

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Regulatory and Reliability Challenges During the Energy Transition – North American Perspective

Hugo F. Pérez, Manager of North American Relations (NERC)

October 27, 2022



To ensure the reliability and security of the North American Bulk Power System (BPS)

- Develop and enforce reliability standards
- Assess current and future reliability issues
- Analyze system events and recommend improved practices
- Critical Infrastructure Protection
- Education, training and awareness
- Accountable as Electric Reliability Organization (ERO) to regulatory bodies in the United States (FERC) and Canada (Canada Energy Regulator and provincial governments)

1965: Northeast blackout

1968: National Electric Reliability Council (NERC) established by the electric industry

1996: August 10th WSCC blackout; worst in the West

2002: NERC operating policy and planning standards become mandatory and enforceable in Ontario, Canada

2003: August 14th blackout; worst to date

2005: EPAct Section 215 Federal Power Act creates the Electric Reliability Organization (ERO)

2006: Federal Energy Regulatory Commission (FERC) certifies NERC as the ERO; Memorandums of Understanding (MOUs) with some Canadian Provinces

2007: North American Electric Reliability Council becomes the North American Electric Reliability Corporation (still NERC); FERC issues Order 693 approving 83 of 107 proposed reliability standards; reliability standards become mandatory and enforceable





- Interconnected grid with Canada and Mexico; each country with authority within their own jurisdiction
- Roughly 1500 owners, operators, and users of the BPS
 - Focus on reliable operation of the BPS
- Standards cannot require construction of new transmission or generation capacity
- Independent Board of Trustees
- All entities with a material interest in the reliability of the BPS can be NERC members
 - Member Representative Committee reports to the Board
- Six Regional Entities at the front line, performing delegated functions

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

2022 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Plan

Version 1.0
October 2021

RELIABILITY | RESILIENCE | SECURITY

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

The E-ISAC's Vision
To be a world-class, trusted source of quality analysis and rapid sharing of security information for the electric industry.

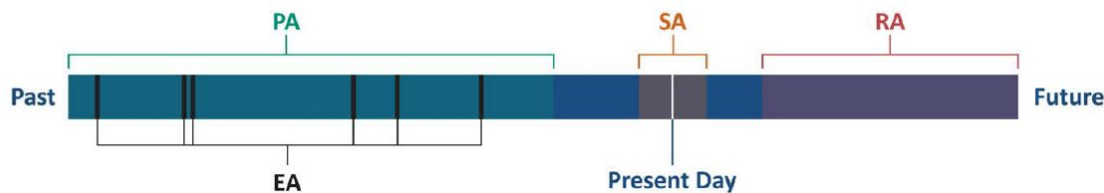
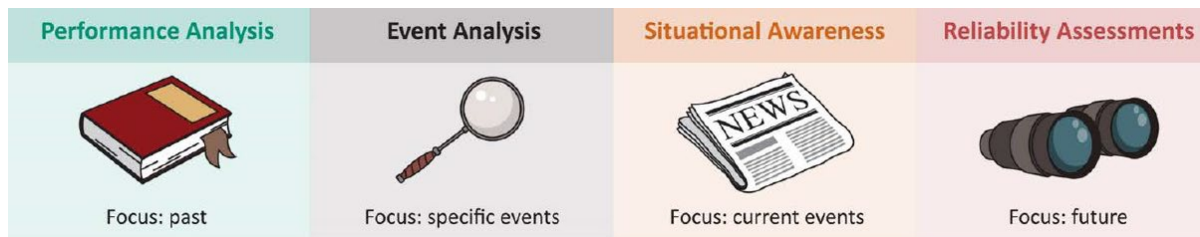
Products and Services

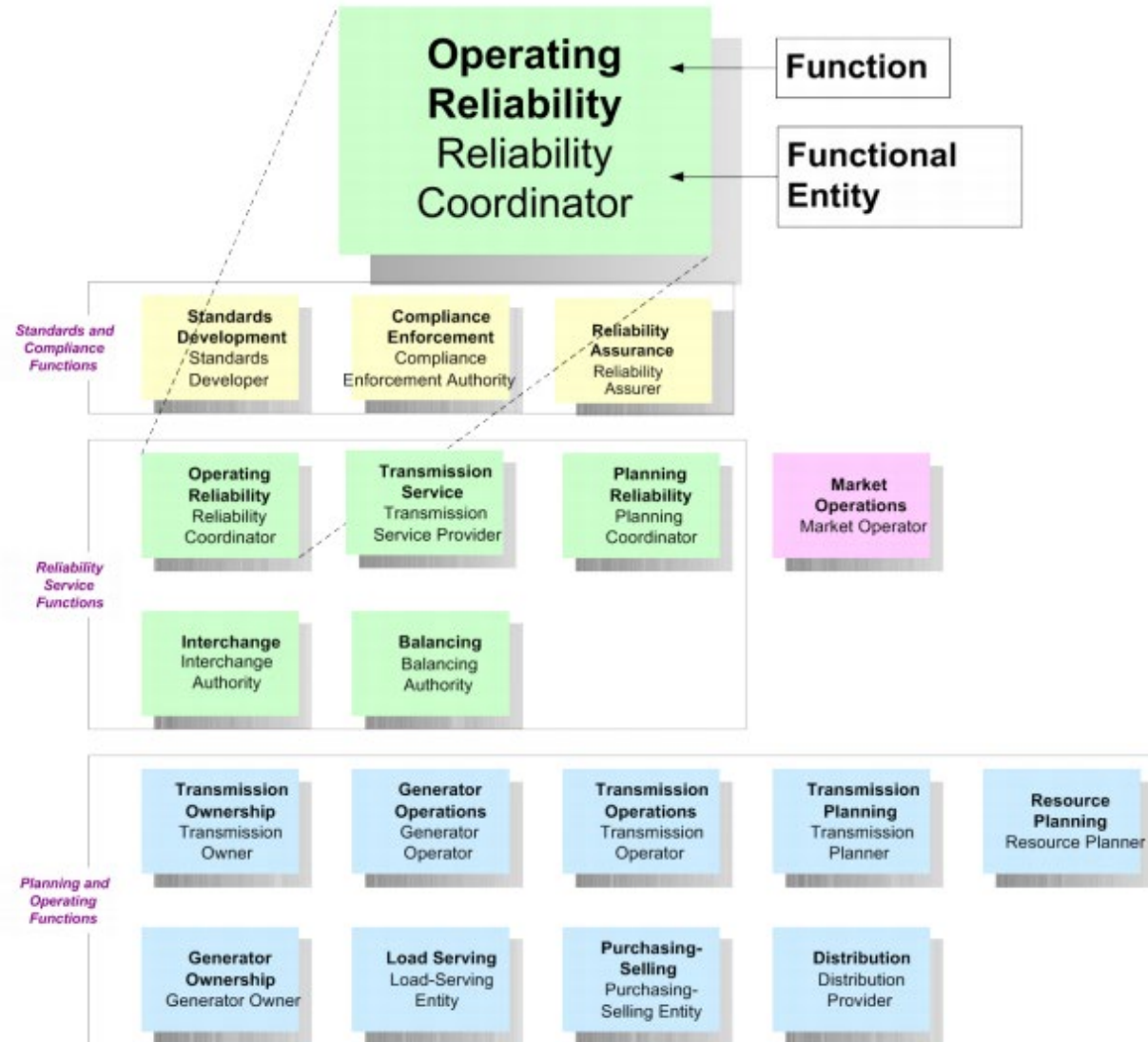
- Secure portal supporting collaboration in a virtual team environment
- Data analytics and analysis
- Reports focused at different levels from analysts to executives
- Cyber and physical bulletins
- Malware drop box
- Industry Engagement Program (IEP)
- Cross-sector shares
- Vulnerability reports
- Monthly webinars
- Critical Broadcast Program
- Unclassified threat workshop
- Biennial grid security exercise (GridEx)
- Annual grid security conference (GridSecCon)
- Cybersecurity Risk Information Sharing Program (CRISP)
- Cyber Automated Information Sharing System (CAISS)

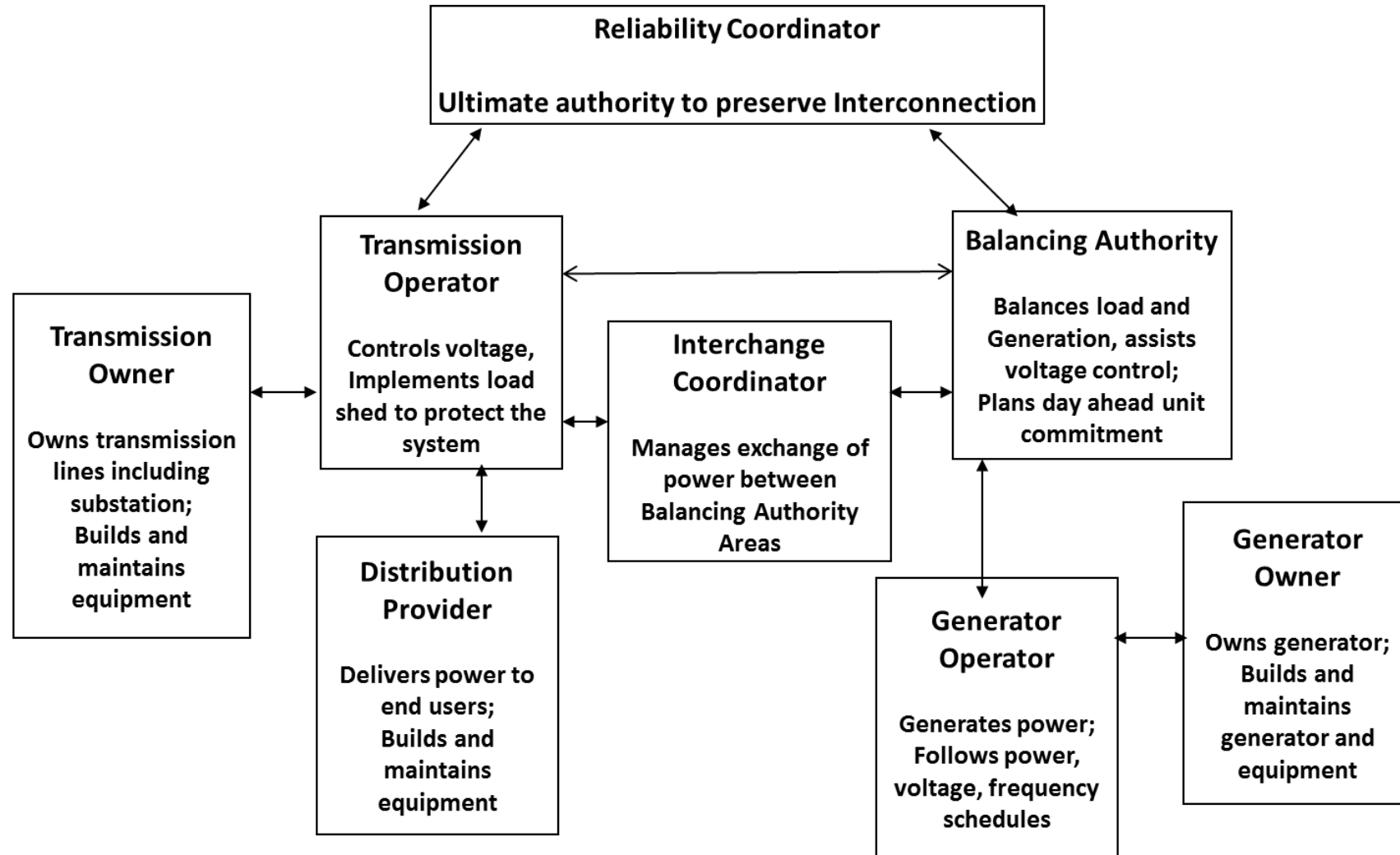
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

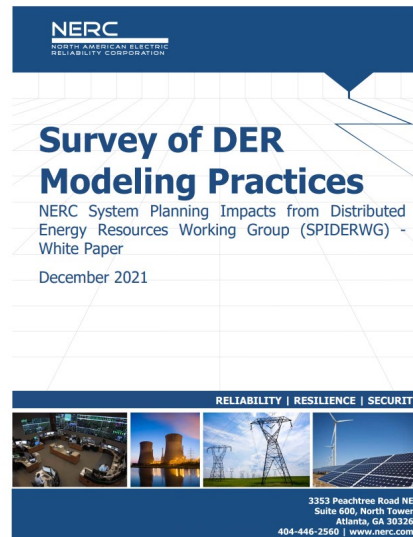
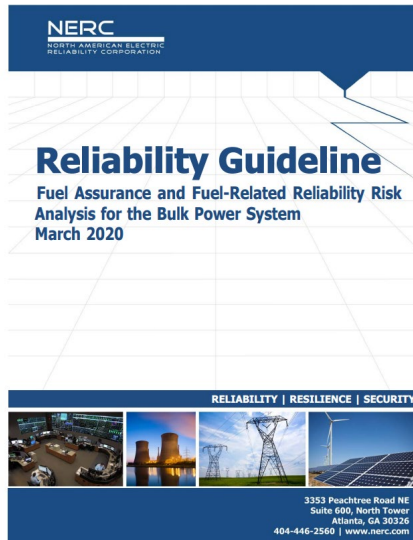
1325 G Street NW, Suite 600
Washington, D.C. 20005
24/7 Operations Desk: 202-790-6000
Email: operations@eisac.com
Portal: www.eisac.com

- Standards
- Compliance & Enforcement
- Reliability Risk Management
- Reliability Assessment and System Analysis
- System Operator Certification and Continuing Education
- Electricity Information Sharing and Analysis Center (E-ISAC)



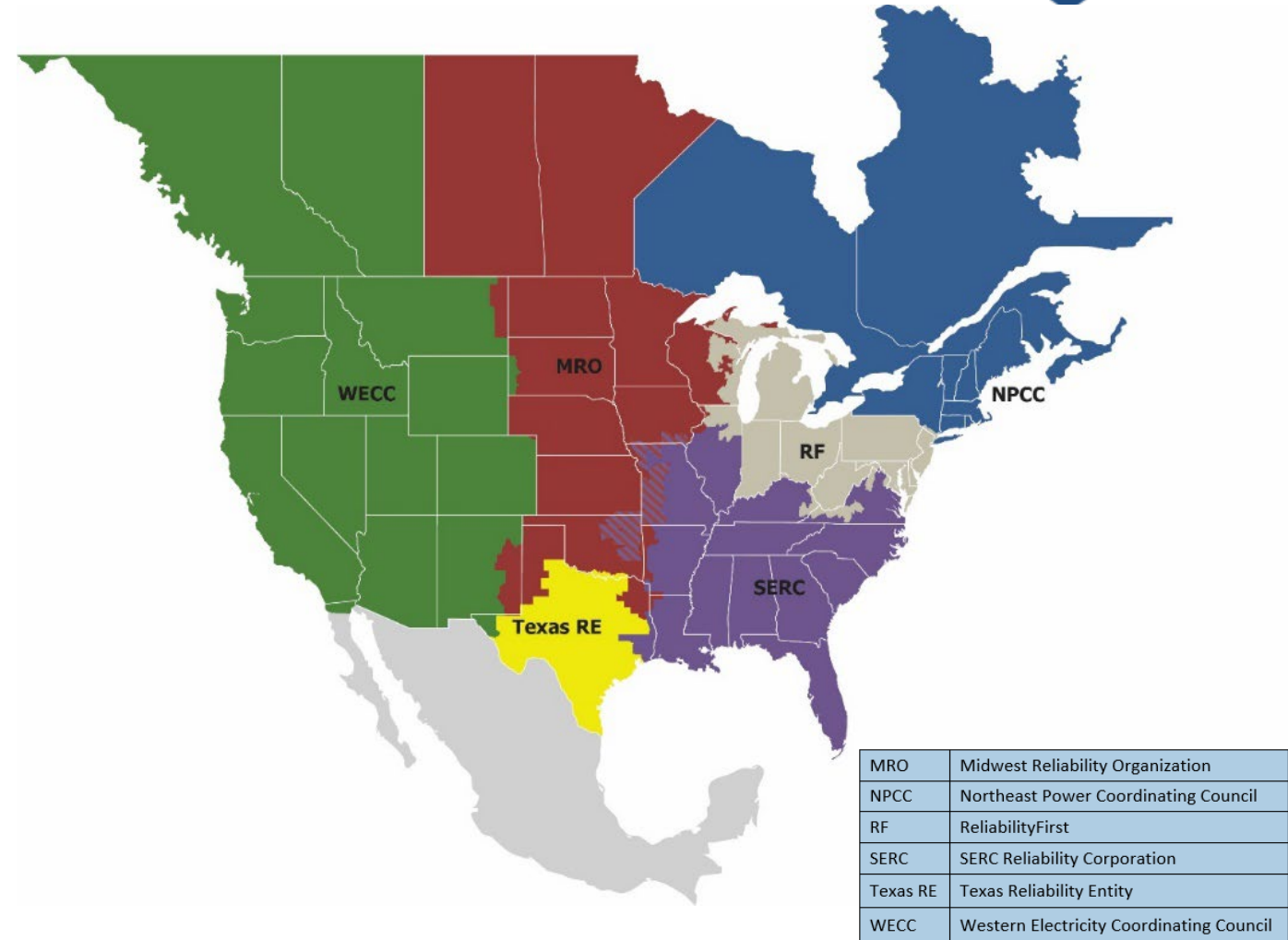






- Through NERC’s technical committees, experts from all segments of the electricity industry contribute their knowledge to promote the reliability of the North American BPS
 - Compliance and Certification Committee (CCC)
 - Personnel Certification Governance Committee (PCGC)
 - Reliability and Security Technical Committee (RSTC)
 - Reliability Issues Steering Committee (RISC)
 - Standards Committee (SC)

- NERC provides delegated authority to Regional Entities (REs)
- Delegated functions:
 - Compliance Monitoring and Enforcement
 - Reliability Standards Development
 - Organization Registration
 - Reliability Assessments and Performance Analysis
 - Training and Education
 - Situation Awareness
 - Infrastructure Security
- Regional consistency is key for transparency and predictability



NERC Compliance Registry Summary of Entities and Functions as of October 03, 2022*																
Regional Compliance Enforcement Authority****	BA	DP		GO	GOP	PA/PC	RC	RP	RSG	FRSG	RRSG	TO	TOP	TP	TSP	Entities
		DP	DP-UFLS													
MRO	19	61	13	150	147	4	3	51	2	0	0	77	37	47	8	229
NPCC	6	35	19	125	124	6	5	6	3	0	0	45	18	24	14	206
RF	13	46	3	192	198	2	2	17	1	0	0	40	16	14	2	274
SERC	34	82	12	179	161	28	8	47	7	0	0	71	43	43	23	279
Texas RE	1	21	15	232	185	1	1	1	0	0	0	31	20	27	1	303
WECC	34	72	8	298	254	32	2	50	2	1	0	79	47	63	34	407
Totals	107	317	70	1176	1069	73	21	172	15	1	0	343	181	218	82	1698

NERC Compliance Registry Summary of Unique Entities and Functions as of October 03, 2022*****																
BA	DP		GO	GOP	PA/PC	RC	RP	RSG	FRSG	RRSG	TO	TOP	TP	TSP	Entities	
	DP	DP-UFLS														
104	310	70	1115	990	69	16	166	13	1	0	333	175	211	78	1594	

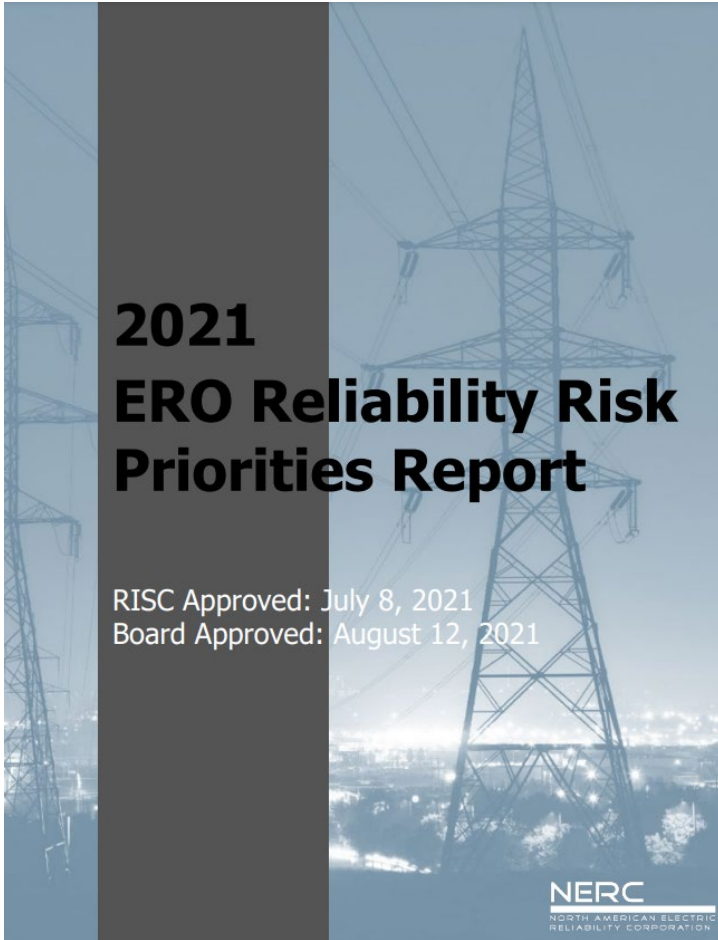
*This table does not reflect the physical location of the listed entities or functions. It reflects the Regional CEA responsibility for compliance monitoring.

** Frequency Response Sharing Group

*** Regulation Reserve Sharing Group

****This table counts Entities and Functions multiple times when said Entities or Functions span more than one Regional CEA's jurisdiction.

*****This table counts each Entity and Function once regardless of how many Regional CEA jurisdictions it may span.



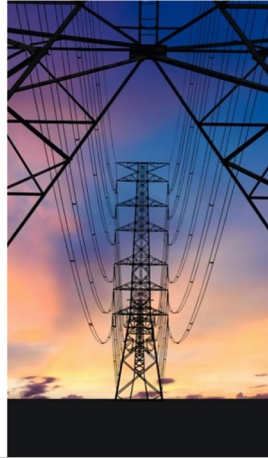
Risk Ranking





Energy: Tackle the challenge of grid transformation and climate change-driven, extreme weather

- More in-depth BPS situation awareness
- Expanded analytics and modeling
- Responsive emerging risk mitigation



Security: Move the needle by focusing supply chain, IT/OT system monitoring, cyber design, and evolution of the CIP Standards

- An expanded, stronger E-ISAC
- A more secure, less vulnerable BPS
- A more secure, less vulnerable NERC



Agility: Tool the company to be more nimble in key areas, particularly in BPS risk identification and tracking and standards development

- Comprehensive risk registry
- Efficient enforcement program
- Mitigation of emerging risks BEFORE a crisis

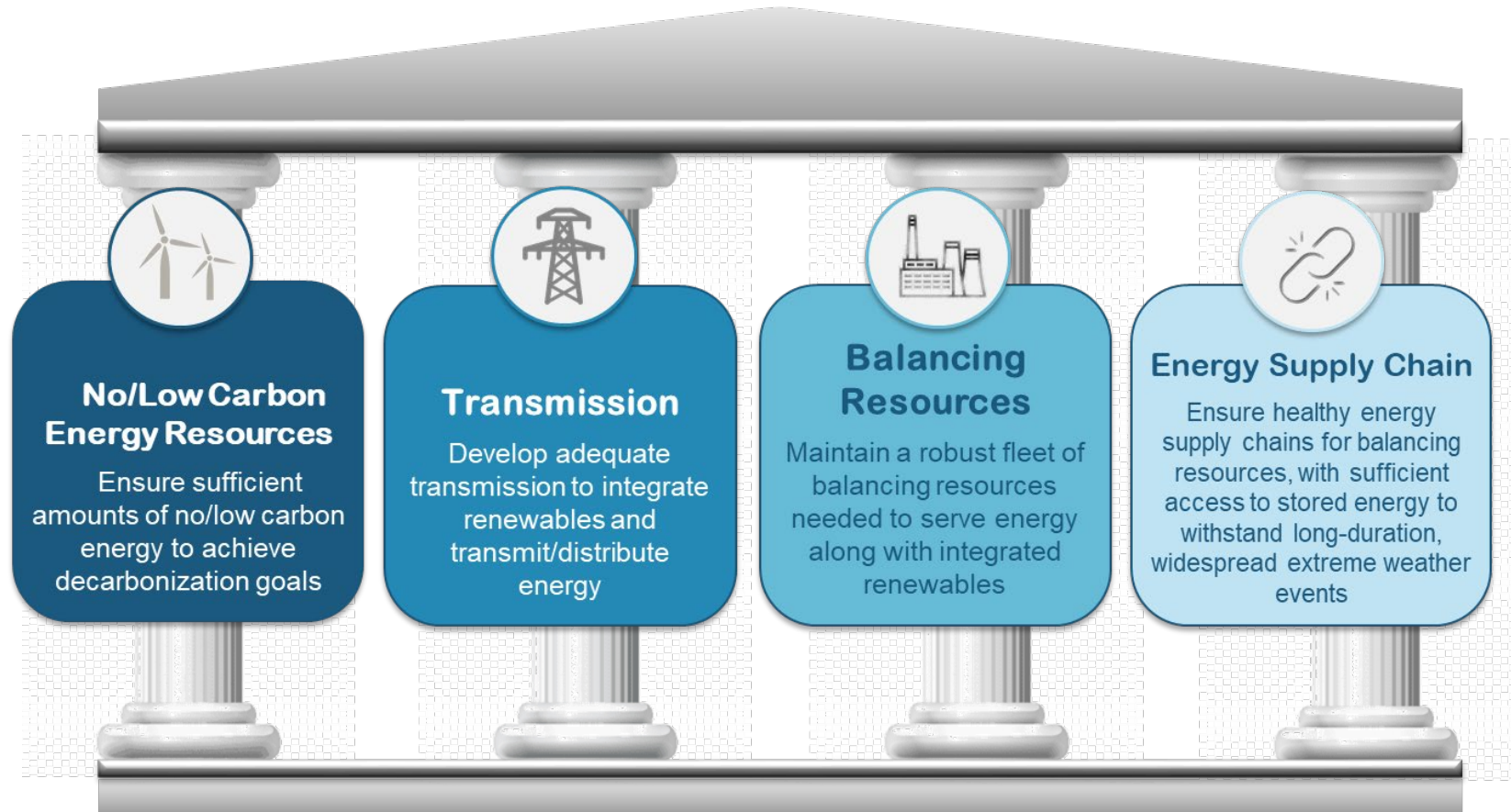


- Improve Bulk Electric System (BES) resilience for wide-spread long-term extreme temperature events
- Deepen planning and operating focus beyond capacity adequacy, towards energy sufficiency
- Enhance and develop new Standards: cyber (bright-line criteria), weatherization, energy sufficiency and inverter performance
- Expand the impact of the E-ISAC through enhanced information sharing, communications, and monitoring of critical security threats

- 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



Four Pillars of the Energy Transition



The Challenge: Sufficient Energy Availability





Mid-to-Long Term (1-5 years)

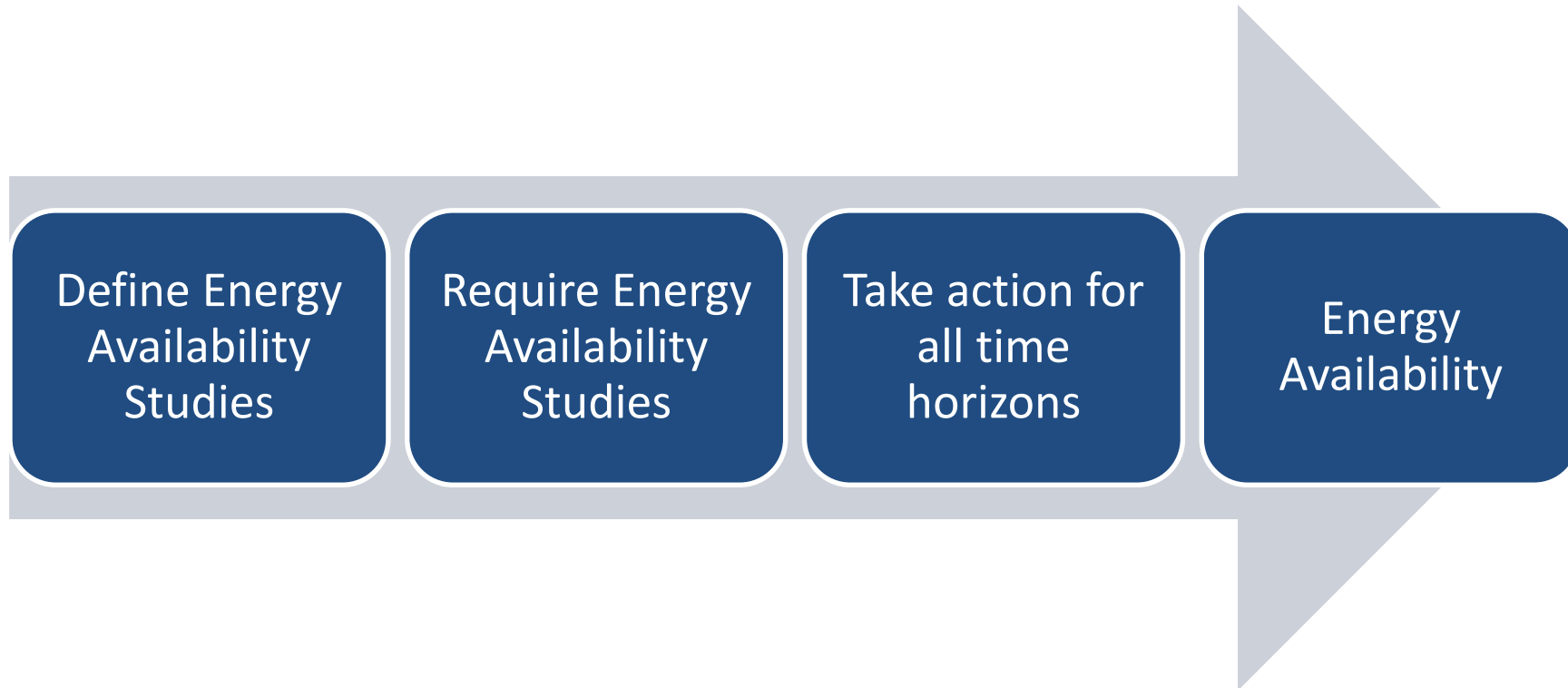
- Ensure that resources are planned that can provide options to obtain sufficient and flexible energy resources
- Review tools, rules-of-thumb and processes to support the need for these energy resources

Operational Planning (1 day – 1 year)

- Ensure sufficient resources are available and able to provide energy to meet demand and off-set 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





Reliability Guideline

Suggested approaches or behavior in a given technical area for the purpose of improving reliability. Guidelines are not enforceable, but may be adopted by a responsible entity in accordance with its own policies, practices, and conditions.



NERC Alert: Level 2-3

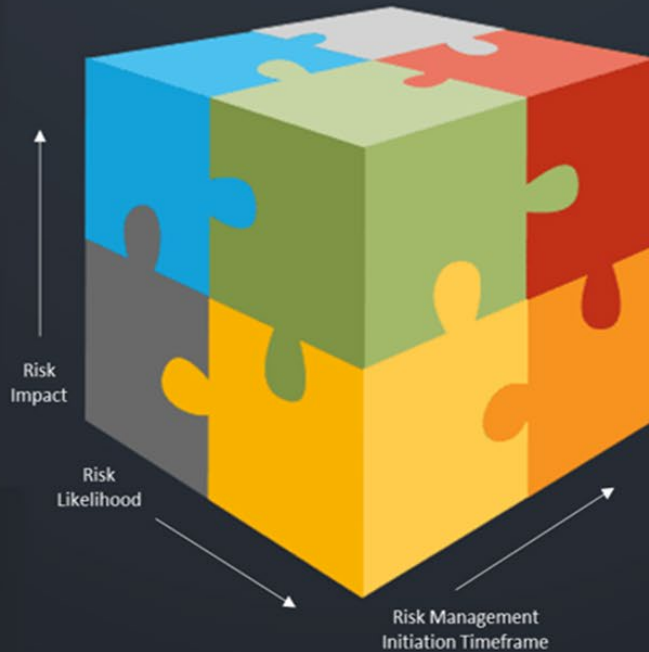
NERC alerts are divided into three distinct levels, 1) Industry Advisory, 2) Recommendation to Industry, and 3) Essential Action, which identifies actions to be taken and require the industry to respond to the ERO.



Technical Engagement

Technical Engagement is a catch-all for a variety of technical activity that is conducted between the ERO and entities. This includes, technical committee activities, technical reference documents, workshops and conferences, assist visits, joint and special studies, etc.

Electric Reliability Organization: Reliability Risk Mitigation Toolkit



Reliability Standards



NERC Reliability Standards define the mandatory reliability requirements for planning and operating the North American BPS and are developed using a results-based approach focusing on performance, risk management, and entity capabilities.

Reliability Assessment

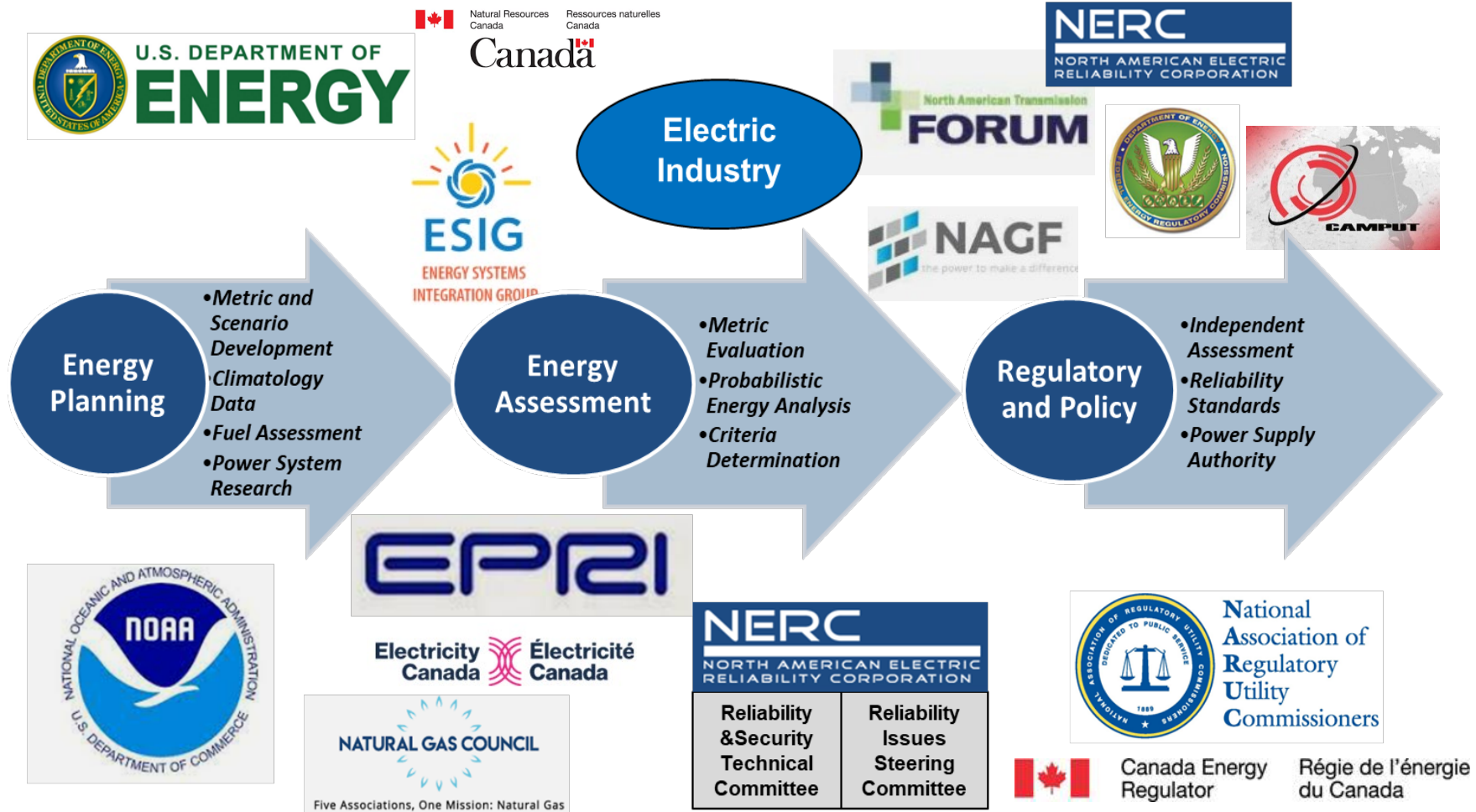


NERC independently assesses and reports on the overall reliability, adequacy, and associated risks that could impact BPS reliability. Long-term assessments identify emerging reliability issues that support public policy input, improved planning and operations, and general public awareness.

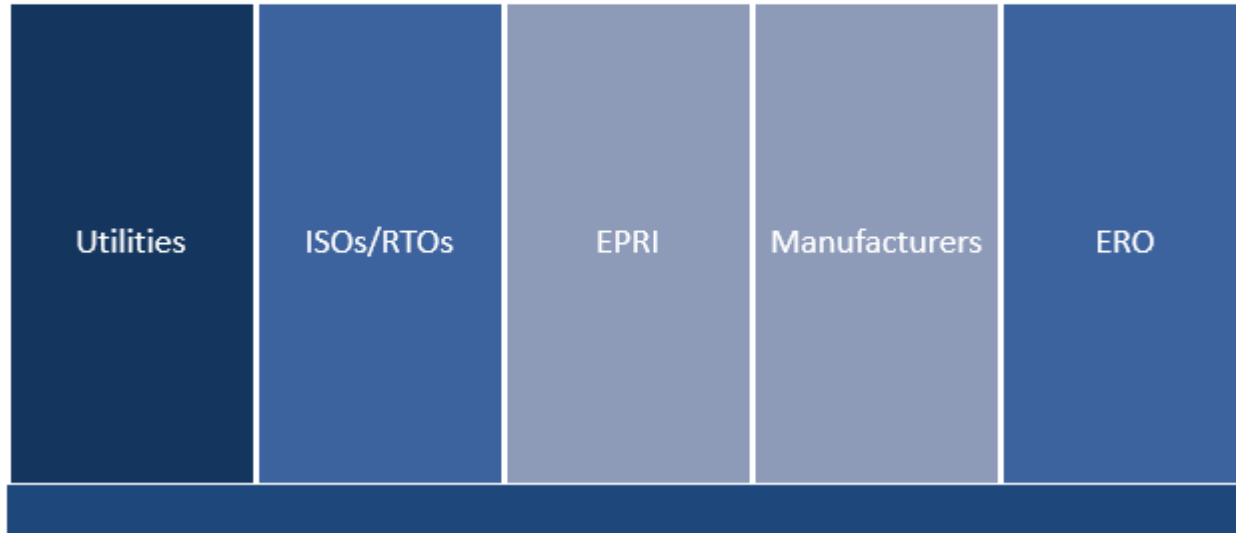
NERC Alert: Level 1



NERC Alerts are divided into three distinct levels, 1) Industry Advisory, 2) Recommendation to Industry, and 3) Essential Action, which identifies actions to be taken and require the industry to respond to the ERO.



Energy Reliability Assessments Task Force (ERATF)



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 (on-site stock-piles can be frozen) and nuclear (during some tidal conditions, affected intake).
² The method determining Planning Reserve Margins was 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

SURVEY

- 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

- 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**

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

Integrating Cyber and Physical Security for a More Reliable, Resilient, and Secure Energy Sector



- Supply chain threats continue to pose significant risk to the BPS
- Efforts underway to improve security posture of overall supply chain ecosystem
 - Suppliers, vendors, consultants, and other related parties that interact with and provide services or products to registered entities
- Risk of access to systems, equipment, environments, information, and data by malicious threat actors
 - Nation-states with high levels of sophistication and resources continue to be a key challenge

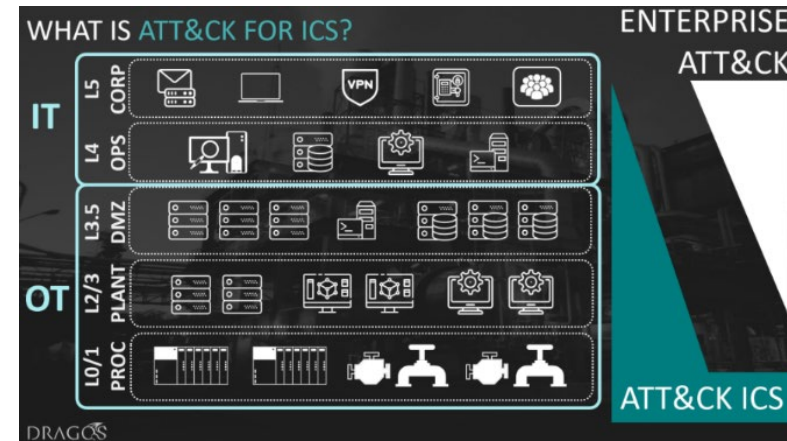


- Organizational IT/OT convergence
- IT tools, architectures, capabilities in the OT environment
 - Replacing or integrating with existing systems
- External connectivity – vendor, consultant, manufacturer access
 - Challenges securing operations and appropriate visibility of critical systems
- “Air gap” not viable to protect OT systems from threats
- Additional security measures needed to secure OT operation
- Appropriate monitoring and visibility across the IT/OT barrier



[Source: Omicron]

- New technologies, systems, and equipment
 - Significant benefits to operational costs yet pose security vulnerabilities that can and will need to be secured for OT-based systems in particular
- IP-based improvements to existing communications protocols
 - DNP3 over TCP/IP
 - Secure ICCP
 - Could pose risk if security controls not established
- Advanced features and functions
- Cloud computing
- Virtualization



[Source: Dragos]

- Wide range of emerging technologies
 - Virtualization
 - Cloud computing
 - Zero trust network access
 - Artificial intelligence
 - Grid edge technology
 - 5G communications
 - Blockchain
 - Mobile resources
 - DERs and aggregators
 - Inverters
- Many span multiple organizations and segments of energy sector
- Many require coordinated effort to address and fully understand
- Some we will have ability to “manage” the emergence; others will be driven by external factors



[Source: QAD]

- Generally smaller, more dispersed resources
 - Across BPS and on distribution system
 - Wind, solar PV, battery energy storage, hybrid plants, HVDC circuits, etc.
- Highly capable, flexible, controllable resources
- Remote accessibility from equipment manufacturers, EPCs, etc.
- Need coordinated effort within industry to secure these resources from cyber perspective
 - Particularly equipment standards (IEEE, IEC, etc.)



[Source: SMA]



[Source: GE]



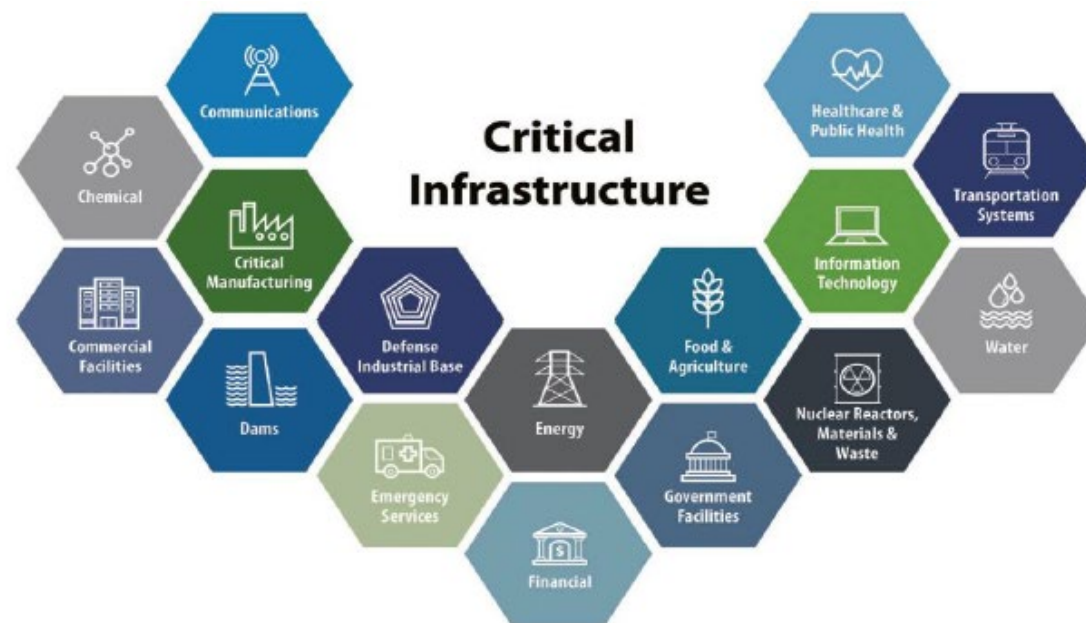
[Source: MISO]

- Need workforce expertise in:
 - OT network security, not just IT expertise
 - Utility experience and understanding of engineering practices
 - Blended cybersecurity and engineering background
 - Protocols, network architectures, tools, engineering needs
- Issue covers generation, transmission, and distribution levels as well as independent system operators, regulatory bodies, and government agencies
- Need range of experience levels; build a strong bench
- Academia beginning offerings; needs to be accelerated

Georgia Tech ECE program offers MS Cybersecurity degree with focus on cyber-physical and energy systems!



- Modern life relies on safe, reliable, and secure electric energy
 - Critical energy infrastructures – telecommunications, banking, public safety, water, and many others
- Electric-natural gas interdependence
- Precious metals and minerals mined around the world (including from regions involving foreign adversaries).
 - Wind, solar photovoltaic, and battery technologies
- Need coordinated risk mitigation across wide range of stakeholders and policymakers
 - Cyber security and energy security



© US Cybersecurity & Infrastructure Security Agency (CISA)

[Source: CISA]

- Widespread cyber-physical threat one of highest priority risk mitigations for NERC and E-ISAC
 - Core component of E-ISAC's role to help information share, coordinate with key agencies and organizations, and ensure a strong security posture
- Key BPS elements compromised (denial of control, damage, etc.) for a prolonged period of time could greatly hinder ability of system to operate in reliable manner; hinder restoration
 - Ex: Blackstart resources in conjunction with key BPS elements
- Difficult to study *a priori*; hard to differentiate “credible” for malicious attack scenarios




- Can we plan a grid more resilient to cyber and physical attacks?
- Can we design a grid with security as a critical consideration up front rather than at the end?
- Can we operate the grid in a way that can easily identify, detect, and respond to security incidents?
- Can we restore the grid effectively following any compromise?
- No more “bolt on” security measures – integrate them up front

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Standards for the Bulk Electric Systems of North America

Updated July 5, 2022

RELIABILITY | ACCOUNTABILITY



3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326

EOP-011-1 Emergency Operations

A. Introduction

1. **Title:** Emergency Operations
2. **Number:** EOP-011-1
3. **Purpose:** To address the effects of operating Emergencies by ensuring each Transmission Operator and Balancing Authority has developed Operating Plan(s) to mitigate operating Emergencies, and that those plans are coordinated within a Reliability Coordinator Area.
4. **Applicability:**
 - 4.1. **Functional Entities:**
 - 4.1.1 Balancing Authority
 - 4.1.2 Reliability Coordinator
 - 4.1.3 Transmission Operator
5. **Effective Date:**
See *Implementation Plan for EOP-011-1*
6. **Background:**
EOP-011-1 consolidates requirements from three standards: EOP-001-2.1b, EOP-002-3.1, and EOP-003-2.

The standard streamlines the requirements for Emergency operations for the Bulk Electric System into a clear and concise standard that is organized by Functional Entity. In addition, the revisions clarify the critical requirements for Emergency Operations, while ensuring strong communication and coordination across the Functional Entities.

B. Requirements and Measures

- R1. Each Transmission Operator shall develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area. The Operating Plan(s) shall include the following, as applicable: [*Violation Risk Factor: High*] [*Time Horizon: Real-Time Operations, Operations Planning, Long-term Planning*]
 - 1.1. Roles and responsibilities for activating the Operating Plan(s);
 - 1.2. Processes to prepare for and mitigate Emergencies including:
 - 1.2.1. Notification to its Reliability Coordinator, to include current and projected conditions, when experiencing an operating Emergency;
 - 1.2.2. Cancellation or recall of Transmission and generation outages;
 - 1.2.3. Transmission system reconfiguration;
 - 1.2.4. Redispatch of generation request;


NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Standard Processes Manual

VERSION 4

March 1, 2019

RELIABILITY | ACCOUNTABILITY



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

- First Standards approved in 2007
- SPM has been continually modified to achieve efficiencies
- Bulk Power System 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

- 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 and FERC must approve any revisions to RoP
- ANSI reviews revisions to SPM under its accreditation activities

Action is needed

- 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 ERO model
 - Stakeholder ballot of process is critical
 - Industry technical expertise is necessary
- 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

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





Muchas gracias por su atención...