

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Standards Actions

Howard Gugel, Vice President of Engineering and Standards, NERC
Board of Trustees Meeting
May 12, 2022

RELIABILITY | RESILIENCE | SECURITY



- Background

- The purpose of Project 2020-05 was to address an ambiguity in the FAC-001 and FAC-002 standards regarding the term “materially modified”
 - Added a new Requirement R6 in FAC-002-4 to require the Planning Coordinator to define what constitutes a “qualified change” for purposes of FAC-001 and FAC-002 studies
 - Replaced the phrase “materially modified” throughout the two standards with the new phrase “qualified change”, which refers to the Planning Coordinator’s definition

- Reliability Benefits
 - Address ambiguity regarding “materially modified”
 - Replace “materially modified” with “qualified change”
 - Require the Planning Coordinator to define “qualified change”
- Action
 - Adopt
 - FAC-001-4 Facility Interconnection Requirements
 - FAC-002-4 Facility Interconnection Studies

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cold Weather Standard Development Update

RELIABILITY | RESILIENCE | SECURITY



- Initial drafting complete, undergoing quality review
- Plan to ask for approval for initial posting and shorten the comment periods at May 19, 2021 Standards Committee (SC) meeting
- Planned 30 day posting following SC meeting
- Addresses all four recommendations for phase 1
 - EOP-011 contains recommendation 1j
 - EOP-012 is new standard applicable to Generator Owner and Generator Operator

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Standards Process Improvement Opportunities

RELIABILITY | RESILIENCE | SECURITY



- Existing process
- Case for change
- Action needed
- Essentials that must be maintained
- Proposed areas for improvement
- Next steps

- Governed by NERC's Rules of Procedure (RoP)
 - Appendix 3A – Standard Processes Manual (SPM)
 - Roles of Standards Committee (SC), drafting teams, and ballot body
 - Provisions for reasonable notice and opportunity for public comment
- American National Standards Institute (ANSI) accredited
- Standards and SPM approved by ballot body
- Board of Trustees (Board) and Federal Energy Regulatory Commission (FERC) must approve any revisions to RoP
- ANSI reviews revisions to SPM under its accreditation activities

- First Standards approved in 2007
- SPM has been continually modified to achieve efficiencies
- Bulk Power System (BPS) is rapidly evolving, process needs to adapt
- Lessons learned through completing over 100 projects
- Significant changes
 - 2010 – Section 321
 - 2013 – Improvements from Standards Process Improvement Group
 - 2019 – Field tests, technical documents

- Processes must be agile to address the reliability challenges of the transforming grid
 - Successes when deadlines involved
 - Lengthy otherwise

- Stakeholder input and transparency
 - Essential to Electric Reliability Organization (ERO) model
 - Stakeholder ballot of process is critical
 - Industry technical expertise is necessary
 - All can be maintained without ANSI accreditation
- Open and inclusive process for Standards development
 - Required by section 215 of Federal Power Act
 - Stakeholders propose alternative approaches and raise concerns, resulting in better Standards
 - Few Standards are challenged after submission for regulatory approval

- Board should have the authority to direct the development of Reliability Standards to address urgent reliability needs
- Streamline the Standard Authorization Request (SAR) Process
 - SARs endorsed by the Reliability and Security Technical Committee should be posted for informal comment
 - Standards Committee appoint standard drafting teams
 - “Re-acceptance” of SARs not required for informal posting
 - Technical vetting achieved by technical committee or comment period, not SC
 - SAR describe accurately the scope, technical foundation, and, where appropriate, possible solutions, not wordsmithing standard language

- Streamline balloting
 - Clarify when waivers may be used
 - Consider alternatives to usual procedures for reposting SARs during Standards drafting
 - Eliminate the requirement for a final ballot
 - Shorten formal comment period posting requirements
- NERC staff to draft interpretations
 - Still balloted by industry
 - Still presented to Board and regulatory authorities
- Streamline SC processes
 - Expand role of SC Executive Committee
- Streamline Standard Drafting Team responsibilities
- Update Standards naming convention

- Convene stakeholder group to consider and provide feedback
- Post recommendations as modified for industry comment
- Present to Board by December 2022

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Critical Infrastructure Protection Board Resolution Update

RELIABILITY | RESILIENCE | SECURITY



- Standards
 - Work continues on CIP-003
 - Drafting team is considering comments and preparing changes
- Low Impact Criteria Review team
 - Work continues on white paper
 - Identification of risks and management strategies
 - Input to be solicited (Q2 target)

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Supply Chain Effectiveness – ERO Enterprise

Lonnie J Ratliff, Senior Manager, Cyber and Physical Security Assurance
Board of Trustees Meeting
May 12, 2022

RELIABILITY | RESILIENCE | SECURITY



- December 2021 – NERC committed to plan to measure the effectiveness of the Supply Chain Standards
 - Project Scope
 - Surveys on supply chain awareness
 - Compiling statistics on identified key risk indicators.
 - Software validation discrepancies
 - Information on vendors that support supply chain frameworks
 - Entities who performed vendor risk assessments in the prior 24 months
 - Analysis of vendor vulnerability and cyber security incident notifications.
 - Collaboration with Supply Chain Working Group (SCWG)
 - ERO Enterprise observations

- Industry has latitude to define “vendor”
- Periodicity of risk review, narrow scope and applicability
- Trends
 - Industry comment – “..non-prescriptive Standards hard to implement.”
 - Emergency and/or expedited procurements are common
 - Many questions/concerns around “vendor” and “procurement”
- ERO Enterprise Next Steps
 - Collaborate with SCWG and Standards on results

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Supply Chain Working Group

Tony Eddleman, NPPD and SCWG Chair
Board of Trustees Meeting
May 12, 2022

RELIABILITY | RESILIENCE | SECURITY



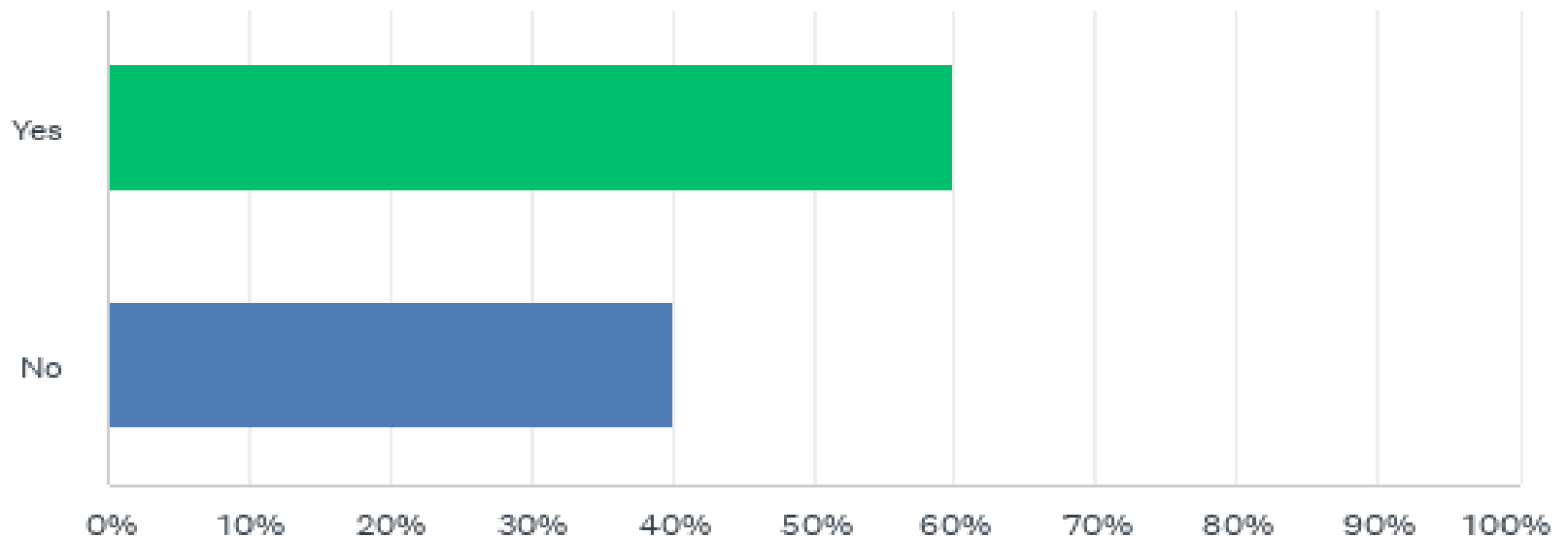
- The NERC Supply Chain Risk Management (SCRM) Reliability Standards are:
 - CIP-013-1; CIP-005-6 (parts 2.4 and 2.5); and CIP-010-3 (part 1.6)
 - Initially effective on October 1, 2020
 - CIP-013-2, CIP-005-7 and CIP-010-4 to be effective on October 1, 2022
- Supply Chain Working Group (SCWG) developed the Supply Chain Effectiveness Survey and provided it to the Reliability and Security Technical Committee (RSTC) at the September 2021 meeting
 - Voluntary survey sent to Registered Entity compliance contacts on October 12, 2021 – survey closed on November 30, 2021

- The results of this survey have been reviewed, key takeaways and conclusions developed by the SCWG
 - Results provided to the RSTC at the March 8, 2021 meeting

- 201 total responses
 - Eleven (11) responders did not select any responses nor provide any comments
 - The survey was sent to approximately 900 compliance contacts at Registered Entities and requested their voluntary response
- Survey responses came from the United States, Canada, and Mexico
 - Responses also came from all six NERC Regions
- Majority of 190 responses, 60% (114), selected NERC Supply Chain Risk Management (SCRM) Reliability Standards applicable to them as Registered Entities
- Responders provided very good comments which have been incorporated into key takeaways and conclusions
- Survey was conducted through SurveyMonkey

Q2: Are the NERC Supply Chain Risk Management (SCRM) Reliability Standards applicable to you as a registered entity?

- Answered: 190 Skipped: 11



Q2: Are the NERC Supply Chain Risk Management (SCRM) Reliability Standards applicable to you as a registered entity?

- Answered: 190 Skipped: 11

ANSWER CHOICES	RESPONSES	
Yes	60.00%	114
No	40.00%	76
TOTAL		190

SCRM Reliability Standards are not applicable to you as a registered entity:

Q3: Are you applying the SCRM principles from the SCRM standards to your operational, business and/or contract language?

- Answered: 64 Skipped: 137

ANSWER CHOICES	RESPONSES	
Yes	37.50%	24
No	62.50%	40
TOTAL		64

- Of the 64 respondents that indicate the SCRM **requirements are not applicable** to their entity, 24 responders are applying the SCRM principles from the SCRM standards to their operational, business, and/or contract language
 - Standards have been a good basis to determine what is needed if entity was to have a formal NERC program.
 - **Conclusion:** The SCRM requirements are relatively new, but some entities that don't have compliance requirements are using the requirements to develop programs

- Of the 60% of respondents (114) that the SCRM requirements are applicable to them, over half of the respondents are applying SCRM principles to some degree to cyber assets not in scope of the requirements
 - Once the supply chain process is more mature and the larger implications of the standard are better understood, some will evaluate implementing the SCRM principles in other areas
 - **Conclusion:** Entities are generally working towards applying the SCRM requirements to other systems

- 61% of respondents felt the requirements are clear but have questions about compliance evidence
 - Compliance ambiguity is a significant concern for respondents
 - **Conclusion:** Entities have some questions about the requirements but are more concerned about what to expect from an audit
- 59% of respondents indicate they have a clear understanding of what constitutes a violation
 - **Conclusion:** Entities are relatively unclear about what would be deemed a noncompliance
- Two-thirds of respondents do not believe there are gaps in the requirements
 - **Conclusion:** Entities are hesitant to say there are gaps in the standards as they would like stability and answers before more changes are made

- 84% of respondents have not reached out to the ERO with questions and concerns
 - **Conclusion:** While a few entities reported positive interactions with regions, most entities are getting answers through workshops, guidance, consultants or other non-personal interactions
- 45% of respondents indicated vendors are reasonably supportive in responding to requests on risk assessments
 - 19% indicated vendors are resistive
 - **Conclusion:** Recognize that vendors receive SCRM questionnaires from multiple clients, in varied formats, across multiple industries. Better consistency and effectiveness can be achieved through industry convergence on a standard questionnaire

- 51% indicated vendors don't provide enough information to determine risk
 - **Conclusion:** Registered entities should expect to invest more time in vetting questionnaire responses; not all vendors have the knowledge to respond properly
- 72% of respondents support vendors providing a Software Bill of Material (SBoMs)
 - **Conclusion:** Entities support the concept of SBOMs, but are concerned about having the resources to conduct analysis; they would like to see a consistent format that provides information from the data
- 59% of respondents indicated CIP-013 has not enabled them to identify previously unknown risks
 - **Conclusion:** People have identified some risks and have had some positive internal actions, but these are limited, which could be due to limited experience with the standard

- 70% of respondents indicate they have not implemented new supply chain mitigations
 - **Conclusion:** People have limited experience with the standard, so few are implementing new mitigations. Some are implementing new contract terms
- 65% of respondents indicate they have not implemented compensating security measures other than specification and procurement activities
 - **Conclusion:** People appear to be putting analysis tools and contract terms in place for security measures, but other additional security measures have not been required

- 64% of respondents indicate they gather the information and perform the risk assessment while the other respondents indicate some involvement of contracts for services
 - **Conclusion:** The majority of responders are gathering information and conducting the risk assessments themselves, while others are contracting out some or all of the process

- 63% of respondents indicate they have added new or updated contract language to procurements
 - **Conclusion:** The majority of responders are adding attachments to current contracts and are updating contracts as they are renewed
- 60% of respondents indicate no existing contracts were renegotiated, 1% indicate all were renegotiated while the other respondents are somewhere between
 - **Conclusion:** Responders are not renegotiating all contracts. Most are not updating existing contracts, but some are updating or adding attachments as opportunities arise

- For vendors being agreeable to renegotiating existing contracts - 69% of respondents indicated “not applicable” or did not attempt to renegotiate existing contracts
 - **Conclusion:** The majority of responders are not renegotiating contracts. Approximately one third of responders that are subject to the standard responded that vendors were agreeable to renegotiating (updating, adding attachments) when responders are requesting it

- The SCWG wanted to understand the impact of the new requirements on entities, so SCWG asked for two percentages:
 - Percentage of CIP Compliance Program resources dedicated to SCRM compliance
 - Percentage growth of CIP Compliance Program because of implementing SCRM compliance
 - And, asked for any comments from the entities
- 57 entities responded by providing percentages or comments and some provided both
- Average of 22.5% (49 responses) of CIP Compliance Program resources dedicated to SCRM compliance
- Average of 9.15% (49 responses) growth of CIP Compliance Program because of implementing SCRM compliance

- A concerning observation from the survey is entities are more apt to pull CIP staff from other areas to address SCRM processes than add additional resources. This may further deplete strained resources in the other CIP areas and continue to increase compliance fatigue. Finding trained, experienced, staff willing to tie their career to compliance is getting even more difficult
- Sobering quote: “We all cringe when we know we have a to make a purchase.”
- Conclusion: SCRM is requiring significant resources to implement and stealing resources from other CIP programs. The resource drain is both on entities and vendors

- Supply Chain is a global issue for all critical infrastructure and not just electric utilities
 - The vendor is held harmless, and utilities are held accountable for the vendor's actions which utilities have no control over. Simply buying a product or not buying a product from a vendor may not influence their security practices. The vendor must be held accountable and not the consumer using the product
- Industry is asking for a certification program
 - Third-party certification recognized by NERC for example, SOC2 type 2 would simplify the compliance process and address non-cyber security risks (financial, geopolitical) through appropriate channels and/or specialists

- Acknowledge that SCRM requirements will drive up the cost of goods and services from vendors that choose to continue to supply our industry. The nuclear industry provides examples.
- The term "vendor" is not clear for some Entities

- Entities are gradually expanding Supply Chain Risk Management principles to Cyber Assets outside compliance requirements
- Entities have some questions about the requirements but are more concerned about what to expect from an audit
- Vendors are working with the Electric Industry, but the solution needs to be bigger than the Electric Industry
 - Electric Industry has developed a Critical Infrastructure leading program
- Entity work on Supply Chain Risk Management is taking significant resources and vendors are also being impacted
 - Entities are more apt to pull CIP staff from other areas to address SCRM processes than add additional resources

- Industry work on Supply Chain Risk Management is a journey and not a quick fix
 - Requirements have and will increase costs



Questions and Answers

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

2022 Summer Reliability Assessment Preview

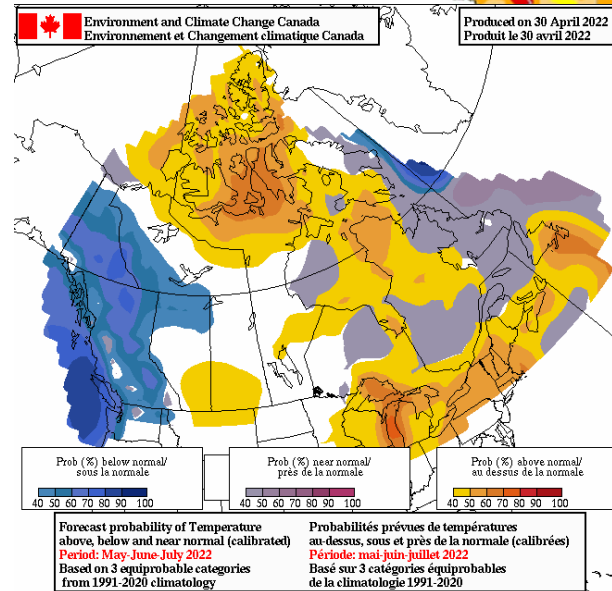
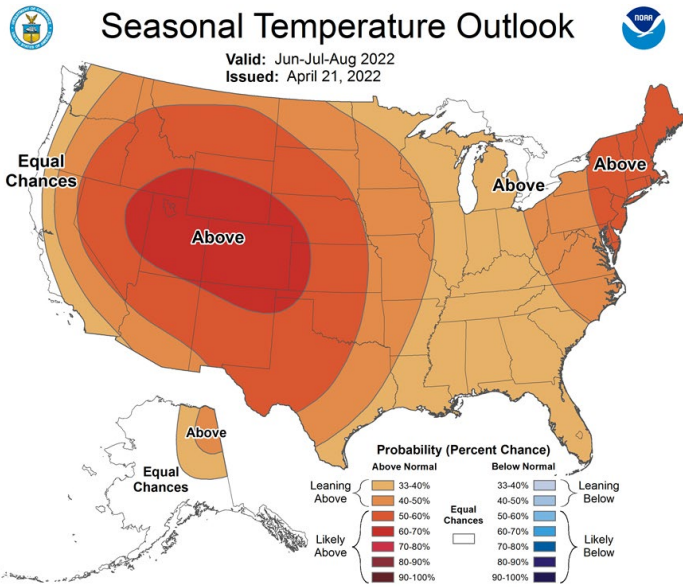
Status and Preliminary Findings

John Moura, Director, Reliability Assessment and Performance Analysis
Board of Trustees Meeting
May 12, 2022

RELIABILITY | RESILIENCE | SECURITY

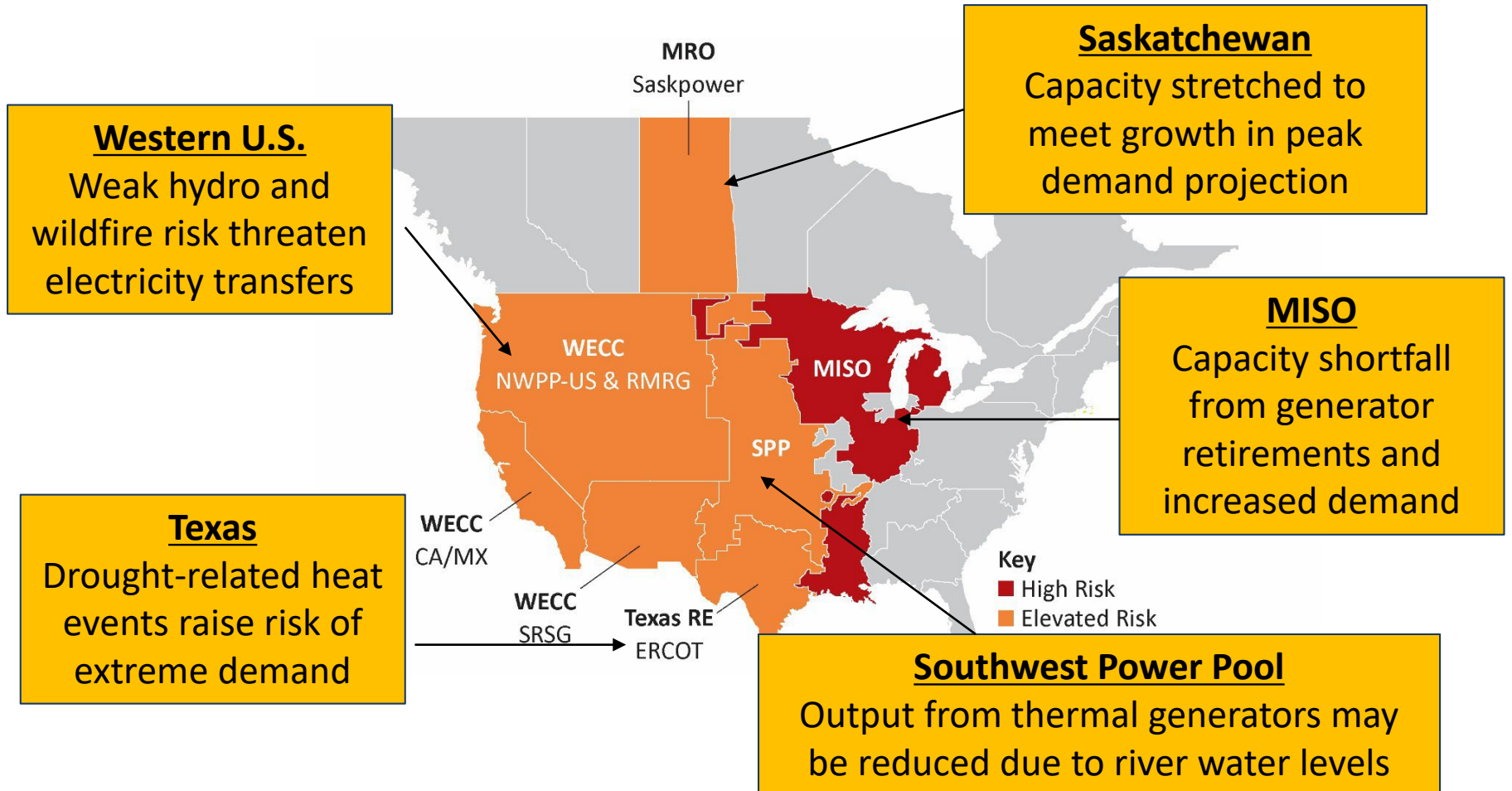


- Drought conditions create heightened reliability risks
- High temperatures are key driver of peak electricity demand

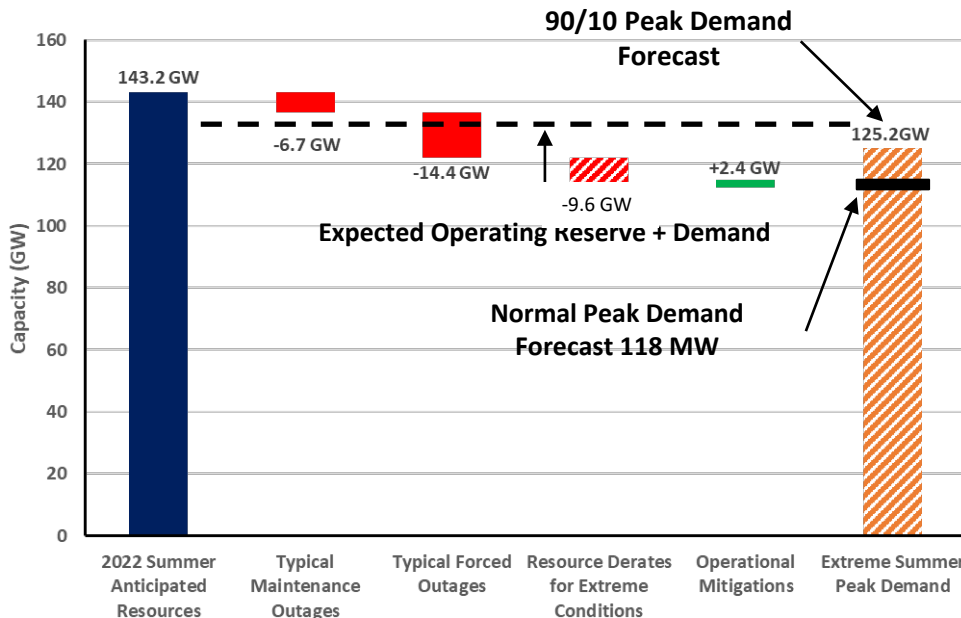
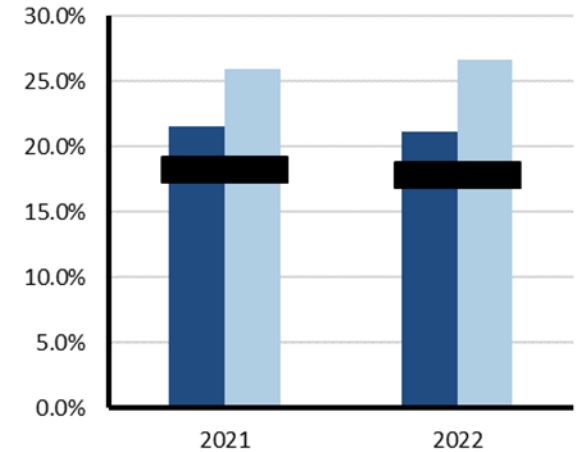


3-Month Temperature Outlook (U.S. National Weather Service, Environment and Climate Change Canada) and April North American Drought Monitor (NADM)

- Parts of North America are at **elevated** or **high** risk of energy shortfalls during peak summer conditions

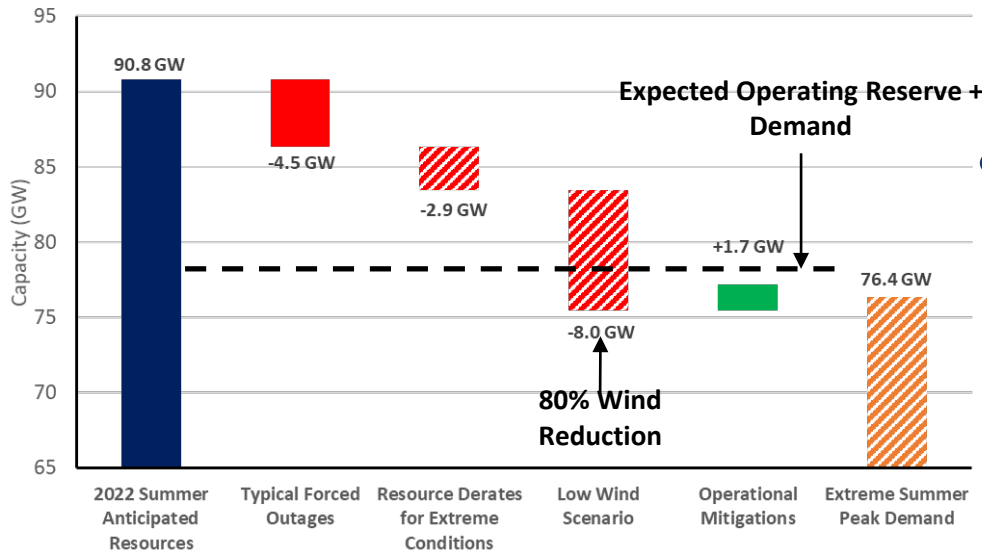
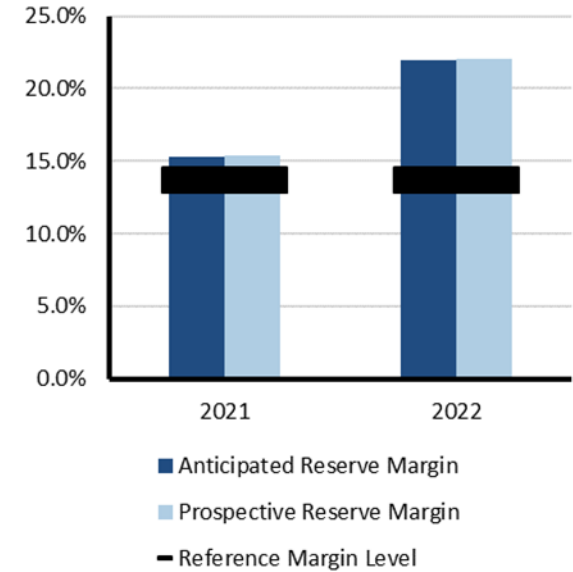


- Generation capacity declined 2.3% since 2021 resulting in lower reserve margin
- North and central areas at risk of reserve shortfall in extreme temperatures, high generation outages, or low wind



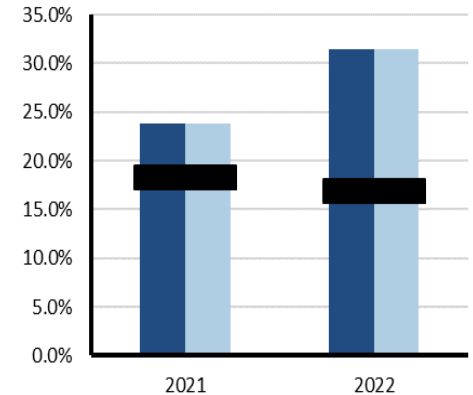
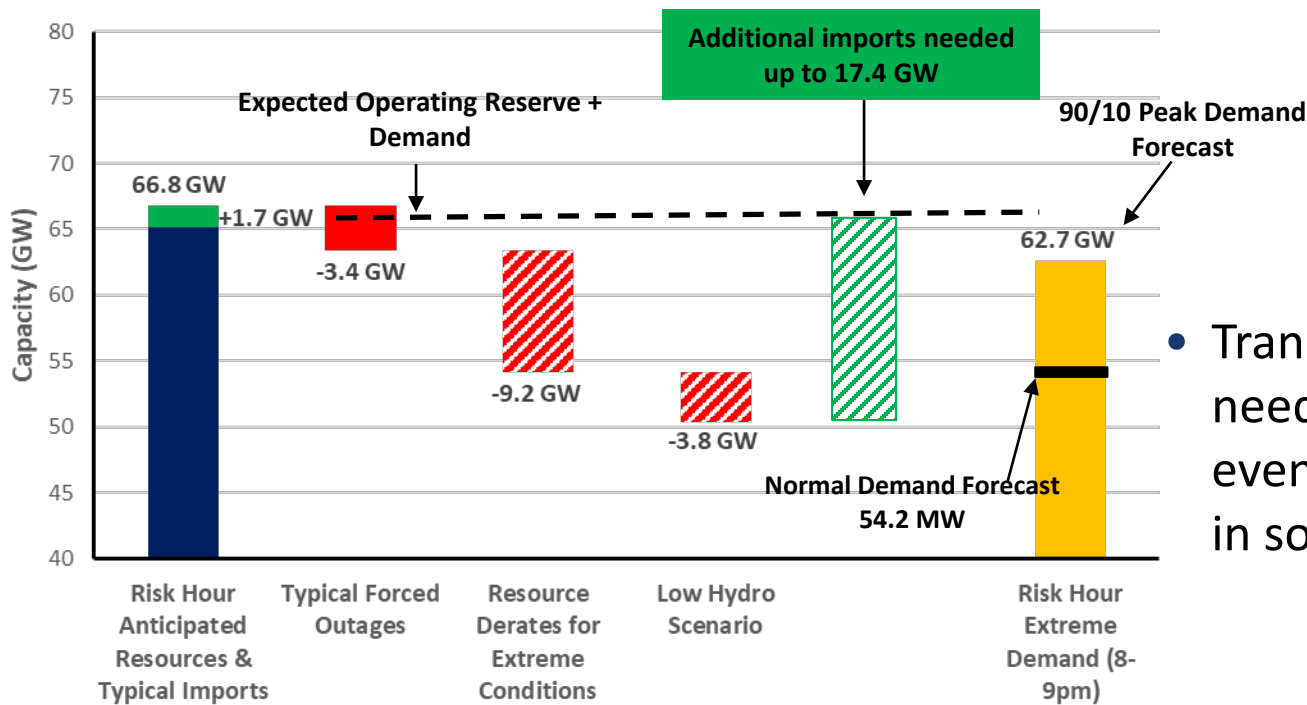
- Some risk of insufficient operating reserves at normal peak demand

- Extreme drought in Texas can cause wide-area heat events and extreme demand
- Extreme demand, low wind, and high thermal generation outages could lead to emergency procedures and load shedding



- Transmission projects needed to reliably integrate new resources being monitored for delays

- Output from hydro generators affected by widespread drought and low snowpack
- Risk of insufficient supply of electricity for transfer to support system balancing during extreme conditions



CAMX Reserve Margins

- Transfers into CAMX are needed in afternoon and evening to offset decline in solar PV output

- Supply chain issues and commissioning challenges on new resource and transmission projects
- Electricity and other critical infrastructure sectors face added cyber security threats in current geopolitical situation
- Unexpected tripping of solar photovoltaic (PV) resources during grid disturbances continues to be a reliability concern
- Active late-summer wildfire season anticipated in Western U.S. and Canada

- The SRA report was reviewed by the NERC Reliability and Security Technical Committee (RSTC) in April
- Risk analysis is based on inputs from probabilistic studies and deterministic risk scenarios
- NERC Staff is preparing the report for RSTC endorsement and NERC Senior Leadership approval

Date	Milestone
Early May	Report sent to RSTC for Endorsement
May 10	Report sent to NERC Executive Leaders
May 12	Final Report sent to NERC Board of Trustees
May 17	Pre-publication Report sent to ERO Executive Committee and MRC
May 18	Report Release



Questions and Answers

- NERC's Summer Reliability Assessment (SRA) examines potential regional resource deficiencies and operating reliability concerns
 - Describes industry preparations to manage seasonal risks
- Developed with the Reliability Assessment Subcommittee (RAS) and reviewed by the Reliability & Security Technical Committee



NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

2022 State of Reliability Report

Preview

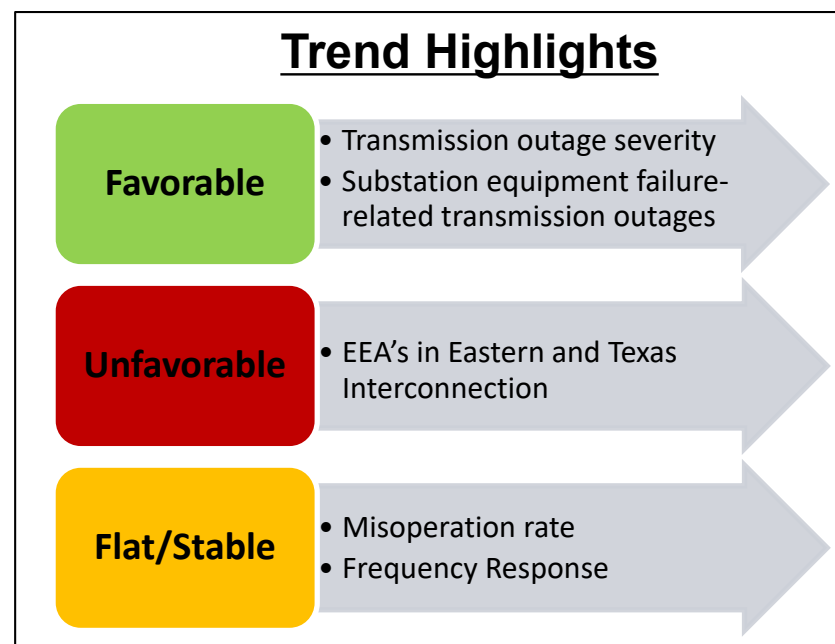
John Moura, Director of Reliability Assessment and Performance Analysis
Board of Trustees Meeting
May 12, 2022

RELIABILITY | RESILIENCE | SECURITY



- Provide objective, credible, and concise information to policy makers, industry leaders, and the NERC Board of Trustees on issues affecting the reliability and resilience of the North American bulk power system (BPS)
 - Identify system performance trends and emerging reliability risks
 - Determine the relative health of the interconnected system
 - Measure the success of mitigation activities deployed
- Evaluates the 2021 Operating Year and Historical Trends

- Extreme cold weather led to largest load-shedding event across South Central U.S. and Texas
 - Increased reliance on natural gas generation, generator freezing, higher than expected demand, uncertainty of renewable energy production
- Dramatic increase in the amount of unserved energy and operator-initiated load shed
 - Hurricane Ida, Northwest Heat Dome, Western Wildfires, December Tornadoes
- Cybersecurity threat landscape relentlessly evolves and presents new challenges to the electricity industry
- Multiple loss of solar events in Texas and California continue to impact the grid reliability



4,585,939 GWh

2021 Actual Energy

1,056.98 GW

2021 Summer Peak Capacity

511,099 mi

Total Transmission Circuit Miles > 100kV

5,966

Number of Conventional Generating Units > 20MW

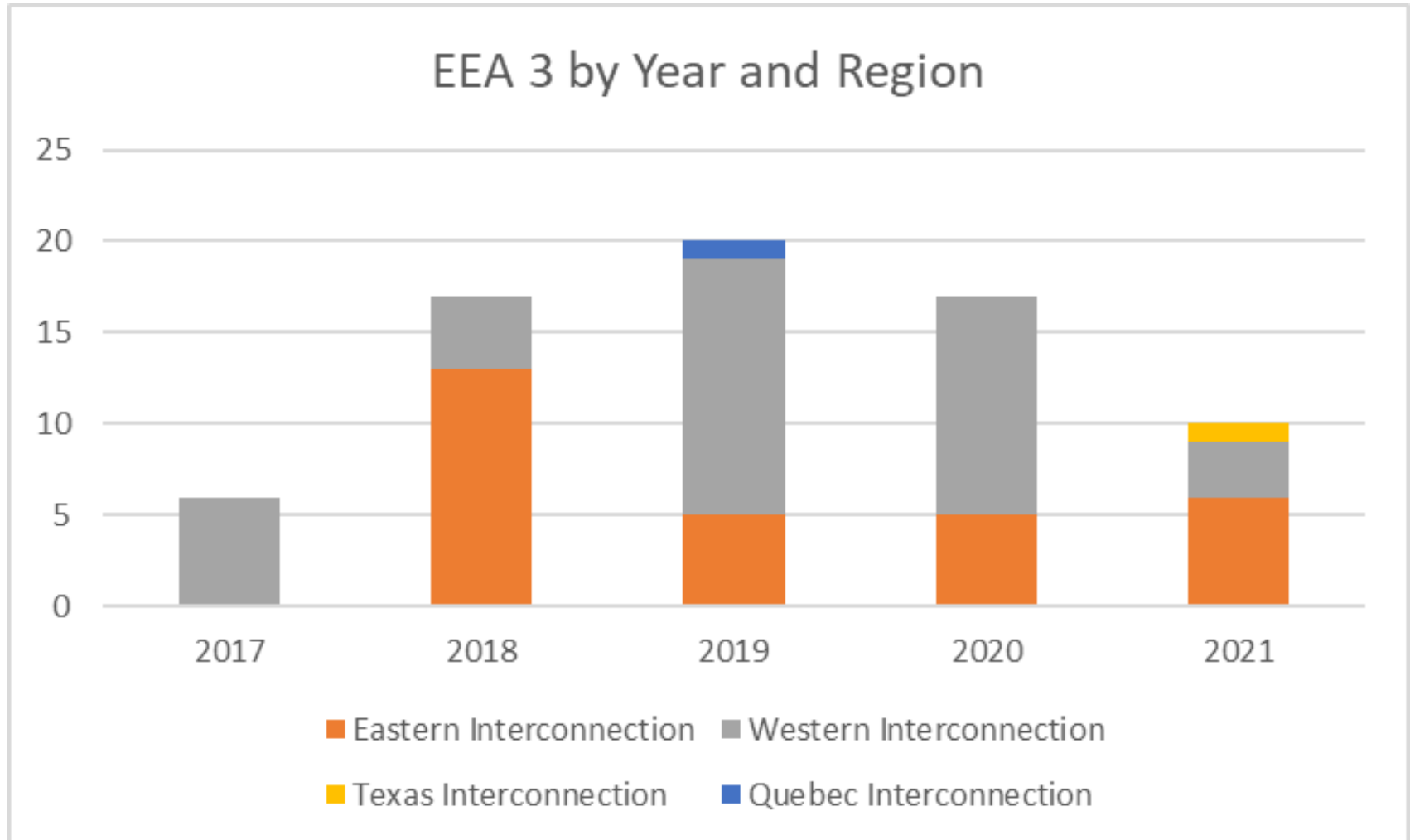
99.19%

Time with no operator-initiated firm load shedding associated with EEA-3 (1,015.5 GWh energy unserved or 0.022% of total energy served)

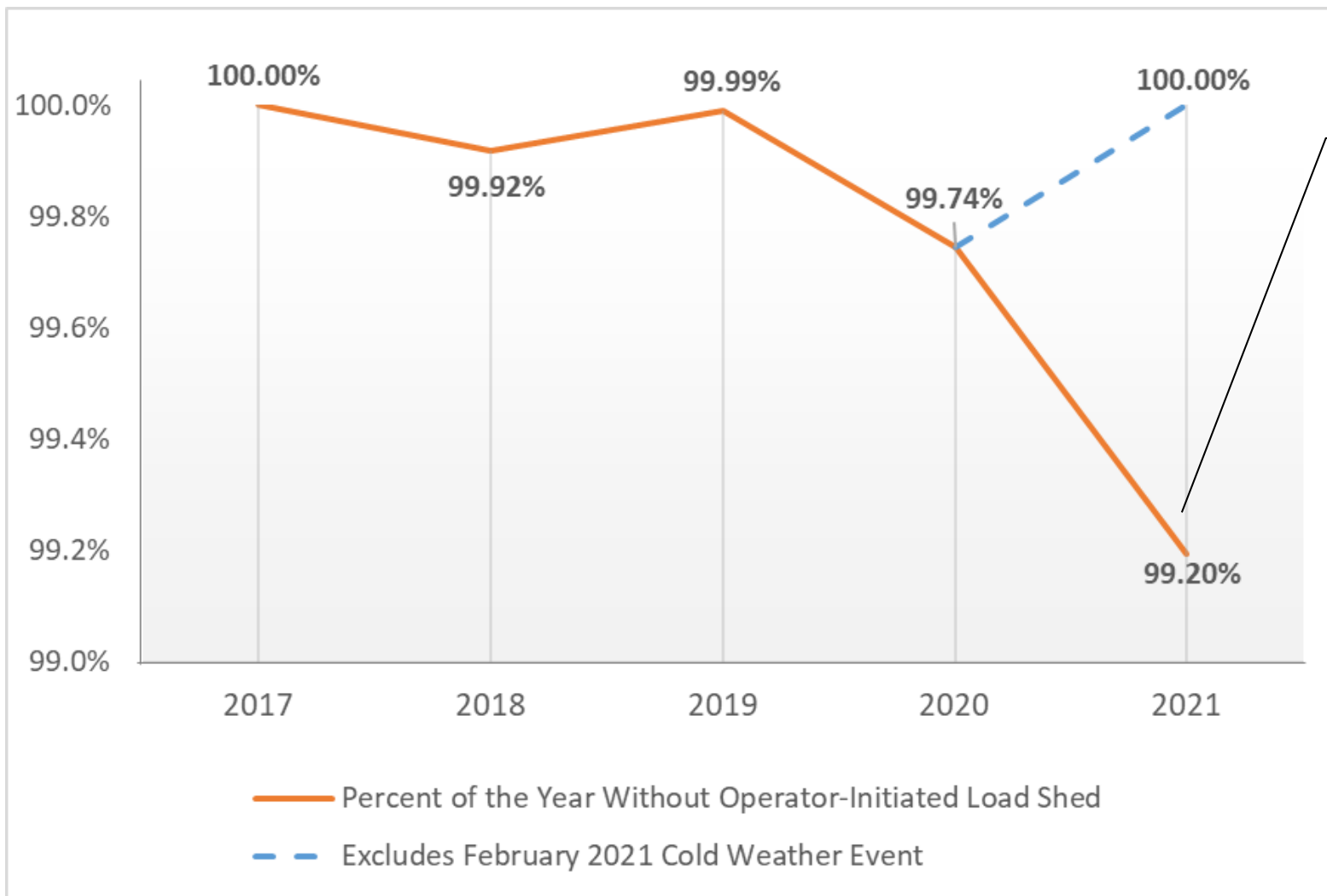
0

Category 3, 4, or 5 Events (non-weather related)



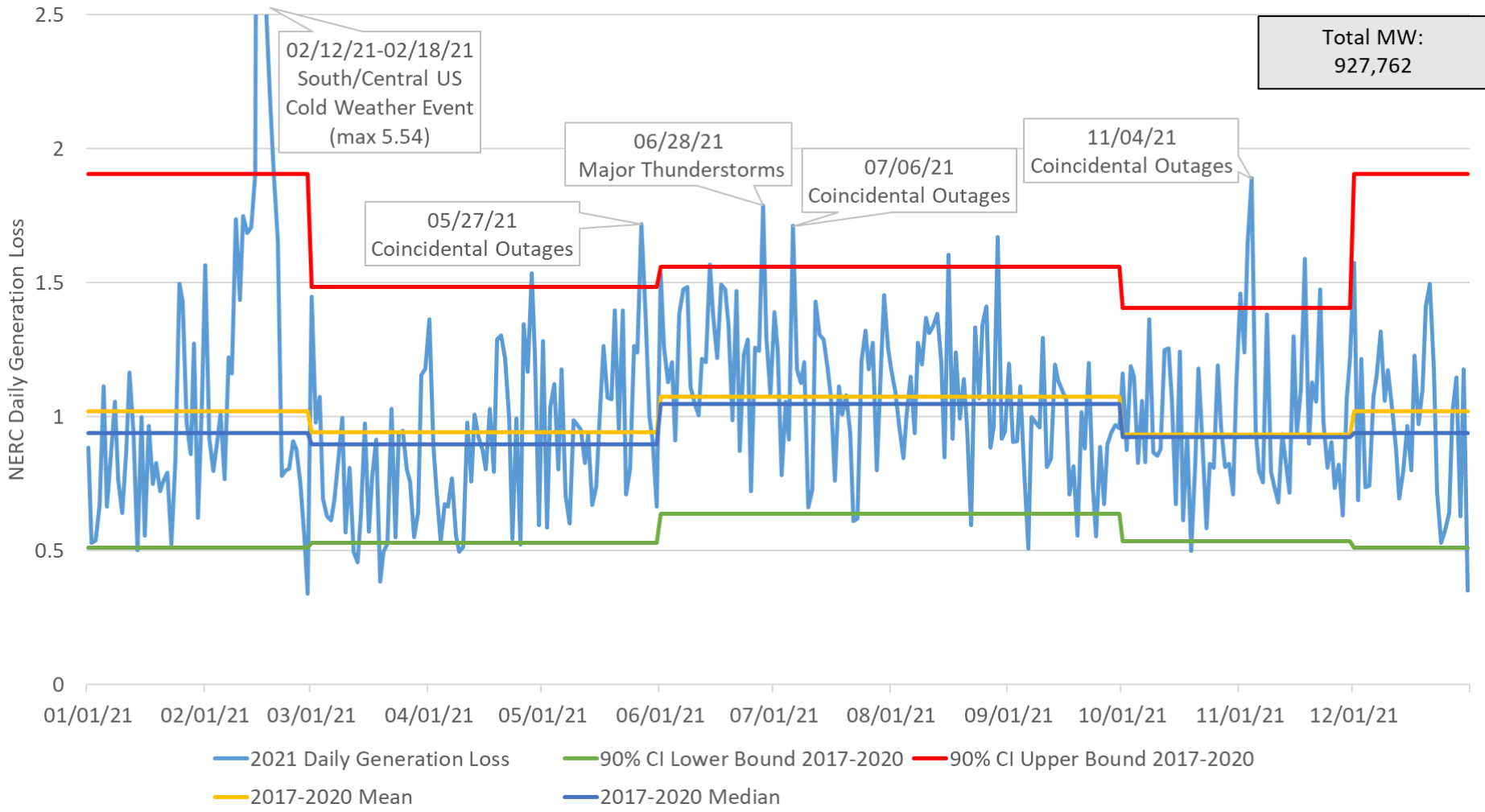


Hours Without Operator-Initiated Firm Load Shed (%/year)

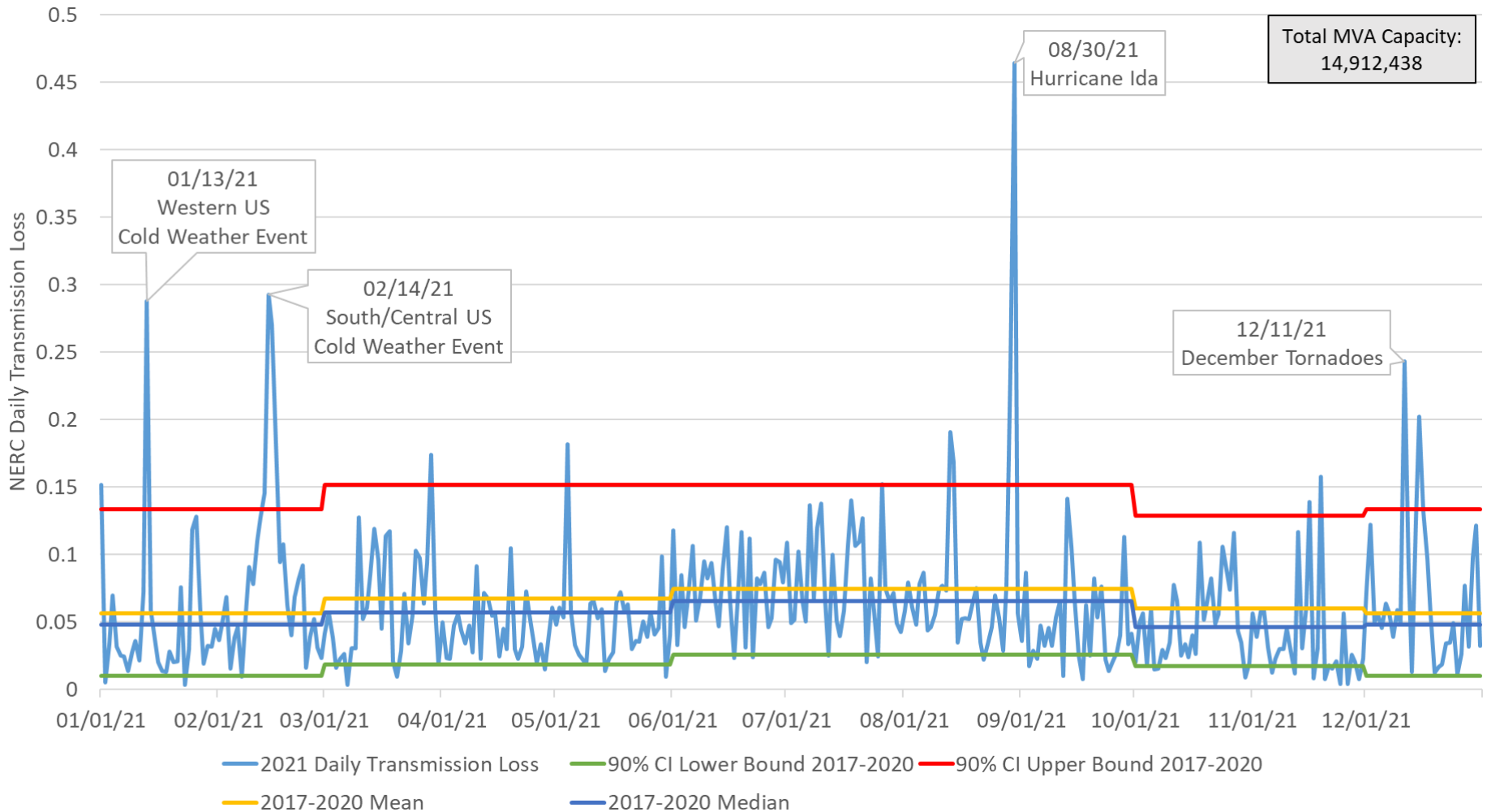


2021

- 10 EEA-3 Alerts
- 1,015 GWh unserved
- Occurred February

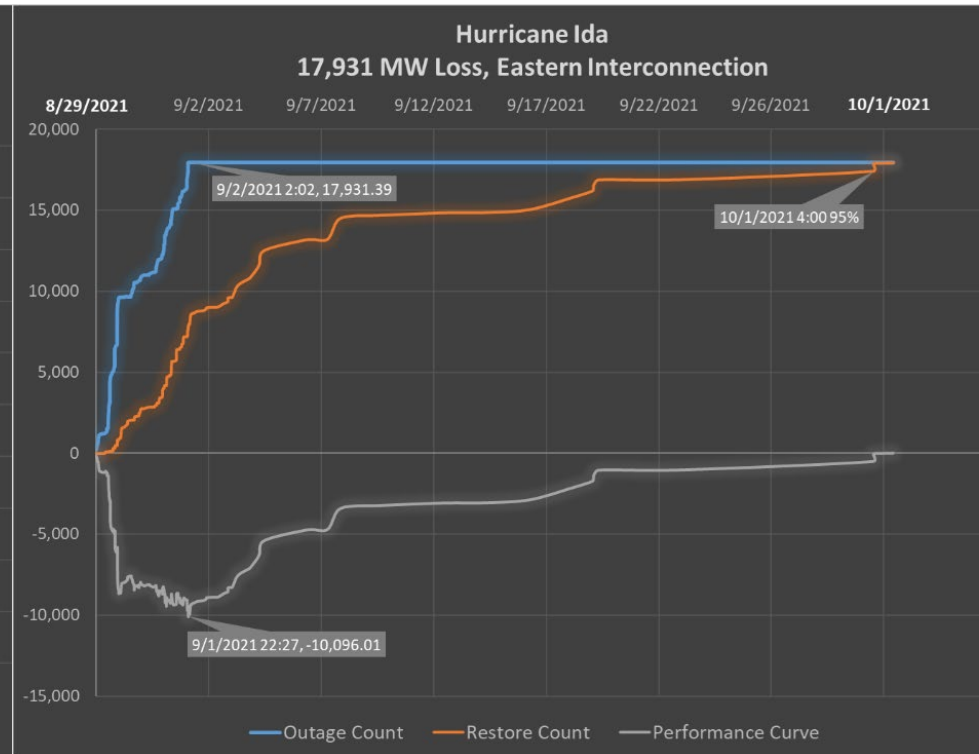
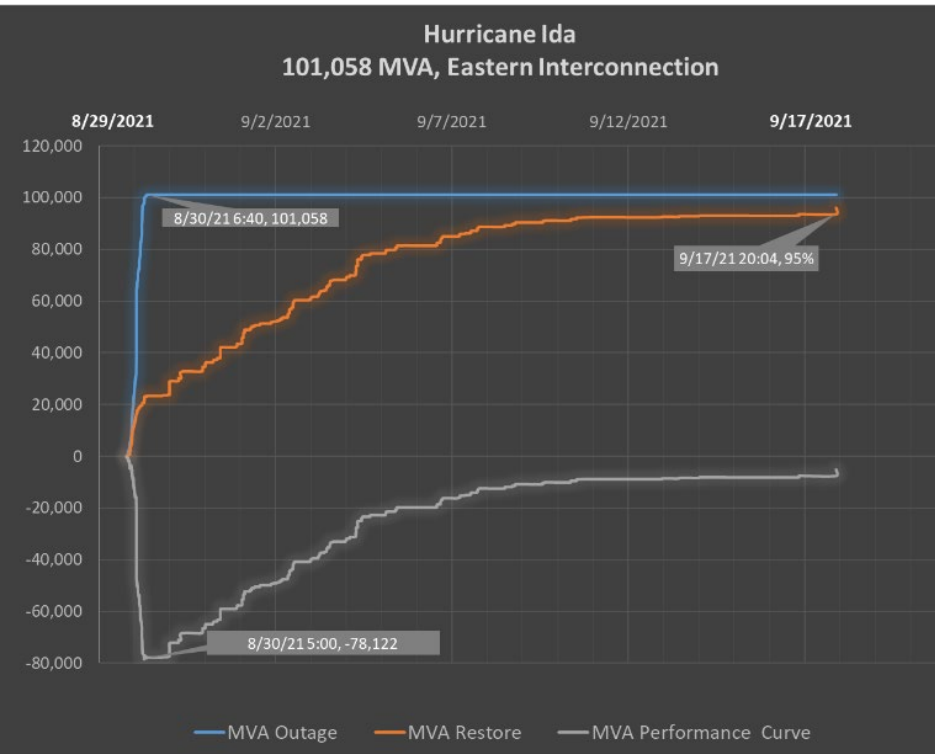


Leading Cause of Outages on Extreme Days:
1) Fuel Systems, 2) Economics 3) Catastrophe



Transmission

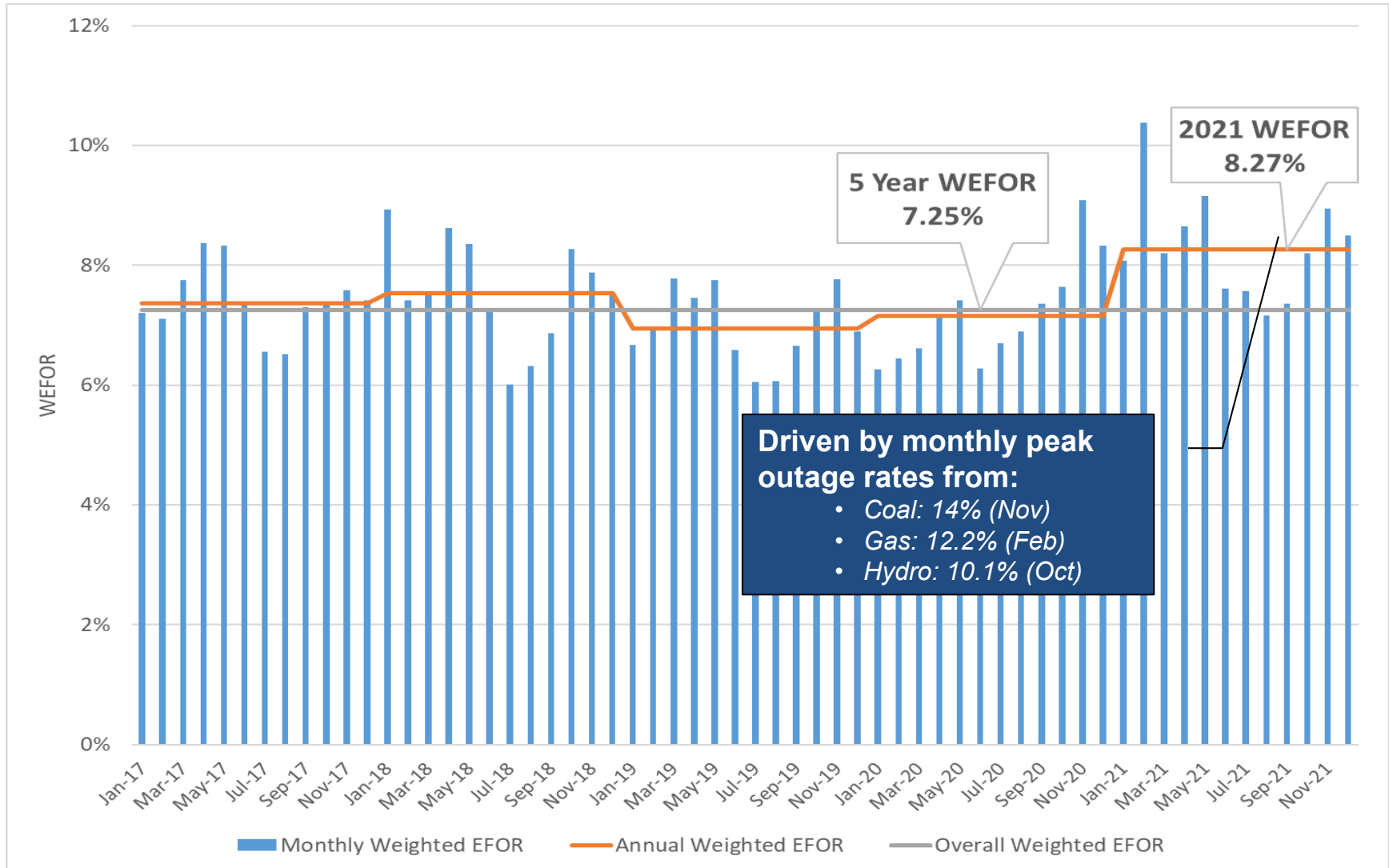
Generation



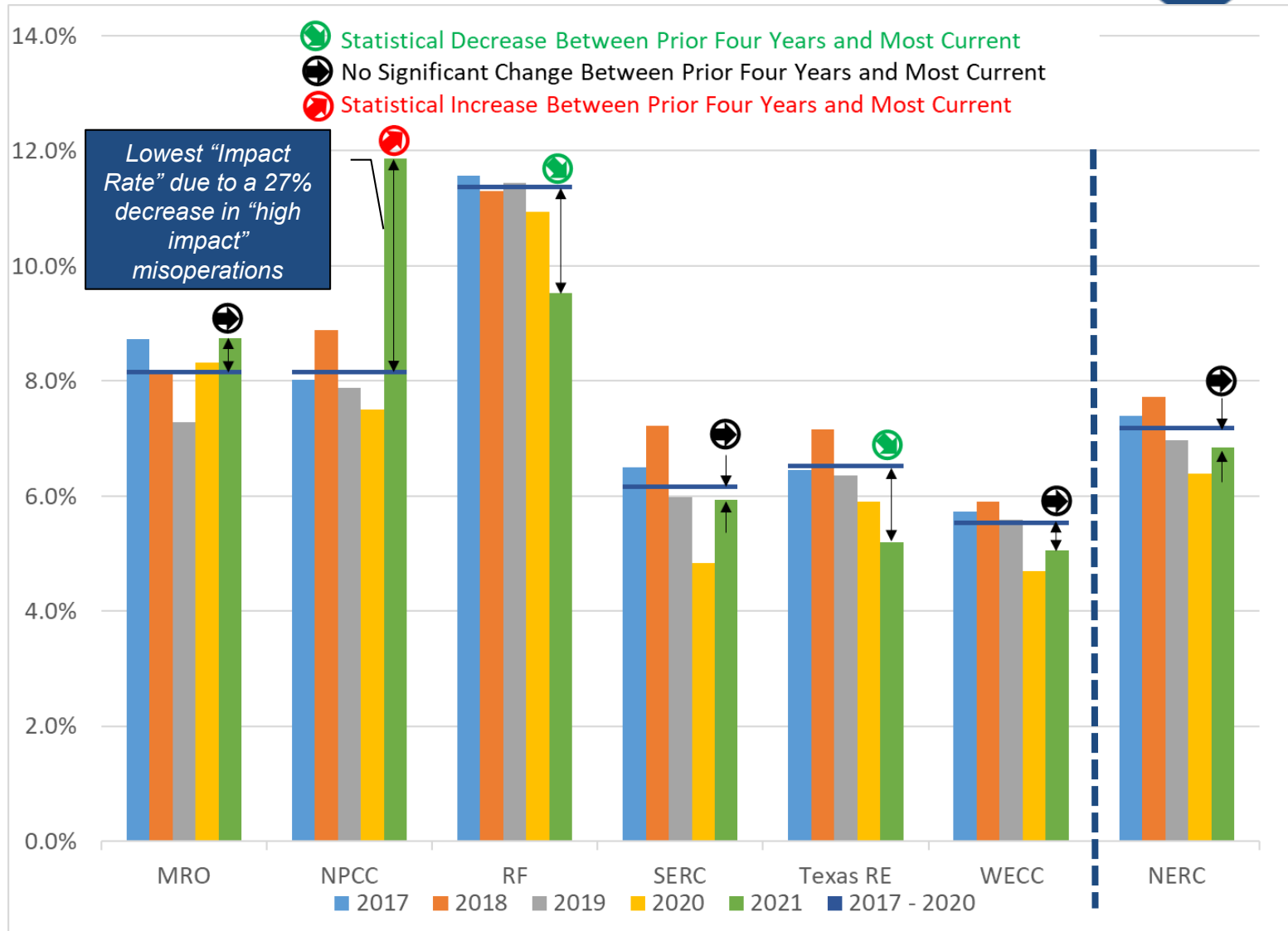
Peak Outage: 101,058 MVA
Time to first restoration: 47 minutes
95% restoration: 459 hours
Total restoration: 124 days

Peak Outage: 17,931 MW
Time to first restoration: 9.5 hours
95% restoration: 792 hours
Total restoration: 34 days

Generation Forced Outage Rate: Conventional Fleet



Protection System Misoperations





Supply Chain



**Geopolitical
Threats**



Ransomware



**Domestic
Extremists**



Drones



COVID-19

Date	Description
June 7	Presentation to RSTC, Beginning of Review Period
Mid-June	RSTC Endorsement
Early July	Board and MRC Review
Mid-July	Report release (Target)



Questions and Answers

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

2022 First Quarter Reliability Indicators

Soo Jin Kim, Director of PRISM
Board of Trustees Meeting
May 12, 2022

RELIABILITY | RESILIENCE | SECURITY


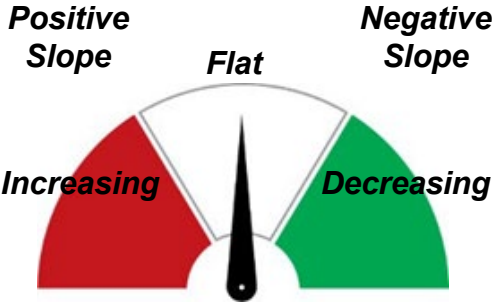


- **Why is it important?**

- Provides a quantitative measure and trend of actual impacts on the BPS

- **How is it measured?**

- Count: Number of Category 3 or above events
- Trend: Statistical test is performed on the five-year cumulative daily event Severity Risk Index (eSRI) for (Category 1–3) events

<p>Data (Annual Measurement)</p> <ul style="list-style-type: none"> ○ Threshold: No Category 3 or above events: <i>Zero is green, else is red</i> 	<p>2022 Status</p> 
<p>Data (Compared to a 5-year rolling average)</p> <ul style="list-style-type: none"> ○ Slope of eSRI line is flat to decreasing and does not show an increase above zero that is statistically significant (95% Confidence Interval). ○ “2022 Status” relates to the slope of the 5 year rolling average (Positive, Flat, or Negative), not just the 2022 performance. 	

- **Why is it important?**

- Reduce risk to BPS reliability from Standard violations by registered entities

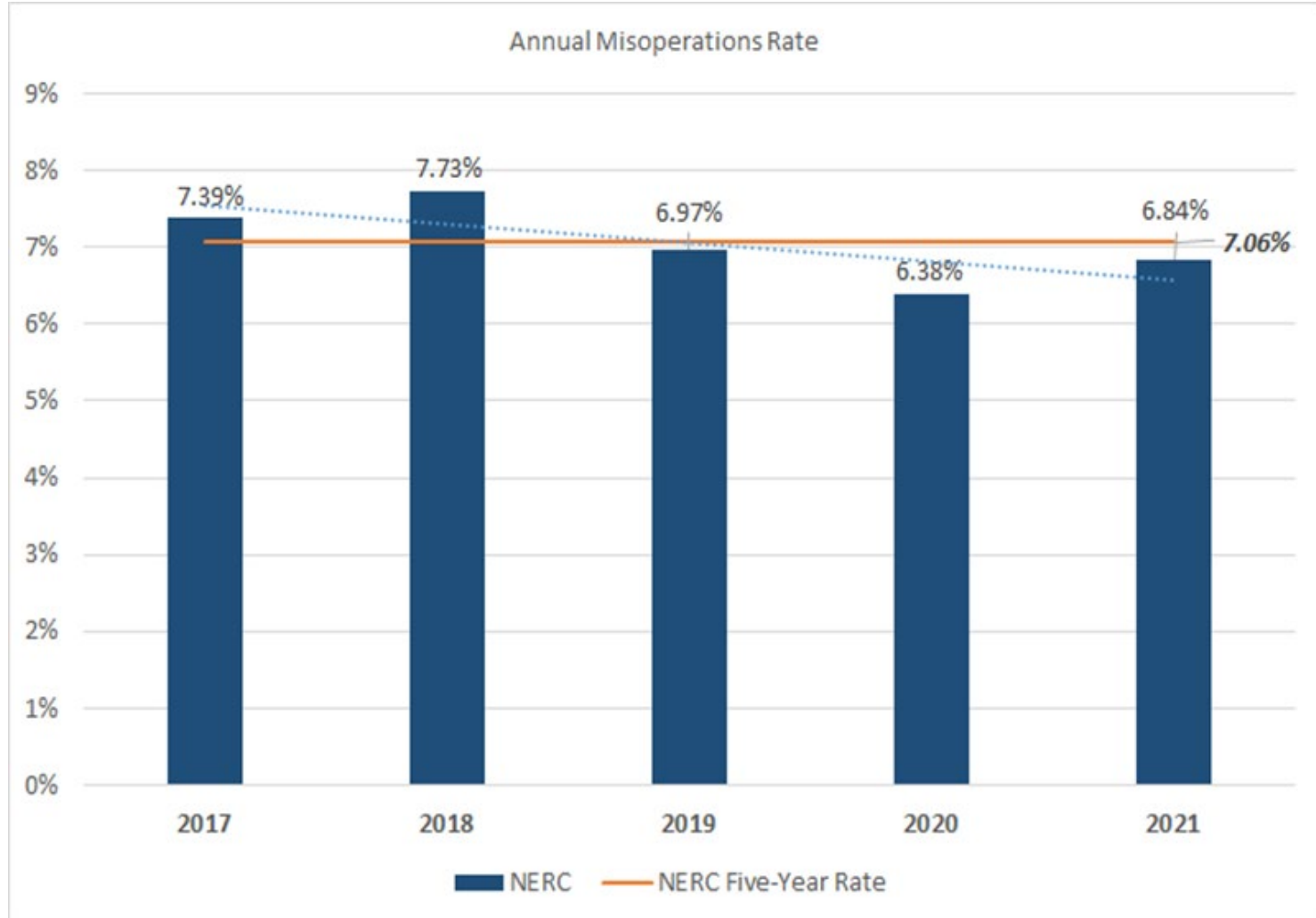
- **How is it measured?**

- Moderate and serious risk noncompliance with a relevant history of similar past conduct: **7% of moderate and serious risk violations filed in Q1 2022 had relevant past conduct.**
- The number of violations discovered through self-reports: **87% of noncompliance submitted in Q1 2022 were self-reported.**
- Risk to the BPS based on the severity of Standard violations: **17% of the violations filed in Q1 2022 were assessed as serious risk.**
 - *3% of past 5-year filings are assessed as serious risk.*

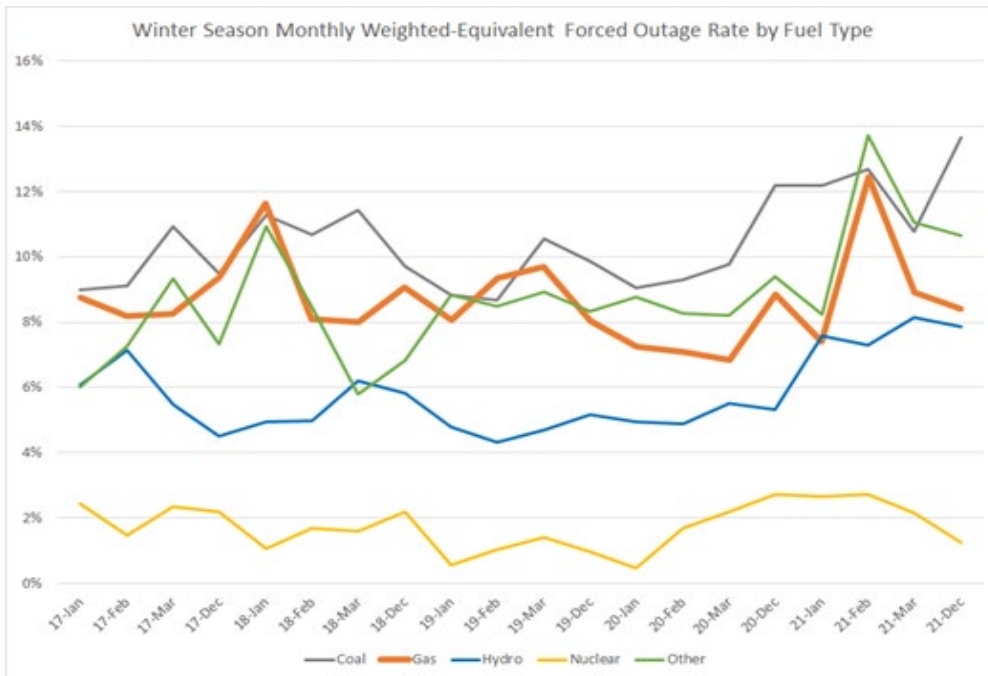
** For additional detail please refer to Q1 2022 CMEP report.*



Indicator 3: Protection System Misoperations Rate

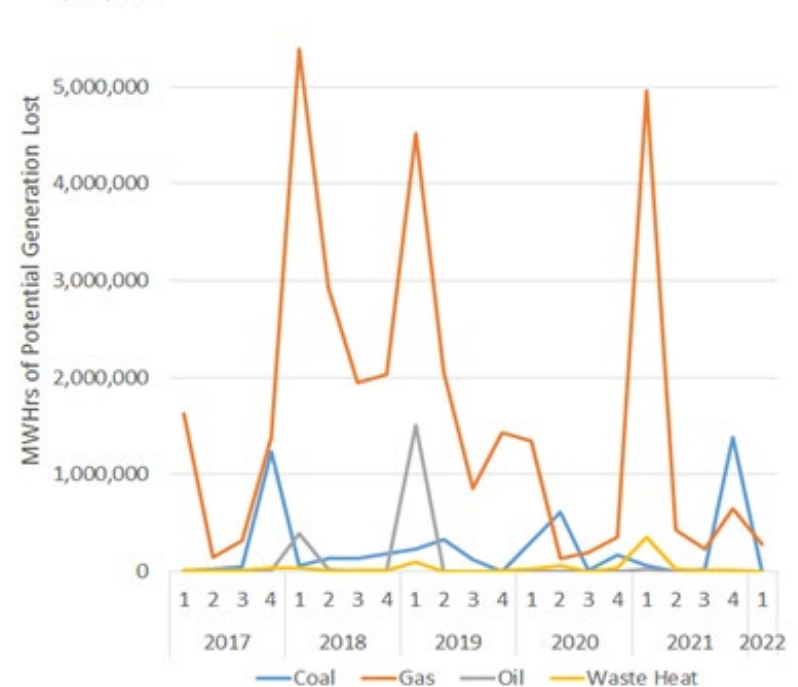


Indicator 4: Forced Outage Rate During Cold Weather Months and Potential Production MWH Loss Due to Lack of Fuel

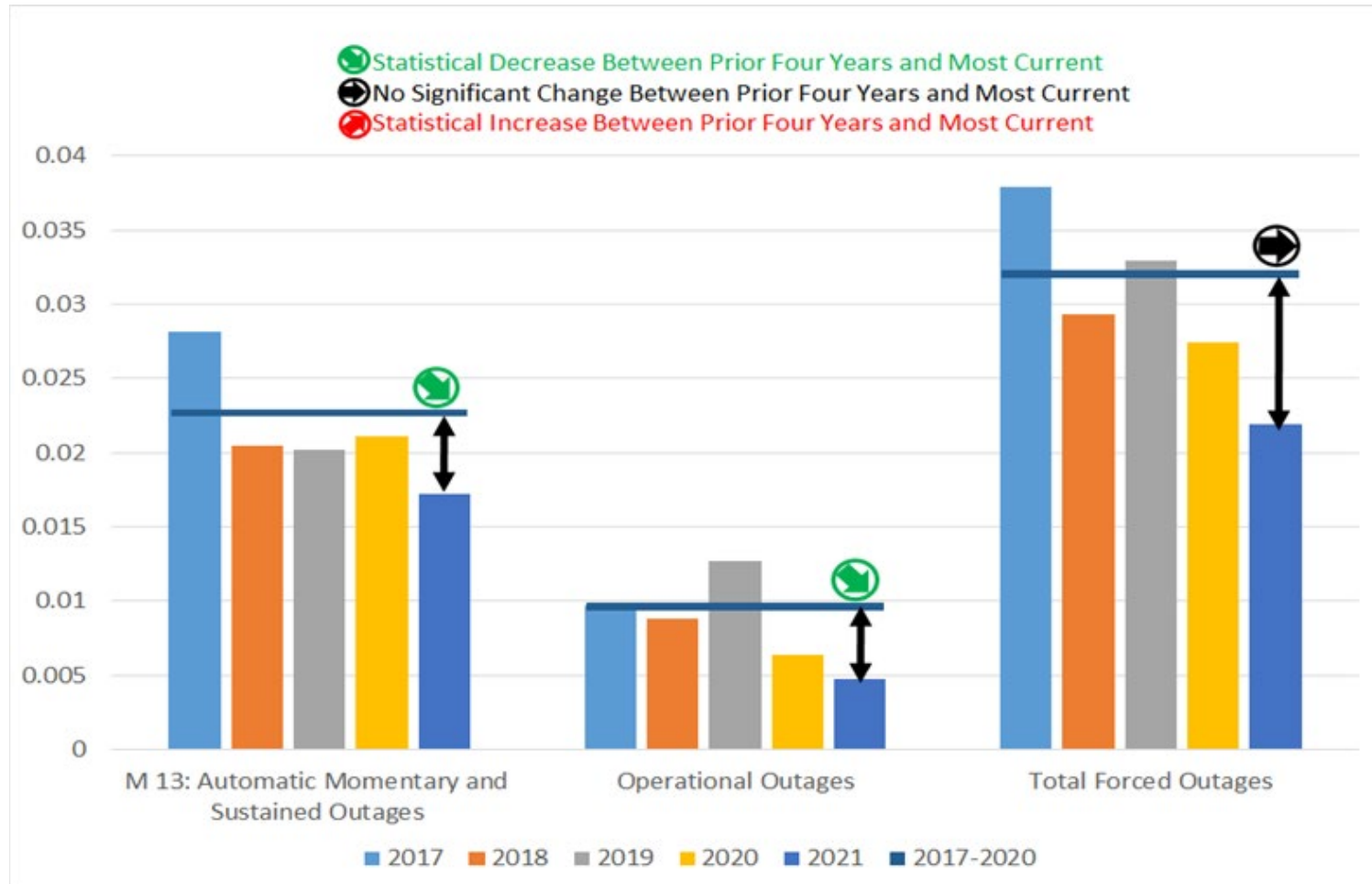


Winter Season Monthly Weighted EFOR by Fuel Type

Quarterly MWH of Lost Production Potential Due to Lack of Fuel

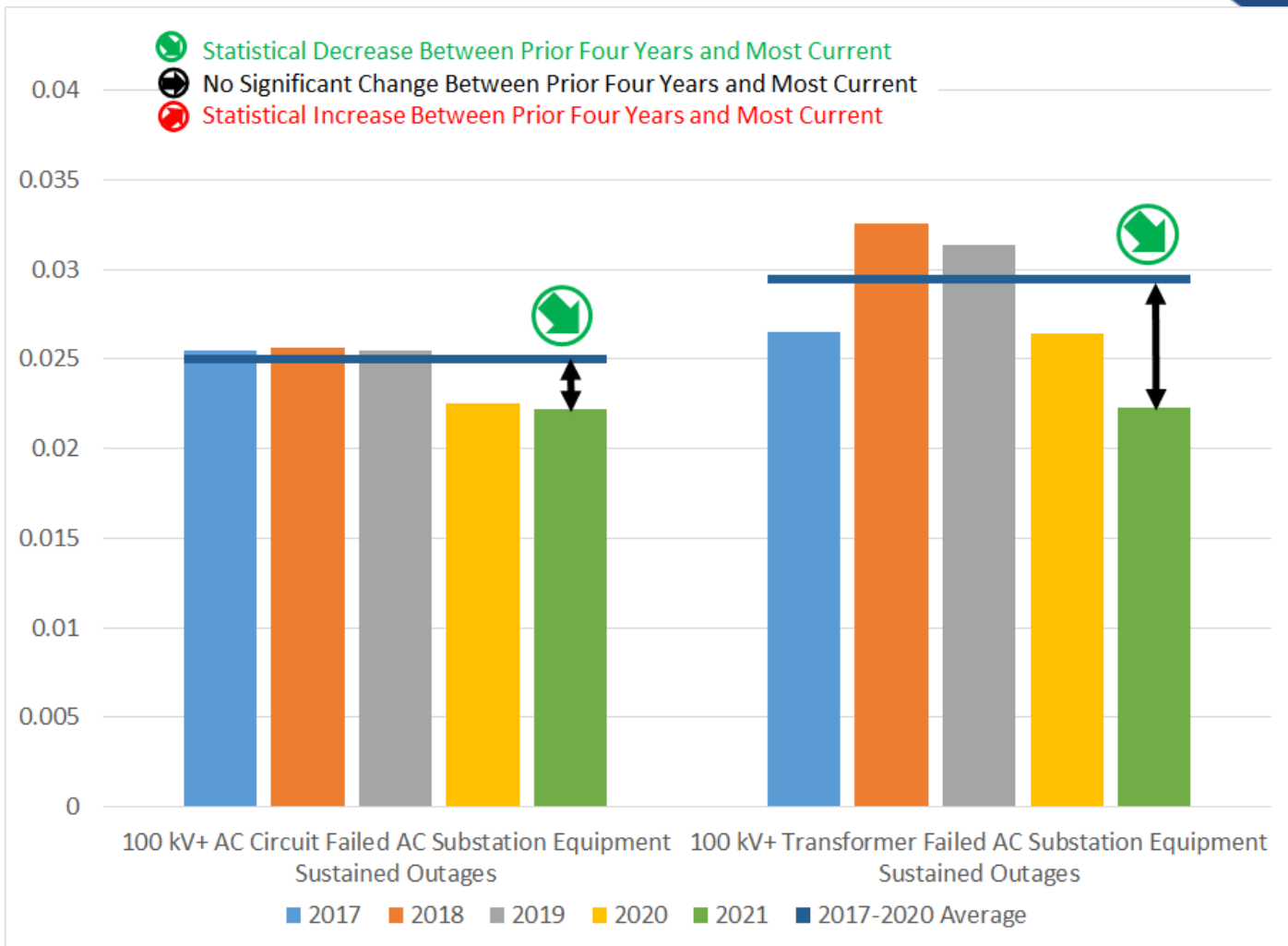


Percent of Potential Production Lost Due to Lack of Fuel



**Outages Caused by Human Error
AC Circuits**

Indicator 5b: Substation Equipment Failures or Failed Circuit Equipment



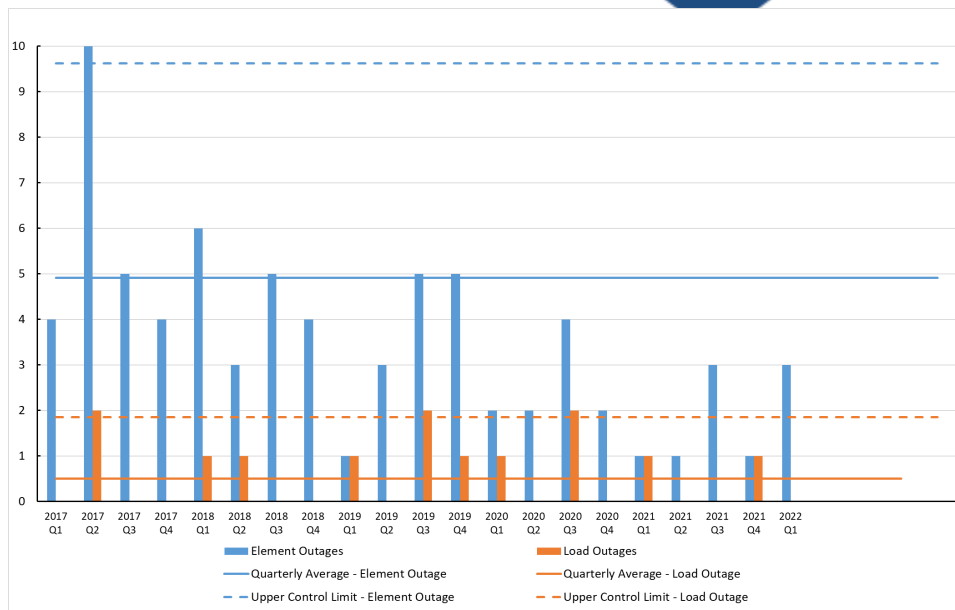
Failed AC Substation Equipment

- **How is it measured?**

- Number of vegetation encroachments: **No Vegetation encroachment from inside of the right-of-way was reported to NERC during Q1 2022.**

• How is it measured?

- Number of applicable DOE OE-417 Electric Emergency Incident and Disturbance Reports and NERC EOP-004 Event Reports



Data (Compared to 2016-2018 Quarterly Baseline)

- No disruption* of BES operations due to cyber security incidents
Zero disruptions of BES operations due to cyber attacks in 2022 Q1
- Number of disruptions* of BES operations due to physical security incidents: *Below baseline Upper Control Limit is green, else is red*
Three disruptions of BES operations (Zero with load loss) due to physical attacks in 2022 Q1

*A disruption means that a BES element was removed from service as a result of the cyber or physical incident

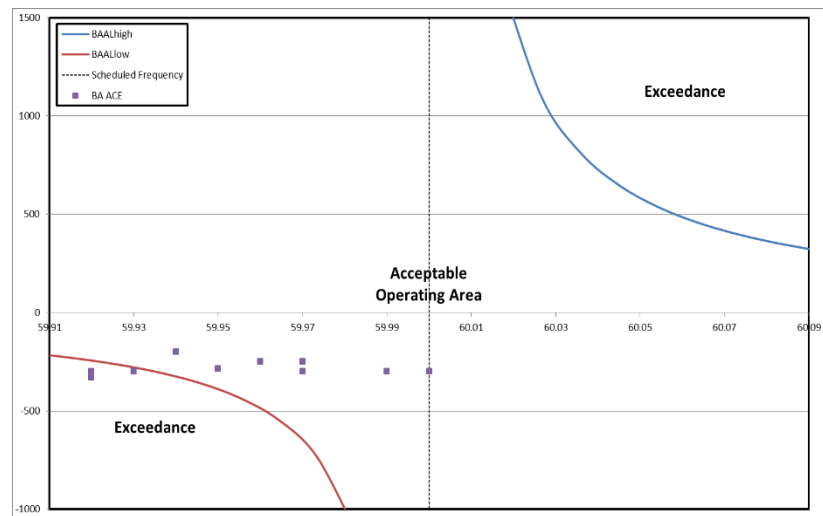
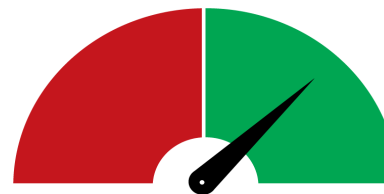


Why is it important?

Each Balancing Authority (BA) is required to operate such that its clock-minute average of reporting area control error (ACE) does not exceed its clock-minute BA ACE limit (BAAL) for more than 30 consecutive clock-minutes. The purpose of this metric is to measure risk to the BPS by monitoring the trend in the number of clock minutes in which BAs return their ACE to within their BAAL after an exceedance has occurred.

How is it measured?

Success (**green**) is achieved when the linear regression line of the most recent four years of quarterly BAAL exceedances greater than or equal to 15 clock minutes has a statistically significant negative slope or when the slope of the time trend is statistically neither increasing nor decreasing. This equates to either improvement or no decline in performance. Failure (**red**) occurs if slope of the time trend is increasing with statistical significance.



Why is it important?

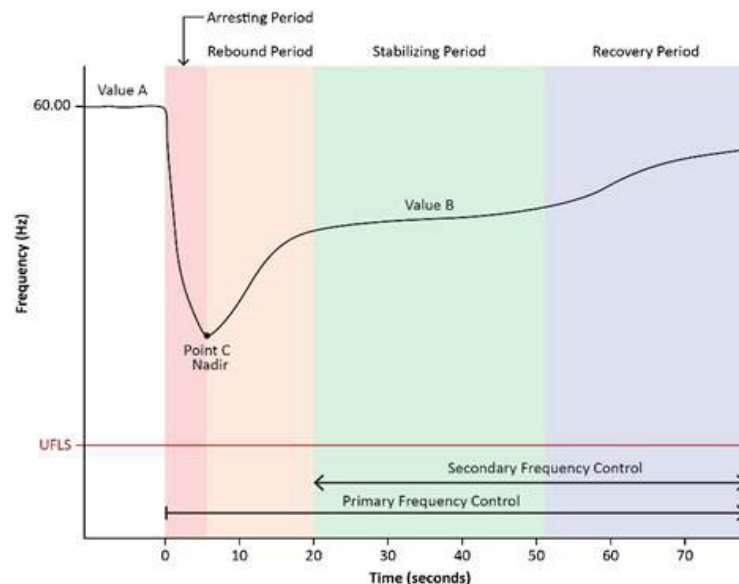
Measures risk and impact to the BPS by evaluating the trend in the magnitude of the decline in Interconnection frequency experienced in each Interconnection during low frequency events selected for BAL-003-1 compliance. The Indicator will evaluate whether the risk of activating under frequency load shed devices is increasing or decreasing.

How is it measured?

Success (green) is achieved when the linear regression line of the most recent four years of quarterly mean values of Frequency A minus Frequency C has a statistically significant negative slope or when the slope of the time trend is statistically neither increasing nor decreasing. This equates to either improvement or no decline in performance where Interconnection risk has not changed or declined. Failure (red) occurs if the slope of the time trend is increasing with statistical significance or if under frequency load shedding is activated for any single BAL-003 frequency event in any Interconnection.



EI, WI, QI, TI



- **Why is it important?**

- Measures risk and impact to the BPS by measuring the interconnection frequency response performance measure (IFRM) for each BAL-003-2 event as compared to the Interconnection Frequency Response Obligation (IFRO)

- **How is it measured?**

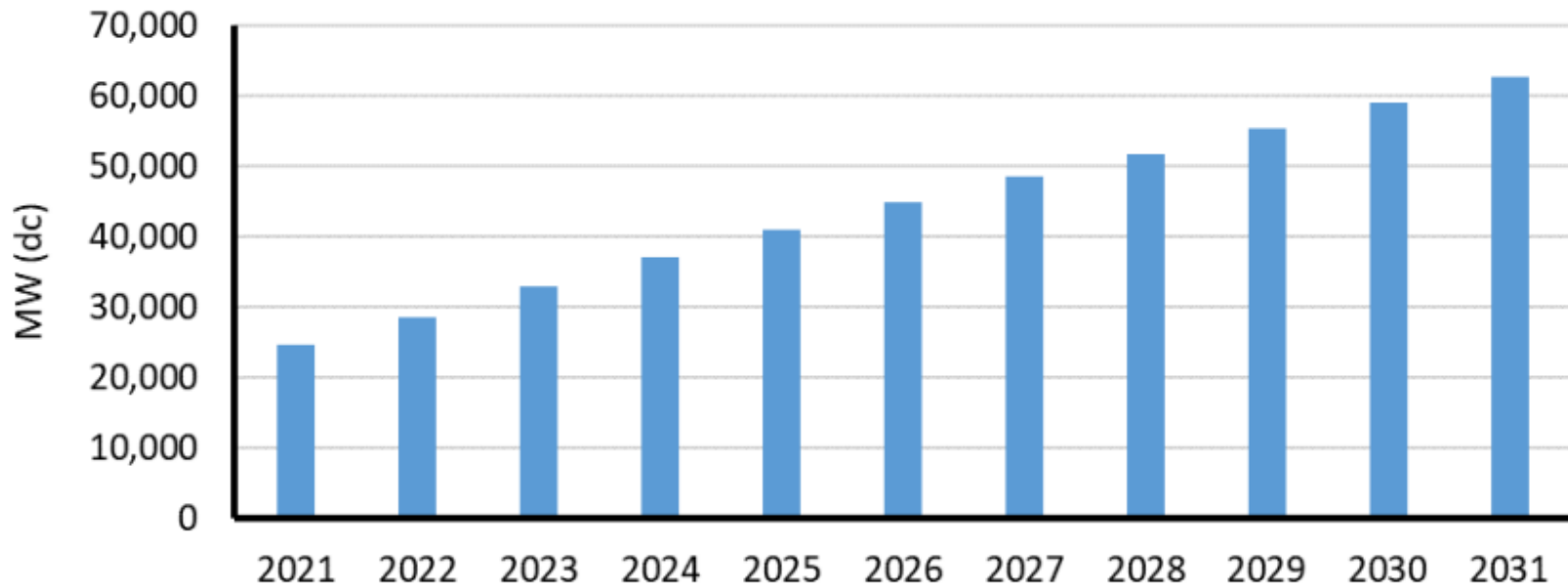
- IFROs are calculated and recommended in the Frequency Response Annual Analysis Report for Reliability Standard BAL-003-2.1 implementation
- IFRM performance is measured for each event by comparing the resource (or load) MW loss to the frequency deviation
- Due to the timing in selection of events the metric is updated one quarter in arrears.

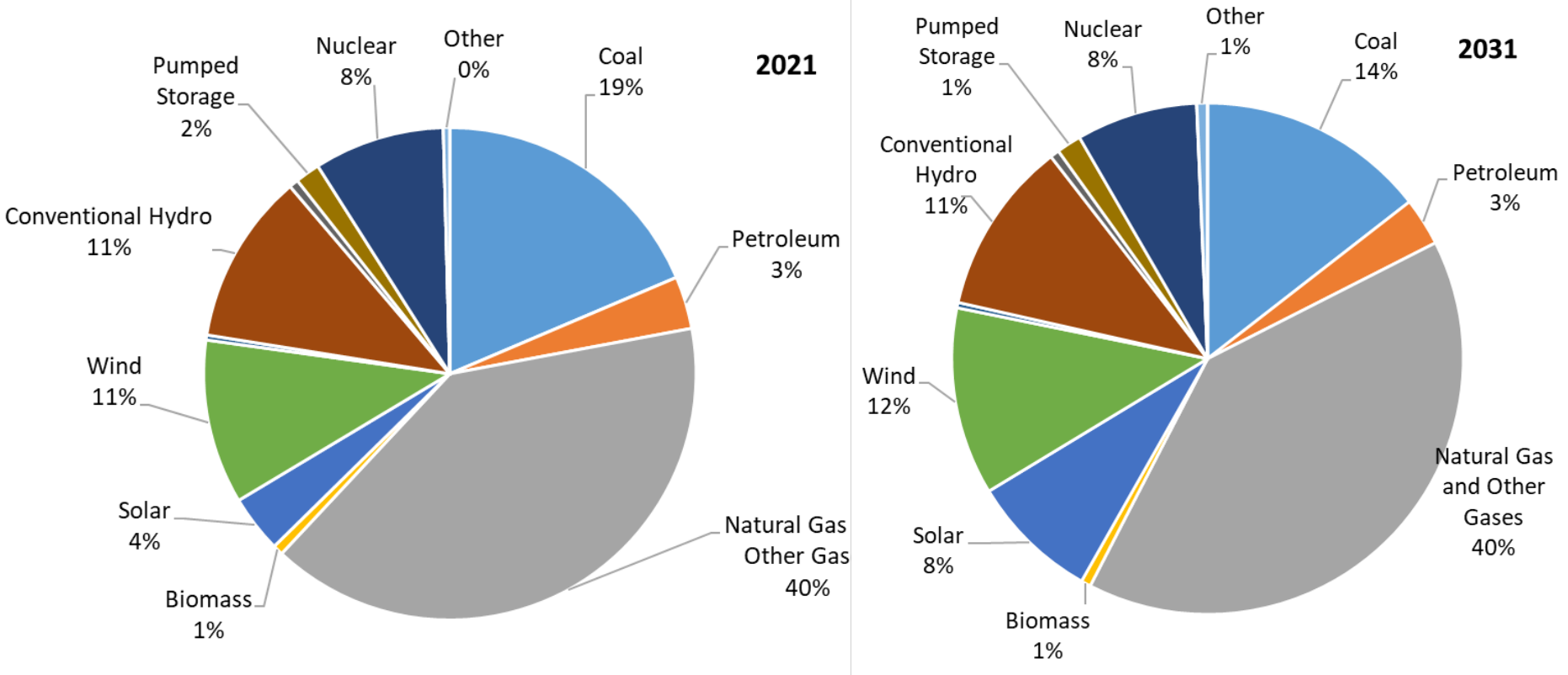
Data (Quarterly & Annual Measurement), NEW

- IFRM for each BAL-003-2 event is compared to the IFRO for each quarter of the 2021 operating year
- Success is no Interconnection experiencing a BAL-003-2 frequency event where IFRM performance is below their respective IFRO: *Zero is green, else is red*
- **Metric Results through 1Q22:** No Interconnection experienced a BAL-003-2 event where their IFRM was below their IFRO

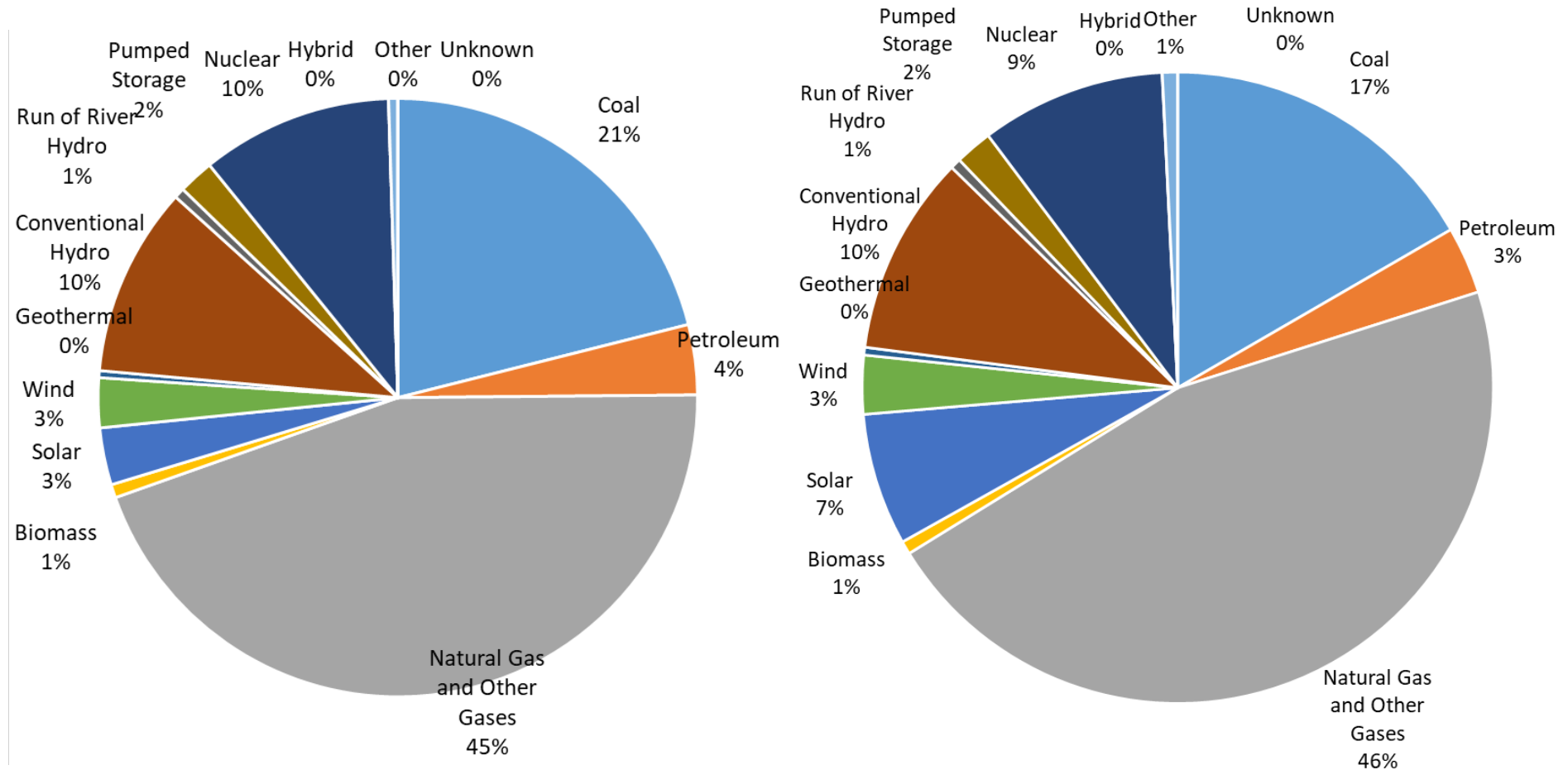
2022 Status







Installed Nameplate Capacity by Fuel Mix Trend



On-Peak Anticipated Capacity Trend by Fuel Mix



Questions and Answers