RELIABILITYFIRST

Annual Reliability and Compliance Workshop: Embracing the Transformation

Day 1

Tuesday, September 27, 2022

1 – 5 p.m. Eastern

PUBLIC

Welcome and Logistics

- Safety and Logistics
- This WebEx event is not being recorded
- Please submit all questions through Slido
- We will provide the workshop survey live at the end of Day #2
- Today's presentations (minus the E-ISAC presentation) are posted on the RF website

Join the conversation at

Slido.com

#RFWorkhshop

Slido

For our virtual participants, what city and state are you joining from?

For our in-person guests, what city and state did you travel from?

Join the conversation at

Slido.com

#RFWorkhshop

Today's Agenda

Tuesday, Sept. 27		
Presentation	**Presenter(s)**	**Time**
Lunch		12 – 1 p.m.
Opening Remarks	Brian Thiry, Director of Entity Engagement, RF	1 – 1:10 p.m.
Day 1 Keynote	Tim Gallagher, CEO, RF	1:10 – 1:40 p.m.
Energy Availability and the Changing Generation Resource Mix	Mark Lauby, Senior VP NERC; and Jim Uhrin, Director, Engineering & Reliability Services, RF	1:40 – 2:40 p.m.
Break		2:40 – 3 p.m.
OT Cyber Threats and Recommendations for the Electric Sector	Robert Lee, CEO and Co-Founder Dragos, Inc.	3 – 3:40 p.m.
Electricity Threat Landscape and CIP-008 Submission Considerations	Matt Duncan, Director of Intelligence, E-ISAC	3:40 – 4:20 p.m.
CMEP Updates	Zack Brinkman, CIP Compliance Monitoring Manager, RF	4:20 – 4:50 p.m.
Closing Remarks	Brian Thiry, Director of Entity Engagement, RF	4:50 – 5 p.m.
Reception		5 – 7 p.m.

Trivia Giveaways

RF is offering the opportunity to win a $50 Amazon gift card at the end of each workshop day for five participants!

To Enter: Use Slido (Slido.com, Slido app or the QR code). At the closing of each workshop day, we will announce that a content-based trivia question is coming. You will have one minute to enter your name into Slido before the questions are asked. You must enter your first and last name; anonymous responders are not eligible to win.

To Win: A skill-based question will be visible in Slido. You must answer correctly and be the fastest respondent, as recorded in Slido, to win. We will announce the winners who will then email Jody Tortora to receive the $50 Amazon gift card.

Join the conversation
at **Slido.com**
#RFWorkshop

NO COST TO ENTER. Governed by the rules of Ohio. Registrants and Entrants hold RF harmless from any associated claim and RF is not responsible nor may be held liable for any technical errors or events that may prevent the promotion from running smoothly. Must be over the age of 18 with a valid US address and not an Employee of ReliabilityFirst to win. Any resulting taxes are the responsibility of the winner.

RF Anti-Trust Statement

It is ReliabilityFirst's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct which violates, or which might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every ReliabilityFirst participant and employee who may in any way affect ReliabilityFirst's compliance with the antitrust laws to carry out this policy.

Keynote Speaker

Tim Gallagher
President & CEO, ReliabilityFirst

Energy Availability

Mark Lauby and Jim Uhrin
ReliabilityFirst 2022 Fall Workshop
September 27, 2022

Strong Regions + Strong NERC = Brilliant ERO

Mark Lauby

NERC Senior Vice President and Chief Engineer

Mr. Lauby joined NERC in January 2007 and has held a number of positions, including vice president and director of Standards and vice president and director of Reliability Assessments and Performance Analysis.

In 2012, Mr. Lauby was elected to the North American Energy Standards Board and was appointed to the Department of Energy's Electric Advisory Committee by the Secretary of Energy from 2013-2017. He has been recognized for his achievements, including the 1992 IEEE Walter Fee Young Engineer of the Year Award. He was named a Fellow by IEEE in November 2011 for "leadership in the development and application of techniques for bulk power system reliability," and in 2014, Mr. Lauby was awarded the IEEE Power and Energy Society's Roy Billinton Power System Reliability Award. In 2020, the National Academy of Engineering (NAE) elected Mr. Lauby as a member.

Prior to joining NERC, Mr. Lauby worked for the Electric Power Research Institute (EPRI) for 20 years.

Mr. Lauby began his electric industry career in 1979 at the Mid-Continent Area Power Pool in Minneapolis, Minnesota. Mr. Lauby is the author of more than 100 technical papers. He earned his bachelor's and master's degrees in Electrical Engineering from the University of Minnesota. In addition, Mr. Lauby attended the London Business School Accelerated Development Program, as well as the Executive Leadership Program at Harvard Business School.

Jim Uhrin

Director, Engineering and Reliability Services

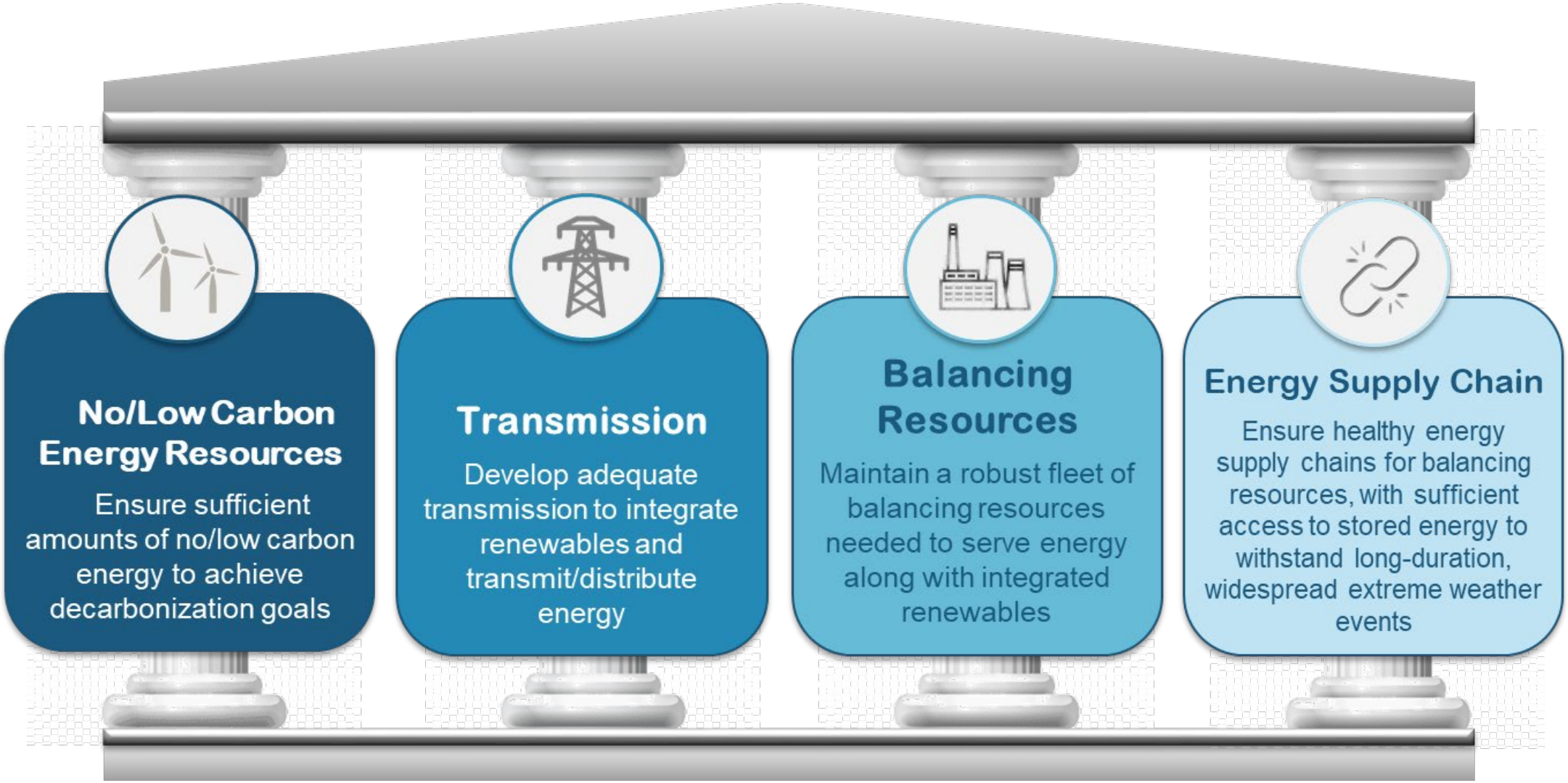
Mr. Uhrin joined ReliabilityFirst in 2007 and has about forty years of working experience in the electric utility industry. In his current role Mr. Uhrin is responsible for overseeing the Engineering and System Performance and the Operational Analysis and Awareness groups. Prior to serving in this role, Mr. Uhrin, held the position of Director, Compliance Monitoring, at ReliabilityFirst Corporation for 8 years. In that role, Mr. Uhrin was responsible for directing and served in an oversight role over all Compliance Monitoring functions performed at RF (Ops/Planning and CIP). In Mr. Uhrin's previous role at ReliabilityFirst, he served as the Manager of Compliance Service and Investigations, where he was responsible for the oversight of the Compliance Monitoring and Enforcement Program (CMEP), Regulatory Reviews, and implementation of most of the CMEP related activities.

Prior to joining ReliabilityFirst, Mr. Uhrin was the Manager of Dispatch and Operation for PJM Interconnection, L.C.C, in their West Office, where he managed both the day-to-day operations of the Bulk Power System and the West Regional office operations. Before joining PJM, Mr. Uhrin held various positions with Allegheny Power as Operations Support Manager, Team Leader in Network Planning and various Engineering positions in Allegheny's Operations and System Planning Groups. Mr. Uhrin is a graduate of University of Pittsburgh with a Bachelor of Science degree in Electrical Engineering and has taken some MBA course work at Duquesne University. He is a Registered Professional Engineer in the state of Pennsylvania and was a NERC Certified System Operator (2010).

Energy Transition Underway

- The following drivers have led to rapid changes in energy resources:
  - Governmental policies
  - Changes in resource economics
  - Consumer demand for clean energy
- In addition to the shift in resources, an increase in extreme weather presents new challenges
  - Fuel sources are inherently less secure

Four Pillars of the Energy Transition



The Challenge: Sufficient Energy Availability

The Challenge: Sufficient Energy Availability

- Power grid transition is resulting in a higher level of energy uncertainty, regardless of fuel type
  - The current tools, rules of thumb, and approaches used to determine the system's ability to meet demand were not designed for today's grid

- **The focus needs not be on fuel type, but rather on energy availability**

Considerations in Solving This Challenge

- Rapidly changing generation fleet
- Increasing electrification
- Widespread, long-duration, extreme weather events
- Historically, industry ensured energy through capacity and reserve margins with assurance of fuel

Refresher - Capacity, Nameplate and Energy

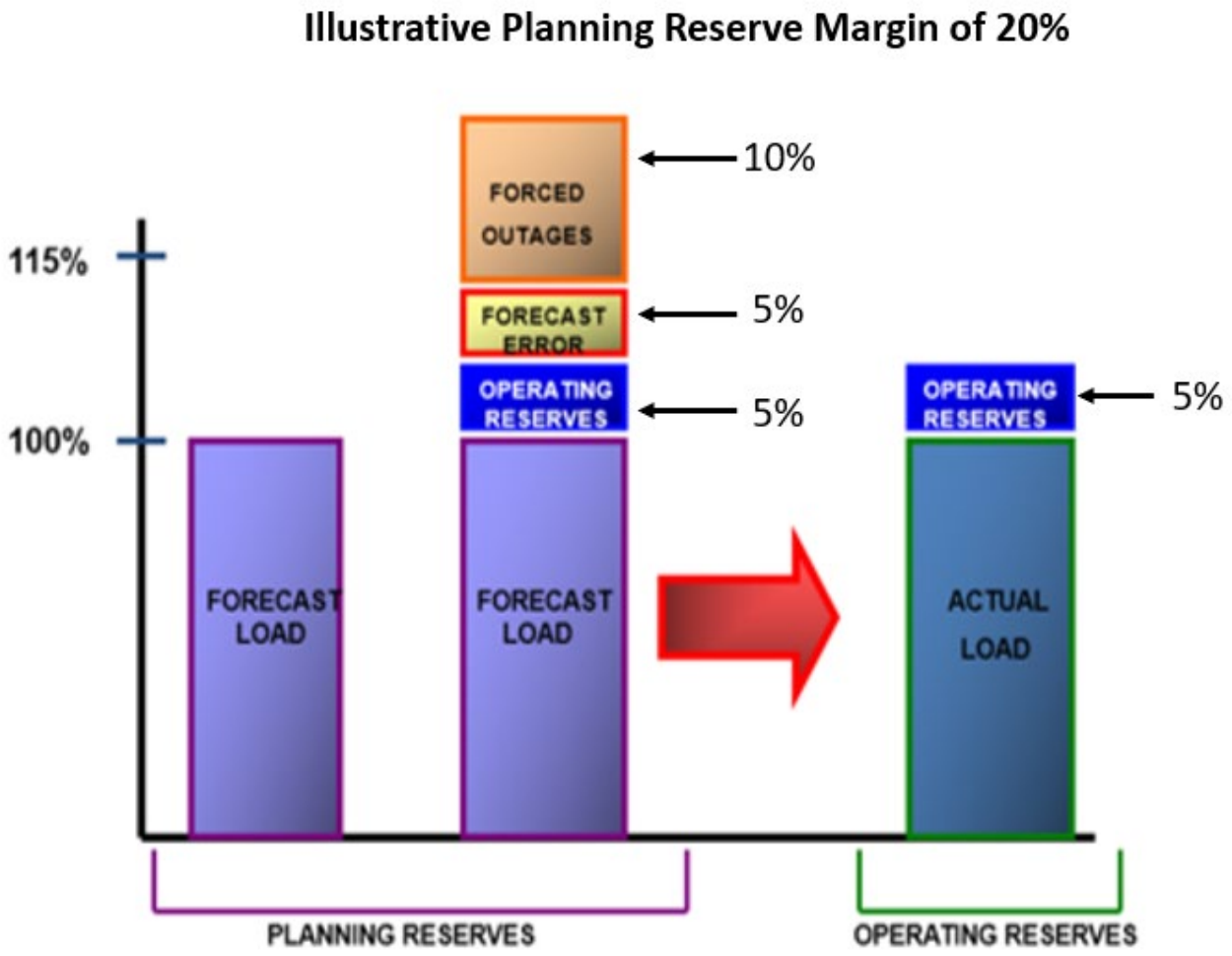
Capacity is the maximum electric output a generator can produce under specific conditions, typically on peak. (MW)

Energy is the amount of electricity a generator produces over a specific period of time. (MWh)

Nameplate is determined by the generator's manufacturer and indicates the maximum output of electricity a generator can produce without exceeding design thermal limits.

https://www.iso-ne.com/about/what-we-do/in-depth/capacity-vs-energy-primer#:~:text=Electricity%20is%20measured%20in%20both,measured%20in%20megawatts%20(MW).

Refresher - Planning Reserve Margin



Sufficient resources includes a planning reserve margin to account for weather variations, generation outages and load forecasting error

Year One - The planning year that begins with the upcoming annual Peak Period

Planning Reserve Margin Methodology

- Both PJM and MISO adhere to the ReliabilityFirst BAL-502-RF-03 Standard
  - Establishes the “one day in ten years” loss of load event criterion
  - Only requires performing a study / no required reinforcements
- PJM considers the following:
  - Includes existing and generation with signed agreements
  - Does not include energy-only resources
  - Generation availability rates based on forced, planned and maintenance outages
  - Load forecast uncertainty
  - Likelihood of emergency assistance from adjacent regions
- MISO considers the following:
  - Assumes no internal transmission limitations within the MISO Region
  - Uses an unforced capacity requirement based upon the weighted average forced outage rate for resources

2021-2022 Performance and Trends

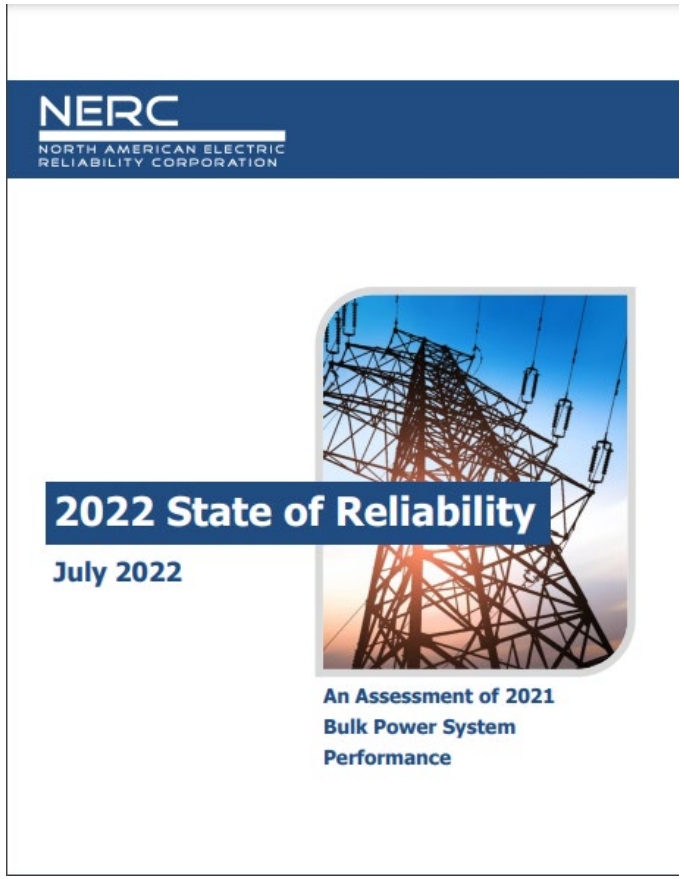
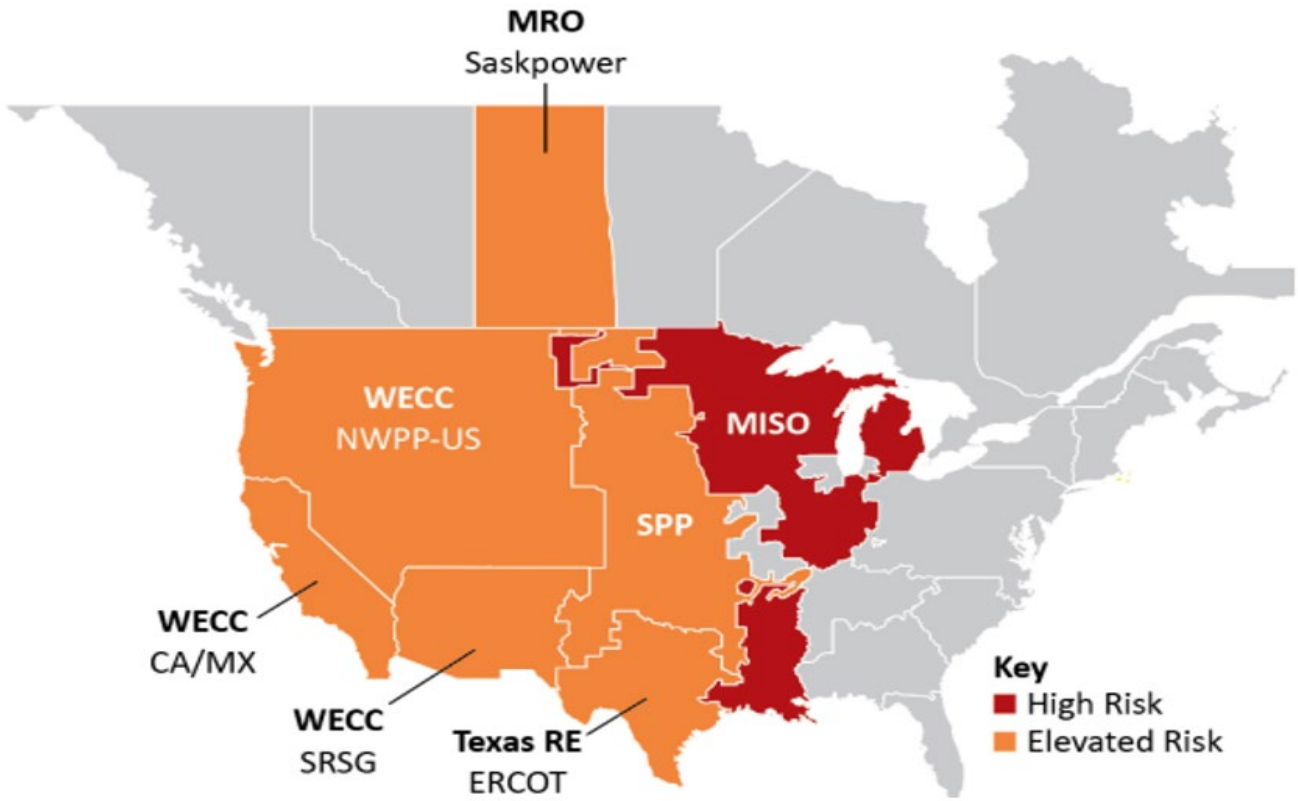


Table 3.1: Seasonal Risk Scenario Margins

Assessment Area	Summer 2021			Winter 2021–2022		
	Anticipated Reserve Margin	Typical Outages	Extreme Conditions	Anticipated Reserve Margin	Typical Outages	Extreme Conditions
MISO	21.60%	4.60%	-4.20%	48.50%	20.50%	-1.20%
MRO-Manitoba	26.90%	21.20%	8.40%	17.20%	14.30%	4.20%
MRO-SaskPower	19.80%	16.40%	5.70%	19.30%	16.10%	11.60%
NPCC-Maritimes	69.80%	58.80%	27.60%	26.50%	19.90%	-2.10%
NPCC-New England	22.00%	9.50%	-0.70%	71.10%	55.30%	25.90%
NPCC-New York	27.30%	17.00%	18.30%	78.60%	58.40%	33.50%
NPCC-Ontario	20.30%	20.30%	8.50%	20.00%	20.00%	21.30%
NPCC-Québec	46.40%	40.80%	37.90%	12.40%	8.50%	0.80%
PJM	33.50%	25.60%	12.10%	42.00%	29.10%	11.30%
SERC-Central	25.20%	25.20%	10.20%	32.50%	24.40%	9.30%
SERC-East	22.50%	22.50%	12.70%	25.90%	20.60%	4.30%
SERC-Florida Peninsula	23.40%	23.40%	15.40%	35.40%	29.70%	23.20%
SERC-South East	34.10%	34.10%	15.60%	38.70%	31.60%	21.10%
SPP	29.90%	10.80%	-3.90%	56.40%	30.90%	0.80%
Texas RE-ERCOT	15.30%	10.50%	-13.30%	41.90%	26.80%	-37.10%
WECC-AB	34.70%	25.00%	14.50%	34.70%	28.60%	8.30%
WECC-BC	37.50%	37.30%	9.30%	17.90%	17.80%	-0.60%
WECC-CAMX	23.80%	16.70%	-19.30%	40.30%	33.30%	12.30%
WECC-NWPP-US & RMRG	16.90%	15.10%	-10.10%	27.10%	26.60%	-1.50%
WECC-SRSG	20.60%	3.90%	-13.80%	103.30%	93.30%	56.50%

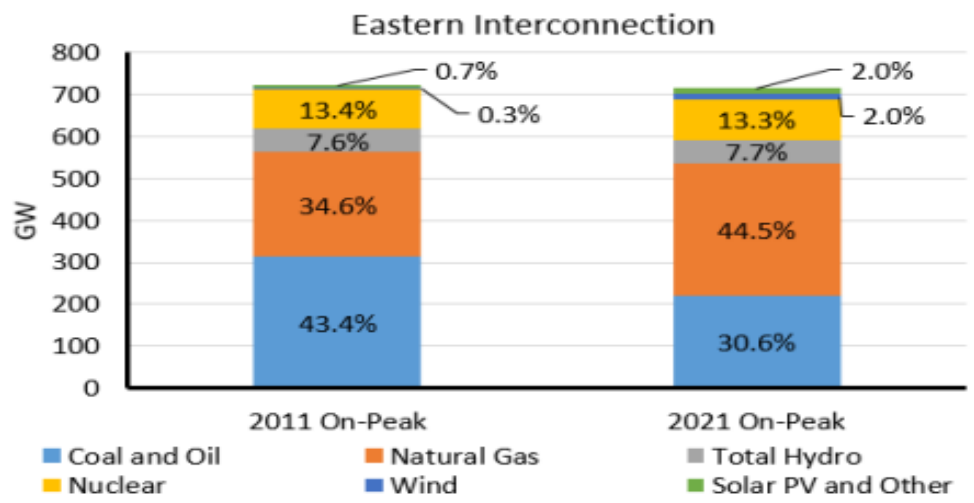
Note: The extreme conditions in Table 3.1 represent higher than average derates of resource capacity and demand.

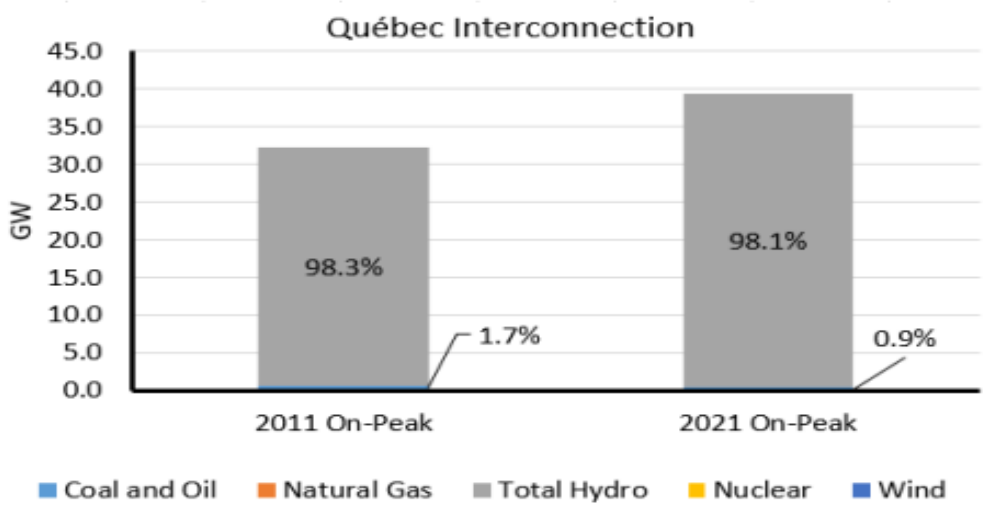
Summer Planning Reserve Margins

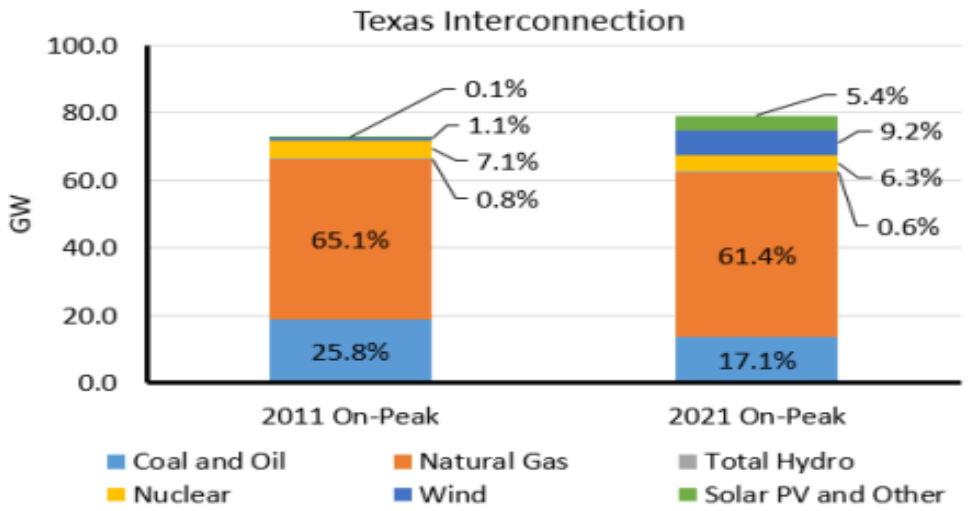


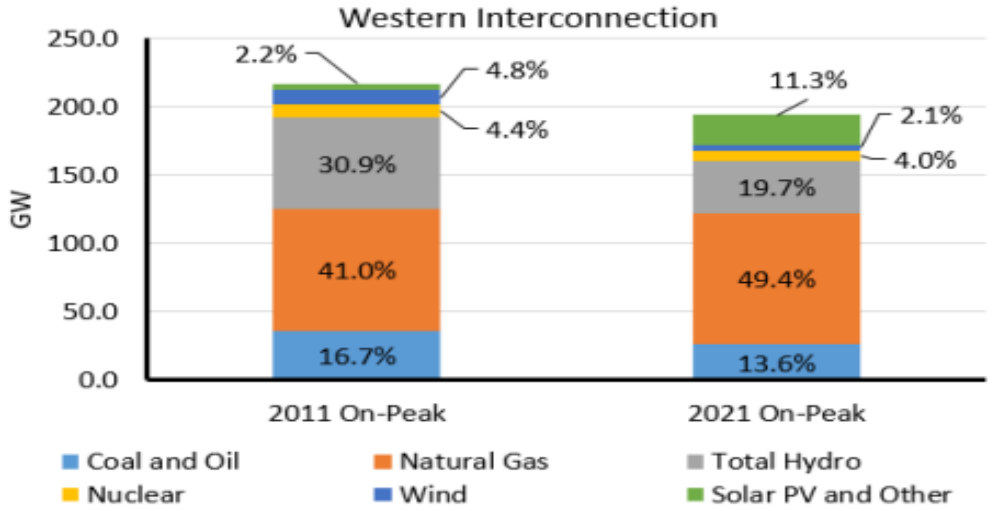
Seasonal Risk Assessment Summary	
High	Potential for insufficient operating reserves in normal peak conditions
Elevated	Potential for insufficient operating reserves in above-normal conditions
Low	Sufficient operating reserves expected

Generation Resource Mix Since 2011



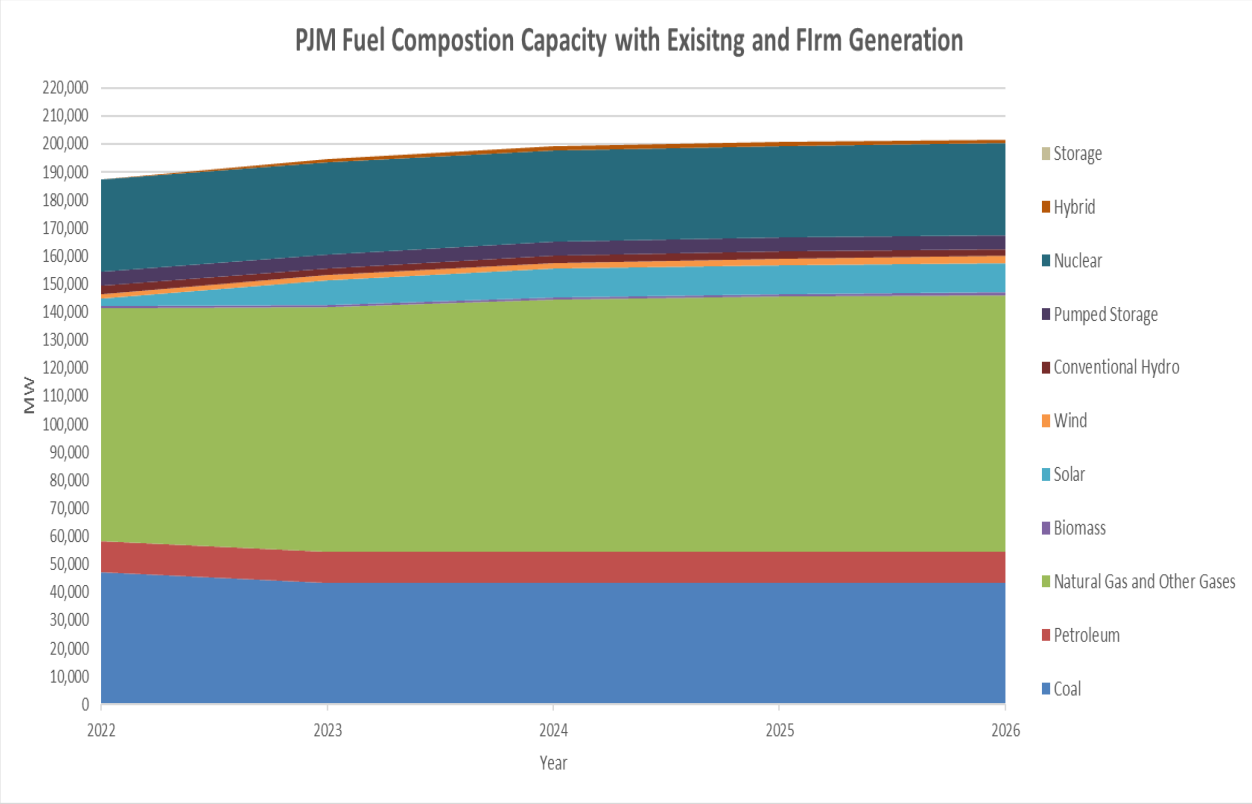


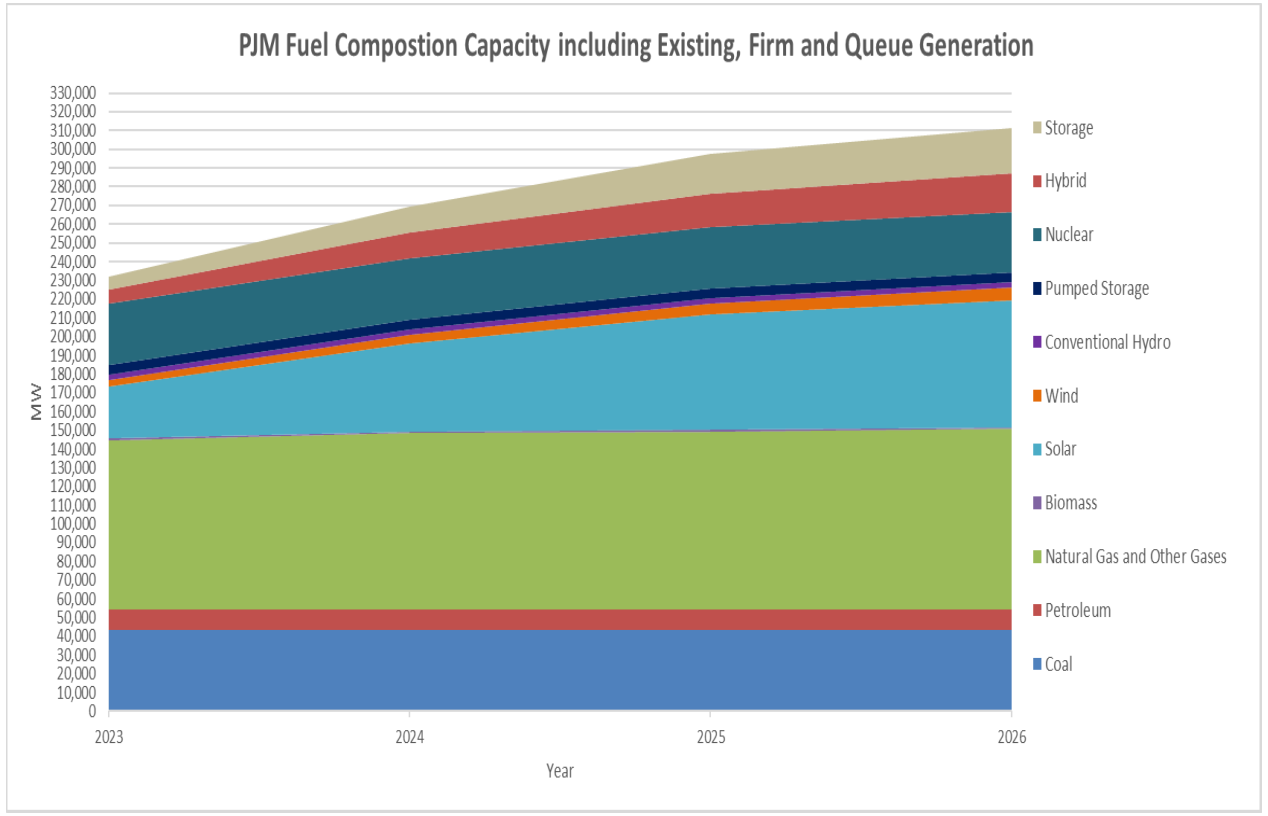




NERC | State of Reliability | 2022

PJM Generation Resource Mix

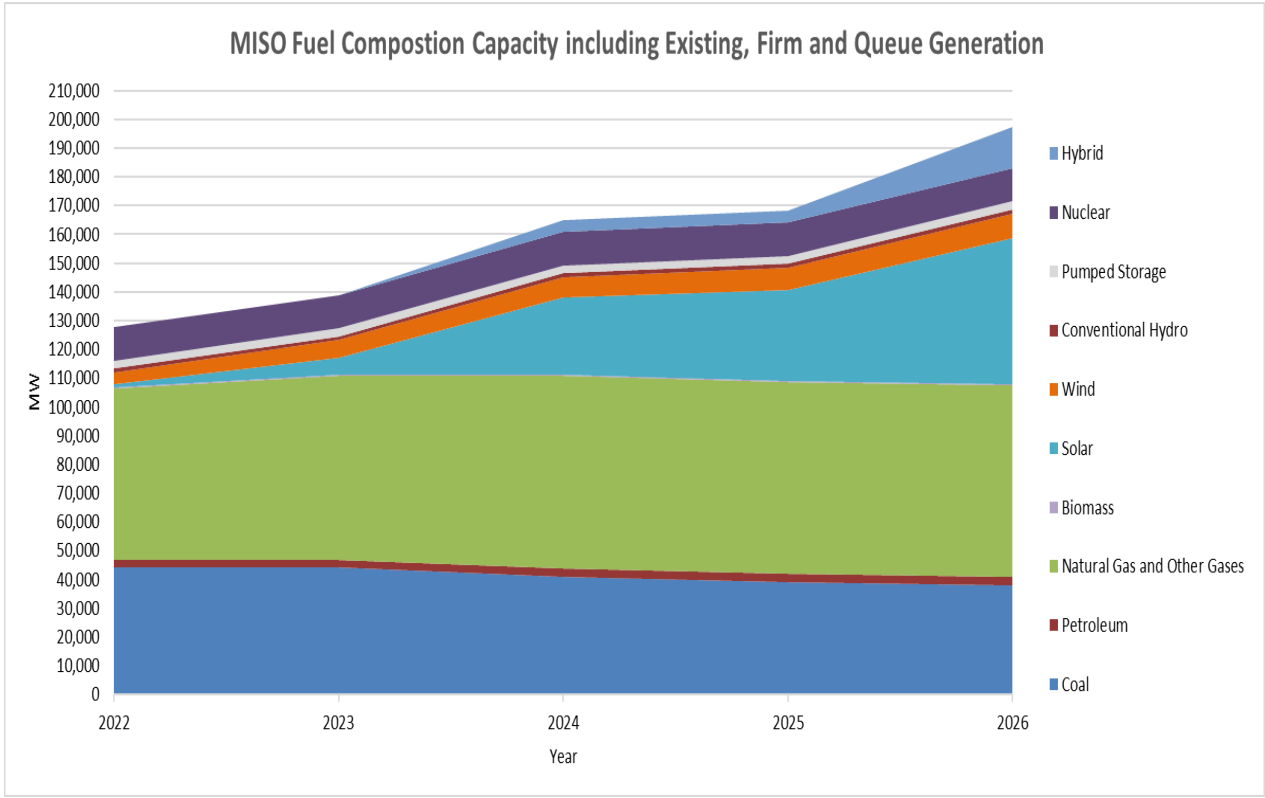




Hybrid Resources includes - Solar and Battery, Wind and Battery, Natural Gas and Battery and Other and Battery

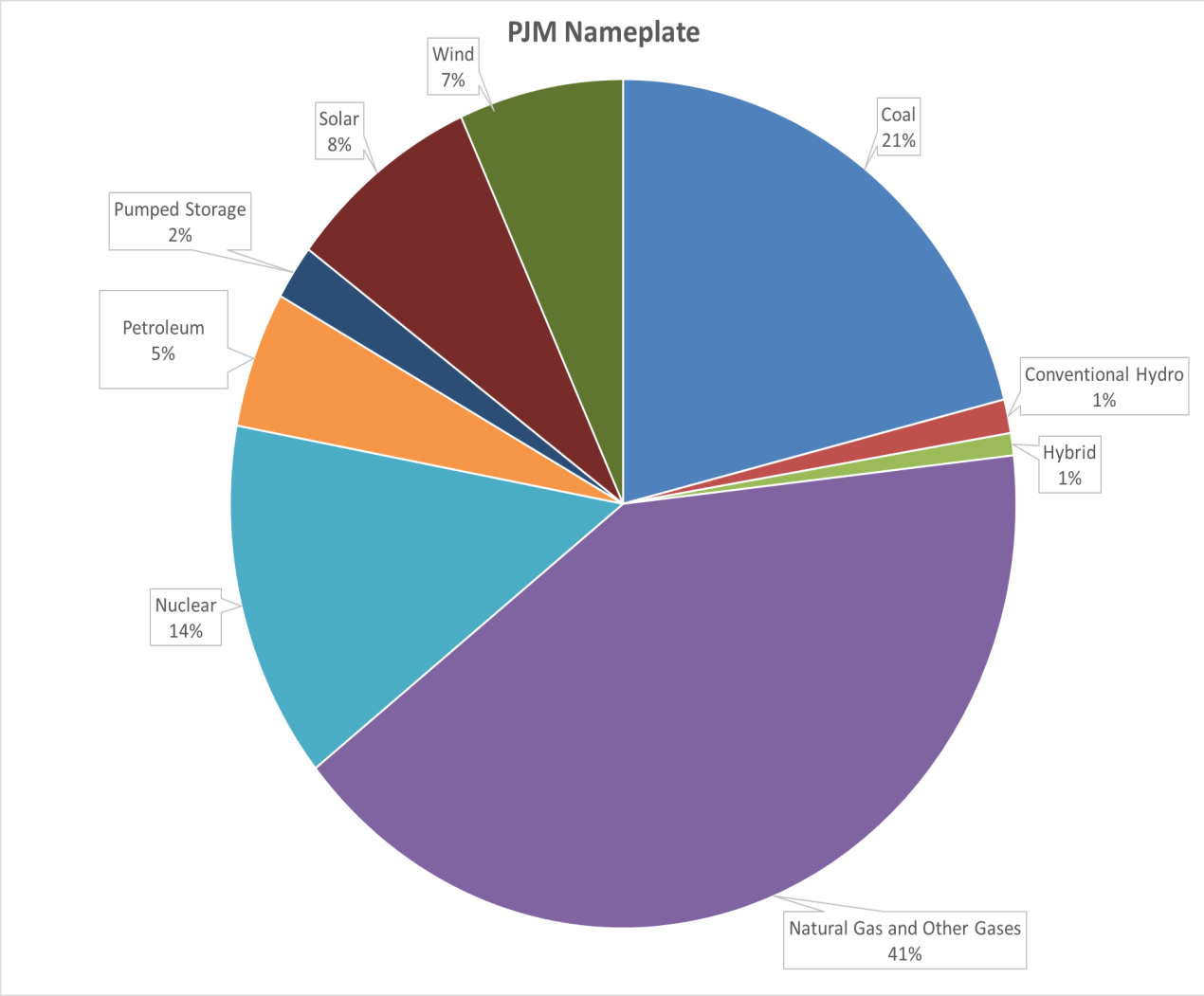
Storage includes – Battery Energy Storage

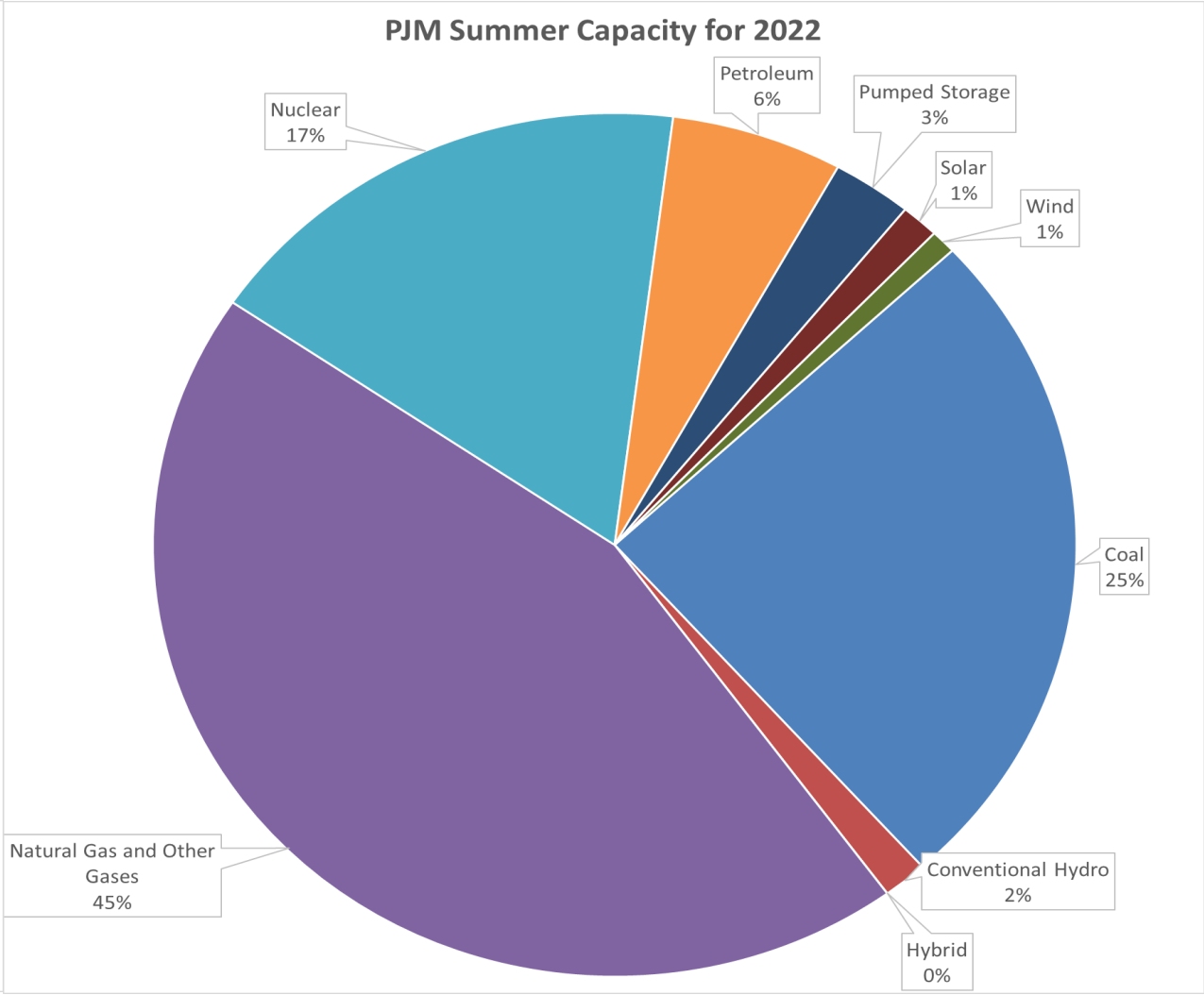
MISO Generation Resource Mix



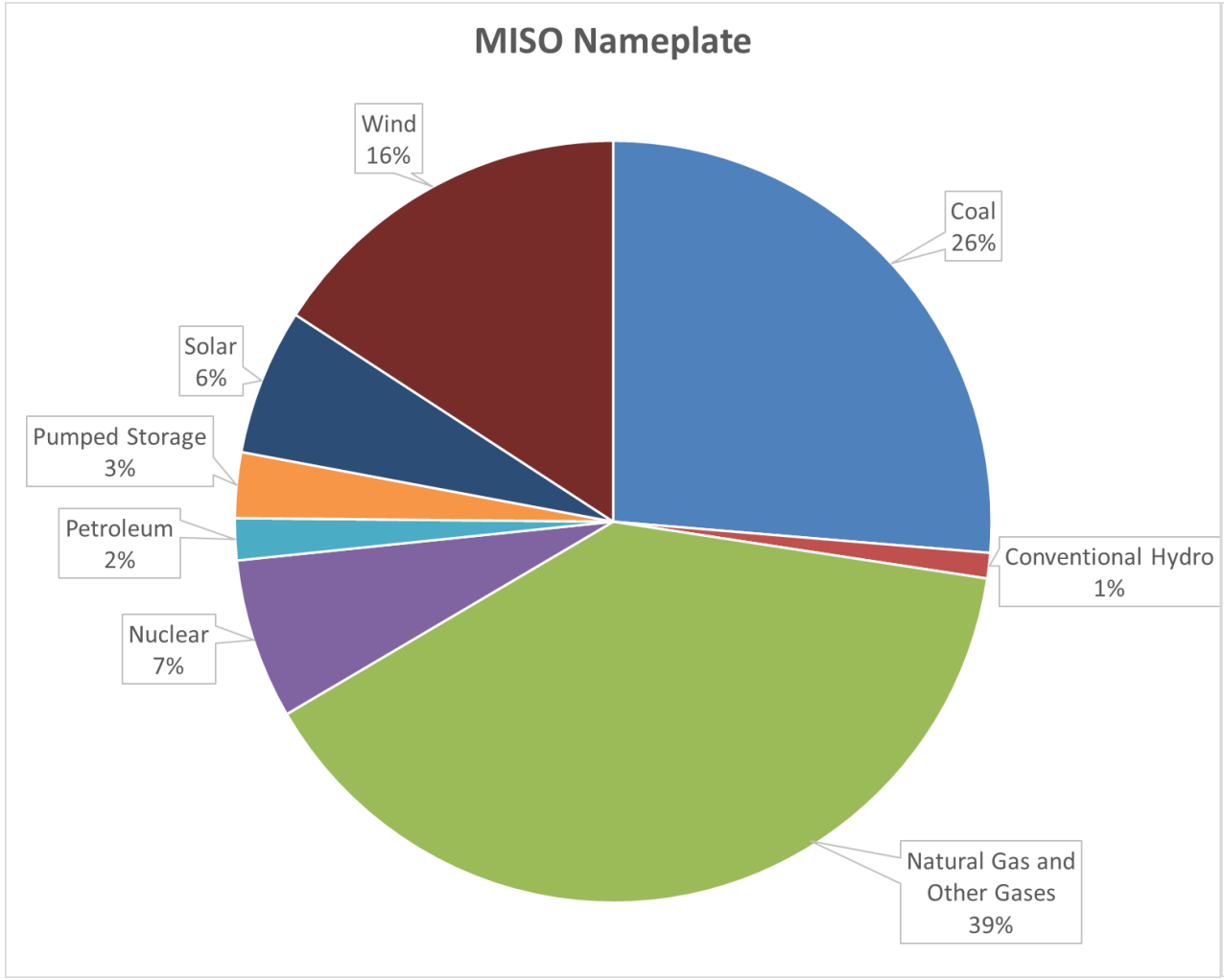
Hybrid Resources includes - Solar and Battery, Wind and Battery, Natural Gas and Battery and Other and Battery

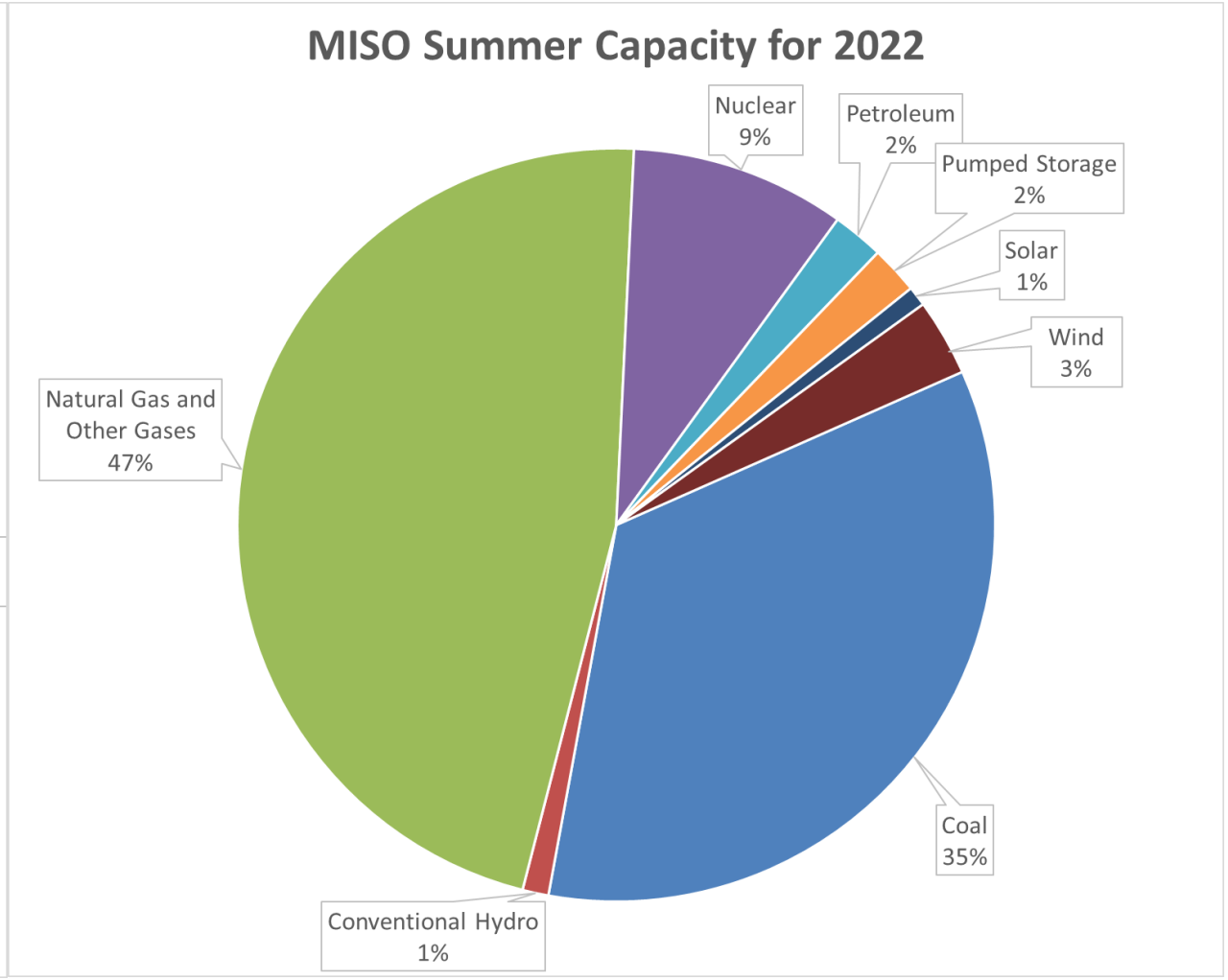
PJM Nameplate vs Capacity



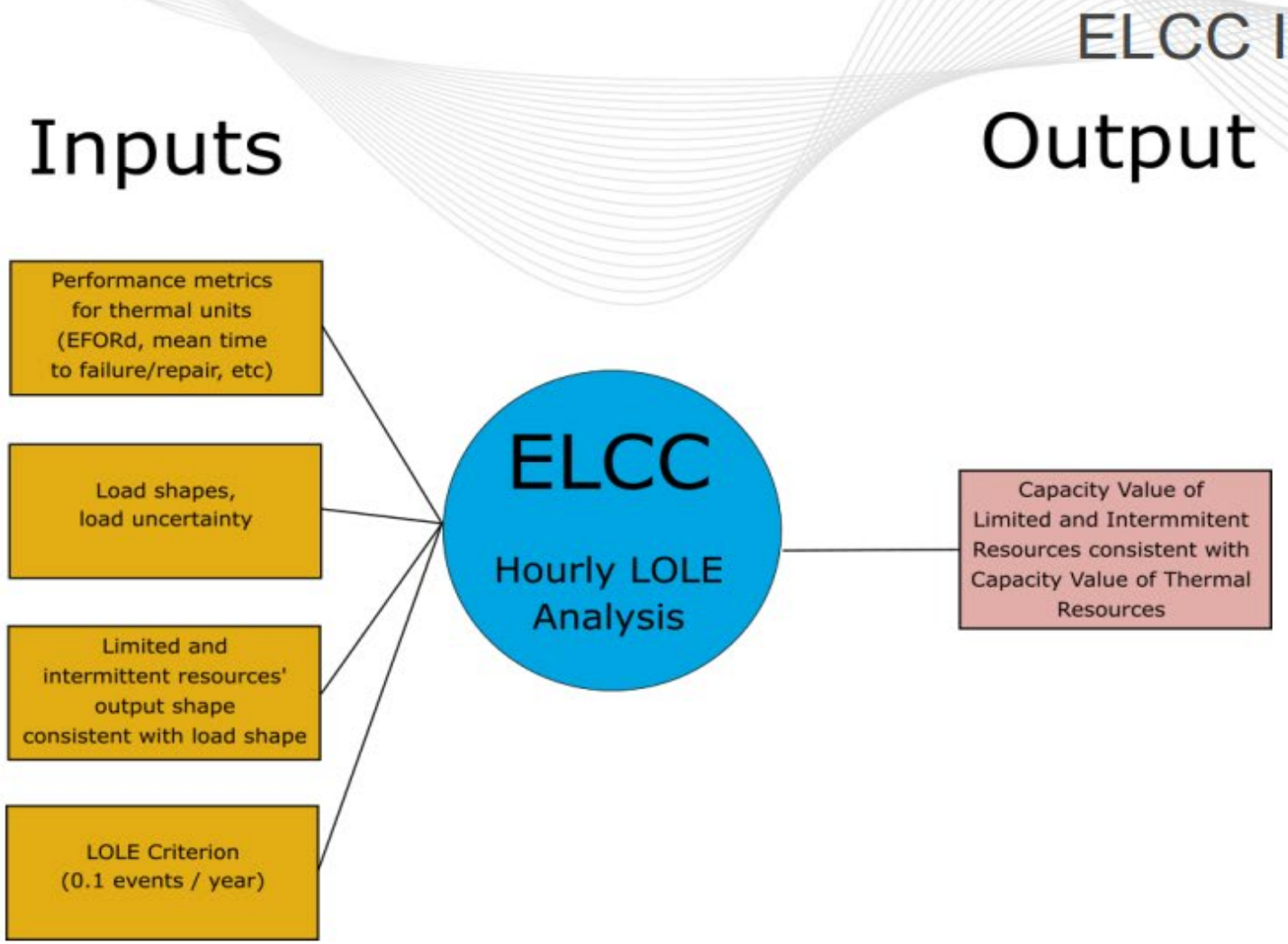


MISO Nameplate vs Capacity





PJM Effective Load Carrying Capability (ELCC)



https://www.pjm.com/-/media/committees-groups/task-forces/ccstf/2020/20200407/20200407-item-04-effective-load-carrying-capability.ashx

Effective Load Carrying Capability (ELCC)

- Variable resources are only counted partially for PJM resource adequacy studies
- Both wind and solar initially utilize class average capacity expected at the time of peak value
  - 13 percent for wind
  - 38 percent for solar
- Performance over the peak period (typically for three years of operation) is used to determine a unit's individual capacity
- Biomass and hydro are typically counted at full capacity

MISO ELCC

Effective Load Carrying Capability (ELCC)

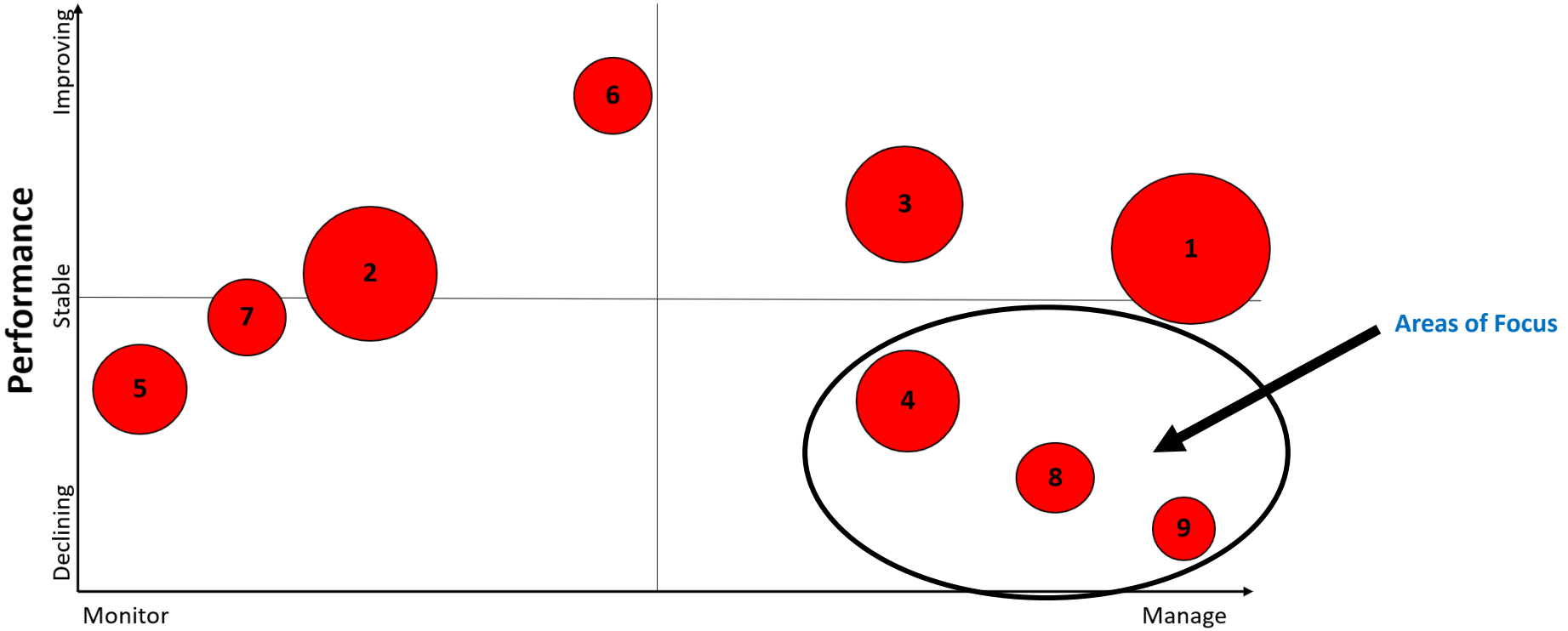
- MISO utilizes a probabilistic approach with inputs regarding historical output to calculate ELCC for wind resources
  - 15.5 percent for wind
- MISO has begun discussion on the possibility of using the ELCC calculation for Solar resources and this is still in the stakeholder review process
  - 50 percent for solar

- All other Non-wind intermittent resources use 15 years of historical summer output

ReliabilityFirst Risks

List of Risk Categories
Misoperations
Cyber/Physical Security
Human Performance
Environmental Factors
Unknowns & Uncertainty
Event Response/Resilience
Situational Awareness
Changing Generation Mix
Planning & Modeling

Assessing Regional Risk



Gather information or develop metrics to track performance for a specific risk

Actively engage stakeholders to drive performance improvement for risk categories

1. **Misoperations**
2. **Cyber/Physical Security**
3. **Human Performance**
4. **Environmental Factors**
5. **Unknowns & Uncertainty**
6. **Event Response/Resilience**
7. **Situational Awareness**
8. **Changing Generation Mix**
9. **Planning & Modeling**

Strong Regions + Strong NERC = Brilliant ERO

Enhancing the Assessment of Regional Risks

- ReliabilityFirst staff and our Committee and Subcommittees will begin to collaborate on:
  - Identify risks that may have a higher probability of occurrence and/or impact within the ReliabilityFirst footprint
  - Assess the resulting risks in terms of impact and likelihood
  - Build in a feedback loop into our RRA

Energy Availability in 3 Timeframes

Mid-to-Long Term

(1-5 years)

- Ensure that resources are planned that can provide options to obtain sufficient and flexible energy resources
- Review tools, rules-of-thumb and processes to support the need for these energy resources

Operational Planning

(1 day – 1 year)

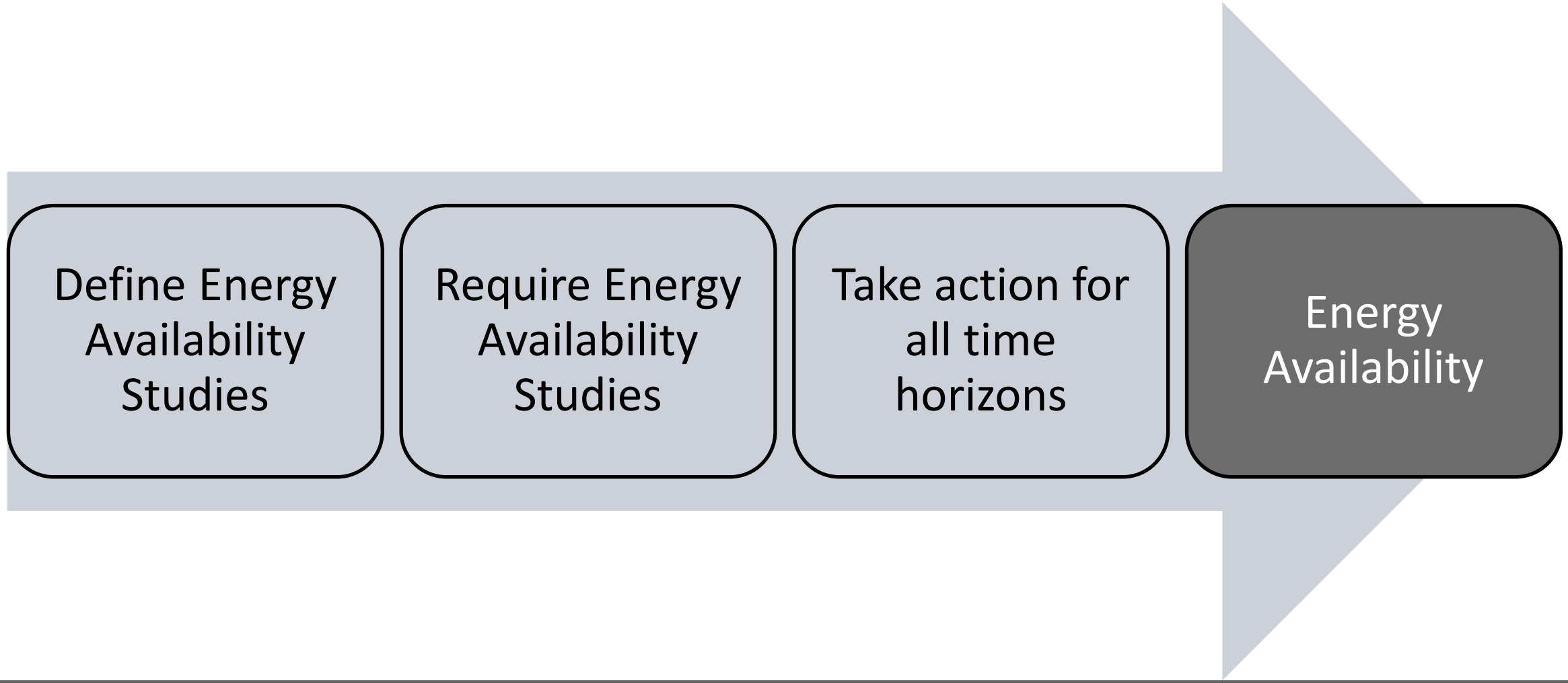
- Ensure sufficient resources are available and able to provide energy to meet demand and offset ramping requirements
- Electrical energy production needs to reflect status of energy availability given the uncertainties

Real-Time

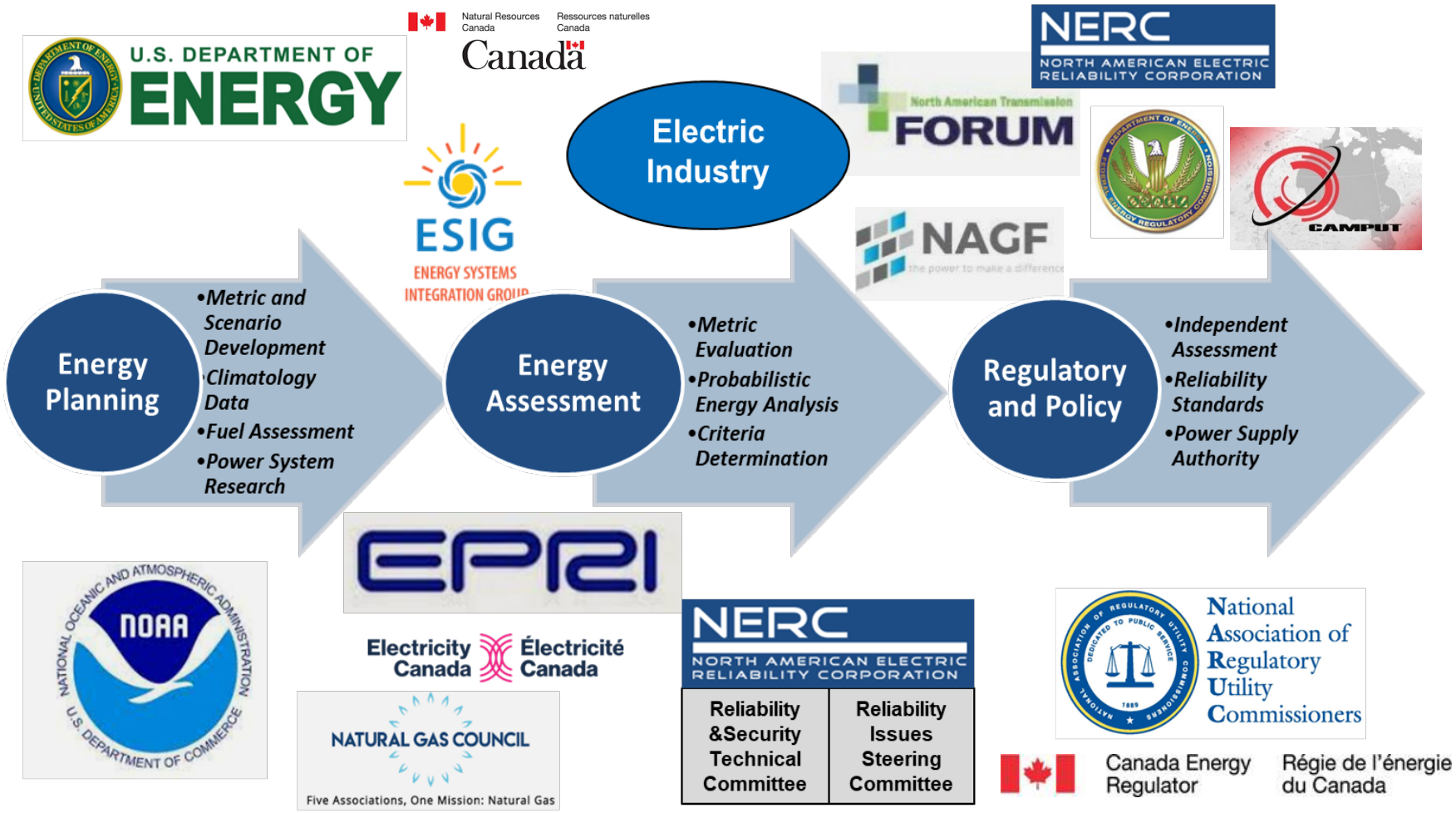
(0-1 day)

- Ensure sufficient amounts of capacity, energy, and ramp flexibility are available from available resources

What MUST Be Done?



Partners to Get Us There

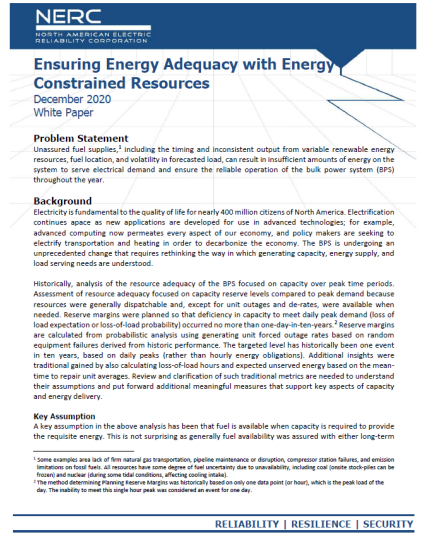


Strong Regions + Strong NERC = Brilliant ERO

New NERC Industry Group

Energy Reliability Assessments Task Force (ERATF)

Utilities	ISOs/RTOs	EPRI	Manufacturers	ERO



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Ensuring Energy Adequacy with Energy Constrained Resources
December 2020
White Paper

Problem Statement
Unassured fuel supplies,[1] including the timing and inconsistent output from variable renewable energy resources, fuel location, and volatility in forecasted load, can result in insufficient amounts of energy on the system to serve electrical demand and ensure the reliable operation of the bulk power system (BPS) throughout the year.

Background
Electricity is fundamental to the quality of life for nearly 400 million citizens of North America. Electrification continues apace as new applications are developed for use in advanced technologies; for example, advanced computing now permeates every aspect of our economy, and policy makers are seeking to electrify transportation and heating in order to decarbonize the economy. The BPS is undergoing an unprecedented change that requires rethinking the way in which generating capacity, energy supply, and load serving needs are understood.

Historically, analysis of the resource adequacy of the BPS focused on capacity over peak time periods. Assessment of resource adequacy focused on capacity reserve levels compared to peak demand because resources were generally dispatchable and, except for unit outages and de-rates, were available when needed. Reserve margins were planned so that deficiency in capacity to meet daily peak demand (loss of load expectation or loss-of-load probability) occurred no more than one-day-in-ten-years.[2] Reserve margins are calculated from probabilistic analysis using generating unit forced outage rates based on random equipment failures derived from historic performance. The targeted level has historically been one event in ten years, based on daily peaks (rather than hourly energy obligations). Additional insights were traditional gained by also calculating loss-of-load hours and expected unserved energy based on the mean-time to repair unit averages. Review and clarification of such traditional metrics are needed to understand their assumptions and put forward additional meaningful measures that support key aspects of capacity and energy delivery.

Key Assumption
A key assumption in the above analysis has been that fuel is available when capacity is required to provide the requisite energy. This is not surprising as generally fuel availability was assured with either long-term

[1] Some examples area lack of firm natural gas transportation, pipeline maintenance or disruption, compressor station failures, and emission limitations on fossil fuels. All resources have some degree of fuel uncertainty due to unavailability, including coal (onsite stock-piles can be frozen) and nuclear (during some tidal conditions, affecting cooling intake).
[2] The method determining Planning Reserve Margins was historically based on only one data point (or hour), which is the peak load of the day. The inability to meet this single hour peak was considered an event for one day.

RELIABILITY | RESILIENCE | SECURITY

Strong Regions + Strong NERC = Brilliant ERO

Industry Input Received

- What do we do with high impact, low likelihood energy assessments?
- Energy assessments need to be performed throughout the year, not just for peak cases
- Geographical nuances to reliability issues related to energy availability
- Dependency on other critical infrastructure is a key aspect of this risk, and there is a likely need to model fuel infrastructure
- Need to create metrics and criteria for energy assessments
- Assumptions used in studies must be a focus, and various scenarios considered including extreme events
- Assessments need to be considered in the operational timeframe as well, not just long-term planning

Actions Taken

- Industry workshop held to discuss feedback and survey results
- Reviewed current NERC Standards against this risk
  - Determined need for new Standards related to both real-time operations and planning

Recent and Next Steps

- May 2022 – Review industry comments and proposed responses at NERC MRC (Members Representative Committee)
- May 2022 – Hold an outreach conference on the proposed responses to industry comments and update the SAR (Standard Authorization Request)
- June 2022 – NERC RSTC (Reliability and Security Technical Committee) SAR endorsement
- June or July 2022 – NERC Standards Committee SAR acceptance
- July 2022 – Solicit industry volunteers for Standard Drafting Teams

Questions and Answers

Break

See you back at 3:00 for a presentation from Robert Lee from Dragos, Inc.

Join the conversation at

Slido.com

#RFWorkhshop

Break – Please Return at 3:00 pm Eastern

WECC

Resource Adequacy Discussion Series

The Future of Storage
October 5 Registration

Spanning the Technology Gap
November 2 Registration

Reliability & Security Workshop
October 25-26 Registration

MIDWEST RELIABILITY ORGANIZATION

Security Conference Training
October 4-5 Registration

Cold Weather Preparedness Workshop
October 12 Registration

NPCC, Inc.

Compliance and Reliability Conference
November 9-10 Registration

RELIABILITYFIRST

Technical Talk with RF October 24
NERC / E-ISAC GridSecCon October 18-19

TEXAS RE
Ensuring electric reliability for Texans

Fall Standards, Security, and Reliability Workshop
October 27 Registration

Talk with Texas RE: CIP-008
November 8 Registration

SERC Reliability Corporation

Fall Reliability & Security Seminar
October 4-5 Registration

Extreme Weather Webinar
October 20 Registration

Guest Speaker

Robert Lee
CEO and Co-Founder, Dragos, Inc.

Electricity Threat Landscape

Matt Duncan
Director, Intelligence, E-ISAC

A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

Electricity Threat Landscape and CIP-008 Submission Considerations

Matthew Duncan, Director, Intelligence

ReliabilityFirst (RF) Reliability and Compliance Workshop

September 26, 2022

TLP:WHITE

RELIABILITY | RESILIENCE | SECURITY

Agenda

- E-ISAC Overview
- Electricity Threat Landscape
  - Cyber Threats
  - Physical Threats
- CIP-008-6 Submission Considerations
- Collective Defense Actions

E-ISAC OVERVIEW

Engagement

Information Sharing

Analysis

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER
A Division of NERC

E-ISAC CRISP
CYBERSECURITY RISK INFORMATION SHARING PROGRAM

E-ISAC Membership

Active Member and Partner Orgs:	**2022 YTD New Orgs (8%↑):**	**E-ISAC/RF Joint Orgs:**
1,496	87 Members 30 Partners	176 Members (14% of all E-ISAC members)

Threat Landscape - Overview

- Primary member shares with E-ISAC = Phishing
- Exploitation of legacy vulnerabilities (LOG4SHELL)
- Supply Chain / Managed Service Provider (MSP) threats
- Industrial code research by ransomware operators
- Domestic Violent Extremism

Threat Landscape - Geopolitical

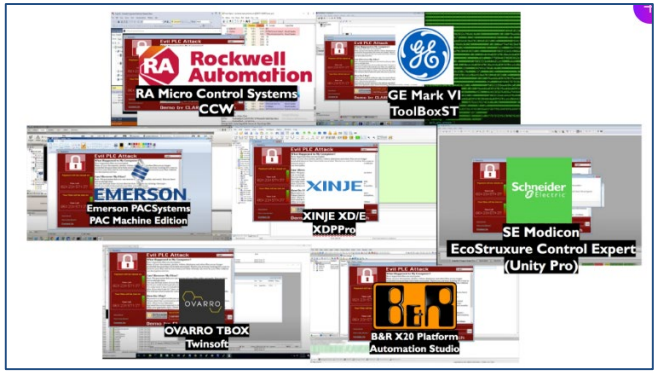
China

- Tension over U.S. Congressional visits to Taiwan
- Ongoing Log4j scanning and exploitation
- New groups scanning renewable industry
  - KOSTOVITE (Dragos) overlap with UNC2630 (Mandiant)

Russia

- Industroyer2 malware discovered in Ukraine
- ICS 'Swiss Army Knife' – Incontroller (Mandiant) Pipedream (Dragos)
- Ransomware groups support of Russia
- APT29 (SVR) ongoing activities against Microsoft
- APT28 (GRU) Historic Destructive Attacks

Threat Landscape – Operational Technology

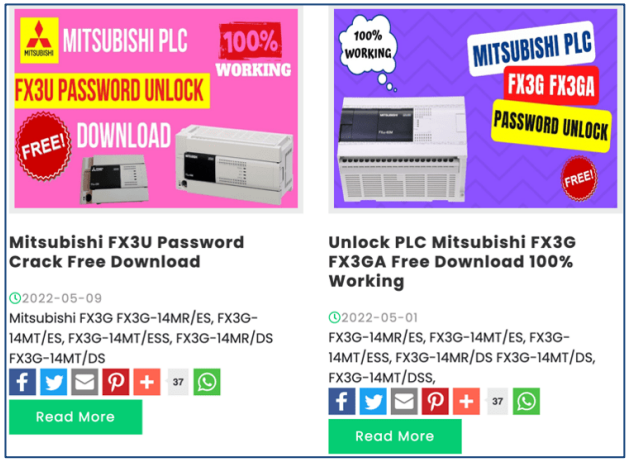


Claroty "Evil PLC" *proof of concept attack*

Image Source: Claroty T82

European ***Wind Turbine Cyber*** *Events*

Image Source: Bing Creative Commons



Sality malware ICS *'password cracker' –*

Image Source: Dragos

Threat Landscape – Ransomware

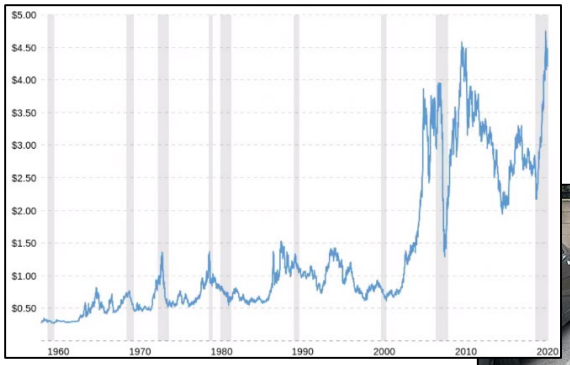
- Ransomware operator research of industrial code (FBI)
- **Manjusaka Framework** observed
- **Yanluowang Ransomware** and Cisco compromise
- **Luxembourg Energy Company** attack – BlackCat/ALPHV

Source: Cisco Talos

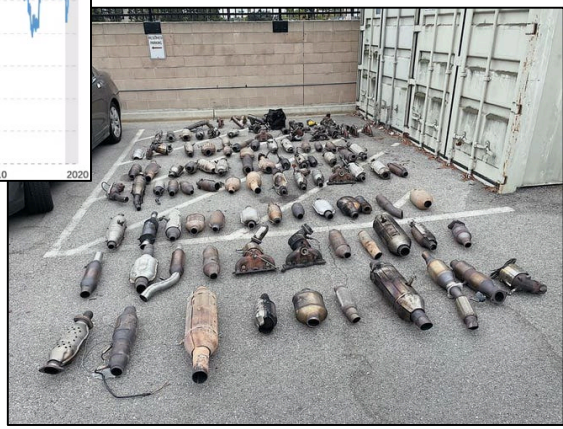
Source: Bleeping Computer

Threat Landscape – Physical

- **Theft**
  - Copper
  - Catalytic converters
  - Safety
  - Damage
- **Vandalism**
  - Safety
  - Damage
- **Ballistic Damage**
  - Transmission Lines
  - Transformers



Courtesy of Macrotrends



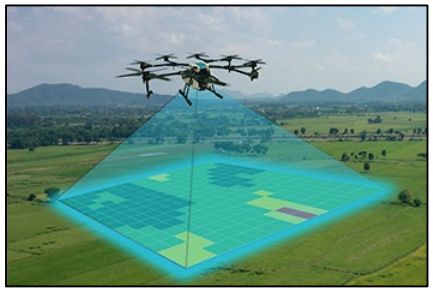
Courtesy of Torrance Police Department via USAToday

Courtesy of RTE

Activist Manual

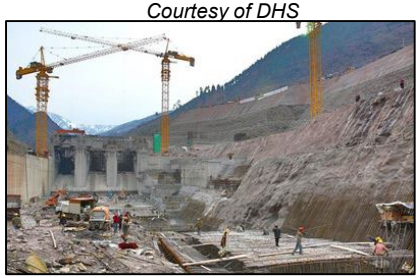
Threat Landscape – Physical

- **Emerging Threats**
  - Drones
  - Cyber-Physical
- **Activism**
  - Security response
  - New construction



Courtesy of DHS

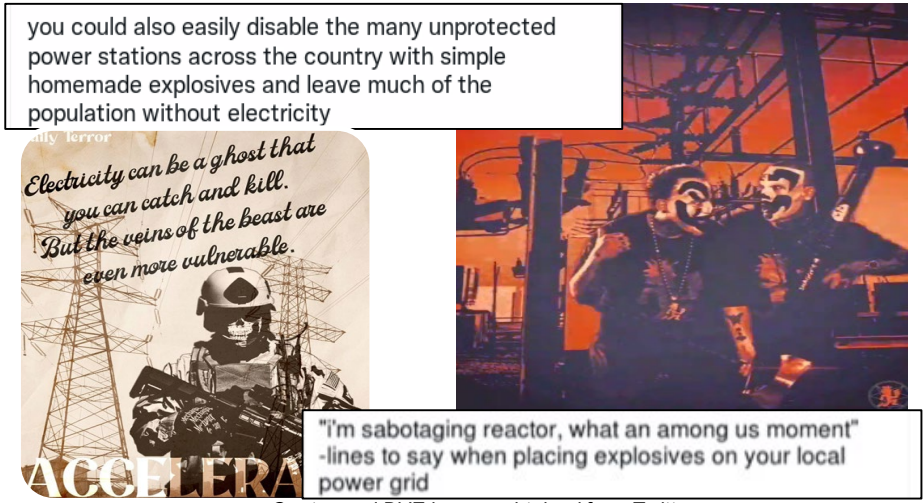
Vendor



Courtesy of HydroPower.org

Courtesy of The Irish Times

- **Lone Wolf / Small Group Action**
  - Targeting key assets
- **Civil Unrest**
  - Personnel in zone
  - Assets in zone
  - Cover for action



Quotes and DVE images obtained from Twitter

CIP-008-6 Requirements

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and NCCIC. Now "CISA"
4.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the "Applicable Systems" column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC. Now "CISA"

How to Submit a CIP-008 Report

- Submit to E-ISAC and CISA
- No required way to submit, many options:
  - E-ISAC: Email operations@eisac.com or call 202-790-6000
    - Will accept DOE-417, EOP-004, CISA Incident Form, Email, Portal Post, phone call
  - CISA: https://us-cert.cisa.gov/forms/report
  - TIP: **Fill out CISA Incident Reporting System Form and send E-ISAC the PDF**
- REQUEST – **Please label your submission "CIP-008 Report"**

CIP-008 Submission #1

From: [redacted]
Sent: Monday, May 10, 2021 5:02 PM
To: operations@eisac.com
Subject: Acme Utility Company NCRXXXXX SAMPLE US-CERT Report

US-CERT-Report.pdf
3 MB

As part of the NERC CIP-008- R4.2, we are informing of an attempt to compromise.

As part of patching the Pulse Secure VPN per AA21-110A, five system files were found to be mismatched at approximately 4:50 pm ET on May 10, 2021. While mitigation is in process, we wanted to provide a notice in accordance with CIP-008-6 R4.2.
There were no known impacts to any systems at this time.

Please contact me for further questions.

- **4.1.1 – Impact:** *"… no known impacts to any systems at this time."*
- **4.1.2 – Vector:** "… *Pulse Secure VPN per AA21-110A*"
- **4.1.3 – Level of Intrusion**: "*… five system files… mismatched*"

CIP-008 Submission #2

From: [redacted]
Sent: Friday, May 11, 2021 10:11 AM
To: operations@eisac.com
Subject: Acme Utility NCRXXXXX CIP-008 Report

E-ISAC,
We are informing you of an attempt to compromise of our EACMS in a Medium Control Center as part of the NERC CIP-008- R4.2. We also filled out the CISA incident report.

Functional Impact – none noted. Confirmed through analysis of OT Network logs and/or performance.
Attack Vector – Malicious software introduced via a trusted patch source. Investigation is ongoing.
Level of intrusion – At this time, we have identified it as a compromise and have found no indicators of compromise on the DMZ, location of the EACMS that the attempt was detected, or the OT network.

Please contact our SOC for further questions and follow-up.

- **4.1.1 – Impact:** *"… none noted. Confirmed through analysis of OT network logs and/or performance."*
- **4.1.2 – Vector: "***Malicious software introduced via a trusted patch source*."
- **4.1.3 – Level of Intrusion**: "*Compromise of our EACMS in a Medium Control Center*."

Collective Defense

- Rapid Information Sharing *24x7*
- Original Analysis and Threat Hunting
- CRISP
- Government Partnership
- Energy Threat Analysis Center (ETAC)
- Vendor Affiliate Program
- Collaboration with Natural Gas
- **You**

Questions and Answers

RELIABILITY FIRST

Engagement Timeline Adjustments

Zack Brinkman – Manager, CIP Compliance Monitoring






Overview

- **Drivers for Adjustments?**
- **Audit**
  - 270 Day Notification
  - 120 Day Audit Notification Letter
  - 30 Days to Review and Comment on Draft Report
- **Self Certification**
  - 60 Day Self Certification Notification Letter

Drivers for Change

➢ Audit Timeline

- Appendix 4C
  - Section - 4.1.1 Compliance Audit Process
  - Section - 4.1.5 Compliance Audit Report
- 120 Day Audit Notification Package
  - Allows for additional time for collaboration, evidence gathering, organization and review.

➢ Self-Certification Timeline

- Section - 4.2.1 Self Certification Process
  - At least sixty (60) days in advance, the CEA requests the Registered Entity to make a Self-Certification.

270 Day Audit Notification

- **What is this notification?**
- **Previous Process**
  - Notified before October 1st of proceeding year
- **New Process**
  - Rolling Calendar
  - 270 Day Notification – Start After April 1st
  - No longer Publicly Posting Audit Schedule

270 Day Notice	Audit Notification Letter	Onsite/Offsite Week
9/8/2022	2/1/2023	6/1/2023

120 Day Audit Notification Letter

➢ Previous Process

- 90 Day Notification Letter

➢ New Process Changes

- Notification letter will be sent 120 days prior to onsite/offsite week
- Extra Days will be split between Entity and RF

120 Day Notice	Evidence Due	Onsite/Offsite Week
2/1/2023	4/2/2023	6/1/2023

Comment Period

➢ Previous Process

- 10 Days to Review Draft Report

➢ New Process Changes

- Entity will be allotted 30 Calendar Days to Review Draft Report

Exit Presentation	Draft Report Due to Entity	Entity Returns Comments	Final Report to Entity
6/5/2023	7/30/2023	8/29/2023	9/13/2023

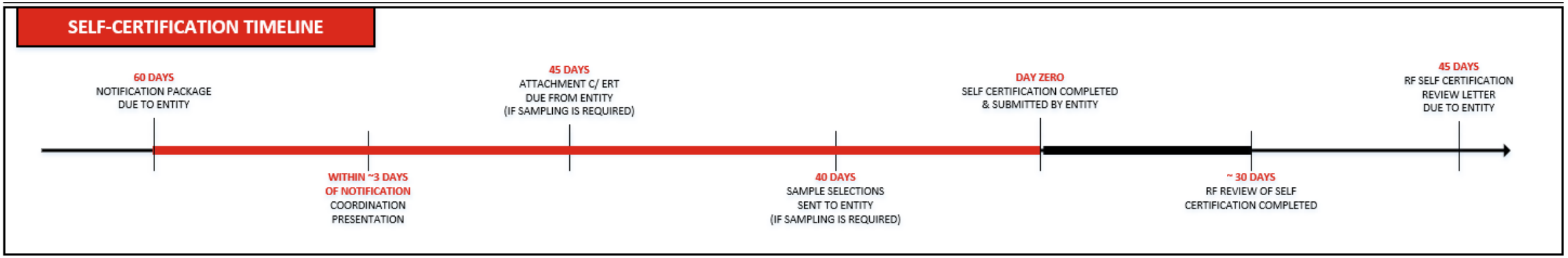
Self-Certification Timeline

➢ Previous Process

- Notification Package sent 30 Business Days prior to due date

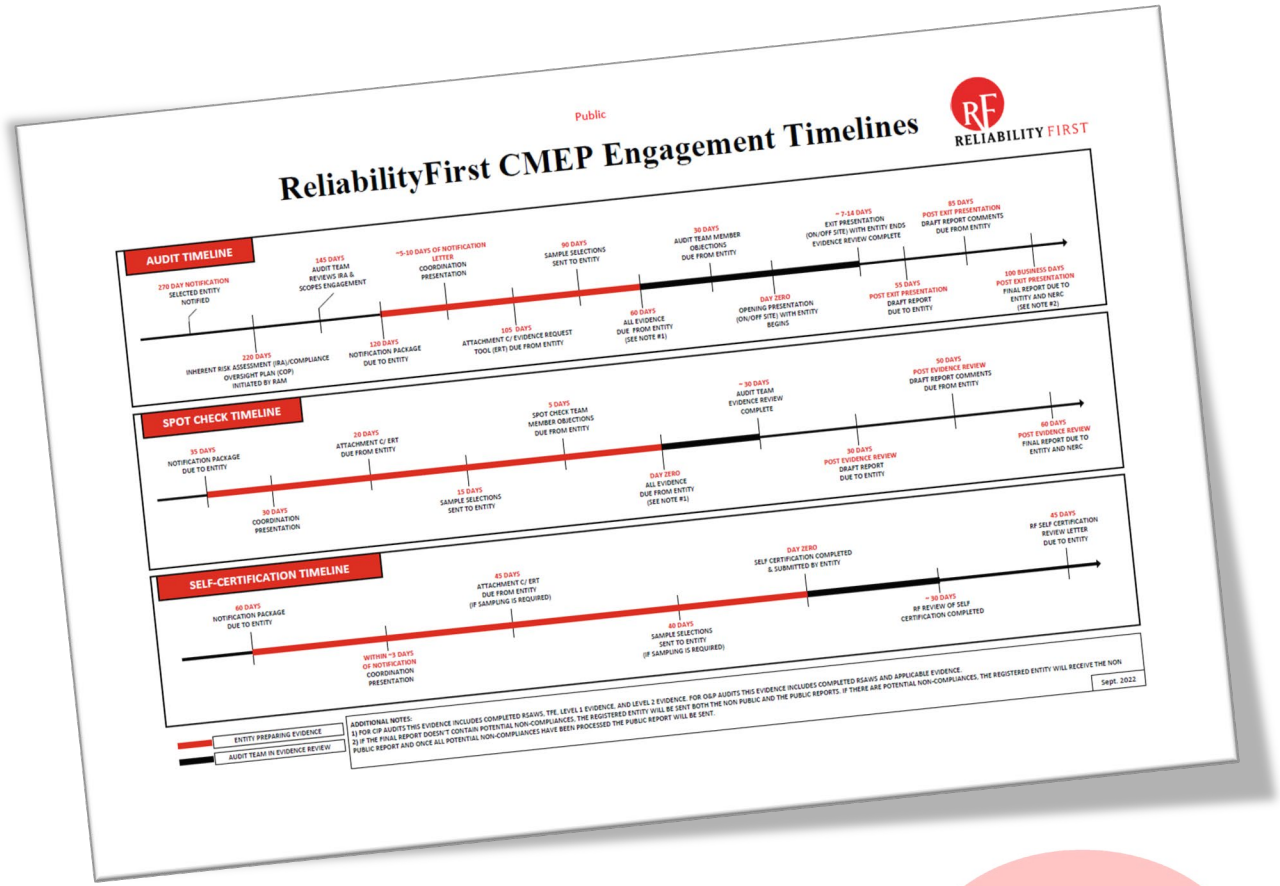
➢ New Process Changes

- Notification Package sent at 60 Days prior to due date
- Additional time given to Entity to submit Self-Certification



Review

- **Audit**
  - 270 Day Notification
  - 120 Day Audit Notification Letter
  - 30 Days to Review and Comment on Draft Report
- **Self Certification**
  - 60 Day Self Certification Notification Letter
- **Updated Timeline**
  - https://rfirst.org/ProgramAreas/COMO/ > Documents



Questions

Forward Together ReliabilityFirst

Trivia Giveaway Day 1

Please log into Slido now for the opportunity to win a $50 Amazon gift card!

- You have one minute from the time this slide is shown to enter your name into Slido before the question is asked.
- You must enter your first & last name; anonymous responders are not eligible to win.
- To win, you must answer the questions correctly and be the fastest respondent, as recorded in Slido.
- Prizes for the top five participants.

Slido.com
#RFWorkshop

Trivia Giveaway Winners

Thank you and congrats to today's five trivia winners!

To claim your $50 Amazon gift card, please email Jody Tortora at Jody.Tortora@rfirst.org.

Reception

Please join us at the Evening Reception, 5:00 – 7:00 Eastern held at the Courtyard by Marriott, Cleveland Independence located at:

5051 West Creek Road
Independence, OH 44131