 percent for NERC. Second, FRCC’s top-risk ICC is Foreign Interference, which ranks very low for NERC and other Regions. Note that NERC’s top nonweather-related contributors, Misoperation, and Failed AC Substation Equipment, together comprise only 12 percent of FRCC’s transmission risk compared with 14 percent for Failed AC Circuit Equipment.

Study 4: TADS Sustained Events of 100 kV+ AC Circuits (2015–2016)

Sustained Events with Common ICC by Year and Estimates of Event Probability

TADS provides information to classify automatic outages as momentary or sustained.¹⁰⁴ A momentary outage is defined as an automatic outage with an outage duration less than one minute. If the circuit recloses and trips

¹⁰⁴ <http://www.nerc.com/pa/RAPA/tads/Pages/default.aspx>.

again within less than a minute of the initial outage, it is only considered one outage. The circuit would need to remain in service for longer than one minute between the breaker operations to be considered two outages.

A Sustained Outage¹⁰⁵ is defined as an automatic outage with an outage duration of a minute or greater. The definition of Sustained Outage has been extended to a TADS event with duration of a minute or greater.

The addition of the BES elements below 200 kV, beginning in the year 2015, significantly increased TADS inventory, especially for ac circuits. It should be noted that only sustained outages were collected by TADS for voltages less than 200 kV. This study is based on the 2015–2016 TADS data for sustained outages of the 100 kV and above ac circuits.

Table B.11 provides information on the number of sustained events in different ICC groups by year. Some ICC groups of sustained events do not have a population large enough to determine statistically significant year-over-year changes in TOS. For this analysis, the three smallest ICC groups (Fire; Environmental; and Vandalism, Terrorism, or Malicious Acts) were combined into a new group (Combined Smaller ICC groups Study 4–5). Vegetation is not one of Study 4’s three smallest ICC groups, as it was in Study 1-3. For ac circuits below 200 kV, Vegetation initiates 7.5 percent of 100 kV+ ac circuits sustained events versus only 1.4 percent of sustained events of the 200 kV+ ac circuits.

In Table B.11, the reciprocal of the probability per hour of 0.653 estimates that in the defined BES system, a sustained ac circuit event started, on average, every one hour and 32 minutes.

Initiating Cause Code	2015	2016	2015–2016	Sustained Event Initiation Probability/Hour
Weather (excluding lightning)	941	1,083	2,024	0.115
Failed AC Circuit Equipment	674	831	1,505	0.086
Unknown	781	712	1,493	0.085
Lightning	632	637	1,269	0.072
Failed AC Substation Equipment	522	545	1,067	0.061
Foreign Interference	440	539	979	0.056
Misoperation	330	435	765	0.044
Vegetation	301	317	618	0.035
Human Error (w/o Type 61 OR Type 62)	272	323	595	0.034
Other	177	157	334	0.019
Power System Condition	107	159	266	0.015
Contamination	76	178	254	0.014

¹⁰⁵ The TADS definition of Sustained Outage is different from the NERC *Glossary of Terms* used in *Reliability Standards* definition of Sustained Outage that is presently only used in FAC-003-1. The glossary defines a Sustained Outage as follows: “The de-energized-energized condition of a transmission line resulting from a fault or disturbance following an unsuccessful automatic reclosing sequence and/or unsuccessful manual reclosing procedure.” The definition is inadequate for TADS reporting for two reasons. First, it has no time limit that would distinguish a sustained outage from a momentary outage. Second, for a circuit with no automatic reclosing, the outage would not be “counted” if the TO has a successful manual reclosing under the glossary definition.

Table B.11: Sustained Events 100 kV+ AC Circuits and Hourly Event Probability by ICC (2015–2016)				
Initiating Cause Code	2015	2016	2015–2016	Sustained Event Initiation Probability/Hour
Combined Smaller ICC Groups Study 4-5	139	142	281	0.016
<i>Fire</i>	113	120	233	0.013
<i>Environmental</i>	22	11	33	0.002
<i>Vandalism, Terrorism, or Malicious Acts</i>	4	11	15	0.001
With ICC Assigned	5,392	6,058	11,450	0.653
All Sustained Events	5,392	6,058	11,450	0.653

Out of the 11,450 sustained events in 2015–2016, a total of 7,445 (65 percent) events involve 100-199 kV ac circuits, 3,899 events (34.1 percent) involve 200 kV+ ac circuits, and only 106 events (0.9 percent) involve outages of ac circuits from both groups of voltage classes: 100-199 kV and 200 kV+.

From 2015 to 2016, the number of sustained ac circuit events increased by 12 percent. While the biggest increase, by 175 percent for ICC Vandalism, Terrorism, or Malicious Acts, can be considered as anecdotal (from four events in 2015 to 11 events in 2016), some larger groups also had significant increases: Weather, excluding lightning, (15 percent), Failed AC Circuit Equipment and Foreign Interference (23 percent each), Misoperation (32 percent), and Power System Condition (49 percent). On a positive side, the third biggest group, Unknown, had a decrease of nine percent.

Correlation Analysis and Distribution of TOS of Sustained AC Circuit Events by ICC

Figure B.8 shows the correlations between calculated TOS and the given ICC. A red bar corresponds to an ICC with statistically significant positive correlation with TOS, a green bar corresponds to an ICC with statistically significant negative correlation, and a blue bar indicates no significant correlation.

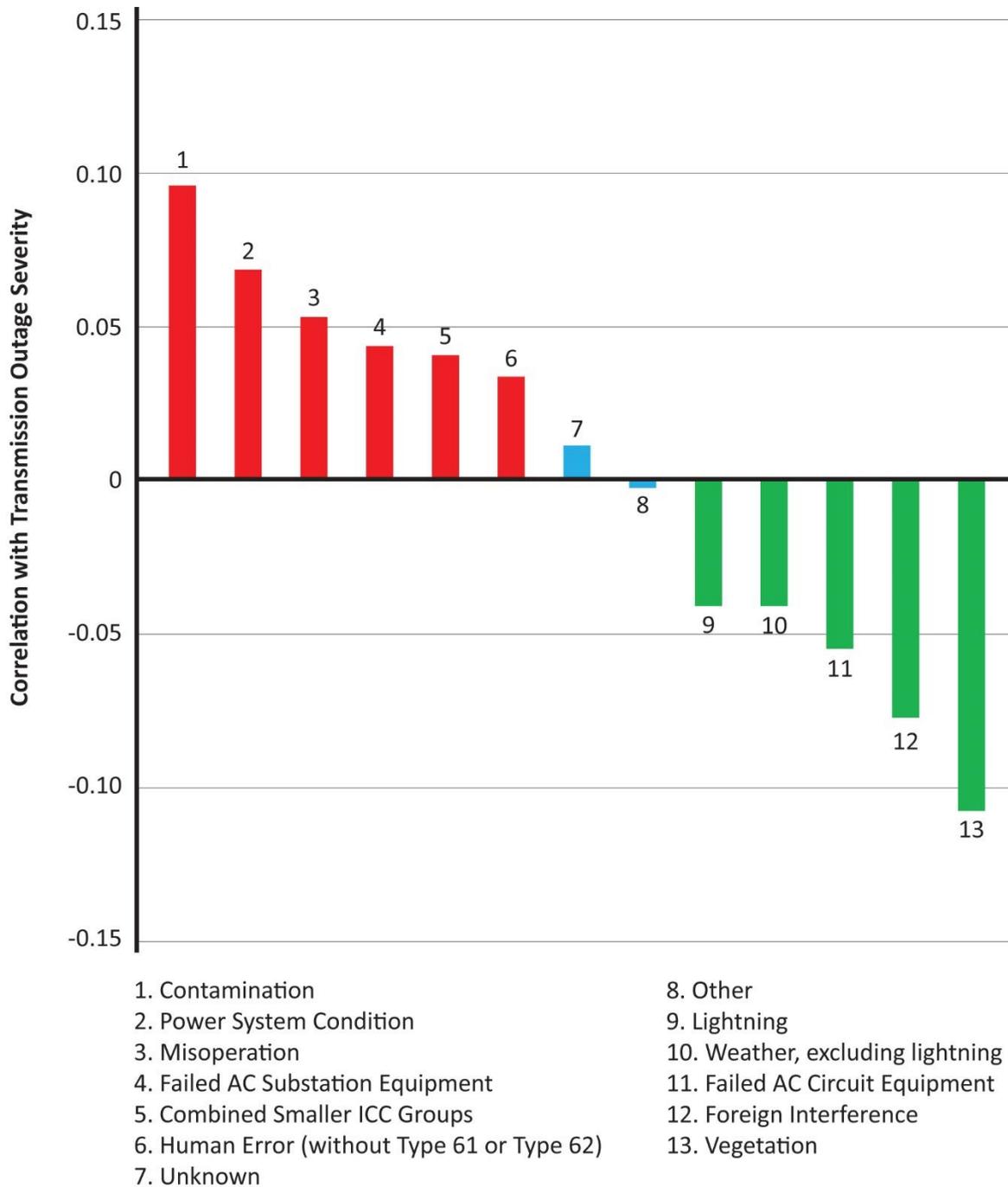


Figure B.8: Correlation between ICC and TOS of Sustained Events of 100 kV+ AC Circuits (2015–2016)

The results for most ICC groups are similar to the analysis of all 200 kV+ TADS events as illustrated by [Figure B.3](#). However, the ICC with the highest positive correlation for sustained events, Contamination, does not have a significant correlation with TOS for all momentary and sustained events of the 200 kV+ ac circuits. Correlation analysis results are also different for ICCs Lightning and Unknown.

The distribution of TOS was studied separately for events with a given ICC and the complete dataset of sustained events for the two years combined. The TOS of the 2015–2016 TADS sustained events (100 kV+ ac circuits data

set) has a sample mean of 0.051 and a sample standard deviation of 0.055. The sample statistics for TOS are listed in Table B.12 with the ICCs ordered from the largest average TOS to the smallest.

Statistical tests confirms that the groups of events initiated by Contamination, Power System Condition, Combined Smaller ICC groups, Misoperation, Human Error, Failed AC Substation Equipment Fire, and Unknown have statistically¹⁰⁶ greater expected outage severity than other events. This means that when an event initiated by one of these causes occurs, it has a greater impact and a higher risk to the transmission system on average. Moreover, the tests on homogeneity of variances highlights statistically greater variances (and the standard deviations) for the top six ICC groups as compared with other events. The greater variance is an additional risk factor since it implies more frequent occurrences of events with high TOS. Note that Combined Smaller ICC groups has a higher average TOS due to events initiated by Fire, which have the mean outage severity of 0.070.

Table B.12 also provides a column that lists ICCs with TOS statistically smaller than for a given ICC referenced by the table’s initial column index. For example, Contamination initiates events with statistically larger TOS than any other ICC (indices 2–13).

Table B.12: Distribution of TOS of Sustained Events of 100 kV+ AC Circuits by ICC (2015–2016)

Index No.	ICC	Average TOS	Is Expected TOS Statistically Significantly Different than for Other Sustained Events?	ICC with Statistically Significantly Smaller Average TOS	Stand Deviation of TOS
1	Contamination	0.086	Larger	2,3,4,5,6,7,8,9,10,11,12,13	0.064
2	Power System Condition	0.075	Larger	3,4,5,6,7,8,9,10,11,12,13	0.081
3	Combined Smaller ICC Groups Study 4-5	0.066	Larger	7,8,9,10,11,12,13	0.063
4	Misoperation	0.062	Larger	7,8,9,10,11,12,13	0.070
5	Human Error (w/o Type 61 OR Type 62)	0.060	Larger	9,10,11,12,13	0.060
6	Failed AC Substation Equipment	0.059	Larger	9,10,11,12,13	0.069
7	Unknown	0.055	Larger	9,10,11,12,13	0.053
8	Other	0.054	No	10,11,12,13	0.063
	All Sustained events	0.051	N/A	N/A	0.055
	With ICC assigned	0.051	N/A	N/A	0.055
9	Lightning	0.050	No	10,11,12,13	0.054
10	Weather (excluding lightning)	0.046	Smaller	12,13	0.048
11	Failed AC Circuit Equipment	0.043	Smaller	12,13	0.046
12	Foreign Interference	0.036	Smaller	13	0.038
13	Vegetation	0.025	Smaller	none	0.027

¹⁰⁶ At significance level 0.05

Average TOS of Sustained Events by ICC: Annual Changes

Year-over-year changes in calculated TOS for 100 kV+ ac circuit events by ICC are reviewed next. **Figure B.9** shows changes in the average TOS for each ICC for the 2015–2016 dataset. The groups of ICC events are listed from left to right by descending average TOS for the two years combined. The largest average TOS over the data period was observed for sustained events initiated by Contamination.

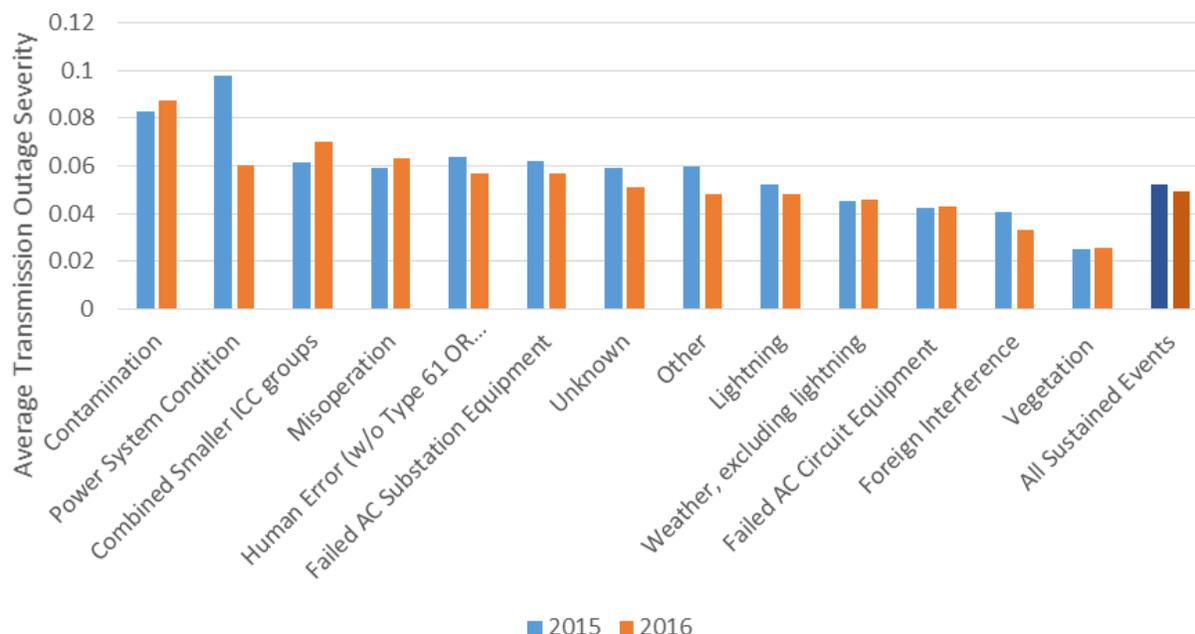


Figure B.9: Average of 100 kV+ AC Circuit Sustained Events by ICC and Year (2015–2016)

There were only three ICCs with statistically significant changes in the average TOS from 2015 to 2016: Power System Condition, Unknown, and Foreign Interference. All three were decreases. Overall, the average TOS of sustained events also statistically decreased from 2015 to 2016.

TOS Risk and Relative Risk of 100 kV+ AC Circuit Outage Events by ICC

The transmission risk and relative risk by ICC group were calculated, ranked, and are provided in Table B.13 with a breakdown of relative risk of sustained events by ICC.

Table B.13: Evaluation of 100 kV+ AC Circuit Sustained Event ICC Contribution to TOS (2015–2016)

Group of Sustained Events	Probability that an Event from a Group Starts During a Given Hour	Expected Impact (Expected TOS of an Event)	Risk Associated with a Group Per Hour	Relative Risk by Group
All Sustained Events	0.653	0.051	0.033	100%
Sustained with ICC Assigned	0.653	0.051	0.033	100%
Weather (excluding lightning)	0.115	0.046	0.005	16.0%
Unknown	0.085	0.055	0.005	14.3%
Failed AC Circuit Equipment	0.086	0.043	0.004	11.1%
Lightning	0.072	0.050	0.004	11.0%
Failed AC Substation Equipment	0.061	0.059	0.004	10.9%
Misoperation	0.044	0.062	0.003	8.1%
Human Error (w/o Type 61 OR Type 62)	0.034	0.060	0.002	6.2%
Foreign Interference	0.056	0.036	0.002	6.2%
Contamination	0.014	0.086	0.001	3.8%
Power System Condition	0.015	0.075	0.001	3.5%
Combined Smaller ICC Groups Study 4–5	0.016	0.066	0.001	3.2%
Other	0.019	0.054	0.001	3.1%
Vegetation	0.035	0.025	0.001	2.7%

Analysis of TADS sustained events indicates that the ICC Weather (excluding lightning) has the greatest relative risk from 2015 to 2016 followed by Unknown. Sustained events with ICCs Failed AC Circuit Equipment and Failed AC Substation Equipment are the two largest contributors to TOS with the exception of Unknown and weather-related events. The two ICCs with the highest expected severity, Contamination and Power System Condition, rank low in Table B.13 because of relatively rare occurrences of sustained events with these ICCs. On the other hand, AC Circuit Equipment failures initiate sustained events with lower than average expected transmission severity, but the relative risk of this ICC ranks third due to the high frequency of these outages.

Figure B.10 shows year-over-year changes in the relative risk of TADS events by ICC. The groups of ICC events are listed from left to right by descending relative risk for the most recent two years combined. The top contributor to transmission risk—Weather (excluding lightning)—had an increase in relative risk in 2016 due to an increase in the number (and the frequency) of sustained events as reflected in Table B.11. In contrast, ICC Unknown had a decrease from 16.5 percent in 2015 to 12.2 percent in 2016; this was due to both a drop in the number of Unknown events and a statistically significant decrease in the average TOS of an event.

The relative risk of Misoperation increased from 7.0 percent in 2015 to 9.3 percent in 2016; this was mostly due to an increase in the number of outage events initiated by Misoperation. Also, there was an increase in the relative risk for the ICCs Failed AC Circuit Equipment, and decreases for Lightning and Failed AC Substation Equipment.

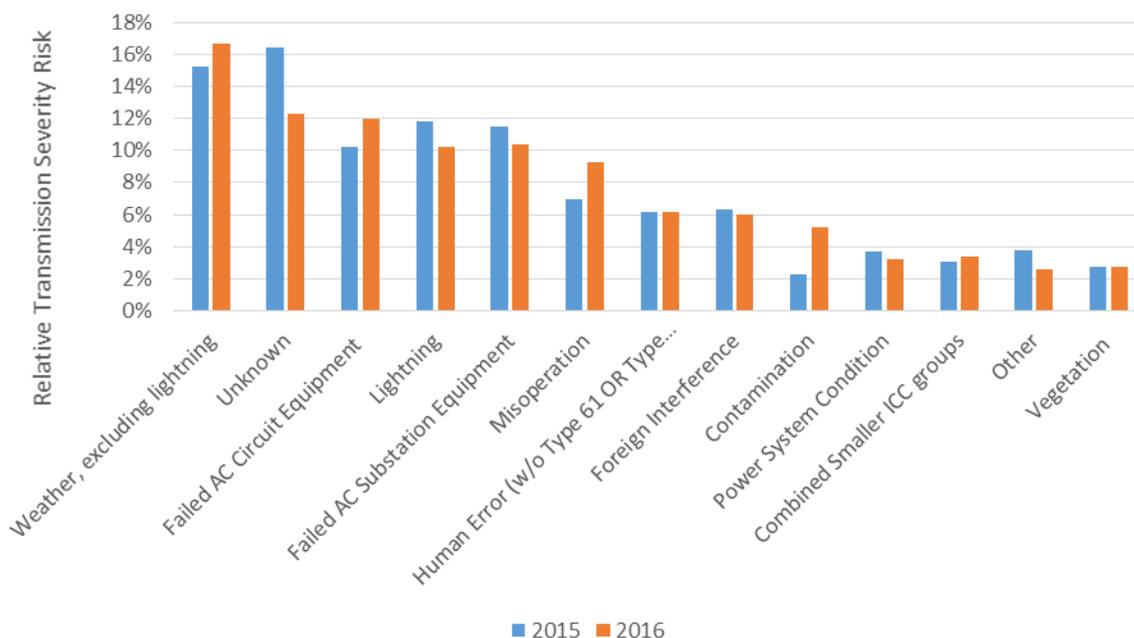


Figure B.10: Relative Risk 100 kV+ AC Circuit Sustained Events by ICC and Year (2015–2016)

Study 5: Sustained Events for 100 kV+ AC Circuits and Transformers (2016)

Sustained Events with Common ICC and Estimates of Event Probability

For the first time, NERC performs an ICC analysis for a combined set of ac circuit and transformer outage events. All 2016 sustained events involving these TADS elements of 100 kV and above are included in the study. The TOS of an event is calculated by applying [Equation B.2](#) and [Table B.1](#).

Table B.14 provides information on the number of sustained events in different ICC groups in 2016. Some ICC groups of sustained events do not have a population large enough for a reliable statistical comparison with other ICC groups. Similar to Study 4, the three smallest ICC groups (Fire; Environmental; and Vandalism, Terrorism, or Malicious Acts) were combined into a new group (Combined Smaller ICC groups Study 4–5). In Table B.14, the reciprocal of the probability per hour of 0.720 estimates that in the defined BES system, a sustained ac circuit or transformer event started, on average, every hour and 23 minutes.

Table B.14: Sustained Events 100 kV+ AC Circuits and Transformers and Hourly Event Probability by ICC (2016)		
Initiating Cause Code	2016	Sustained Event Initiation Probability/Hour
Weather (excluding lightning)	1090	0.124
Failed AC Circuit Equipment	841	0.096
Unknown	741	0.084
Lightning	647	0.074
Failed AC Substation Equipment	618	0.070
Foreign Interference	555	0.063
Misoperation	480	0.055
Human Error (w/o Type 61 or Type 62)	343	0.039
Vegetation	318	0.036
Contamination	178	0.020
Other	164	0.019
Power System Condition	159	0.018
Combined Smaller ICC Groups Study 4-5	151	0.017
<i>Fire</i>	<i>128</i>	0.015
<i>Vandalism, Terrorism, or Malicious Acts</i>	<i>13</i>	0.001
<i>Environmental</i>	<i>10</i>	0.001
Sustained with ICC Assigned	6285	0.716
Sustained Events	6332	0.721

Comparison of the information in Table B.14 and the 2016 column in [Table B.11](#), which lists the counts of sustained events for 100 kV+ ac circuits, leads to several conclusions. First, the majority of sustained events in Study 5 involves ac circuits (6,058 out of 6,332 events). Second, the ICC ranking with respect to the number of events did not change after addition of the transformer events. These results are not surprising because TADS ac circuit inventory and outage counts are much larger than those for transformers.

Table B.14: Sustained Events 100 kV+ AC Circuits and Transformers and Hourly Event Probability by ICC (2016)		
Initiating Cause Code	2016	Sustained Event Initiation Probability/Hour
Weather (excluding lightning)	1,090	0.124
Failed AC Circuit Equipment	841	0.096
Unknown	741	0.084
Lightning	647	0.074
Failed AC Substation Equipment	618	0.070
Foreign Interference	555	0.063
Misoperation	480	0.055
Human Error (w/o Type 61 or Type 62)	343	0.039
Vegetation	318	0.036
Contamination	178	0.020
Other	164	0.019
Power System Condition	159	0.018
Combined Smaller ICC groups Study 4–5	151	0.017
<i>Fire</i>	<i>128</i>	0.015
<i>Vandalism, Terrorism, or Malicious Acts</i>	<i>13</i>	0.001
<i>Environmental</i>	<i>10</i>	0.001
Sustained with ICC Assigned	6,285	0.716
Sustained Events	6,332	0.721

Correlation Analysis and Distribution of TOS of Sustained AC Circuit and Transformer Events by ICC

Figure B.11 shows the correlations between calculated TOS and the given ICC. A red bar corresponds to an ICC with statistically significant positive correlation with TOS, a green bar corresponds to an ICC with statistically significant negative correlation, and a blue bar indicates no significant correlation.

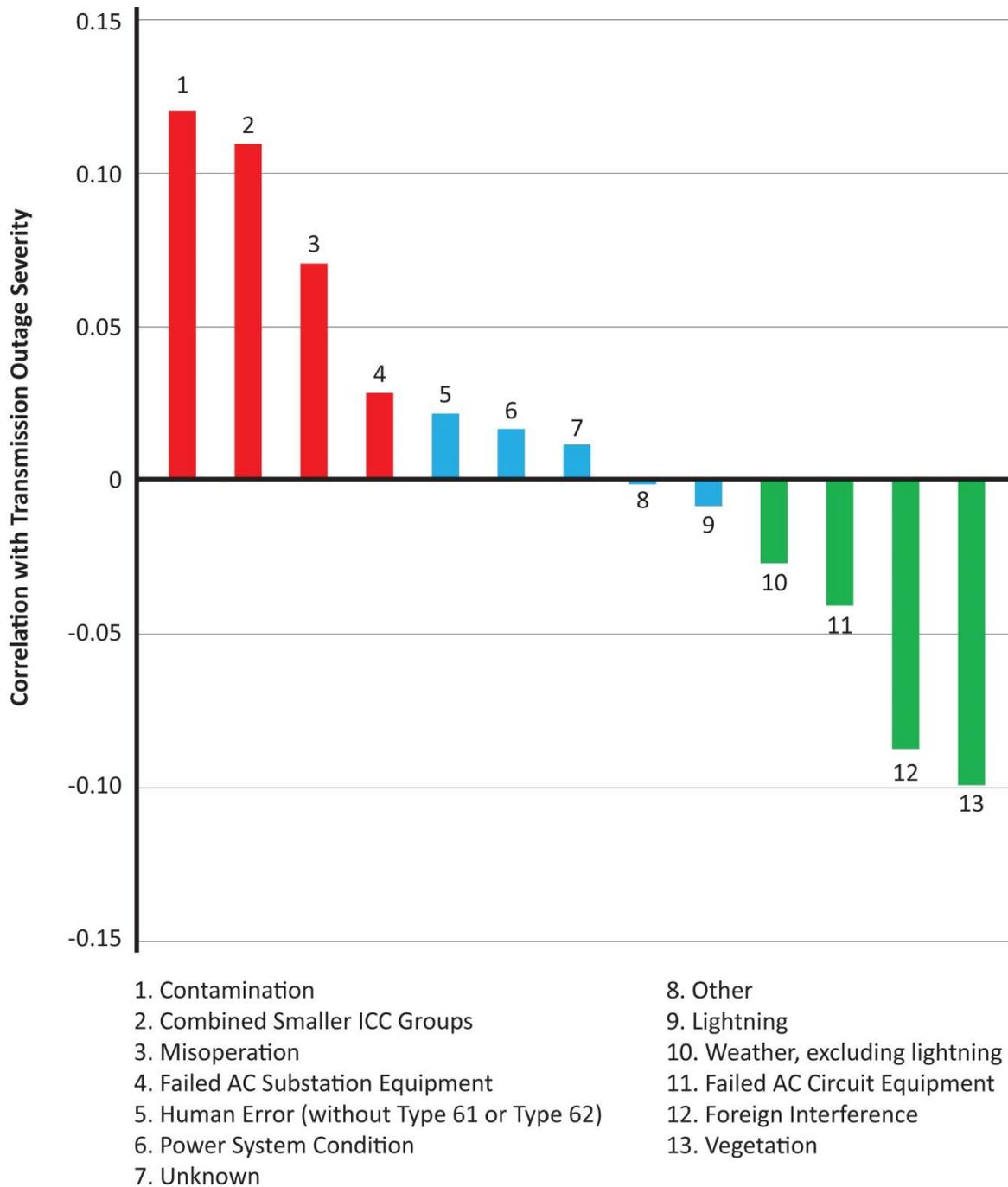


Figure B.11: Correlation between ICC and TOS of Sustained Events of 100 kV+ AC Circuits and Transformers (2016)

The ICC Power System Condition for the mixed inventory does not have a significant correlation with the transmission severity, unlike results for ac circuit events only. This is shown in [Figure B.3](#) and [Figure B.8](#).

The distribution of TOS was studied separately for events with a given ICC and the complete dataset of sustained events. The TOS of the 2016 TADS sustained events 100 kV+ ac circuit and transformer data set has a sample mean of 0.042 and a sample standard deviation of 0.047. The sample statistics for TOS are listed in Table B.15 with the ICCs ordered from the largest average TOS to the smallest. The addition of transformers to Study 4 leads to an

overall decrease in the TOS of the events, reflecting differences in equivalent MVA's for ac circuits and transformers when compared to [Table B.1](#).

Table B.15: Distribution of TOS of Sustained Events of 100 kV+ AC Circuits and Transformers by ICC (2016)

Index No.	Initiating Cause Code (ICC)	Average TOS	Is Expected TOS Statistically Significantly Different than for Other Sustained Events?	ICC with Statistically Significantly Smaller Average TOS	Stand Deviation of TOS
1	Contamination	0.074	Larger	3,4,5,6,7,8,9,10,11,12,13	0.054
2	Combined Smaller ICC Groups	0.073	Larger	3,4,5,6,7,8,9,10,11,12,13	0.084
3	Misoperation	0.053	Larger	5,6,7,8,9,10,11,12,13	0.056
4	Power System Condition	0.046	No	11,12,13	0.048
5	Human Error (w/o Type 61 or Type 62)	0.045	No	10,11,12,13	0.042
6	Failed AC Substation Equipment	0.045	No	9,10,11,12,13	0.053
7	Unknown	0.043	No	11,12,13	0.042
	All Sustained Events	0.042	N/A	N/A	0.047
	Sustained with ICC Assigned	0.041	N/A	N/A	0.046
8	Other	0.041	No	12,13	0.037
9	Lightning	0.040	No	12,13	0.044
10	Weather (excluding lightning)	0.039	Smaller	12,13	0.042
11	Failed AC Circuit Equipment	0.037	Smaller	12,13	0.042
12	Foreign Interference	0.028	Smaller	13	0.027
13	Vegetation	0.021	Smaller	none	0.025

Statistical tests found that the groups of events initiated by Contamination, Combined Smaller ICC groups, and Misoperation have statistically¹⁰⁷ greater expected outage severity than other events. This means that when an event initiated by one of these causes occurs, it has a greater impact and a higher risk to the transmission system on average. Moreover, the tests on the homogeneity of variances highlights statistically greater variances (and the standard deviations) for the top six ICC groups as compared with other events. The greater variance is an additional risk factor since it implies more frequent occurrences of events with high TOS. The Combined Smaller ICC groups Studies 4–5 have a higher average TOS due to events initiated by Fire and Environmental, which both have the mean outage severity of 0.077.

Table B.15 also provides a column that lists ICCs with TOS statistically smaller than for a given ICC referenced by the table's initial column index. For example, Contamination initiates events with statistically larger TOS than any

¹⁰⁷ At significance level 0.05

other ICC except Combined Smaller ICC groups (indices 3-13 in Table B.15). Therefore, an expected impact of events initiated by Contamination and Combined Smaller ICC groups is statistically similar.

TOS Risk and Relative Risk of 100 kV+ AC Circuit and Transformer Events by ICC

The transmission risk and relative risk by ICC group were calculated, ranked, and are provided in Table B.16 with a breakdown of relative risk of sustained events by ICC.

Group of Sustained Events	Probability that an Event from a Group Starts During a Given Hour	Expected Impact (Expected TOS of an Event)	Risk Associated with a Group Per Hour	Relative Risk by Group
All Sustained Events	0.721	0.042	0.030	100%
Sustained with ICC Assigned	0.721	0.041	0.030	97.8%
Weather (excluding lightning)	0.039	0.124	0.005	15.8%
Unknown	0.043	0.084	0.004	11.9%
Failed AC Circuit Equipment	0.037	0.096	0.003	11.6%
Failed AC Substation Equipment	0.045	0.070	0.003	10.5%
Lightning	0.040	0.074	0.003	9.8%
Misoperation	0.053	0.055	0.003	9.5%
Foreign Interference	0.028	0.063	0.002	5.9%
Human Error (w/o Type 61 or Type 62)	0.045	0.039	0.002	5.9%
Contamination	0.074	0.020	0.001	4.9%
Combined Smaller ICC Groups	0.073	0.017	0.001	4.2%
Power System Condition	0.046	0.018	0.001	2.8%
Vegetation	0.021	0.036	0.001	2.6%
Other	0.041	0.019	0.001	2.5%

Analysis of TADS sustained events indicate that the ICC Weather (excluding lightning) had the greatest relative risk in 2016, following by Unknown. Sustained events with ICCs Failed AC Circuit Equipment and Failed AC Substation Equipment are the two largest contributors to TOS with the exception of Unknown and weather-related events. The two ICCs with the highest expected severity, Contamination and Combined Smaller ICC groups, rank low in Table B.16 because of relatively rare occurrences of sustained events with these ICCs. However, AC Circuit Equipment failures initiate sustained events with lower than average expected transmission severity, but due to high frequency of these outages, the relative risk of this ICC ranks third.

Overall, the ICC rankings by contribution to the total transmission severity shown in [Table B.13](#) (sustained ac circuit events), and [Table B.15](#) (sustained events of ac circuits and transformers) are very similar. As noted above, the addition of TADS transformer outage events and inventory data to Study 4 does not change most results and conclusions of the analysis.

Study 6: Sustained Cause Code Study for Sustained Outages of 100 kV+ AC Circuits (2015–2016)

Beside an ICC, a sustained cause code (SCC) is assigned to a sustained outage. The SCC describes the cause that contributed to the longest duration of the outage. The list of TADS SCCs is the same as the list of ICCs as shown in [Table B.4](#). A method of assigning a single SCC to a TADS event with multiple outages having different SCCs has not yet been developed; therefore, it is not yet possible to analyze SCCs by applying the same methodology as described in Studies 1–5 for ICCs.

In this study, the 2015–2016 sustained outages of the 100 kV+ ac circuits with a TOS calculated by [Equation B.1](#) are investigated by SCC. TADS outages, unlike TADS events, can be dependent; thus, they do not represent a statistical sample with independent observations. Therefore, the risk analysis for outages is limited to the TOS calculation, numerical comparison of the TOS of SCC groups, and their ranking. However, there is another important variable reported for sustained outages—the outage duration. Provided in [Table B.17](#) are some statistics on the outage duration by SCC and suggested a way to incorporate duration into analysis of the relative risk by SCC.

[Table B.17](#) lists the number of outages, the average, the median, and the maximum outage duration by SCC and overall for the 2015–2016 sustained outages of the 100 kV+ ac circuits. SCCs are listed in decreasing order by number of outages.

Sustained Cause Code	Number of Outages	Average Outage Duration (Hours)	Median Outage Duration (Hours)	Maximum Duration (Days)
Failed AC Circuit Equipment	2,441	54.0	12.23	366.0
Failed AC Substation Equipment	1,611	39.4	3.05	264.4
Weather (excluding lightning)	1,435	16.8	1.32	107.8
Unknown	1,377	7.4	0.17	83.4
Other	1,314	8.4	0.27	95.1
Misoperation	1,146	8.7	0.85	34.5
Foreign Interference	959	9.7	2.13	25.6
Lightning	815	3.7	0.12	37.6
Vegetation	732	32.7	0.25	57.9
Human Error	732	4.6	10.96	40.1
Power System Condition	581	21.6	0.48	111.9
Contamination	223	7.8	0.33	5.6
Fire	186	34.9	4.25	52.9
Environmental	53	39.6	8.77	24.2
Vandalism, Terrorism, or Malicious Acts	15	11.1	7.18	1.0
All Sustained Outages	13,620	23.0	1.90	366.0

The SCC order differs from that seen for ICC groups in studies 1, 2, and 4 ([Tables B.4](#), [B.8](#), [B.11](#) and [B.14](#)). Outages with SCC Failed AC Circuit Equipment not only comprise the largest group, but they have also, on average, the longest duration. Another observation is that SCC Unknown, being the fourth biggest group, has the third shortest average outage duration (7.4 hours versus 23.0 hours for all sustained events).

The TOS of each outage is calculated by [Equation B.1](#), then the total TOS of each SCC group is calculated, and the relative risk of a SCC is determined based on contribution of the group to the total TOS of all 2015–2016 sustained outages. The analysis is repeated for the TOS weighted with an outage duration with the purpose to take into account the outage duration and incorporate it as a factor that impacts transmission outage risk. The results of these two analyses of the relative SCC risk are compared to illustrate how outage duration affects the SCC ranking.

Since there are outages with very large durations (up to 366 days), two types of sensitivity analysis are performed to the evaluation of transmission severity weighted with outage duration: First, the SCC analysis is repeated for all outages not longer than one month (with the 78 outages or about 0.6 percent of the total dataset removed); second, the analysis is rerun with the top percent of longest outages removed (132 outages longer than 14.4 days removed).

Figure B.12 summarizes results of the four analyses of the relative transmission outage risk by SCC. The SCCs with relative transmission outage risks rounded to zero percent. Environmental and Vandalism, Terrorism, and Malicious Acts, the two SCC groups with less than 1 percent of the relative transmission outage risk each, are not shown.

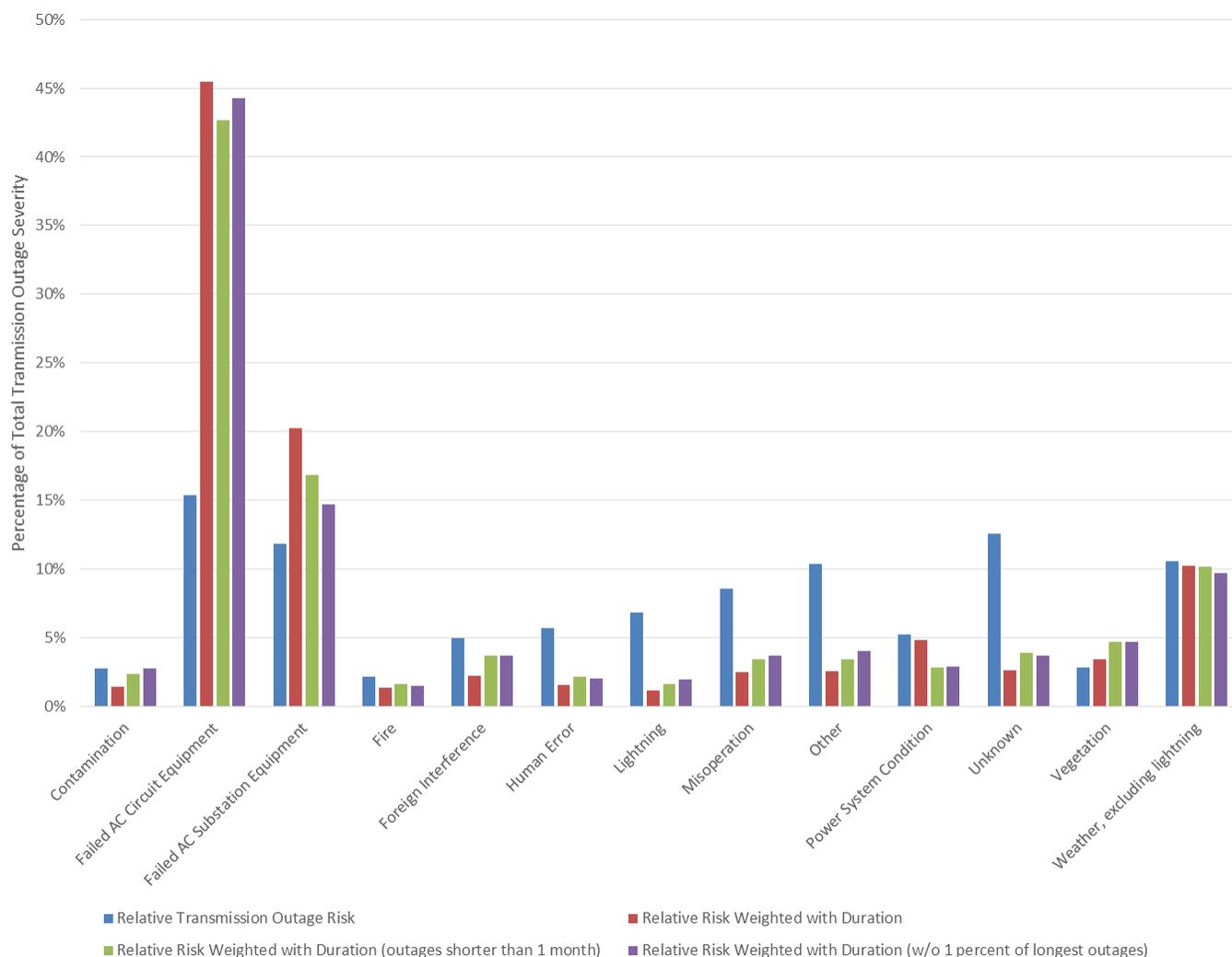


Figure B.12: Relative TOS Risk by SCC for Sustained Outages of the 100 kV+ AC Circuits (2015–2016)

Figure B.12 shows the SCC relative transmission outage risk and the SCC relative transmission outage risk weighted with duration. The largest differences are observed for the SCCs with “nontypical” average outage durations (i.e., the average outage duration significantly different from the average duration of 23 hours).

Events with SCC Failed AC Circuit Equipment have the highest average duration. The relative transmission outage risk of this SCC increases from 15 percent to 45 percent. For SCCs with shorter average durations such as Unknown, Other, Lightning, Misoperation, Human Error, and Foreign Interference, the relative transmission outage risks are noticeably lower when weighted with outage duration (e.g., for SCC Unknown from 13 percent to three percent of the total transmission severity and for SCC Misoperation from nine percent to two percent).

Comparison of the three right-hand side bars for each SCC allows us to draw some observations on sensitivity analyses and evaluate effect of the longest outages on the SCC relative risk. Overall, an SCC relative risk does not change much among these three types; this fact confirms that the SCC relative transmission outage risk weighted with duration calculations are robust with respect to duration outliers.

Table B.18 shows the SCC rankings by relative transmission outage risk (unweighted and weighted with outage duration).

Table B.18: SCC Ranking for TADS Sustained Outages 100 kV+ AC Circuits (2015–2016)		
Sustained Cause Code	By Relative Transmission Outage Risk	By Relative Transmission Outage Risk Weighted with Outage Duration
Contamination	12	11
Environmental	14	14
Failed AC Circuit Equipment	1	1
Failed AC Substation Equipment	3	2
Fire	13	12
Foreign Interference	10	9
Human Error	8	10
Lightning	7	13
Misoperation	6	8
Other	5	7
Power System Condition	9	4
Unknown	2	6
Vandalism, Terrorism, or Malicious Acts	15	15
Vegetation	11	5
Weather (excluding lightning)	4	3

For several SCCs, there are significant differences between their respective ranks. As the result of Study 6, both rankings are derived and presented without making a decision about superiority of either method of the relative transmission outage risk evaluation. Each method has its advantages and disadvantages: the transmission outage risk that is based on TOS calculations without duration is simpler and allows for the analysis of all outages and events (which is more important) of both momentary and sustained. The transmission outage risk, based on the TOS weighted with outage duration discards momentary outages from the analysis, and while it does take into account differences in sustained outage duration, more analysis and the industry expert discussions are needed to decide whether the weighing is fair. For example, as a result of this weighting, an one-hour ac circuit outage from the 300–399 kV voltage class contributes to the total weighted transmission severity equally with an outage of the 100–199 kV ac circuit with duration of six hours and 30 minutes; with an outage of the 200-299 kV ac circuit with duration of one hours and 51 minutes; with an outage of the 400-599 kV ac circuit with duration of 39 minutes; and with an outage of the 600–799 kV ac circuit with duration of 26 minutes).

Summary of TADS Data Analysis

The statistical analysis of the 2012–2016 TADS data on the TOS, initiating and sustained causes of TADS outage events, yields the following observations:

- **Weather (excluding lightning)** was a top contributor to TOS of the 2016 sustained events for ac circuits and transformers (Study 5). From 2015 to 2016, the number of the weather-initiated momentary and sustained events of 200 kV+ ac circuits increased by 28 percent (Study 1) and the number of weather-initiated sustained events of 100 kV+ ac circuits increased by 15 percent (Study 4) while the respective TADS inventory increases were below 0.6 percent. Additionally, Weather (excluding lightning) ranks 3rd among sustained causes of ac circuit outages (Study 6).

- **Unknown** initiated fewer TADS events in 2016 compared with 2015: the number of Unknown momentary and sustained events of 200 kV+ ac circuits and the number of Unknown sustained events of 100 kV+ ac circuits both reduced (Studies 1 and 4, respectively). Moreover, from 2015 to 2016, the average transmission severity of sustained events with ICC Unknown statistically significantly reduced while the relative transmission outage risk of this ICC decreased from 16.5 percent to 12.2 percent.
- The number of combined momentary and sustained events of 200 kV+ ac circuits and sustained events of 100 kV+ circuits initiated by **Misoperation** increased in 2016 (Study 1 and Study 4, respectively). Relative risk of the ICC Misoperation also increased for these two datasets (studies 1 and 4). For 2012–2016 events with multiple outages (CDM events), Misoperation is a biggest group and the top contributor to the TOS (Study 2).
- The number of TADS events initiated by **Failed AC Circuit Equipment** increased significantly in 2016: by 43 percent for combined momentary and sustained events of 200 kV+ ac circuits (Study 1) and by 23 percent for sustained events of 100 kV+ ac circuits (Study 4). Events with this ICC on average have a smaller TOS, but because of their high frequency of occurrence they rank as the 3rd contributor of the TOS of sustained events of ac circuits (Study 4). Sustained outages with sustained cause code Failed AC Circuit Equipment are the largest group of ac circuit sustained outages; moreover, they have, on average, the longest duration among all sustained outages (Study 6).
- The number of combined momentary and sustained events of 200 kV+ ac circuits and the number of sustained events of 100 kV+ ac circuits both increased from 2015 to 2016, but the average TOS of an event statistically significantly decreased for both datasets (Studies 1 and 4).
- The addition of TADS transformer outages and inventory to the data for sustained events of 100 kV+ ac circuits did not significantly increase the number of events and did not lead to big changes in ranking of ICCs by size and by relative risk and other results of the analysis (Study 4 and Study 5).

Appendix C: Analysis of Generation Data

GADS, beginning in 2013, collects for conventional generating units that are 20 MW. In addition, smaller units and other units outside of NERC’s jurisdiction report into GADS on a voluntary basis. The analysis for this report includes only active units with a mandatory reporting obligation.¹⁰⁸ Data used in the analysis includes information reported into GADS through the end of 2016.

GADS does not include wind, solar, other renewable technology generating assets, distributed energy resources, or other small energy sources. Wind performance data reporting requirements have been developed, and a phased-in reporting process begins in 2017 and continues through 2020. Reporting data requirements for solar have been initiated with a target goal of data submittal by 2021.

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. **Table C.1** shows the number of units and average age characteristics of the population in GADS and select unit types for each year.

Metric/year	2012	2013	2014	2015	2016
Number of Reporting Units	4,486	6,121	6,125	6,083	5,961
Average Age of the Fleet (years)	34	36	36	35	35
Average Age of Coal Units (years)	47	46	46	45	43
Average Age of Gas Units (years)	23	24	24	23	23
Average Age of Nuclear Units (years)	38	38	38	38	37

The age of the generating fleet is considered to be a particularly relevant statistic derived from GADS because an aging fleet could potentially see increasing outages. However, with proper maintenance and equipment replacement, older units may perform comparably to newer units. In addition, the weighted equivalent forced outage rate, reported later in this section, shows declining rates of forced outages. **Table C.1** also provides some validation of the retirements of older coal units, which is reflected in the decline in average age of coal units between 2015 and 2016. Future reports will continue to monitor this to help illustrate how the fleet is changing.

Figure C.1 uses GADS data to plot fleet capacity by age and fuel type. **Figure C.1** shows two characteristics of the fleet reported to GADS: 1) an age bubble exists around 37–46 years, by a population consisting of coal and some gas units; and 2) a significant age bubble around 12–20 years is comprised almost exclusively of gas units. The data shows a clear shift toward gas-fired unit additions, and the overall age of the fleet across North America is almost 10 years younger than the age of the coal-fired base-load plants that have been the backbone of power supply for many years. This trend is projected to continue given current forecasts around price and availability of natural gas as a power generation fuel as well as regulatory impetus.

¹⁰⁸ In 2015, fewer than 100 MW of units had a voluntary reporting status in GADS.

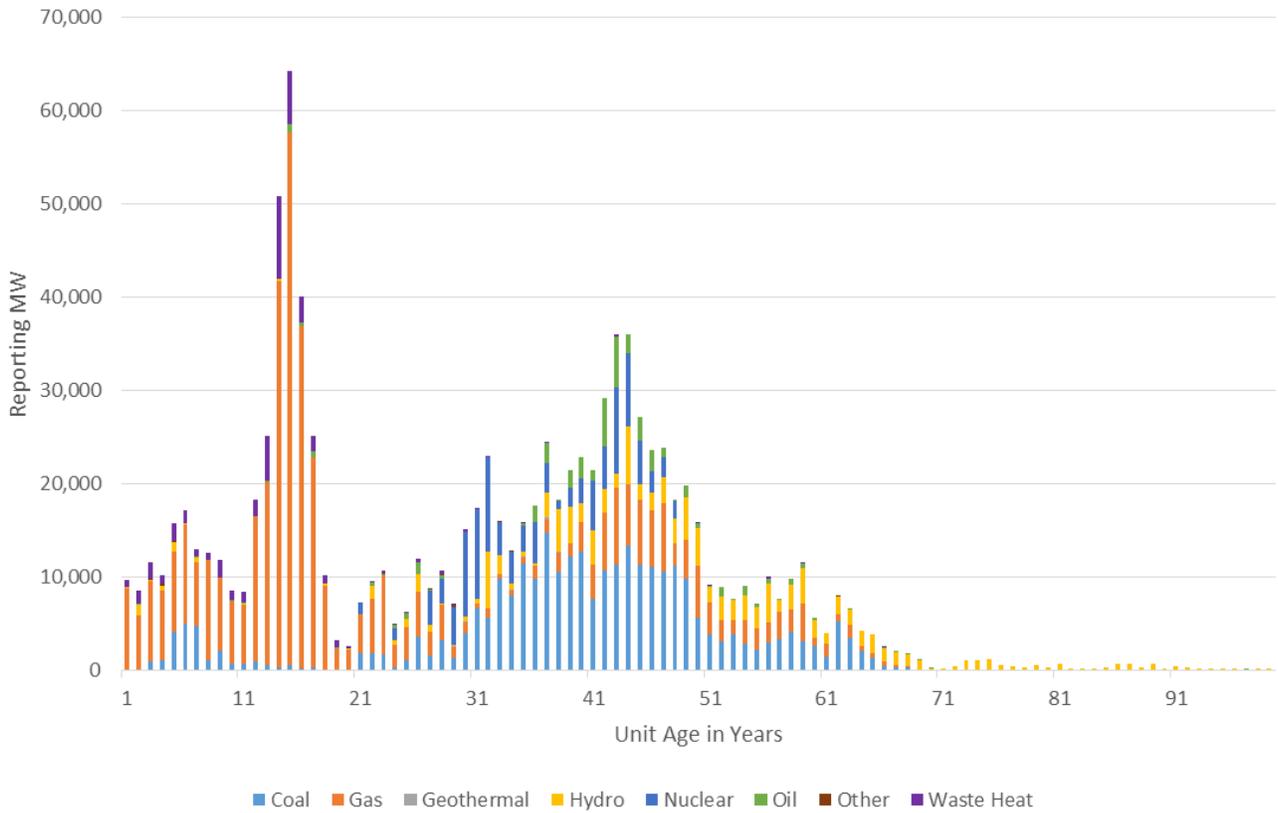


Figure C.1: Fleet Capacity by Age and Fuel Type as of January 1, 2017

Generator Fleet Reliability

GADS contains information that can be used to compute several reliability measures such as WEFOR. WEFOR is a metric measuring the probability that a unit will not be available to deliver its full capacity at any given time, taking into consideration forced outages and derates.

Figure C.2 presents the monthly megawatt-weighted EFOR¹⁰⁹ across the NERC footprint for the five-year period of 2012–2016.¹¹⁰ The horizontal steps show the annual EFOR compared to the monthly EFOR; the solid horizontal bar in Figure C.2 show the mean outage rate over each year. The mean outage rate over the analysis period is 7.1 percent. The EFOR has been fairly consistent with a near-exact standard distribution.

¹⁰⁹ The use of the weighted EFOR (weighted by the Net Maximum Capacity- NMC as reported in GADS Performance data) allows for comparison of units that vary by size.

¹¹⁰ The reporting year covers January 1 through December 31.

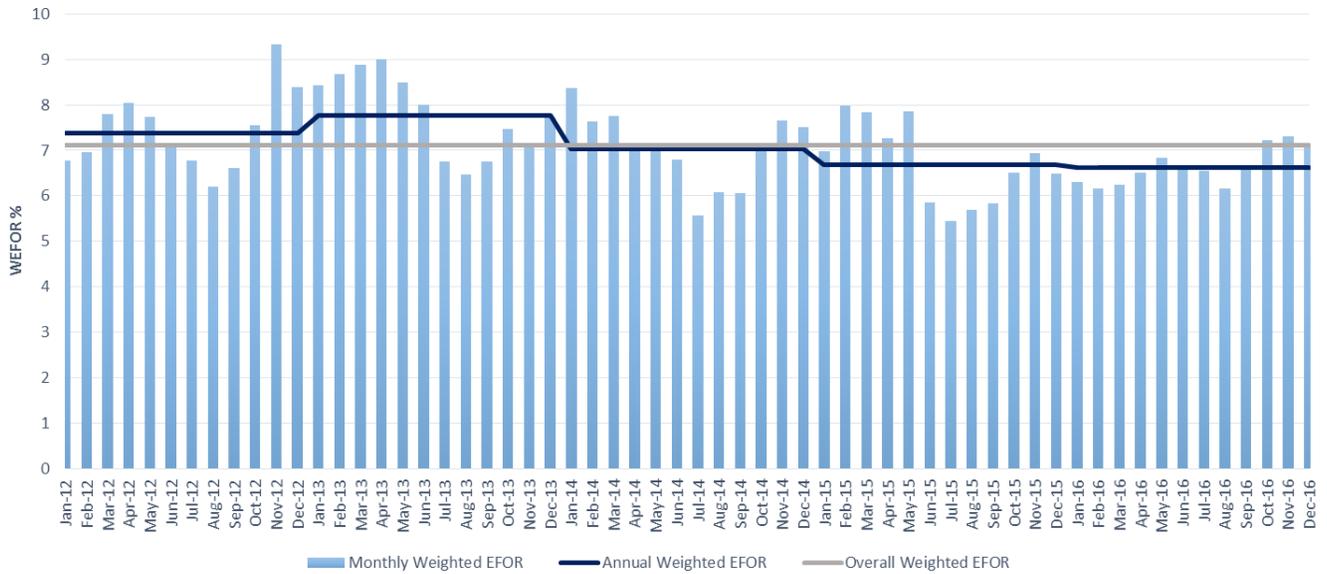


Figure C.2: Monthly MW Capacity-Weighted EFOR 2012–2016

Forced Outage Causes

To better understand the causes of forced outages of generators, the annual and top 10 forced outage causes for the summer and winter seasons¹¹¹ were analyzed for the period of 2012–2016. This analysis is focused on forced outage causes measured in terms of net MWh of potential production lost, so both the amount of capacity affected and the duration of the outages are captured.

The levels of forced outages reported into the GADS database are presented in [Figure C.3](#) and [Table C.2](#), providing detail on the net MWh of potential production lost due to forced outages for the period 2012–2016 by calendar year.

¹¹¹ Winter includes the months of January, February and December. When analysis is performed on a calendar year basis, as for this report, these three months are included from the same calendar year. Summer includes May through September; all other months are categorized as Spring/Fall.

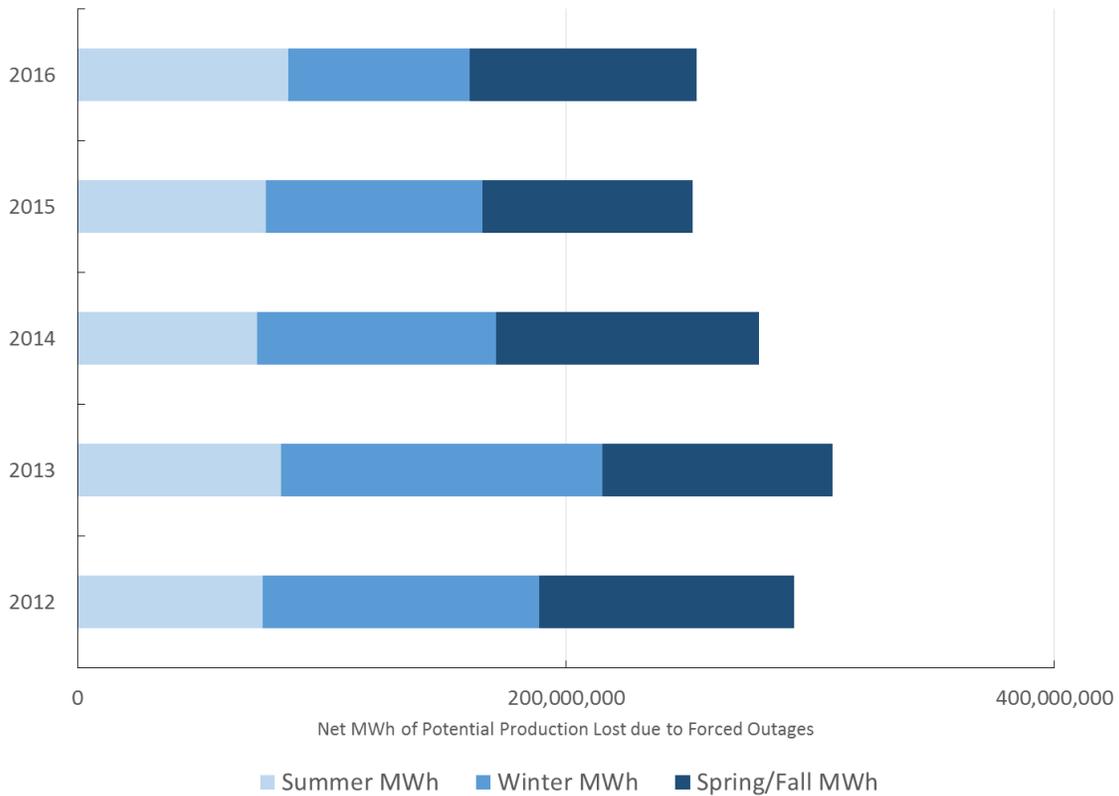


Figure C.3: Total Net MWh of Potential Production Lost Due to Forced Outages 2012–2016

Table C.2: Total Net MWh of Potential Production Lost Due to Forced Outages, by Calendar Year 2012–2016				
NERC	Total Annual MWh	Summer MWh	Winter MWh	Spring/Fall MWh
2012	293,475,653	75,914,722	112,989,119	104,571,812
2013	309,011,065	83,422,362	131,422,688	94,166,015
2014	278,987,876	73,610,732	97,782,322	107,594,822
2015	251,795,168	76,955,351	88,651,639	86,188,178
2016	253,530,864	86,112,430	74,256,269	93,162,171

Based on the five years of available data since GADS reporting became mandatory, the following observations can be made:

- Severe storms in the last quarter of 2012, such as Hurricane Sandy, resulted in an increase in the net MWh of potential production lost due to forced outages reported for Winter 2013.¹¹²
- The shoulder months of Spring/Fall in 2014 and 2016 have higher forced outage net MWh than the corresponding summer or winter periods.

Further analysis into the causes of forced outages considered the impact of weather. The percentage of net MWh of potential production lost due to weather-related forced outage cause codes reported each year ranges from two percent to four percent annually. This indicates that while weather does cause major headlines and affects

¹¹² For this analysis, the season of a forced outage is associated with the season in which the start date of the event was reported in that year; when an event continues into the next year, a new event record is created in January. This results in the event being categorized as occurring in the winter for the continuation event.

the days included in the SRI, the overall effect of weather on the fleet is minimal. The real impacts of weather-related events are localized impacts and of relatively short duration.

To gain additional insight into the drivers for the reported net MWh of potential production lost due to forced outages, the top 10 forced outage causes were examined to determine their impact on the annual total of net MWh of potential production lost. The number of events reported in the top 10 forced outage causes represent between seven percent and 12 percent of all forced outage events reported annually while contributing an average of 28 percent to the annual total megawatt hours lost. **Table C.3** shows the contribution of the top 10 forced outage causes to net MWh of potential production lost on a NERC-wide basis over the period 2012–2016.

Table C.3: Percentage of Top 10 Forced Outage Cause MWh by Year to Annual Net MWh of Potential Production Lost Due to Forced Outages by Calendar Year 2012-2016				
NERC	Total Annual MWh	Summer MWh	Winter MWh	Spring/Fall MWh
2012	29%	5%	13%	11%
2013	29%	7%	13%	9%
2014	28%	6%	11%	11%
2015	24%	7%	9%	8%
2016	28%	8%	9%	11%

The top 10 causes vary annually, and the contribution from each of the top 10 causes to the total megawatt hours lost varies as well. **Table C.4** lists the top 10 forced outage causes on an annual basis in order of the most impactful cause to the least, based on annual net MWh of potential production lost due to forced outages.

Table C.4: Top 10 Cause Codes as Percentage of Annual Net MWh of Potential Production Lost Due to Forced Outages					
Rank	2012	2013	2014	2015	2016
1	Waterwall (furnace wall) 5.2%	Waterwall (furnace wall) 5.9%	Waterwall (furnace wall) 7.7%	Waterwall (furnace wall) 6.4%	Waterwall (furnace wall) 6.9%
2	Rotor – General 3.3%	Main Transformer 4.1%	Lack of Fuel (Interruptible Supply of Fuel) 3.7%	Main Transformer 5.7%	Main Transformer 4.7%
3	Steam Generator Tube Leaks 3.2%	Rotor – General 3.2%	Main Transformer 3.2%	First Reheater 2.3%	Stator Windings, Bushings, and Terminals 2.8%
4	Main Transformer 2.8%	Second Superheater 2.9%	Second Superheater 2.7%	Lack of Fuel (interruptible supply of fuel) 1.8%	Other Exciter Problems 2.5%
5	Transmission System Problems other than Catastrophes 2.8%	Operator Error 2.8%	First Reheater 2.5%	Second Superheater 1.5%	Flood 2.1%
6	Steam Generator Tube Inspections 2.8%	Stator Windings, Bushings, and Terminals 2.3%	Emergency Generator Trip Devices 1.8%	Boiler – Miscellaneous 1.5%	First Reheater 1.9%

Table C.4: Top 10 Cause Codes as Percentage of Annual Net MWh of Potential Production Lost Due to Forced Outages

Rank	2012	2013	2014	2015	2016
7	Containment Structure 2.6%	Stator – General 2.1%	AC Conductors and Buses 1.7%	Generator Vibration 1.5%	Second Superheater 1.7%
8	Stator Windings, Bushings, and Terminals 2.1%	Hurricane 2.0%	Other Low Pressure Turbine Problems 1.7%	First Superheater 1.5%	Other Miscellaneous Generator Problems 1.7%
9	Second Superheater 2.1%	Rotor Windings 2.0%	First Superheater 1.6%	Other Boiler Tube Leaks 1.5%	Residual Heat Removal/Decay Heat Removal System 1.5%
10	Generator Output Breaker 1.8%	First Reheater 1.7%	Boiler – Miscellaneous 1.5%	Other Exciter Problems 1.4%	Other Boiler Tube Leaks 1.5%

Several outage causes appear in the top 10 more often than others: Weather-related outages in 2012 due to Hurricane Sandy resulted in flooding which impacted several units that continued to report forced outages into 2013 and 2014. Lack of Fuel occurs within the top causes in 2014 and 2015. [Table C.5](#) lists the recurring cause codes and number of years that the cause code appears in the top 10.

Table C.5: Recurring Top-10 Cause Codes

Code	Description	Number of Years in Top 10 Causes
1050	Second Superheater	5
1000	Waterwall (furnace wall)	5
3620	Main Transformer	5
1060	First Reheater	4
4520	Stator Windings, Bushings, and Terminals	3
9131	Lack of Fuel (interruptible supply of fuel)	2
1090	Other Boiler Tube Leaks	2
1999	Boiler – Miscellaneous	2
1040	First Superheater	2
4511	Rotor – General	2
4609	Other Excited Problems	2

The First Superheater (cause code 1040), Second Superheater (1050), Waterwall (1000), and First Reheater (1060) are all related to tube leaks in the respective systems. Given the amount of steam generating units that make up the fleet, the magnitude of these outages would not be unusual. These are not uncommon failures that occur in normal operation.

Both the Main Transformer (3620) and Stator Windings (4520) are high on the list. These items are the result of a very low likelihood event occurring that has a high impact. Most plants do not have spares available for these assets because the likelihood of failure is very low. However, if an event does occur, it can take several months to remedy, causing the event to show very high on this cause code list.

Recommendations:

- NERC, through the GADSWG, should consider requiring design data from the units to help improve analytics on the generating fleet and its possible impacts to BES reliability.
- NERC, through the GADSWG, should continue to investigate seasonal performance trends for all types of reported generation. As the generation fleet continues to shift toward gas-fired units, and the overall age of the fleet reduces, new emerging trends must be examined to identify common outage concerns across fuel types.
- NERC, through the GADSWG, should trend forced outage rates to determine if there are immediate concerns with newly installed generation.
- NERC, through the GADSWG, should examine outage cause codes for specific equipment types (e.g., generator, boiler, turbine, etc.)

Appendix D: Analysis of Demand Response Data

Overview

In 2016, the DADSWG continued efforts to improve data collection, reporting through outreach, and developing of training materials. The outreach efforts developed a process for annual attestation of BAs and Distribution Providers (DPs) to declare whether they meet the criteria for reporting into DADS. The outreach efforts resulted in a nominal increase in the number of entities reporting into DADS, indicating that the population that has been reporting into DADS is representative of the demand response programs in operation. Future DADSWG efforts are focused on improving data collection, updating existing materials and developing additional guidance documents, maintaining data quality, and providing observations of possible demand response contributions to reliability.

Demand Response Programs

Demand Response Registered Program data provides important information about the individual programs that include product and service type, relationships to other entities and programs, and monthly registered capacities. DADS data is reported semiannually as summer and winter seasons with the summer season representing program data from April 1 through September 30 and the winter season representing program data from October 1 to March 31 of the following year. This report includes data reported through September 2016.

BAs and DPs that administer demand response programs that have been commercially in service for at least 12 months with 10 MW or more of enrolled capability are required to report into DADS. In accordance with two 2015 FERC orders¹¹³, reporting by Purchasing-Scheduling Entities and Load-Serving Entities was discontinued.

Registered Capacity

Figure D.1 represents the registered capacity MW for all demand response registered programs in NERC; registered capacity for summer is based on August of each year, and winter is based on January of each year. The total registered capacity in summer has increased slightly since 2013 but remained relatively flat from 2015. However, the winter capacity experienced a 12.7 percent increase from 2015. This increase is due to changes in program rules and implementation of new programs. The increase also reflects a continued increase in development of capacity-based demand response programs since 2013.

It is important to note that the demand response registered capacity is considered fungible (resources and associated capacities are interchangeable). For example, an entity's reported demand response program may be an aggregation of individual resources and each year the individual resources could be from different sources and programs.

¹¹³ Orders RR15-4-000: http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order_RBR_ROP_20150319_RR15-4.pdf and RR-15-4-001: http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order_RBR_ROP_10152015_RR15-4.pdf

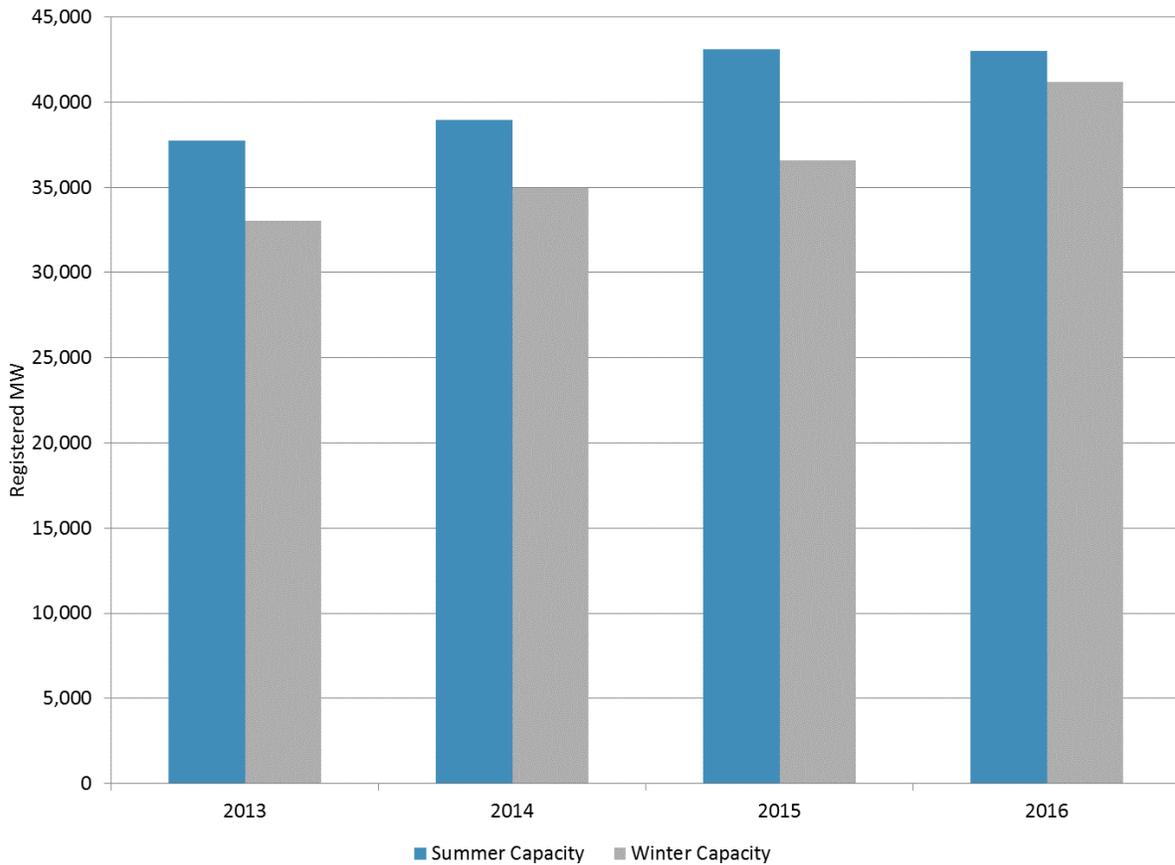


Figure D.1: Registered Demand Response Capacity MW by Season for All Registered Programs, 2013–2016

Product and Service Types

The webDADS portal collects information about demand response programs based on product type and product service type. Current product types in DADS include Energy, Capacity, and Reserves. [Figure D.2](#) shows the registered capacity MW of demand response across NERC for Summer 2013–2016 and Winter 2013–2016 by reported product and service type.

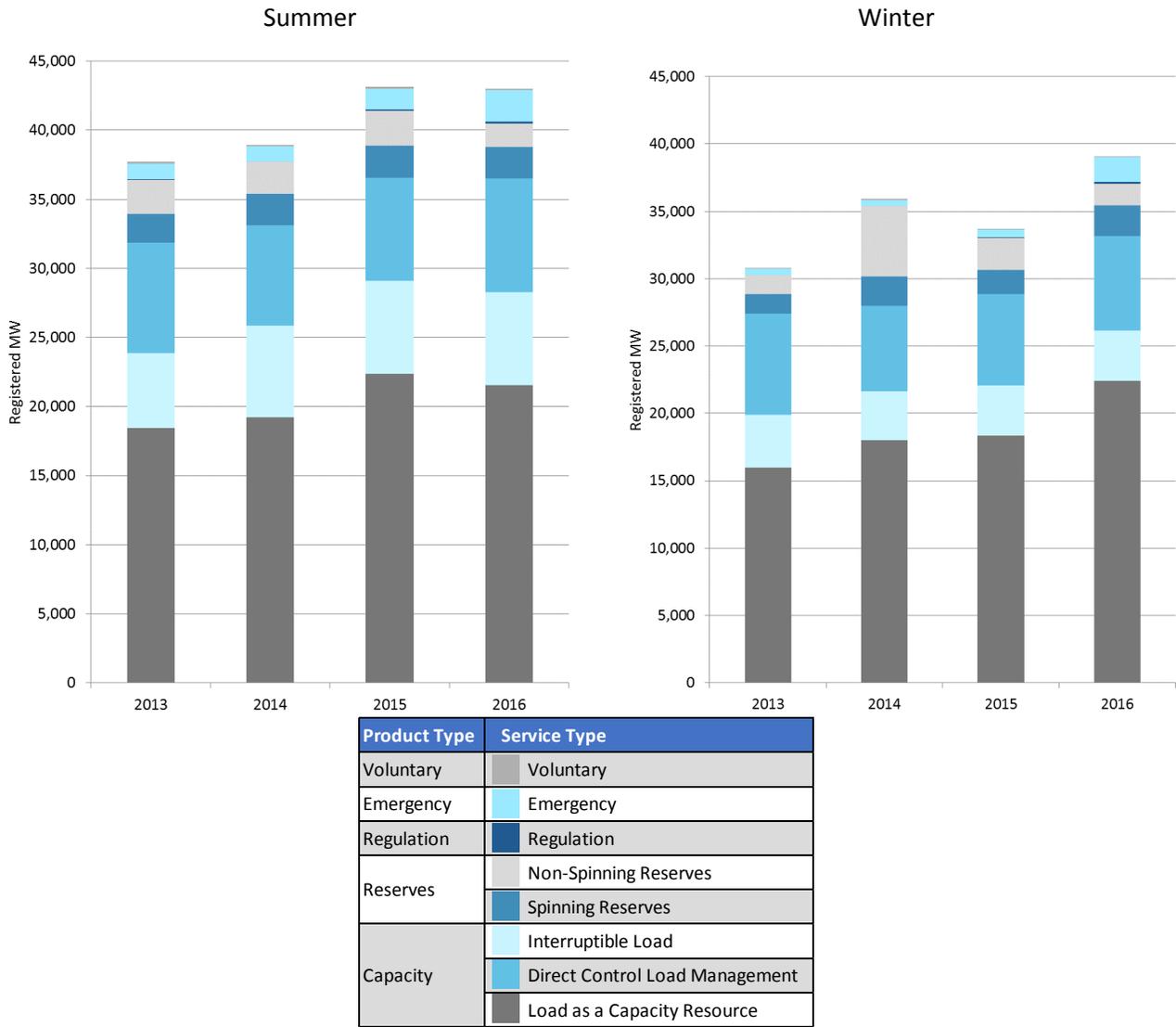


Figure D.2: Registered Demand Response Capacity MW by Service Type and Season, 2013–2016

A review of available capacity registered for each service type supports the following observations:

Summer Registered Program:

- The total of registered program enrollments remained stable.
- Increases in emergency and interruptible program enrollments were offset by decreases in load as a capacity resource and nonspinning reserves.
- There was a nominal reduction in summer registered program MW (approximately 100 MW).
- There were anecdotal reports of reductions in load as a capacity resource due in part to changes in environmental regulations for emergency engines.

Winter Registered Program:

- New emergency programs in two Regions have doubled the registered MW over Winter 2015.
- Interruptible load increased due to existing program that began reporting in Winter 2015/2016.

- There was an increase in load as a capacity resource that occurred primarily from the implementation of new wholesale market demand response programs in a single Region.

Demand Response: Reliability Events

Demand response programs are deployed by system operators that are monitoring conditions on the grid. Demand response program rules may require advanced notification for the deployment of these resources that can be several hours ahead of when the emergency condition actually occurs. As the potential for the emergency condition approaches, many operators have more responsive demand response resources that may be deployed with as little as 10 minutes of notification to ramp and curtail load.

Reliability event reasons reported and summarized in DADS are categorized as one of three types of events where demand response supports the BPS: forecast or actual reserve shortage, reliability event, and frequency control.

Reserve shortage events tend to be driven by extreme weather events. For example, the Polar Vortex of 2014 or extreme heat conditions seen on the East Coast and Northeast during 2013 and the West Coast during the summer of 2015. Reliability events can occur at almost any time, day, or month. These can typically be caused by a large number of unit trips or extreme weather that occurs during periods when the generation fleet is going through fleet maintenance periods in the shoulder months. Frequency control reliability events are a type of event that is more local and in isolated areas. For example, a large unit trip may cause a frequency disturbance which is then arrested by the instantaneous tripping of loads using under-frequency relays.

Figure D.3 shows demand response events reported into DADS from January 2013 through September 2016, grouped by month for the four years of event data.¹¹⁴ The black diamond in each column indicates the number of calendar days in a month when demand response was deployed for a reliability event. The stacked bars show the number of days that demand response events occurred in each NERC Region. When the stacked bar exceeds the black diamond, it is an indication that multiple Regions had demand response events on the same day within the month.

¹¹⁴ Event data for October 2016 through December 2016 is not reported until after publication of this report.

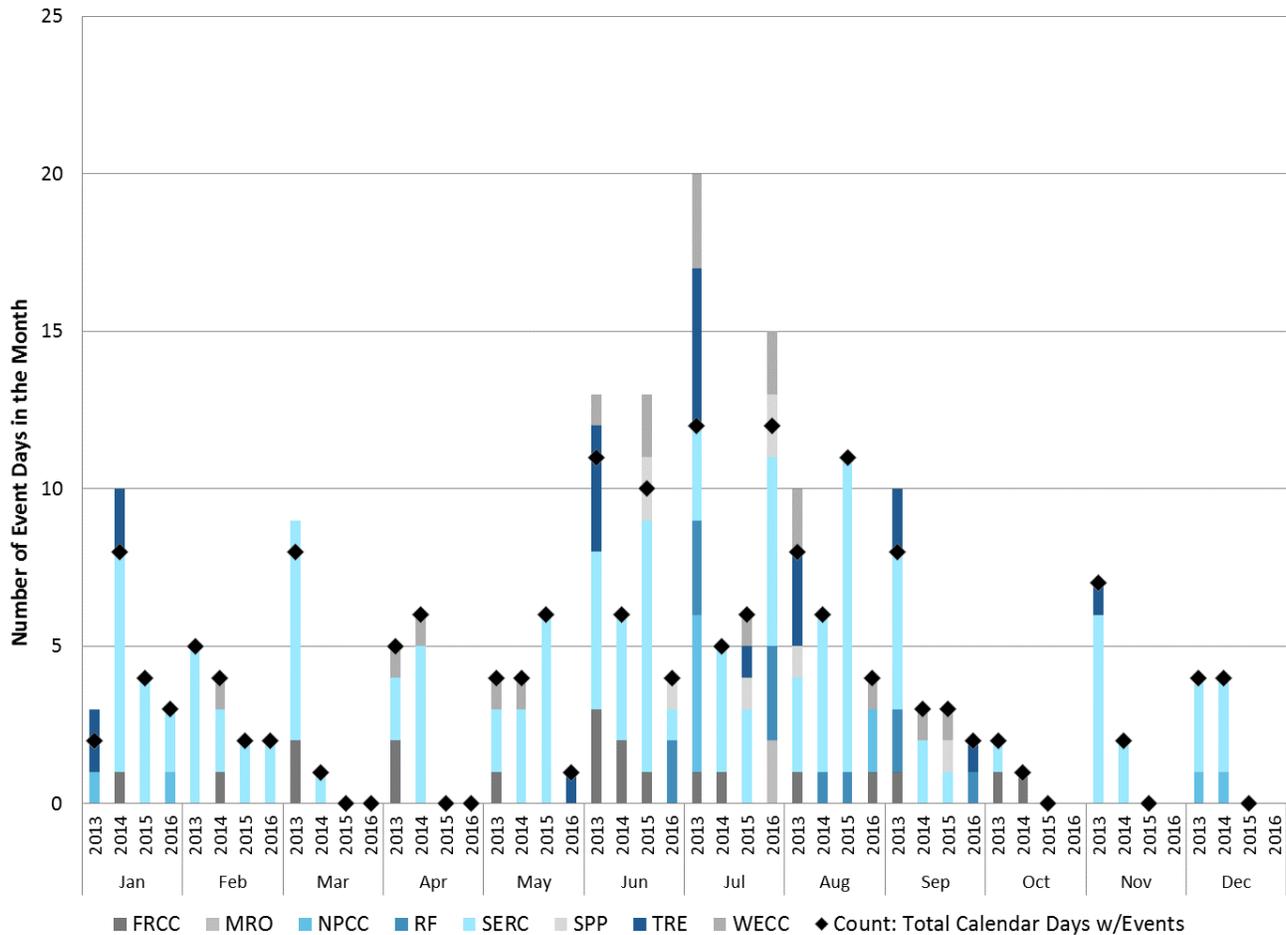


Figure D.3: Demand Response Events by Month and Region, 2013–2016

The peak number of events of DR capacity during this four-year period occurred around the summer peak season, and was especially evident during June and July of 2013. The second highest number of demand response deployments occurred during July of 2016. While there were deployments in several other months in 2016, overall the frequency of deployment events was lower than the previous three years. For example, the Summer¹¹⁵ of 2015 had 36 calendar days with deployments while the Summer of 2016 had 23 calendar days with deployments (a 36 percent drop in the number of calendar days during which demand response was deployed.). The impact of the Polar Vortex is also evident in the number of days and Regions that dispatched demand response in January 2014. Winter deployments for 2015 and early 2016 were down from 2014, due to warmer weather without the severity of the Polar Vortex events that occurred in 2014.

Figures D.4 and Figure D.5 represent reliability events from a slightly different perspective. In this case, the cumulative dispatched MW by Region illustrates the locational aspects of the utilization of demand response. The amount of deployed capacity is typically associated with the severity of the events—the more demand response dispatched indicates the greater need for the service it provides. This is evident in 2013 where the high number of deployments shown in Figure D.3 show a corresponding increase in deployed cumulative dispatched capacity in several Regions in Figure D.4. It should be noted that the summer of 2016 had a marked drop in the dispatched capacity from earlier years. However, all Regions deployed demand response in 2016 with most of the capacity being deployed in NPCC and SERC. There was one event in TRE during the summer of 2016 involving a deployment of almost 1000 MW of Load in response to a frequency excursion caused by a large unit trip.

¹¹⁵ Defined as April 1- September 30

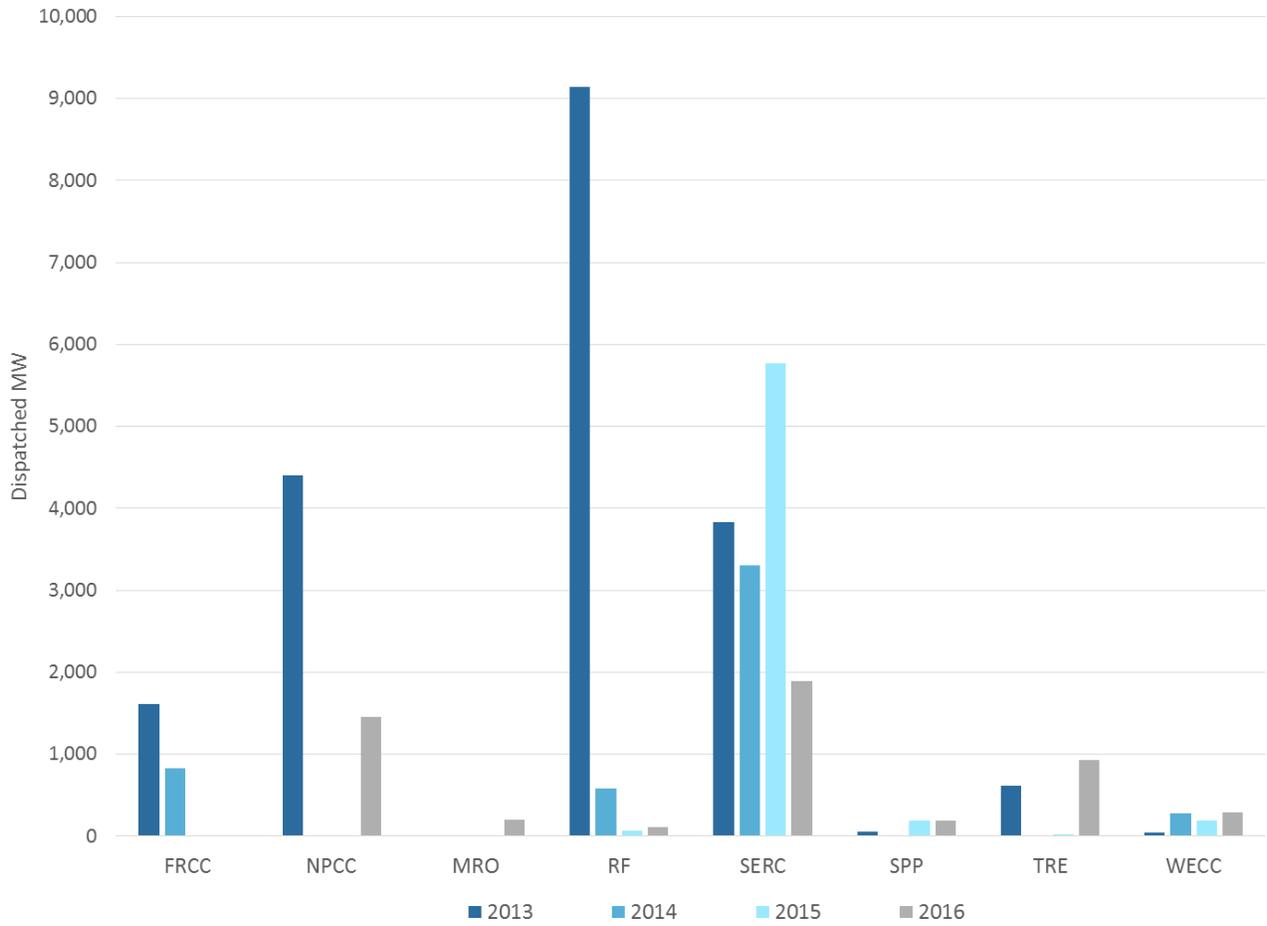


Figure D.4: Cumulative Dispatched MW by Region for Summer Demand Response Events, 2013–2016

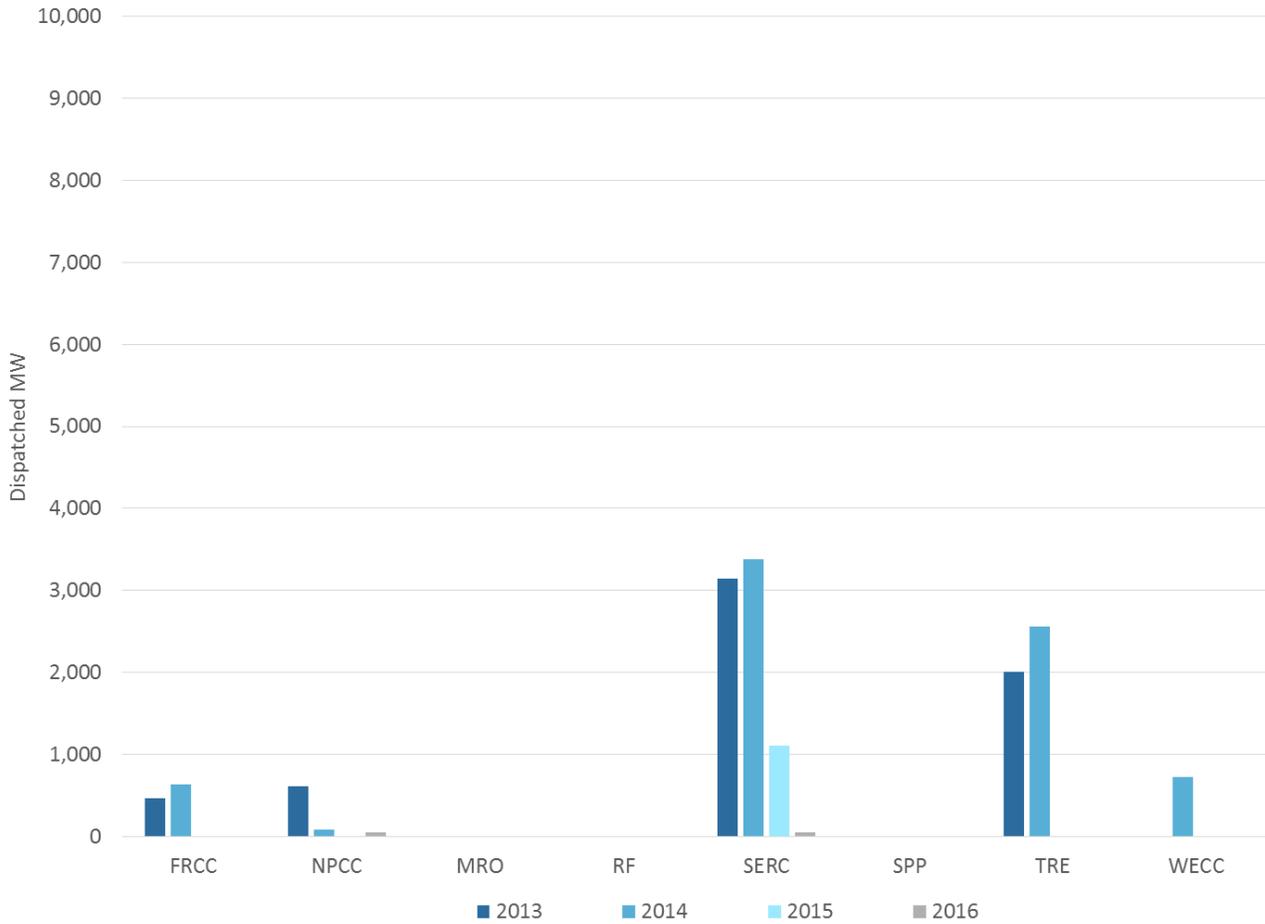


Figure D.5: Cumulative Dispatched MW for Winter Demand Response Events, 2013–2016

Figures D.6 and Figure D.7 show the cumulative amount of capacity deployed by the duration of the events. The majority of the Dispatched MW during the 2014 and 2015 years are in events lasting less than 60 minutes. Deployments associated with the heat wave over the East Coast and Northeast during the summer of 2013 tended to show much longer deployments, typically lasting four hours or more. Similarly, the events during the Polar Vortex phenomenon were much longer and extended over a broader stretch of the Southeastern US.

The frequency at which demand response is deployed may be a function of the demand response program’s design and not an indication of extensive reliability issues in a Region. For example, as shown in Figure D.3 note that in the SERC Region, demand response was deployed nearly every month during the analysis period. When viewed by event duration, the number of dispatched MW for these events shows that these deployments predominantly last for less than one hour.

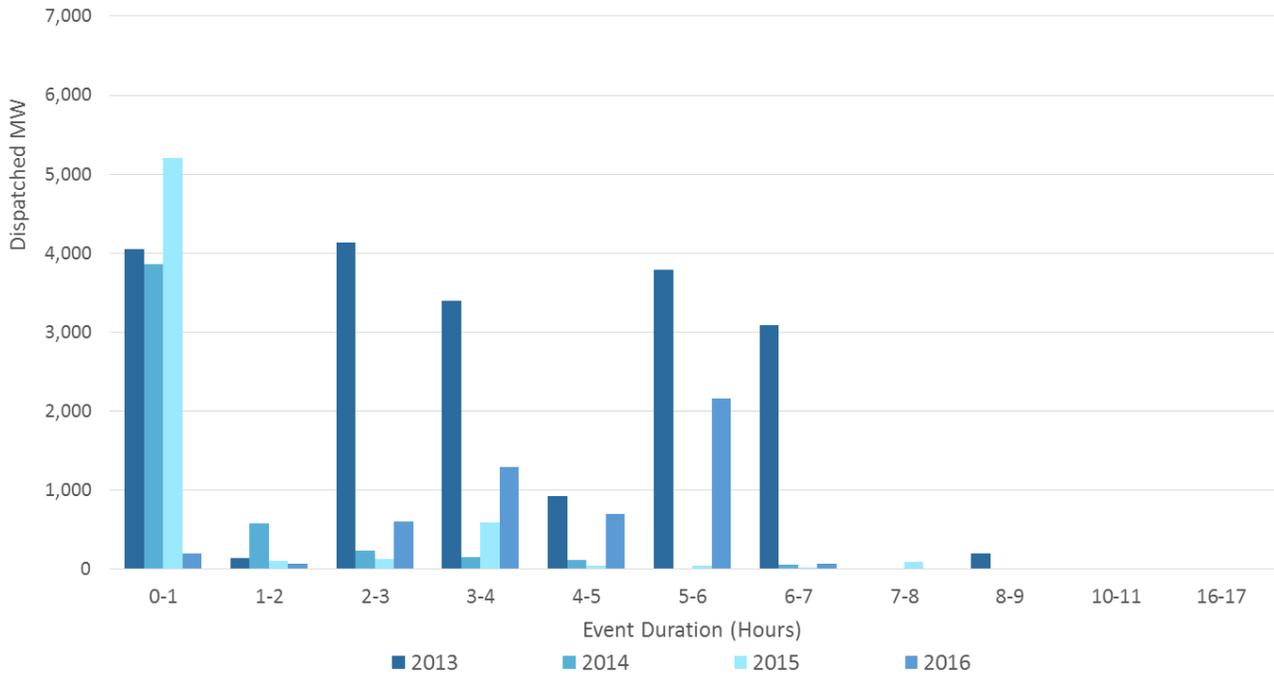


Figure D.6: Cumulative Dispatched MW by Duration for Summer Demand Response Events, 2013–2016

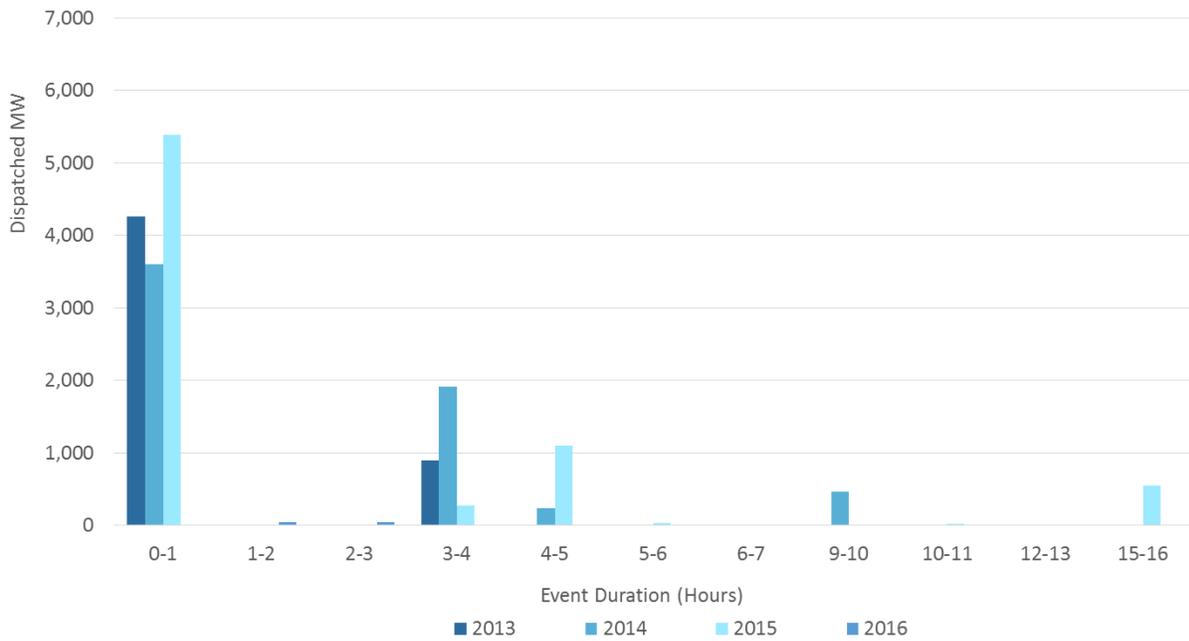


Figure D.7: Cumulative Dispatched MW by Duration for Winter Demand Response Events, 2013–2016

DADS Metrics

In 2015, four DADS metrics were developed by the DADSWG and approved by PAS. These metrics are described in [Table D.1](#).

Table D.1: DADS Metrics	
Title	Purpose
DADS Metric 1: Realized Demand Reduction of Event Deployment by Month	Shows the amount of demand response reduction (in MW) provided during all the reliability events deployed in a given month by time of day.
DADS Metric 2: Dispatched Demand Response MW by Service Type	Reflects the cumulative megawatts of demand reduction dispatched by service type in reliability event days per month at the NERC or Region level
DADS Metric 3: Realized Demand Response MW by Service Type	Reflects the cumulative time weighted megawatts of demand reduction realized by service type in reliability event days per month at the NERC or Region level
DADS Metric 4: Demand Response Events by Month – Dispatched vs. Realized	Allows for the creation of a demand response realization rate for reliability events to be established and trending

The DADSWG has completed initial analysis of Metrics 2, 3, and 4; the results are provided below. The work group will continue to monitor and analyze the DADS metrics and will provide additional information in future *State of Reliability* reports.

DADS Metric 1

While all metrics require software changes to DADS, Metric 1 requires extensive additional processing and formatting to support reporting this metric.

DADS Metric 2

The amount and types of demand response dispatched by year illustrates how much weather can affect the deployment of demand response. [Figure D.8](#) and [Figure D.9](#) show the cumulative dispatched MW of demand response by service type for summer and winter, respectively. During the summer of 2013, the cumulative amount of demand response deployed over all events was nearly 20,000 MW with over 70 percent of the demand response dispatched from load as a capacity resource and nearly equal amounts of direct load control and Interruptible Load. The summers of 2014 and 2015 were much milder, resulting in few deployments and more conservative utilization of demand response, primarily from direct load control and interruptible load. During the summer of 2016, deployments included a marked increase in the amount of demand response providing spinning reserves.

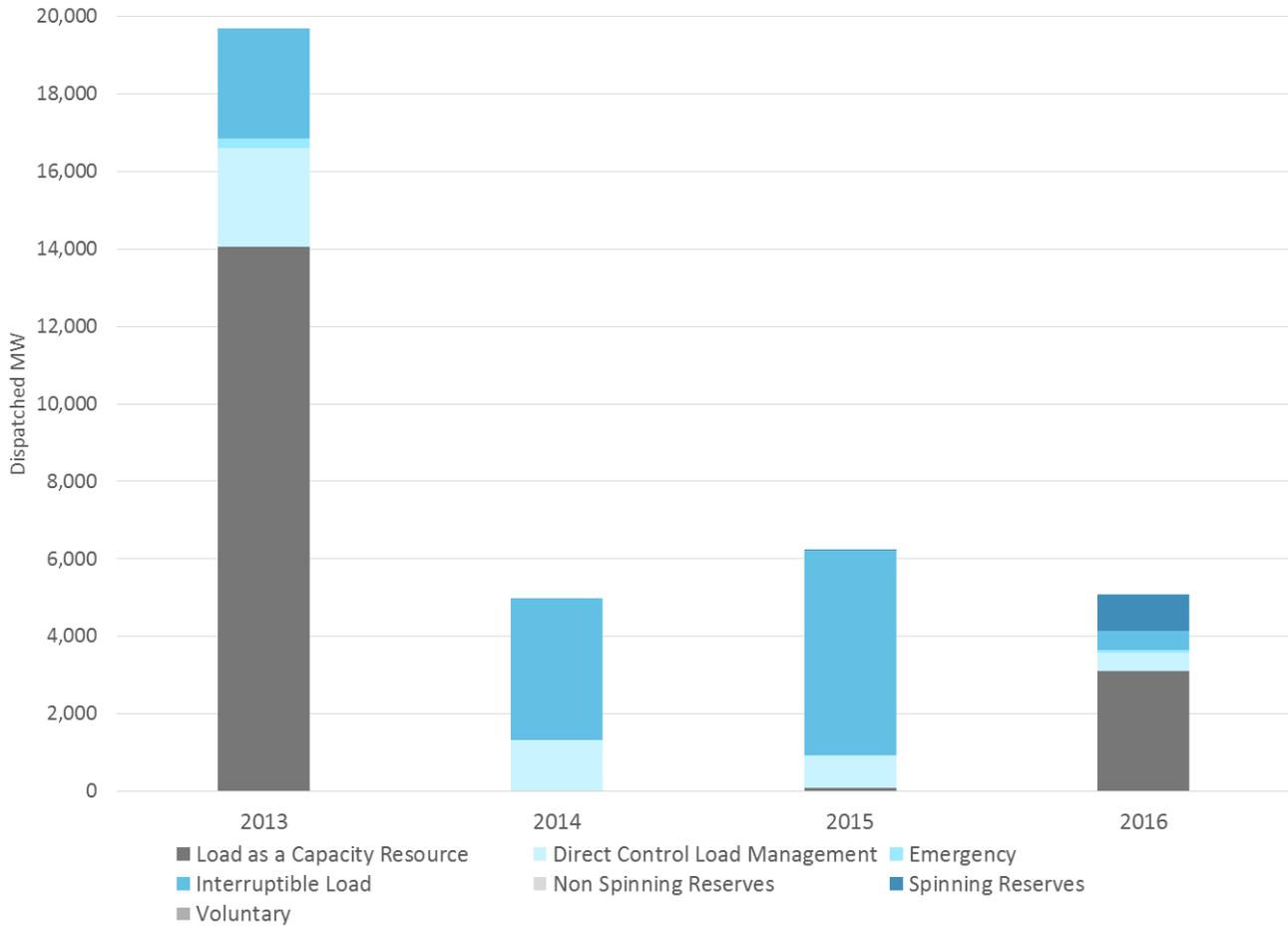


Figure D.8: Cumulative Dispatched MW by Service Type for Summer Demand Response Events, 2013–2016

Winter deployments of demand response are much less extensive as reflected in the cumulative MW dispatched each winter in the analysis period (Figure D.9). Deployments during the analysis period were primarily to demand response provided from interruptible load resources. During the winters of 2013 and 2014, demand response providing reserves (spinning and nonspinning) accounted for almost one-third of the cumulative dispatched MW each year.

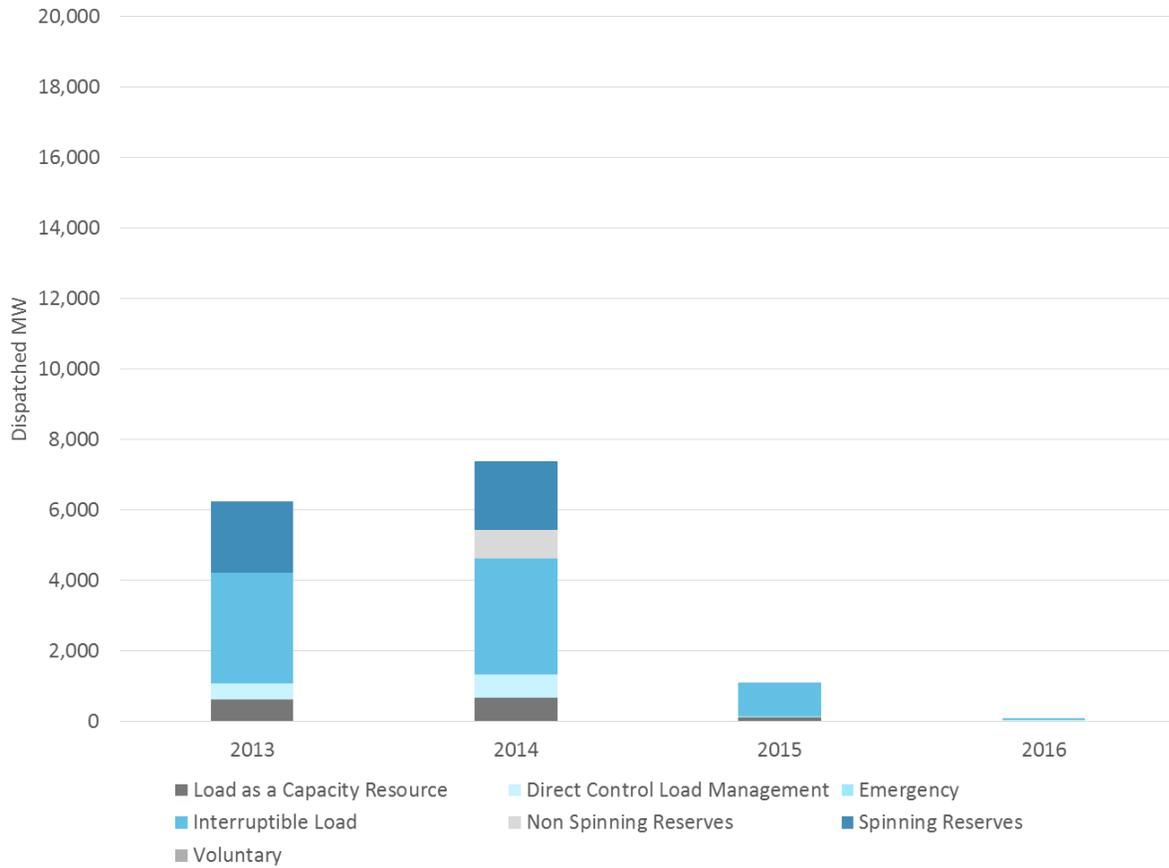


Figure D.9: Cumulative Dispatched MW by Service Type for Winter Demand Response Events, 2013–2016

DADS Metric 3

Figures D.10 and Figure D.11 report the performance of demand response resources based on service type for summer and winter, respectively. Average hourly response is calculated for each event as the sum of reported response divided by the number of dispatched hours reported with the event.

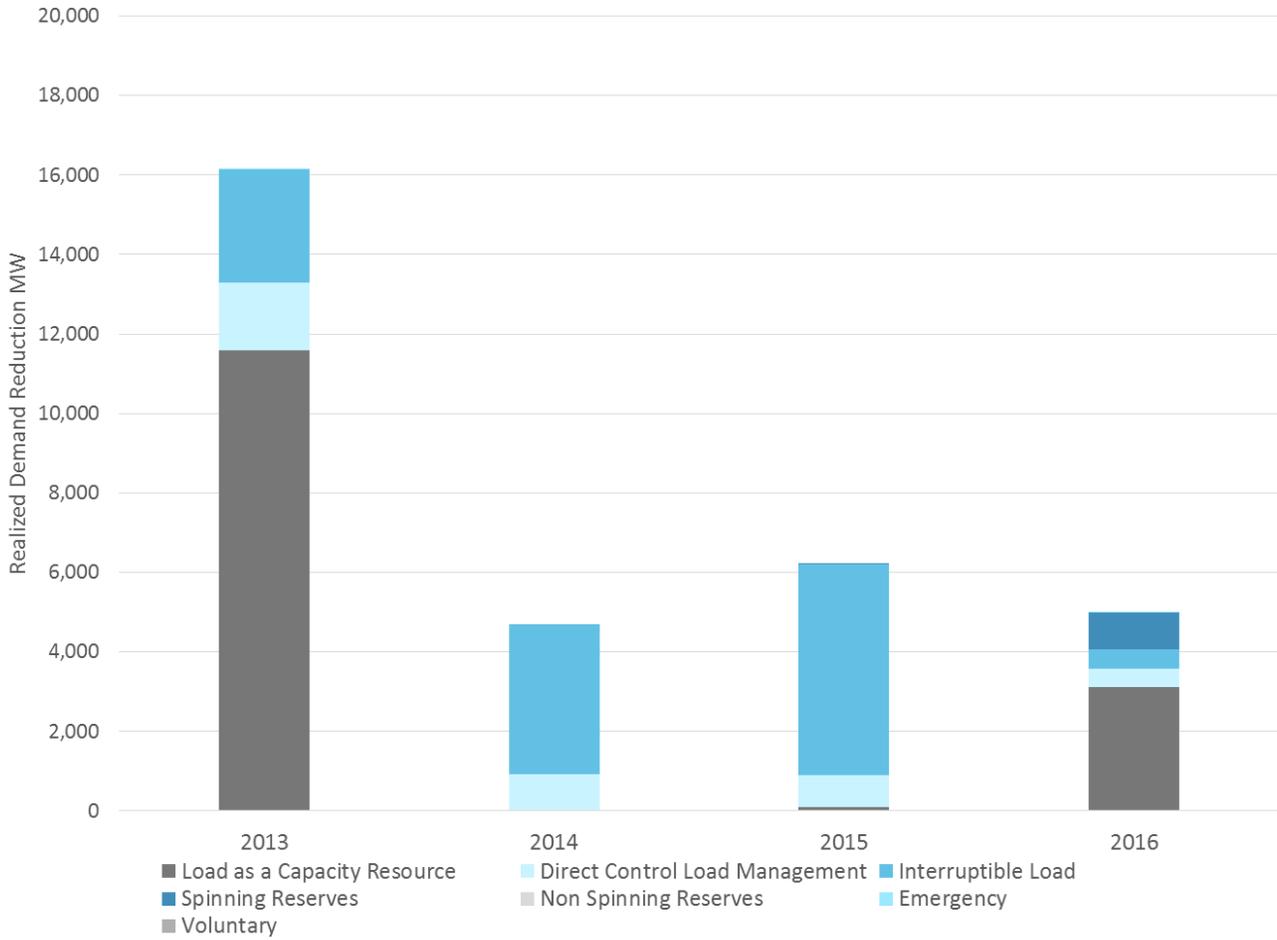


Figure D.10: Cumulative Realized Demand Reduction MW by Service Type for Summer Demand Response Events, 2013–2016

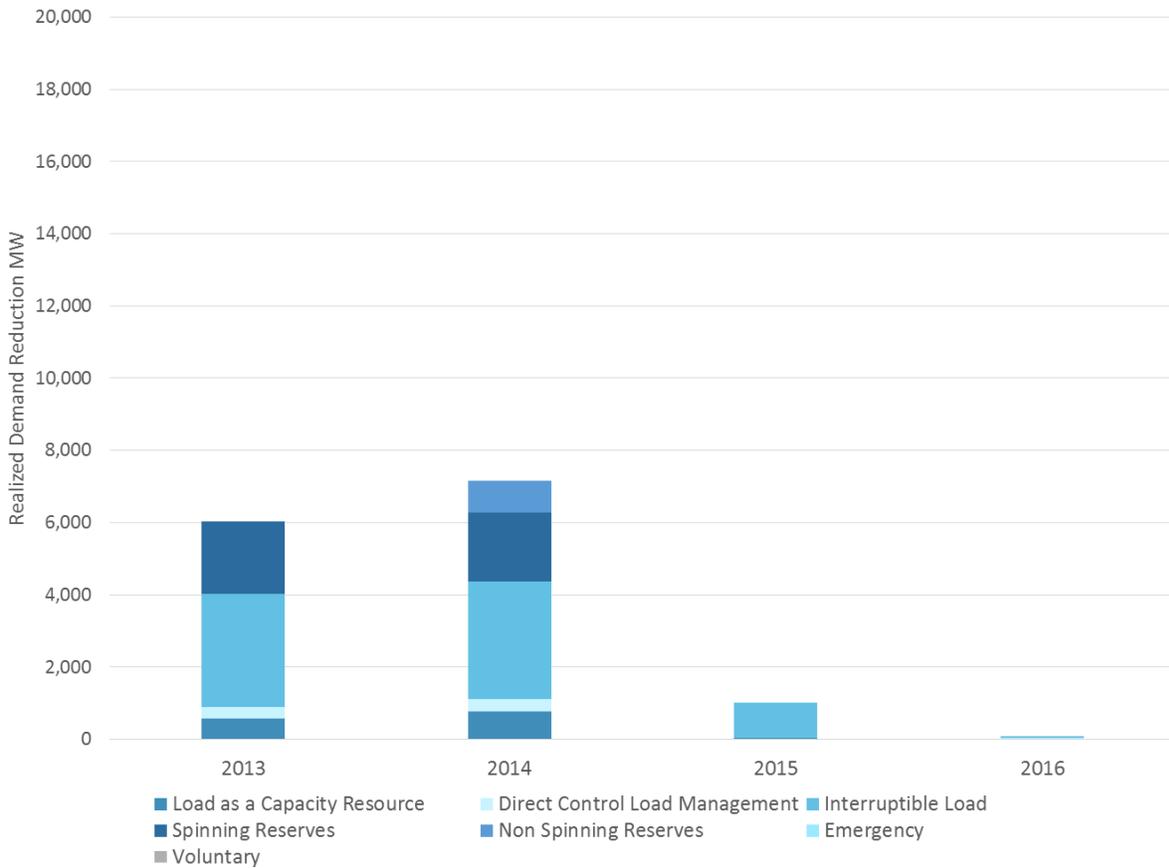


Figure D.11: Cumulative Realized Demand Reduction MW by Service Type for Winter Demand Response Events, 2013–2016

DADS Metric 4

The effectiveness of demand response to support reliability is illustrated by a comparison of the cumulative dispatched MW to the average realized reduction MW each season and year. **Figures D.12** and **Figure D.13** show the cumulative dispatched MW and corresponding performance of all demand response types deployed in a season for each year of the analysis period.

During the summer of 2013, demand response performed at 82 percent of its committed capacity (**Figure D.12**). This includes the deployment of voluntary and emergency types of demand response, which typically performs at a much lower rate (about 15 percent of registered) than other categories of demand response. The voluntary and emergency types of demand response deployed in the summer of 2013 represented 1.3 percent of all dispatched MW. When the summer of 2013 performance was evaluated without the voluntary and emergency types of demand response, there was a slight increase in performance, from 82.1 percent to 82.9 percent. Performance during the summers of 2014 through 2016 was well above 90 percent, due to the amount and types of demand response deployed.

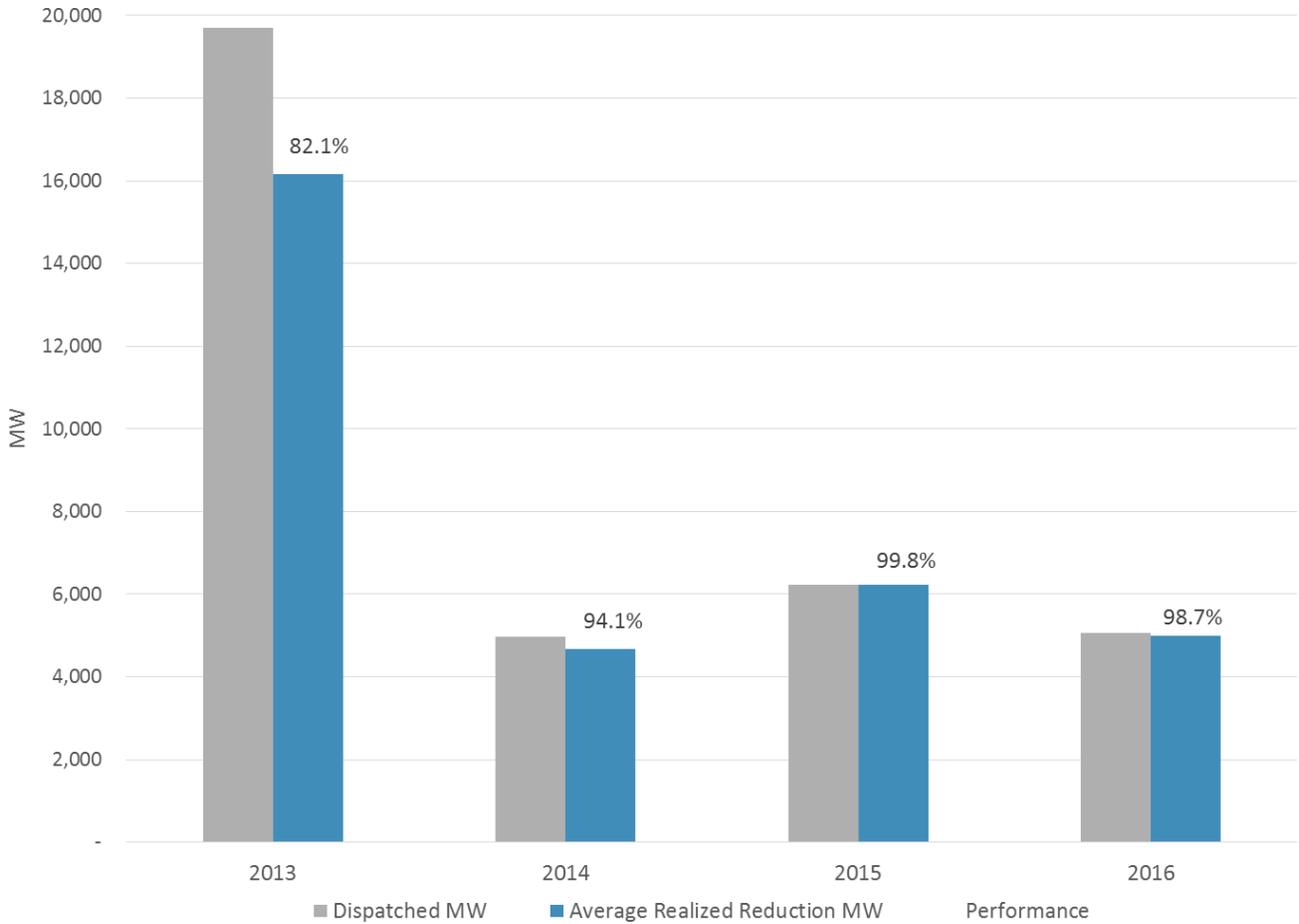


Figure D.12: Demand Response Performance for Summer Demand Response Events, 2013–2016

As previously stated, fewer MW of demand response were deployed in the winter seasons. Performance exceeded 96 percent during events in the winters of 2013–2014 and 90 percent in 2015 (Figure D.13). Fewer than 100 MW of demand response were deployed in the winter of 2016.

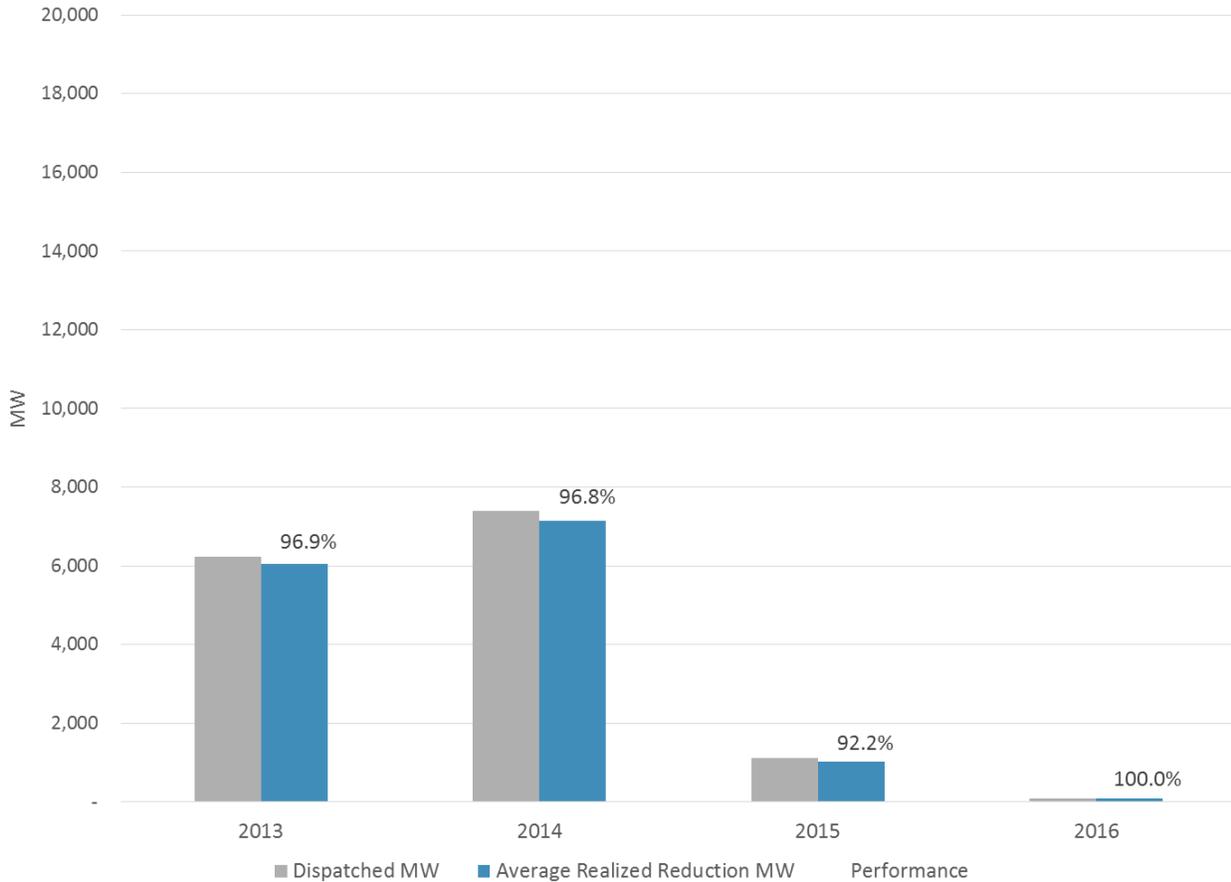


Figure D.13: Demand Response Performance for Winter Demand Response Events, 2013–2016

Looking Ahead

The DADSWG is focused on improving the quality of the demand response data collected by NERC, and this will provide a better perspective on how this type of resource is being used to support reliability. To achieve this objective, the following initiatives are planned for 2017 and beyond:

- Improvements to the DADS application to better support data reporting capabilities for market-based demand response programs that support reliability.
- Development and implementation of training to improve data reporting.
- Participate in the evaluation of demand response data used in the Long-Term Reliability Assessment (LTRA) and other NERC special assessments.

Appendix E: Reliability Indicator Trends

This appendix contains detailed supporting analysis for most of the reliability indicators (metrics) listed and assigned trending values in Chapter 4, [Table 4.1](#). Any metric that particularly speaks to BPS reliability trend changes in 2016 is explained to some degree in [Chapter 4](#). Those metrics might be completely covered in that chapter or might have more detailed analyses in this appendix. For those metrics that generally speak to reliability in any year but did not identify trend changes in 2016, their analyses are completely contained in this appendix.

An exception is M-4: Interconnection Frequency Response; this metric is particularly important given current changes to the BPS resource mix that might threaten adequate ERSs. Description of the focused actions regarding M-4 that BPS stakeholders and regulators took in 2016 are detailed in Chapter 2: 2016 Reliability Highlights rather than in Chapter 4: Reliability Indicator Trends, but all detailed analysis of M-4 is contained in this appendix.

M-1 Planning Reserve Margin

Background

This metric demonstrates the amount of generation capacity available to meet expected demand. It is a forward-looking or leading metric. PAS and Reliability Assessment Subcommittee are collaboratively working to determine if there is a better metric for this report.

This metric is reported in the annual LTRA¹¹⁶ and the Summer¹¹⁷ and Winter¹¹⁸ Assessments. NERC's 2015 LTRA¹¹⁹ discussed the observed tightening of reserve margins in several assessment areas. Similarly identified have been changes to the resource mix as some areas have diminishing resource diversity and flexibility. These two issues in conjunction could present additional operational issues even if an assessment area is showing sufficient planning reserve margins.

The most recent LTRA¹²⁰ indicates, as shown in [Figure E.1](#), that all Regions project sufficient reserve margins in the near term (five year window).¹²¹

¹¹⁶ <http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/2016%20Long-Term%20Reliability%20Assessment.pdf>

¹¹⁷ http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/2016%20SRA%20Report_Final.pdf

¹¹⁸ http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/WRA%202016_2017_final.pdf

¹¹⁹ <http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/2015LTRA%20-%20Final%20Report.pdf>

¹²⁰ <http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/2016%20Long-Term%20Reliability%20Assessment.pdf>

¹²¹ The reserve margins in Figure E.1 reflect the most critical peak season for each reporting entity when reserves are lowest. This includes consideration of whether each entity is summer or winter peaking.

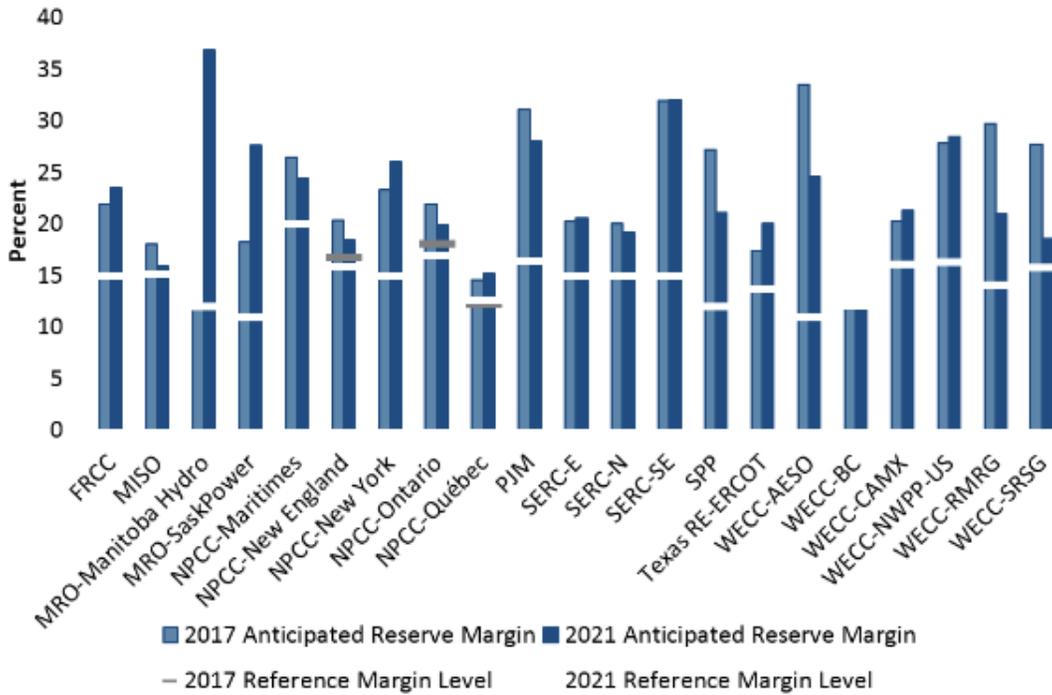


Figure E.1: M-1 Planning Reserve Margin

M-3 System Voltage Performance

Background

This metric was retired from the monitored set of metrics in 2014.

Future Development

Maintaining system voltage and adequate reactive control remains an important reliability performance objective that must be incorporated into the planning, design, and operation of the BES. The ERSWG developed a November 2015 framework report¹²² that recommended a set of voltage measures with PAS assigned to develop data collection to support Measure 7: Reactive Capability on the System.

During 2016, PAS developed and conducted a voluntary data collection and released the data for analysis to the SAMS for analysis of Measure 7 as a potential voltage and reactive metric.

M-4 Interconnection Frequency Response

Summary

This metric measures primary frequency response trends for each interconnection so that adequate frequency support is provided to arrest and stabilize frequency during large frequency events. The statistical trends discussed for operating years 2012–2016 should be considered within the context of longer term trends analyzed and discussed in the *Frequency Response Initiative Report* from 2012.¹²³

Figure E.2 shows the decline in frequency response since 1994 for the Eastern Interconnection that was discussed in the 2012 *Frequency Response Initiative Report* with data and the short-term trend for the operating years 2012–

¹²² <http://www.nerc.com/comm/Other/essntlrbltysrvkstskfrDL/ERSTF%20Framework%20Report%20-%20Final.pdf>

¹²³ http://www.nerc.com/docs/pc/FRI_Report_10-30-12_Master_w-appendices.pdf

2016 added. While there is insufficient data to show the same historic time trends for the Western, ERCOT, and Québec Interconnections, many of the issues that led to the decline in the Eastern Interconnection, such as incorrect governor deadband settings, generator controls, and plant-level control interactions have been observed in those interconnections.

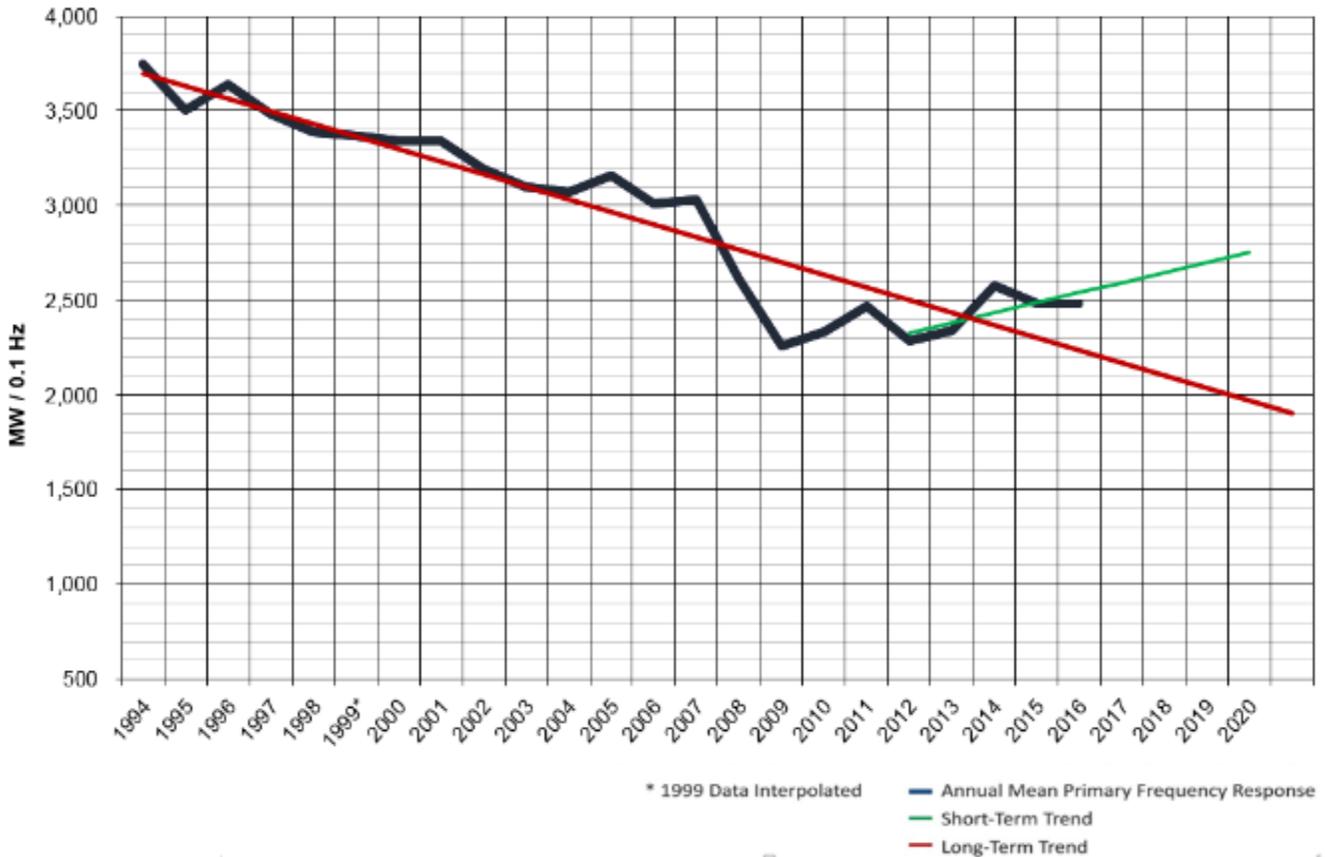


Figure E.2: Eastern Interconnection Frequency Response Trend¹²⁴

Statistical Trends in Frequency Response by Interconnection

NERC applies statistical tests to interconnection frequency response datasets. An operating year, for frequency event purposes, runs from December of the previous year through November of that year. For the 2012–2016 operating years, historical frequency response was statistically analyzed to evaluate performance trends by interconnection. An increasing trend over time indicates that frequency response is improving in that interconnection. It should be noted that in the 2016 operating year no interconnection had an M-4 frequency event where the frequency response performance was below its IFRO. It is important to note that there is a difference between the measured frequency response for a given event and the amount of response that was actually available at the time of the event. Measured response varies depending on starting frequency as well as the size of the resource loss. The following are overall observations and recent trends for each interconnection:

¹²⁴ The source of the Frequency Response data from 1994–2009, displayed in Figure E.2, is a report by J. Ingleson & E. Allen, “Tracking the Eastern Interconnection Frequency Governing Characteristic” that was presented at the 2010 IEEE PES. The source of the data from 2010 and 2011 are the daily automated reliability reports. The data for 1999, designated by *, was interpolated. Figure E.2 also reflects a change in the method for calculation of frequency response in 2009 (See FRI Report p. 25).

- Eastern Interconnection frequency response (FR) time trend, over the 2012–2016 operating years, was neither statistically increasing nor decreasing.¹²⁵ The mean FR in 2016 statistically significantly increased compared with 2013 but was similar to 2014 and 2015. The 2016 median FR was statistically similar to 2014 and 2015. The Eastern Interconnection shows incremental improvements in frequency response performance as demonstrated by higher mean Point C and mean Value B frequencies. This suggests improved primary frequency response during the arresting phase and recovery phase of the events. However, variability increased in 2016 with a higher maximum and lower minimum FR for all years studied. This could be due to a reduced mean resource MW loss and should be monitored in future years. The overall performance trend for the Eastern Interconnection is considered improving, albeit incrementally, due to these results.
- The ERCOT Interconnection has shown a statistically significant increase in frequency response over the 2012–2016 operating years. The mean and the median FR in 2016 was the highest in the five years. The Interconnection has demonstrated higher mean Point C and higher mean Value B frequencies, suggesting improved overall primary frequency response in both the arresting and recovery phases. However, variability increased in 2016 with the lowest Point C observed trending lower since the 2014 operating year. This could be due to an increase in the number of events sampled and should be monitored in future years. Since 2014, the lowest Point C frequency has been decreasing and the lowest Point C to UFLS margin has been smaller each year, which is a trend that should be monitored. The overall performance trend for the ERCOT Interconnection is considered improving due to these results.
- The Québec Interconnection frequency response trend over the 2012–2016 operating years was neither statistically increasing nor decreasing. In the 2015 and 2016 operating years, mean and median frequency response increased, however only the median increase was statistically significant from 2014 to 2016. No clear trend was observed in the mean Point C or Value B frequencies or in the distribution of events. The overall performance trend for the Québec Interconnection is considered to be stable (unchanged) due to these results.
- The Western Interconnection frequency response time trend in the 2012–2016 operating years was neither statistically increasing nor decreasing. There was a statistically significant increase in FR in 2016 versus 2014. The 2016 median FR was numerically higher than in 2014 and 2015. However, the 2016 variance also statistically significantly increased compared with both 2014 and 2015. The Western Interconnection shows incremental improvements in frequency response performance as demonstrated by higher mean Point C and mean Value B frequencies beginning in 2014. This suggests improved primary frequency response during the arresting phase and recovery phase of the events. However, this could be due to a reduced mean resource MW loss and should be monitored in future years. The performance trend for the Western Interconnection is considered to be improving, albeit slightly, due to these results.

In the 2016 operating year, a change in selection criteria was implemented that included frequency events with a smaller MW loss if the event resulted in a sufficient frequency deviation. Note that this change resulted in a larger sample of events for all interconnections as compared to previous years.

Further statistical significance tests were applied to interconnection frequency response datasets with additional correlation analysis on time of year, load levels, and other attributes also conducted. These results and further statistical analysis can be found in the background for the metric.

Background

Stable frequency is a key ALR performance outcome. Frequency response is essential to support frequency during disturbances that result in large frequency deviations as well as during system restoration efforts. Frequency

¹²⁵ A statistical test is performed to determine if the time trend line is increasing or decreasing. A statistically significant trend means that the slope, positive or negative, is unlikely to have occurred by chance. The complete statistical analysis can be found in Appendix E.

response (primary frequency control) is comprised of the actions provided by the interconnection to arrest and stabilize frequency in response to frequency deviations. Frequency response comes from automatic generator governor response, load response (typically from motors), and devices that provide an immediate response based on locally detected changes in frequency by device-level control systems. The purpose of the M-4 metric is to monitor frequency response trends for each interconnection so that adequate primary frequency control is provided to arrest and stabilize frequency during extreme frequency events and avoid tripping the first stage of UFLS for each interconnection.

The IFRO is intended to be the minimum amount of frequency response that must be maintained by an interconnection and is reviewed and determined annually in the *Frequency Response Annual Analysis*¹²⁶. Each BA in the interconnection is allocated a portion of the IFRO that represents its minimum responsibility in accordance with Reliability Standard BAL-003-1.¹²⁷ The analysis in this chapter shows how the events resulting in the lowest frequency response compare with the IFRO.

Figure E.3 illustrates a frequency deviation due to a loss of generation resource and the methodology for calculating frequency response. The event starts at time t0. Value A is the average frequency from t-16 to t-2 seconds, Point C is the lowest frequency point observed in the first 12 seconds and Value B is the average from t+20 to t+52 seconds. The difference between Value A and Value B is the change in frequency used for calculating primary frequency response. Frequency response is calculated as the ratio of the megawatts lost when a resource trips and the frequency deviation. For convenience, frequency response is expressed in this report as an absolute value. A large absolute value of frequency response, measured in MW/0.1Hz, is better than a small value.

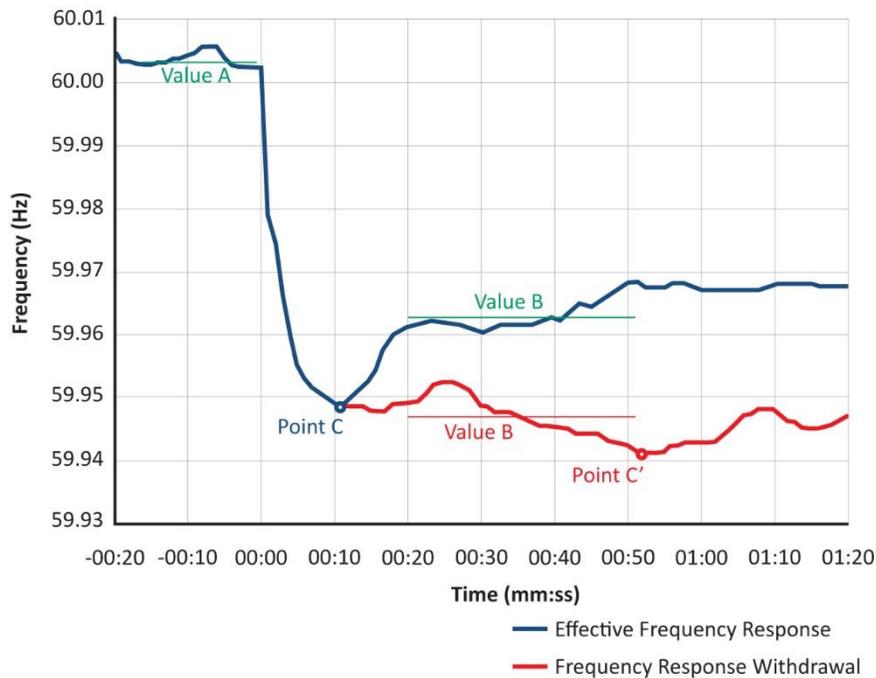


Figure E.3: Criteria for Calculating Value A and Value B

Selected events for frequency response analysis are vetted by the NERC Frequency Working Group (FWG). The event data is used to support Reliability Standard BAL-003-1 in addition to the M-4 metric.

¹²⁶ The analysis effective for the 2016 operating year can be found at: http://www.nerc.com/comm/OC/RS%20Landing%20Page%20DL/Related%20Files/2015_FRAA_Report_Final.pdf
¹²⁷ <http://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-003-1.1.pdf>

The NERC RS has identified issues related to the ability of existing generating resources to provide sustained frequency response including incorrect governor dead-band settings and plant or generator control logic. The NERC OC issued *Reliability Guideline: Primary Frequency Control v1.0 Final*¹²⁸ to encourage the industry to address these issues. Additionally, FERC issued a NOPR in 2016¹²⁹, seeking comment on FERC’s proposal to modify generator interconnection agreements to require that all new generation resources be capable of providing frequency response.

The North American BPS resource mix is changing to integrate an increasing level of inverter-based generation, such as wind turbine and solar, in addition to distributed energy resources and demand response programs. NERC established the ERSWG¹³⁰ to assess the impact on reliability resulting from a changing resource mix and developed measures to track and trend reliability impacts including frequency support. The analysis of these metrics may be included in future *State of Reliability* reports in accordance with the adoption of the metrics and data collection processes.

Interconnection Frequency Event Statistics

Table E.1 through **Table E.4** compare the M-4 frequency event statistics for the four Interconnections in accordance with the frequency response methodology shown in **Figure E.3**. It is useful to consider the mean Value B minus Point C to observe whether the frequency characteristics suggest changes in primary frequency response during the arresting and recovery phases. It is also useful to consider the mean and lowest Point C values in relation to the interconnection first-step UFLS relay settings.

In the 2016 operating year, a change in selection criteria was implemented that included frequency events with a smaller MW loss if the event resulted in a sufficient frequency deviation. Note that this change resulted in a larger sample of events for all interconnections as compared to previous years.

Table E.1: Frequency Event Statistics for Eastern Interconnection									
Operating Year	Total Number of Events	Mean Resource Loss (MW)	Mean Value A (Hz)	Mean Pt C (Hz)	Mean Value B (Hz)	Mean B-C Margin (Hz)	Mean Pt C-UFLS Margin (mHz)	Lowest Pt C (Hz)	Lowest Pt C-UFLS Margin (mHz)
2012	10	1259	60.001	59.948	59.946	-0.002	0.448	59.937	0.437
2013	32	1157	60.000	59.950	59.948	-0.001	0.450	59.909	0.409
2014	34	1212	59.995	59.947	59.948	0.001	0.447	59.910	0.410
2015	36	1103	59.996	59.948	59.950	0.002	0.448	59.928	0.428
2016	61	938	59.999	59.956	59.959	0.003	0.456	59.930	0.430

The following are observations from **Table E.1**:

- There is an increasing mean B-C margin each year since 2012, suggesting incremental improvements in the Eastern Interconnection frequency response.
- The lowest Point C to UFLS margin has increased each year, beginning in 2013.

¹²⁸ http://www.nerc.com/comm/OC/Reliability%20Guideline%20DL/Primary_Frequency_Control_final.pdf

¹²⁹ <https://www.ferc.gov/whats-new/comm-meet/2016/111716/E-3.pdf>

¹³⁰ [http://www.nerc.com/comm/Other/Pages/Essential-Reliability-Services-Task-Force-\(ERSTF\).aspx](http://www.nerc.com/comm/Other/Pages/Essential-Reliability-Services-Task-Force-(ERSTF).aspx)

- Point C and Value B frequencies have both trended higher since 2014. This trend should be monitored in light of a reduced mean resource loss in 2016.
- For frequency events in the 2016 operating year, the lowest Point C frequency was above the first-step UFLS setting of 59.5 Hz¹³¹ by 430 mHz, which is a slightly larger margin than in 2015.

Table E.2: Frequency Event Statistics for ERCOT Interconnection

Operating Year	Total Number of Events ¹³²	Mean Resource Loss (MW)	Mean Value A (Hz)	Mean Pt C (Hz)	Mean Value B (Hz)	Mean B-C Margin (Hz)	Mean Pt C-UFLS Margin (Hz)	Lowest Pt C (Hz)	Lowest Pt C-UFLS Margin (Hz)
2012	46	672	59.995	59.825	59.872	0.047	0.525	59.729	0.429
2013	40	721	59.997	59.836	59.896	0.061	0.536	59.732	0.432
2014	33	639	59.996	59.850	59.900	0.050	0.550	59.744	0.444
2015	34	642	59.999	59.866	59.912	0.046	0.566	59.728	0.428
2016	50	601	59.998	59.868	59.920	0.052	0.568	59.704	0.404

The following are observations from **Table E.2**:

- The mean Point C and Value B frequencies have both trended higher each year since 2012, suggesting improved overall primary frequency response in both the arresting and recovery phases.
- The mean Point C to UFLS margin has improved each year since 2012.
- For frequency events in the 2016 operating year, the lowest Point C frequency was above the first-step UFLS setting of 59.3 Hz by 404 mHz, which is a slightly larger margin than in 2015.

Table E.3: Frequency Event Statistics for Québec Interconnection

Operating Year	Total Number of Events ¹³³	Mean Resource Loss (MW)	Mean Value A (Hz)	Mean Pt C (Hz)	Mean Value B (Hz)	Mean B-C Margin (Hz)	Mean Pt C-UFLS Margin (Hz)	Lowest Pt C (Hz)	Lowest Pt C-UFLS Margin (Hz)
2012	25	852	60.003	59.452	59.854	0.402	0.952	58.792	0.292
2013	35	973	59.996	59.395	59.825	0.430	0.895	58.868	0.368
2014	33	806	60.004	59.413	59.836	0.423	0.913	58.986	0.486
2015	29	627	60.003	59.555	59.872	0.292	1.055	59.273	0.773
2016	49	740	59.998	59.487	59.859	0.372	0.977	59.019	0.519

The following are observations from **Table E.3**:

- There is no clear trend in primary frequency response statistics due to loss of resources.

¹³¹ The highest UFLS setpoint in the Eastern Interconnection is 59.7 Hz in FRCC, based on internal stability concerns. The FRCC concluded that the IFRO starting frequency of the prevalent 59.5 Hz for the Eastern Interconnection is acceptable in that it imposes no greater risk of UFLS operation in FRCC for an external resource loss event than for an internal FRCC event.

¹³² One loss of load event was excluded from the ERCOT statistics in Table E.2 for the 2014 operating year.

¹³³ In the Québec Interconnection, loss of load events were excluded from the statistics in Table E.3 for the following operating years: 2012 (6), 2013 (5), 2014 (9), 2015 (5), and 2016 (18).

- For frequency events in the 2016 operating year, the lowest Point C frequency was above the first-step UFLS setting of 58.5 Hz by 519 mHz, which is a smaller margin than in 2015 but larger than all other years above.

Table E.4: Frequency Event Statistics for Western Interconnection

Operating Year	Number of Events	Mean Resource Loss (MW)	Mean Value A (Hz)	Mean Pt C (Hz)	Mean Value B (Hz)	Mean B-C Margin (Hz)	Mean Pt C-UFLS Margin (Hz)	Lowest Pt C (Hz)	Lowest Pt C-UFLS Margin (Hz)
2012	5	1016	60.010	59.906	59.939	0.033	0.406	59.880	0.380
2013	13	945	59.993	59.887	59.924	0.037	0.387	59.843	0.343
2014	17	1095	60.001	59.880	59.917	0.036	0.380	59.671	0.171
2015	21	846	59.998	59.903	59.934	0.032	0.403	59.845	0.345
2016	47	734	60.008	59.918	59.956	0.037	0.418	59.819	0.319

The following are observations from Table E.4:

- Point C and Value B frequencies have both trended higher since 2014, which could suggest improved overall primary frequency response in both the arresting and recovery phases. This trend should be monitored in light of a declining mean resource loss in those years.
- For frequency events in the 2016 operating year, the lowest Point C frequency was above the first-step UFLS setting of 59.5 Hz by 319 mHz, which is a smaller margin than in 2015 but larger than the lowest margin of 171 mHz in 2014.

Interconnection Frequency Response: Time Trends

The time trend analyses uses the interconnection FR datasets for the 2012–2016 operating years. In this section, relationships between FR and the explanatory variable T (time = year, month, day, hour, minute, second) are studied. **Figures E.4** through **Figure E.7** show the interconnection FR scatter plots with a linear regression trend line, the 95 percent confidence interval for the data, and the 95 percent confidence interval for the slope of the time trend line.

It is important to note that there is a difference between the measured frequency response for a given event and the amount of response that was actually available at the time of the event. Measured response varies depending on starting frequency as well as the size of the resource loss.

Eastern Interconnection

In the Eastern Interconnection, there is a positive correlation of 0.12 between T and FR; however, the statistical test on the significance of the correlation (and the equivalent test of the significance of a linear regression) fails to reject the null hypothesis about zero correlation at a standard significance level (p value of both tests is 0.10). This result leads to the inference that the positive correlation may have occurred simply by chance. It implies that even though a linear trend line for the scatter plot connecting T and FR, shown in **Figure E.4**, has a positive slope (0.00000184), the slope of the linear regression is not statistically significant, and on average, the Eastern Interconnection FR trend has been stable from 2012–2016.

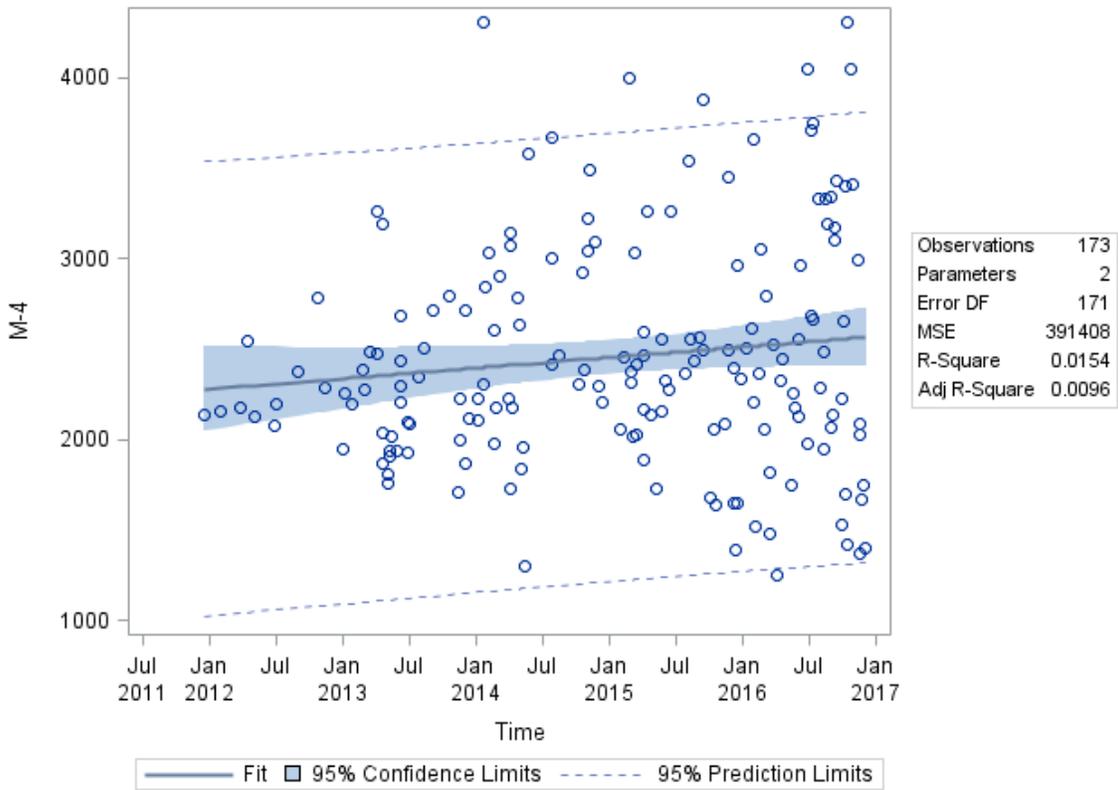


Figure E.4: Eastern Interconnection FR Scatter Plot and Time Trend Line 2012–2016

ERCOT Interconnection

In the ERCOT Interconnection, there is a positive correlation of 0.32 between T and FR; further, the statistical test on the significance of the correlation (and the equivalent test of the significance of a linear regression) results in a rejection of the null hypothesis about zero correlation at a standard significance level (p-value of both tests is below 0.0001). This proves that it was very unlikely that the observed positive correlation occurred simply by chance. A linear trend line for the scatter plot connecting T and FR (shown in [Figure E.5](#)) has a positive slope (0.00000163), and the linear regression slope is highly statistically significant. On average, the ERCOT interconnection FR grew from 2012 to 2016 at the monthly rate of 4.25 MW/0.1 Hz.

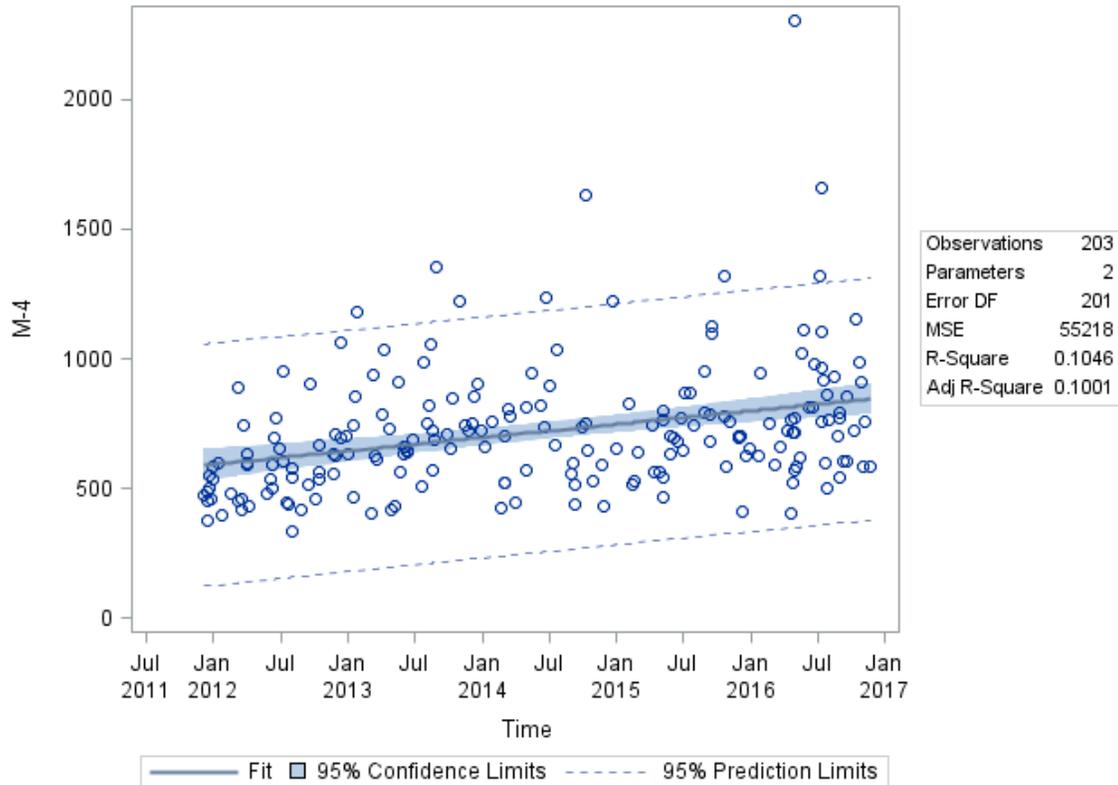


Figure E.5: ERCOT Interconnection Frequency Response Scatter Plot and Time Trend Line 2012–2016

Québec Interconnection

In the Québec Interconnection, there is a negative correlation of -0.12 between T and FR; however, the statistical test on the significance of the correlation (and the equivalent test of the significance of a linear regression) fails to reject the null hypothesis about zero correlation at a standard significance level (p value of both tests is 0.10). This result leads to the conclusion that the negative correlation very likely has occurred simply by chance. It implies that even though a linear trend line for the scatter plot connecting T and FR, shown in [Figure E.6](#), has a negative slope (-0.000000621), the linear regression is not statistically significant, and, on average, the Québec Interconnection FR has been flat from 2012 to 2016.

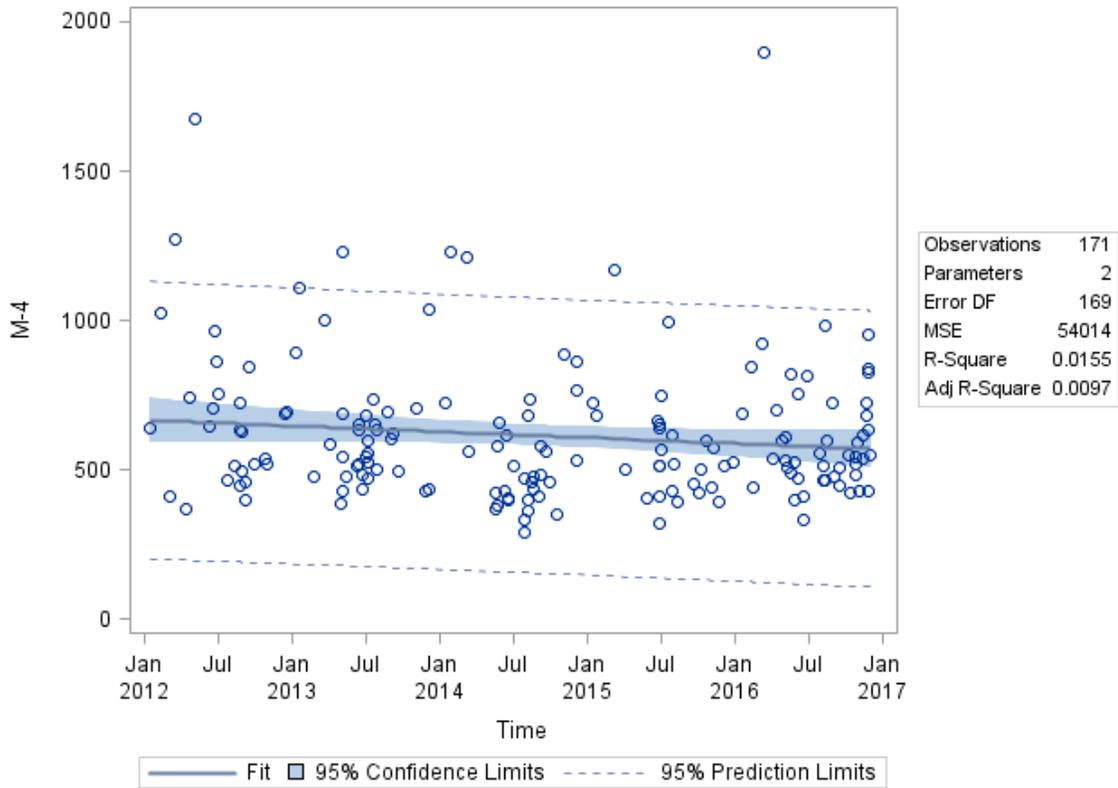


Figure E.6: Québec Interconnection Frequency Response Scatter Plot and Time Trend Line 2012-2016

Western Interconnection

In the Western Interconnection, there is a positive correlation of 0.12 between T and FR; however, the statistical test on the significance of the correlation (and the equivalent test of the significance of a linear regression) fails to reject the null hypothesis about zero correlation at a standard significance level (p value of both tests is 0.21). This result leads to the conclusion that the positive correlation very likely have occurred simply by chance. It implies that even though a linear trend line for the scatter plot connecting T and FR, shown in [Figure E.7](#), has a positive slope (0.00000151), the slope of the linear regression is not statistically significant, and on average, the Western Interconnection FR trend has been stable from 2012–2016.

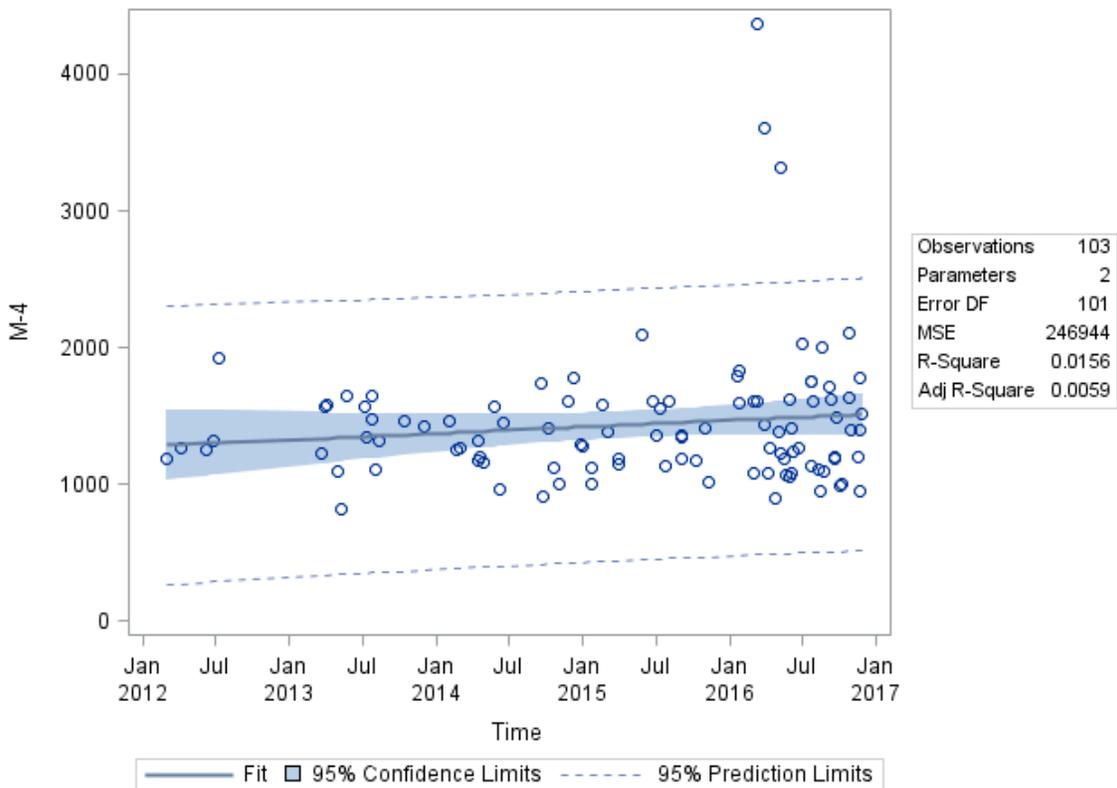


Figure E.7: Western Interconnection Frequency Response Scatter Plot and Time Trend Line 2012–2016

Interconnection Frequency Response: Year-to-Year Changes

The analyses of changes by year use the interconnection FR datasets from the 2012–2016 operating years. The sample statistics are listed by year in Tables E.5 through E.8. The last column lists the number of FR events that fell below the absolute IFRO.¹³⁴

Figures E.8 through Figure E.11 show the box and whisker plots of the annual distribution of the interconnection’s FR. The boxes enclose the interquartile range with the lower edge at the first (lower) quartile and the upper edge at the third (upper) quartile. The horizontal line drawn through a box is the second quartile or the median. The lower whisker is a line from the first quartile to the smallest data point within 1.5 interquartile ranges from the first quartile. The upper whisker is a line from the third quartile to the largest data point within 1.5 interquartile ranges from the third quartile. The data points beyond the whiskers represent outliers, or data points more than or less than 1.5 times the upper and lower quartiles, respectively. The diamonds represent the mean.

Next, to statistically compare parameters of the annual distributions of the frequency response listed in Tables E.5 to E.8, ANOVA’s Fisher’s Least Significant Difference test and t-test were used to analyze all pair-wise changes in the mean FR, the Mann-Whitney and Wilcoxon test was used to compare annual medians, and the tests on the homogeneity of variances to analyze changes in variance (and, thus, in the standard deviation).¹³⁵

In the 2016 operating year, a change in selection criteria was implemented that included frequency events with a smaller MW loss if the event resulted in a sufficient frequency deviation. Note that this change resulted in a larger sample of events for all interconnections as compared to previous years.

¹³⁴ [http://www.nerc.com/FilingsOrders/us/NERC Filings to FERC DL/Final Info Filing Freq Resp Annual Report 03202015.pdf](http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Final%20Info%20Filing%20Freq%20Resp%20Annual%20Report%2003202015.pdf)

¹³⁵ All tests at the significance level 0.05.

Eastern Interconnection

Table E.5 and Figure E.8 illustrate Eastern Interconnection year-to-year changes in the average and median FR as well as in its variation. There were no frequency events with FR below IFRO in 2012–2016.

Table E.5: Sample Statistics for Eastern Interconnection								
Operating Year (OY)	Number of Events	Mean of Frequency Response	Standard Dev. of Frequency Response	Median	Minimum	Maximum	IFRO for the OY	Number of Events with FR Below the IFRO
2012–2016	173	2,456.7	628.7	2,329.8	1,253.2	4,307.4	N/A	0
2012	10	2,288.3	222.7	2,187.5	2,081.5	2,783.5	1002	0
2013	32	2,239.1	384.1	2,200.7	1,707.0	3,264.4	1002	0
2014	34	2,639.7	626.9	2,619.7	1,300.3	4,304.1	1014	0
2015	36	2,479.9	577.1	2,372.0	1,635.8	3,996.9	1014	0
2016	61	2,482.9	767.4	2,368.6	1,253.2	4,307.4	1015	0

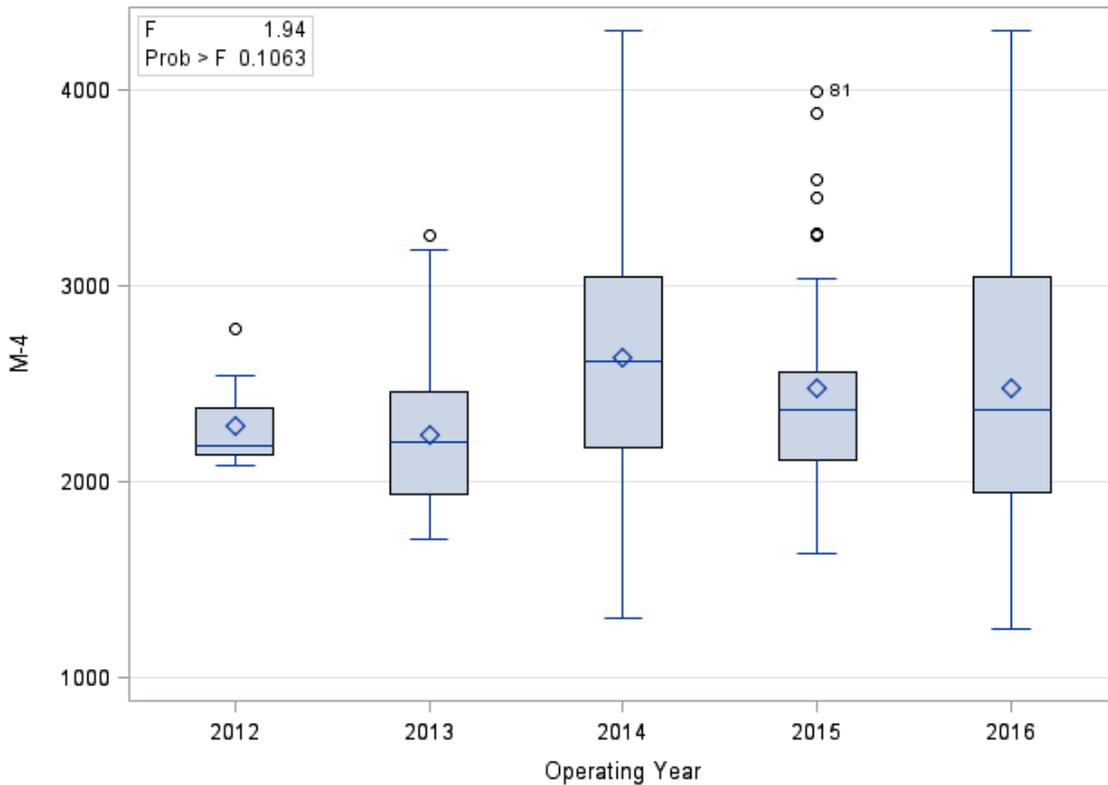


Figure E.8: Eastern Interconnection Frequency Response Distribution by Operating Year 2012–2016

There was a statistically significant increase in both the mean frequency response and the variance of frequency response in 2014 vs. 2013 and in 2016 vs. 2013 operating years; the 2014 median statistically significantly increased compared with 2013 and has not changed statistically after that (a very small number of events in the 2012 operating year does not allow for a reliable statistical comparison with other years). For the 2016 operating

year, frequency events with the minimum frequency response of 1253 MW/0.1Hz were 23.4 percent above the IFRO with the event resulting in a C point frequency within 460 mHz of the interconnection first step UFLS setting from a starting frequency of 60.008 Hz.

ERCOT Interconnection

Table E.6 and [Figure E.9](#) illustrate year-to-year changes in the average and median FR as well as in its variation. Over the five years, there was one frequency event with FR below IFRO (in 2015).

Table E.6: Sample Statistics for ERCOT Interconnection								
Operating Year (OY)	Number of Events	Mean of Frequency Response	Standard Dev. of Frequency Response	Median	Minimum	Maximum	IFRO for the OY	Number of Events with FR Below the IFRO
2012–2016	203	719.0	247.7	688.7	336.7	2,304.4	N/A	1
2012	46	561.6	135.6	540.8	336.7	948.6	286	0
2013	40	752.2	218.2	704.9	406.6	1,353.9	286	0
2014	33	727.2	245.9	720.2	425.7	1,628.0	413	0
2015	34	755.8	196.7	722.1	468.6	1,315.8	471	1
2016	50	806.7	315.7	752.0	403.6	2,304.4	381	0

[Figure E.9](#) shows the box plot of the annual distribution of the ERCOT FR.

The mean and the median FR in the 2013, 2014, 2015 and 2016 operating years were significantly better than in the 2012. Numerically, the mean and the median FR in 2016 were the highest over the five years in the study, but the variance also statistically significantly increased compared with 2015. These results corroborate an observation on the improving frequency response trend in ERCOT. For 2016 operating year frequency events had the lowest frequency response of 404 MW/0.1Hz, which was 6.0 percent above the IFRO with the event resulting in a C point frequency nadir within 605 mHz of the interconnection first step UFLS setting from a starting frequency of 60.015 Hz.

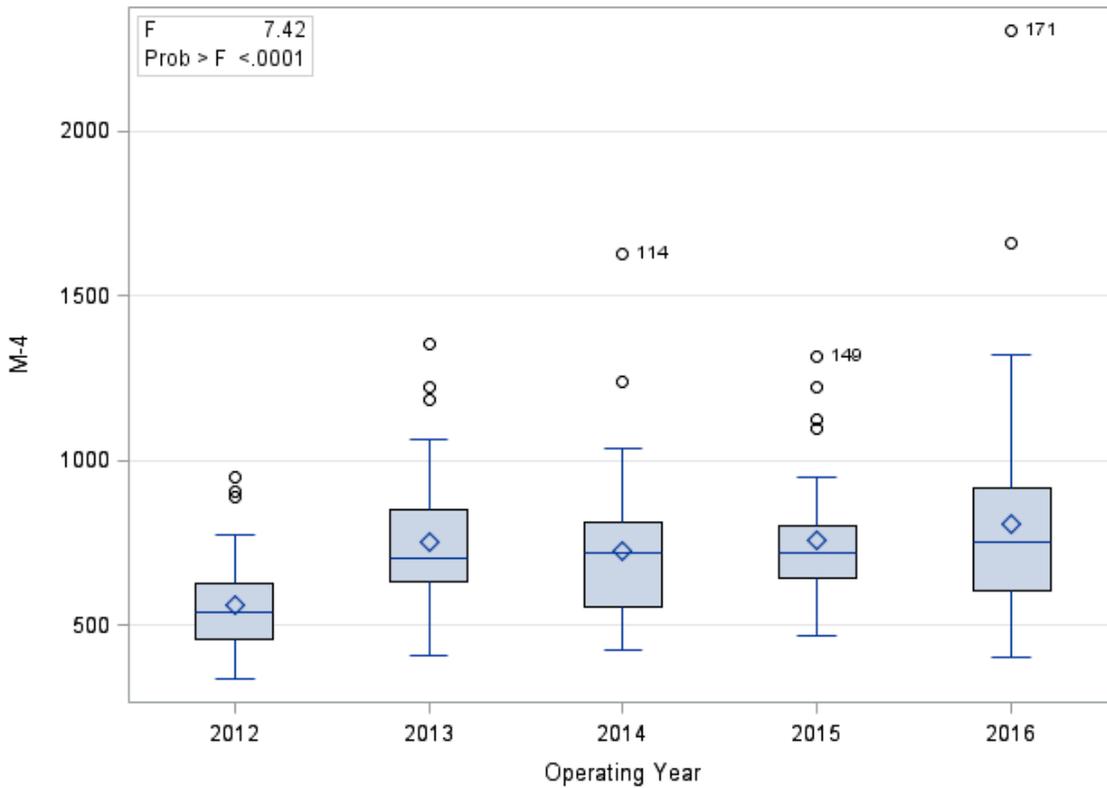


Figure E.9: ERCOT Frequency Response Distribution by Operating Year 2012–2015

Québec Interconnection

Table E.7 and **Figure E.10** illustrate year-to-year changes in the average and median FR as well as in its variation. There were no frequency events with FR below IFRO in 2012–2016.

Table E.7: Sample Statistics for Quebec Interconnection

Operating Year (OY)	Number of Events	Mean of Frequency Response	Standard Dev. of Frequency Response	Median	Minimum	Maximum	IFRO for the OY	Number of Events with FR Below the IFRO
2012–2016	171	612.9	233.5	545.9	288.3	1900.0	N/A	0
2012	25	689.8	299.1	635.0	370.8	1673.6	179	0
2013	35	624.1	187.5	596.3	389.1	1227.8	179	0
2014	33	555.5	236.0	468.8	288.3	1230.6	180	0
2015	29	586.2	190.1	531.8	320.1	1167.4	183	0
2016	49	620.0	243.7	543.8	334.5	1900.0	179	0

Figure E.10 shows the box plot of the annual distribution of the Québec Interconnection FR.

Fisher’s Least Significant Difference test found only one statistically significant change in the mean FR; a decrease in 2014 vs. 2012. In the 2015 and 2016 operating years the mean FR consistently but not significantly increased. The Wilcoxon test showed that after the lowest median value in 2014, the 2015 and 2016 medians consistently

increased with the 2016 being statistically significantly greater than in 2014. Finally, tests for homogeneity of variance detected a statistically significant increase in the 2016 variance compared with 2015. For 2016 M4 frequency events the lowest frequency response of 334 MW/0.1Hz occurred during a loss-of-load event and was 86.6 percent above the IFRO with the event resulting in a C point frequency of 60.510 Hz from a starting frequency of 59.975 Hz.

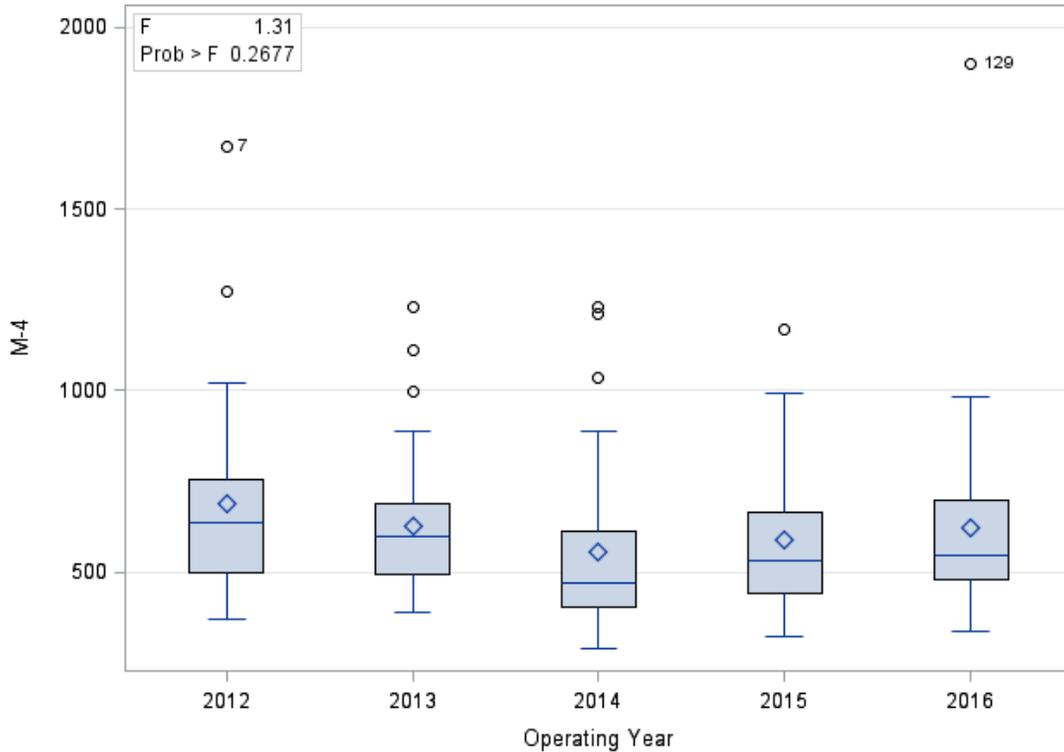


Figure E.10: Québec Interconnection Frequency Response Distribution by Operating Year 2012–2016

Western Interconnection

Table E.8 lists the average and median FR as well as in its variation. Over the five years, there were two frequency events with FR below IFRO (2013 and 2014).

Table E.8: Sample Statistics for Western Interconnection

Operating Year (OY)	Number of Events	Mean of Frequency Response	Standard Dev. of Frequency Response	Median	Minimum	Maximum	IFRO for the OY	Number of Events with FR Below the IFRO
2012–2016	103	1,436.7	498.4	1,349.8	821.9	4,368.4	N/A	2
2012	5	1,692.2	978.1	1,267.0	1,184.1	3,439.7	840	0
2013	13	1,373.6	251.0	1,463.1	821.9	1,645.0	840	1
2014	17	1,288.9	228.1	1,265.6	905.0	1,743.2	949	1
2015	21	1,360.7	269.4	1,348.5	1,007.6	2,098.8	906	0
2016	47	1,544.6	672.7	1,400.0	901.7	4,368.4	858	0

Figure E.11 shows the box plot of the annual distribution of the Western Interconnection FR. The lowest 2016 IFRM of 902 MW/0.1 Hz occurred for an event at approximately 2:15 a.m. in April. Frequency responsive resource dispatch was low during this light load period.

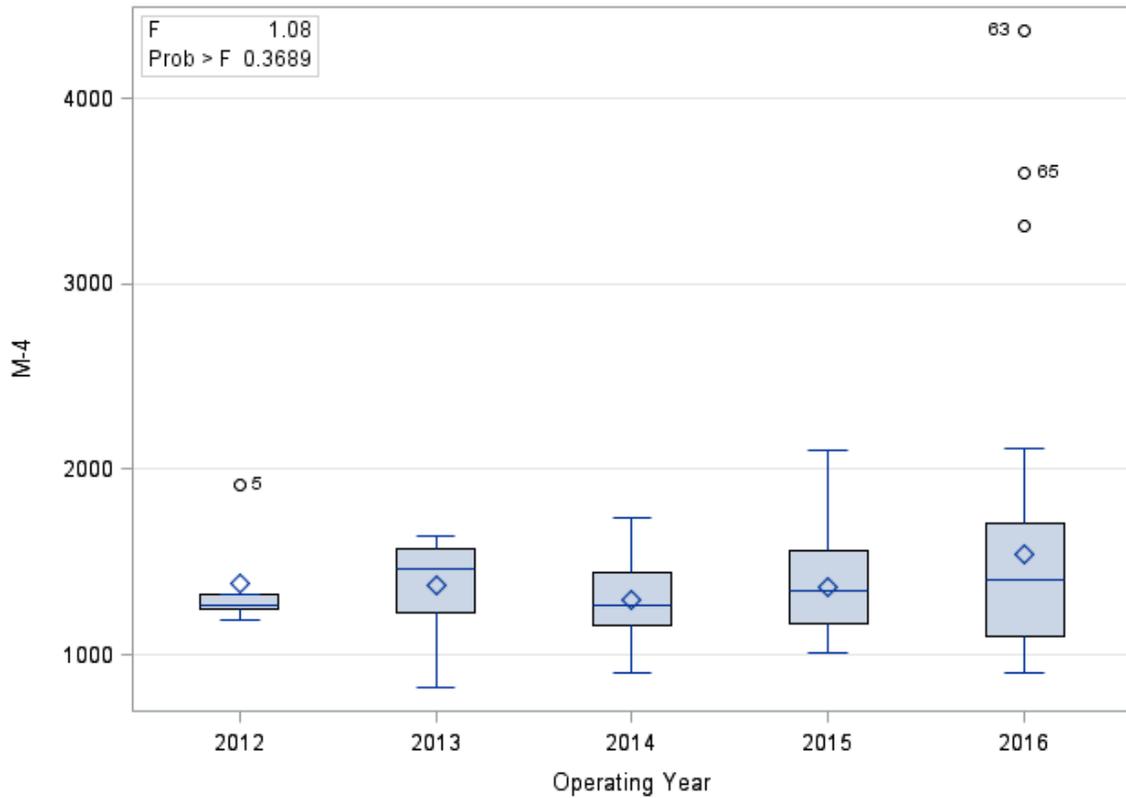


Figure E.11: Western Interconnection Frequency Response Distribution by Year 2012–2016

There was a statistically significant increase in the expected FR in 2016 versus 2014. The 2016 median FR was numerically higher than in 2014 and 2015. However, the 2016 variance also statistically significantly increased compared with both 2014 and 2015 (the 2012 and 2013 data sets were too small for a valid statistical inference). For 2016 frequency events, the minimum frequency response of 902 MW/0.1Hz was 5.1 percent above the IFRO with the event, resulting in a C point frequency nadir within 438 mHz of the interconnection first step UFLS setting from a starting frequency of 60.037 Hz.

Interconnection Frequency Response: Analysis of Distribution

Eastern Interconnection

Figure E.12 shows the histogram of the Eastern Interconnection FR for the 2012–2016 operating years based on the 173 observations of M-4. This is a right-skewed distribution with the median of 2,329.8 MW/0.1 Hz, the mean of 2,456.7 MW/0.1 Hz, and the standard deviation of 628.7 MW/0.1 Hz.

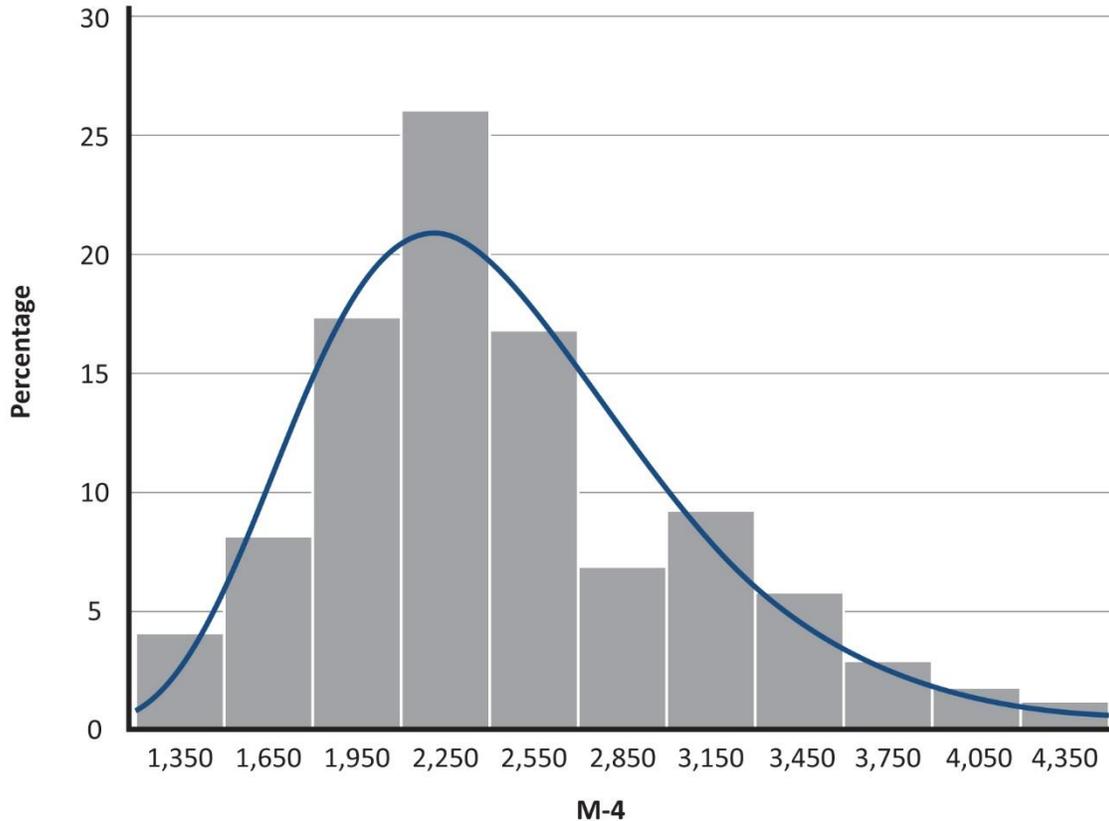


Figure E.12: Histogram of the Eastern Interconnection Frequency Response 2012–2016

Kolmogorov-Smirnov, Cramer-von Mises, and Anderson-Darling Goodness-of-Fit tests varied in conclusions: Kolmogorov-Smirnov and Anderson-Darling tests showed that a lognormal distribution can be an appropriate approximation for the five year Eastern Interconnection FR distribution (p-values of 0.13 and 0.06 point out to a not very good fit) while Cramer-von Mises test resulted in rejection of the null hypothesis on the lognormality of the distribution. No other table distribution fit the Eastern FR data.

The parameters of this lognormal distribution are as follows: the threshold = 672.0, the scale = 7.6, and the shape = 0.28. The probability density function of the fitted distribution is shown in Figure E.12 as a green curve.

ERCOT Interconnection

Figure E.13 shows the histogram of the ERCOT Interconnection FR for the 2012–2016 operating years based on the 203 observations of M-4. This is a right-skewed distribution with the median of 688.73 MW/0.1 Hz, the mean of 718.95 MW/0.1 Hz and the standard deviation of 247.72 MW/0.1 Hz.

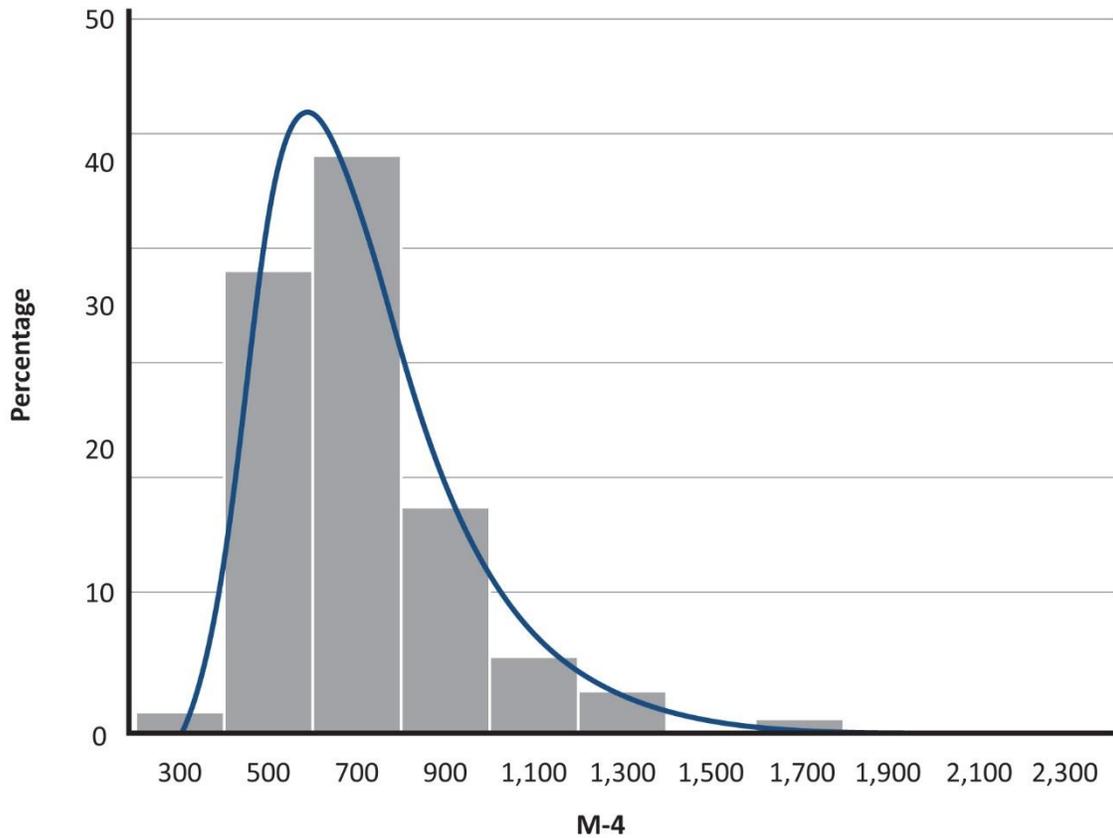


Figure E.13: Histogram of the ERCOT Interconnection Frequency Response 2012–2016

The Kolmogorov-Smirnov, Cramer-von Mises, and Anderson-Darling Goodness-of-Fit tests showed that a lognormal distribution can be a good approximation for the ERCOT FR distribution for the four years (p-values are greater than 0.25, 0.13 and 0.17, respectively). The parameters of this lognormal distribution are as follows: the threshold = 225.6, the scale = 6.1, and the shape = 0.46. The probability density function of the fitted distribution is shown in [Figure E.13](#) as a green curve.

Québec Interconnection

[Figure E.14](#) shows the histogram of the Québec Interconnection FR for the 2012–2016 operating years based on the 171 observations of M-4. This is a right-skewed distribution with the median of 545.9 MW/0.1 Hz, the mean of 612.9 MW/0.1 Hz, and the standard deviation of 233.5 MW/0.1 Hz.

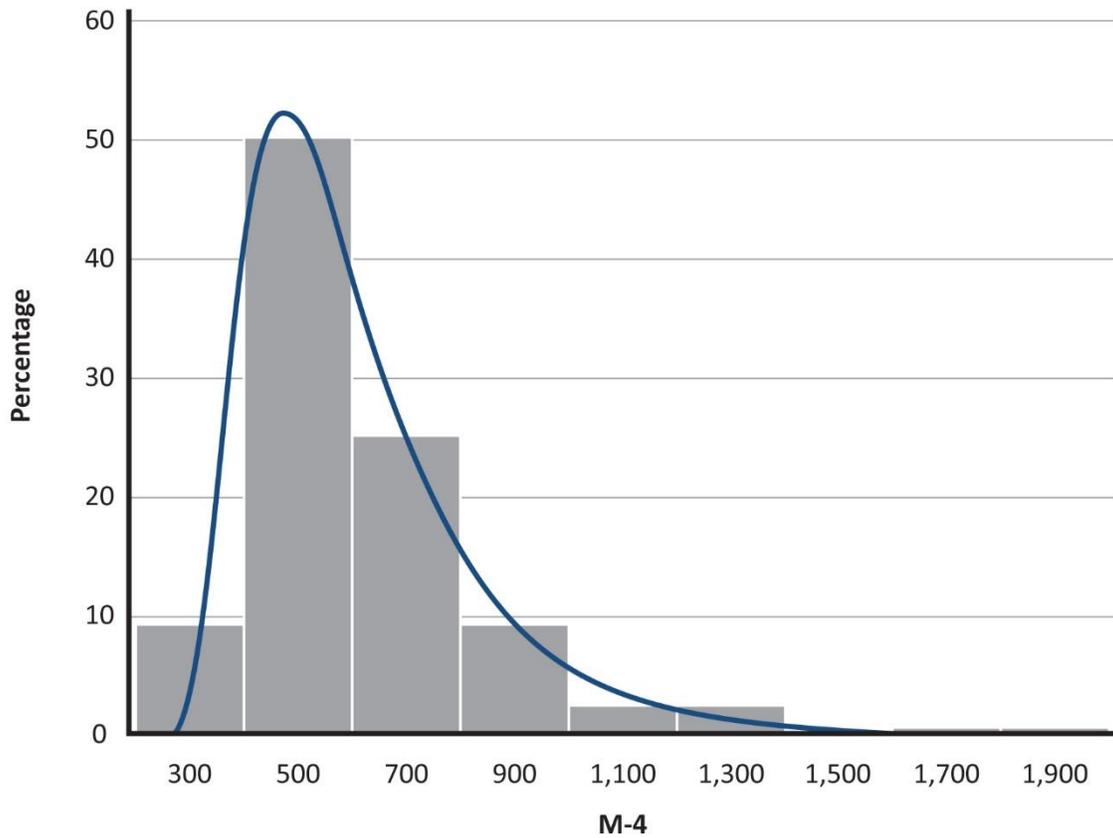


Figure E.14: Histogram of the Québec Interconnection Frequency Response 2012–2016

Kolmogorov-Smirnov, Cramer-von Mises, and Anderson-Darling Goodness-of-Fit tests showed that a lognormal distribution can be a good approximation for the Québec Interconnection FR distribution for the five years (all p-values are greater than 0.25). The parameters of this lognormal distribution are as follows: the threshold = 235.2, the scale = 5.8, and the shape = 0.55. The probability density function of the fitted distribution is shown in [Figure E.14](#) as a green curve.

Western Interconnection

[Figure E.15](#) shows the histogram of the Western Interconnection FR for the 2012–2016 operating years based on the 103 observations of M-4. This is a right-skewed distribution with the median of 1349.8 MW/0.1 Hz, the mean of 1436.7 MW/0.1 Hz, and the standard deviation of 498.4 MW/0.1 Hz.

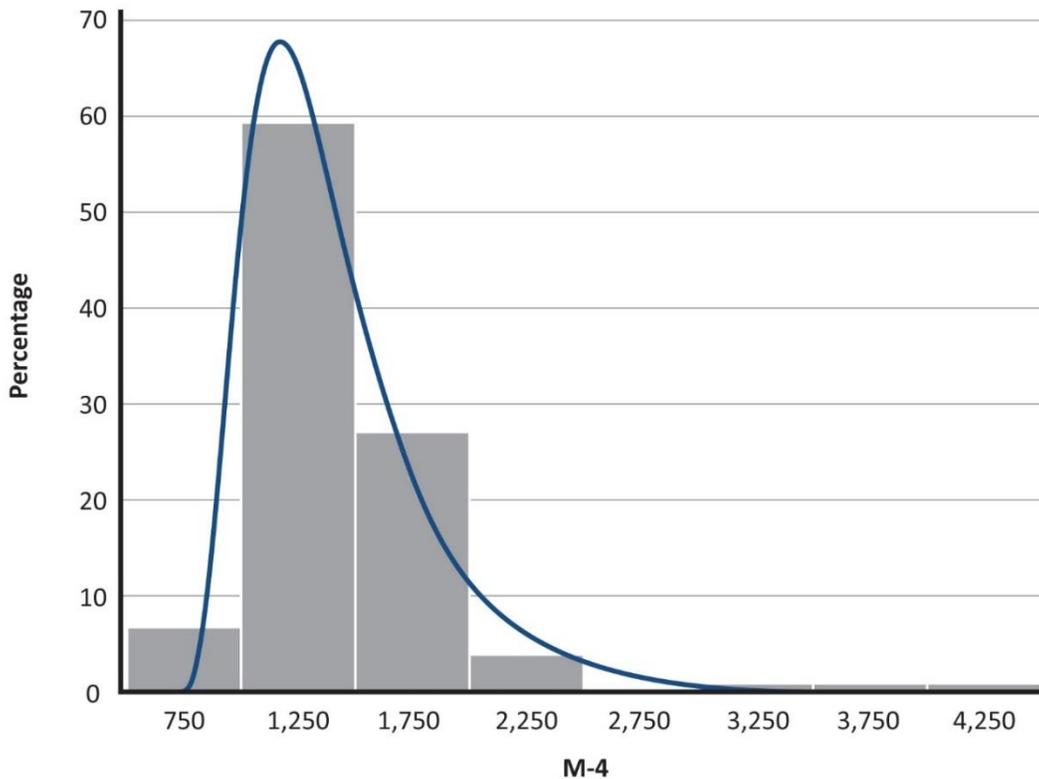


Figure E.15: Histogram of the Western Interconnection Frequency Response 2012–2016

Kolmogorov-Smirnov, Cramer-von Mises, and Anderson-Darling Goodness-of-Fit tests varied in conclusions: the first two tests showed that a lognormal distribution can be an appropriate approximation for the five-year Western Interconnection FR distribution (p-values of 0.12 and 0.19 point out to a not very good fit, partly due to the three 2016 upper outliers as seen in [Figure E.11](#)) while Anderson-Darling test resulted in rejection of the null hypothesis on the lognormality of the distribution (p-value=0.06). No other table distribution fit the Western FR data.

The parameters of the lognormal distribution are as follows: the threshold = 699.8, the scale = 6.5, and the shape = 0.54. The probability density function of the fitted lognormal distribution is shown in [Figure E.15](#) as a green curve.

Explanatory Variables for Frequency Response and Multiple Regression

Explanatory Variables

In the 2013–2016 *State of Reliability* reports, NERC staff evaluated how specific indicators could be tied to severity of frequency deviation events. In 2016, a set of explanatory variables that might affect the interconnection FR has been extended to 10 variables. This year, the renewable generation is added by source for all interconnections except the Eastern Interconnection. The selected variables are neither exhaustive nor pair-wise uncorrelated, and some pairs are strongly correlated; however, all are included as candidates to avoid the loss of an important contributor to the FR variability. First, the frequency response and explanatory variables are tested for a significant correlation (positive or negative); if a significant correlation is found, numerical estimates are provided of the explanatory variable impact to the FR. Then a multiple (i.e., multivariate) regression model, describing the frequency response with these explanatory variables as regressors, is built for each interconnection. Model selection methods help ensure the removal of highly correlated regressors and run multicollinearity diagnostics

(variance inflation diagnostics) for a multiple regression model selected. The explanatory variables included in this study are as follows:

Time: A moment in time (year, month, day, hour, minute, second) when an FR event happened. Time is measured in seconds elapsed between midnight of January 1, 1960 (the time origin for the date format in SAS), and the time of a corresponding FR event. This is used to determine trends over the study period.

Winter (Indicator Function): Defined as one for FR events that occur from December through February, and zero otherwise.

Spring (Indicator Function): Defined as one for FR events that occur from March through May, and zero otherwise.

Summer (Indicator Function): Defined as one for FR events that occur from June through August, and zero otherwise.

Fall (Indicator Function): Defined as one for FR events that occur from September through November, and zero otherwise.

On-peak Hours (Indicator Function) Defined as one for FR events that occurred during on-peak hours, and zero otherwise. On-peak hours are designated as follows: Monday to Saturday from 0700–2200 (Central Time) excluding six holidays: New Year’s Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, and Christmas Day.

Predisturbance Frequency A: Value A as shown in [Figure E.3](#) (measured in Hz).

Margin = C-UFLS: Difference between an event nadir, Point C, as shown in [Figure E.3](#) and the UFLS for a given interconnection. Measured in Hz. The UFLS values are listed in [Table E.9](#).

Table E.9: Underfrequency Load Shed	
Interconnection	Highest UFLS Trip Frequency
Eastern	59.5 Hz
ERCOT	59.3 Hz
Québec	58.5 Hz
Western	59.5 Hz

Interconnection Load Level: Measured in megawatts.

Interconnection Load Change by Hour: Difference between interconnection load at the end of the hour and at the beginning of the hour during which the frequency event occurred. Measured in megawatts.

Renewable Generation by Type: ERCOT provided the 2012–2016 hourly data for wind generation load. Note that wind is the only significant renewable source in ERCOT with the average hourly generation of about 4600 MW in 2015 (for comparison, solar generation is still less than 200 MW total installed capacity and hydroelectric generation is even smaller).

The Québec Interconnection provided the 2013–2016 hourly data for wind generation load.

WECC provided the 2013–2015 hourly data for renewable generation load level in the WI by generation type (Hydro, Wind, and Solar).

Data Sets: Some datasets (Interconnection load for the EI and the WI, Wind Load for ERCOT and the WI, Hydro and Solar loads) are not available for the five-year range for the 2012–2016 operating years. In such cases, the correlation between FR and this explanatory variable is calculated based on the available data. Even complete five-year data sets have insufficient sizes for a good explanatory and predictive model, which requires estimates of big number of parameters. An adequate model for each interconnection can only come with an annual increase of the FR data sets.

Summary of Correlation Analysis

For each interconnection, results of the correlation and a single regression analysis are shown in [Table E.12](#), [Table E.15](#), [Table E.18](#) and [Table E.21](#) and explained in details in the respective sections below. The explanatory variables are ranked from highest Pearson’s coefficient of determination to the smallest; the coefficient indicates the explanatory power of an explanatory variable for the frequency response. Summary [Table E.10](#) lists the ranks of statistically significant¹³⁶ variables for frequency response in each interconnection. In [Table E.10](#), the “Positive” indicates a statistically significant positive correlation, “Negative” indicates a statistically significant negative correlation, and a dash indicates no statistically significant linear relation.

Table E.10: Observation Summary				
Explanatory Variable	Eastern	ERCOT	Québec	Western
Time	-	2 (positive)	-	-
Winter	-	6 (negative)	3 (positive)	-
Spring	3 (negative)	-	4 (positive)	4 (positive)
Summer	4 (positive)	5 (positive)	5 (negative)	-
Fall	-	-	7 (negative)	-
Predisturbance Frequency A (Hz)	1 (negative)	1 (negative)	6 (negative)	2 (negative)
Margin = C-UFLS (Hz)	2 (negative)	-	2 (positive)	-
On-Peak Hours	-	-	-	-
Interconnection Load	-	4 (positive)	1 (positive)	1 (positive)
Interconnection Load Change by Hour	-	-	-	-
Wind Load	No data	3 (positive)	-	-
Hydro Load	No data	No data	No data	3 (positive)
Solar Load	No data	No data	No data	-

A statistically significant positive correlation between time and FR confirms an increasing trend for FR in the ERCOT Interconnection. Predisturbance Frequency has a statistically significant impact to FR in all the interconnections—the higher A the lower FR. Low frequency events with a starting frequency above 60 Hz (Value A) tend to have smaller FR since it is less likely that frequency will drop below the governor deadband setting. Interconnection load is significantly and positively correlated with FR in all interconnections except the EI. Among interconnections with renewable generation data available, Hydro load in the WI and Wind load in ERCOT positively and statistically significantly affect the respective FR.

¹³⁶ At the significance level 0.1.

For each interconnection there is found at least one season with statistically different expected FR than the other seasons combined. Winter events have on average smaller FR than other seasons in ERCOT but greater FR than other seasons in Québec. Spring events have on average smaller FR than other seasons in the EI but greater FR than other seasons in the Québec Interconnection (QI) and the WI. Summer events have on average smaller FR than other seasons in the QI but greater FR than other seasons in the EI and ERCOT. Finally, fall events have on average smaller FR than other seasons in the QI.

Margin = C-UFLS is statistically significantly correlated with FR in the EI and the QI; however, in the QI the correlation is positive (the higher Margin the higher FR) while in the EI the correlation is negative.

Other observations from the comparative analysis by interconnection are as follows:

- As expected with larger datasets, the statistical significance of the results and the explanatory power of regressors improve. However, to build good explanatory and predictive models of frequency response with multiple explanatory variables, more years of data and possibly additional variables are needed.
- The majority of the events occurs during on-peak hours, ranging from 57 percent in the WI to 66 percent in the QI.
- In the EI, 44 percent of events start with Predisturbance Frequency A<60 Hz while the other interconnections majority of events start with A>60 Hz (54 percent in ERCOT and the QI, and 57 percent in the WI).
- In the QI, more events occur when the Interconnection load level decreases, and more events occur in the other interconnections when the load level increases.

More details on the correlation analysis and multivariate models by Interconnection are provided in the following information.

Eastern Interconnection: Correlation Analysis and Multivariate Model

Descriptive statistics for the 10 explanatory variables and the Eastern Interconnection FR are listed in Table E.11.

Table E.11: Descriptive Statistics: Eastern Interconnection						
Variable	N	Mean	Standard Dev.	Median	Minimum	Maximum
Time	173				12/1/2011	11/30/2016
Winter	173	0.21	0.41	0	0	1
Spring	173	0.32	0.47	0	0	1
Summer	173	0.21	0.41	0	0	1
Fall	173	0.25	0.44	0	0	1
Predisturbance Frequency A (Hz)	173	60.00	0.01	60.00	59.97	60.03
Margin = C-UFLS (Hz)	173	0.45	0.01	0.45	0.41	0.49
On-Peak Hours	173	0.65	0.48	1	0	1
Interconnection Load (MW)	118	341,334	58,385	333,204	229,029	496,521
Load Change by Hour (MW)	118	402	10,366	441	-32019	28,611
Frequency Response	173	2,457	629	2,330	1,253	4,307

Interconnection load and interconnection load change by hour data are available for the 118 FR events that occurred from 2012–2015 calendar years. Other data are available for all 173 events.

The correlation and a single regression analysis result in the hierarchy of the explanatory variables for the Eastern Interconnection FR as shown in **Table E.12**. The table lists p-values of the test on the significance of correlation between each explanatory variable and FR. If p-value is smaller than 0.1, the correlation is statistically significant at the 0.1 significance level. For such a variable, the value of a coefficient of determination R^2 in the last column indicates the percentage in variability of the FR data that can be explained by variability of this explanatory variable.

Table E.12: Correlation and Regression Analysis: Eastern Interconnection			
Explanatory Variable	Correlation with FR	P-value	R² If Statistically Significant¹³⁷
Predisturbance Frequency A (Hz)	-0.55	<.0001	30.7%
Margin = C-UFLS (Hz)	-0.35	<.0001	12.2%
Spring	-0.19	0.013	3.6%
Summer	0.18	0.016	3.3%
Time	0.12	0.104	N/A
Load Change by Hour (MW)	0.08	0.380	N/A
Interconnection Load (MW)	0.08	0.399	N/A
Fall	0.06	0.423	N/A
On-Peak Hours	-0.05	0.497	N/A
Winter	-0.03	0.673	N/A

Out of the 10 explanatory variables, four have a statistically significant correlation with the Eastern Interconnection FR. Predisturbance Frequency A has the strongest correlation with and the greatest explanatory power (30.7 percent) for the FR. Predisturbance Frequency and Margin are negatively correlated with FR. Thus, events with higher A have smaller expected FR: on average, the EI frequency response decreases by 309.3 MW/0.1 Hz as A increases by 10 mHz. Similarly, events with larger Margin (and therefore higher nadir C) have statistically significantly smaller expected FR: on average, FR decreases by 189.1 MW/0.1 Hz as Margin increases by 10 mHz. Note that A and Margin are not independent variables: there is a statistically significant positive correlation of 0.70 between them (p-value of the test of the significance of correlation <0.0001).

Next, Indicator of spring has a significant negative correlation with FR, which means that on average spring events have a statistically significantly smaller FR than the other seasons (2283 MW/0.1 Hz versus 2538 MW/0.1 Hz); they also have a larger variability (FR variance). Finally, summer has a significant positive correlation with FR, which means that on average summer events have a statistically significantly higher FR than the other seasons (2676 MW/0.1 Hz versus 2397 MW/0.1 Hz); their variance is similar to events for the other seasons. The remaining six variables do not have a statistically significant linear relationship with FR.

Since both Interconnection load and Load Change by Hour are not significantly correlated with FR, these two variables are excluded from the multiple regression model to keep the sample size relatively large (173 observations versus 118). The step-wise selection and backward elimination algorithms result in a multiple

¹³⁷ At the significance level 0.1

regression model that connects the 2012–2016 Eastern Interconnection FR with Predisturbance Frequency A and spring (the other variables are not selected or were eliminated by the algorithms).¹³⁸ The model’s coefficients are listed in **Table E.13**.

Variable	DF	Parameter Estimate	Standard Error	t-value	p-value	Variance Inflation Value
Intercept	1	1877785	207283	9.06	<.0001	0.00
Spring	1	-276.9	83.3	-3.32	0.0011	1.000082
Predisturbance Frequency A (Hz)	1	-31255	3455	-9.05	<.0001	1.000082

The adjusted coefficient of the determination $adj R^2$ of the model is 34.2 percent; the model is highly statistically significant ($p < 0.0001$). The random error has a zero mean and the sample deviation σ of 510 MW/0.1 Hz. Variance inflation factors for the regressors are very close to 1, which confirms an acceptable level of multicollinearity that does not affect a general applicability of the model. The parameter estimates, or the coefficients for the regressors, indicate how change in a regressor value impacts FR. Note that the regressors in the final model are not correlated: t-test confirms that the spring events and the other seasons combined have statistically similar expected A and the variance of A.

ERCOT: Correlation Analysis and Multivariate Model

Descriptive statistics for the 11 explanatory variables (including Hourly Wind Load) and the ERCOT Interconnection FR are listed in **Table E.14**.

Variable	N	Mean	Standard Dev.	Median	Minimum	Maximum
Time	203				12/1/2011	11/30/2016
Winter	203	0.20	0.40	0	0	1
Spring	203	0.28	0.45	0	0	1
Summer	203	0.30	0.46	0	0	1
Fall	203	0.23	0.42	0	0	1
Predisturbance Frequency A (Hz)	203	60.00	0.02	60.00	59.95	60.03
Margin = C-UFLS (Hz)	203	0.55	0.05	0.56	0.41	0.82
On-Peak Hours	203	0.64	0.48	1	0	1
Interconnection Load (MW)	203	42,153	10,438	40,015	23,905	67,209
Load Change by Hour (MW)	203	92	1,760	8	-4937	4,601
Wind Load (MW)	203	3,834	2,634	3,057	81	13,865
Frequency Response	203	719	248	689	337	2,304

¹³⁸ Regressors in the final model have p-values not exceeding 0.1

For all variables, the data is available for the 203 FR events that occurred from 2012–2016 operating years. The correlation and a single-regression analysis result in the hierarchy of the explanatory variables for the ERCOT Interconnection FR shown in **Table E.15**. The table lists p-values of the test on the significance of correlation between each explanatory variable and FR. If p-value is smaller than 0.1, the correlation is statistically significant at the 0.1 significance level. For such a variable, the value of a coefficient of determination R^2 in the last column indicates the percentage in variability of the FR data that can be explained by variability of this explanatory variable.

Table E.15: Correlation and Regression Analysis: ERCOT Interconnection			
Explanatory Variable	Correlation with FR	P-value	R^2 (If Statistically Significant¹³⁹)
Predisturbance Frequency A (Hz)	-0.362	<.0001	13.1%
Time	0.323	<.0001	10.5%
Wind Load (MW)	0.219	0.002	4.8%
Interconnection Load (MW)	0.135	0.055	1.8%
Summer	0.132	0.060	1.8%
Winter	-0.123	0.080	1.5%
Margin = C-UFLS (Hz)	-0.100	0.157	N/A
Spring	-0.078	0.271	N/A
On-Peak Hours	-0.073	0.303	N/A
Fall	0.055	0.436	N/A
Load Change by Hour (MW)	-0.015	0.833	N/A

Out of the 11 parameters, five are statistically significantly correlated with ERCOT’s FR. Predisturbance Frequency A has the strongest correlation with and the greatest explanatory power (13.1 percent) for the FR. A and FR are negatively correlated (the higher A the smaller expected FR). On average, the frequency response decreases by 36.3 MW/0.1 Hz as A increases by 10 mHz. Time and FR are positively correlated; on average, frequency response improves in time. The average rate of the FR increase over the 2012–2016 operating years is 4.3 MW/0.1 Hz a month.

Next, wind load and interconnection load are positively correlated with FR; it is noteworthy that the correlation of FR with Wind generation is stronger than with the overall load (almost 5 percent in the variability of ERCOT frequency response in 2012–2016 can be explained by variability in its wind generation) and that there is no significant correlation between wind and overall interconnection load during FR events. On average, a wind load increase of 1,000 MW corresponds to a frequency response increase of 25.7 MW/0.1 Hz, while an Interconnection load increase of 1,000 MW corresponds to a frequency response increase of 3.2 MW/0.1 Hz. Note that both wind generation and interconnection load significantly grew over the 2012–2016 operating years.

Last, indicators of summer and winter have a statistically significant correlation with the ERCOT FR. On average, summer events have a significantly higher FR than the other seasons combined (769 MW/0.1 Hz versus 698 MW/0.1 Hz); the summer events variance is similar to events from the other seasons. The indicator of winter has a negative correlation with FR, which means that winter events have smaller FR on average than the other seasons

¹³⁹At the significance level 0.1

(658 MW/0.1 Hz versus 734 MW/0.1 Hz); their variance is similar to events for the other seasons combined. The remaining six variables do not have a statistically significant¹⁴⁰ linear relationship with FR.

Both the step-wise selection algorithm and the forward selection algorithm result in a multiple regression model that connects the ERCOT Interconnection FR with time, Predisturbance Frequency A and Wind load (the other eight variables are not selected or were eliminated as regressors).¹⁴¹ The coefficients of the multiple model are listed in **Table E.16**.

Variable	DF	Parameter Estimate	Standard Error	t-value	p-value	Variance Inflation Value
Intercept	1	286,931	46,774	6.13	<.0001	0.00
Time	1	0.00000159	0.00	5.03	<.0001	1.07
Predisturbance Frequency A (Hz)	1	-4817	780	-6.17	<.0001	1.01
Wind Load	1	0.011	0.006	1.92	0.0569	1.07

The model’s adjusted coefficient of multiple determination adj R² is 25.4 percent (that is the model accounts for more than 25 percent of the ERCOT FR variability); the model is highly statistically significant (p < 0.0001). The random error has a zero mean and the sample deviation σ of 214 MW/0.1 Hz. Variance inflation factors for the regressors do not exceed four, and this confirms an acceptable level of multicollinearity that does not affect a general applicability of the model. The parameter estimates, or the coefficients for the regressors, indicate how change in a regressor value impacts FR.

Québec: Correlation Analysis and Multivariate Model

Descriptive statistics for the 11 explanatory variables and the Québec Interconnection FR are in **Table E.17**.

Variable	N	Mean	Standard Dev.	Median	Minimum	Maximum
Time	171				12/1/2011	11/30/2016
Winter	171	0.12	0.33	0	0	1
Spring	171	0.20	0.40	0	0	1
Summer	171	0.41	0.49	0	0	1
Fall	171	0.26	0.44	0	0	1
Predisturbance Frequency A (Hz)	171	60.00	0.02	60.00	59.94	60.06
Margin = C-UFLS (Hz)	171	1.19	0.45	1.07	0.29	2.28
On-Peak Hours	171	0.66	0.47	1	0	1
Interconnection Load (MW)	171	21,003	4,558	19,330	13,520	35,000
Load Change by Hour (MW)	171	2	711	-40	-2010	2,450

¹⁴⁰ At the significance level 0.1

¹⁴¹ Regressors in the final model have p-values not exceeding 0.1.

Table E.17: Descriptive Statistics - Québec Interconnection

Variable	N	Mean	Standard Dev.	Median	Minimum	Maximum
Wind Load (MW)	144	753	575	651	8	2,475
Frequency Response	171	613	234	546	288	1,900

The Wind generation hourly data are available for the 144 frequency response events that occurred from 2013–2016. Other data are available for all 171 events.

The correlation and a single-regression analysis result in the hierarchy of the explanatory variables for the Québec Interconnection FR shown in **Table E.18**. The table lists p-values of the test on the significance of correlation between each explanatory variable and FR. If p-value is smaller than 0.1, the correlation is statistically significant at the 0.1 significance level. For such a variable, the value of a coefficient of determination R^2 in the last column indicates the percentage in variability of the FR data that can be explained by variability of this explanatory variable.

Table E.18: Correlation and Regression Analysis: Québec Interconnection

Explanatory Variable	Correlation with FR	P-value	R^2 (If Statistically Significant) ¹⁴²
Interconnection Load (MW)	0.319	<.0001	10.2%
Margin = C-UFLS (Hz)	0.214	0.0049	4.6%
Winter	0.203	0.008	4.1%
Spring	0.195	0.010	3.8%
Summer	-0.164	0.032	2.7%
Predisturbance Frequency A (Hz)	-0.153	0.046	2.3%
Fall	-0.147	0.055	2.2%
Time	-0.125	0.105	N/A
On-Peak Hours	-0.081	0.295	N/A
Load Change by Hour (MW)	-0.078	0.309	N/A
Wind Load (MW)	0.055	0.509	N/A

Seven explanatory variables are statistically significantly correlated with FR. Interconnection load has the strongest correlation and the greatest explanatory power (10.2 percent) for the FR. The load level and FR are positively correlated (i.e., the higher interconnection load is during a frequency response event, the higher expected frequency response value of this event). On average, a load increase of 1,000 MW leads to a frequency response increase of 16.4 MW/0.1 Hz. The margin is positively correlated with FR: on average, a margin increase of 10 mHz corresponds to a FR increase of 1.1 MW/0.1 Hz.

All four seasons are statistically significantly correlated with FR. On average, winter and spring events have significantly higher frequency response than the other seasons combined (739 MW/0.1 Hz versus 595 MW/0.1 Hz

¹⁴² At the significance level 0.1

and 703 MW/0.1 Hz versus 590 MW/0.1 Hz, respectively). The spring events (unlike winter events) have significantly greater FR variance than the other seasons combined. Next, the summer and fall events have, on average, significantly smaller frequency response than the other seasons combined (567 MW/0.1 Hz versus 645 MW/0.1 Hz and 556 MW/0.1 Hz versus 633 MW/0.1 Hz, respectively) and significantly smaller FR variance than the other seasons. The main reason winter events have a higher FR is because winter is the peak usage season in the Québec Interconnection. More generator units are on-line; therefore, there is more inertia in the system, so it is more robust in responding to frequency changes in the winter (the highly significant positive correlation between variables winter and interconnection load also confirms this). Another observation is that only 12 percent of the Québec Interconnection events have occurred in winter.

Finally, A and FR are statistically significantly and negatively correlated; on average, frequency response decreases by 19.3 MW/0.1 Hz as A increases by 10 mHz. Note that unlike the EI, the QI events do not show a correlation between A and margin (p-value of the test on the significance of correlation is 0.42). The remaining four variables do not have a statistically significant¹⁴³ linear relationship with FR.

Since wind load is not significantly correlated with FR, and this variable is excluded from the multiple regression model to keep the sample size larger (171 observations versus 144). Both the step-wise selection algorithm and the backward elimination algorithm result in a multiple regression model that connects the Québec Interconnection FR with fall, Predisturbance Frequency A, margin and interconnection load (the other variables are not selected or were eliminated).¹⁴⁴ The coefficients of the multiple model are listed in **Table E.19**.

Table E.19: Coefficients of Multiple Model: Québec Interconnection						
Variable	DF	Parameter Estimate	Standard Error	t-value	p-value	Variance Inflation Value
Intercept	1	161,567	53,350.0	3.03	0.003	0
Fall	1	-97.55	37.2	-2.62	0.010	1.037
Predisturbance Frequency A (Hz)	1	-2690.1	889.2	-3.03	0.003	1.042
Margin = C-UFLS (Hz)	1	114.8	35.7	3.21	0.002	1.005
Interconnection Load (MW)	1	0.0163	0.0035	4.61	<.0001	1.002

The model’s adjusted coefficient of multiple determination adj R² is 19.0 percent (19 percent of the Québec Interconnection FR variability can be explained by the combined variability of these four parameters); the model is highly statistically significant (p<0.0001). The random error has a zero mean and a sample deviation σ of 210 MW/0.1 Hz. Variance inflation factors for the regressors do not exceed 1.05, which confirms an acceptable level of multicollinearity that does not affect a general applicability of the model. Variables of winter and summer bring little new information about variability of FR due to their high correlation with Interconnection Load; therefore, they become redundant and eliminated from the model. On the other hand, Predisturbance Frequency and Margin (and, thus, A and nadir C) are not significantly correlated and both stay in the final model.

Western Interconnection: Correlation Analysis and Multivariate Model

Descriptive statistics for the 13 explanatory variables (including wind, solar, and hydro loads by hour). The Western Interconnection FRs are listed in **Table E.20**.

¹⁴³ At the significance level 0.1.

¹⁴⁴ Regressors in the final model have p-values not exceeding 0.1.

Table E.20: Descriptive Statistics - Western Interconnection						
Variable	N	Mean	Standard Dev.	Median	Minimum	Maximum
Time	103				12/1/2011	11/30/2016
Winter	103	0.16	0.36	0	0	1
Spring	103	0.23	0.42	0	0	1
Summer	103	0.28	0.45	0	0	1
Fall	103	0.33	0.47	0	0	1
Predisturbance Frequency A (Hz)	103	60.00	0.02	60.00	59.97	60.05
Margin = C-UFLS (Hz)	103	0.40	0.04	0.41	0.17	0.46
On-Peak Hours	103	0.57	0.50	1	0	1
Interconnection Load (MW)	56	89,539	15,248	87,355	65,733	146,424
Load Change by Hour (MW)	56	1571	3331	1929	-6311	6404
Wind Load	51	4,695	2,627	3,735	1,125	11,339
Hydro Load	51	30,174	6,557	31,562	16,405	43,105
Solar Load	51	2,046	1,959	1,699	0	6,033
Frequency Response	103	1,437	498	1,350	822	4,368

Interconnection load and interconnection load change by hour data are available for the 56 frequency response events that occurred during the 2012–2015 years. Renewable generation (Wind, Hydro, and Solar Load) is available by source for the 2013–2015 events. Other data is available for all 103 events.

The correlation and a single-regression analysis result in the hierarchy of the explanatory variables for the Western Interconnection FR are shown in [Table E.21](#). The table lists p-values of the test on the significance of correlation between each explanatory variable and FR. If the p-value is smaller than 0.1, the correlation is statistically significant at the 0.1 significance level. For such a variable, the value of a coefficient of determination R^2 in the last column indicates the percentage in variability of the FR data that can be explained by variability of this explanatory variable.

Table E21: Correlation and Regression Analysis: Western Interconnection			
Explanatory Variable	Correlation with FR	P-value	R² (If Statistically Significant¹⁴⁵)
Interconnection Load (MW)	0.361	0.006	13.0%
Predisturbance Frequency A (Hz)	-0.340	0.001	11.5%
Hydro Load	0.303	0.031	9.2%
Spring	0.191	0.053	3.7%
Solar Load	0.163	0.252	N/A
Load Change by Hour (MW)	0.148	0.277	N/A
Fall	-0.127	0.202	N/A
Time	0.125	0.209	N/A
On-Peak Hours	0.112	0.261	N/A
Summer	-0.028	0.782	N/A
Winter	-0.024	0.807	N/A
Wind Load	0.015	0.917	N/A
Margin = C-UFLS (Hz)	-0.006	0.952	N/A

Four explanatory variables are statistically significantly correlated with FR. Interconnection Load has the strongest correlation and the greatest explanatory power (13 percent) for the FR. The load level and FR are positively correlated (i.e., the higher Interconnection Load is during a frequency response event—the higher expected frequency response of this event). On average, a load increase of 1,000 MW leads to a frequency response increase of 6.0 MW/0.1 Hz. Next, Predisturbance Frequency A and FR are statistically significantly and negatively correlated; on average, frequency response decreases by 105.0 MW/0.1 Hz as A increases by 10 mHz. Hydro generation is positively correlated with FR; on average, a hydro load increase of 1,000 MW leads to a frequency response increase of 11.6 MW/0.1 Hz. It is interesting to note that the Hydro load and the overall load for the WI events are not correlated (p-value of the test on the significance of correlation is 0.32).

Out of four seasons, only spring is statistically significantly correlated with FR. On average, the spring events have higher frequency response than the other seasons combined (1,609 MW/0.1 Hz versus 1,384 MW/0.1 Hz); they also have significantly greater FR variance than the other seasons combined. The remaining nine variables do not have a statistically significant¹⁴⁶ linear relationship with FR.

Even though five explanatory variables have smaller data size than the others, their exclusion from a multiple regression model do not improve the model (neither by increasing its explanatory power nor by reducing the error). Using all 13 variables as input regressors, the step-wise selection algorithm results in a multiple regression model that connects the Western Interconnection FR with interconnection load and indicator of on-peak hours (the other variables are not selected or were eliminated).¹⁴⁷ The coefficients of the multiple model are listed in [Table E.22](#).

¹⁴⁵ At the significance level 0.1.

¹⁴⁶ At the significance level 0.1.

¹⁴⁷ Regressors in the final model have p-values not exceeding 0.1.

Variable	DF	Parameter Estimate	Standard Error	t-value	p-value	Variance Inflation Value
Intercept	1	832.9	183.7	4.53	<.0001	0.00
On-Peak Hours	1	155.1	68.6	2.26	0.028	1.11
Interconnection Load (MW)	1	0.0046	0.0021	2	0.035	1.11

The adjusted coefficient of the determination $\text{adj } R^2$ of the model is 19.8 percent; the model is highly statistically significant ($p < 0.0001$). The random error has a zero mean and the sample deviation σ of 225 MW/0.1 Hz. Variance inflation factors for the regressors are close to 1, which confirms an acceptable level of multicollinearity that does not affect a general applicability of the model even though the two regressors are significantly correlated. Overall, the small sample size of the WI data does not allow the building of a good predictive model; it should be refined when more data becomes available

M-6 Disturbance Control Standard Failures

Background

This metric measures the ability of a BA or reserve sharing group (RSG) to balance resources and demand following a reportable disturbance, thereby returning the interconnection frequency to within defined limits; this could include the deployment of contingency reserves. The relative percent recovery of a BA's or RSG's area control error (ACE) provides an indication of performance for disturbances that are equal to or less than the most severe single contingency (MSSC). NERC Reliability Standard BAL-002-1¹⁴⁸ requires that a BA or RSG evaluate performance for all reportable disturbances and report findings to NERC on a quarterly basis.

M-7 Disturbance Control Events Greater than Most Severe Single Contingency (MSSC)

Background

This metric measures the ability of a BA or RSG to balance resources and demand following reportable disturbances that are greater than their MSSC. The results will help measure how much risk the system is exposed to during extreme contingencies and how often they occur. NERC Reliability Standard BAL-002-1 requires that a BA or RSG report all disturbance control standard (DCS) events and instances of nonrecovery to NERC, including events greater than MSSC.

Assessment for M-6 and M-7

Figure E.16 shows that the trend of M-6 DCS-reportable events is essentially unchanged in 2016 from 2013, 2014, and corrected 2015 data. **Table E.23** shows that in 2016, there was no M-6 DCS event for which there was less than 100 percent recovery within the determined period.

Figure E.16 also shows that the number of M-7 events were higher in 2016 than in 2015, although still considerably lower than in 2012, 2013, or 2014. There was one M-7 event in 2016 for which 100 percent recovery was not achieved within the required timeframe.

Based on the similar annual results over the last four years, M-6 is stable.

¹⁴⁸ <http://www.nerc.com/files/BAL-002-1.pdf>

Based on the improvement in both 2016 and 2015 relative to 2012–2014, M-7 is stable for the short term in the approved state achieved in 2015.

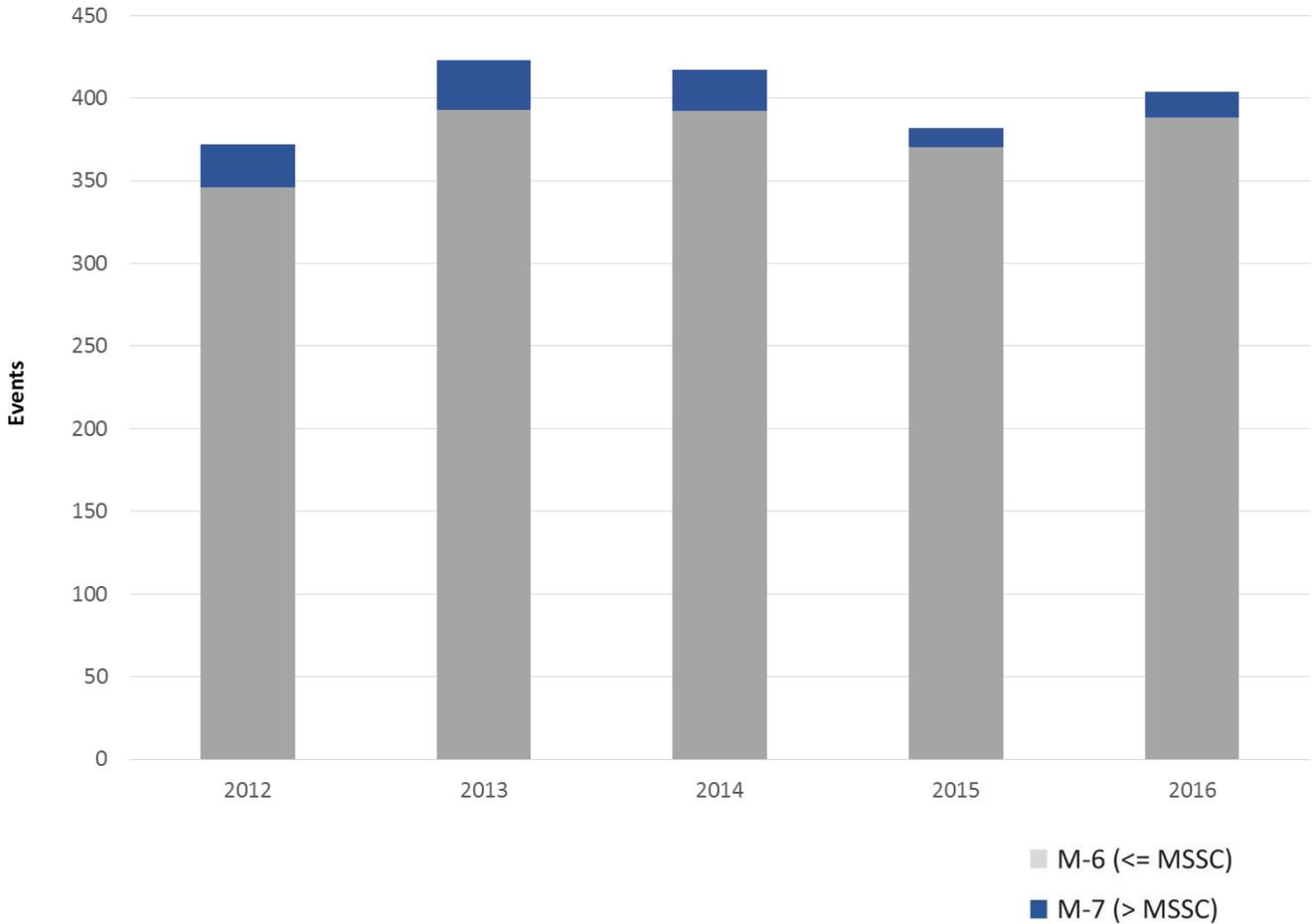


Figure E.16: M-6 & M-7 DCS Events

Table E.23: M-6 & M-7 DCS Events

YEAR	M-6 100% Recovery	M-6 < 100% Recovery	M-7 100% Recovery	M-7 < 100% Recovery
2012	346	0	26	2
2013	390	3	28	2
2014	392	0	25	0
2015	370	1	12	0
2016	388	0	15	1

M-8 Interconnection Reliability Operating Limit Exceedances

Background

This metric measures both the number of times and duration that an IROL is exceeded. An IROL is a SOL that, if violated, could lead to instability, uncontrolled separation, or cascading outages.¹⁴⁹ Each RC is required to operate

¹⁴⁹ T_v is the maximum time that an interconnection reliability operating limit can be violated before the risk to the interconnection or other RC area(s) becomes greater than acceptable. Each interconnection reliability operating limit's T_v shall be less than or equal to 30 minutes.

within IROL limits and minimize the duration of such exceedances. IROL exceedance data is reported in four duration intervals as shown in **Figures E.17** through **Figure E.19**.

Assessment

Figure E.17 demonstrates the performance for the EI from 2011–2016. The *State of Reliability 2015* described some changes in data reporting for two of the Regions in the EI that led to an increase in the number of exceedances in 2014. In 2015, the number of exceedances declined from 2014 levels. While the number of exceedances less than 10 mins increased a declining trend of exceedances greater than 10 mins can be seen. This may have signaled an increase in operating near an IROL limit but a decrease in time necessary to respond to operations outside of IROL limits. In 2016, the number of exceedances increased not only in the less than 10 mins range but also in the greater than 10 mins.

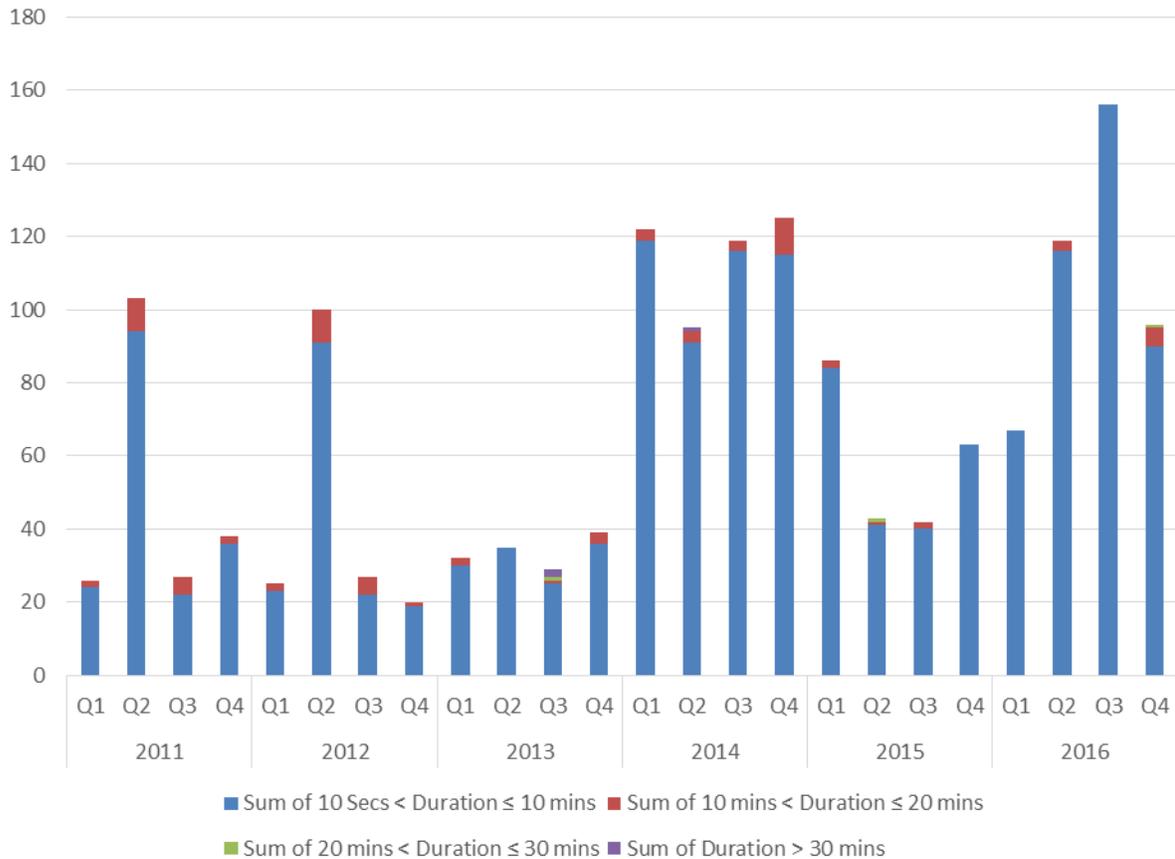


Figure E.17: Eastern Interconnection: IROL Exceedances

Figure E.18 demonstrates the performance of the ERCOT Interconnection from 2011-2016. The trend has been stable at no exceedances since the second quarter of 2013.

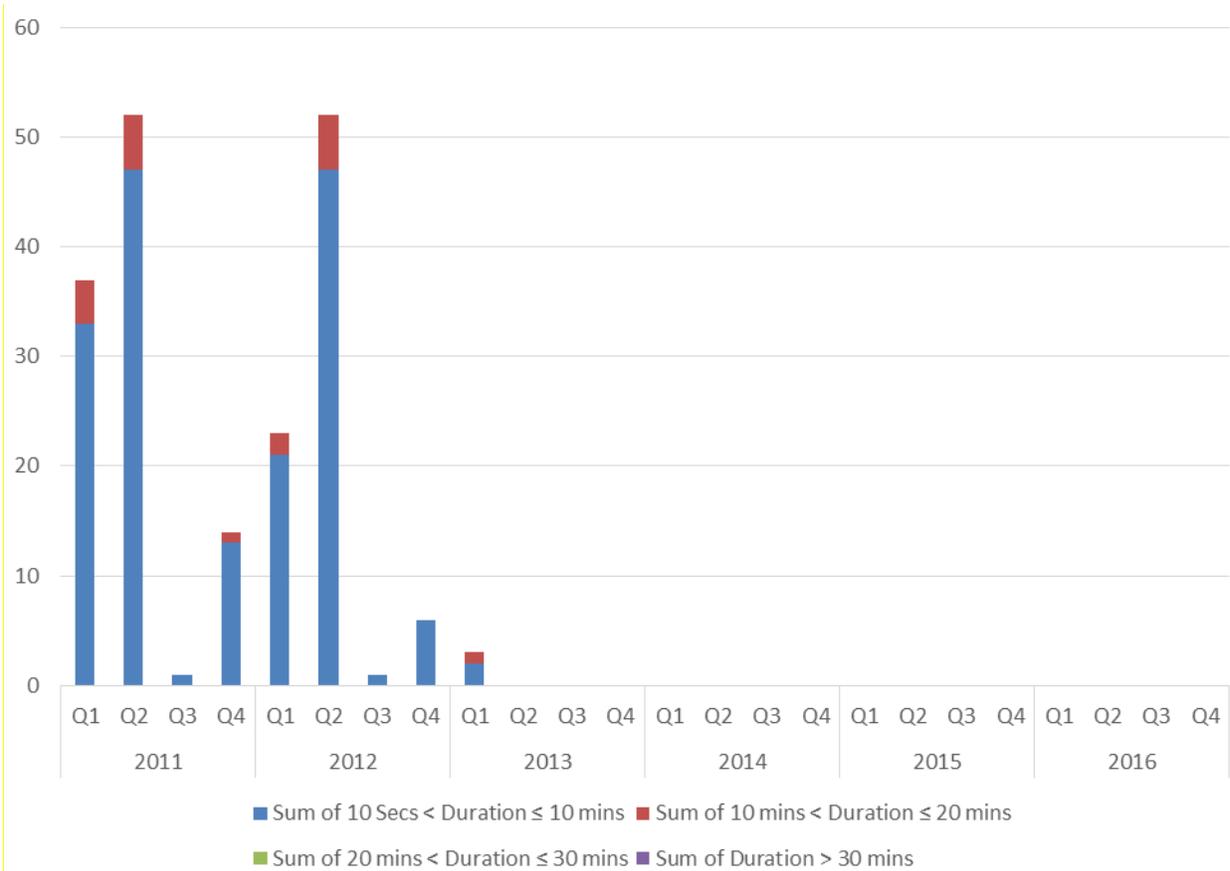


Figure E.18: ERCOT Interconnection: IROL Exceedances

Figure E.19 demonstrates performance for the Western Interconnection from 2011–2016. The *State of Reliability Report 2015* noted changes in data reporting for the Western Interconnection that led to the reporting of IROLs. Prior to 2014, only SOLs were reported. Since 2014, the trend has been stable with no IROL exceedances reported.

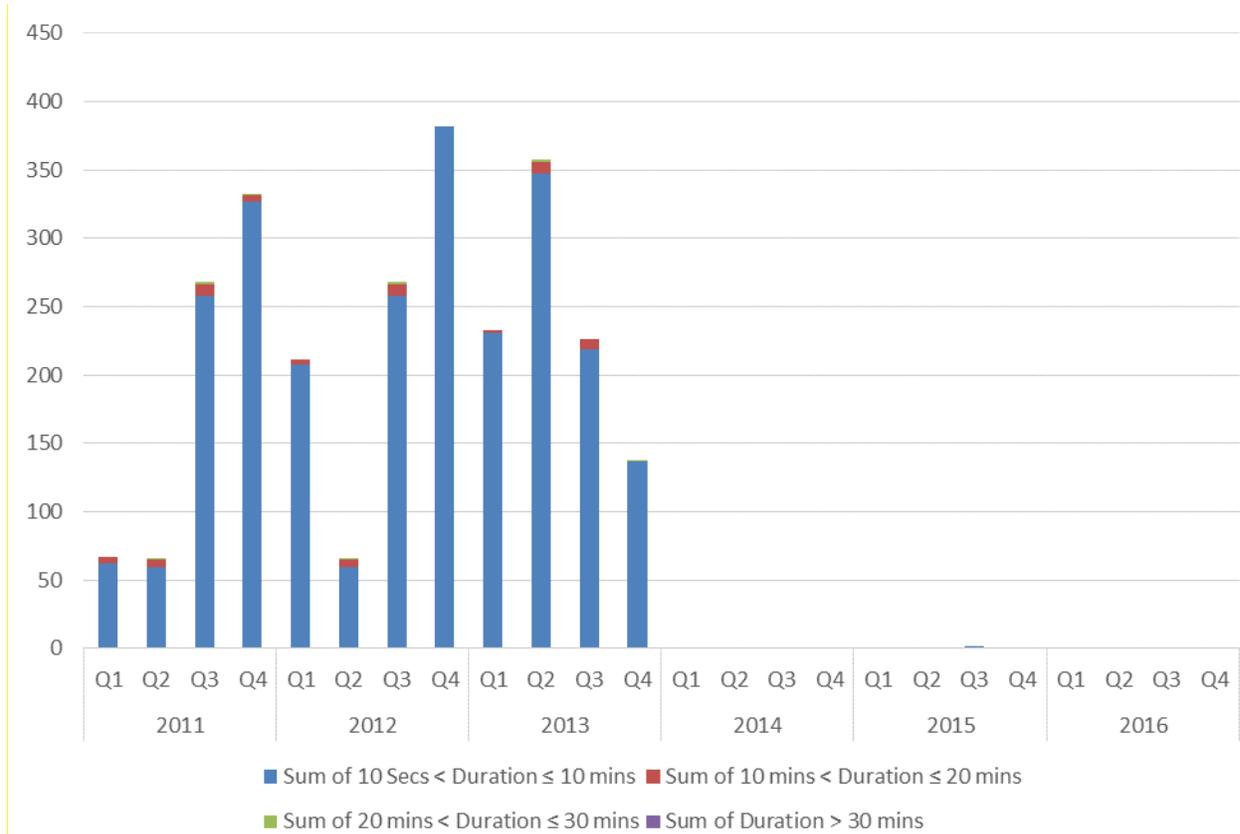


Figure E.19: Western Interconnection – SOL/IROL Exceedances

M-9 Correct Protection System Operations

Background

Protection system misoperations were identified as an area that required further analysis in past *State of Reliability* reports. The improvements to the data collection process, that the SPCS proposed, were implemented and have improved the accuracy of misoperation reporting. At the recommendation of the SPCS, the respective protection system subcommittees (within each RE) began misoperation analysis in early 2014 and have continued to conduct such analysis on an annual basis. In 2016, NERC updated to an online collection of data with updates and enhancements to the system expected in 2017.

Assessment

[Figure 4.4](#) shows the correct operations rate for NERC during the reporting period. Total protection system operations were first requested with fourth quarter 2012 misoperations data. This is to reflect the updated metric M-9 Correct Protection System Operations. The rate provides a consistent way to trend misoperations and to normalize for weather and other factors that can influence the count. Incremental improvements continue to be seen.

Figure E.20 shows the count of misoperations by month through the third quarter of 2016. The counts can show variability or similarity by year for each month and seasonal trends. For example, the chart shows higher numbers of misoperations in summer than the rest of the year.

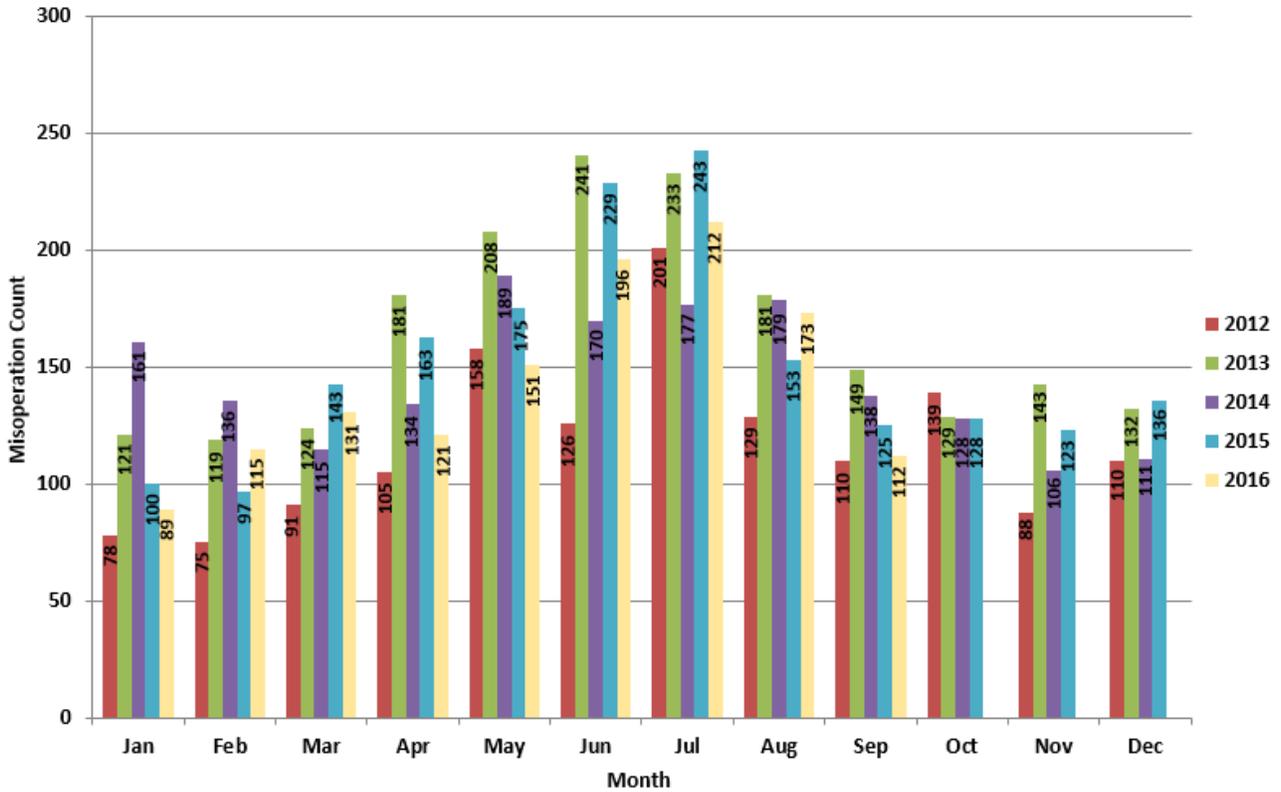


Figure E.20: Protection System Misoperations by Month (2Q 2012–3Q 2016)

Figure E.21 illustrates misoperations by cause code where the top three causes continue to be incorrect setting, logic, or design error; relay failures/malfunctions; and communication failure. These cause codes have consistently accounted for approximately 65 percent of all misoperations since data collection started in 2011. Recent reporting updates have broken down the single “Incorrect Setting, Logic, or Design Error” cause code into separate cause codes of “Incorrect Settings,” “Logic Errors,” and “Design Errors” to allow analysis at a higher granularity to address issues that may exist in one of the cause code subgroups. In [Figure E.21](#), however, these causes are still shown by an aggregated wedge and are analyzed together (illustrated in [Figure 4.7](#)) for a consistent year-to-year comparison over the four-year time frame.

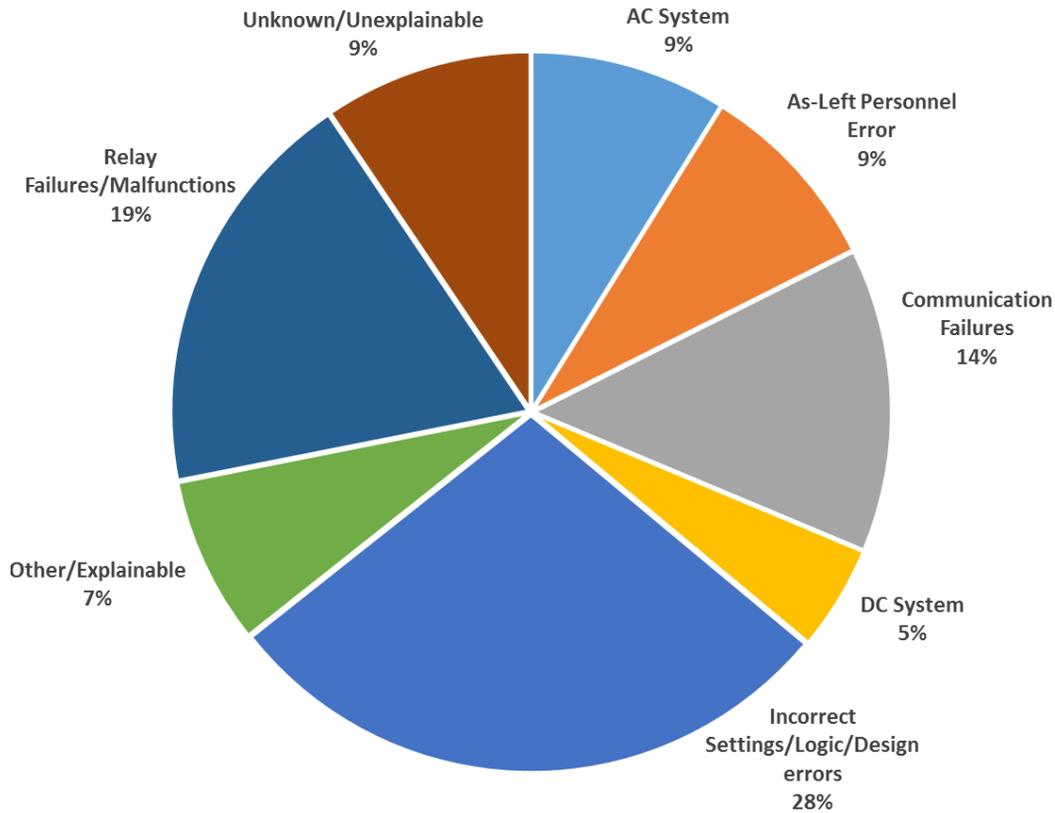


Figure E.21: NERC Misoperations by Cause Code (2Q 2012–3Q 2016)

Linkage between Misoperations and Transmission-Related Qualified Events

An analysis of misoperation data and events in the EA Process found that in 2015 there were 50 transmission-related system disturbances which resulted in a qualified event. Of those 50 events, 34 events, or 68 percent, had associated misoperations. Of the 34 events, 33 of them, or 97 percent, experienced misoperations that significantly increased the severity of the event. There were four events where one or more misoperations and a substation equipment failure occurred in the same event. The relay ground function accounted for 11 misoperations in 2014 causing events that were analyzed in the EA Process. This was reduced to six events in 2015. It was further reduced to only one event in 2016. The focus on the relay ground function has been attended by a reduction in its involvement in qualified events. It is not clear if any statistical basis will be able to confirm that its role in relay misoperations has been similarly decreasing.

Actions to Address Misoperations

To increase awareness and transparency, NERC will continue to conduct industry webinars¹⁵⁰ on protection systems and document success stories on how GOs and TOs are achieving high levels of protection system performance. The quarterly protection system misoperation trend can be viewed on NERC’s website.¹⁵¹ NERC introduced MIDAS in 2016, a data collection site for misoperations. MIDAS updates are scheduled for 2017 to improve data submission and analysis. NERC collaborates closely with the Regions to relay best practices and improve data collection.

Summaries of Individual Regional Entity Initiatives:

¹⁵⁰ http://www.nerc.com/files/misoperations_webinar_master_deck_final.pdf

¹⁵¹ <http://www.nerc.com/pa/RAPA/ri/Pages/ProtectionSystemMisoperations.aspx>

FRCC

The FRCC SPCS conducted peer reviews of protection system misoperations prior to the protection system owners submitting the data to NERC MIDAS. The FRCC SPCS is a member services group but includes FRCC staff as part of the review. The subcommittee is working on developing new and refining existing internal metrics with FRCC staff in order to better understand where to focus attention in the FRCC footprint. In 2017, FRCC will be conducting a misoperations assessment to identify lessons learned and make recommendations for improvements at the entity and Region levels.

MRO

The MRO Protective Relay Subcommittee (PRS) is preparing a second white paper to discuss the misoperation modes of several protection system schemes that have been observed to have a greater negative impact on system reliability within MRO. This paper will then identify effective approaches to reduce their occurrence. This paper will be distributed to all applicable Entities and also presented at the MRO annual Reliability Conference.

The MRO has also conducted event review meetings between the PRS and entities experiencing particularly severe events involving misoperations. The intent of these meeting is both to provide additional expertise and experience to the reporting entities, and to also disseminate lessons learned from the event to other entities.

Finally, MRO will be altering its misoperation review policy to conform to the requirements of NERC's MIDAS reporting application.

NPCC

The NPCC has instituted a procedure for peer review and analysis of all NPCC protection system misoperations. The NPCC review process is intended as a feedback mechanism that promotes continuous improvements based on lessons learned from reported protection system misoperations. The NPCC task force on system protection reviewed NERC lessons learned and NPCC-reported protection system misoperations while providing regional perspectives for entities' use to further improve performance and reduce misoperations.

NPCC collected additional data on microprocessor-based relay misoperations to develop potential measures that address misoperations caused by Incorrect Setting/Logic/Design Errors and to share knowledge of identified relay vendor specific product concerns along with the vendor recommended mitigations.

RF

RF has addressed the NERC misoperation reduction goal by providing training opportunities on protection topics to RF's member entities. The RF Protection Subcommittee has initiated annual refresher training in the areas of protection issues identified as the top misoperation causes in the Region and in NERC. The topics have included design concepts for protection communication systems and polarization techniques associated with protection system settings. In 2016, RF added a training opportunity for field protection engineers and technicians; these personnel are responsible for the installation and (commissioning) testing of protection system equipment, and they ensure that these protection systems are installed and function as designed. RF will continue to offer these opportunities into the future and has invited the other Regions to participate.

Also, in 2016, RF implemented a peer review process using members of the RF Protection Subcommittee to analyze the reported misoperations and to offer feedback on analysis and mitigation techniques. This process leverages the expertise and experiences of the Protection Subcommittee to help entities in the Region reduce their misoperations.

SERC

The SERC Protection and Controls Subcommittee (PCS) has created a SERC Regional Best Practices for Protection System Misoperations Reduction¹⁵² paper for entities to reference. SERC has also developed a metric to measure risk based on cause, category, voltage, Misoperation rate, and CAP response time.

SPP RE

The SPP System Protection & Control Working Group (SPCWG) has prepared a white paper discussing misoperations caused by communication failures,¹⁵³ a leading cause of misoperations in the SPP Region. The SPCWG is currently working on a white paper that discusses misoperations caused by Incorrect Settings/Logic/Design Errors, the second leading cause of misoperations in the SPP Region. These white papers then identify effective approaches to reduce misoperation occurrences.

Texas RE

Texas RE has worked with ERCOT's System Protection Working Group (SPWG) on the following:

- Development and monitoring of multiple metrics and historical trends for misoperations by voltage class, cause, corrective action plan completion rates, etc.
- Development of a metric on human performance issues as it relates to the cause of misoperations
- Presentation of the analysis and summary of quarterly protection system misoperation data and historical trends at each SPWG meeting
- Analysis of historical misoperations due to incorrect settings and determination that over 40 percent were due to ground fault overcurrent coordination issues
- Assisted the SPWG in the creation of a white paper to document best practices regarding ground overcurrent coordination to be shared among all entities in the Region

These efforts have raised the awareness of the main causes of misoperations in the Region and have led to the reduction in misoperations caused by Incorrect Settings, Logic, and Design Errors.

WECC

WECC tracks trends in misoperations in its annual *State of the Interconnection*¹⁵⁴ report and is conducting an in-depth analysis to identify the most effective areas to focus on to reduce misoperations. WECC will publish a report in 2017 that targets the top three cause categories contributing to misoperations in the West: Incorrect Settings, Relay Failures, and Unknown. This report will include recommendations and best practices that entities can use to evaluate their own practices regarding misoperations. Through outreach efforts and working with its Relay Work Group, WECC encourages entities to evaluate their individual systems to best determine ways to reduce misoperations. WECC is working with a team of stakeholders to develop a strategy to reduce misoperations in the Western Interconnection. In Fall 2017, WECC will hold a misoperations summit to share and discuss the reduction strategy and the issue of misoperations in general.

¹⁵² <http://www.serc1.org/docs/default-source/committee/ec-protection-and-control-subcommittee/serc-regional-best-practices-for-protection-system-misoperations-reduction-8-19-2016.pdf>

¹⁵³ https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.spp.org%2Fdocuments%2F23167%2Fspcwg_commmisops_whitepaper_final_mopc.doc

¹⁵⁴ <https://www.wecc.biz/Reliability/2016%20SOTI%20Final.pdf>

Misoperations Analysis

Misoperation Rate by Region and for NERC

Table E.24 lists the NERC operation and misoperation counts and the corresponding misoperation rates by Region and for NERC with the 16 available quarters (Q4 2012–Q3 2016). NERC’s numbers are based on the combined data for the Regions available for the respective time periods. It should be noticed that due to an improving performance of M-9, the most recent, year 4, rate stands lower than the overall rate for the for years (8.7 percent versus 9.5 percent).

Region	Operations	Misoperations	Misoperation Rate
FRCC	2,673	263	9.8%
MRO	5,624	613	10.9%
NPCC (Q1 2013 to Q3 2016)	10,126	743	7.3%
RF	10,677	1,468	13.7%
SERC	16,443	1,381	8.4%
SPP	7,975	903	11.3%
TRE	8,940	644	7.2%
WECC (Q2 and Q3 2016 only)	3,002	179	6.0%
NERC	65,461	6,194	9.5%

Comparison of Regional Misoperation Rates

Regional misoperation data was analyzed to find statistically significant differences¹⁵⁵ in misoperation rates between Regions based on the four-year data (except for Q1 2013–Q3 2016 for NPCC and Q2 and Q3 2016 for WECC). **Table E.25** shows results of the statistical tests that compare misoperation rates by Region. The second column lists Regions with a statistically significantly higher rate than the Region in each row, the fourth column lists Regions with a lower rate, and the third column—Regions with no significant difference in the misoperation rate.

Region	Regions with Higher Rate	No Significant Difference	Region with Lower Rate
RF	none	none	SPP, MRO, FRCC, SERC, NPCC, TRE, WECC
SPP	RF	MRO	FRCC, SERC, NPCC, TRE, WECC
MRO	RF	SPP, FRCC	SERC, NPCC, TRE, WECC
FRCC	RF, SPP	MRO	SERC, NPCC, TRE, WECC
SERC	RF, SPP, MRO, FRCC	none	NPCC, TRE, WECC
NPCC	RF, SPP, MRO, FRCC, SERC	TRE	WECC
TRE	RF, SPP, MRO, FRCC, SERC	NPCC	WECC
WECC	RF, SPP, MRO, FRCC, SERC, NPCC, TRE	none	none

¹⁵⁵ Large sample test on population proportions at the 0.05 significance level

M-10 Transmission Constraint Mitigation

This metric was approved for retroactive retirement by the PC in June of 2017.

Complete data for this metric was no longer collected for the *State of Reliability 2016*. The metric measured the number of mitigation plans that included SPSs, RASs, and/or operating procedures developed to meet reliability criteria.

M-11 Energy Emergency Alerts

Background

To ensure that all RCs clearly understand potential and actual energy emergencies in the interconnection, NERC has established three levels of energy emergency alerts (EEA) as detailed in EOP-002-3.1.¹⁵⁶ 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 event. EEA trends may provide an indication of BPS capacity. This metric may also provide benefits to the industry when considering correlations between EEA events and planning reserve margins.

When an EEA3 alert is issued, firm-load interruptions are imminent or in progress in accordance with EOP-002-3.1. The issuance of an EEA3 may be due to a lack of available generation capacity or when resources cannot be scheduled due to transmission constraints.

Assessment

Table E.26 shows the number of EEA3 events declared from 2006–2016. Only two EEA3s were declared in 2016, one more than the previous year. However, this was less than in any year 2006–2014.

Region	Number of Events										2016
	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	
NERC	5	26	13	38	7	23	14	6	4	1	2
FRCC	0	0	0	0	0	0	0	1	2	0	0
MRO	0	0	0	0	0	0	0	0	0	0	0
NPCC	0	0	0	1	0	0	0	0	1	0	0
RF	0	0	0	0	0	0	0•	0	0	0	0
SERC	2	14	2	0	3	2	7	0	1	0	0
SPP	1	9	8	37	4	15	6	2	0	0	0
TRE	0	0	0	0	0	1	0	0	0	0	0
WECC	2	3	3	0	0	5	1	3	0	1	2

Table E.27 shows the number of all EEAs declared in 2016, broken out by Region as well as event level.

Region	EEA1	EEA2	EEA3	Total
FRCC	0	0	0	0
MRO	6	7	0	13
NPCC	6	4	0	10
RF	0	0	0	0
SERC	0	0	0	0

¹⁵⁶ http://www.nerc.com/files/EOP-002-3_1.pdf

Region	EEA1	EEA2	EEA3	Total
SPP	0	0	0	0
WECC	5	2	2	9
TRE	0	0	0	0
Grand Total	17	13	2	32

In **Figure E.22**, a graph is provided for 2013–2016, showing the duration and amount of load shed (by category), if any, by all EEAs in each year. The two 2016 EEA3s had a combined duration of 9.7 hours and 515 MW of load.

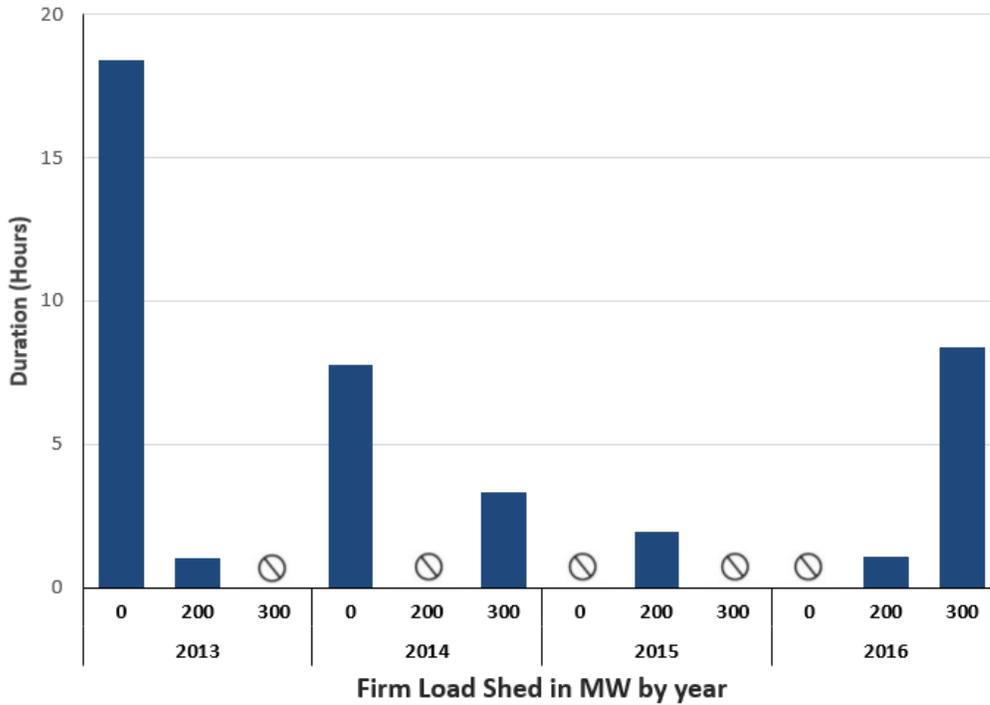


Figure E.22: Firm Load Shed and Duration Associated with EEA3 Events by Year

Appendix F: Statistical Significance Whitepaper

One of the main goals of performance analysis is to measure the performance of the BPS to identify significant reliability risk factors. This is accomplished, in part, by developing and tracking key reliability indicators. Significant changes in these indicators can point to improvements in reliability or signal reliability risks.

The significance of these changes is evaluated using *hypothesis testing*, which is a statistical method for making inferences about a population based on a representative sample. If hypothesis testing indicates the changes are indeed significant, they are referred to as *statistically significant*. This report introduces and explains statistical hypothesis testing and the meaning of the term statistically significant for readers without a background in statistics.

Theoretical Background

Statistical Hypotheses

A statistical hypothesis is a statement about the properties of a population or the relationship between different populations. Statistical tests are run on a representative sample of the population to determine if the hypothesis is true or false. Statisticians and data analysts evaluate the hypotheses by comparing data observed in reality to results expected if the statement were true. If observations differ markedly from the expectations, the hypothesis is rejected in favor of an alternative hypothesis. If they do not, the hypothesis is accepted.¹⁵⁷

The statement to be disproved is called the *null hypothesis*; the statement to accept (in favor of the null hypothesis) is called the *alternative hypothesis*. For example, an engineer studying failure rates of generating units may wish to test the following hypotheses:

- Null hypothesis: “Model A units fail as often as Model B units.”
- Alternative hypothesis: “Model A units fail more often than Model B units.”

The exact testing procedure depends on the alternative hypothesis. Slightly different procedures would be used for the engineer to test the alternative hypothesis: that Model A units fail either more often or less often than Model B units.

Testing Statistical Hypotheses

To decide between the null and alternative hypotheses, the engineer collects samples from both types of units and calculates a *test statistic*. A test statistic is a quantity derived from these two samples. In this example, it measures “a distance” between the rates for the two populations. The distribution of the test statistic is known if the null hypothesis is true. In another words, the probability that the statistic will take any given value or belong to any given interval is known in advance.

To conduct the test, the range of possible values of the test statistic is divided into two parts: an *acceptance region* and a *critical region* as shown in [Figure F.1](#). The boundary between is called the *critical value*. If the test statistic falls in the acceptance region, the sample is consistent with the null hypothesis, thus it is accepted. If the test statistic falls in the critical region, the sample is not consistent with the null hypothesis and it is rejected in favor of the alternative hypothesis.

In the above example, the engineer will calculate average observed failure rates for a sample of Model A units and a sample of Model B units. If the null hypothesis is true, and the units have the same underlying failure rate, the

¹⁵⁷ Some authors prefer to say “fail to reject” rather than “accept.”

difference between the observed failure rates will follow a standard normal distribution with an average value of zero.¹⁵⁸ The test is as follows:

- The engineer rejects the null hypothesis if the difference between the observed failure rates is large due to a sampling error.¹⁵⁹ In that case, it can be concluded that Model A units indeed have a higher failure rate.
- On the other hand, if the difference is not much larger than zero, the null hypothesis is not rejected. The failure rate of Model A units may be smaller or equal to the failure rate of Model B units, but it is not larger.¹⁶⁰

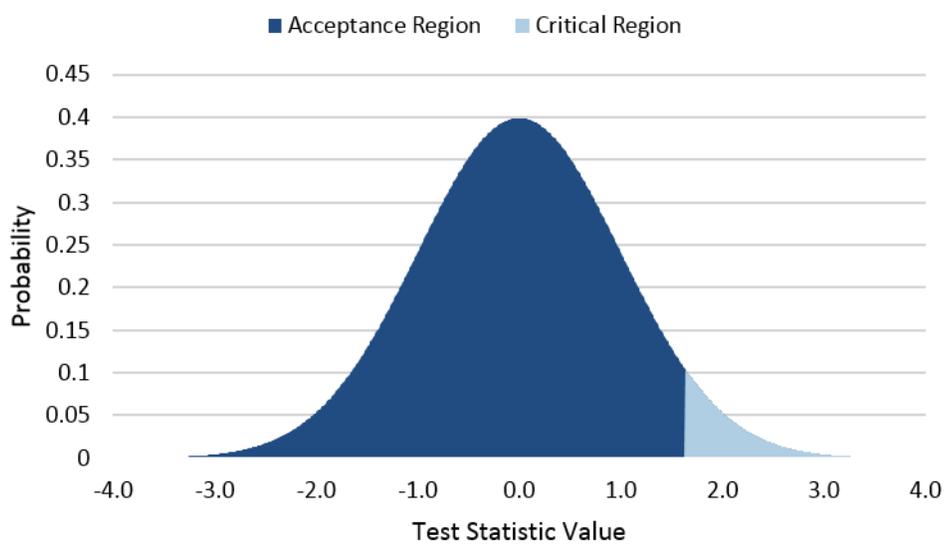


Figure F.1: Distribution of the Test Statistic If the Null Hypothesis Is True

Selecting Critical Values

There are four possible outcomes of a hypothesis test visible in [Figure 4.2](#). A correct decision can be either to reject a null hypothesis when it is false or to accept a null hypothesis when it is true. However, if the null hypothesis is true, but the test statistic falls in the critical region, the analyst would falsely reject a true hypothesis. This is called a *Type I error*. If the null hypothesis is false, but the test statistic falls in the acceptance region, the analyst would falsely accept a false hypothesis. This is called a *Type II error*.

¹⁵⁸ This follows from the Central Limit Theorem if the sample sizes are large. The observed rates must first be multiplied by a scaling factor specified by the test.

¹⁵⁹ Sampling error arises from dissimilarity between a population and a sample from it. A large randomly selected sample will have less sampling error than a small nonrandom sample.

¹⁶⁰ The test was designed based on the alternative hypothesis, “Model A units fail more often than Model B units.” No conclusion can be made about whether the Model A units fail less often. A different alternative hypothesis and test would be used for this purpose.

		Test Statistic Location	
		Critical Region	Acceptance Region
Null Hypothesis	False	Correct Rejection	Type II Error
	True	Type I Error	Correct Acceptance

Figure F.2: Possible Outcomes of a Hypothesis Test

The size of the critical region determines the probability of a Type I error. When conducting a hypothesis test, it is decided in advance how acceptable this outcome is and an appropriate *significance level* is selected accordingly. This is the probability that a Type I error will occur, the probability that a sample will lead to rejecting the null hypothesis, even though it is true. Some common values are 0.10 (10 percent chance of a Type I error) and 0.05 (Five percent chance of a Type I error). Based on the distribution of the test statistic under the null hypothesis and the selected significance level, the critical value is chosen in such a way that the probability for the test statistic to fall above it (or below, depending on the test) is equal to the significance level.¹⁶¹

The significance level cannot be set to be an arbitrarily low. As the probability of a Type I error decreases, the probability of a Type II error increases (The exact probability depends on the distribution of the test statistic.) The significance level of a test must be chosen carefully to balance the probability of each type of error.

Statistical Significance

If the test statistic falls in the critical region, the result is called *statistically significant*. It means the data does not support the null hypothesis; the probability of observing this result if the null hypothesis were true does not exceed the chosen significance level.

Instead of merely saying whether the test statistic was significant at a given significance level, it is common to report the *P-value*. The P-value of a test statistic is the probability of observing that test statistic (or the test statistic more extreme) in the event the null hypothesis is true. This value is the smallest significance level that would lead to rejecting the null hypothesis.

When documenting test results, it could be reported that the difference in failure rates was significant with a P-value of 0.03. This means that the probability of at least the observed difference occurring if the null hypothesis were true is 3 percent. Reporting the P-value, rather than simply saying the results were significant, allows readers to see why the analysts have arrived at their conclusion and to then decide for themselves whether the results are significant.

Statistical Versus Practical Significance

Depending on the nature of the population under study, it is possible for hypothesis testing to detect very small differences. If the sample size is large, and the variability in failure rates between units is small, the engineer might

¹⁶¹ This rule allows a generalization for a two-sided test with several critical values.

find a statistically significant difference in failure rates that is not worth mentioning in practical terms. This practicality is often referred to as practical significance. One must take care when interpreting practical significance versus statistical significance, especially when the result will drive decision-making. Therefore, one should examine and understand the situation to determine if a result is not only statistically significant but also practically significant.

Examples from Performance Analysis

Reliability Indicator M-9: Misoperation Rate

Table F.1 presents observed protection system misoperation rates for two twelve-month periods.¹⁶² The misoperation rate declined by 1.2 percent from one period to the next. Hypothesis testing allows us to evaluate whether this was a significant change or one simply due to chance.

Time Period	Misoperations	Total Operations	Misoperation Rate
July 2014–June 2015	1,436	14,789	9.7%
July 2015–June 2016	1,357	16,016	8.5%

First, a statistical model that will allow defining of the testable hypotheses must be established. Suppose that when an operation occurs, it will be a misoperation with a fixed but unknown probability p . Then, out of a given number of operations n , the number of misoperations x follows a binomial distribution. Then the question to answer becomes whether the misoperation rate during the first period (p_1) was significantly greater than the misoperation rate during the second period (p_2). Thus, the null and alternative hypotheses are defined as follows:

- Null hypothesis: $p_1 = p_2$
- Alternative hypothesis: $p_1 > p_2$

For large samples, such as this one, the difference between the observed misoperation rates will follow a standard normal distribution with an average value of zero.¹⁶³ [Figure F.1](#) illustrates the acceptance and critical regions for this test with a significance level of 0.05. The null hypothesis is rejected if the test statistic is greater than 1.64. The probability of seeing a difference larger than this critical value, if the null hypothesis is true, is less than five percent.

In fact, the calculated test statistic is 3.78. This is well above the critical value, indicating that the difference is statistically significant. Its P-value (7.90×10^{-5}) is much lower than the established significance level of 0.05. To illustrate how strong this result is, it would require a confidence level of more than 99.99 percent before considering the results of this test not statistically significant. The difference in rates is much too large to be due to chance. It can be concluded that the misoperation rate decreased statistically significantly between the two time periods.

Reliability Indicator M-14: Outages Initiated by Failed Substation Equipment

Reliability Indicator M-14 is the average number of automatic outages per ac circuit 200 kV and above, initiated by Failed AC Substation Equipment. This Indicator increased between 2013 and 2014 as listed in [Table F.2](#). Again, hypothesis testing was used to evaluate whether this was the result of random chance.

¹⁶² Excluding WECC

¹⁶³ The difference in rates must first be multiplied by a scaling factor specified by the test.

Table F.2: Reliability Metric M-14			
Year	Outages Initiated by Failed AC Substation Equipment	AC Circuits > 200 kV	Outages per Circuit
2013	229	7,655	0.030
2014	267	7,753	0.033

To frame testable hypotheses, it is assumed that occurrences of the outages an ac circuit experiences follow a Poisson process with an average rate r of outages per year.¹⁶⁴ If the average outage rate in 2013 is r_1 and the rate in 2014 is r_2 , the hypotheses are:

- Null hypothesis: $r_1 = r_2$
- Alternative hypothesis: $r_1 \neq r_2$

According to Hoel,¹⁶⁵ if the null hypothesis is true, a particular function $\lambda(r_1, r_2)$ follows a known distribution.¹⁶⁶ Figure F.3 displays the distribution of the test statistic if the null hypothesis is true. The shaded critical region reflects a 0.05 significance level. At that level, the test states the critical value to be 3.84. If the rates are equal, the probability that $\lambda(r_1, r_2)$ is greater than the critical value is less than five percent.

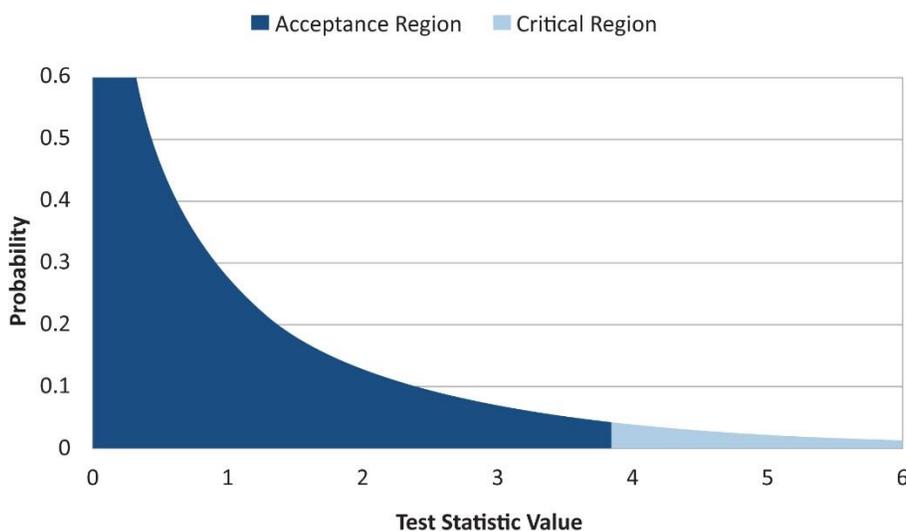


Figure F.3: Distribution of Test Statistic If Outage Rates Are Equal

In fact, the test statistic is $\lambda(r_1, r_2) = 2.45$, which has a P-value of 0.12. Since $\lambda(r_1, r_2)$ is smaller than the critical value, it belongs in the acceptance region. It is concluded that the increase in the number of outages per circuit between 2013 and 2014 is not statistically significant.

Conclusion

This report explains hypothesis testing and statistical significance for readers without a background in statistics. A hypothesis test compares real-world observations to expectations from a statistical model to choose between null and alternative hypotheses. If what is observed differs sufficiently from what is expected, the difference is called statistically significant.

¹⁶⁴ A Poisson process is a model describing the behavior of many natural phenomena. In a Poisson process, events occur independently of each other, according to a fixed average rate proportional to a fixed interval of time or space (in this example, the span of a year).

¹⁶⁵ P.G. Hoel. Testing the Homogeneity of Poisson Frequencies. 1945. Annals of Mathematical Statistics. pp. 362-368.

¹⁶⁶ χ^2 -distribution with 1 degree of freedom.

Statistical significance does not imply practical significance. The result of a hypothesis test must be interpreted with the particular assumptions of the test and the context in mind. Interpretation should also incorporate the inherent uncertainty of the result and a relation between the predetermined probability of Type I Error and the resulting probability of Type II Error.

The most appropriate statistical test to use in a given situation must be determined by the analyst based on an understanding of the fundamental nature of the population in question. This report is not a guide on making that determination.

Common Statistical Tests

Below is a list of statistical tests frequently used in NERC's reports:

- Test on significance of correlation
- Large-sample test on population proportion
- Test on significance of a regression line slope
- Test on homogeneity of Poisson frequencies
- ANOVA
- Tests on homogeneity of variance: Bartlett, F-folded
- T-tests: Fisher's Least Significant Difference, Pooled, Satterthwaite
- Nonparametric tests: Mann-Whitney, Wilcoxon, Mood
- Multiple regression model: by step-wise selection, by backward elimination
- Goodness-of-fit tests: Kolmogorov-Smirnov, Cramer-von Misses, Anderson-Darling

References

1. M. Kendall and A. Stuart. *The Advanced Theory of Statistics*. Vol. 2. Fourth Edition. MacMillan Publishing Co., Inc. New York.
2. E.L. Lehmann. *Testing Statistical Hypotheses*. 1986. Third Edition. John Wiley & Sons Inc.
3. D.C. Montgomery and G.C. Runger. 2006. *Applied Probability and Statistics for Engineers*. Fourth Edition. John Wiley & Sons Inc.
4. R. L. Wasserstein and N.A. Lazar. 2016. The American Statistical Association's statement on p-values: context, process, and purpose, *The American Statistician*, DOI: 10.1080/00031305.2016.1154108.
5. *NERC State of Reliability report 2016*.
http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2016_SOR_Report_Final_v1.pdf
6. *NERC Frequency Response Annual Analysis report 2016*.
http://www.nerc.com/comm/oc/documents/2016_fraa_report_2016-09-30.pdf
7. P.G. Hoel. Testing the Homogeneity of Poisson Frequencies. 1945. *Annals of Mathematical Statistics*. pp. 362-368.

Appendix G: Security Performance Metrics

Background

For the past two years, the *State of Reliability* report has included a chapter for security performance metrics based largely on data collected by NERC's E-ISAC. These metrics help provide answers to basic questions often asked by industry executives and senior managers, such as the following:

- How often do physical and cyber security incidents occur?
- To what extent do these reported incidents cause a loss of customer load?
- What is the extent of security information-sharing across the industry?
- Are cyber security vulnerabilities increasing?

These security performance metrics are derived from data collected and validated by the E-ISAC during 2015 and 2016. On a quarterly basis, the E-ISAC collaborates with the BESSMWG to review the results and ensure the definitions are being correctly applied to the raw data. In some cases, the BESSMWG has revised the definitions to clarify the metric or make it more meaningful. The E-ISAC and BESSMWG are continuing to consider new security metrics that may be useful to the industry.

Purpose

For many years now, NERC and the electricity industry have taken actions to address cyber and physical security risks to the BPS as a result of potential and real threats, vulnerabilities, and events. These security metrics complement other NERC reliability performance metrics by defining lagging and leading indicators for security performance as they relate to reliable BPS operation. These metrics help inform senior executives in the electricity industry (e.g., NERC's Board of Trustees, management, the Member Representatives Committee, and the RISC) by providing a global and industry-level view of how security risks are evolving and indicating the extent the electricity industry is successfully managing these risks. Due to the vast array of different operations technology systems used by individual electricity entities, the BESSMWG has not developed cyber security metrics applicable to the day-to-day operation of individual entities

NERC Alert Process and Security Incidents During 2016

One of the responsibilities of the E-ISAC is to provide subject matter expertise to issue security-related threat alerts, warnings, advisories, notices, and vulnerability assessments to the industry. While these alerts may provide some indication of the relative risks facing the electricity industry, they have so far not occurred frequently enough to indicate trends.

During 2016, NERC issued two industry-wide alerts¹⁶⁷ and one industry advisory that described large-scale distributed denial-of-service attacks, an increasing presence of ransomware, and the cyber attack that affected a portion of Ukraine's electricity system. The following summarizes the three alerts and advisories issued by NERC:

- A series of large-scale denial-of-service attacks affected a wide array of consumer internet-capable devices. While these attacks did not impact the reliable operation of the grid, they highlighted the potential vulnerability of some equipment, such as video cameras, that are widely used in the electricity industry.
- Ransomware, used to infiltrate networks and deny access to information and systems until the victim meets payment demands, continues to pose a threat as demonstrated by attacks against, for example,

¹⁶⁷ Ref. <http://www.nerc.com/pa/rrm/bpsa/Pages/Alerts.aspx>

hospitals and municipalities. NERC's industry advisory helped raise awareness across the industry regarding this threat.

- In December 2015, a portion of the Ukraine's electricity distribution system was disrupted by a cyber attack. The E-ISAC was involved in the post-event review, and NERC issued an alert to inform the industry and recommended actions to prevent or mitigate such an attack.

Security Performance Metrics and Results

This section provides eight security performance metrics. The E-ISAC and BESSMWG have reviewed these results and have identified trends where possible, recognizing that these results are based on only two years of data.

Security Metric 1: Reportable Cyber Security Incidents

Responsible entities must report cyber security incidents to the E-ISAC as required by the NERC Reliability Standard CIP-008-5 Incident Reporting and Response Planning. This metric reports the total number of reportable cyber security incidents¹⁶⁸ that occur over time and identifies how many of these incidents have resulted in a loss of load. It is important to note that any loss of load will be counted regardless of direct cause. For example, if load was shed as a result of a loss of situation awareness caused by a cyber incident affecting an entity's energy management system, the incident would be counted even though the cyber incident did not directly cause the loss of load. This metric provides the number of reportable cyber security incidents and an indication of the resilience of the BES to operate reliably and continue to serve load.

While there were no reportable cyber security incidents during 2015 and 2016, and therefore none that caused a loss of Load, this does not necessarily suggest that the risk of a cyber security incident is low, as the number of cyber security vulnerabilities is continuing to increase (ref. security metric 5).¹⁶⁹

Cyber Security Incident Case Study: Ukraine

In December 2015, Ukraine fell victim to a cyber attack that included spear phishing, credential harvesting and lateral movement, unauthorized remote access, telephony denial of service, and sustaining persistent access. In February 2016, the E-ISAC provided subject matter expertise to develop the NERC alert *Mitigating Adversarial Manipulation of Industrial Control Systems as Evidenced by Recent International Events*¹⁷⁰, which shared techniques observed in the Ukraine cyber attacks. Most of these same tactics and techniques were used in a subsequent series of attacks against Ukraine in December 2016, when Ukraine's state-owned national power company Ukrenergo experienced an outage at an electrical substation in the capital city of Kyiv. Service was restored as a result of manual operator intervention. Researchers confirmed that the outage was the result of a cyber attack that occurred during the end of a protracted campaign.

In addition to the 2016 NERC Alert, the E-ISAC worked with SANS to publish a *Ukraine Defense Use Case*¹⁷¹ (DUC). This 29-page report "summarizes important learning points and presents several mitigation ideas based on publicly available information on ICS incidents in Ukraine."

The techniques used against Ukraine have several options for remediation and prevention. NERC, through standards and compliance; and the E-ISAC, through information sharing, industry collaboration, and publications like the alert and DUC, often stresses and shares these remediation and prevention tips with the international electricity industry.

¹⁶⁸ Ref. NERC Glossary of Terms: "A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity."

¹⁶⁹ ERO Reliability Risk Priorities, [RISC Recommendations to the NERC Board of Trustees](#), November 2016, p. 9 Risk Mapping chart depicts Cyber Security Risk as having high potential impact and relative likelihood of BPS-wide occurrence.

¹⁷⁰ The alert is not publicly available.

¹⁷¹ https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

The events in Ukraine underscore the importance of grid security and provide a real life example of consequences of a cyber attack on the electrical grid. The events abroad highlight the importance of user training and information sharing in order to prevent a similar attack on the North American power grid. To date, there have been zero reportable cyber security incidents resulting in loss of load (Metric 1).

Security Metric 2: Reportable Physical Security Events

Responsible Entities must report physical security events to the E-ISAC as required by the *NERC EOP-004-3 Event Reporting Reliability Standard*¹⁷². This metric reports the total number of physical security reportable events¹⁷³ that occur over time and identifies how many of these events have resulted in a loss of load. It is important to note that any loss of load is counted regardless of direct cause. For example, if load was shed as a result of safety concerns due to a break-in at a substation, the event is counted even though no equipment was damaged which directly caused the loss of load. The metric provides the number of physical security reportable events and an indication of the resilience of the BES to operate reliably and continue to serve load.

Note that this metric does not include physical security events reported to the E-ISAC that do not meet the reporting threshold as defined by the *NERC EOP-004-3 Reliability Standard*, such as physical threats and damage to substation perimeter fencing. Also, this metric does not include physical security events that affect equipment at the distribution level (i.e., non-BES equipment).

During 2015 and 2016, one physical security event occurred that caused a loss of load as reflected in **Figure G.1**. This near-zero result does not necessarily suggest that the risk of a physical security event causing a loss of load is low as the number of reportable events has not declined over the past two years. Although this metric does not include physical security events affecting equipment at the distribution level (i.e., non-BES equipment), NERC receives information through both mandatory and voluntary reporting that indicates that distribution-level events are more frequent than those affecting BES equipment.

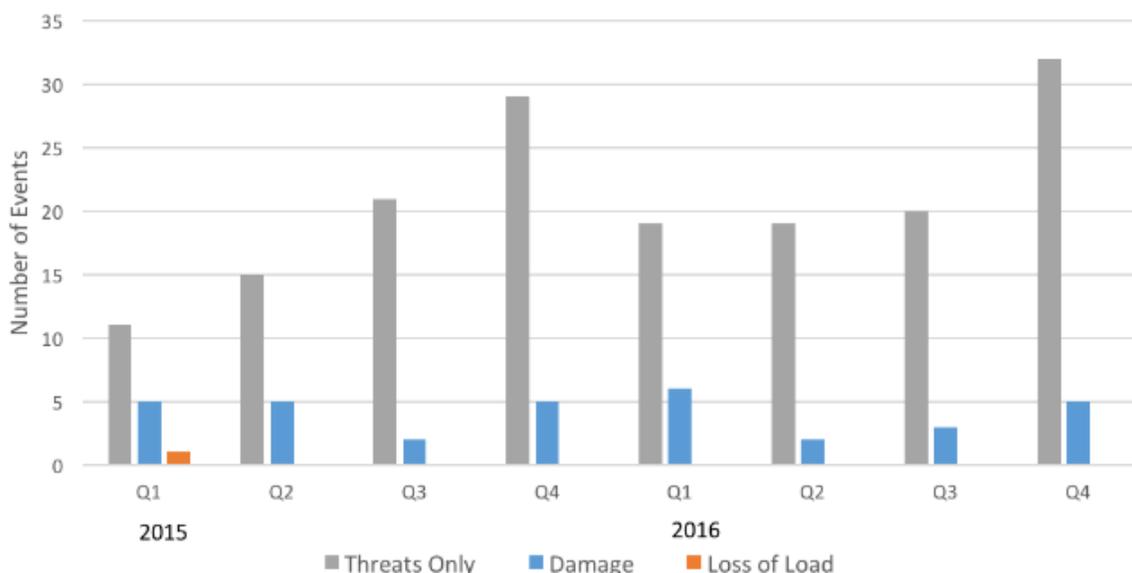


Figure G.1: Reportable Physical Security Events

¹⁷² <http://www.nerc.com/layers/PrintStandard.aspx?standardnumber=EOP-004-3&title=Event%20Reporting&jurisdiction=United%20States>

¹⁷³ Reportable Events are defined in Reliability Standard EOP-004-2 Event Reporting, Attachment 1.

Security Metric 3: E-ISAC Membership

This metric reports the total number of electricity sector organizations and individuals registered as members of the E-ISAC. E-ISAC members include NERC registered entities and others in the electricity sector, including distribution utilities (i.e., membership is not limited to BPS organizations). Given today’s rapidly changing threat environment, it is important that entities be able to quickly receive and share security-related information. This metric identifies the number of organizations registered as well as the number of individuals as depicted in **Figure G.2**. Increasing E-ISAC membership should serve to collectively increase awareness of security threats and vulnerabilities and enhance the sector’s ability to respond quickly and effectively.

During the latter half of 2016, the E-ISAC implemented a password reset policy in an effort to enhance the security of its information-sharing portal by requiring members to change their passwords every 90 days and limit access to only members who actively use the portal.

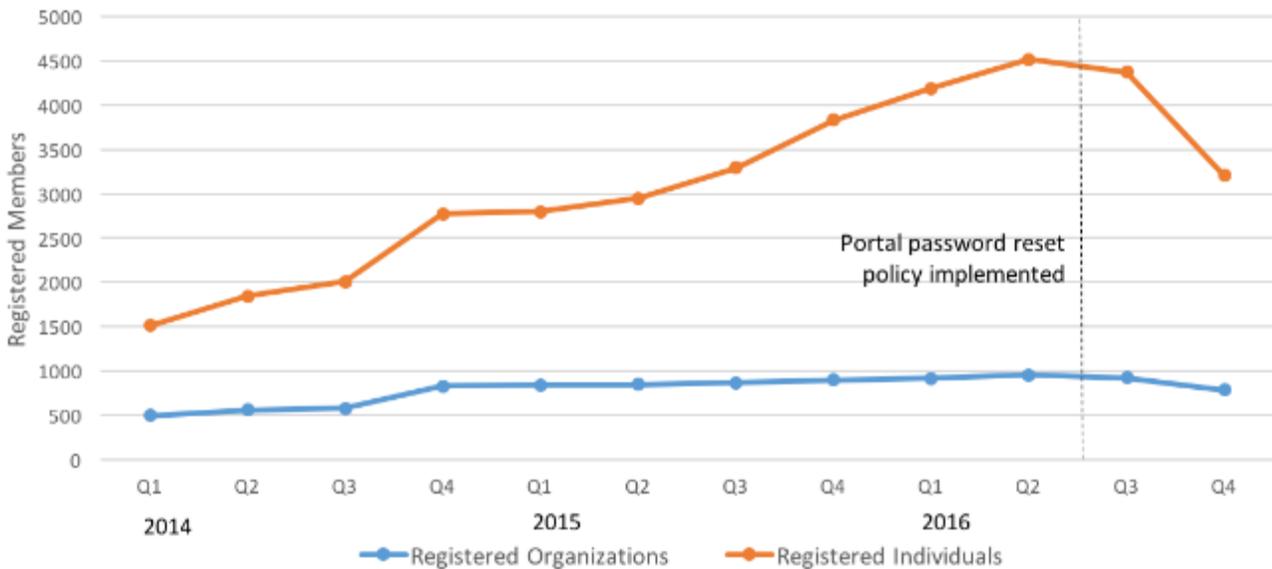


Figure G.2: E-ISAC Membership

The data indicates the following:

- As of the end of 2016, all RCs and 85 percent of Bas had an active account with the E-ISAC. As defined by the NERC functional model, RCs and Bas perform an essential coordinating role in the operation of the BPS within their respective areas and with each other.
- Since 2014, the number of registered organizations has steadily increased. However, additional outreach across the industry is needed to further increase awareness and encourage active use of the E-ISAC portal.
- The number of individual users has increased at a faster rate than the number of registered organizations. Organizations are increasing the number of individuals with access to the E-ISAC portal, likely as part of efforts to increase their security staffing capabilities and capacity.
- The E-ISAC’s new portal password reset policy, implemented during 2016, has resulted in a significant decrease in the number of registered organizations and individuals. Going forward, this metric will more accurately reflect the number of members who actively use the portal as a routine part of their job.

Security Metric 4: Industry-Sourced Information Sharing

This metric reports the total number of incident bulletins (i.e., cyber bulletins and physical bulletins) published by the E-ISAC based on information voluntarily submitted by the E-ISAC member organizations as shown in **Figure**

G.3.¹⁷⁴ E-ISAC member organizations include NERC registered entities and others in the electricity sector, including distribution utilities (i.e., it is not limited to the BPS). Incident bulletins describe physical and cyber security incidents and provide timely, relevant, and actionable information of broad interest to the electricity sector. Given today's complex and rapidly changing threat environment, it is important that electricity sector entities share their own security-related intelligence as it may help identify emerging trends or provide an early warning to others. This metric provides an indication of the extent to which the E-ISAC member organizations are willing and able to share information related to cyber and physical security incidents they experience. As the E-ISAC member organizations increase the extent that they share their own information, all member organizations will be able to increase their own awareness and ability to respond quickly and effectively. This should enhance the resilience of the BPS to new and evolving threats and vulnerabilities. The modest but steady increase in the number of bulletins published by the E-ISAC during 2016, compared with 2015, suggests that member organizations are sharing security-related information.

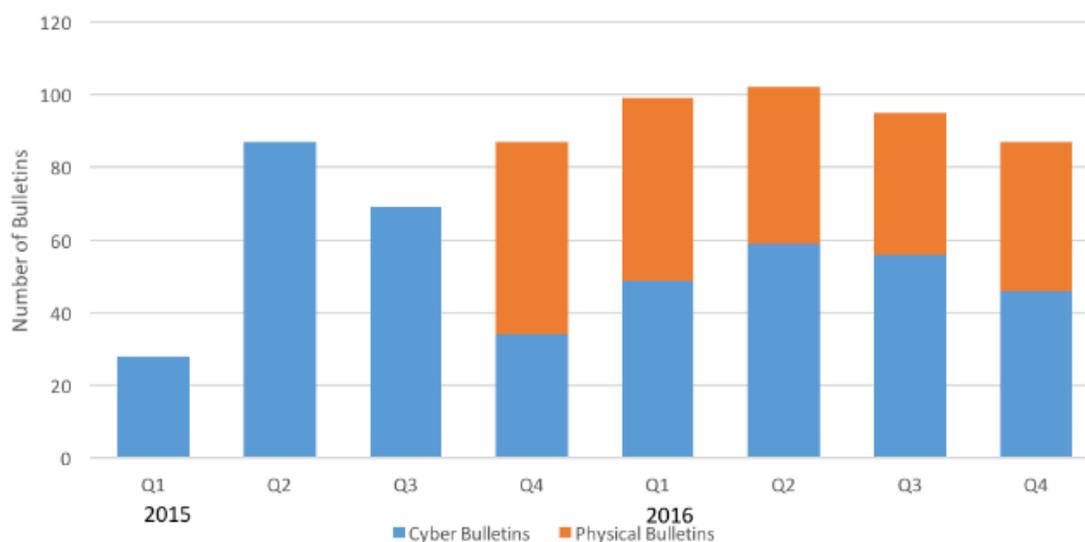


Figure G.3: Industry-Sourced Information Sharing

Security Metric 5: Cyber Security Risk Information Sharing Program Reporting Statistics

CRISP is a public-private partnership cofounded by the DOE and NERC and managed by the E-ISAC that facilitates the exchange of detailed cyber security information among industry, the E-ISAC, DOE, and Pacific Northwest National Laboratory. The program facilitates information sharing and enables owners and operators to better protect their networks from sophisticated cyber threats.

Participation in the program is voluntary and enables owners and operators to better protect their networks from sophisticated cyber threats. The purpose of CRISP is to collaborate with energy sector partners to facilitate the timely bi-directional sharing of unclassified and classified threat information. CRISP information helps support development of situational awareness tools to enhance the sector's ability to identify, prioritize, and coordinate the protection of its critical infrastructure and key resources.

CRISP participant companies serve approximately 75 percent of electricity consumers in the United States. The quantity, quality, and timeliness of the CRISP information exchange allows the industry to better protect itself against cyber threats and to make the BPS more resilient.

¹⁷⁴ In September 2015, the E-ISAC launched its new portal. Watchlist Entries are now called Cyber Bulletins. The category Physical Bulletins is on the portal to share physical security information. Prior to 2015 Q4, physical security reports were shared through the E-ISAC Weekly Report, but not through Watchlist Entries.

In 2016, CRISP identified intrusion methods used by threat actors with a wide variety of technical prowess and continued to identify and monitor activities of threat actors and their escalating risk to the U.S. electricity industry.

In 2016, the E-ISAC saw 41 cases predicated on IOCs provided by CRISP participants that resulted in all-site reports. CRISP all-site reports leverage ISD data and all-source intelligence to provide actionable information to support security operations across the CRISP community with company-specific information removed. **Table G.1** details the reporting statistics for 2016.

Table G.1: CRISP 2016 Reporting Statistics	
Product	2016 Total
Cases Opened	1,553
Analyst Generated Reports	194
Site Annexes	442
Automated Reports	~165,000

Security Metric 6: Global Cyber Vulnerabilities

This metric reports the number of global cyber security vulnerabilities considered to be high severity (as reflected in **Figure G.4**) based on data published by the National Institute of Standards and Technology (NIST). NIST defines high severity vulnerabilities as those with a common vulnerability scoring system¹⁷⁵ (CVSS) of seven or higher. The term “global” is an important distinction as this metric is not limited to information technology typically used by electricity sector entities. The year-over-year increase in global cyber security vulnerabilities (23 percent) compared with global cyber security incidents (38 percent) indicates that vulnerabilities are increasingly being successfully exploited, and reinforces the need for organizations to continue to enhance their cyber security capabilities.

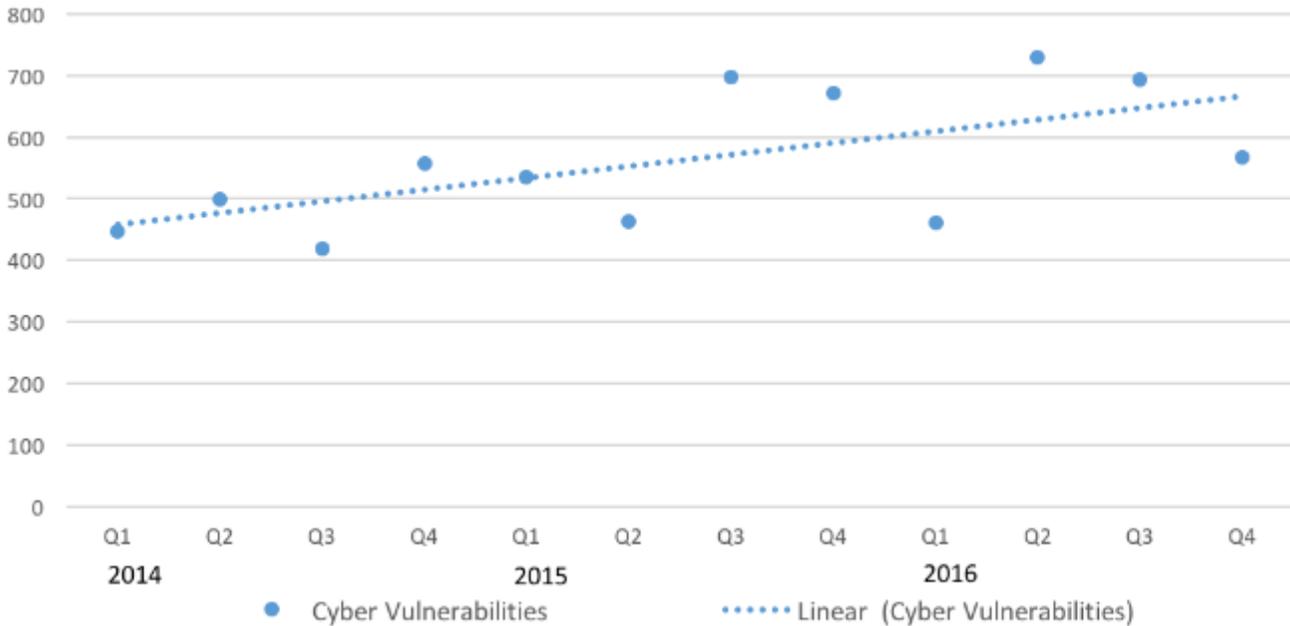


Figure G.4: Global Cyber Vulnerabilities

¹⁷⁵ Ref. NIST <http://nvd.nist.gov/cvss.cfm>

Security Metric 7: Global Cyber Vulnerabilities and Incidents

This metric compares the number of annual global cyber security vulnerabilities and incidents to identify a possible correlation between them as illustrated in [Figure G.5](#). This metric is based on surveys of chief information technology officers and chief information security officers, and although the survey respondents change from year to year, reports of this nature tend to have consistent results and will continue to be a valid indicator. While many different sources for this information are publicly available, the BESSMWG had selected the PwC Global State of Information Security report because it had consistently reported the number of incidents since at least 2013. Unfortunately, PwC did not provide the data for 2016; the BESSMWG is working to determine if this information will be available in future. If not, the BESSMWG will seek alternate sources for similar data.



Figure G.5: Global Vulnerabilities versus Incidents

Security Metric 8: GridEx Exercise Participation

This metric compares the number of organizations participating in each of the GridEx security and crisis response exercises conducted by NERC every two years as shown in [Figure G.6](#). NERC’s large-scale GridEx exercises provide electricity organizations with the opportunity to respond to simulated cyber and physical security attacks affecting the reliable operation of the North American grid.

Increasing participation rates indicate the extent to which organizations consider the evolving GridEx program to be a valuable learning opportunity. Increasing participation may indicate the extent to which the electricity industry as a whole is ready to respond to a real cyber or physical attack. The metric distinguishes between “active” and “observing” organizations. Active organizations participate by assigning staff to participate in the exercise from their work locations at control centers or power plants as if it were a real event. Observing organizations participate in a more limited way, typically through an internal tabletop exercise. The metric shows a significant increase in total numbers of participating electricity organizations and an increasing proportion of active organizations.

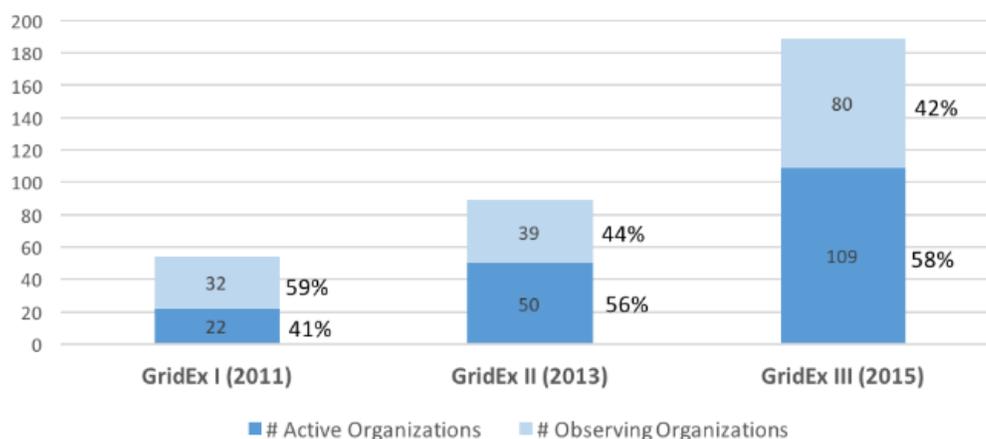


Figure G.6: GridEx Participants

Roadmap for Future Metrics Development

The BESSMWG and the E-ISAC have developed a roadmap for future metrics development, including refining the initial set of metrics that are based on operational experience. The roadmap addresses consideration of the challenges associated with collecting security-related data:

- Historically, NERC and the E-ISAC have limited data related to cyber and physical security incidents as these incidents have been relatively rare and have had little or no impact on BPS reliability.
- Nobody yet knows the magnitude or number of constantly changing security threats and vulnerabilities with any degree of certainty, particularly as they relate to BPS reliability.
- The number and type of cyber systems and equipment used by the industry is vast, making it difficult to develop metrics that are meaningful to individual entities across the industry.
- Data that details security threats, vulnerabilities, and real incidents is highly sensitive. Handled inappropriately, this can expose vulnerabilities and encourage adversaries to develop new and more sophisticated exploits.

The BESSMWG has researched security metrics developed by leading experts outside the electricity industry and examined over 150 of these to assess their applicability from a BPS reliability perspective. Out of these 150 metrics, the BESSMWG concluded that about 30 would be relevant. This assessment underscores the challenges associated with developing relevant and useful security metrics that rely on data willingly and ably provided by individual entities. The BESSMWG will continue to investigate potential new physical and cyber security metrics.

Two particular areas stand out for further study during 2017:

- The extent to which the industry uses automated communications methods¹⁷⁶ to share cyber security information between individual organizations and the E-ISAC.
- While global cyber security vulnerabilities and incidents provide a very high-level view of threats facing the industry, a more relevant metric for the industry would focus on EMS and SCADA commonly used by the electricity industry.

¹⁷⁶ For example, CRISP uses information sharing devices to collect and transmit security information from electricity operator participant sites. Data is shared with CRISP participants, and unattributed data is shared with the broader E-ISAC membership. For organizations not participating in the CRISP program, TAXII, STIX, and CybOX are community-driven technical specifications designed to enable automated information sharing for cyber security situational awareness, real-time network defense, and sophisticated threat analysis. These methodologies are international in scope and free for public use.

Appendix H: Abbreviations Used in This Report

Acronym	Description
AC	Alternating Current
ACE	Area Control Error
ACSETF	AC Substation Equipment Task Force
AESO	Alberta Electric System Operator
ALR	Adequate Level of Reliability
ANOVA	Analysis of Variance
AOO	Asset Owners and Operators
APC	Element Availability Percentage
BA	Balancing Authority
BAL	Resource and Demand Balancing
Bcf	Billion cubic feet
BES	Bulk Electric System
BESSMWG	BES Security Metrics Working Group
BPS	Bulk Power System
BPSA	Bulk Power System Awareness
CAISO	California Independent System Operator
CAISS	Cyber Automated Information Sharing System
CAP	Corrective Action Plan
CAT	Category
CCC	Compliance and Certification Committee
CDM	Common/Dependent Mode
CEATI	Centre for Energy Advancement through Technical Innovation
CIP	Critical Infrastructure Protection
CIPC	Critical Infrastructure Protection Committee
CP-1	Compliance Process-1
CP-2	Compliance Process-2
CRISP	Cybersecurity Risk Information Sharing Program
CVSS	Common Vulnerability Scoring System
DADS	Demand Response Availability Data System
DADSWG	Demand Response Availability Data System Working Group
DCS	Disturbance Control Standard
DDoS	Distributed Denial-of-Service
DER	Distributed Energy Resources
DERTF	Distributed Energy Resources Task Force
DHS	Department of Homeland Security
DNS	Domain Name System
DOE	Department of Energy
DP	Distribution Provider
DR	Demand Response
DUC	Defense Use Case
EA	Event Analysis
EAR	Event Analysis report
EAS	Event Analysis Subcommittee
EEA	Energy Emergency Alert
EFOR	Equivalent Forced Outage Rate

Acronym	Description
EFORd	Equivalent Forced Outage Rate – demand
EI	Eastern Interconnection
E-ISAC	Electricity Information Sharing and Analysis Center
EMS	Energy Management Systems
EMSWG	Energy Management System Working Group
EOP	Emergency Operations
EPRI	Electric Power Research Institute
ERCOT	Electric Reliability Council of Texas
ERO	Electric Reliability Organization
ERS	Essential Reliability Services
ERSWG	Essential Reliability Service Working Group
ESCC	Electricity Subsector Coordinating Council
eSRI	Event Severity Risk Index
EU	European Union
FACTS	Flexible Alternating Current Transmission Systems
FBI	Federal Bureau of Investigation
FERC	Federal Energy Regulatory Commission
FR	Frequency Response
FRCC	Florida Reliability Coordinating Council
FWG	Frequency Working Group
GADS	Generating Availability Data System
GADSWG	Generating Availability Data System Working Group
GO	Generator Owner
GOP	Generator Operator
GridEx	Grid Exercise
HP	Human Performance
Hz	Hertz
ICC	Initiating Cause Code
ICS	Industrial Control System
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IFRO	Interconnection Frequency Response Obligation
IOC	Indicators of Compromise
IoT	Internet of Things
IROL	Interconnection Reliability Operating Limit
ISAC	Information Sharing and Analysis Centers
ISO	Independent System Operator
ISO-NE	ISO New England
IT	Information Technology
JAR	Joint Analysis Report
KCMI	Key Compliance Monitoring Index
LTRA	Long Term Reliability Assessment
MEC	Member Executive Committee
MEITF	Methods of Establishing IROs Task Force
MEPS	Member Engagement, Products, and Services
MRO	Midwest Reliability Organization
MSSC	Most Severe Single Contingency
MVA	Mega Volt Ampere

Acronym	Description
MW	megawatt
MWh	megawatt hour
NAGF	North American Generator Forum
NATF	North American Transmission Forum
NCCIC	National Cybersecurity and Communications Integration Center
NCI	National Council of ISACs
NCIRP	National Cyber Incident Response Plan
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NOI	Notice of Inquiry
NOP	Notice of Penalty
NOPR	Notice of Proposed Rulemaking
NPCC	Northeast Power Coordinating Council
NYISO	New York Independent Service Operator
OC	Operating Committee
OE	Office of Electricity Delivery and Energy Reliability
OTT	Operations, Tools, and Technologies
OY	Operating Year
PAS	Performance Analysis Subcommittee
PC	Planning Committee
PCS	Protection and Controls Subcommittee (SERC)
PNNL	Pacific Northwest National Laboratory
PRC	Protection and Control
PRS	Protective Relay Subcommittee
PwC	PricewaterhouseCoopers LLC
QI	Québec Interconnection
RAS	Remedial Action Scheme
RC	Reliability Coordinator
RCIS	Reliability Coordinator Information System
RE	Regional Entities
RF	ReliabilityFirst
RISC	Reliability Issues Steering Committee
RPS	Renewable Portfolio Standard
RS	Resources Subcommittee
RSG	Reserve Sharing Group
RTO	Regional Transmission Organization
SAMS	System Analysis and Modeling Subcommittee
SANS	System Administration, Networking, and Security
SAS	Statistical Analysis System
SCC	Sustained Cause Code
SERC	SERC Reliability Corporation
SNL	Sandia National Laboratories
SOL	System Operating Limit
SPCS	System Protection and Control Subcommittee (NERC)
SPCWG	System Protection & Control Working Group (SPP)
SPOD	Single Point of Disruption
SPP-RE	Southwest Power Pool Regional Entity

Acronym	Description
SPS	Special Protection Schemes
SPWG	System Protection Working Group (TRE)
SRI	Severity Risk Index
SS	Statistically Significant
SVC	Static Var Compensators
TADS	Transmission Availability Data System
TADSWG	Transmission Availability Data System Working Group
Texas RE	Texas Reliability Entity
TOP	Transmission Operators
TOS	Transmission Outage Severity
UFLS	Underfrequency Load Shed
WECC	Western Electricity Coordinating Council
WEFOR	Weighted Equivalent Forced Outage Rate
WI	Western Interconnection

Appendix I: Contributions

NERC would like to express its appreciation to the many people who provided technical support and identified areas for improvement. These include the NERC Industry Groups in [Table H.1](#), Contributing Regional Staff in [Table H.2](#), and NERC Staff in [Table H.3](#).

Table H.1: NERC Industry Group Acknowledgements	
Group	Officers
Planning Committee Reviewers	Chair: David Weaver, Peco Energy Vice Chair: Brian Evans-Mongeon, Utility Services, Inc. Gary Brownfield, Ameren Services Phil Fedora, NPCC Michael Goggin, American Wind Energy Association Wayne Guttormson, Sask Power David Mercado, Center Point Energy Katy Onnen, Kansas City Power and Light Russell Schussler, Georgia Transmission Branden Sudduth, WECC Carl Turner, Florida Municipal Power Agency Brian Van Gheem, ACES
Operating Committee Reviewers	Chair: Jim Case, Entergy Vice Chair: Lloyd Linke, WAPA Peter Brandien, ISO-New England Alan Bern, Oncor Stuart Goza, TVA Hassan Hamdar, FRCC Jeffrey Harrison, Associated Electric Cooperative Inc. Sydney Jackson, Rochester Public Utilities Michelle Rheault, Manitoba Hydro Sammy Roberts, Duke Energy David Zwergel, MISO
Critical Infrastructure Protection Committee Reviewers	Chair: Marc Child, Great River Energy Vice Chair: Nathan Mitchell, APPA Vice Chair: David Revill, GTC
Bulk Electric System Security Metrics Working Group (BESSMWG)	Chair: Larry Bugh, Reliability First
Performance Analysis Subcommittee	Chair: Paul Kure, ReliabilityFirst Vice Chair: Maggie Peacock, WECC State of Reliability Report Lead: John Seidel, MRO Statistical & SRI Support: Heide Caswell, PacifiCorp
Demand Response Availability Data System Working Group	Chair: Bob Reynolds, SPP RE Vice Chair: Joe Ballantine, ISO-New England
Events Analysis Subcommittee	Chair: Hassan Hamdar, FRCC Vice Chair: Rich Hydzik, Avista Corporation
Generation Availability Data System Working Group	Chair: Leeth DePriest, Southern Company Vice Chair: Steve Wenke, Avista Corporation Additional Support: Ron Fluegge, GADSOS
Transmission Availability Data System Working Group	Chair: Kurt Weisman, ATC Vice Chair: Brian Starling, Dominion

Table H.1: NERC Industry Group Acknowledgements

Resources Subcommittee	Chair: Troy Blalock, SCE&G Vice Chair: Tim Reynolds, WECC
Operating Reliability Subcommittee	Chair: Eric Senkowicz, FRCC Vice Chair: Dave Devereaux, IESO
Frequency Working Group	Chair: Tony Nguyen, BC Hydro
Reliability Assessment Subcommittee	Chair: Phil Fedora, NPCC Vice Chair: Tim Fryfogle, Reliability First
System Protection and Control Subcommittee	Chair: Rich Quest, Midwest Reliability Org Vice Chair: Mark Gutzmann, Xcel Energy
Compliance and Certification Committee	Chair: Patricia E. Metro, NRECA Vice Chair: Jennifer Flandermeyer, KCP&L

Table H.2: Contributing Regional Staff

Name	Regional Entity
ERO - Executive Management Group	
Regional Subject Matter Experts	
Vince Ordax	FRCC
John Seidel	MRO
Phil Fedora	NPCC
Paul Kure	RF
Brian Thumm	SERC
Bob Reynolds	SPP RE
David Penney	Texas RE
Maggie Peacock	WECC

Table H.3: NERC Staff

Name	Officers	E-mail Address
Mark Lauby	Senior Vice President and Chief Reliability Officer	mark.lauby@nerc.net
James Merlo	Vice President and Director, Reliability Risk Management	james.merlo@nerc.net
David Till	Senior Manager, Performance Analysis	david.till@nerc.net
Brad Gordon	Manager, Performance Analysis, Balancing and Frequency Control	brad.gordon@nerc.net
Svetlana Ekisheva	Senior Manager, Statistical Analysis and Outreach	svetlana.ekisheva@nerc.net
Jack Norris	Engineer, Performance Analysis	jack.norris@nerc.net
Margaret Pate	Reliability Risk Control Liaison, Performance Analysis	margaret.pate@nerc.net
Donna Pratt	Manager, Performance Analysis, Data Analytics	donna.pratt@nerc.net
Elsa Prince	Principal Advisor, Performance Analysis	elsa.prince@nerc.net
Lee Thaubald	Technical Analyst, Performance Analysis	lee.thaubald@nerc.net
Matthew Varghese	Senior Engineer, Performance Analysis	matthew.varghese@nerc.net
Katrina Blackley	Administrative Assistant	katrina.blackley@nerc.net
Rich Bauer	Associate Director, Event Analysis	rich.bauer@nerc.net

Table H.3: NERC Staff

Name	Officers	E-mail Address
Laura Brown	Director, Programs and Engagement	laura.brown@nerc.net
Terry Campbell	Manager of Technical Publications	terry.campbell@nerc.net
Alex Carlson	Technical Publications Specialist	alex.carlson@nerc.net
Thomas Coleman	Director, Reliability Assessments	thomas.coleman@nerc.net
Bob Cummings	Senior Director, Engineering and Reliability Initiatives	bob.cummings@nerc.net
Howard Gugel	Senior Director, Standards	howard.gugel@nerc.net
Aaron Hornick	Senior Enforcement Analyst, Enforcement	aaron.hornick@nerc.net
Ed Kichline	Senior Counsel and Director of Enforcement	ed.kichline@nerc.net
Ben McMillan	Manager, Event Analysis	ben.mcmillan@nerc.net
Mani Mardhekar	Senior Engineer, Bulk Power System Awareness	mani.mardhekar@nerc.net
Kimberly Mielcarek	Senior Director of Communications	kimberly.mielcarek@nerc.net
John Moura	Director of Reliability Assessment and Systems Analysis	john.moura@nerc.net
Elliott Nethercutt	Senior Technical Advisor, Reliability Assessments	elliott.nethercutt@nerc.net
Steve Noess	Director of Standards Development	steve.noess@nerc.net
Ryan Quint	Senior Manager, System Analysis	ryan.quint@nerc.net
Janet Sena	Senior Vice-President, Policy and External Affairs	janet.sena@nerc.net
Sandy Shiflett	Senior Program Specialist	sandy.shiflett@nerc.net
Jule Tate	Associate Director, Events Analysis	jule.tate@nerc.net
Ganesh Velummylum	Senior Manager, System Analysis	ganesh.velummylum@nerc.net
Tobias Whitney	Senior Manager, CIP, Grid Assurance	tobias.whitney@nerc.net
Kristen Worosz	Senior Advisor, E-ISAC Products and Services	Kristen.Worosz@eisac.com