

Spring 2018 Compliance and Standards Workshop May 23 - 24, 2018

Criteria Services Update

Gerry Dunbar
Manager, Reliability Criteria

Criteria Services Program Area 2018 Initiatives

- A-10 Classification of BPS Elements
- Strategic Review of NPCC Criteria
- Remedial Action Schemes (RAS)

NPCC Criteria

- NPCC Full Members Develop and ‘Own’ Criteria
- Who:
 - NPCC Full Members Obligated to Comply
 - Non-Members via Other Agreements (Tariff and Interconnection)
- What:
 - Applies to the NPCC Bulk Power System (A-10 Methodology)
- Why:
 - Section 313 NERC Rules of Procedure
 - Promote Reliability
 - Augment and Enhance ERO Standards

A-10

BPS Classification

- Scope of Review:
 - Identify critical facilities for the applicability of NPCC criteria
 - Simplify the existing methodology to make it less labor intensive
 - Improve consistency across areas in application and outcomes
- Phase #1 2017:
 - Review Existing Methodology
 - Propose Improvements
 - Propose New Methodologies
 - Recommendation to the RCC for Testing.

A-10

BPS Classification

- Phase #2 2018:
 - Testing of 3 RCC Approved Methodologies.
 - First Iteration of Test Results to the Task Forces June 2018.
 - RCC Endorsement of a Preferred Methodology December 2018
- Anticipated 2019 Activity:
 - Revise A-10 Document
 - Open Process Postings
 - Full Member Ballot

Strategic Review of NPCC Criteria

- Strategic Review of the Need for NPCC More Stringent Criteria.
 - Directed by the NPCC Board of Directors.
 - Arranged by Focus Area
 - Operations
 - Planning
 - Protection
 - High Level
 - Not Directory Specific or Requirement by Requirement.
- Action Plan and Scope Approved April 2018.
 - Task Force Review August 2018.
- RCC and RSC Review and Comment September 2018.
- Final Report to RCC and RSC December 2018.

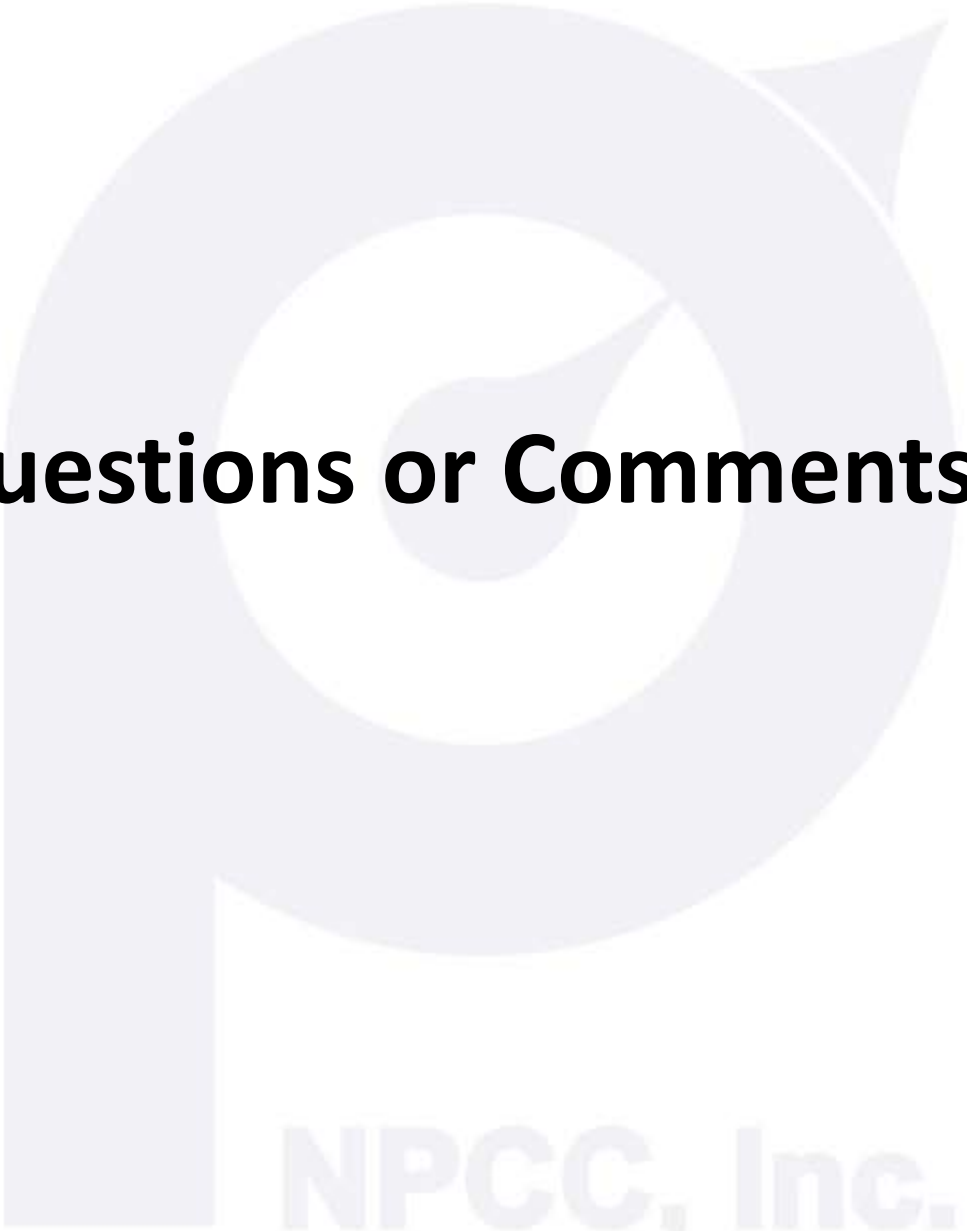
Remedial Action Schemes (RAS)

- RAS Definition Approved by FERC 11/19/2015
 - Continent wide need to establish a uniform definition.
 - NERC Glossary term for SPS revised ('See RAS')
- PRC-012-2 (RAS) Approved by FERC 9/20/2017
 - PRC-12-1, PRC 13-1, PRC-14-1 Withdrawn
 - PRC-15-1 and PRC-16-1 Retired
- PRC-012-2
 - Limited Impact RAS Established (NPCC Type III)
 - Regional Review Retained

Remedial Action Schemes (RAS)

NPCC Transition

- NPCC Transition to RAS:
 - Existing NPCC RAS/SPS List:
 - SPS that conform to Revised Definition of RAS
 - SPS does not conform
 - Newly Identified RAS
 - Regional Review.
 - NPCC Glossary Term SPS
 - ‘See NERC RAS’
 - NPCC Directory #7 –Appendix B
 - Other NPCC Documents

A large, light gray watermark of the NPCC logo is centered in the background of the slide. It consists of a large 'p' with a circular arrow inside, and the text 'NPCC, Inc.' below it.

Questions or Comments ?



NPCC Spring 2018

NAGF Update

Agenda



- **NAGF – what, who and how**
- **Cold Weather Preparations**
- **Recent & Upcoming Activities**

What is the NAGF?



The NAGF is an independent, member-driven, non-profit organization of generator owners and operators, focused on NERC and other grid reliability issues.

Our mission is to promote the safe, reliable operation of the generator segment of the bulk electric system through collaboration with grid operators and regulators.

What we do



We provide a unified voice for the generator segment to NERC and the Regional Entities.

We do this through open source collaboration and information exchange among our members and with other industry professionals.



NAGF's dual focus



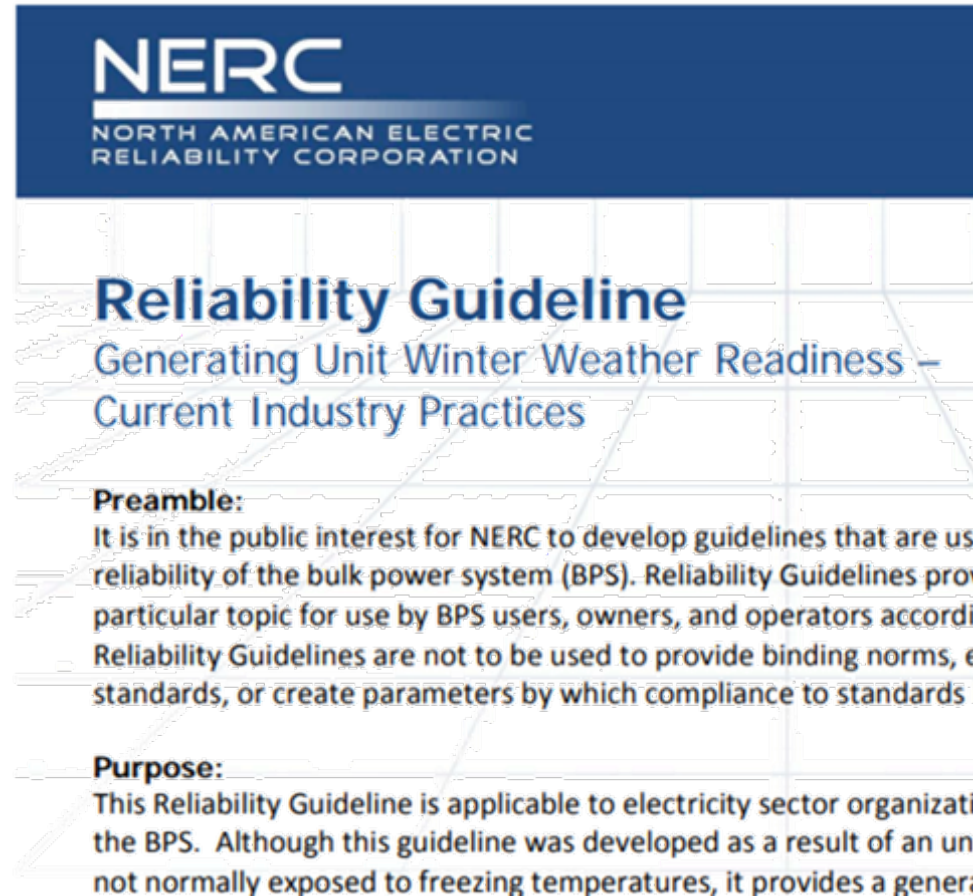
- Compliance with existing Standards
 - “The here and the now”
 - Collaborative efforts
 - Best Practice sharing
 - Discussion boards, file cabinet, etc. on Groupsite

- Shaping policy
 - Helping paint the futurescape
 - Ensuring the unique perspective of the generation segment is understood and accounted for.
 - Improve “first time success” of new regulations

Cold Weather Preparations



- Lots of attention in the wake of the Polar Vortex '14
 - Created a Working Group to assemble information
 - Created a Greatest Hits document
- NERC engaged NAGF to review and revise:
Reliability Guideline for Generating Unit Winter Weather Readiness – Current Industry Practices



Cold Weather Preparations



- Winter 2018
 - Improved Reliability and Resiliency
 - Trending in the right direction



Recent and Upcoming Activities



- Coordinated with UVIG to kickstart the IRPTF
 - Initial meeting in Washington DC fall '17

<https://www.nerc.com/comm/PC/Pages/Inverter-Based-Resource-Performance-Task-Force.aspx>
- Frequency Response & Battery Storage Workshop, August 1-2, Washington DC
- FERC discussions:
 - Changing resource mix
 - Shifting from OER to market / policy
 - FERC's CIP Audits

FERC's CIP audits



- **FERC completed 5 CIP audits in 2017; planning more 3 in 2018**
 - Non-public audits
 - Notification 120 days prior to coming onsite
 - Regional Entities do not know ahead of time
 - Measured compliance with CIP standards, then went beyond
 - Potential Violations were handed over to the Regional Entity
 - Addressed risk and overall cyber security – generated ORIs
 - Other Risks Identified
 - Ex: - interactive remote access – dual homed machines
 - Developed a 23 page report with 21 lessons learned

FERC's CIP audits

➤ Highlights: ORIs

- Consider all generation assets, not just BES, when determining impact rating. (Control Centers...)
- Identify & categorize cyber systems used to support generation **ex – gas yard feeding multiple plants**
- Review physical key management to ensure the same rigor in policies and testing procedures used for electronic access is applied to physical keys
- Perform regular inspections of BCSs to ensure no unidentified Electronic Access Points (EAPs) exist
- Consider employing host-based malicious code prevention for all BCAs, in addition to network level prevention.

<https://www.ferc.gov/legal/staff-reports/2017/10-06-17-CIP-audits-report.pdf>



2017 Staff Report Lessons Learned from Commission-Led CIP Version 5 Reliability Audits



FERC's CIP audits



Recent and Upcoming Activities



➤ Initial Peer Review – August 2018

- Modeled after NATF's process
- Teams of up to 18 volunteer SMEs from across the NAGF membership come to the host facility/entity
- Scope is controlled by the hosting entity
- Review of up to six technical areas
 - o Compliance Program
 - o Protection Systems and Maintenance Activities
 - o Cyber and Physical Security
 - o Training
 - o Operations (including Cold Weather Preparedness, Normal, and Emergency Operations)
 - o Modeling and Model Verification

Peer Review Schedule



Prior to Peer Review	Action
1 Year – 60 Days	Host Company and potential review teams are identified. Review Teams are trained on conduct of participants and Principals of Excellence for each Technical Area. The host company identifies technical areas to be covered. NDAs are signed by participating review team members.
60 – 45 Days	Host Company has the right of refusal of any participant at host company request. Host company identifies travel (airport), transportation, lodging, and other visitor information to their host location
45 – 30 Days	Each Review Team conducts at least one conference call with Host Company to identify scope of Peer Review
30 – 14 Days	Peer Review Team and Lead conduct readiness meeting with Host Company and Review Teams. Team may request preliminary information that is helpful in identifying scope of review.
Peer Review Day 1	Action
10:00 AM – 12:00 PM	Participants arrive to host city/location
12:00 – 1:00 PM	Host provided lunch (NAGF does ask the host company to provide onsite lunches for participants). Introductions during lunch.
1:00 – 5:00 PM	Conduct Reviews with SMEs from host company
6:00 – 8:00 PM	Optional Break the Ice Dinner for Participants hosted by host company

Peer Review Schedule



Peer Review Day 2	Action
8:00 AM – 12:00 PM	Conduct Reviews with SMEs with host company
12:00 – 1:00 PM	Host provided lunch
1:00 – 3:00	Final Reviews with SMEs with host company
3:00 – 4:30 PM	Review Teams develop exit presentation
4:30 – 6:00 PM	Dry Run Exit Presentation
Peer Review Day 3	Action
8:00 – 9:00 AM	Optional Breakfast by Host – Comments by Peer Lead and Host Company Lead
09:00 – 10:00 AM	Exit Presentation by Peer Review Lead and Review Team Leads
10:00 – 11:00 AM	Questions by the host company
11:00 – 11:15 AM	Final Comments by host company
After Peer Review	Action
0 – 30 Days	Host Company and NAGF will identify too sensitive information to share with members during a Lessons Learned program for NAGF
30 – 60 Days	Review Team Leads will share experience and Best Practices with NAGF during a Lessons Learned Program
6 Months	Host company will be invited to share progress of implementation of recommendations, or share with the Forum why recommendations will not be implemented.

Recent and Upcoming Activities



- NAGF Annual Meeting & Compliance Conference
 - Jim Robb providing Keynote Address
 - ISO/RTO interface session
 - Dual Track: O&P and CIP
 - October 2-3 (4?) in NERC's offices in Atlanta
 - WebEx will be available

NAGF Working Groups



- Security Practices / CIP
- Cold Weather Preparedness
- Standards Review Team
- Training
- Lessons Learned
- Peer Review
- Variable Resources
- Essential Reliability Services

N
E
-
-
N
-
T
F

Collaboration: Groupsite

[SUMMARY](#)[COMMUNICATE ▼](#)[SHARE ▼](#)[NETWORK ▼](#)[WORKING GROUPS ▼](#)[MORE ▼](#)[MANAGER ▼](#)[MY SETTINGS ▼](#)[HELP ▼](#)Notifications **1** [Edit](#)

Everything ▼

Welcome to the North American Generator Forum

The North American Generator Forum (NAGF) was founded in 2009 as a vehicle for utility and non-utility owned generator owners and/or operators to address issues related to registration, compliance, standards development and other NERC-related topics. In 2013, the North American Generator Forum, Inc. became a non-profit, dues-based corporation.

We provide entities who are generator owners and operators in North America a means to collaborate and communicate with FERC, NERC, the Regional Entities, the Canadian Provinces and other organizations with missions similar to ours, with the ultimate goal of improving the reliability of the bulk power system.

More information is available at: <http://generatorforum.org/>

REQUEST TO JOIN BY CLICKING HERE



Add additional storage capacity for sharing documents, photos and more. [Learn More »](#)

THIS GROUP CONSISTS OF

[Edit](#) **445****Group Members**

you can connect with

**205****Discussions**

you can join

**407****Files**

you can download

NAGF Annual Meeting

[Edit](#)

Our annual meeting will be held in NERC's Atlanta Offices on October 2-3, with a potential to add October 4th if we need the time to cover all the topics. More to follow as the agenda comes together...

UPCOMING EVENTS

[Edit](#) **Standard Review Team**

Wednesday, 11am - 12pm EDT

NAGF members



AMEA	DTE Energy	Indeck Energy	NRG	TVA
APGI	Duke Energy	Ingleside Cogen, LP	PG&E	Tri-State G&T
Ameren Missouri	E.ON	Invenergy	Pattern Gulf Wind	TEP
American Electric Power	EDP Renewables	KCP&L	Pattern Energy Group	US SBU
AECI	ENGIE	Lewis County PUD	Penobscot Energy	US BR
Austin Energy	Entergy	MMWEC	PSGC	Vistra Energy
Avista Corp	Essential Power	MEAG Power	Santee Cooper	WEC Energy Group
Basin Electric Power	EthosEnergy	MidAmerican Energy	SCE&G	Westar Energy
Black Hills Corporation	Exelon Generation	Minnesota Power	Southern Company	Xcel Energy
Braintree Electric Light	First Energy Corp.	NAES Corporation	Southwest Generation	
Capital Power	FMPPA	NYP&A	SunPower	
CCI Rensselaer	FPL	NextEra Energy	Sunflower Electric	
Chelan County PUD	Great River Energy	North Carolina Electric	Talen Energy	
Dominion Energy	IL G&E/KY Utilities	NCPA	TECO	

A good presentation must always have...



CIP for Low Impact
is due when??!



Q & A

Northeast Power Coordinating Council, Inc. 2018 Spring Reliability Conference

James Merlo, PhD
VP, Reliability Risk Management
May 24, 2018

RELIABILITY | ACCOUNTABILITY



Wind Event vs. Water Event



Hurricane Ike - 2008 Wind



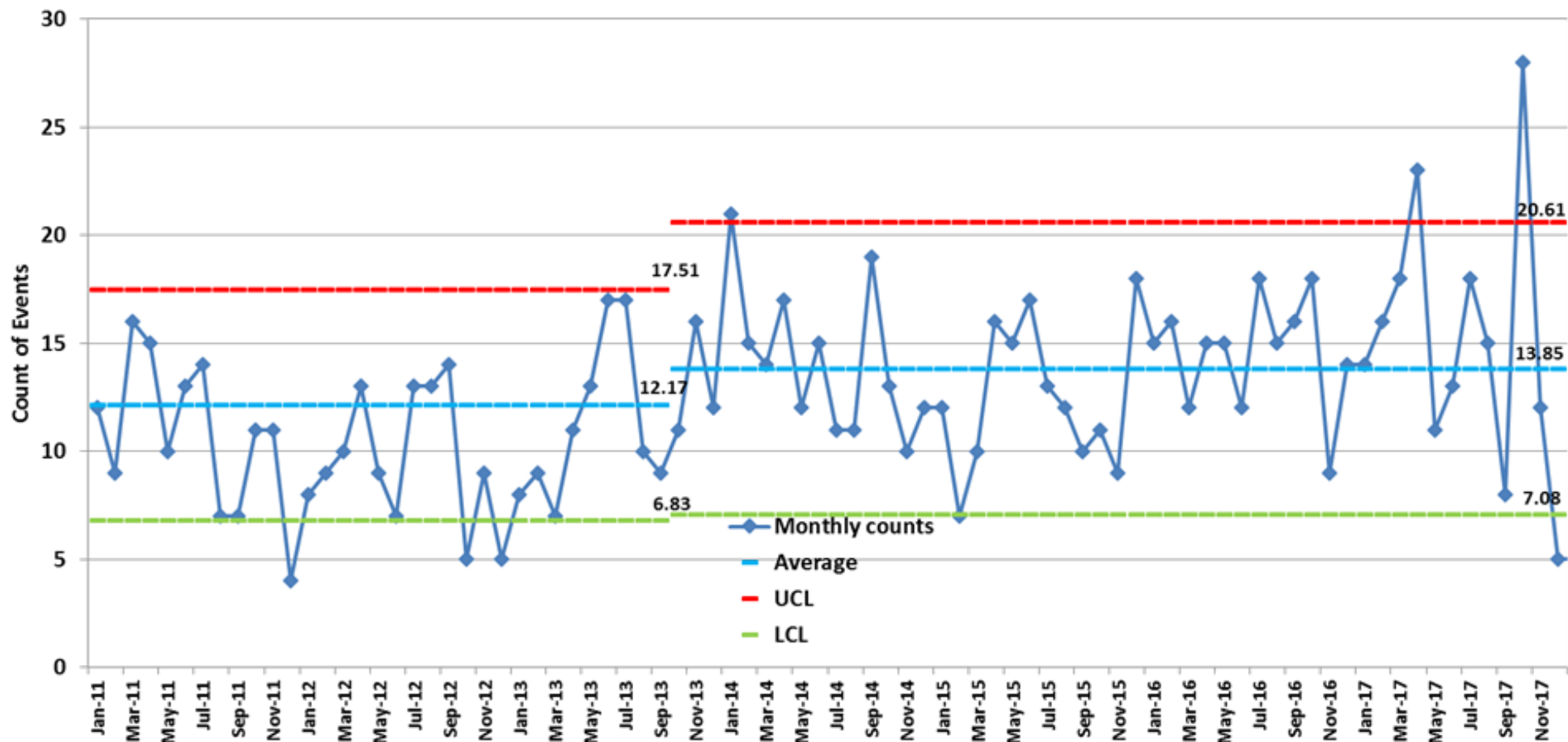
Hurricane Harvey – 2017 Water



- Hurricane Harvey's water flooded Houston and would not quit
- Hurricane Harvey's winds hit South Texas
 - 85 substations damaged
 - 225 transmission line outages
 - Over 850 transmission line structures downed/damaged
 - Over 6000 distribution poles downed/damaged
- Hurricane Irma was the largest impact storm to ever hit Florida
 - A record 4.45 million customers out of service for Florida Power & Light
 - Previous record was 3.24 million during Hurricane Wilma in 2005
 - Irma restoration took only 10 days versus 18 days during Wilma

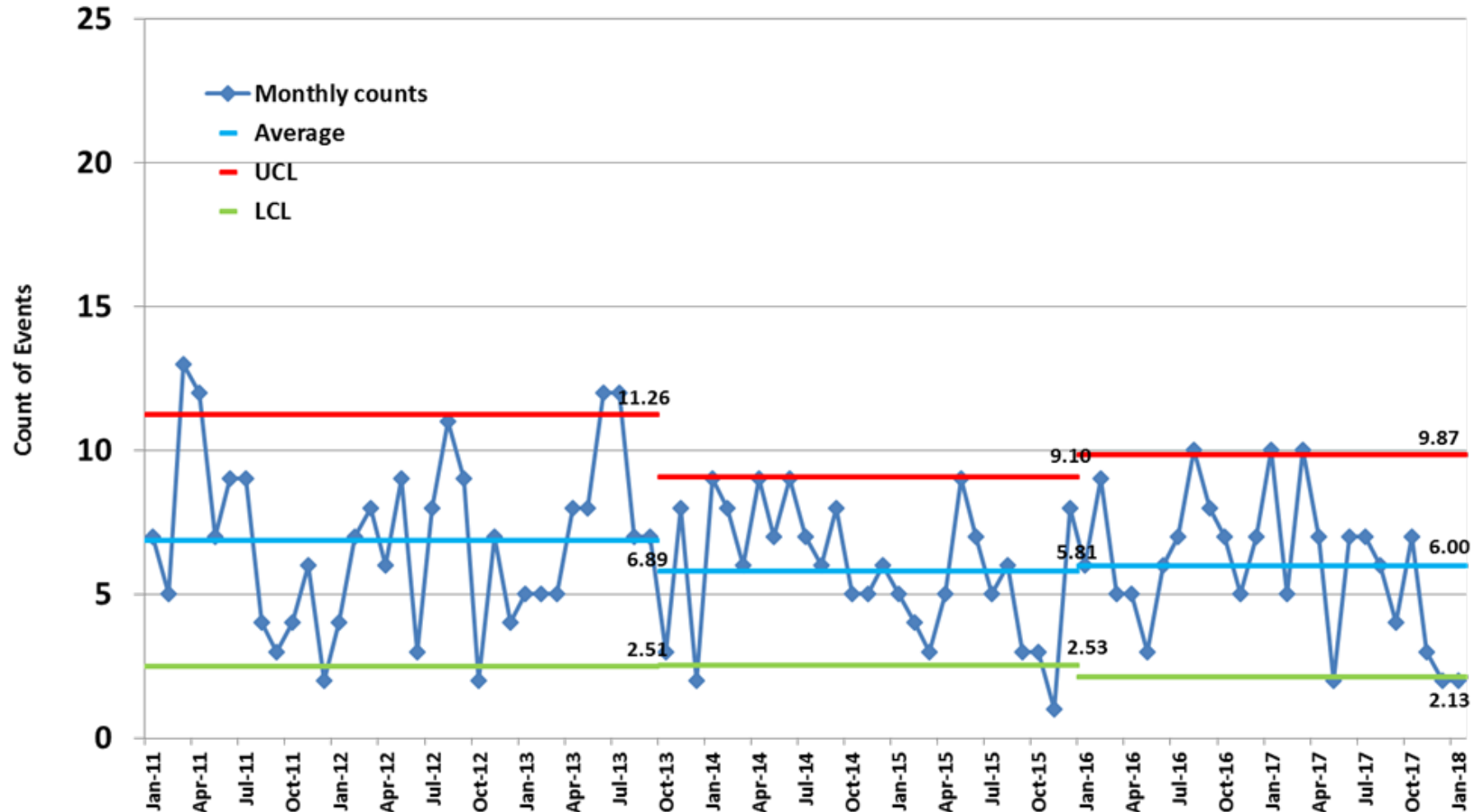
- Drones hastened restoration following both Harvey and Irma with unexpected versatility
- Mutual Assistance agreements provided essential equipment and material for both Harvey and Irma restorations
- Florida and its utilities shortened Irma restoration time with strong, prior investment in system hardening

All Qualified Events (Cat 1 - Cat 5)



Control Chart for the non-EMS Events (Per Month) Over Time

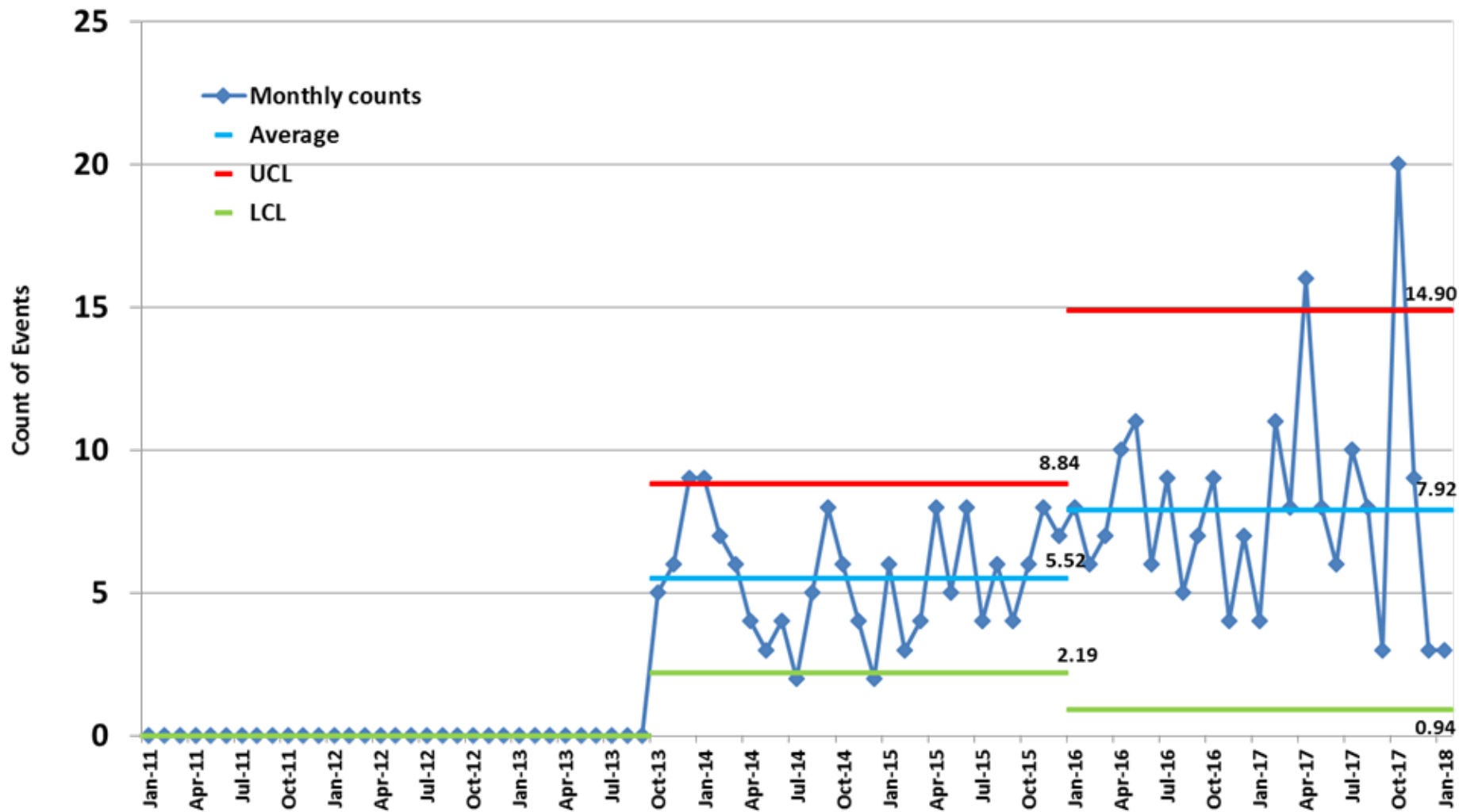
Category 1 Events (non-EMS Events)

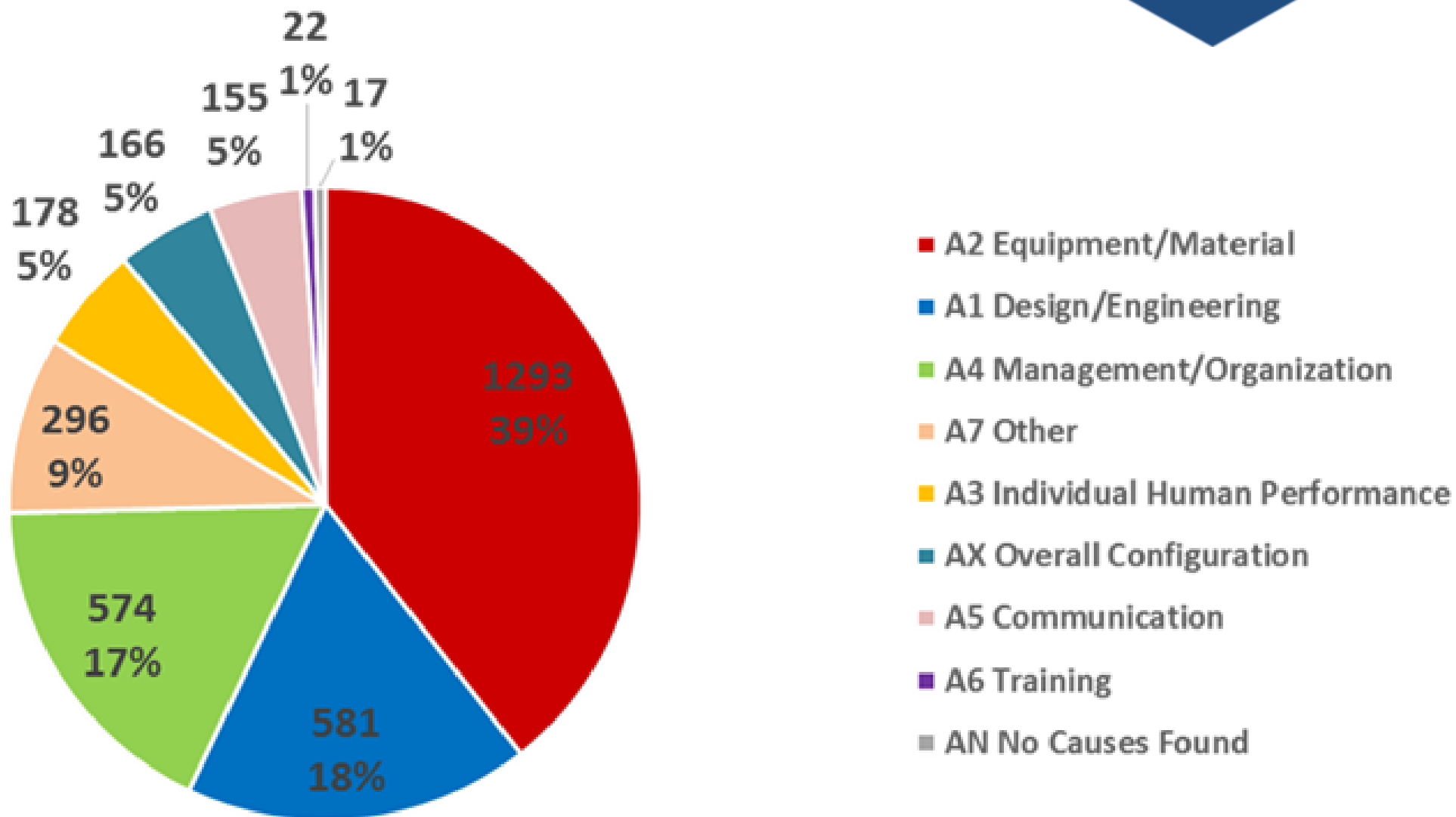


Control Chart for the EMS Events (Per Month) Over Time

Category 1 Events

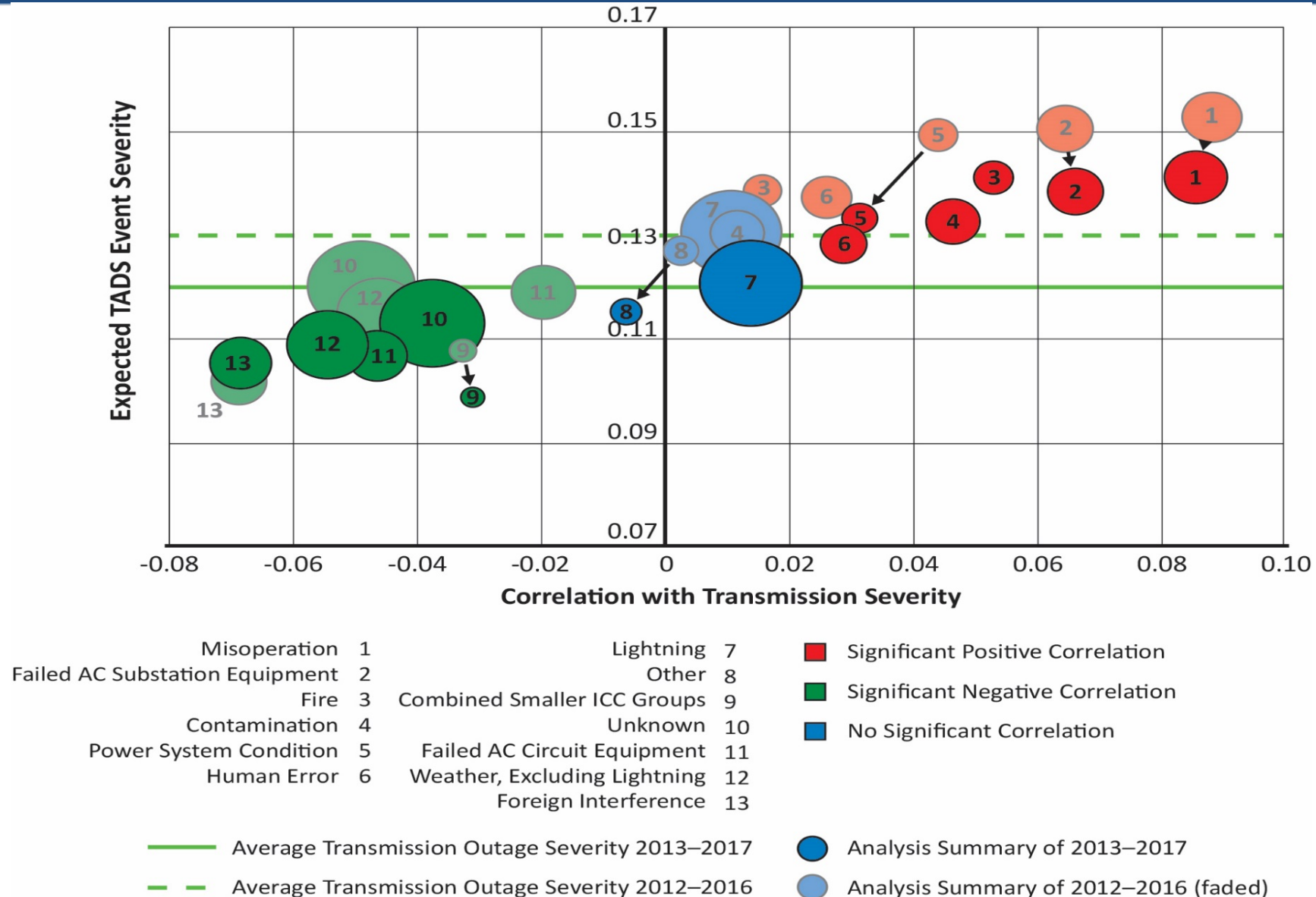
(EMS Events)



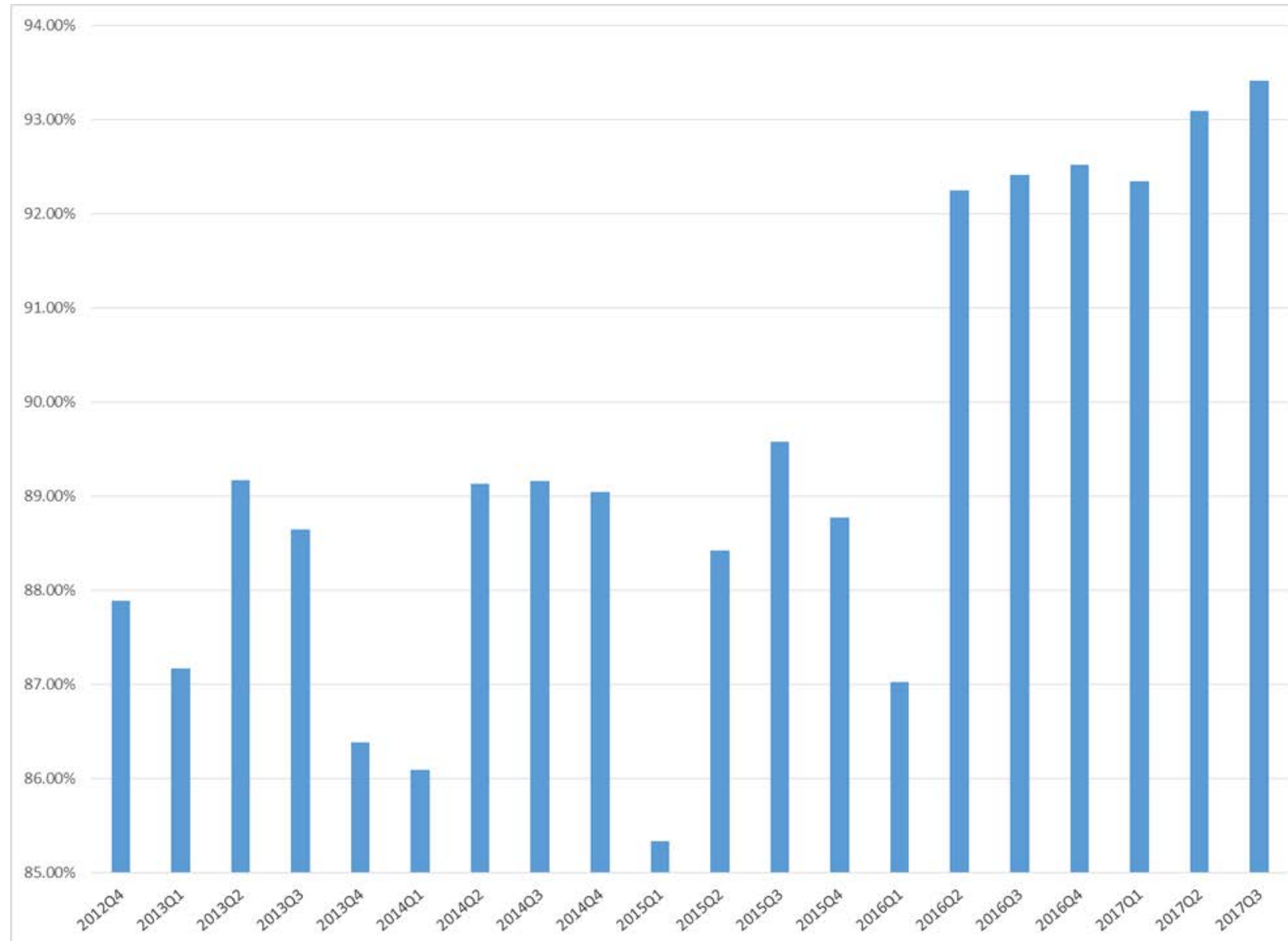


8 943 Events have been cause coded, with 3282 identified causes

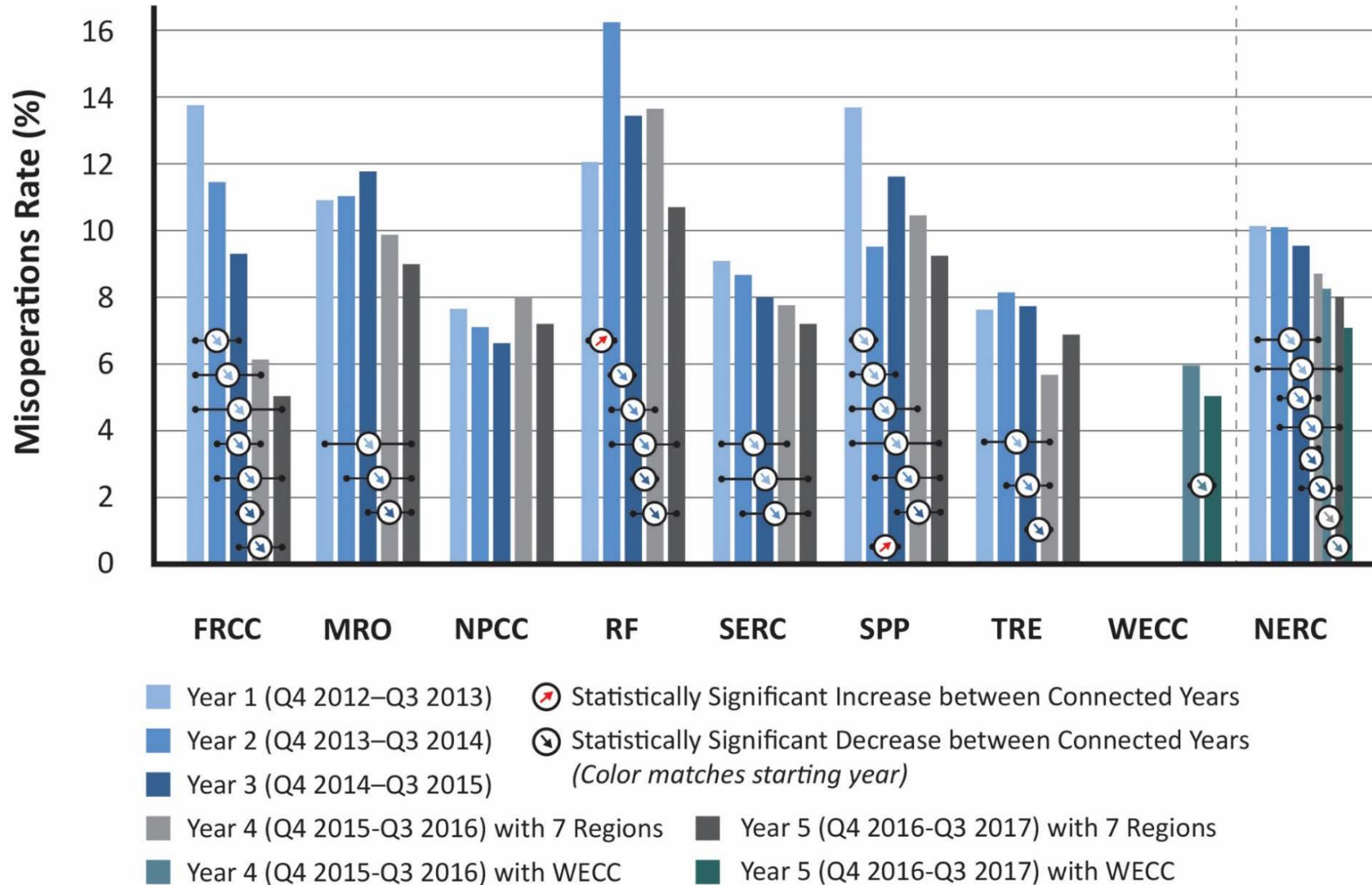
Continued Decline in Average Transmission Outage Severity



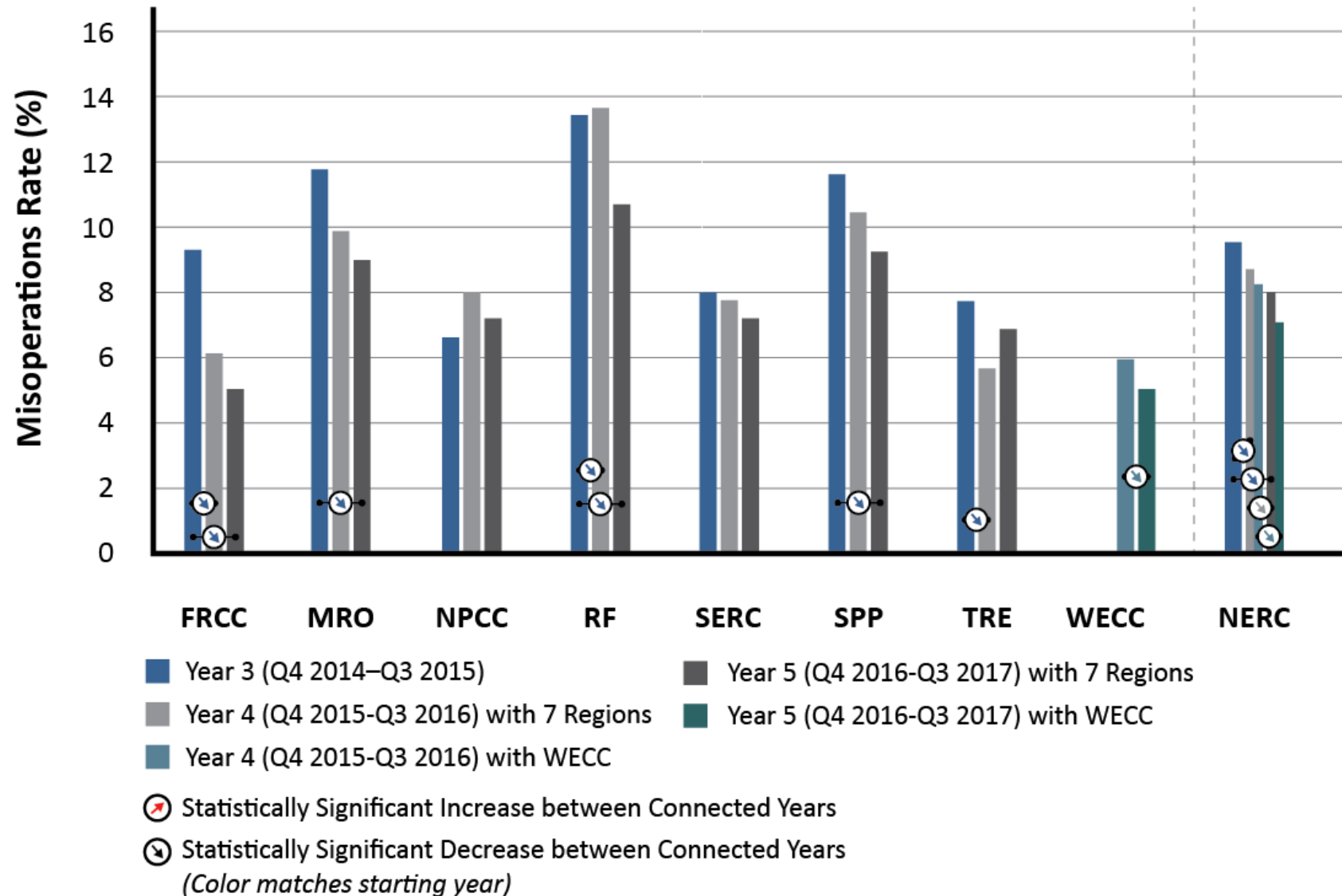
Correct Protection System Operations Rate



Misoperation Rates Continuing to Decline



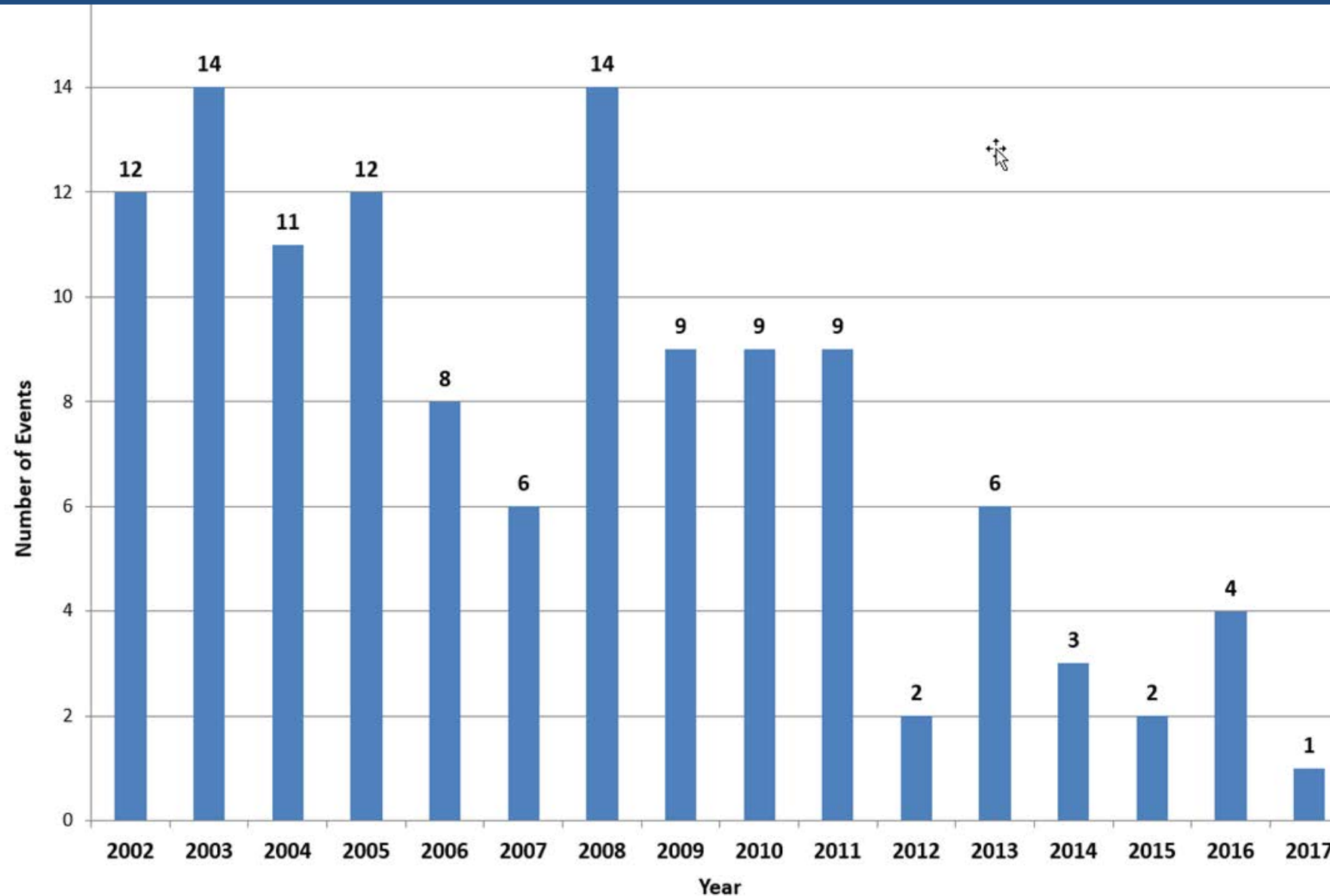
Misoperation Rates Continuing to Decline



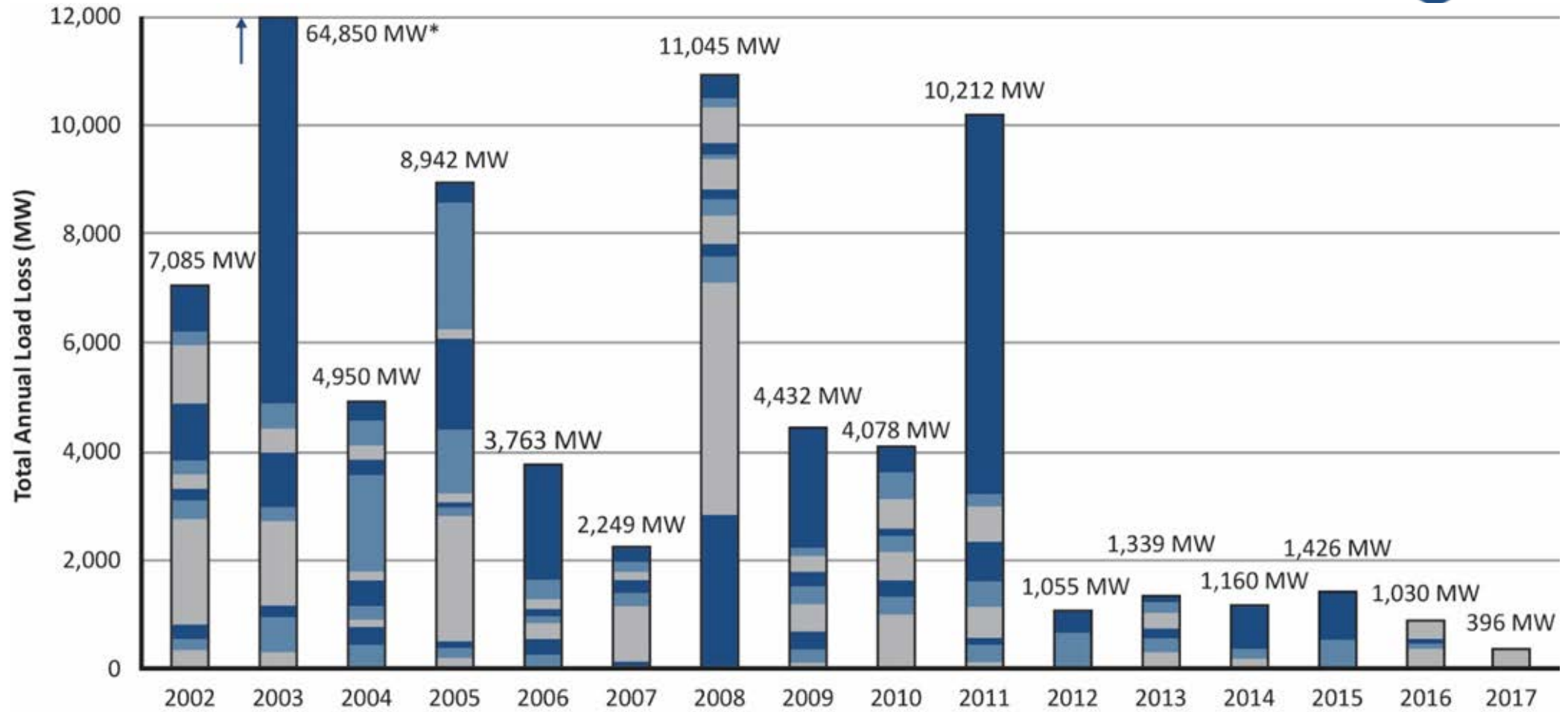
200 kV+ Outages by Cause Code



BPS Transmission Related Events Resulting in Load Loss



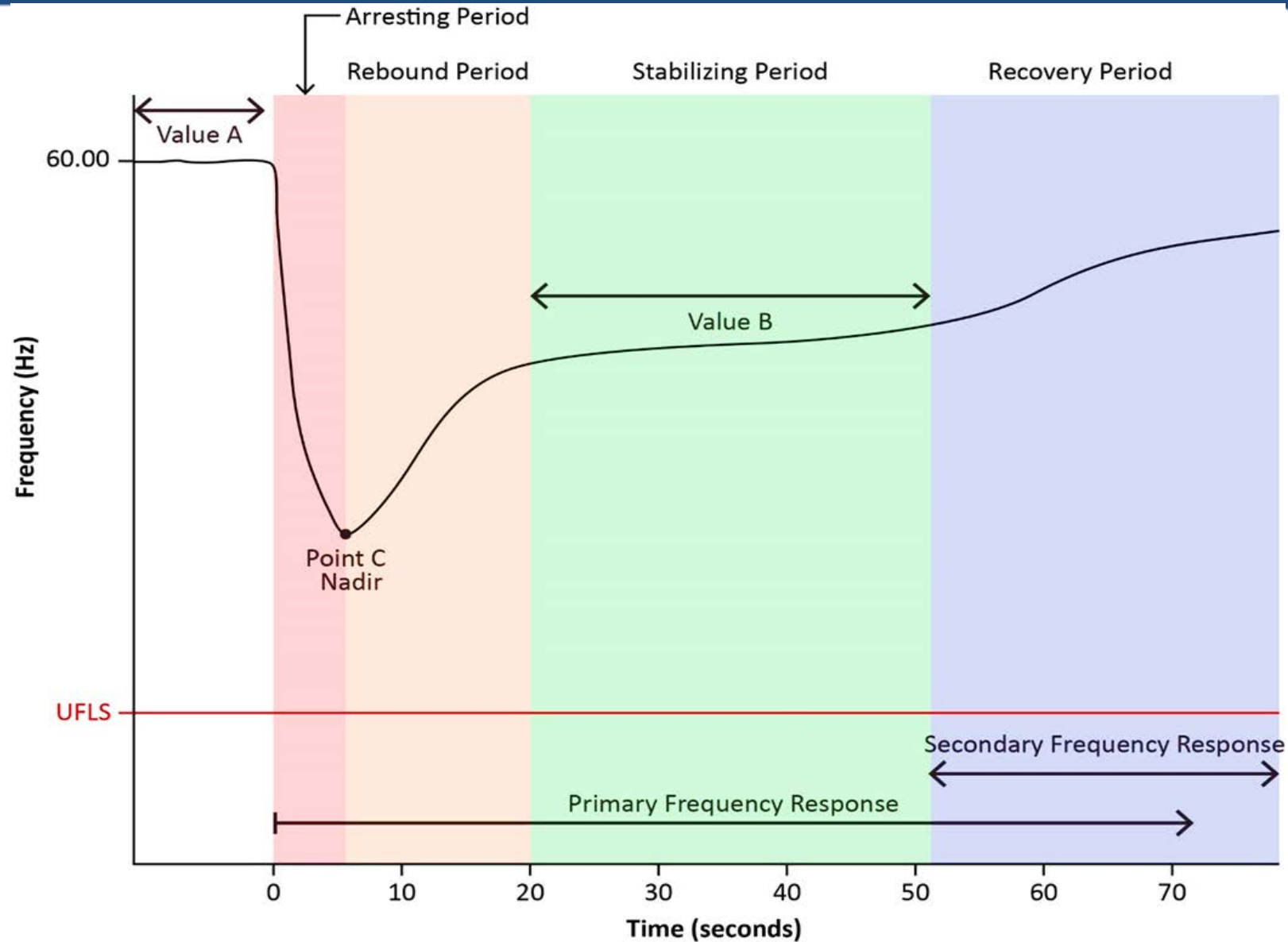
BPS Transmission-Related Events Resulting in Load Loss

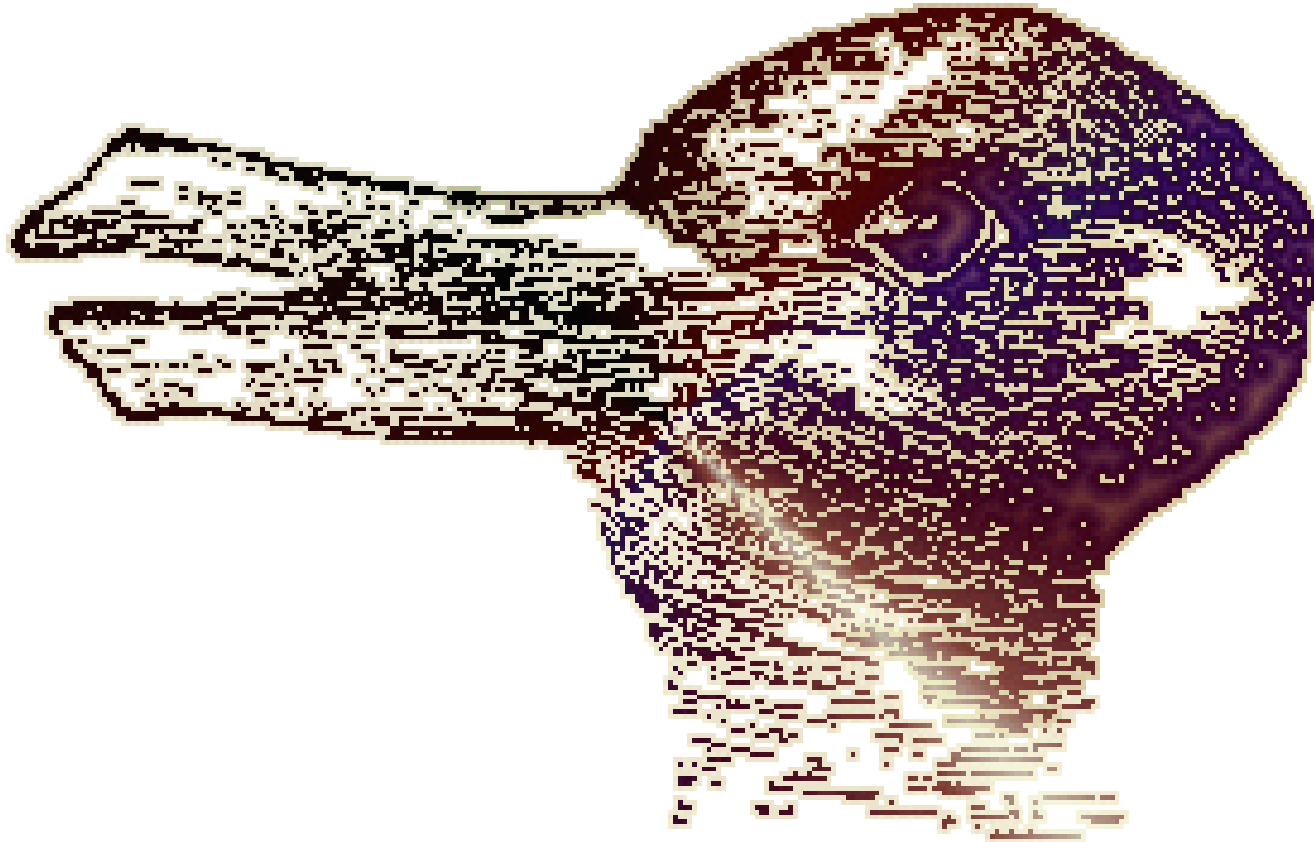


Each band of color represents a different event.

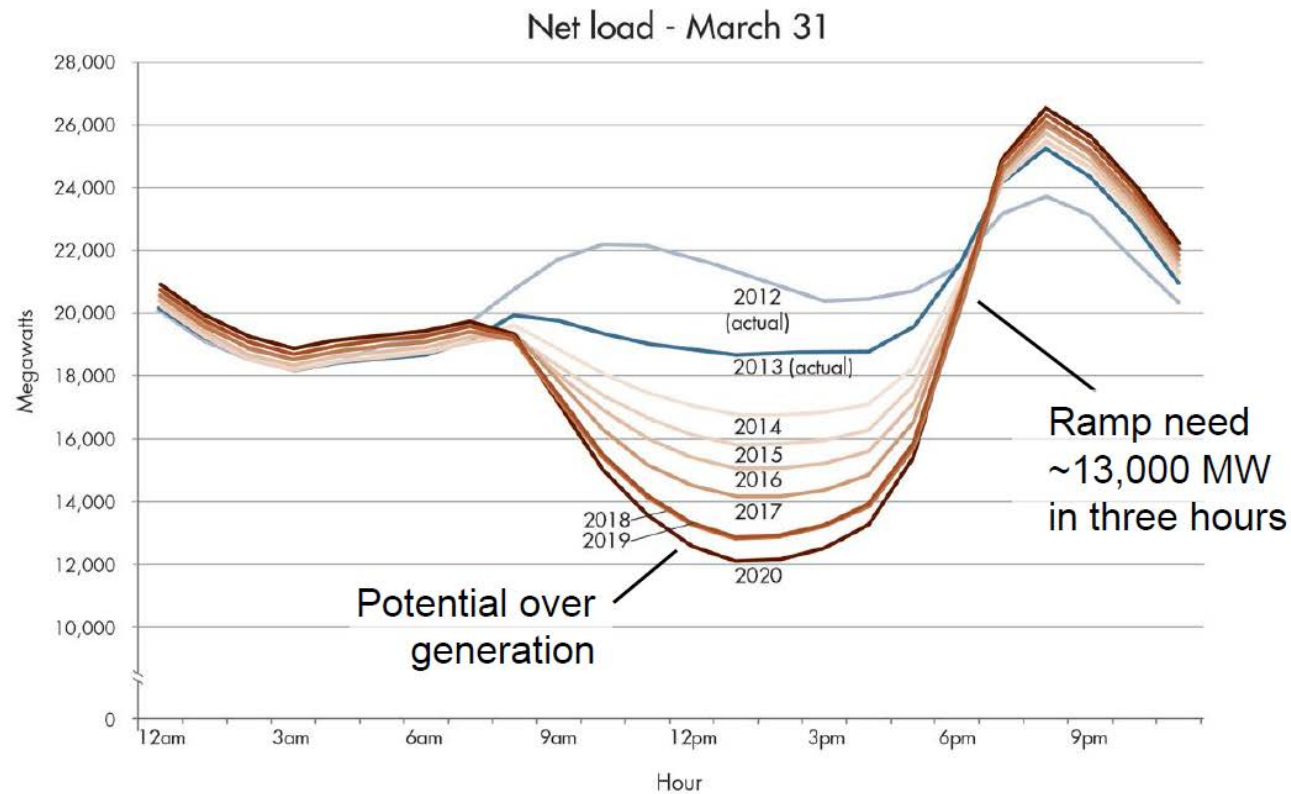
*Vertical axis scale has been reduced due to large value of 2003 NE blackout event.

- Retirement/displacement of conventional generation
 - Variable energy resources
 - Rapid penetration of electronically-coupled resources
- Essential Reliability Services
 - Reduced inertia
 - Frequency Responses
 - Voltage Support
 - Ramping and flexibility needs
- Rapid penetration of new loads
- System controls and protection coordination
- Modeling and simulation constraints
- Increasing interface with distribution-centric resources

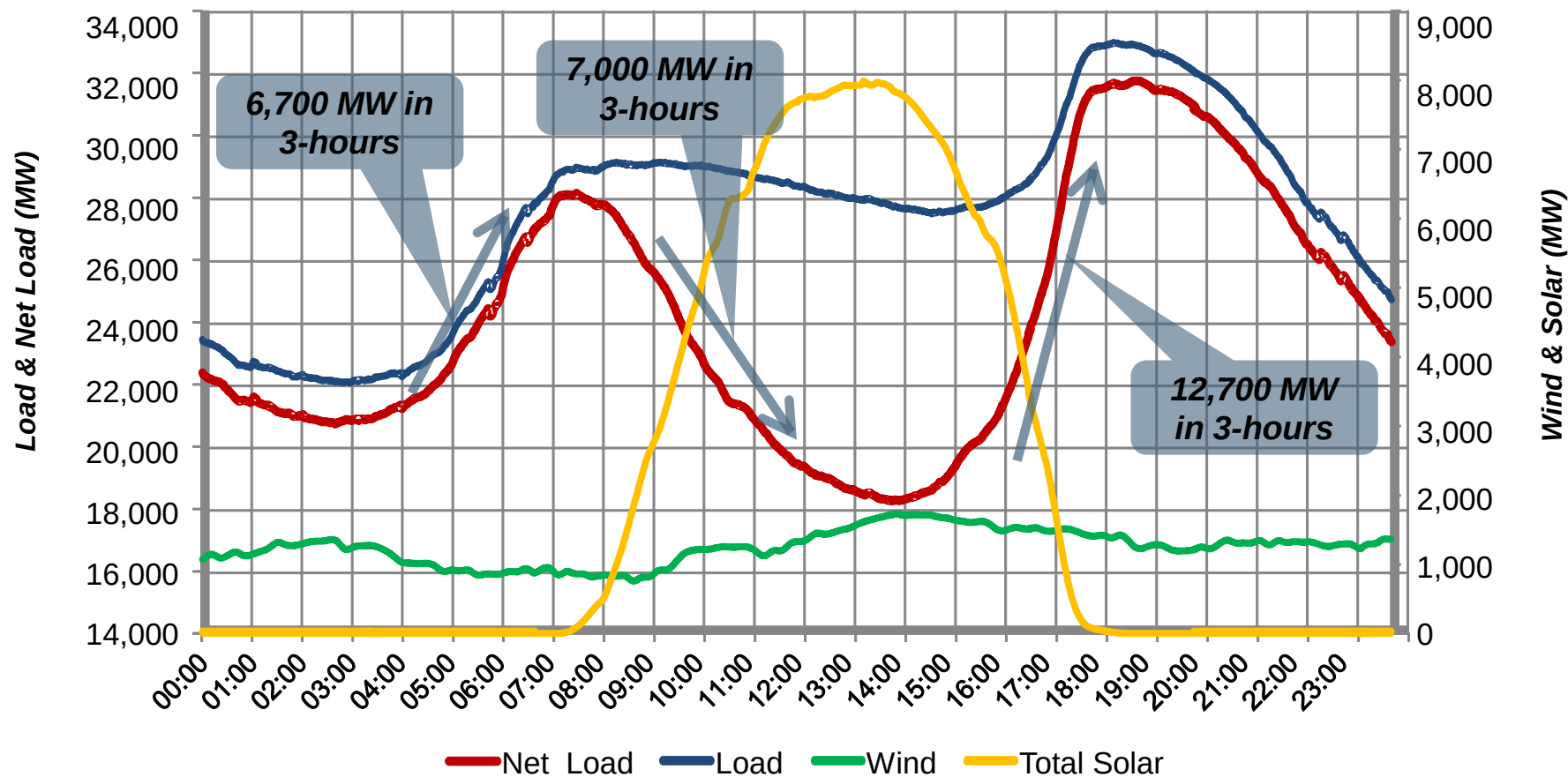




Non-summer months — Net load pattern changes significantly starting in 2014



Load, Wind & Solar Profiles --- Base Scenario
January 2020



$Net\ Load = Load - Wind - Solar$

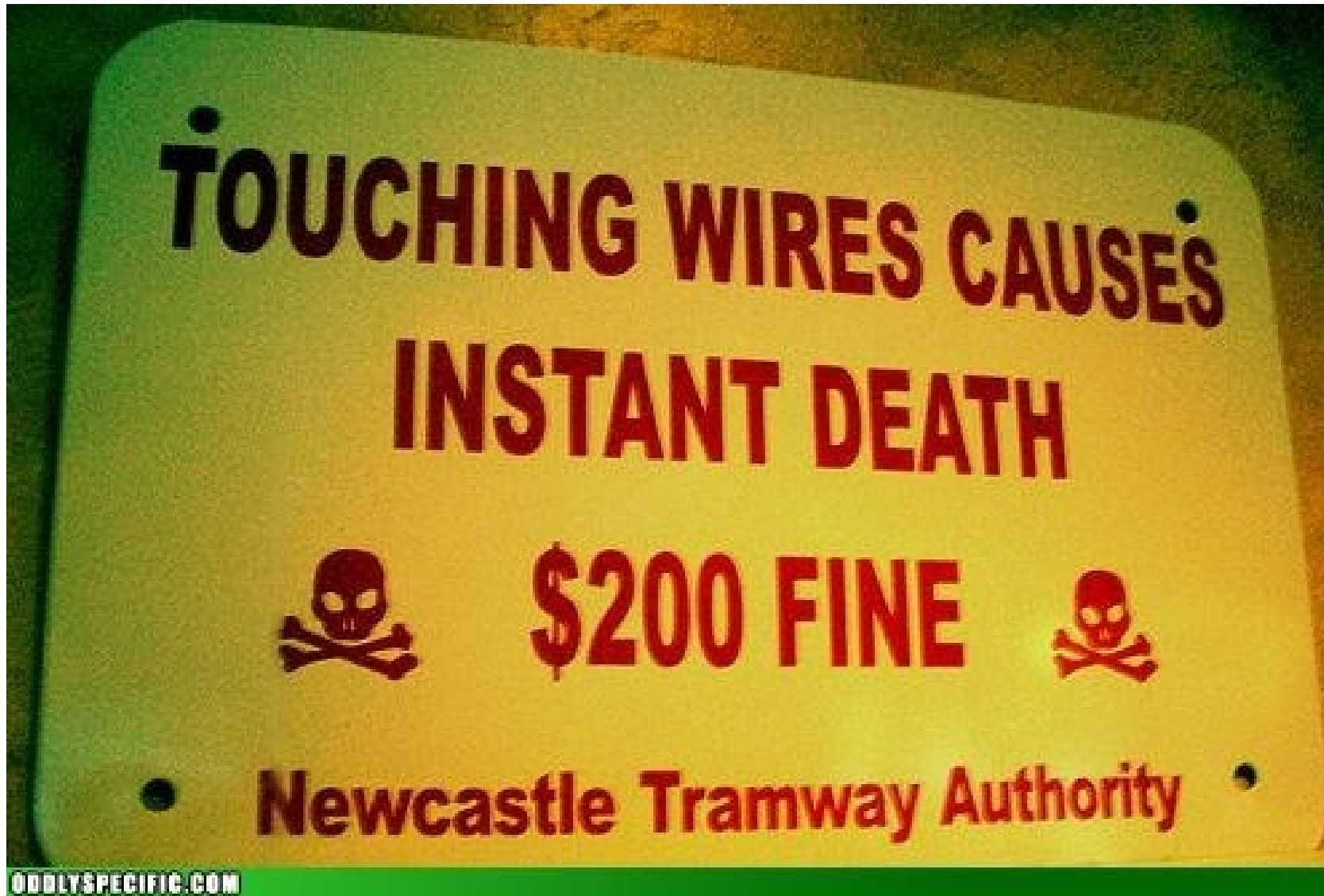






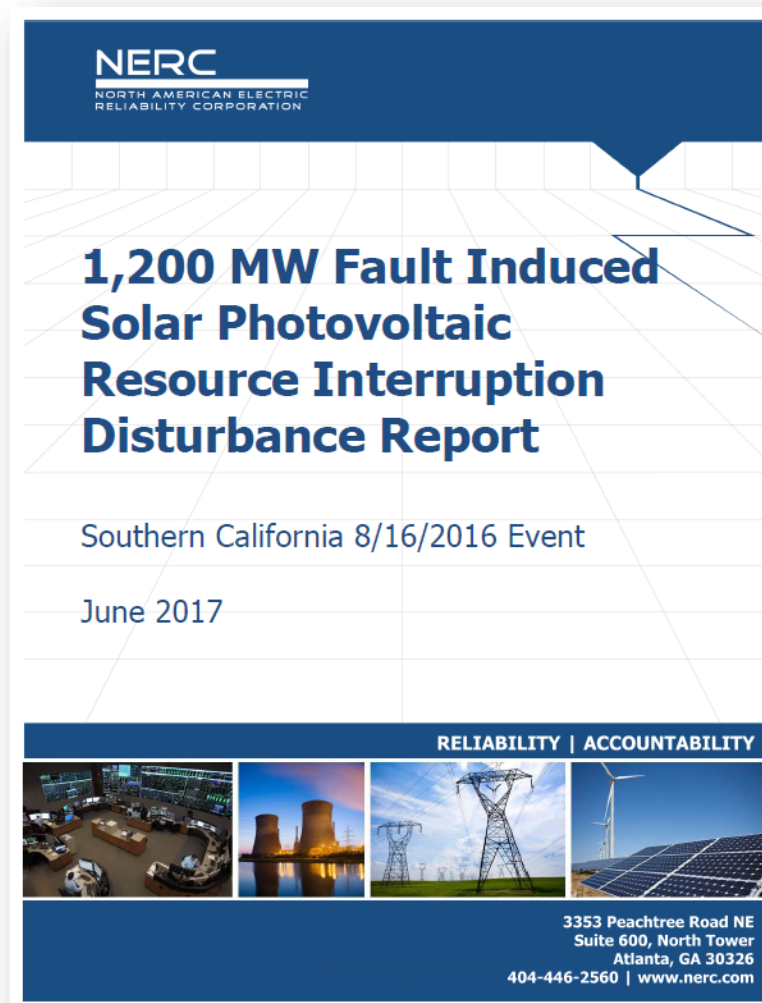








- Event occurred on August 16, 2016
 - Not a qualified event
 - Entities volunteered to work with ERO
- Fire caused 13 500 kV line faults and two 287 kV line faults
- NERC/WECC ad hoc task force created to identify causes
- Published disturbance report in June 2017
- Key Findings:
 - Use of momentary cessation
 - Frequency-related tripping



- Recommended actions:
 - Mitigate erroneous frequency tripping
 - Recovery from momentary cessation
- Data collection to understand extent of condition

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Industry Recommendation

Loss of Solar Resources during Transmission Disturbances due to Inverter Settings

Initial Distribution: June 20, 2017

NERC identified a potential characteristic exhibited by some inverter-based resources, particularly utility-scale solar photovoltaic (PV) generation, which reduces power output during fault conditions on the transmission system. An example of this behavior has been observed during recent BPS disturbances, highlighting potential risks to BPS reliability. With the recent and expected increases of utility-scale solar resources, the causes of this reduction in power output from utility-scale power inverters needs to be widely communicated and addressed by the industry. The industry should identify reliability preserving actions in the areas of power system planning and operations to reduce the system reliability impact in the event of widespread loss of solar-resources during faults on the power system.

For more information, see the [1,200 MW Fault Induced Solar Photovoltaic Resource Interruption Disturbance Report](#)

[About NERC Alerts >>](#)

Status:

Acknowledgement Required by Midnight Eastern on June 27, 2017
 Reporting Required by Midnight Eastern on August 31, 2017



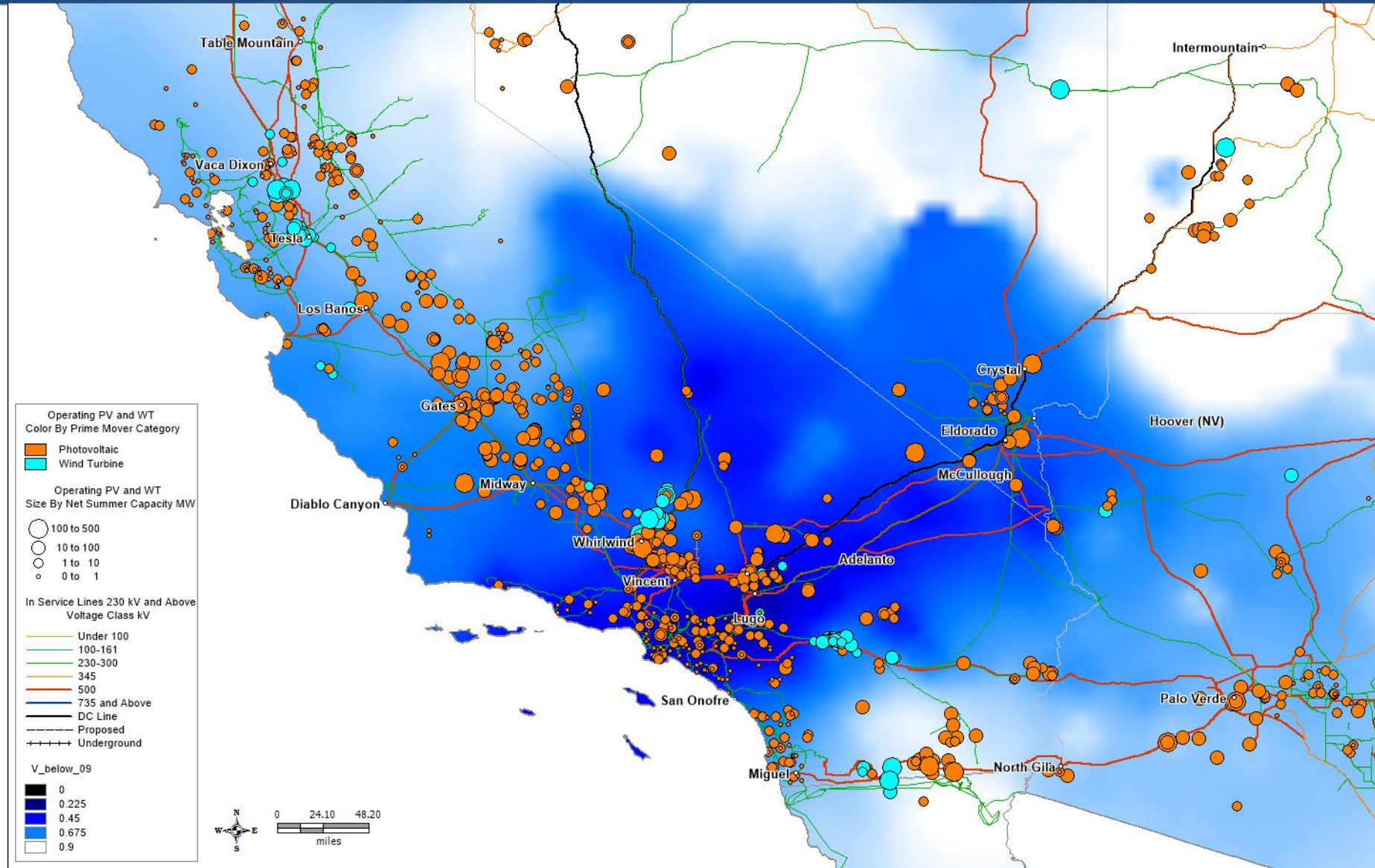



PUBLIC: No Restrictions
[More on handling >>](#)

Instructions:

This recommendation provides specific actions NERC registered entities should consider taking to respond to a particular issue. Pursuant to Rule 810 of NERC's Rules of Procedure, NERC registered entities shall 1) acknowledge receipt of this advisory within the NERC Alert System, and 2) report to NERC on the status of their activities in relation to this recommendation as provided below. For U.S. entities, NERC will compile the responses and report the results to the Federal Energy Regulatory Commission.

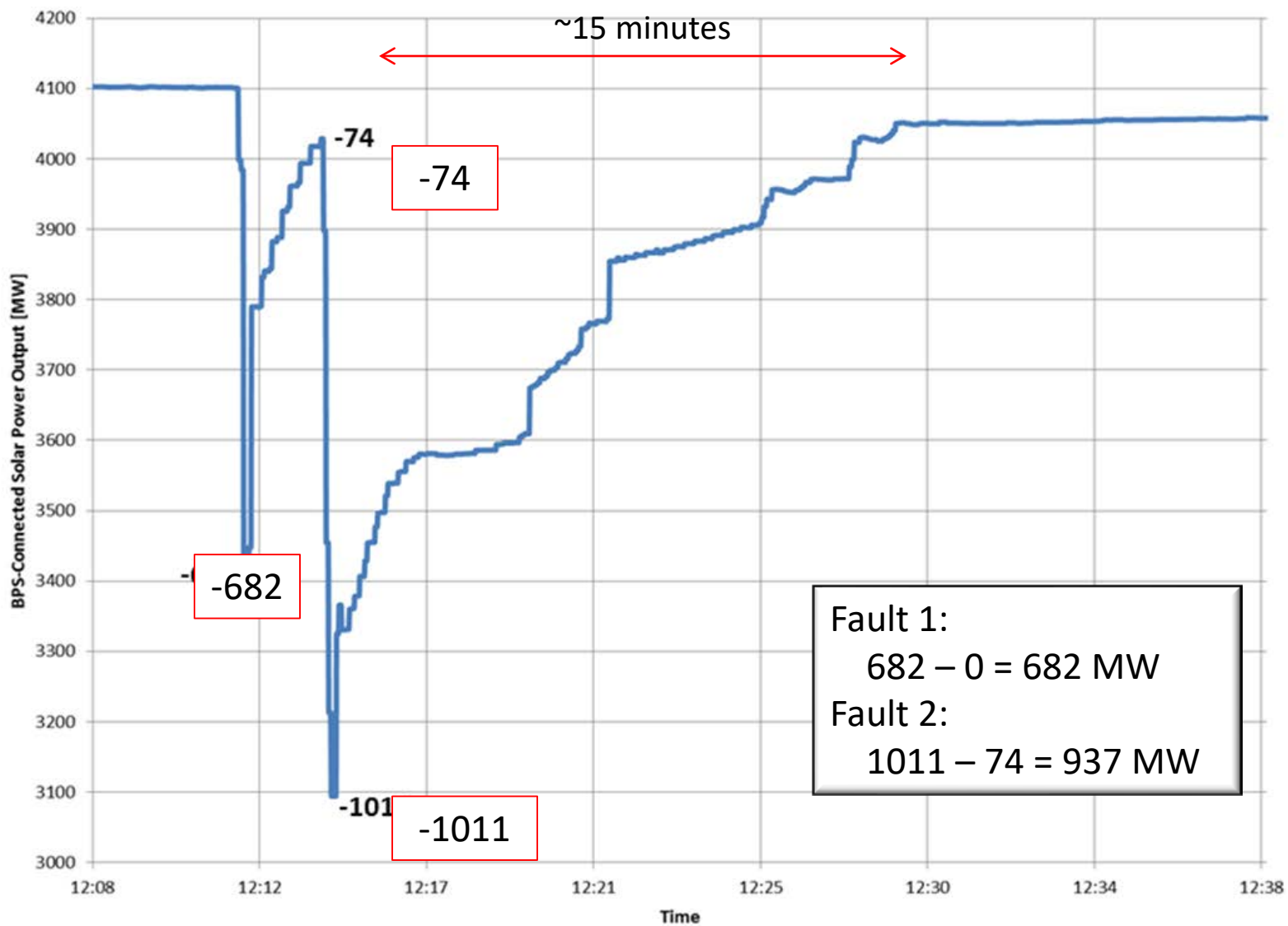
RELIABILITY | ACCOUNTABILITY



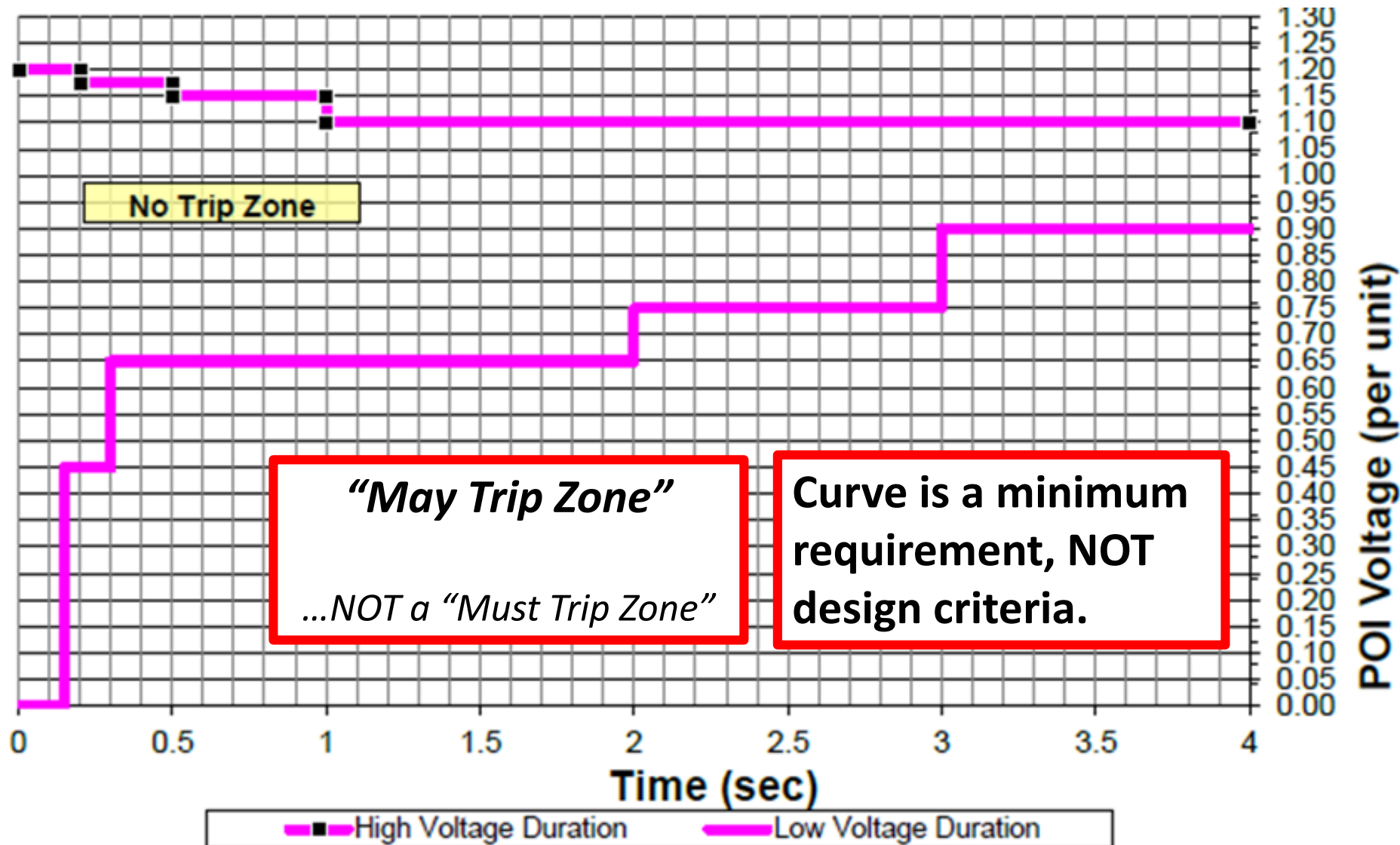
- Event occurred on October 9, 2017
 - Not a qualified event
 - Entities volunteered to work with ERO
- NERC/WECC event analysis, NERC IRPTF technical support
- Published disturbance report in February 2018
- Key Findings:
 - No frequency-related tripping
 - Continued use of momentary cessation
 - Voltage-related tripping



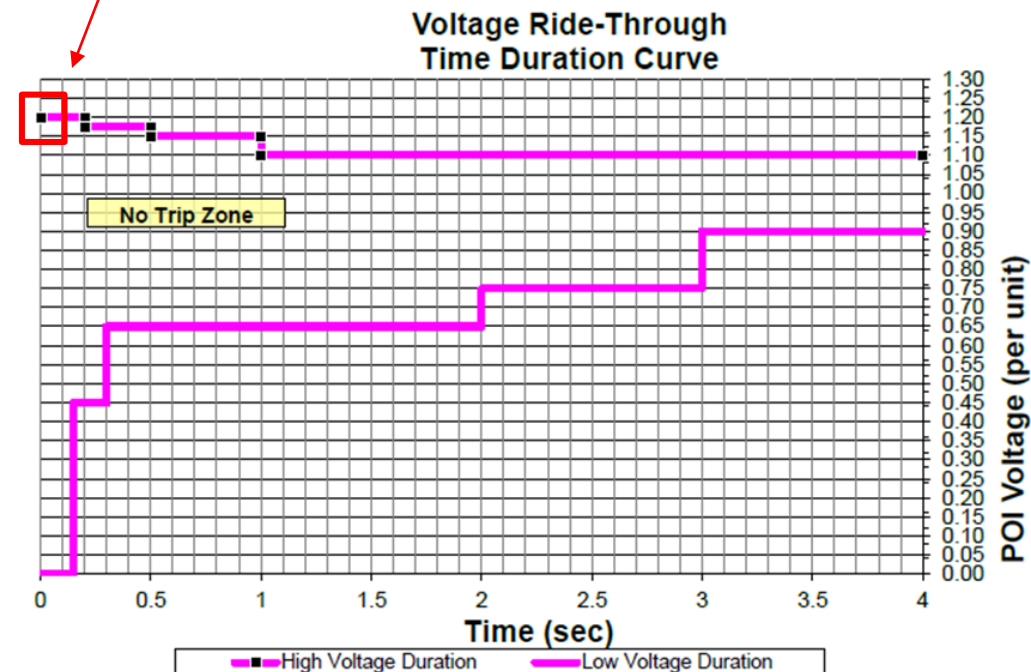
Canyon 2 Fire Disturbance Aggregate Solar PV Response



- No erroneous frequency tripping
 - Actions from first Level 2 Alert appear to have mitigated identified issue
 - By Canyon 2 Fire disturbance, 97% of manufacturer's BPS-connected fleet had been updated
- Continued use of momentary cessation
 - Most inverters use momentary cessation ($V < 0.9$ pu)
 - Recovery following momentary cessation varies, relatively slow for grid dynamics
 - Updated recommendation for momentary cessation – **eliminate the greatest extent possible**
- Transient overvoltage tripping and application of the PRC-024-2 ride-through curve



High Voltage Ride Through Duration		Low Voltage Ride Through Duration	
Voltage (pu)	Time (sec)	Voltage (pu)	Time (sec)
≥ 1.20	Instantaneous Trip	≤ 0.45	0.15
≥ 1.175	0.20	≤ 0.65	0.30
≥ 1.15	0.50	≤ 0.75	2.00
≥ 1.10	1.00	≤ 0.90	3.00



- Mitigating actions:
 - Dynamic model improvements
 - Mitigation of momentary cessation
 - Plant control loop coordination
 - Mitigation of voltage-related tripping
 - Information sharing among operating entities
- Planning and operations studies to ensure no potential stability risks
 - Response to Regional Entity of study findings by December 7, 2018

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Industry Recommendation

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

Initial Distribution: May 1, 2018

NERC has identified adverse characteristics of inverter-based resource performance during grid faults that could present potential risks to reliability of the BPS. As the penetration of inverter-based resources (particularly solar PV resources) continues to increase in North America, these adverse characteristics need to be widely communicated. This Level 2 Industry Recommendation alerts industry to these adverse characteristics observed with BPS-connected solar PV resources, and provides recommended actions to address fault ride-through and timely restoration of current injection by all inverter-based resources connected to the BPS. (See Background section for more information.)

Although this NERC Alert pertains specifically to BES solar PV resources, the same characteristics may exist for non-BES¹ solar PV resources connected to the BPS regardless of installed generating capacity or interconnection voltage. Owners and operators of those facilities are encouraged to consult their inverter manufacturers, review inverter settings, and implement the recommendations described herein.

For more information, see the October 9, 2017 Canyon 2 Fire [Disturbance Report](#).

[About NERC Alerts >>](#)

Status: Acknowledgement Required² by Midnight Eastern on XXXX XX, 2018
Reporting Required by Midnight Eastern on XXXX XX, 2018

PUBLIC: No Restrictions
[More on handling >>](#)

¹ These resources do not meet the Bulk Electric System definition, and are generally less than 75 MVA yet connected to transmission-level voltage.
² To the extent that Canadian jurisdictions have implemented laws or requirements that vary from Section 810 of the ROP, NERC requests entities in such jurisdictions voluntarily participate in response to this Alert.

RELIABILITY | ACCOUNTABILITY

- Issue: Existing models largely DO NOT accurately represent installed resource performance
- Identified issue that needs to be addressed for models in planning and operations studies
- Developed notification to help industry in modeling efforts
- Guidance provided as part of second NERC Alert

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Modeling Notification

Recommended Practices for Modeling Momentary Cessation

Initial Distribution: February 2018

This Modeling Notification provides Generator Owners who own inverter-based resources, particularly solar photovoltaic (PV) resources, with recommendations for accurately modeling momentary cessation for existing resources that are not able to eliminate its use. Specific modeling requirements and steps to accurately model this behavior in the second-generation positive sequence generic renewable energy system models are provided in the notification.

Primary Interest Groups

Generator Owners (GOs), Generation Operators (GOPs), Transmission Planners (TPs), Planning Coordinators (PCs), Reliability Coordinators (RCs), MOD-032 Designees

Background

The [Blue Cut Fire](#) in August 2016 identified that the vast majority of solar PV resources connected to the bulk power system (BPS) use an operating mode known as momentary cessation. Momentary cessation is an inverter operating state where the power electronic “firing commands” are blocked such that both active current and reactive current go to zero output.¹ The NERC Inverter-Based Resource Performance Task Force (IRPTF)² is developing recommended performance specifications for inverter-based resources, including recommendations for momentary cessation. The task force has determined that momentary cessation should not be used for newly interconnecting resources to the BPS and should be eliminated to the greatest extent possible for existing resources on the BPS due to the reliability risk that the operating mode poses.

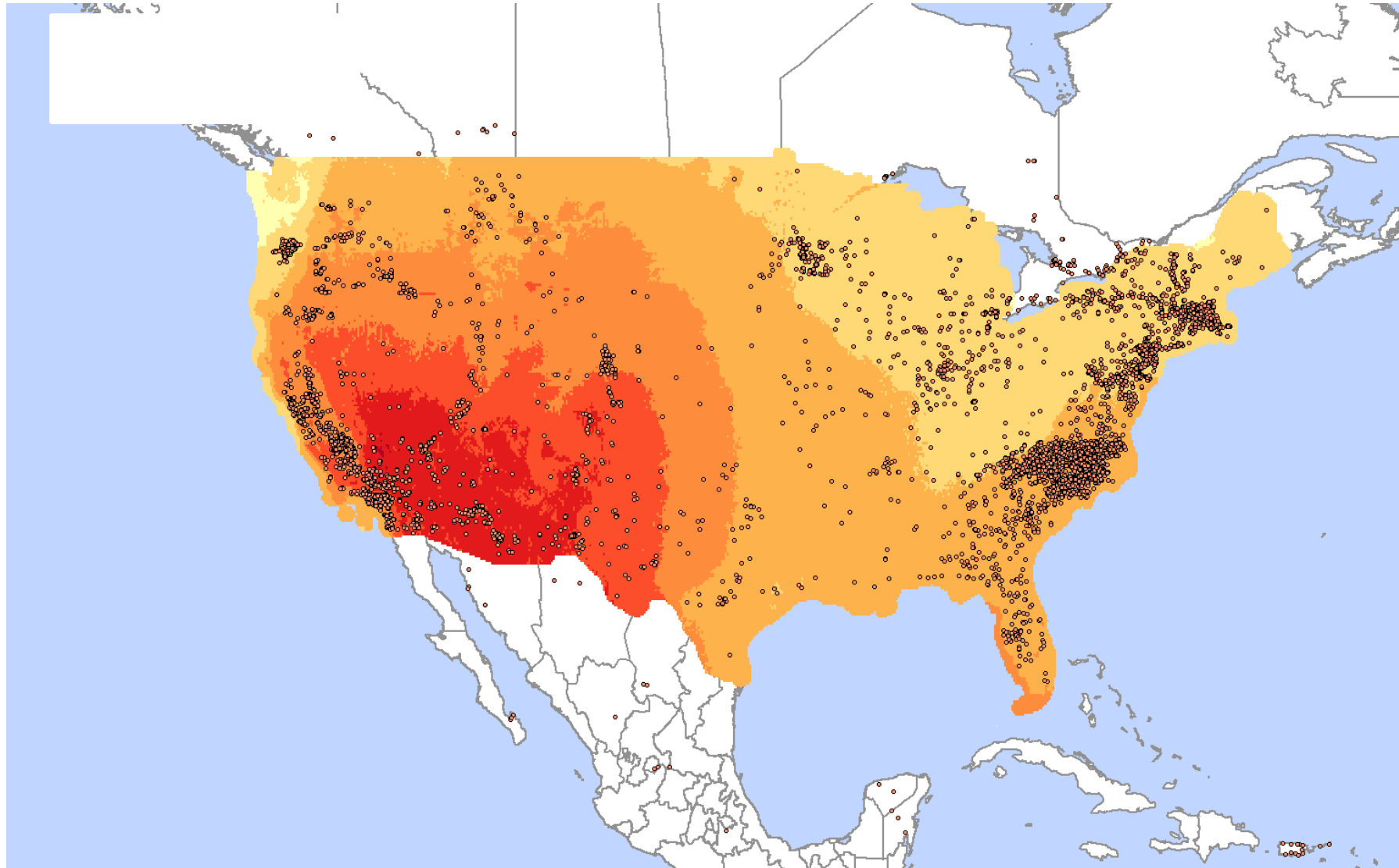
However, the NERC IRPTF recognizes that older vintages of inverters may require that momentary cessation be used due to design considerations at the time of commissioning. This is considered an equipment limitation that should be reported by the GO to their TP and PC. For these resources, it is critical that momentary cessation be captured with the dynamic models used to plan and operate the BPS. The second-generation generic renewable energy system models are, in general, recommended for modeling inverter-based resources in interconnection-wide base cases.^{3,4} These models have some capability to model momentary cessation, and are described in detail in this notification.

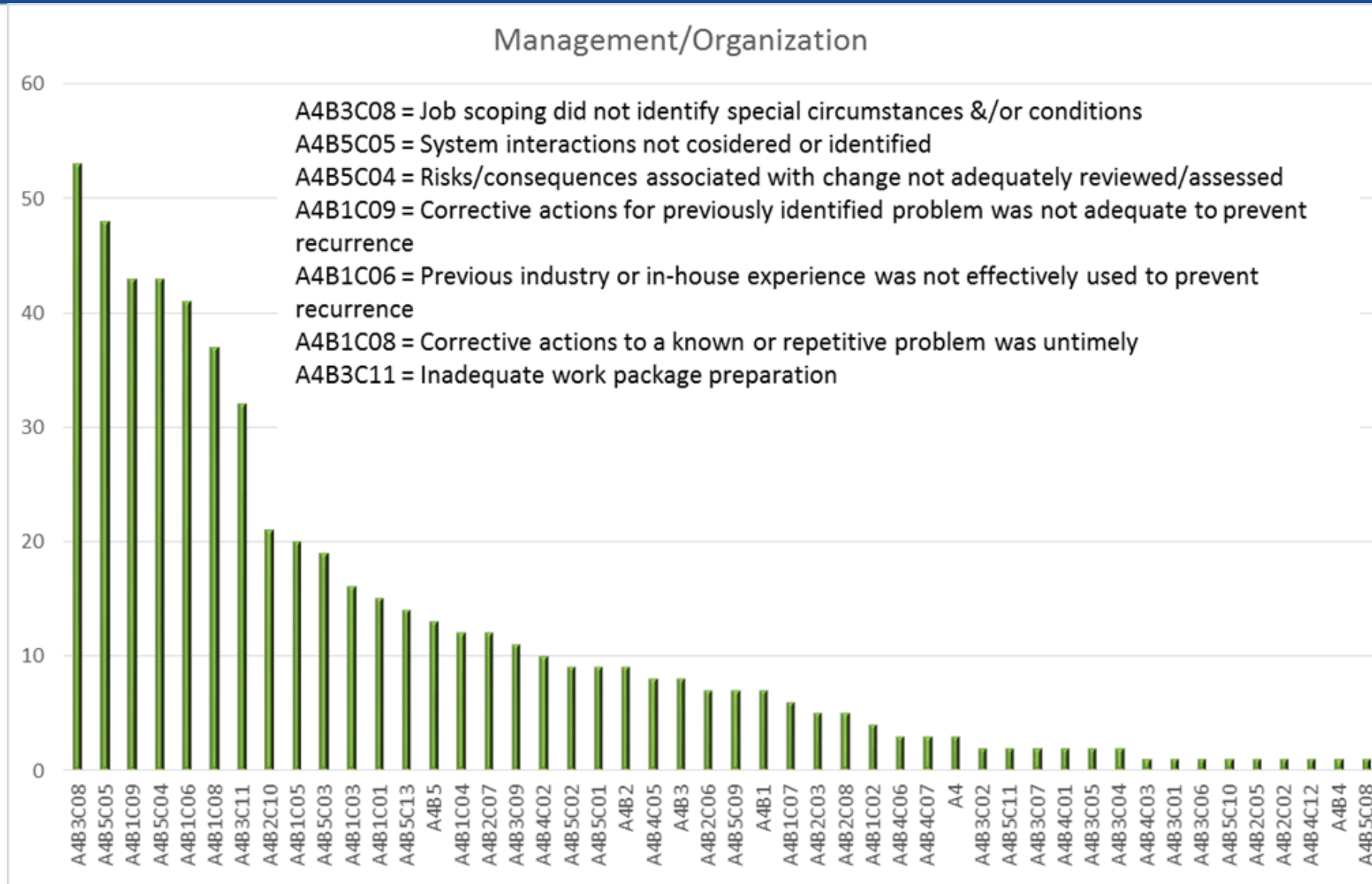
¹ Momentary cessation is sometimes referred to as “blocking” for this reason.
² The NERC IRPTF consists of inverter manufacturers, GOs, GOPs, TPs, PCs, Balancing Authorities (BAs), Fast AC Transmission System (FACTS) device manufacturers, renewable energy resource modeling experts, Regional Entities, NERC, and FERC.
³ “The second-generation generic renewable energy system models” refer to the latest generic models used to represent inverter-based resources (e.g., regc_a and rec_a models).
⁴ More detailed vendor-specific models may be used for local planning studies. These models may already capture momentary cessation. However, they are generally not allowed or recommended for the interconnection-wide cases. The focus of this guideline is on the generic models used for interconnection-wide modeling, and recommends the use of the second-generation renewable energy system models for this reason.
⁵ Some interconnections, for example the Texas Interconnection, allow for more detailed, user-written models in their interconnection-wide cases. This is left to the discretion of the MOD-032 Designees for each interconnection.

RELIABILITY | ACCOUNTABILITY

- Disturbance analyses and reports
 - Blue Cut Fire, Canyon 2 Fire, (and upcoming Angeles Forest) Disturbances
- Level 2 NERC Alerts
 - Identifying extent of condition, and recommending mitigating actions
- IRPTF Reliability Guideline
 - Recommended BPS-connected inverter-based resource performance
- Modeling and simulations
 - Modeling Notifications
 - Leading interconnection-wide stability studies to identify potential risks
- Industry education – webinars and workshops
- Outreach to BPS-connected non-BES resources (e.g., < 75 MVA)
- Reliance on SGIA, LGIA, and Facility Connection Requirements









Questions and Answers

EVENT ANALYSIS PROGRAM “What If” Methodology Presentation

NPCC Spring Workshop
May 23-24, 2018

“What If” Methodology Objective

- Evaluating NERC EAP qualifying events
- Event distribution within tier/category
- Trending of “near miss” events
- Analysis of credible “near miss” events

Methodology Development

Staff accomplished this by:

- Utilizing NERC Continent-wide event Severity Risk Index (eSRI) data
- Developing the eSRI-Categories
- Evaluating outliers
- Analyzing events bordering on the threshold of the next eSRI-Category

The Basis of the Methodology

The eSRI calculation

- NERC's Performance Analysis Subcommittee (PAS) created the Severity Risk Index (SRI).
 - Individual events have their own event Severity Risk Index called an eSRI.
- Input to the eSRI:
- Load Lost, with varying Durations
- Transmission Lost (weighted by voltage class), and
- Generation Lost

Developing the eSRI-Categories

- Correlation between eSRI values & EAP Categories
 - utilizing the NERC-wide EA dataset.
- Fine tune the eSRI-Category ranges
 - Alignment with EAP categories was examined
 - Any outliers were analyzed

eSRI-Category Ranges

eSRI-Category	min(eSRI)	max(eSRI)
1	0.00000	0.28489
2	0.28490	0.49999
3	0.50000	3.79999
4	3.80000	9.00000
5	9.00001	999.99999

Obtained by assessing eSRI values to actual EAP qualifying events.

Methodology provides

- A quick and easy gauge of an event's severity within its eSRI-Category range
- A quantitative assessment
 - additional loss of Load, Transmission, and/or Generation required to increase the eSRI value such that it moves into a higher eSRI-Category
- An exercise of the credible worst case scenario

Application of 'What If' Analysis

- Analyzing events bordering on the threshold of the next eSRI-Category
- Event's eSRI formula input variations
- Assessing Credible scenarios

Methodology Trial

The trial was performed to:

- Illustrate an event's severity within its expected eSRI-Category range
- Provide a quantitative assessment:
 - Amount of the additional Load, Transmission, and/or Generation needed to increase the eSRI-Category
- Provide an evaluation of a credible worst case scenario (if provided by the entity)
 - Ascertain whether an event could have had a higher impact by evolving into a higher eSRI-Category range.

Illustrative Examples

Examples assessed are of actual EAP Cat 1.a.i events.

Category 1.a.i - An event that results in an unexpected outage that is contrary to the design, of three or more BES Facilities caused by a common disturbance.

Chart Explanation

- Baseline column is the actual event variables
- Other columns show changes to individual eSRI variables to see how much would be required to traverse into the next higher eSRI-Category
 - Load & Duration
 - Transmission
 - Generation
- Real column assesses plausible worse- case losses
 - Provided by Entity
 - What additional Load/Transmission/ and/or Generation could have credibly been lost on a different occasion?

What-If Example #1 Chart

	Baseline	Load	Load + Duration	Load + Duration	Gen	Trans	Real
eSRI	0.12935	0.28942	0.290095	0.284942	0.28569	0.28525	0.21560
Load	0	525	265	175	0	0	0
Duration	0	0	240	720	0	0	0
Gen	0	0	0	0	1945	0	0
Trans							
>600	0	0	0	0	0	0	0
>400	0	0	0	0	0	0	0
>300	3	3	3	3	3	6	5
>200	0	0	0	0	0	0	0
>100	0	0	0	0	0	4	0

What-If Example #1 Chart (continued)

For credible scenario provided:

- Only two additional 300-400 kV class transmission circuits could have been lost.

Resultant:

- Although eSRI value is higher, still within the eSRI-Category 1 range.

What-If Example #2 Chart

	Baseline	Load	Load + Duration	Load + Duration	Gen	Trans	Real
eSRI	0.18055	0.28633	0.28781	0.28781	0.28790	0.28838	0.28773
Load	0	355	180	120	0	0	0
Duration	0	0	240	720	0	0	0
Gen	0	0	0	0	1105	0	1000
Trans							
>600	0	0	0	0	0	0	0
>400	0	0	0	0	0	0	0
>300	5	5	5	5	5	8	5
>200	1	1	1	1	1	1	1
>100	0	0	0	0	0	2	2

What-If Example #2 Chart (continued)

For credible scenario provided:

- The additional losses that could have occurred
 - two 100-200 kV class transmission circuits, and
 - an additional 1,000 MW of generation

Resultant:

- For this scenario eSRI value crosses into eSRI-Category 2 threshold - suggesting further analysis may be warranted

What-If Example #3 Chart

	Baseline	Load	Load + Duration	Gen	Trans	Real	Real (max Gen)
eSRI	0.146543	0.284922	0.284922	0.285148	0.28482	0.253112	0.287593
Load	0	450	225	0	0	0	0
Duration	0	0	240	0	0	0	0
Gen	1328	1328	1328	2755	1328	1883	2238
Trans							
>600	0	0	0	0	0	0	0
>400	0	0	0	0	2	0	0
>300	0	0	0	0	1	0	0
>200	1	1	1	1	1	4	4
>100	0	0	0	0	2	0	0

What-If Example #3 (continued)

For credible scenario provided:

- The additional losses that could have occurred
 - Additional loss of three 200-300 kV class transmission circuits (4 in total)
 - an increase in loss of generation to 1,883 MW total.

Resultant:

- Although eSRI value is higher, still within the eSRI-Category 1 range.

What-If Example #3 (continued)

For credible scenario provided:

- Supplemental evaluation was made (see Chart 3 last column), which increased the possible max. loss of generation from 1,883MW (derated due to blended fuel mix usage) to its actual maximum generation of 2,238MW.

Resultant:

- This addition along with the possible loss of transmission previously described was enough to push the eSRI value above the threshold for eSRI-Category 2.

Observations

- What this methodology will allow us to do:
 - Determine the range of severity within the various categories
 - Ascertain whether a specific event description/type is in the proper event EAP category
 - Determine whether to change the existing event category descriptions to more accurately align with their eSRI values.
 - Verify smart design vs fortunate

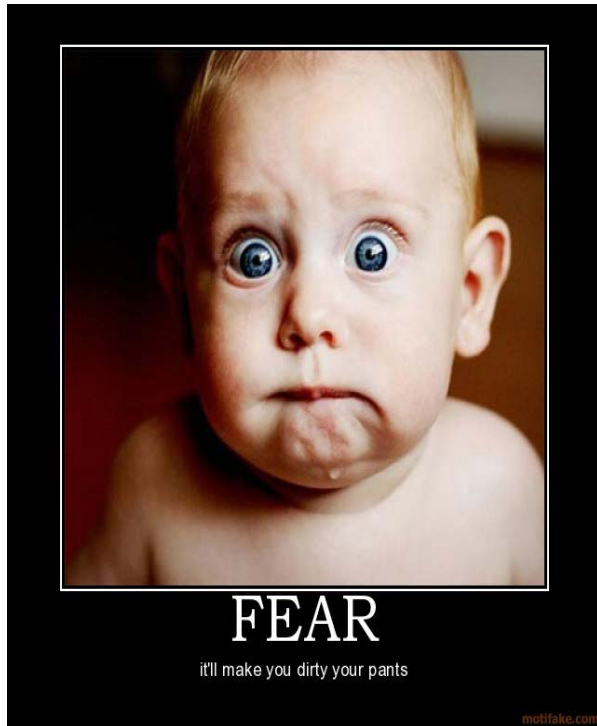
Questions



NPCC Spring Workshop

White Plains, NY

May 22-May 23, 2018



Active Shooter/ Workplace Violence

Don't be scared, be prepared!!

Goals of the presentation

- Enhance your overall awareness of the costly impact of workplace violence
- Identify behaviors of concern
- Learn the distinction between an active shooter and a hostage incident
- Meet your "duty of care" responsibilities to your employees by preparing them for this dreadful possibility and by integrating appropriate guidance into your overall violence prevention program.

Active Shooter vs Hostage

An Active Shooter incident is inherently different than a hostage situation. An Active Shooter is an immediate burst of violence causing as much death and destruction as possible before the shooter is stopped. There is NO reasoning with an Active Shooter as in many cases the shooter has prepared themselves to die, and in their mind, “die in a blaze of glory.”



HOSTAGE

A Hostage situation is VERY different than an Active Shooter. The hostage taker in many cases has nothing personal against his/her hostage. Many times the hostage was just a target of opportunity, easily taken and held. Law enforcement has a proved track record of successfully “talking a hostage taker down” and bringing the incident to a peaceful conclusion. Hostage negotiators are extremely well trained and go through a battery of psychological and other tests before being accepted as a negotiator.



Law Enforcement Response

ACTIVE SHOOTER

Law Enforcement response will be significantly different in response to an Active Shooter vs a Hostage situation. Active Shooter-Law enforcement tactics in response to these incidents have constantly evolved over the past two decades. They no longer establish perimeters and wait for SWAT or a perfect four-man diamond formation before they enter and close with the killer. The faster they enter the more lives are saved. There is immediate entry and confrontation, no talking, again, the quicker the response and confrontation the more lives are saved.

HOSTAGE SITUATION

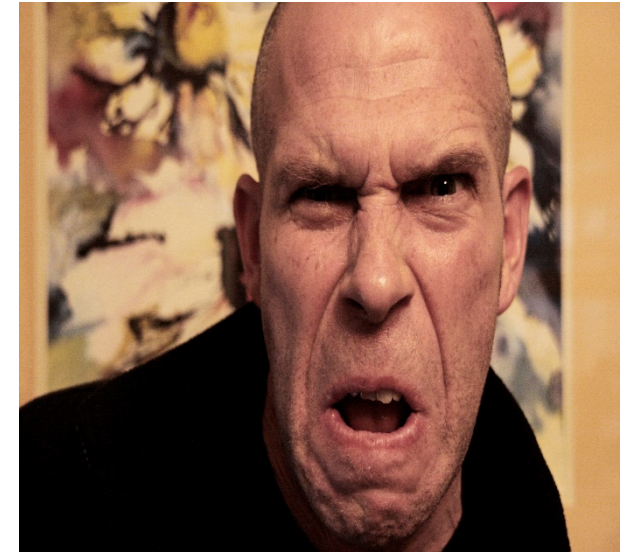


Police will standoff and they will talk the hostage taker into boredom. They will never trade one hostage for another. They will never

make specific promises and will never tell the hostage taker that they are not in control and have to ask someone higher to make a decision.

Recognizing and Preventing Workplace Violence

No one profile exists to predict at-risk and potentially violent persons, but signs and flags most often are present prior to violent acts. These signs and flags may be observed in the person's thinking, emotions, and/or behaviors and allow for reporting and intervening in both informal and formal ways. Unfortunately society has set barriers to reporting or taking action, making people reluctant to report suspicious or "strange behavior."



The 5 Phases of an Active Shooter

What occurs before shots are fired. Understanding these phases will enable your employees to make effective and definitive decisions regarding their involvement and actions they may take.

Fantasy Phase:

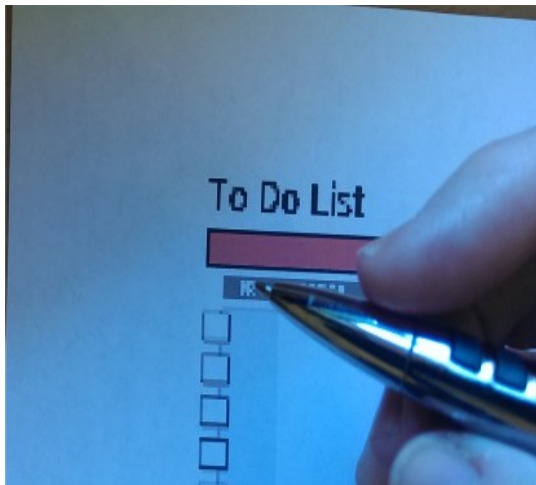
During this phase, the wannabe mass-murderer dreams of his day of achieving an historic level of carnage. Often they will write, draw, and post this fantasy in a variety of venues, from their notebook to their Facebook page. During this time, this person is surprisingly likely to share his thoughts and feelings with someone else. If this shared information makes it to the properly-motivated professional, lives can be saved by that professional alerting authorities. That professional might be a teacher, a doctor, a counselor, a therapist or a law enforcement officer. Too often, people dismiss these warning signs as “crazy talk” and do not take action because they are afraid of being accused of overreacting. Inaction enables carnage, whereas taking proper action can prevent it and save lives.

Planning Phase: During the planning phase, the potential killer lays out the who, what, when, where, how, and why of his plan. In other words, he will document who he will kill, what he will use to accomplish these murders, and when, where and how the slaughter will take place. In many cases the shooter will intricately explain the reasons for his intended actions. His plans may be recorded, sometimes on a hard drive or in hard copy. If recorded plans are found in advance of the attack, lives can be saved.



Preparation Phase: After forming their plan, the person must gather the items he needs to succeed. He must buy or steal the tools required to accomplish his goals. The suspect will also visit the scene to gather intelligence as he finalizes the plan.

The preparation phase is an opportunity for a family member, citizen, school employee, businessman, or police officer to take notice of the suspicious nature of the accumulation of information and equipment. Relaying suspicions here may also save lives.



THE FINAL PHASES

Approach Phase: This phase affords an opportunity for an alert citizen or police officer to notice someone dressed for combat approaching a place of employment, school, hospital, mall, theater, or church carrying a weapon, or weapons. If the citizen calls 911 or officers spot the suspect, the subject can be stopped prior to reaching his target.

Implementation Phase

Regardless of motivations, once they start killing these attackers are going for top score. What is needed is immediate, decisive actions; Run, Fight, or hide. Seconds lost equal lives lost. Even if unarmed, when fleeing is not an option, many potential victims have chosen to fight. Many shooters have been thwarted by an immediate, aggressive unarmed response by those who refused to “go quietly into that good night.”

GRATUITOUS MONKEY SLIDE



Surviving an Active Shooter Situation-VIDEO

- Strategies-Run, Fight, Hide vs Move, Escape, Attack- basically the same but small nuances are different
- This film and model encourage a “soft” response to violence, preconditioning the victim to escape or hide as the preferred means of survival, rather than confronting the attacker with immediate counter-violence. Potential victims are taught that the risks associated with fighting an attacker are much greater than the risks from running away, so violence should only be used “as a last resort” when all of the other options have been tried, and failed.
- The model encourages a mindset and a pattern of behavior that may not adequately prepare potential victims to save themselves and others during an attack.

Run, Hide, Fight- Video



https://www.youtube.com/watch?v=zcnA_Cq_Csk

SURVIVING-CONTINUED

- Humans confronted with sudden and unexpected violence either freeze, flee, or fight. Even if a person later chooses to flee or fight, they often freeze momentarily for a bit before their mind “unlocks” and they take other, more helpful actions. the vast majority of the public lacks the mental conditioning and physical skills to adequately deal with violence, making them especially likely to freeze in an active shooter situation.
- A victim might have to consider using violence as the first and primary response, before avoidance and escape, if circumstances dictate it. In the last fifty years or so, the public has been increasingly conditioned to think that the police have a monopoly on the use of violence in self-defense, and that citizens are not permitted to use violence to defend themselves.

A DIFFERENT VIEWPOINT

There are now differing opinions on what was previously thought to be proper actions as depicted in the Run, Hide, Fight video.

One such opinion can be read in an article by
Lt. Colonel Michael Wood, USAF Ret.

This can be read at :

<https://www.policeone.com/active>

I leave it up to each individual to compare the different viewpoints and offer no opinions.

Emergency Plans for response to violent situations

Proper response techniques, methods of employee notification, evacuation and lock down strategies can significantly lessen the number of injuries or fatalities. Understand how to identify what will work best for your facility.

Code names or signals should be used for employee notification to certain specific situations.

Utilize the expertise of your Federal, State and Local Law Enforcement and take advantage of any training or presentations they may offer.

After conferring with official agencies develop a plan that suits your particular circumstances and facilities.

Share your developed plan with first responders and TRAIN YOUR EMPLOYEES!!!

Corporate Response to the Active Shooter

- Workplace violence is a top concern for all organizations. The most frightening and compelling element is an active shooter. Current events across the country dramatically illustrate that no individual or group is immune to this tragic possibility.
- Planning, prevention, mitigation, and response to active shooters and incidents is essential. Your company must embrace the importance of preparing for, and rehearsing, what is known as a "survival mindset."
- The aftermath-employees, counseling, lawsuits, finger pointing, Duty of Care responsibilities to employees.

Questions



Our Dedicated Team of Experts are here to assist you

CONTACT

PETER SCALICI, CHPP
NPCC SENIOR CIP SPECIALIST
PSCALICI@NPCC.ORG
(212) 205-7065



Cyber Security Outreach Program

Jenifer Wallace Farrell

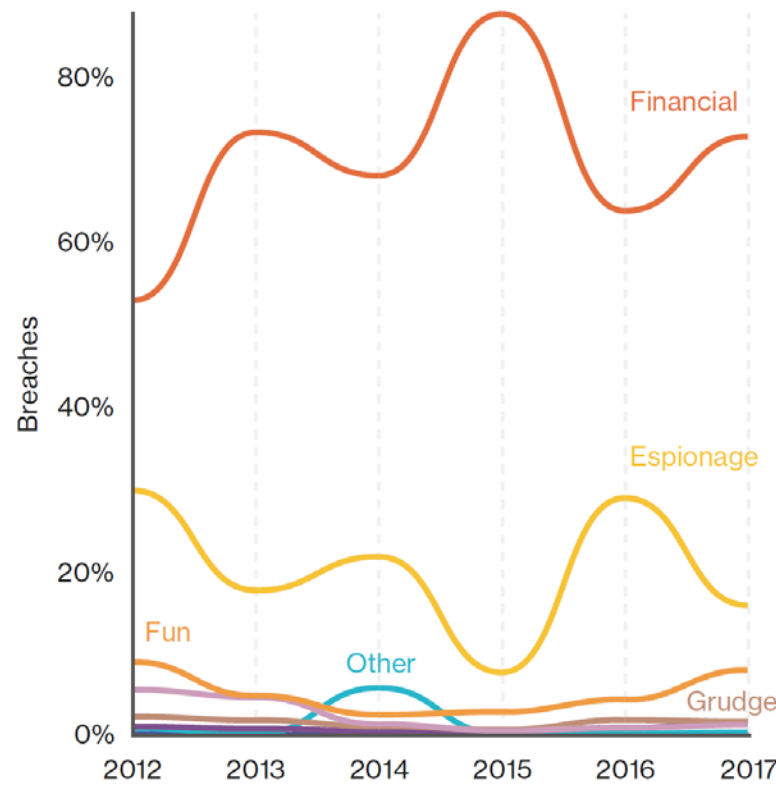
Verizon Data Breach Investigations Report

Reference

- Verizon. (2018, May 16). Verizon 2018 Data Breach Investigations Report. Retrieved from Verizon:
<http://www.verizonenterprise.com/verizon-insights-lab/dbir/>

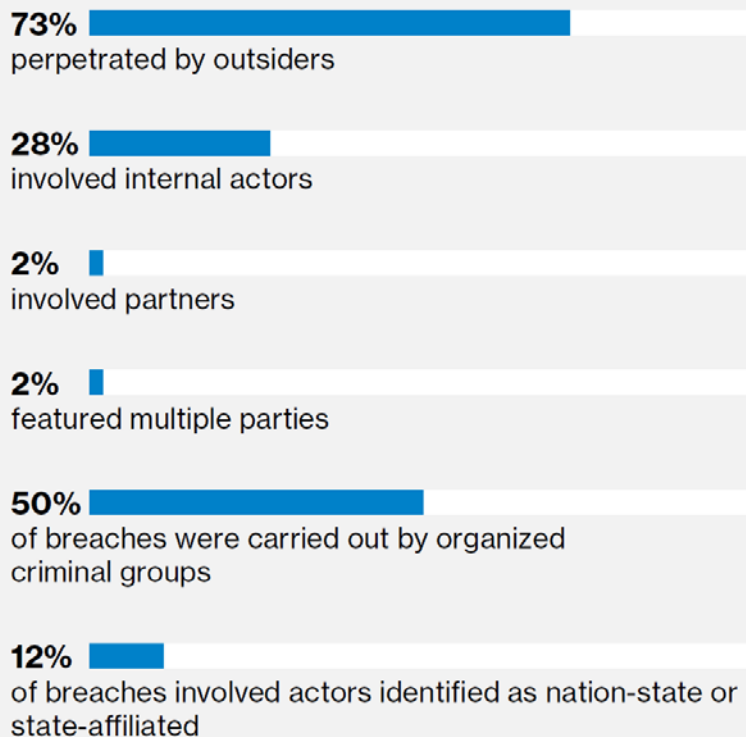
Verizon Data Breach Investigations Report

Actor motives in breaches



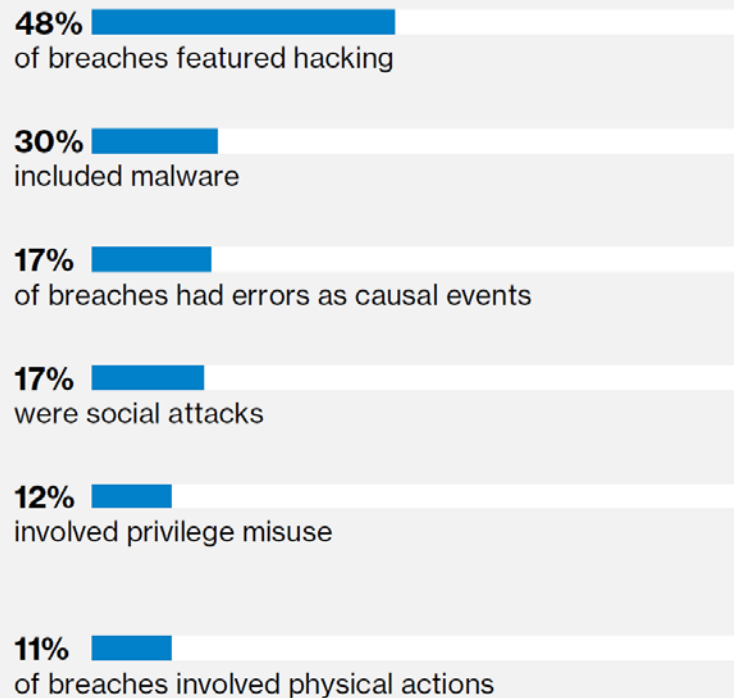
Verizon Data Breach Investigations Report

Who's behind the breaches?



Verizon Data Breach Investigations Report

What tactics are utilized?



Verizon Data Breach Investigations Report

What are other commonalities?

49% 
of non-POS malware was installed via malicious email¹

76% 
of breaches were financially motivated

13% 
of breaches were motivated by the gain of strategic advantage (espionage)

68% 
of breaches took months or longer to discover

Verizon Data Breach Investigations Report

Top 20 action varieties in breaches

Use of stolen credentials (hacking)

399

RAM scraper (malware)

312

Phishing (social)

236

Privilege abuse (misuse)

201

Misdelivery (error)

187

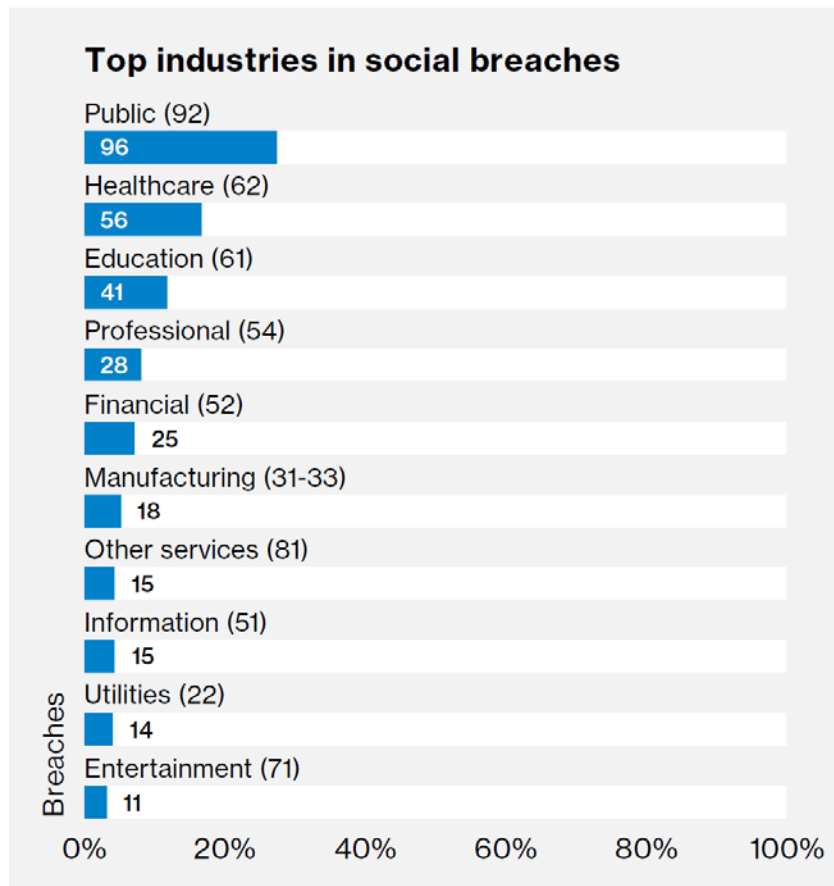
Use of backdoor or C2 (hacking)

148

Theft (physical)

123

Verizon Data Breach Investigations Report



Phishing

- Training / Awareness
 - Test your ability to detect a campaign, identify infected hosts, look for existence of data exfiltration.
- Identify the clickers
 - Give them a tablet or sandboxed OS
 - Segment clients from critical assets
 - Use strong authentication (i.e., more than a keylogger is needed to compromise)

Information Handling

- What information is provided to Vendors
 - Full databases (troubleshooting)
 - Obfuscate data where possible or use test data
 - Ensure vendor knows if data is sensitive
 - Logs
 - Redact usernames and passwords
 - Passwords
 - Have secure method, don't keep a full spreadsheet of unencrypted passwords within your vendor's portal

NPCC Cyber Assessment Process

- 1-2 day onsite review:
 - High level network architecture review
 - Physical inspection of control system
 - CIS Critical Security Controls review

CIS Controls

BASIC CIS Controls

1) Inventory and Control of Hardware Assets

2) Inventory and Control of Software Assets

3) Continuous Vulnerability Management

4) Controlled Use of Administrative Privileges

5) Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6) Maintenance, Monitoring, and Analysis of Audit Logs

CIS Controls

Foundational CIS Controls

7) Email and Web Browser Protections

8) Malware Defenses

9) Limitation and Control of Network Ports, Protocols, and Services

10) Data Recovery Capabilities

11) Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches

12) Boundary Defense

13) Data Protection

14) Controlled Access Based on the Need to Know

15) Wireless Access Control

16) Account Monitoring and Control

CIS Controls

Organizational CIS Controls

17) Implement a Security Awareness and Training Program

18) Application Software Security

19) Incident Response and Management

20) Penetration Tests and Red Team Exercises

Assessment Report

- Onsite debrief and confidential non-public report:
 - Positive observations
 - Better practice elements

Assessment Examples

Current Practice

- Using sticky note for password storage
- 8 char password length
- No formal asset inventory
- Does not build / maintain secure images

Better Practice Elements

- Use secure password manager
- Use passphrases that are longer than 14 char
- Use centralized asset repository
- Remove bloatware, configure security settings, and store secure images in air-gapped environment

Questions?

Jenifer Wallace Farrell, CISSP, CISA

Senior CIP Analyst

jwallace@npcc.org