NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability and Security Technical Committee Meeting

September 8, 2021

RELIABILITY | RESILIENCE | SECURITY




NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

RSTC Nominating Subcommittee

Greg Ford, RSTC Chair
RSTC Meeting
September 8, 2021

RELIABILITY | RESILIENCE | SECURITY




Nominating Subcommittee Overview

- The RSTC NS consists of five members (the RSTC Vice Chair and four members drawing from different sectors and at-large representatives).
- NS members are nominated by the RSTC chair and approved by the full RSTC membership.
- The term for members of the Nominating Subcommittee is two years.
- In addition to recommending individuals for at-large representative seats, the NS manages the process to select the chair and/or vice chair of the RSTC.

Nominating Subcommittee

- Nominating Subcommittee (NS) Members
  - Rich Hydzik– Vice Chair
  - Jodirah Green – Sector 7, 2022
  - Sandra Ellis – At-Large, 2023
  - Wayne Guttormson – At-Large, 2022

Replacement Nominating Subcommittee Timeline

- In June with the approval of Rich Hydzik to Vice Chair, Todd Lucas was appointed to the RSTC Executive Committee and resigned from the NS creating an open seat
- Open nomination period July 14-30, 2021
  - RSTC members only
- Chair Ford reviewed nominations and presented the candidate to the Executive Committee on August 10 for discussion and concurrence
- September – Full RSTC vote for Nominating Subcommittee member

Election Process

- The Chair presents a candidate.
- Elections will be held as follows:
  - The Committee will vote on the presented candidate. If the presented candidate is approved with a 2/3 majority, the presented candidate is elected and the election is closed.
  - Should the presented candidate not get elected the Chair will do the following:
    - Reconvene a review of the nominations already submitted;
    - Open for a second, shortened nomination process for additional submissions; and,
    - Convene a second meeting to evaluate the nominations and present a candidate to be considered at the next RSTC meeting.

Recommended Slate

- For the Nominating Subcommittee member, the Chair nominates and requests approval of:
  - Edison Elizeh, Bonneville Power Administration (Sector 4) to fill the term of the vacant seat (through January 2023)

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability and Security Technical Committee – Policy Input

Greg Ford, RSTC Chair
RSTC Meeting
September 8, 2021

RELIABILITY | RESILIENCE | SECURITY




RSTC Policy Input

- On April 7, 2021, NERC Board of Trustees (Board) Chair, Ken DeFontes, invited the Member Representatives Committee (MRC) to provide policy input on the RSTC
  - Policy Input to be provided in advance of the May 2021 Board meeting
- The Policy Input Letter indicated the RSTC intentionally focused on the tactical work to lay foundation for ongoing operations in its first year
- Further, the RSTC made improvements to subgroup structure, internal collaboration and processes, and cross-coordination
- The RSTC also developed a work plan aligned with the Reliability Issues Steering Committee's *ERO Reliability Risk Priorities Report*

RSTC Transition Objectives

- The objectives for the RSTC transition included the following:
  - Stand up the RSTC to deliver on the goals outlined in its charter
  - Maintain continuity in all ongoing, high-value work across the subgroups.
  - Capture best practices and synergies through the integration of processes across the “legacy” committees
  - Create a more collaborative and bottoms-up operating model that clearly documents roles, responsibilities, and processes, and supports subgroups while maintaining alignment to the overall NERC strategy
  - Provide more effective and efficient processes for technical input on risks to North American bulk power system reliability and security
- The Board requested MRC policy input on whether the RSTC was meeting the objectives of the transition

General Comments

- Most input was supportive and many felt that the RSTC has achieved the goals set forth by the Stakeholder Engagement Team and that the RSTC was effective and efficient
- Some felt that more time was needed to more fully assess effectiveness and efficiency

Work Prioritization and Collaboration

- Many comments included encouragement of collaboration within the ERO Enterprise and other stakeholder groups
  - In particular, close coordination with the RISC was encouraged
- Work plan prioritization and the full RSTC role in prioritization

RSTC Response: Work Prioritization and Collaboration

- A discussion of the RISC Report, RSTC work plan and subgroup activities has been added as agenda items for these Sept. meetings
  - The RSTC will form a team to:
    - Collaborate with the RISC to prioritize identified risks
    - Develop RSTC subgroup work plan items for review and approval by the full RSTC at the December 2021 meeting
  - This will enhance full RSTC participation in work plan prioritization
- The combined subgroup work plan is posted on the RSTC website and a link is included in each RSTC meeting agenda.
- The RSTC concurs that improving relationships and collaboration with other industry groups would be beneficial and an efficient means to address risks to the grid.
  - We currently have quarterly reports to the RSTC from the NAGF and NATF for awareness

RSTC Response: Work Prioritization and Collaboration

- The Facility Ratings Task Force held a meeting with NATF regarding potential collaboration on their work plan
- Several subgroups within the RSTC structure have participants from EPRI and National Labs. For example, security subgroups and groups focused on inverter-based resource and DER issues
- The groups also collaborate with Regional Entity experts

Stakeholder Engagement and RSTC Meetings

- Many who provide Policy Input expressed concerns with improving stakeholder engagement and RSTC meeting agendas and meeting length
- Several comments indicated the RSTC agendas have been very full and prevented a more robust discussion of agenda items

RSTC Response: Stakeholder Engagement and RSTC Meetings

- In an effort to improve on stakeholder engagement, the RSTC will undertake two initiatives
  - Offer of Pre-meeting informational sessions prior to RSTC regular quarterly meetings to provide RSTC members an opportunity to ask questions and/or voice concerns with agenda items prior to the meeting
  - Beginning with the September 2021 meeting, the meeting time expanded by 2 hours each day. The meeting will begin at 11 a.m. Eastern each day with a short break for lunch

RSTC Response: Stakeholder Engagement and RSTC Meetings

- The September meeting will remain as a virtual meeting while we are still evaluating whether the December meeting will be virtual or a hybrid of in-person and virtual.
- For 2022 and beyond, we will plan two in-person RSTC meetings (March and September) and two virtual meetings (June and December).

Sponsors and RSTC Subgroup Coordination

- Suggestions were made to assign a Sponsor to each subgroup
- Initially, the RSTC has assigned 12 Sponsors to high priority subgroups

RSTC Response: Sponsors and RSTC Subgroup Coordination

- Over the course of time since then, we have assigned additional Sponsors for each subgroup that reports directly to the RSTC
  - Working Groups and Task Forces that report to a Subcommittee were not assigned Sponsors as we envision the Subcommittee Sponsor coordinating with the subgroups reporting to that Subcommittee
- Each Working Group or Task Force in the Risk Mitigation Focus area now has a Sponsor
- Effective collaboration between Sponsors in each Focus Area will ensure that work items, activities are aligned and completed efficiently and effectively

Inverter-based Resources and Distributed Energy Resources

- Integration of intermittent resources and the development of SARs, requiring guidance and technical documents to improve the reliability of such integrations
- A number of state and provincial efforts to decarbonize and this will have an impact on the reliability of the grid

RSTC Response: Inverter-based Resources and Distributed Energy Resources

- Address Inverter-based Resources for operations, planning and security through the work of the IRPWG
- Address DER integration for operations, planning and security through the SPIDERWG, SITES, and ERATF
- These RSTC subgroups will collaborate with Regional Entities to ensure that government mandates are included in reliability assessments and reliability and resilience are maintained

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

RSTC Charter Revisions

Nina Johnston, Assistant General Counsel
RSTC Meeting
September 8, 2021

RELIABILITY | RESILIENCE | SECURITY




Timeline

- September 8, 2021 (RSTC meeting)
- September 24, 2021 (Charter comments deadline)
- October 2021 (Email ballot)
- November 4, 2021 (NERC Board of Trustees)

Charter Revisions

- Purpose
  - Emphasize the oversight role of the RSTC vs. its subgroups
  - Empower subgroups as the owners of the technical work
- Functions
  - RSTC strategic work plan vs. Subgroup work plans
  - Strategic work plan (Board approval every 2 years)
  - Quarterly updates vs. Semi-annual updates to the Board
- Membership
  - Affiliate conflicts
  - Conversion of sector seats during annual elections
  - Ability to serve on the Nominating Subcommittee and the Executive Committee

Charter Revisions

- Meetings
  - Establishing quorum
  - Voting method
  - Executive / Open / Closed formats permitted
  - Documenting Executive Committee actions
- Subordinate Groups
  - Subgroup chairs
- Meeting Procedures
  - Polling
- RSTC Deliverables and Approval Processes
  - Member guidance on deliverables
- Meeting Governance
  - Motion practice

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

2021 ERO Reliability Risk Priorities Report

Thomas Coleman, Chief Technical Advisor
RSTC Meeting
September 8, 2021

RELIABILITY | RESILIENCE | SECURITY




RISC Objectives and Activities

- Objectives:
  - Develop the scope, priority and goals to mitigate known and emerging risks to bulk power system reliability
  - Provide a framework to effectively focus NERC and industry resources to improve reliability
- Biennial Activities
  - Reliability Leadership Summit
  - Industry risk survey
  - Identify Priority Risks
  - Identify Mitigating Activities
- Document result in RISC Report

Identified Risks

- 11 risks from multiple inputs (e.g., ERO Leadership Summit, Emerging Risks Survey results, Subject Matter Expertise)
  - Changing Resource Mix
  - Cyber Security Vulnerabilities
  - Resource Adequacy and Performance
  - Critical Infrastructure Interdependencies
  - Loss of Situational Awareness
  - Extreme Natural Events
  - Physical Security Vulnerabilities
  - Bulk Power System Planning
  - Control and Protection Systems Complexity
  - Human Performance and Skilled Workforce
  - Electromagnetic Pulse

Key Functional Areas

Four high level risk profiles:

Grid Transformation

A. Bulk Power System Planning

B. Resource Adequacy and Performance

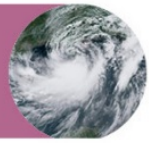
C. Increased Complexity in Protection and Control Systems

D. Situational Awareness Challenges

E. Human Performance and Skilled Workforce

F. Changing Resource Mix

Extreme Natural Events



A. Extreme Natural Events, Widespread Impact

- GMD

B. Other Extreme Natural Events

Security Risks

A. Physical

B. Cyber

C. Electromagnetic Pulse

Critical Infrastructure Interdependencies

A. Communications

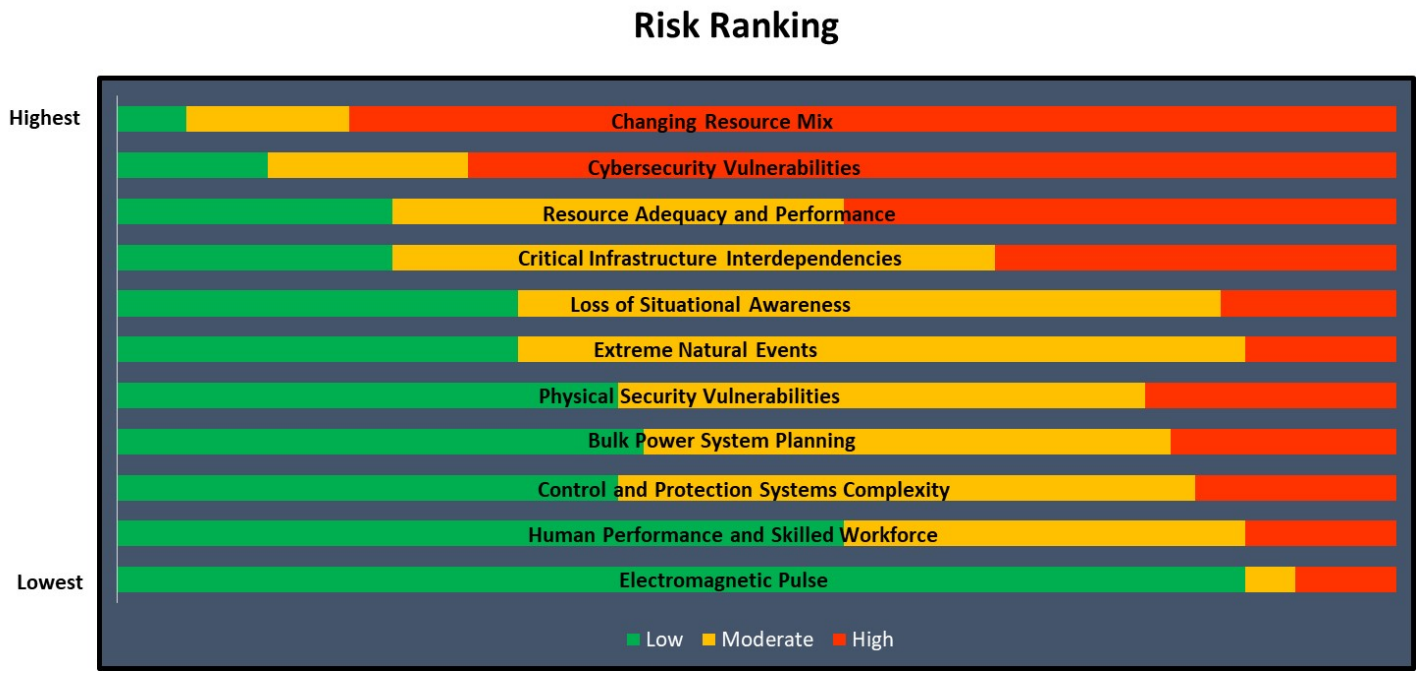
B. Water/Wastewater

C. Oil

D. Natural Gas

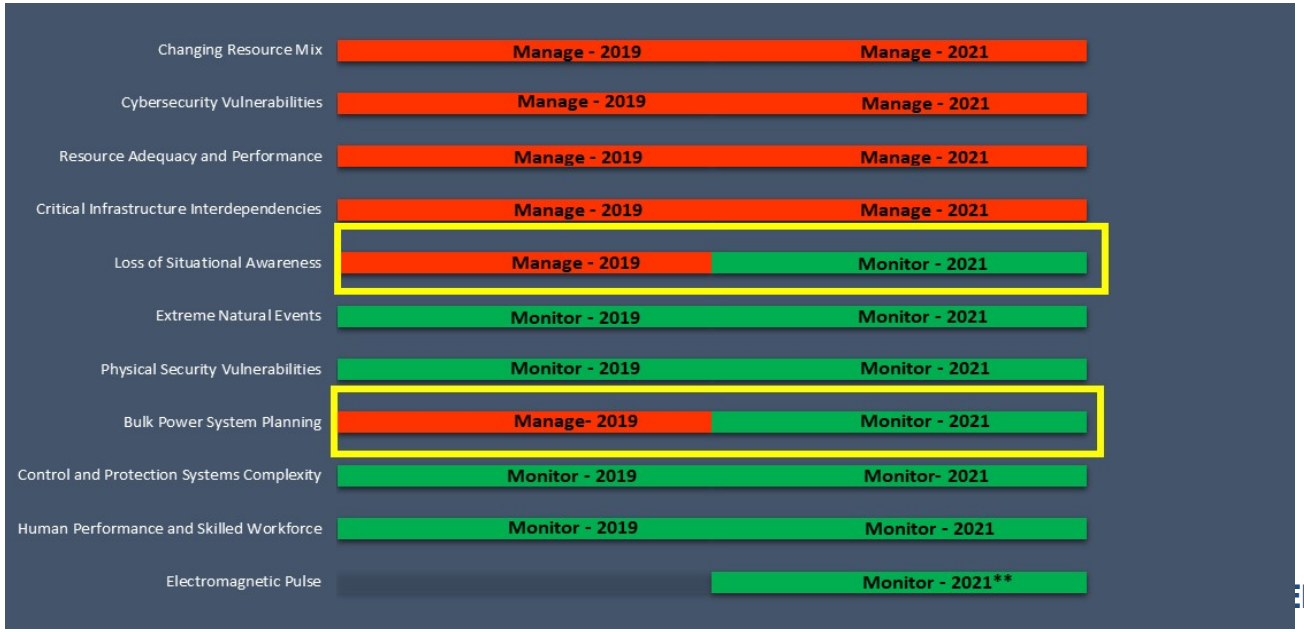
Status of Industry Oversight Risk Ranking

The following chart reveals that Changing Resource Mix followed by Cybersecurity Vulnerabilities lead industry perception on the criticality of these risks. This information is useful for industry as a whole to prioritize and dedicate resources and budget.



Status of Industry Oversight Manage vs. Monitor

- **Manage** – risks are emerging, imminent, and pose significant threats and where thorough strategic planning and industry collaboration are needed for risk mitigation
- **Monitor** - risks that are of critical importance to BPS reliability but are considered well managed with established industry practices in place to mitigate and lessen potential impacts to BPS reliability
  - Extreme events shows monitor, but recent extreme events shows the resource mix is increasingly characterized as one that is sensitive to extreme, widespread, and long duration temperatures as well as wind and solar droughts. Information to be collected going forward on extreme events for which a great deal of experience is available, and events that industry is gaining experience and understanding in due to the grid transformation.
- Loss of Situational Awareness and Bulk Power System – Manage (2019) to Monitor (2021)



RISC/RSTC Coordination

The RISC/RSTC has commenced and will continue implementation of the coordination efforts identified in the *Framework to Address Known and Emerging Reliability and Security Risks*.

Drawing Conclusions

- Analysis of mitigating activities and the effects on risk likelihood and impacts, enable biennial comparison/trending
- A larger emphasis on immediate and short-term actionable activities to reduce risk
- Differentiation between actively manage versus monitor
- Prospectively it will be important for the RISC to:
  - Collaborate with the identified owners of the mitigating activities recommendations to understand actions implemented, if any, to address the risk and recommendations
  - Coordinate with the annual business plan and budget and ERO Enterprise Long-Term Strategy to ensure alignment of priorities and strategic execution on a going-forward basis

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

RISC/RSTC Coordination
2021 RISC Report

Rich Hydzik, RSTC Vice Chair
RSTC Meeting
September 8, 2021

RELIABILITY | RESILIENCE | SECURITY




2021 RISC Report

- The draft RISC *2021 ERO Reliability Risk Priorities Report* (Report) was posted for comment June 9 through June 23, 2021
- Comments received recommended minor adjustments to the 2021 Report, as well as general comments for consideration for future reports
- The RISC voted to approve the Report at the July 8, 2021 meeting
- The Report was accepted by the NERC Board of Trustees at their August 12, 2021 meeting

2021 RISC Report – Risk Process

- *Framework to Address Known and Emerging Reliability and Security Risks (Framework)* was developed jointly by the RISC and RSTC
- The Framework was accepted by the Board on February 4, 2021
- The Framework identifies the steps to be coordinated between the RISC and RSTC as well as the CCC, PCGC and SC

ERO Iterative Risk Management Framework: Standing Committees and RISC Coordination

Risk Identification and Validation – RISC Report and RSTC

- Risk Identification and Validation is completed by the RSTC and RISC as they review the annual State of Reliability Report, Long-Term and Seasonal Reliability Assessments, Event Analysis records and with a joint review the biennial RISC Report incorporating prioritized risks into the RSTC's subgroup's work plans
- Further, the RSTC coordinates with the RISC on long-term risks and mitigations. In this way, risks determined by monitoring the ongoing performance of the bulk power system and those identified by scanning the horizon
- The risk registry will be maintained by the RISC and RSTC to determine if an inherent nature of a risk changes over time, and consider removing risks or adding others

Reliability Risk Prioritization – RISC and RSTC Memberhsip

- Reliability Risk Prioritization is completed collaboratively between the RSTC and RISC on an annual basis
- Ongoing activities are calibrated, and newly identified risks are prioritized
- The SCCG will serve as a coordination point to ensure broad alignment across the Standing Committees

Remediation & Mitigation Identification & Evaluation – RSTC

- Remediation and Mitigation Identification and Evaluation activities to address the risks are assigned to the appropriate RSTC subgroups accounting for changing needs across the BPS
- They create the ERO Policies, Procedures and Programs to address the risks
- Frequent communications ensures coordination of ongoing risk prioritization
- RSTC will provide updates to the RISC on the subgroup activities being taken on a quarterly basis
- The SCCG will serve as a coordination point to ensure broad alignment across the Standing Committees

Deploy Mitigations - RTSC

- Deploy Mitigations by putting ERO Policies, Procedures and Programs into effect
- Depending on the Risk Remediation/Mitigation activities selected, the RSTC, SC, and CCC will be assigned certain activities
  - If Implementation Guidance is identified as an activity through the Framework, the CCC will be assigned to review the developed guidance
  - If a Reliability Standard is identified, the RSTC (or identified stakeholder) will need to submit a SAR to the SC and that project is to be included in the annual Reliability Standards Development Plan
- For all other mitigation/remediation activities, the RSTC will be responsible for developing remediation/mitigation

RISC/RSTC Coordination Timeline

- August 12, 2021 – Board accepted the RISC Report
- August – December, 2021
  - RSTC will form a tiger team to review the Report and develop a strawman for RSTC subgroup work plan items to mitigate risks
  - Once the work plan has been developed, the RSTC will collaborate with the RISC to refine and prioritize the work plan/risk mitigation items
- December, 2021 – Tiger Team reports to RSTC on risk mitigation identification and priorities for inclusion in RSTC and subgroup work plans
- Coordinate with NERC staff to ensure work plan items are included in Risk Registry

RISC/RSTC Coordination Request

- Request: Seeking RSTC volunteers to:
  - Collaborate with the RISC in prioritizing risk mitigation identified in the RISC Report
  - Develop draft risk mitigation activities and assignments for RSTC subgroups
  - Develop proposed subgroup work plan items for full RSTC review and input in December 2021

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

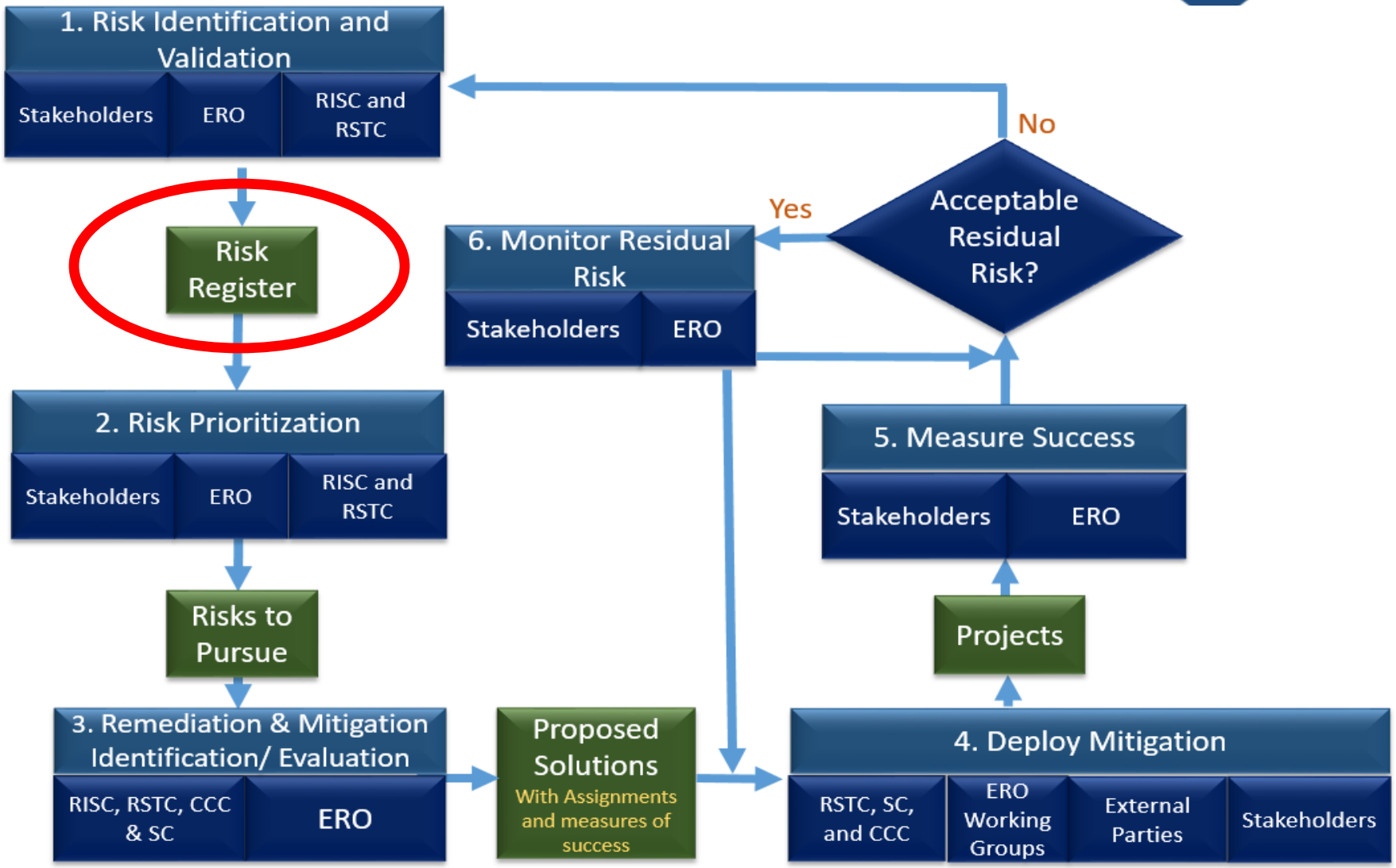
Risk Registry

Soo Jin Kim, Director of PRISM
RSTC Meeting
September 8, 2021

RELIABILITY | RESILIENCE | SECURITY

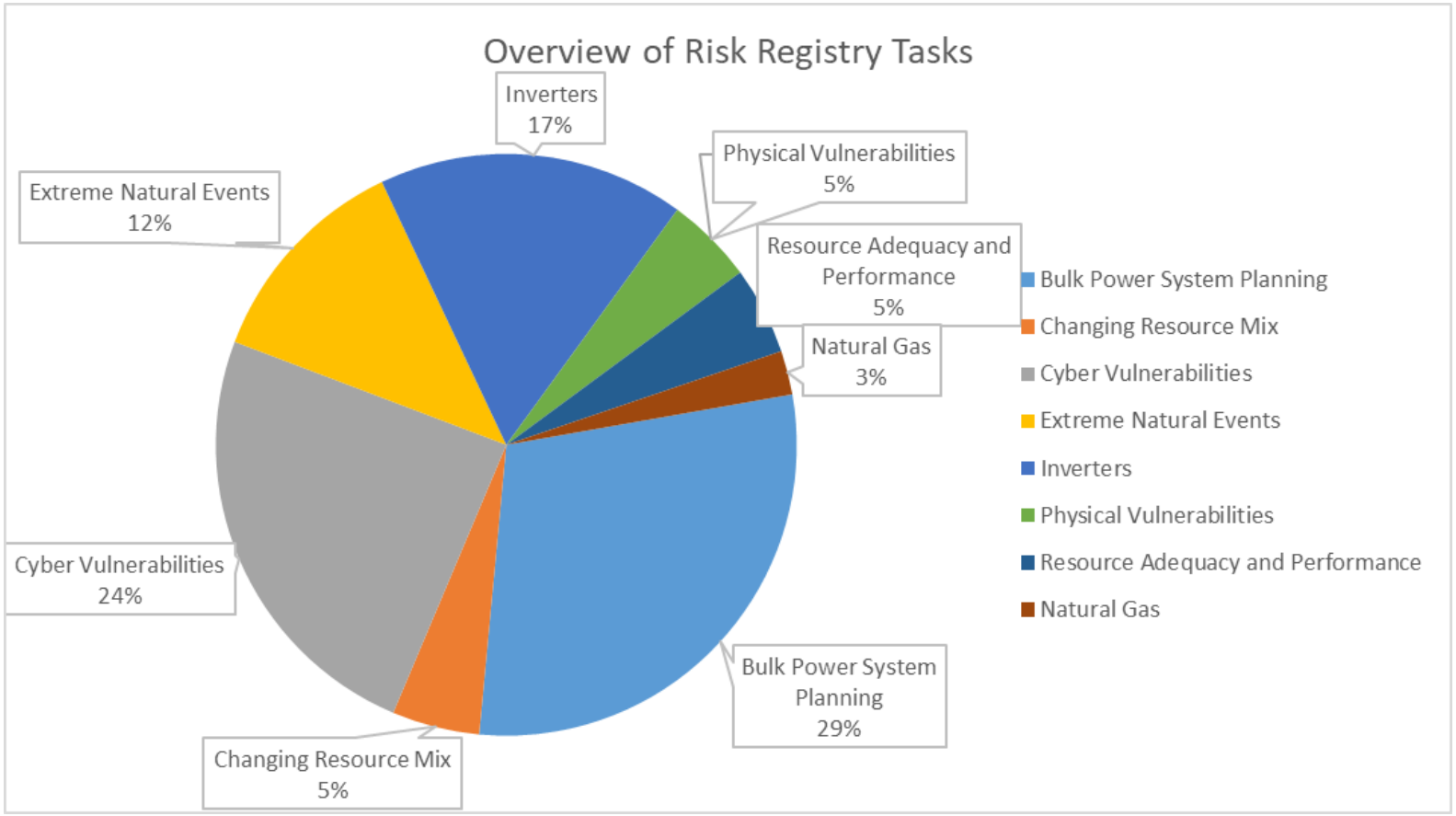



Reliability Risk Framework



Time Horizons

Overview of Risk Registry



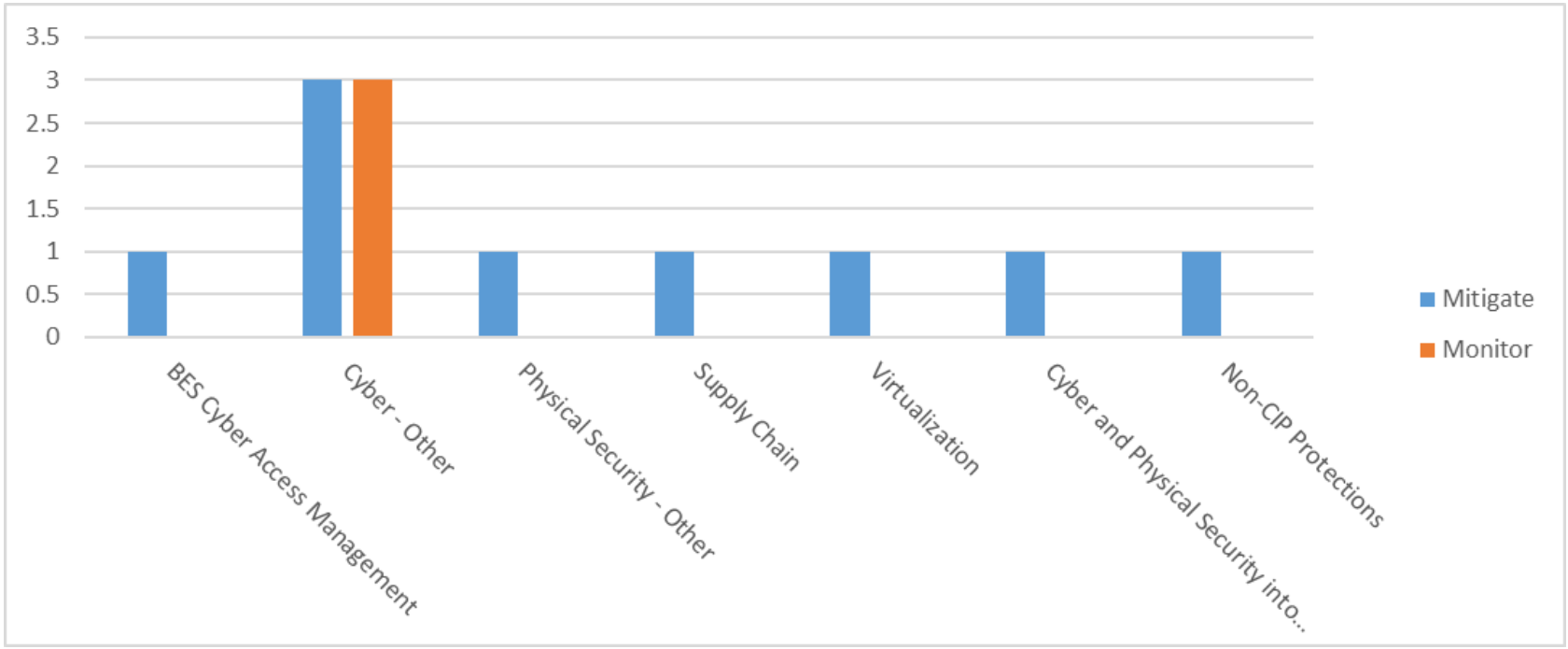
2021 Critical Risk Categories

- Energy Adequacy
- Security Risks (Cyber and Physical)
- Extreme Natural Events (including Cold Weather)
- Inverters

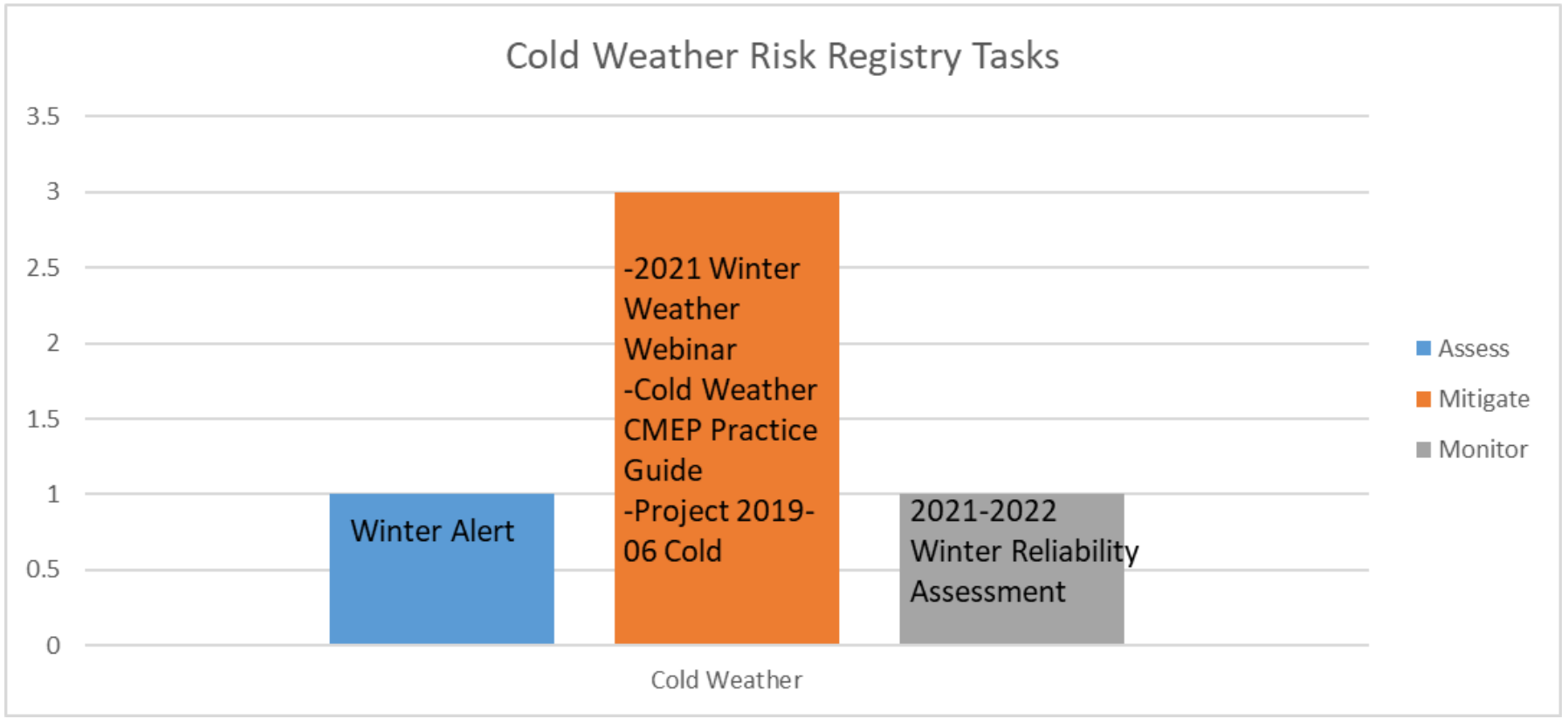
Energy Adequacy

- Probabilistic Analysis Forum
- Energy Reliability Assessment Task Force (ERATF)
- Gas-Electric Planning Basis (N-1)

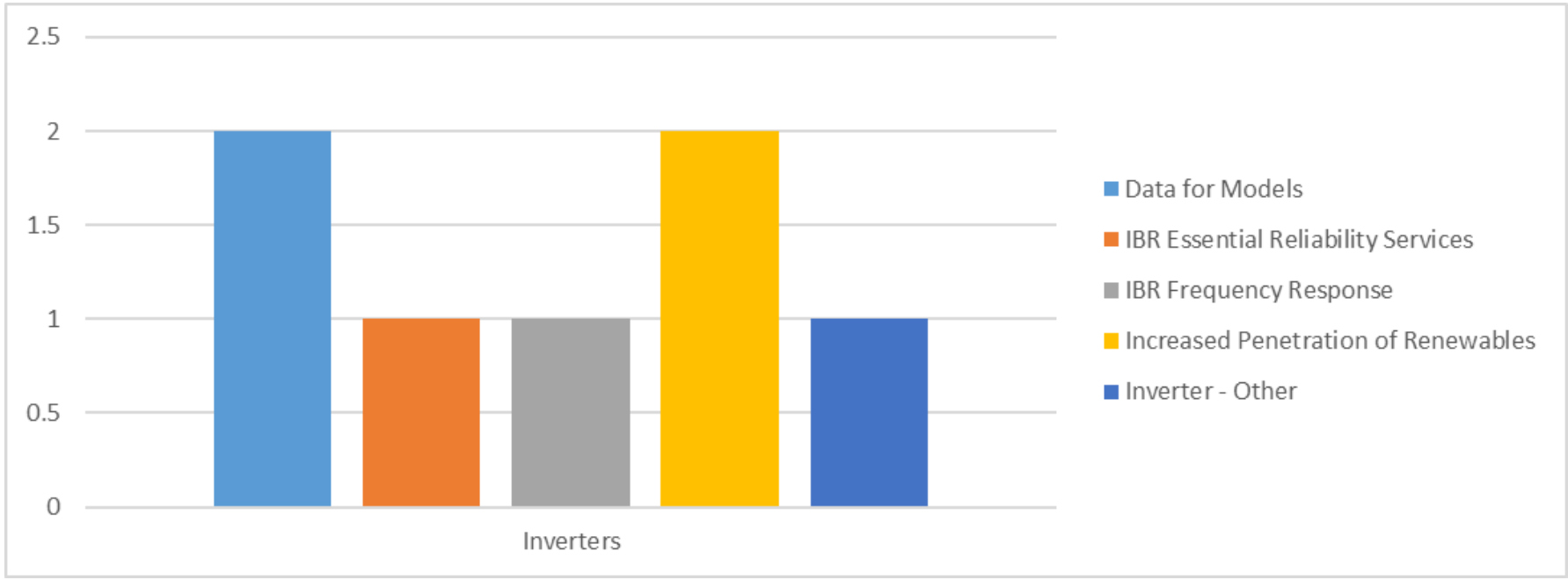
Security Risks



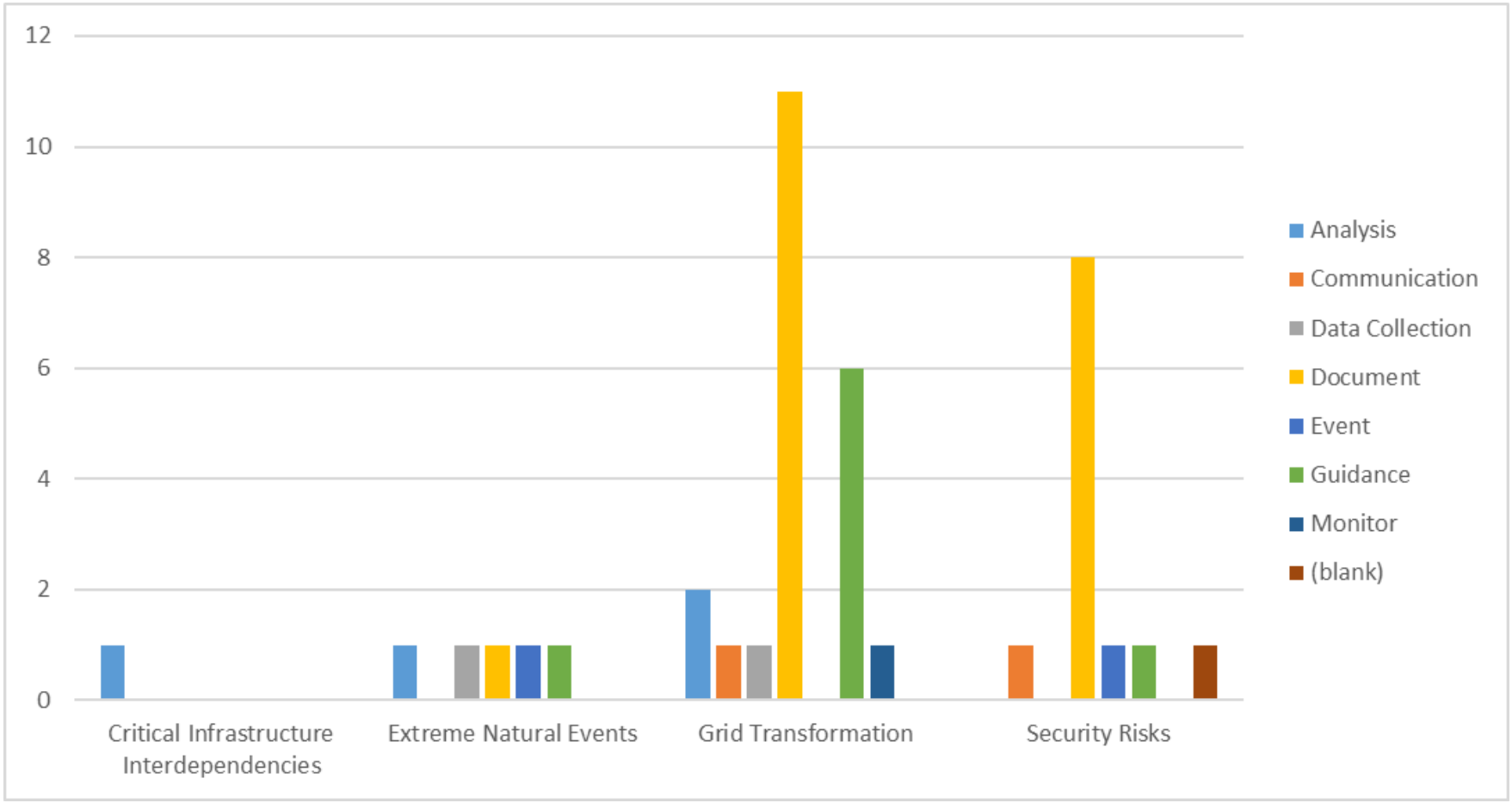
Extreme Natural Events/Cold Weather Preparedness



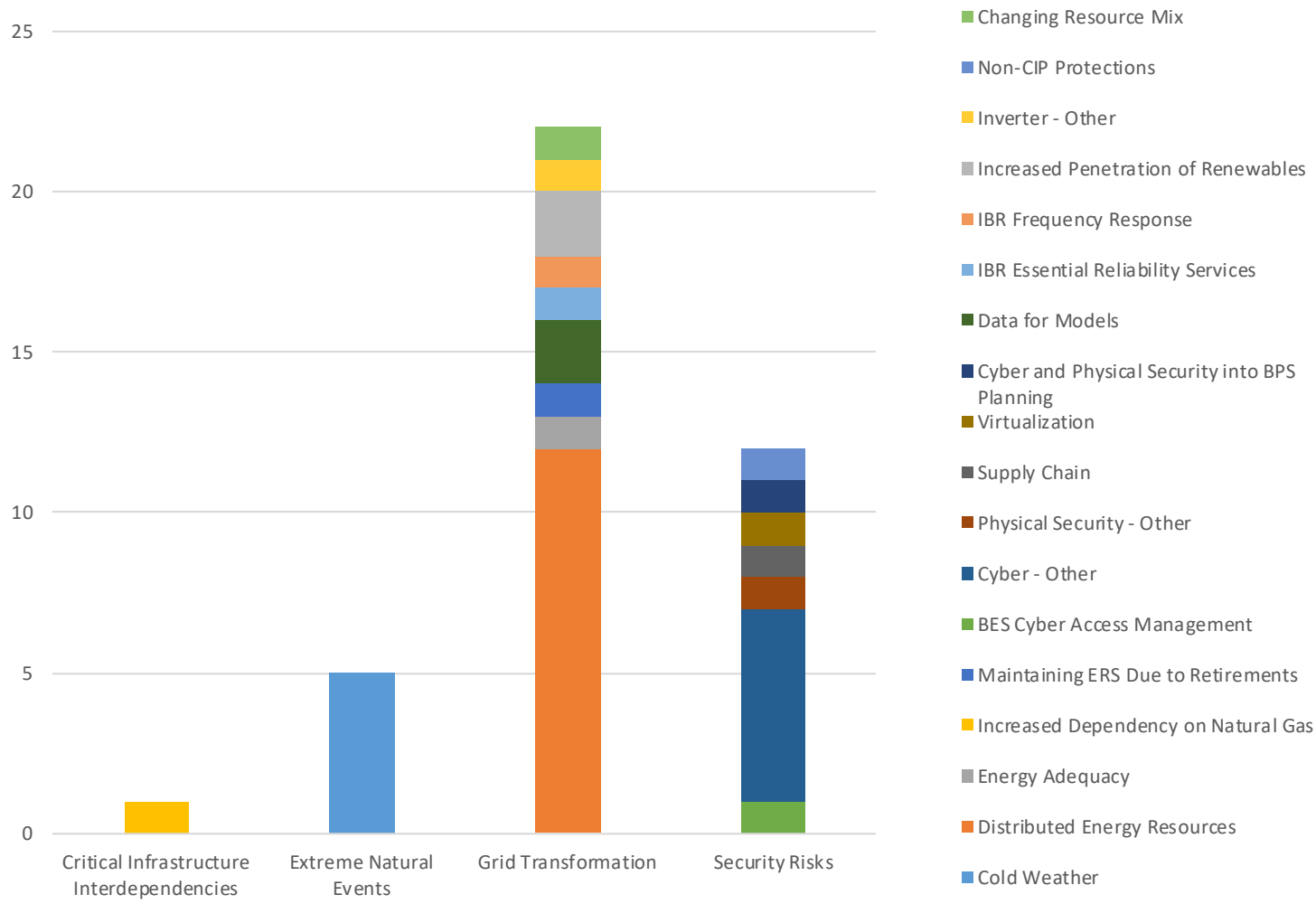
Inverters


2.5
2
1.5
1
0.5
0
Inverters
Data for Models
IBR Essential Reliability Services
IBR Frequency Response
Increased Penetration of Renewables
Inverter - Other

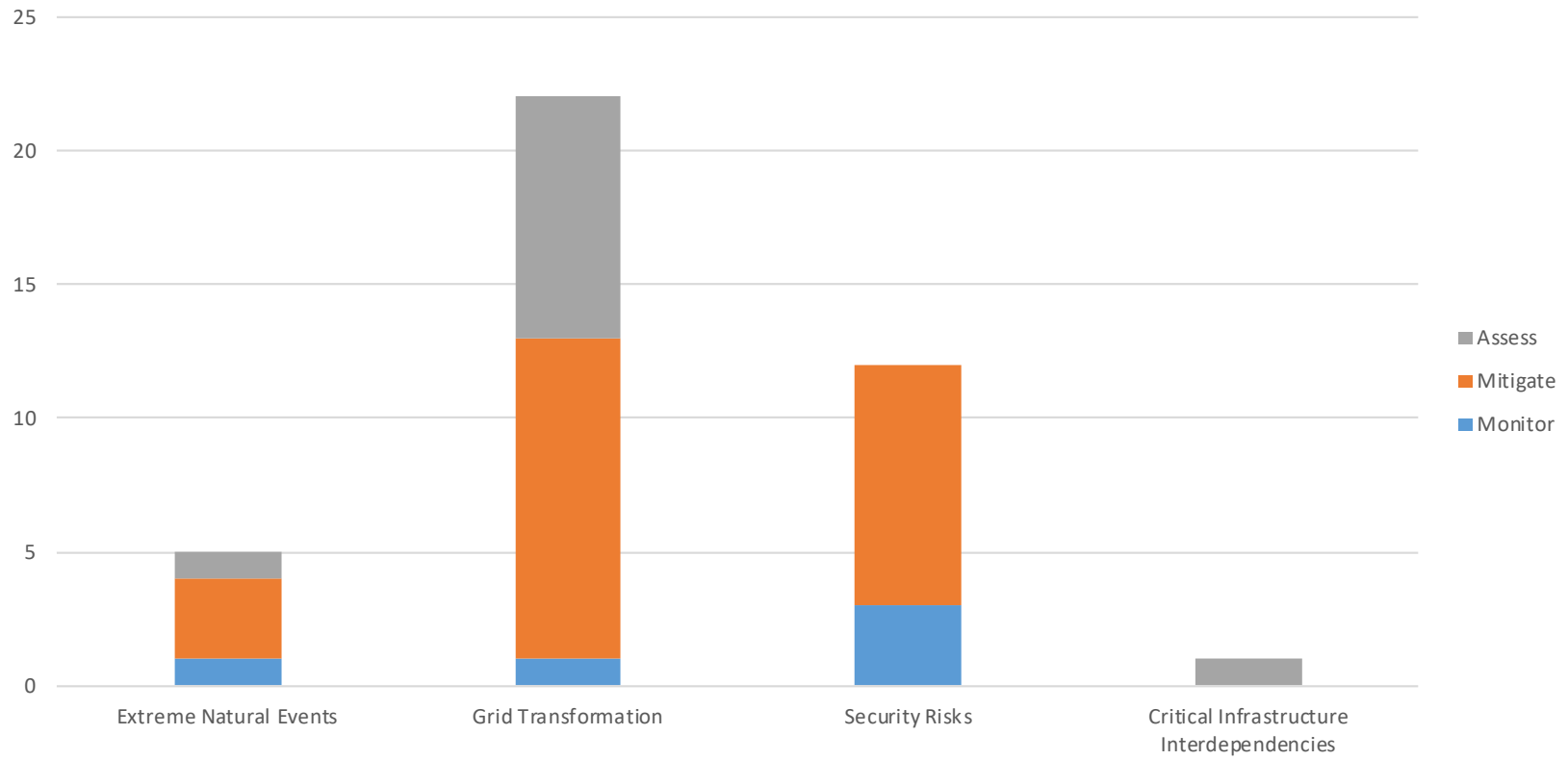
Risk by Risk Profiles



Risk by Risk Profiles



Risk by Risk Profiles



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Failure Modes & Mechanisms Task Force Update

Richard Hackman – NERC Event Analysis
RSTC Meeting
September 8, 2021

RELIABILITY | RESILIENCE | SECURITY




Failure Modes and Mechanisms (FMM)

The joint 2013 NERC Operating and Planning Committees' AC Substation Equipment Task Force report recommended that information on station equipment failures be collected through the NERC Event Analysis Process. The data is intended to aid in analysis of station equipment failures to identify threat trends to the reliability of the BES and potential ways to improve reliability.

The Addendum for Events with Failed Station Equipment (the Addendum) is used to collect failed station equipment information for submittal with the Brief Report for events. It uses a failure modes and mechanisms (FMM) approach. Basically, a failure mode is what gets your attention – it tells you that the equipment has failed, while failure mechanisms are how the equipment gets going on the path to a failure. FMM information is intended to be provided in addition to the identified contributing causes and root cause determined through the entity's root cause analysis of the event. A short video explaining the FMM approach* is available.

The Addendum lists 14 common equipment types, and FMM diagrams are being made available for each equipment type. Currently, there are 8 EAS-approved FMM diagrams and 6 diagrams in the draft stage.

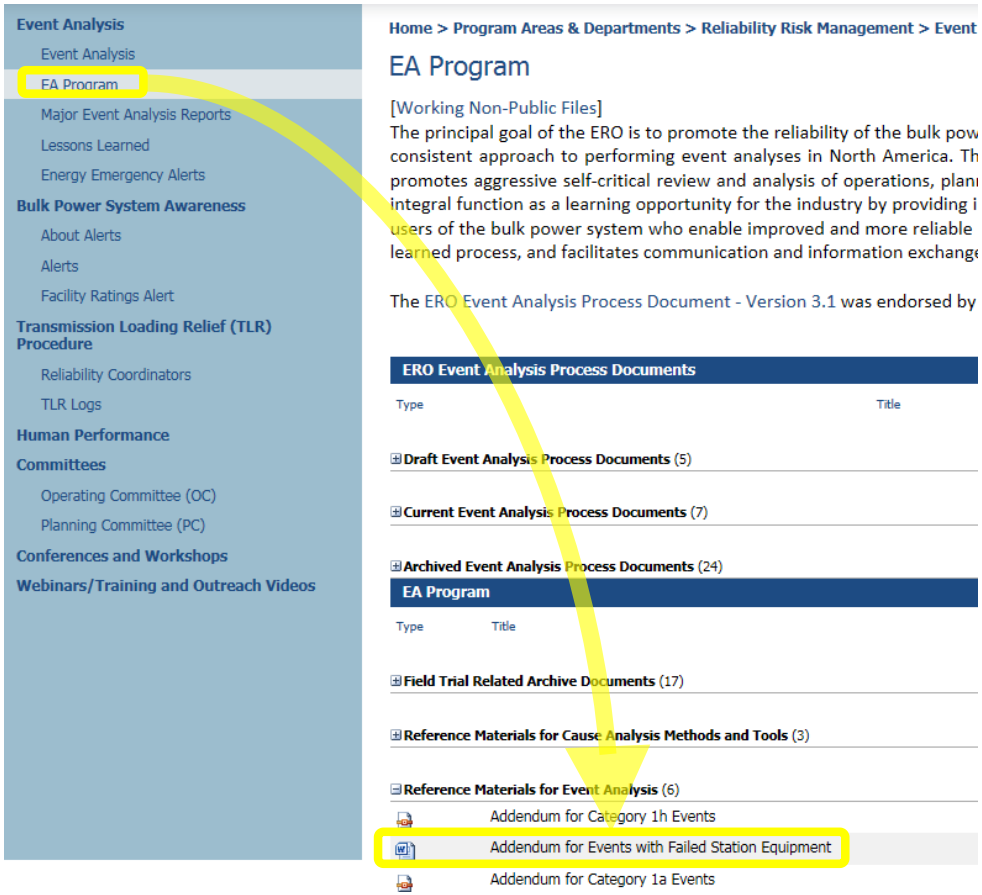
* https://vimeopro.com/nerclearning/cause-coding/video/208745179

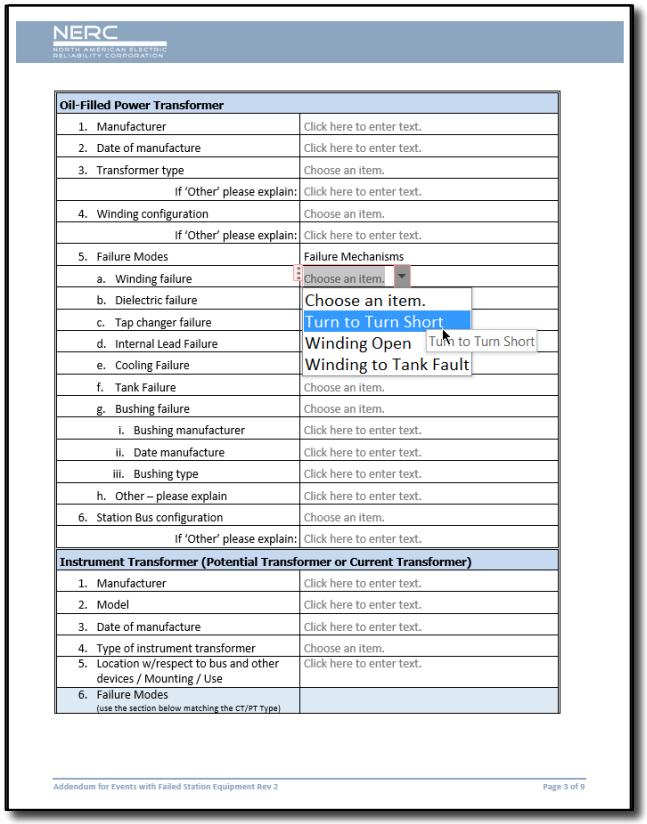
FMMTF Purpose

Formation of the Failure Modes and Mechanisms Task Force (FMMTF) was approved by the EAS in December 2019 to:

- Analyze BES substation equipment types listed in the Addendum to determine their failure modes & mechanisms, FMM trends and patterns, and improve BES reliability by providing information useful for reducing station equipment failures.
- Improve the Addendum and processes to collect data associated with failure of station equipment;
- Derive solutions from FMM studies to
  - Detect and measure the progress of active FMM in station equipment;
  - Avoid, prevent or delay the progression of station equipment failures;
  - Promote development of “good industry practices’.
- Support the Energy Management System Working Group (EMSWG) in their development of energy management system FMM, and provide FMM information and support to other Electric Reliability Organization groups as needed.

NERC Event Analysis Website
Addendum for Events with Failed Station Equipment





The Addendum for Events with Failed Station Equipment is available on the NERC Event Analysis Program webpage.

Failure Modes & Mechanisms Diagrams are shared via the ERO Portal

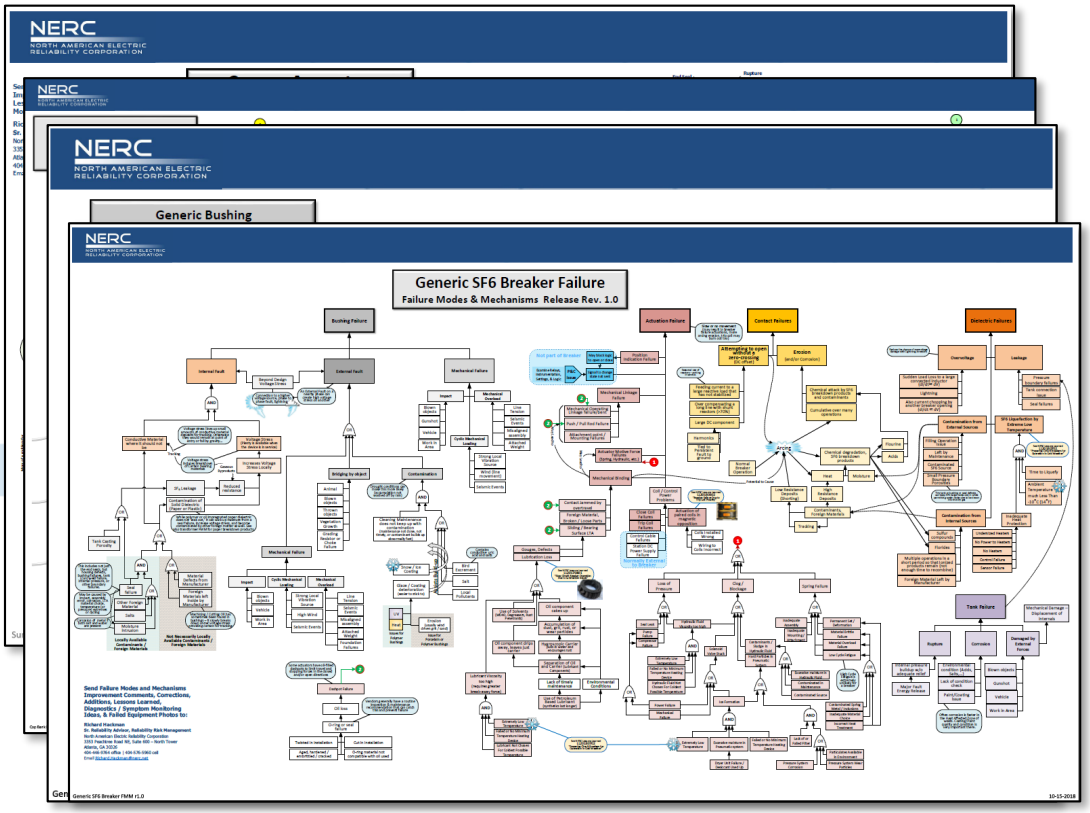
NERC Extranet

ERO EA Data Sharing

Documents

new document or drag files here

- Name
- Crisis Action Plan
- ERO EA Meeting Materials
- ERO SA-EA tuesday meeting info
- Failure Modes and Mechanisms
- Internal Process Documents
- Program Oversight Plans
- Regional Audit Files
- System Maps
- Lessons Learned Keyword Search
- NERC EA Staff Contacts 04_04_2019



These are accessible by the Event Analysis groups of each ERO Region for sharing with entities on an as-needed/as-requested basis.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Sept 2020 FMMTF Status

Substation Equipment	Status	FMMTF lead	FMMTF second	Schedule / priority
Generic Bushing	Release Rev 1			
Oil-Filled Power Transformer	EAS approved to release			
Wire Wound Electromagnetic Potential Transformer		Harvey		Med
Coupling Capacitor Voltage Transformer (markup)	EAS approved to release	Harvey	Bob Kenyon	High
Optical Voltage Transformer	draft			Low
Wire Wound Electromagnetic Current Transformer	draft	Harvey		Med
Optical Current Transformer	draft			Low
SF6 Breaker	Release Rev 1			
Air Blast Breaker	draft			
Oil Breaker	draft	Shawn Adderly	Ryan Snyder	High
Switch	draft	James Houston	Mike Bocovich	High
Oil-Filled Reactor (Inductor)	draft	Bob Kenyon	Mike Bocovich	Med
Capacitor Bank	Release Rev 1			
Surge Arrester	Release Rev 1			
Electromagnetic Relay	Early draft	Max	Laurel	High
Static Relays		Max		Low
Microprocessor Relay	draft	Max	Laurel	High

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Sept 2021 FMMTF Status

Substation Equipment	Status	FMMTF lead	FMMTF second	Priority
Generic Bushing (Will add LL20210701 Dry Wind-Borne Salt Contamination)	Release Rev 1	Rick Hackman		
Oil-Filled Power Transformer	Release Rev 1	Luke Weber		
Wire Wound Electromagnetic Potential Transformer		Harvey Veenstra	Luke Weber	Med
Coupling Capacitor Voltage Transformer	Release Rev 1.01	Harvey Veenstra	Bob Kenyon	
Optical Voltage Transformer	draft	Luke Weber	Harvey Veenstra	Low
Wire Wound Electromagnetic Current Transformer	draft	Harvey Veenstra	Luke Weber	Med
Optical Current Transformer	draft	Luke Weber	Harvey Veenstra	Low
SF6 Breaker (Will add nozzle erosion notes)	Release Rev 1	Jackie Brusoe		
Air Blast Breaker	draft	Rick Hackman		
Oil Breaker	draft	Shawn Adderly	Ryan Snyder	High
Switch	Release Rev 1	James Houston	Mike Bocovich	
Oil-Filled Reactor (Inductor)	Release Rev 1	Bob Kenyon	Mike Bocovich	
Capacitor Bank	Release Rev 1	Rick Hackman		
Surge Arrester	Release Rev 1	Rick Hackman		
Electromagnetic Relay	Early draft	Max Desruisseaux	Laurel Brandt	High
Static Relays		Max Desruisseaux	Ryan Snyder	Low
Microprocessor Relay	draft	Max Desruisseaux	Laurel Brandt	High

Temperature issues and hazard markers are being added

Current FMMTF Membership

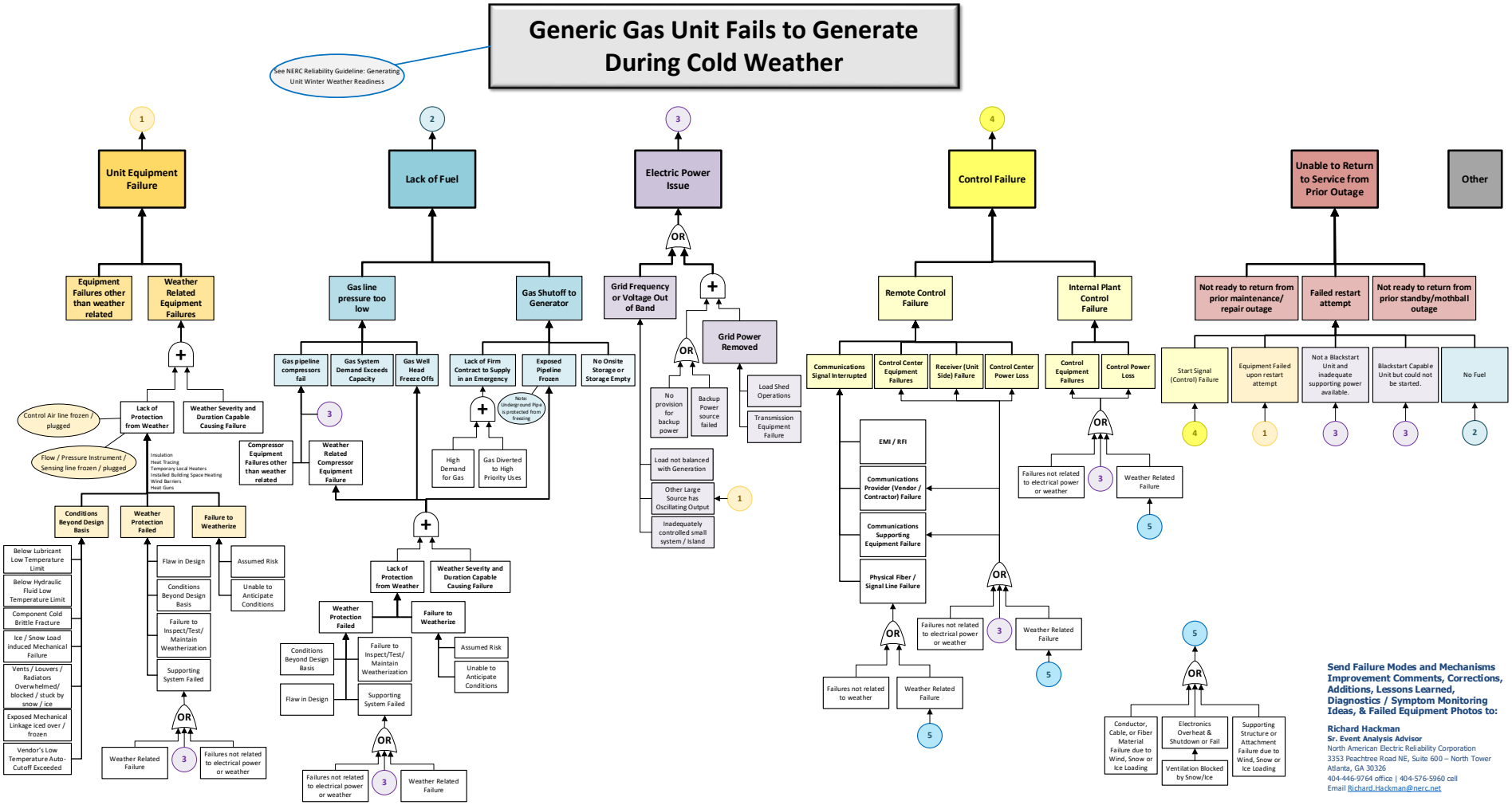
Currently the FMM Task Force has 12 volunteers from entities and ERO portions including:

- Xcel Energy
- McKenzie Electric
- Tennessee Valley Authority
- Florida Power & Light
- Pacific Gas & Electric
- Southern Company
- CenterPoint Energy
- Bonneville Power Authority
- Western Area Power Authority
- Midwest Reliability Organization
- NERC

The FMM Task Force would welcome additional volunteers

Note: Outside of the FMMTF, a FMM approach was used in discussing Cold Weather Generation Problems in the NERC Winter Weather Webinar on September 2nd.

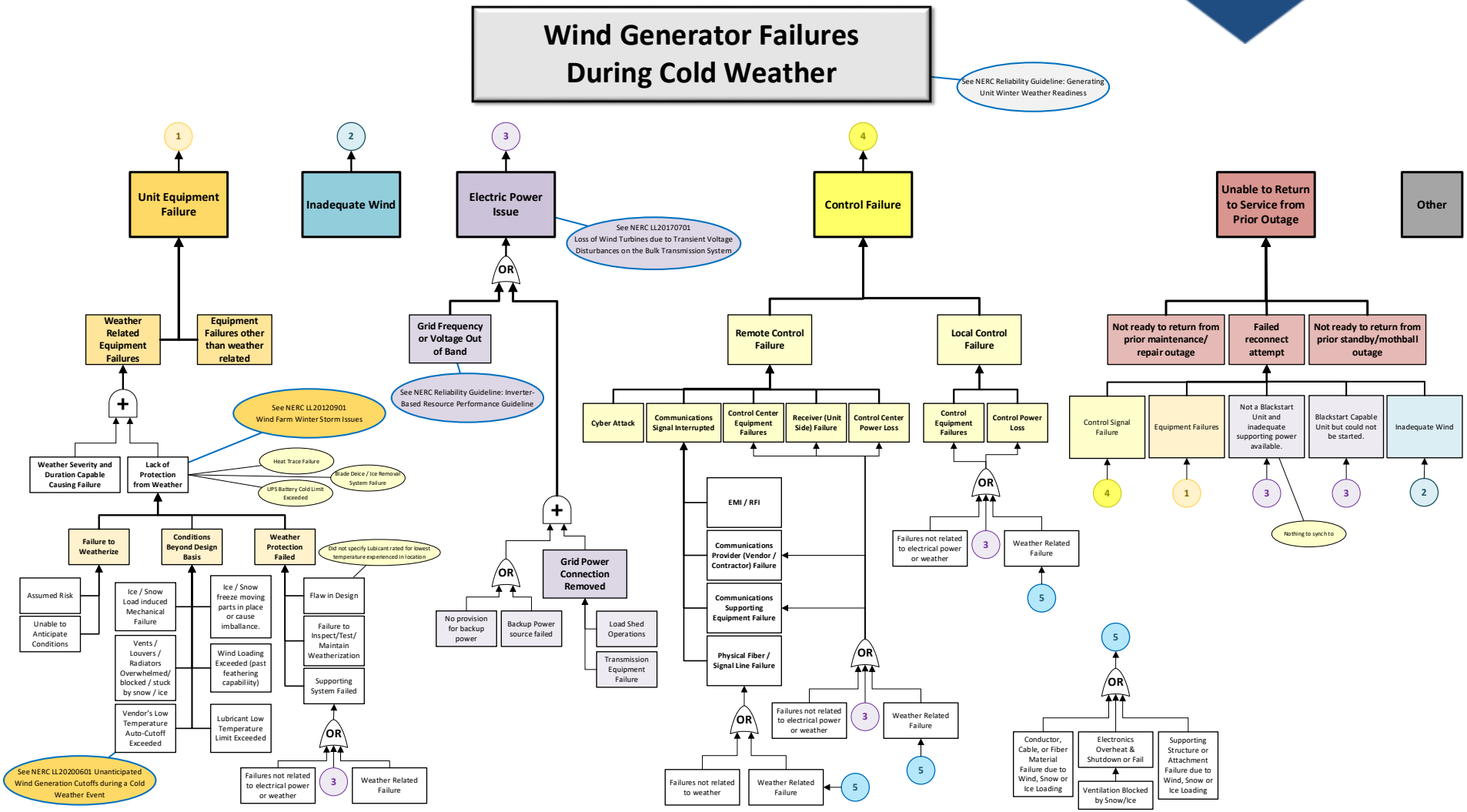
Generic Gas Unit Cold Weather Issues



Send Failure Modes and Mechanisms Improvement Comments, Corrections, Additions, Lessons Learned, Diagnostics / Symptom Monitoring Ideas, & Failed Equipment Photos to:

Richard Hackman
Sr. Event Analysis Advisor
North American Electric Reliability Corporation
3353 Peachtree Road NE, Suite 600 – North Tower
Atlanta, GA 30326
404-446-9764 office | 404-576-5960 cell
Email Richard.Hackman@nerc.net

Wind Generator Cold Weather Issues



Questions and Answers

Richard Hackman
Sr. Event Analysis Advisor
North American Electric Reliability Corporation
3353 Peachtree Road NE, Suite 600 – North Tower
Atlanta, GA 30326
404-446-9764 office | 404-576-5960 cell
Email Richard.Hackman@nerc.net
NERC Lessons Learned webpage

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Restoration Analysis to Evaluate Resilience of the Transmission System under Extreme Weather

Based on the 2015-2020 TADS Data

Svetlana Ekisheva, Ph.D., Principal Data Science Advisor, NERC

RSTC Meeting

September 8, 2021

RELIABILITY | RESILIENCE | SECURITY




Project

- NERC team (Svetlana Ekisheva, Rachel Rieder, Jack Norris) and prof. Ian Dobson (Iowa State University)
- TADS outage events, grouping algorithm development and enhancement
  - Weather-related transmission outage events
    - A paper presented at the 2021 IEEE PES GM (with M. Lauby)
- Restoration and Resilience study for transmission weather-related events
  - Four panel presentations at the 2021 IEEE PES GM
  - Analysis of the 2020 top transmission events included in the 2021 State of Reliability
  - Work on improving the grouping algorithm
  - Plan to extend the SOR section to include analysis by extreme weather type and to define and start tracking restoration metrics

2015-2020 Weather-Related Transmission Events by Extreme Weather Type

Outage Grouping Algorithm

- Input: 2015-2020 TADS automatic outages
  - ~62k outages for all TADS elements, all voltages
- Overlapping outages in the same interconnection are grouped together into transmission outage events
- Weather related events are defined as follows:
  - If an event contains one or more outages with a cause code of “Fire”, “Weather, excluding lightning”, “Environmental” or “Lightning”, it is considered a weather related event

2015-2020 Weather-Related Events

- Overall, weather-related events comprise 36% of the 35,392 transmission outage events for the 6 years
  - Medium events (10-19 outages): 272 weather events and 21 non-weather events
  - Large events (20-378 outages): 86 weather events and 1 non-weather event
- The extreme weather that caused a large weather event was determined from the combination of the following data sources:
  - NERC System Awareness Daily reports
  - NERC Event Analysis reports
  - Public sources: National weather service, news, press releases etc.
- A summary for 22 largest events on the next slide

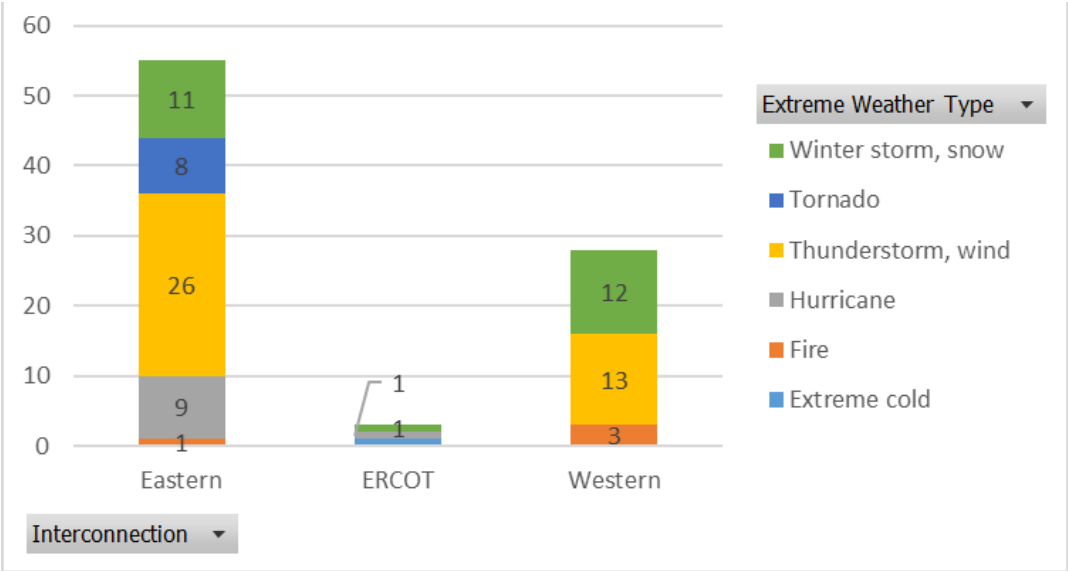
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

2015-2020 Top Large Weather-Related Events (22 largest with 378-44 outages)

Year	Event StartDt	Interconnection	Extreme weather that caused Large Transmission Event	Event Size (Outages)	Event Duration (Days)	Miles Affected	MVA Affected	TADS elem affected
2017	9/10/17 10:16	Eastern	Hurricane Irma	378	19.5	6645	129933	303
2016	10/7/16 5:48	Eastern	Hurricane Matthew	279	59.6	6860	100648	247
2018	10/10/18 11:00	Eastern	Hurricane Michael	200	28.5	4659	62051	184
2020	10/28/20 23:28	Eastern	Hurricane Zeta	153	40.7	3731	56740	127
2015	11/17/15 17:21	Western	Strong wind storms	143	5.9	4844	45578	117
2020	4/12/20 16:50	Eastern	Easter Tornado	116	16.1	2630	42085	109
2020	8/4/20 13:55	Eastern	Hurricane Isaias	108	9.4	1352	43404	87
2017	4/30/17 3:50	Eastern	Heavy rain and thunderstorms	103	246.0	3303	39253	86
2020	8/10/20 15:27	Eastern	Windstorms	74	22.1	1217	26488	73
2015	12/16/15 14:17	Eastern	Wide-spread rains and snowstorms	63	1.5	2141	24118	29
2018	4/14/18 18:57	Eastern	Blizzard, Severe thunderstorms and tornadoes	63	1.7	1336	21076	47
2019	3/13/19 16:18	Western	Strong winter storms with high winds	55	10.4	2177	23895	33
2016	3/23/16 10:35	Western	Heavy snow and freezing rains	52	0.7	1925	21613	37
2019	4/11/19 4:04	Eastern	Storm system with high winds, snow, sleet, and ice	52	81.0	1835	34435	37
2020	8/27/20 6:49	Eastern	Hurricane Laura	49	14.6	791	17604	46
2018	3/2/18 15:29	Eastern	Nor'easter	48	7.2	840	16573	41
2018	3/13/18 12:26	Eastern	Nor'easter	47	2.8	625.7	19966	22
2020	9/7/20 14:03	Western	Wildfires	46	87.2	1617.8	19797	43
2015	12/28/15 1:43	Eastern	tornadoes	45	4.2	1348.8	19963	37
2015	8/29/15 16:43	Western	Strong storms with high winds	44	6.2	671.7	7841	42
2019	9/8/19 3:17	Western	Lightning storm	44	8.6	2173.6	27475	40
2020	10/28/20 14:45	Eastern	Icestorm	44	20.3	923.2	20175	42

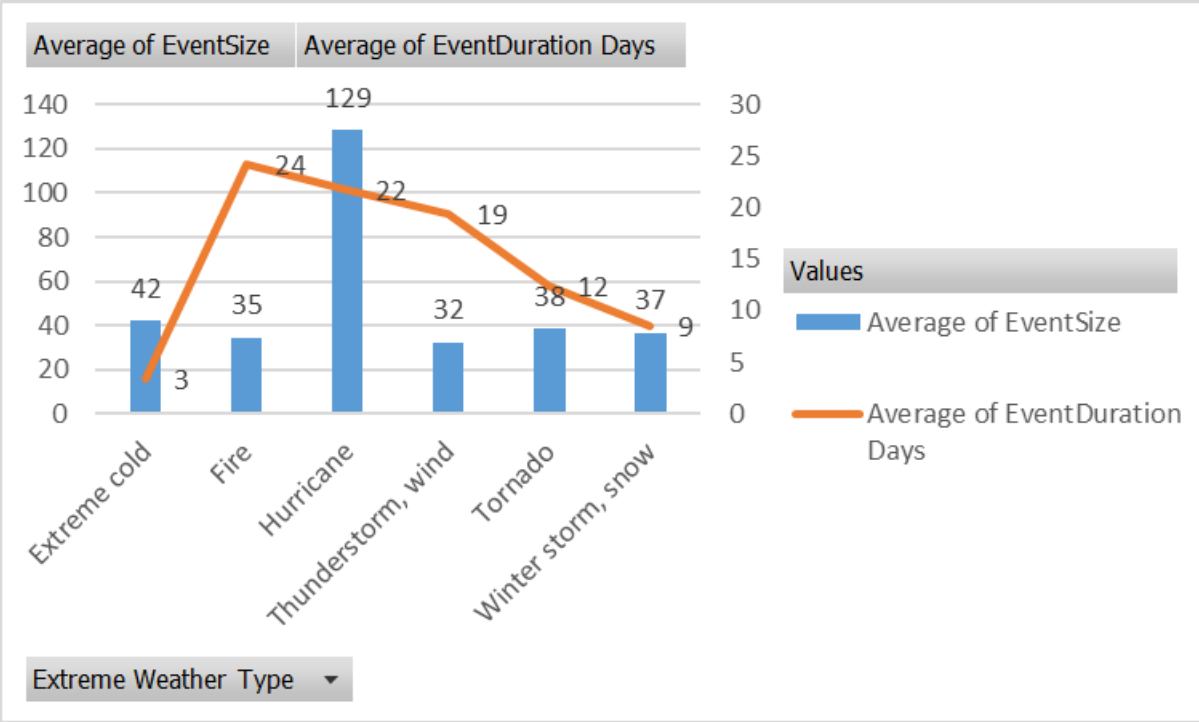
Large Weather Events by Interconnection and Extreme Weather Type

Extreme Weather Type	2015-2020 Large Transmission Events
Thunderstorm, wind	39
Winter storm, snow	24
Hurricane	10
Tornado	8
Fire	4
Extreme cold	1
Grand Total	**86**



- 4 out of the 10 hurricane events occur in 2020

Large Weather Events Statistics by Extreme Weather Type



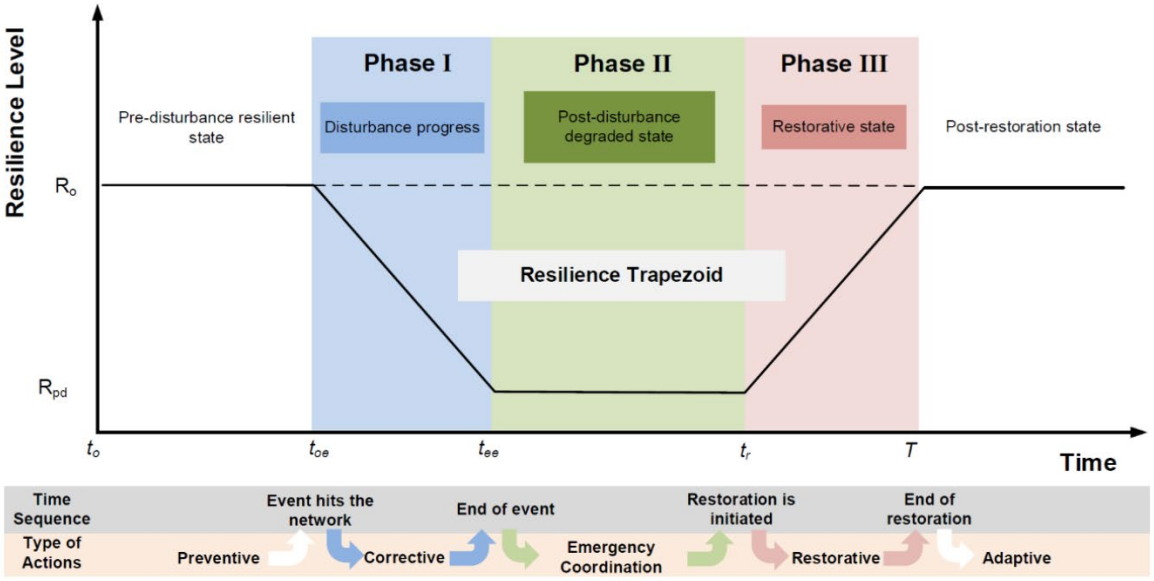
- Overall, the average large event size is 46 outages and the duration is 16.0 days
- The large event size varies from 20 to 368 outages
- There is a huge variability in the event duration (from 3 hours to 246 days)

Analysis of Transmission Events with Outage, Restore, and Performance Functions

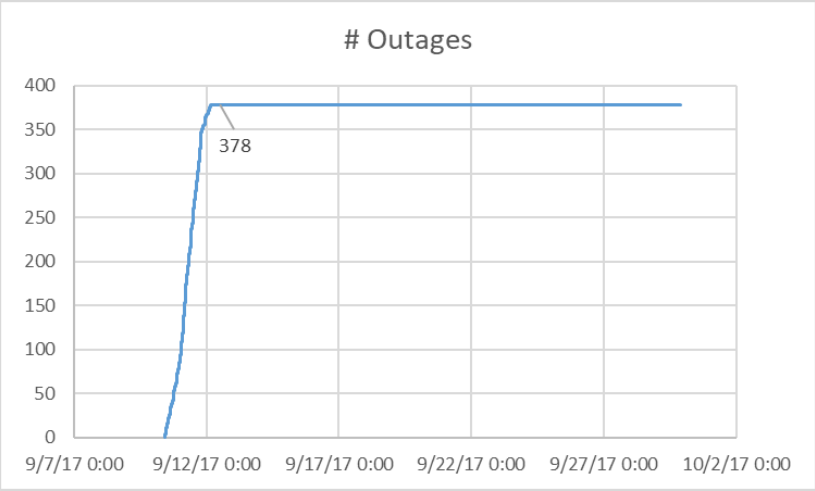
Example: Hurricane Irma (2017)

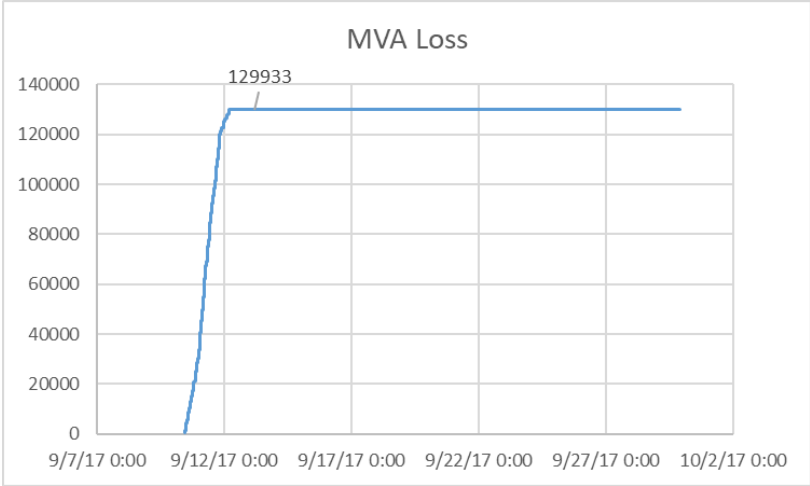
How We Study Transmission Outage Events

- To analyze resilience of the transmission system, we use TADS data to define and draw event curves, similar to a conceptual graph of a resilience event below (DOE-IEEE Technical Report: Resilience Framework, Methods, and Metrics for the Electricity
- These curves provide details about what was happening at every moment in time during an event.



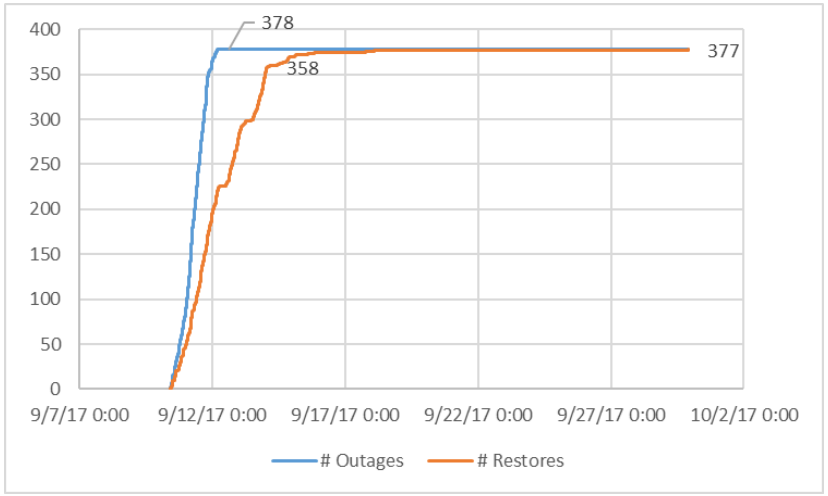
Hurricane Irma: Outage Process

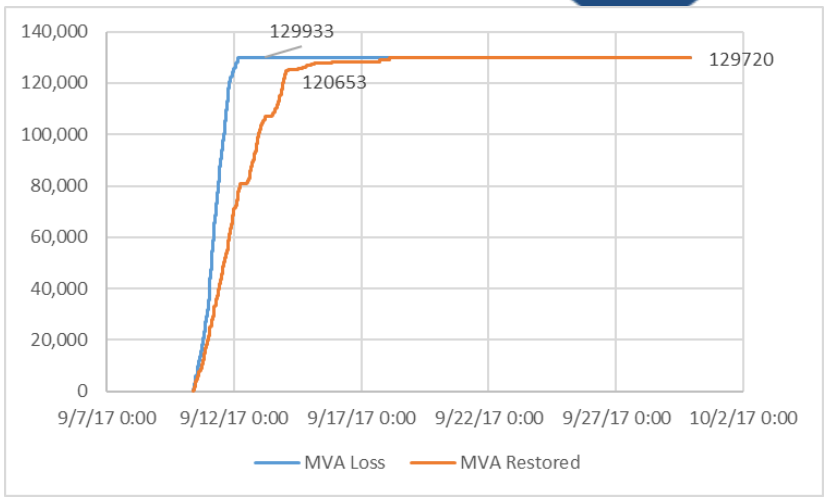




- An event start time: the earliest outage start time (10:16 on September 10, 2017)
- An event end time: the latest restore time (the latest outage end time) (21:36 on September 29)
- An event duration: the end time – the start time (~19.5 days)
- The outage function O(t) counts the cumulative number of outages occurred in the event by time t. (Or MVA loss)
- The outage process lasted 42 hours until the total number of outages was accumulated (at 4:21 AM on September 12, 2017)
- The average outage rate 9.0 outages and ~43,000 MVA per hour

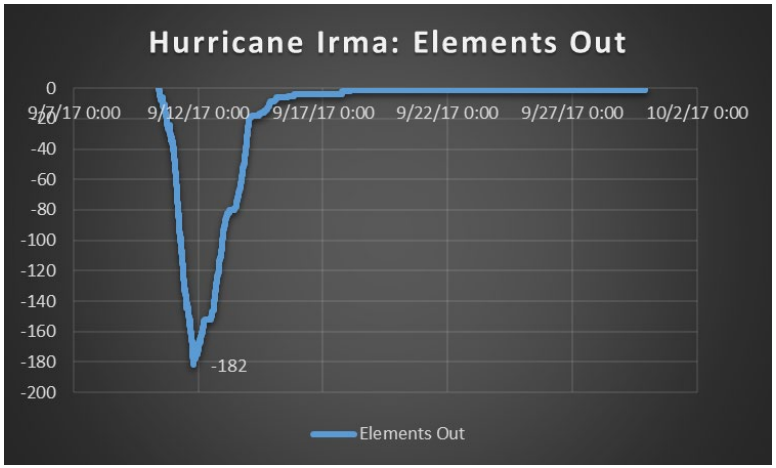
Hurricane Irma: Restore Process

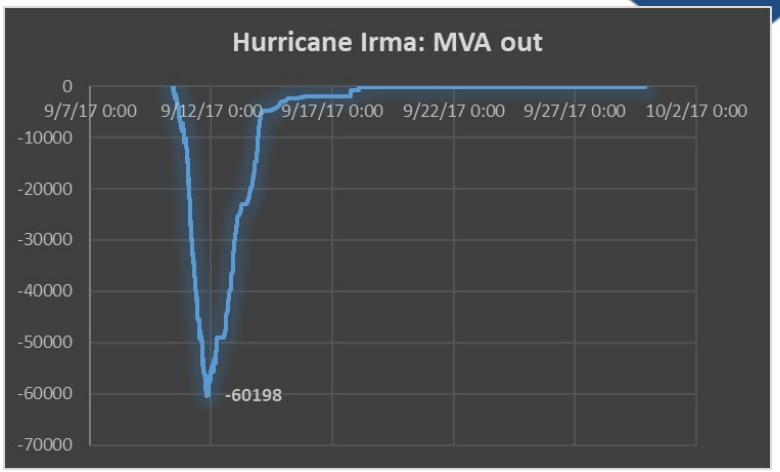




- The restore function R(t) counts the cumulative number of restores occurred in the event by time t.
- The restore process started immediately due to a momentary outage and lasted the full duration of the event.
- The last remaining outage of a 100-199 kV ac circuit (213 MVA) lasted 11.8 days
- 95% of outages were restored for 89.0 Hours (3.7 days)
- 95% of MVA were restored for 86.3 Hours (3.6 days)

Hurricane Irma: Performance Curves

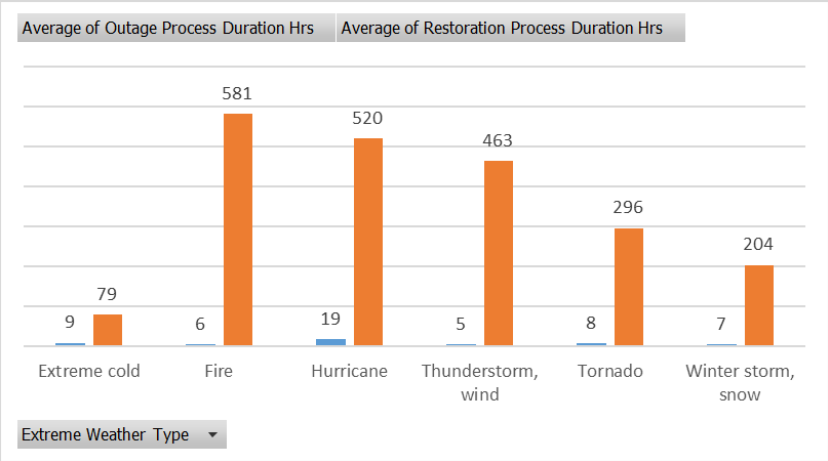


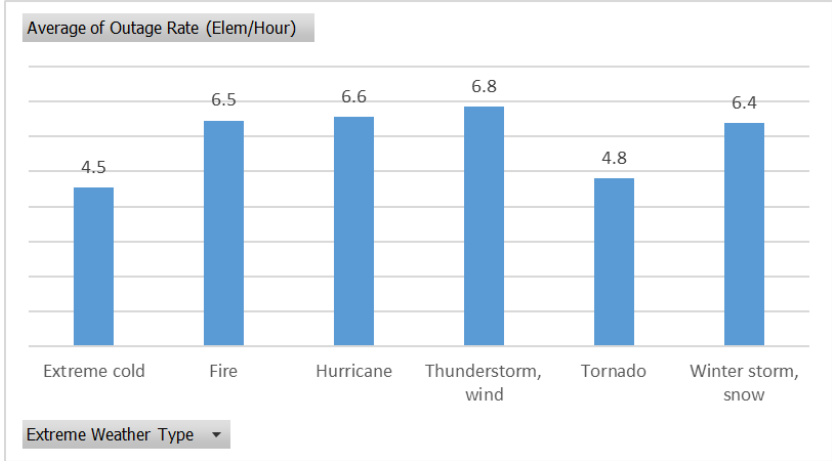


- The performance function is calculated as R(t)-O(t). The element-based performance function is the negative number of TADS elements out at time t.
- The MVA-based performance function is the negative amount of MVAs out at time t
- The nadirs of the performance curves indicate the max simultaneous number of elements out or MVAs out.
- For Irma, they were attained in 33 hours (1.4 days) after the event start. The system stayed at this level for 5 minutes.
- ~390 element-days lost (the area between the x (time) axis and the elements-out curve)
- ~125.5k MVA-days lost (the area between the x (time) axis and the MVA-out curve)

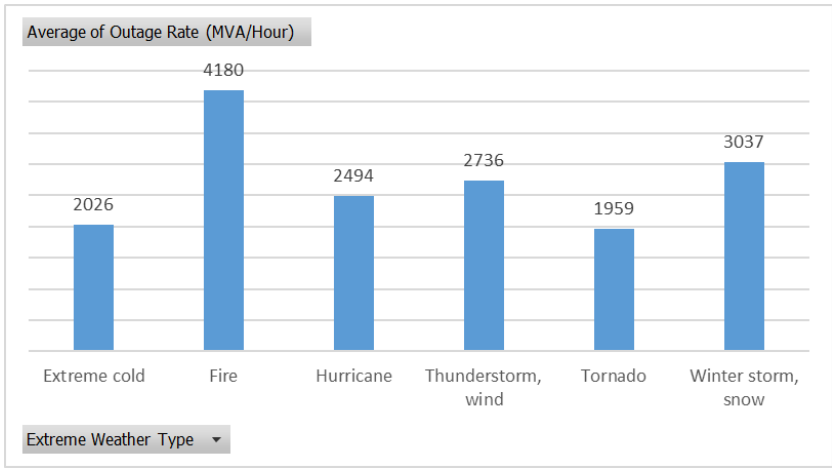
Selected Statistics for Outage, Restore, and Resilience (Restoration Performance) Processes for 2015-2020 Large Weather-Related Events

Outages and Restorations

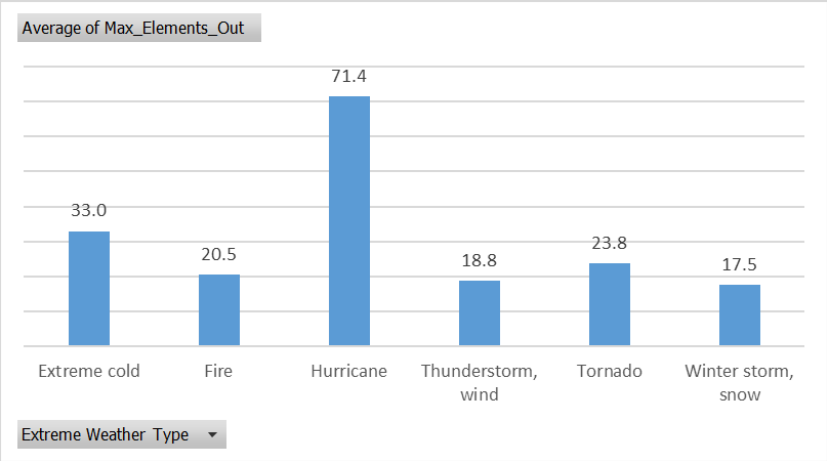


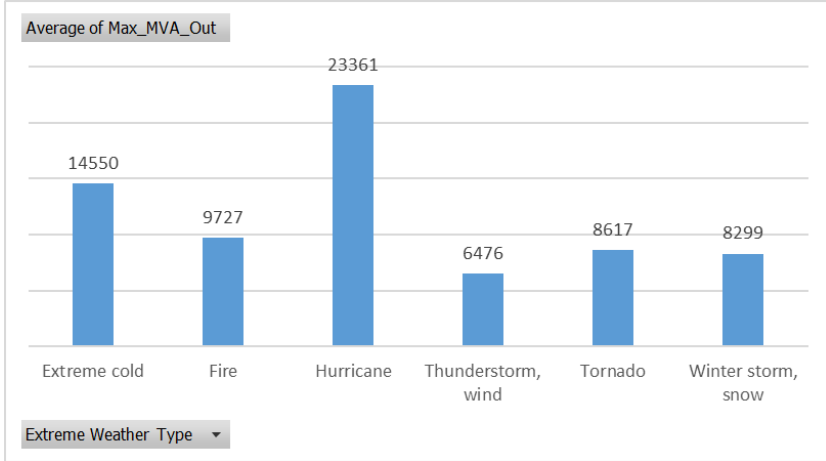


- Typically, the outage process is much shorter than the restore process
- The average outage process durations for different extreme weather types are similar except hurricanes, which is ~2-4 times longer.
- The average time to first restore is 47 minutes
- The outage rates are similar among all types.
- The MVA loss rate is the highest for Fire (ac circuits of higher voltages from WECC are affected)

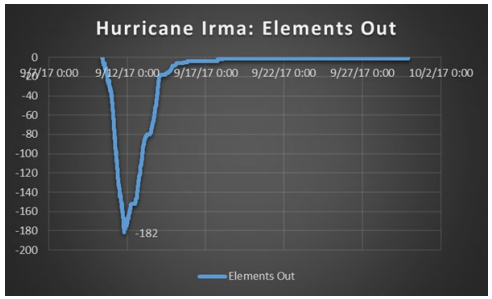


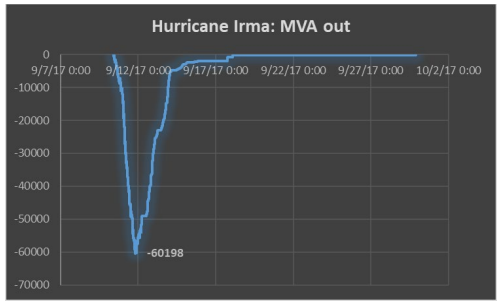
Maximum Simultaneous Number of Elements Out and MVA Out



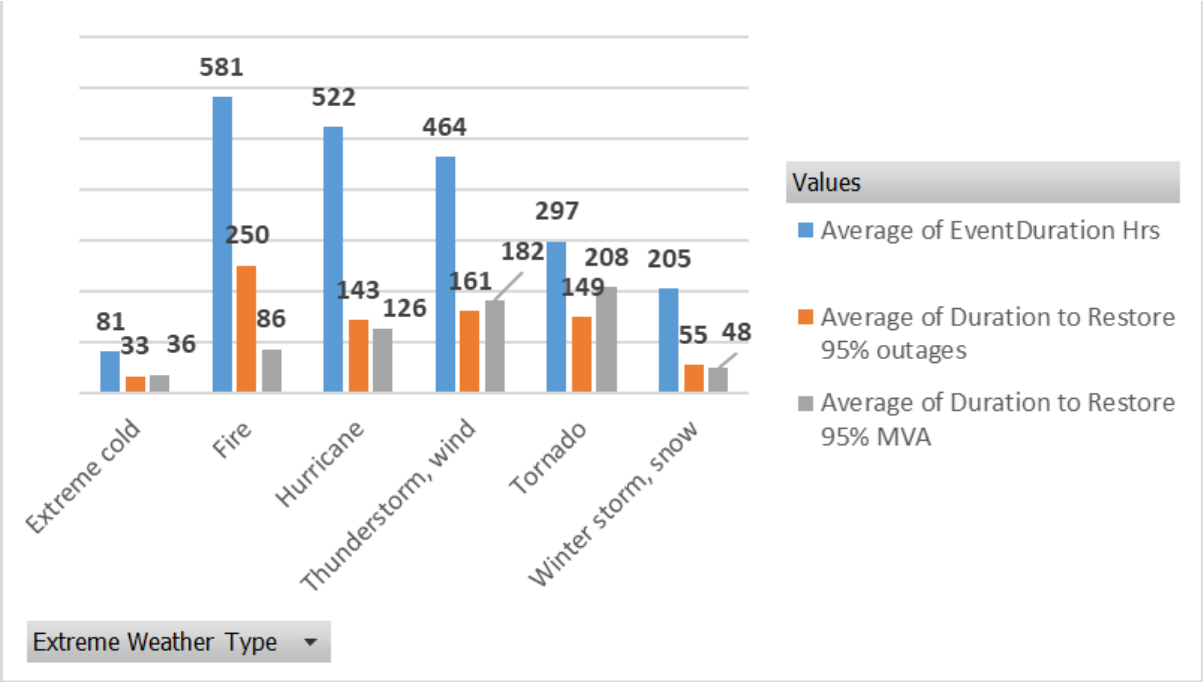


- Typically, the nadirs reached soon after the event started.
- MaxElementOut and MaxMVAOut usually happen at the same time (but not necessarily).
- Hurricanes cause events with highest maximum number of elements out and MVA out.



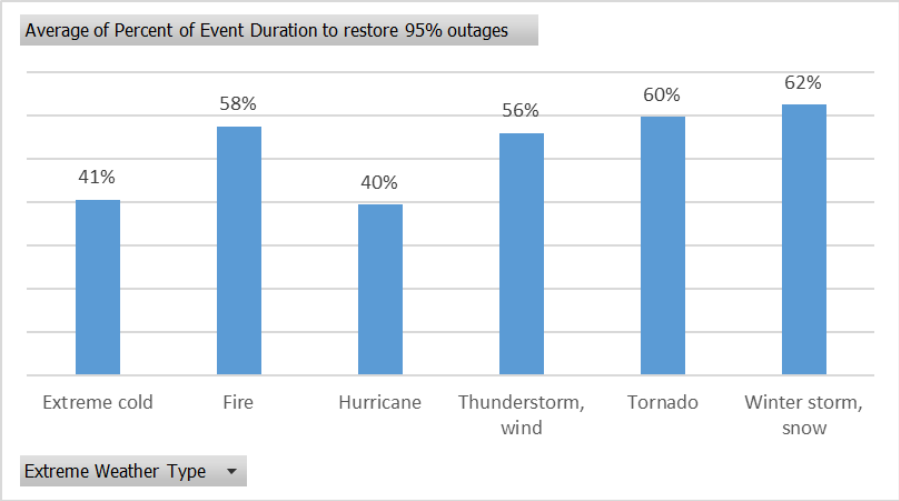


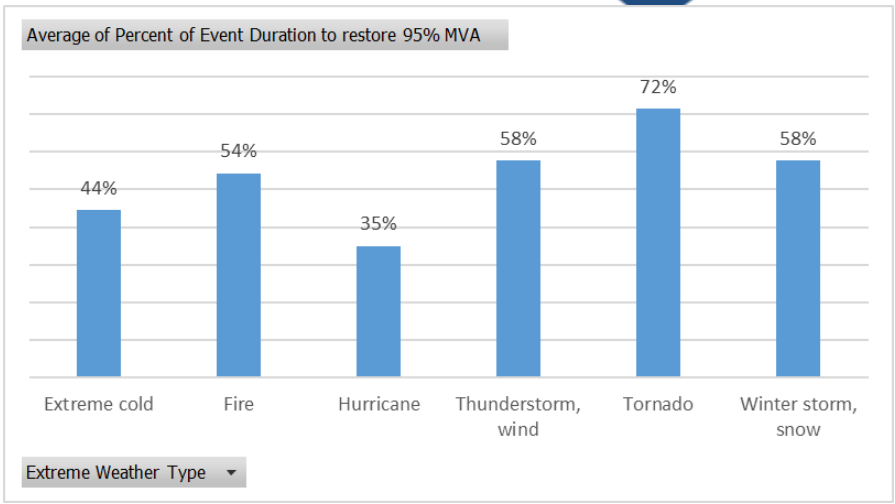
Events "Almost" Restored



- For majority of events only few (sometimes one) outages remain unrestored for a long time before the event ends.
- Time to "almost" restore the system is calculated
- The average times to restore 95% of outages and 95% of MVA are, on average, much shorter than the event duration for all extreme weather types

95% of Outages and 95% of MVA Restored



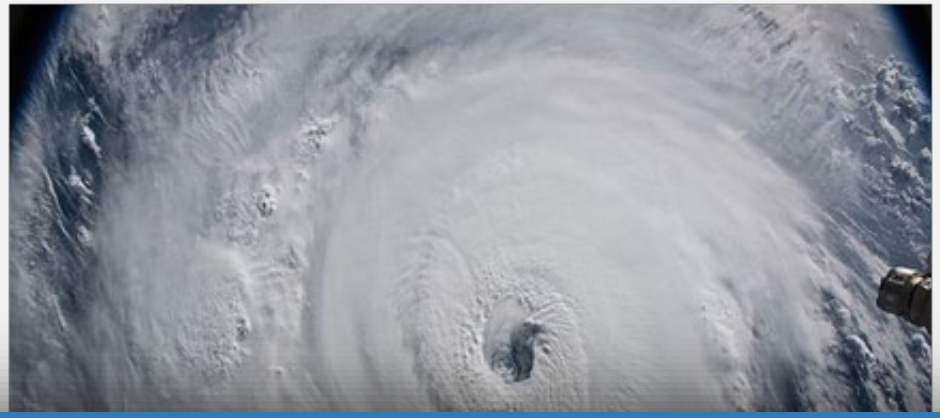


- On average, for the large events the time to restore 95% of outages takes 54% of event duration
- On average, for the large events the time to restore 95% of MVA affected by the event takes 56% of event duration
- For longer events the percent tends to be smaller

Conclusions and Future Work

- TADS outages are grouped in transmission events
- Weather-related events are identified by TADS outage causes
- For large events, the outage, restore, and performance functions are defined
- Statistics for these processes are calculated and analyzed: overall and by extreme weather type
- Partial restoration takes un-proportionally short time: on average, 95% of outages (MVA) are restored for 54% (56%) of event duration
- Future work:
  - The grouping algorithm improvements
  - Plan to extend the SOR section to include analysis by extreme weather type and to define and start tracking restoration metrics

Questions and Answers

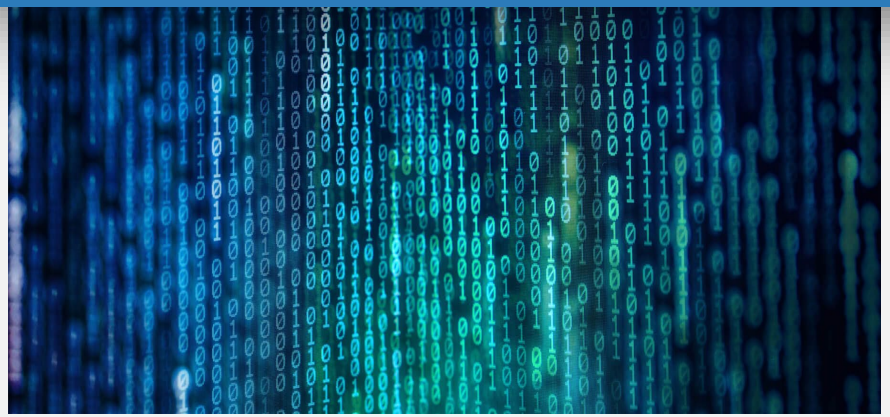


U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

CyOTE Cybersecurity for the Operational Technology Environment

CyOTE™

NERC Reliability & Security Technical Committee – September 8, 2021 – Sam Chanoski, Idaho National Laboratory



Purpose and Goals

CyOTE Cybersecurity for the Operational Technology Environment

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

What Need is CyOTE Targeting?

Today's energy sector IT and OT systems are **complex and interconnected**.

Sophisticated adversaries have the knowledge to target OT environments that result in **physical disruptions** to energy flows or damaged equipment.

Industry visibility, monitoring, and analysis capabilities in the OT space are still relatively new and immature—leaving asset owners and operators (AOOs) struggling to **determine** whether **anomalous operational events** potentially have a malicious cyber cause.

We need to **change the paradigm** for security and begin thinking of security as a holistic analysis of business operations to **identify anomalies** from unalterable data sources and investigate further from those sources.

What is the Problem CyOTE is Trying to Address?

Most AOOs lack the capability to analyze data from their OT networks effectively and consistently identify attacks, much less in real time – in significant contrast to their IT networks.

Even those who have some capabilities still want and need to improve their level of OT understanding.

Improving understanding of OT data enables AOOs to make better risk-informed decisions to secure their OT environments.

Challenges

Regulations limit the information that can be shared.

Geographic dispersion of assets in the field.

Communications channels may be limited.

No common lexicon for data fields and threat information.

Understanding anomalies in operations.

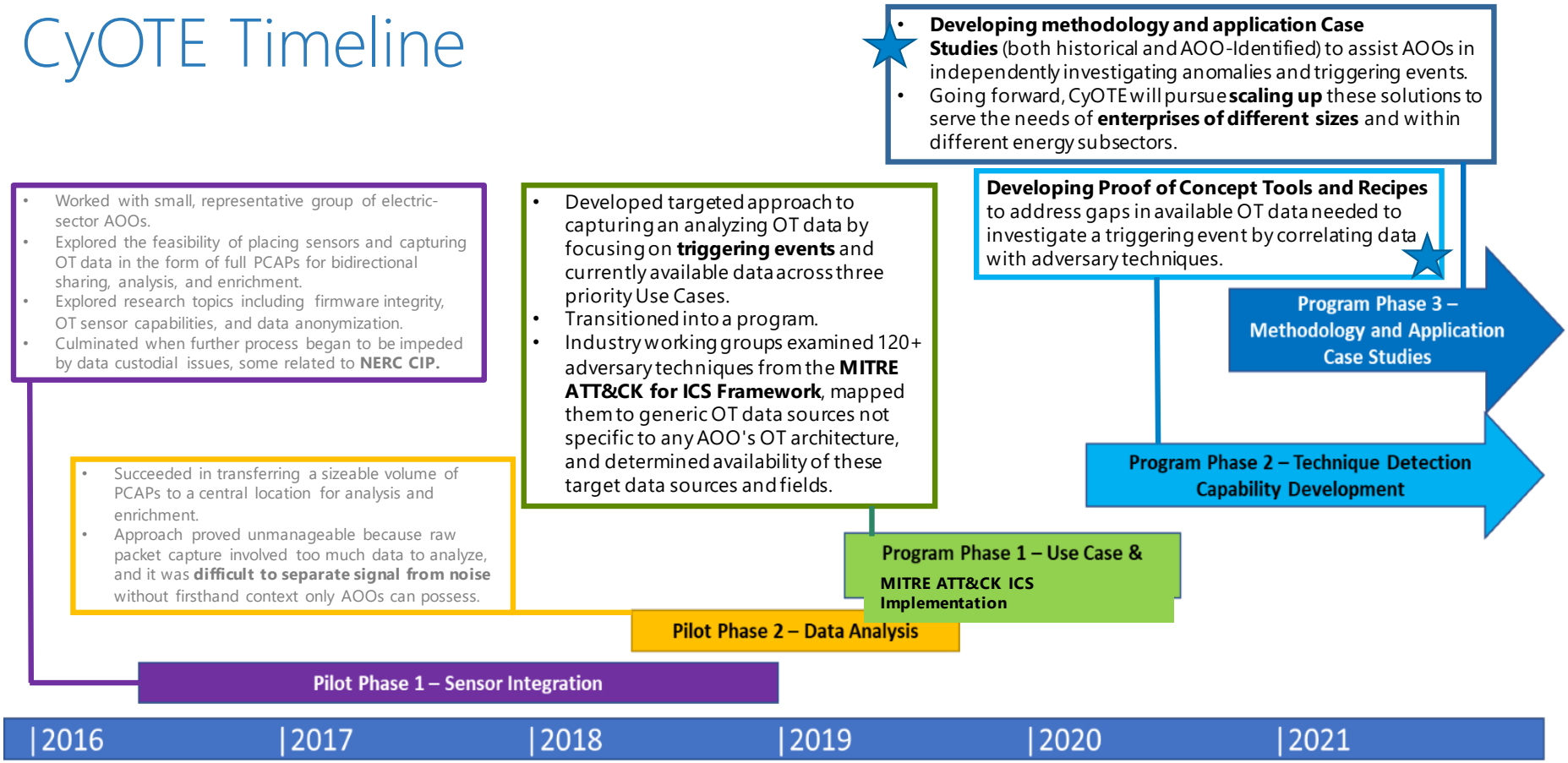
CyOTE Vision

Develop a threat identification capability for energy sector asset owners and operators to independently identify indicators of attack within their operational technology (OT) networks.

Solution

CyOTE aims to move the energy sector AOO's threat detection capability **earlier into an attack campaign**. The better understanding an asset owner has into their OT environment, the less obvious anomalies they may be able to confidently identify as either an attack technique or a non-malicious operational failure. This shifts the AOO's threat detection capability **earlier into an attack campaign** to **identify attacks with ever-decreasing impacts**.

CyOTE Timeline



Fundamental Principles

CyOTE Cybersecurity for the Operational Technology Environment

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Central Concept

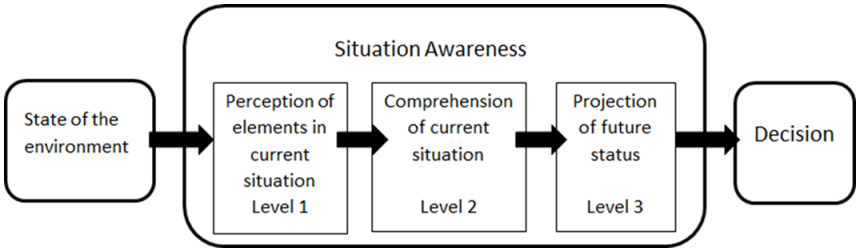
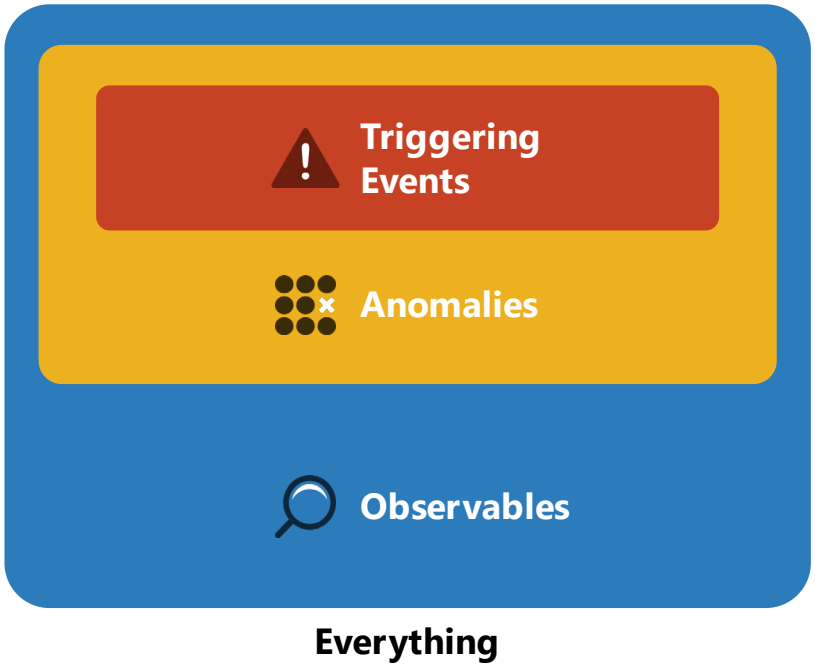


Image: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/SA_for_System_Operators.pdf

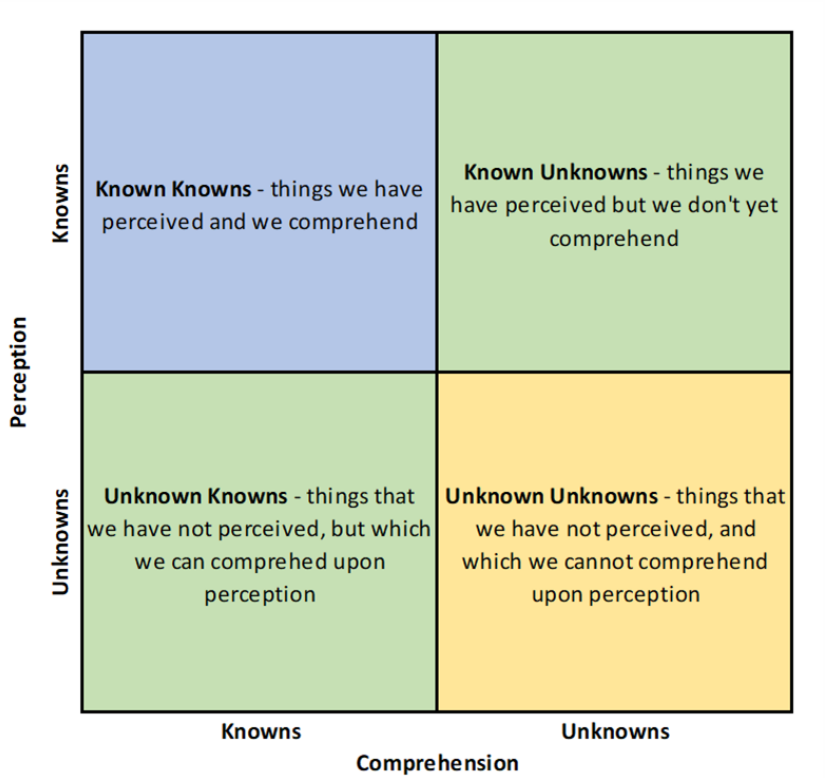
- Adapted from Endsley's 1995 Model of Situation Awareness
- Perception: individual human ability to detect an observable
- Comprehension: organizational human ability to understand an observable

Nested Mental Model of Occurrences



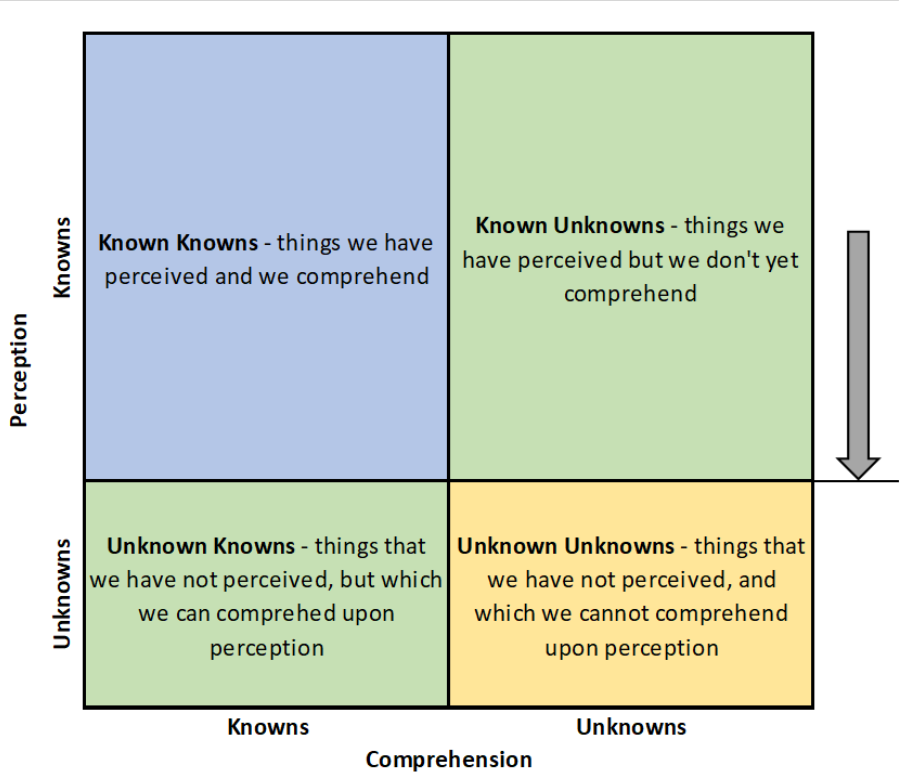
- **Observable:** an occurrence that can be perceived
- **Anomaly:** an observable different from what is expected or "normal"
- **Triggering event:** an anomaly that merits investigation

Knowns and Unknowns



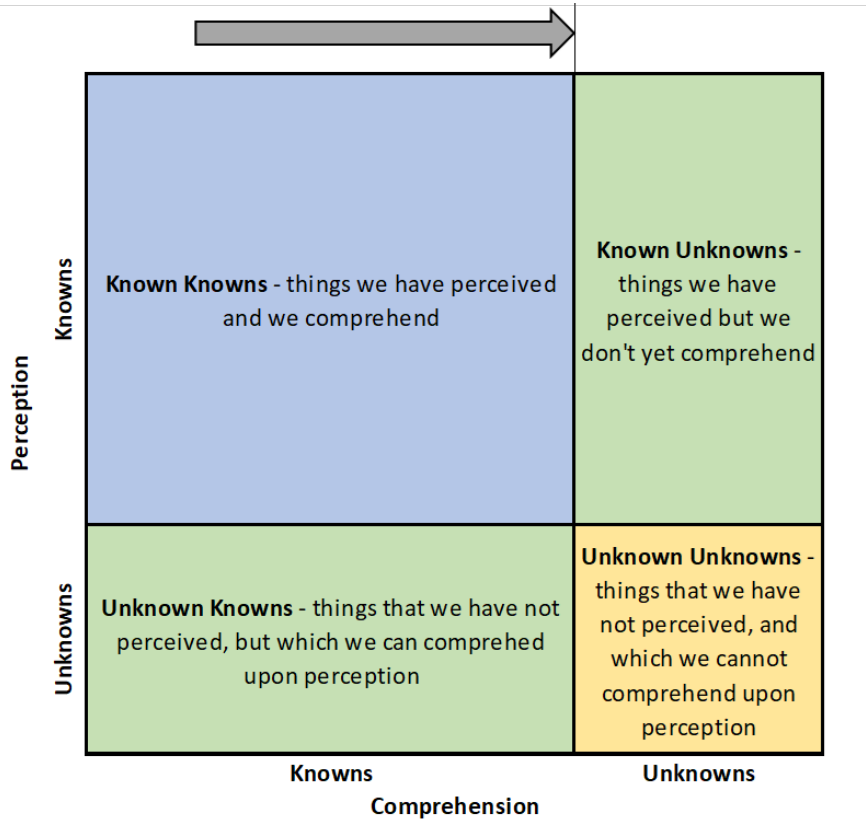
- The world is divided into Knowns and Unknowns
- Division applies to perception and to comprehension

Improving Perception



- Improving our perception shrinks the Unknown world
- Conscious visibility
- Still need to understand the newly perceived observables

Improving Comprehension



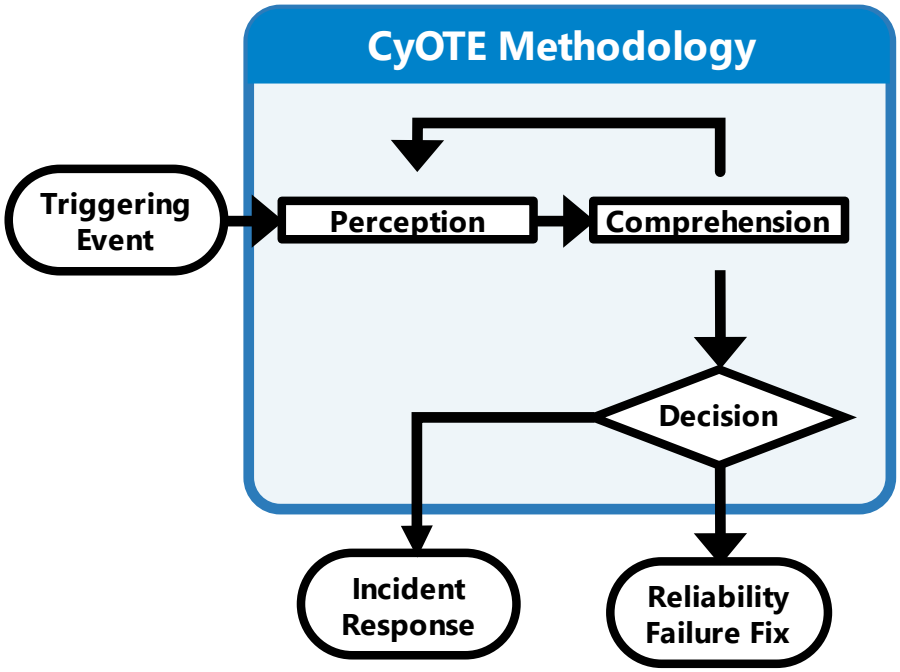
- Improving our comprehension further shrinks the unknown world
- Better idea of what not-yet-perceived observables look like (Fact Sheets and Recipes)

Organizational Capabilities

- Relationships between departments
- Energy monitoring capabilities and practices
- Capability to respond to and resolve reliability failures
- Capability to respond to and resolve cybersecurity incidents*
- Understanding of organizational risk appetite*
- Capability for organizational learning and continuous improvement
- OT instrumented visibility*

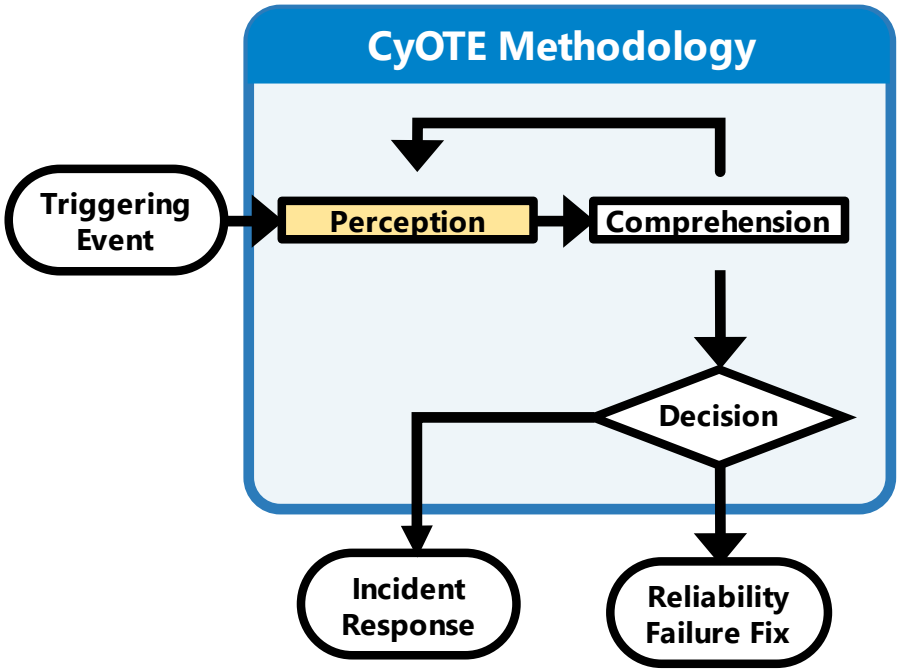
* Relates to a Cybersecurity Capability Maturity Model (C2M2) domain

CyOTE Methodology Overview



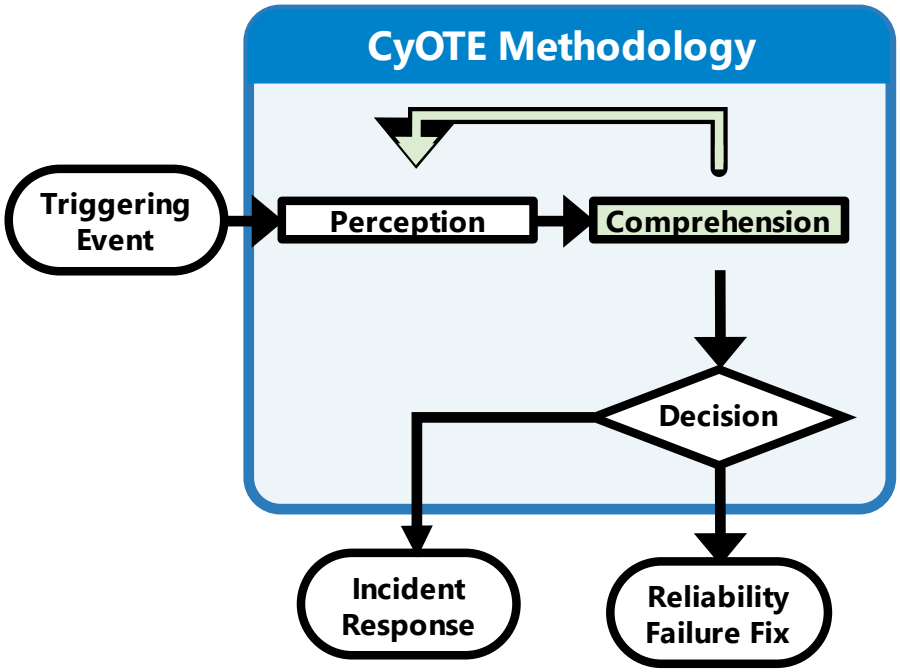
- How to understand the information you have, not get more data
- Applies concepts of perception and comprehension to a world of Knowns and Unknowns
- MITRE ATT&CK® Framework for ICS is a central part of our common lexicon
- Endpoint is making a risk-informed decision to conduct incident response or to treat as a reliability failure
- Over time, detect fainter signals sooner

Employment: Perception



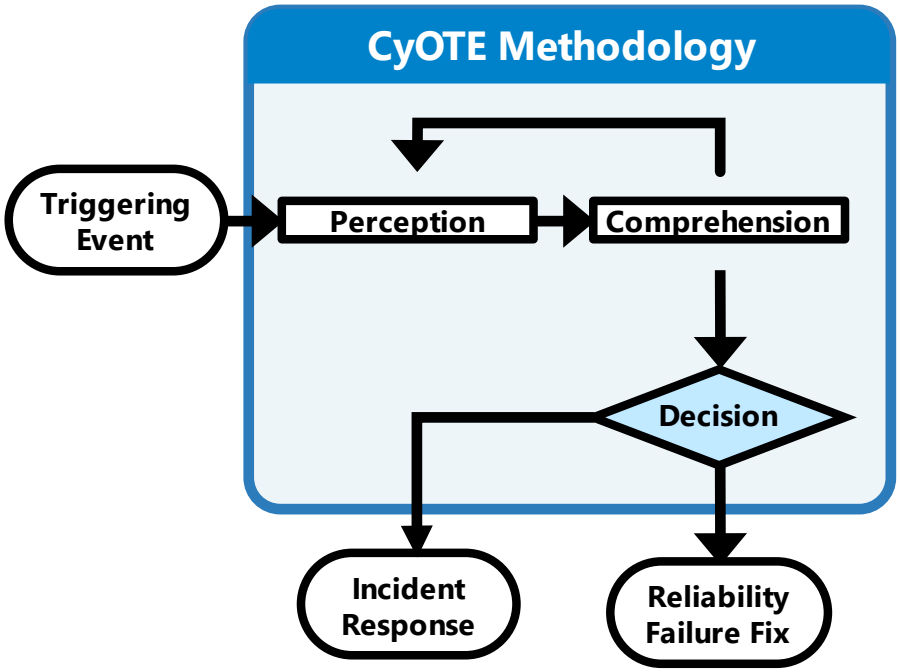
- Define **your** triggering events
- Alarms, human pattern matching, business process exceptions
- Who else needs to know, i.e. transition from individual to organizational awareness

Employment: Comprehension



- Identify and locate sources of information
- Build context: are related observables expected or not, present or not?
- How much does this resemble a known technique?
- Knowledge management and documentation
- Recursive pivots to explore related observables

Employment: Decision



- Risk-informed, binary business decision on how to resolve the situation
- Scientific method analogy
  - H_0: Reliability failure
  - H_1: Incident
  - Confidence level based on risk appetite

Stakeholder Engagement

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Impacts

- CyOTE capabilities are being used by AOOs today
  - Collaboration across business divisions and IT/OT teams to share information on where and how data is collected
  - Aligning sensor placement to allow end to end network visibility
  - Identifying technical criteria to be used in evaluating sensor products for use within OT environments
  - Leveraging Proof-of-Concept Tools and Recipes to develop capabilities for identifying indicators of attack within OT environments
  - Discussion and learning how other companies are tackling OT system monitoring challenges

Learning through Case Studies

- The CyOTE team is creating Case Studies using both historical incidents of relevance and scenarios identified with AOO partners to demonstrate where AOOs could **apply the CyOTE methodology to identify effects of malicious cyber activity** and correlate the effects to techniques.
- These Case Studies provide the opportunity to **better demonstrate how the CyOTE methodology could create broader understanding of OT environments and help** identify attack campaigns with ever-decreasing impacts.

Looking Forward

- Capabilities development for ATT&CK Framework for ICS techniques
- Outreach and transition to industry
  - Tabletops, training
  - Human performance in cybersecurity
  - Methodology decision support capability
- Research questions
- Defensive techniques framework development

Final Thoughts

- We need to **change the paradigm** for security and begin thinking of security as a holistic analysis of business operations to identify anomalies from unalterable information and conduct further investigation of any associated data.
- Correlating **operational anomalies** and observables to techniques and linking them to other anomalies provides the ability to detect attack campaigns with ever-decreasing impacts.
- Read the **full CyOTE methodology paper** at https://inl.gov/wp-content/uploads/2021/07/CyOTE-Methodology-20210625-final.pdf
- **You can help** by employing the CyOTE methodology in your organization and giving feedback
  - look for anomalies in your environments
  - identify anomalies that would trigger further investigations
  - correlate available data sources
  - associate additional anomalies
  - determine if you are in the early stages of an attack campaign

QUESTIONS and DISCUSSION

CyOTE.Program@hq.doe.gov

Sam Chanoski
Technical Relationship Manager | Cybercore Integration Center
samuel.chanoski@inl.gov
Idaho National Laboratory | Atlanta, GA

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Transmission Owner Control Center

NERC SDT Project 2021-03

Marisa Hecht, Counsel, Legal and Regulatory
RSTC Meeting
September 8, 2021

RELIABILITY | RESILIENCE | SECURITY




Background

- Under SDT Project 2016-02, the industry and the NERC Board voted to include a revision of Impact Rating Criteria (IRC) 2.12 in CIP-002-6 (May 14, 2020).
- NERC staff filed CIP-002-6 for FERC approval (June 12, 2020).
- The NERC Board voted (February 4, 2021) to withdraw the filing from FERC.
- The NERC Board directed NERC Staff, working with stakeholders, to promptly conduct further study of the need to readdress the applicability of the CIP Reliability Standards to such Control Centers to safeguard reliability, for the purpose of recommending further action to the Board.

IRC 2.12 from Withdrawn CIP-002-6

- [Each BES Cyber System, not included in Section 1 above, associated with] Each Control Center or backup Control Center, not included in the High Impact Rating, used to perform the reliability tasks of a Transmission Operator in real-time to monitor and control BES Transmission Lines with an "aggregated weighted value" exceeding 6000 according to the table below [shall be Medium Impact]. The "aggregated weighted value" for a Control Center or backup Control Center is determined by summing the "weight value per line" shown in the table below for each BES Transmission Line monitored and controlled by the Control Center or backup Control Center.

Voltage Value of a Line	Weight Value per Line
Less than 100kV (not applicable)	Not Applicable
100 kV to 199 kV	250
200kV to 200 kV	700
300 kV to 499 kV	1300
500 kV and above	0

Field Trial Design

- The SDT is proposing use of a "Field Trial" to obtain technical data from TOPs and TOs. This data will allow the SDT to provide solid justification for the proposed IRC 2.12 language or provide an updated bright line based on the new data obtained.
- The Field Trial must have sign-offs from the RSTC and the NERC Standards Committee before proceeding to the industry.
- Given the need to thoroughly vet BES reliability impacts of changes to IRC 2.12, the Field Trial is expected to be a series of questionnaires presented to industry volunteers. The initial questionnaire will allow the SDT to understand the size and scope of the participating entities. Subsequent questionnaires will require that detailed power flow analysis be performed for a variety of cyber attacks.
- The SDT is looking to start the Field Trial in January 2022.

RSTC Action Request

- The conceptual Field Trial design was presented to industry stakeholders on Sept 2, 2021. This was followed by this informational presentation to RSTC.
- The SDT is requesting the following:
  - The SDT requests RSTC member comments by September 30, 2021.
  - The SDT requests the RSTC to permit the RSTC EC to act to resolve any changes to the Field Trial design from comments received and to provide a temporary RSTC endorsement that would allow the SDT to present and gain Field Trial acceptance from the NERC SC by December 2021. As requested, the SDT can provide further updates to the RSTC as the Field Trial progresses.

Questions and Answers