NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Developments in Physical and Cybersecurity in Power Systems - North American perspective

Lonnie J Ratliff, NERC, Director Compliance Assurance and Certification
May 19, 2023

RELIABILITY | RESILIENCE | SECURITY




About Me

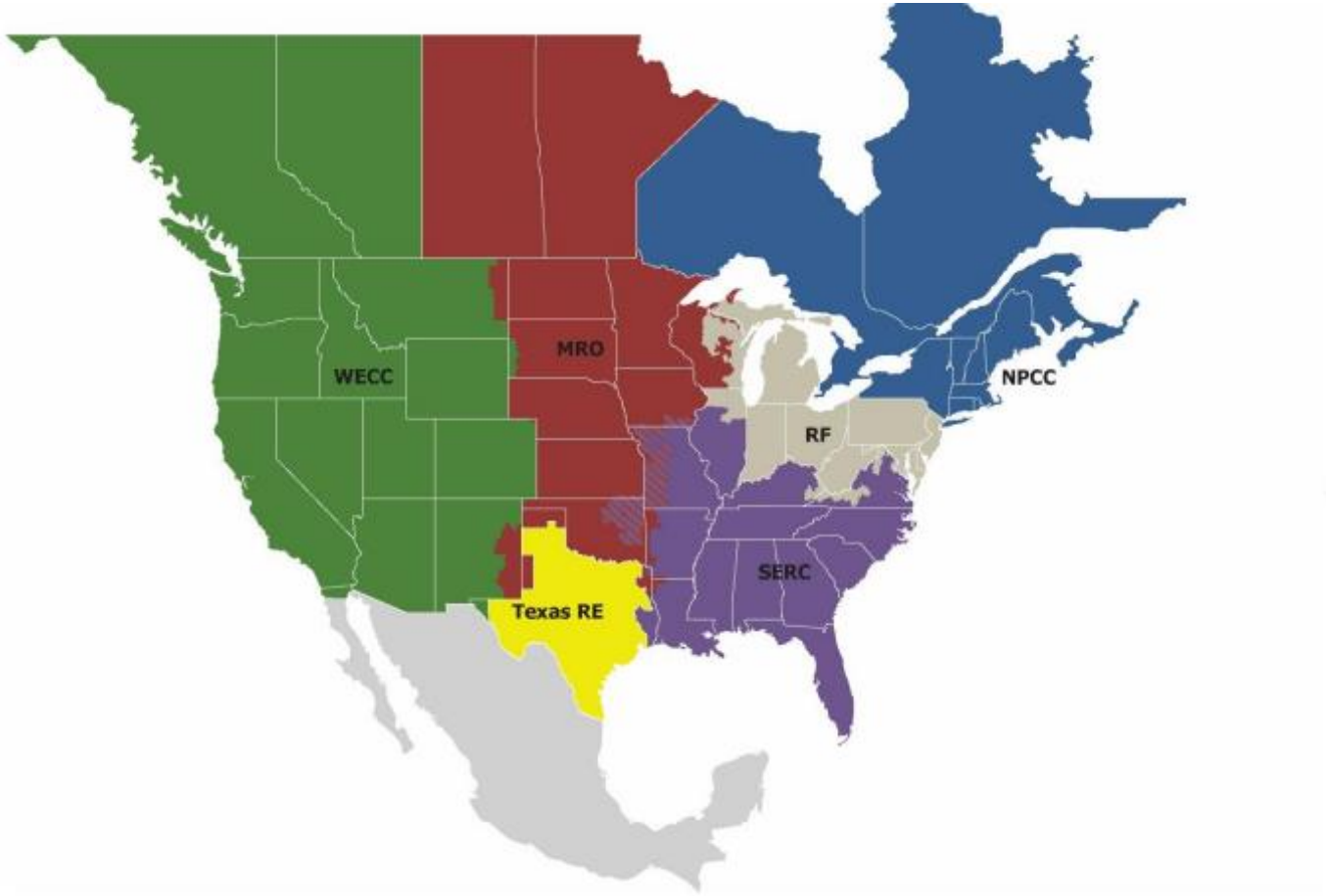
- **Experience**
  - Six years at North American Electric Reliability Corporation
  - Four years at SERC (Region of NERC)
  - Nine years consulting in NERC CIP
  - Cybersecurity subject matter expert
  - Current Certifications
    - CISSP
    - CISA

Brief NERC Overview

The vision for the Electric Reliability Organization Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable and secure North American bulk power system. Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Enterprise Map



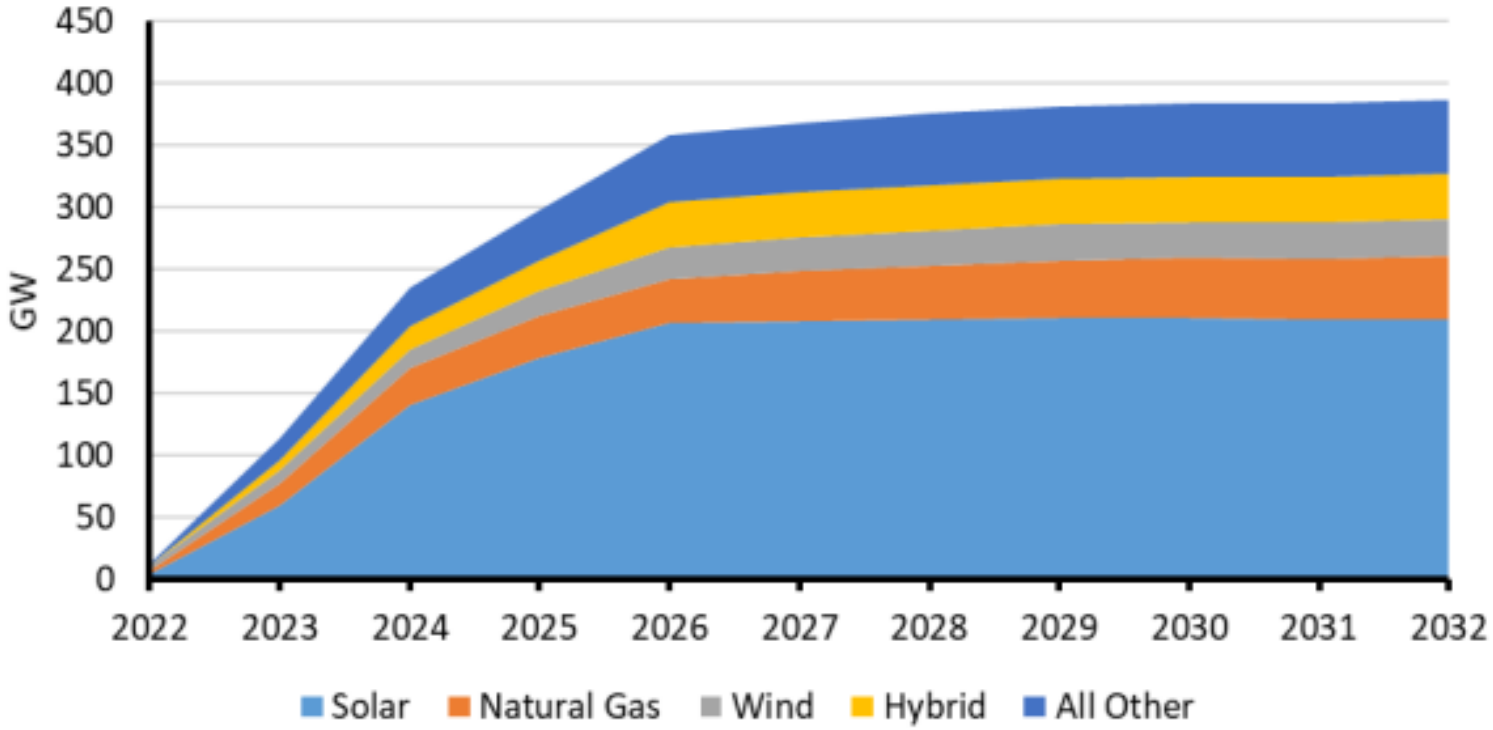
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Topics for discussion

- **Changing nature of the bulk power system**
  - Evolving transition to invertor-based resources
  - New and/or changing technologies and controls
- **Integrating security technology and engineering**
  - Protection of critical assets and cyber systems
  - Coordinated cyber-physical system considerations

New Generation

- **NERC 2022 Long Term Reliability Assessment**



Risk = Threat + Vulnerability

- **Current Risks compared to emerging Risks (IBR)**

Factor	Synchronous World	Inverter-Based World
Fault Current Magnitude	Consistent, High	Consistent, Low
Fault Current Phase Relationship	Consistent, Predictable	Consistent, Unpredictable
Short Circuit Model Accuracy and Certainty	Mature	Immature, Evolving

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Key Security Threats

- ***Supply chain*** compromise
- ***Remote access*** – employees, vendors, third-party and foreign control centers
- ***Convergence of IT and OT networks***
- Recovery from coordinated physical-cyber attacks
- Organizational compliance-centric focus
- Lack of security integration
- ***Lack of qualified security personnel and resources in industry***
- Compromise of operational technology (OT) networks leading to electrical system outage or loss of life
  - Compromise of protection systems in key transmission locations
  - Compromise and control of BPS or distribution elements
  - Compromise of energy supply
  - Loss of situational awareness (e.g., Ukraine 2015)

The Threats

- **Current Threats (continually evolving)**
  - Intentional Threats
    - Malware, ransomware, malicious code
  - Unintentional Threats
    - Inadvertent access to data, etc.
  - Supply Chain
    - Spare parts, equipment
    - Risk Assessments (CIP-013)
  - Malicious Actors

Recurrent and Emergent Threats

- **Copper Theft**
  - Primary component of many electric generation parts
- **Terrorism**
  - Lone Wolf actors, domestic extremists, nation state actors
- **Drones**
  - Surveillance, inadvertent and intentional damage
- **Vandalism**
  - Gun fire, intentional destruction

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attempts to disrupt the Grid

- **2013 – Metcalf Substation Physical Attack**
  - $15 million in damages
  - Initiated creation of CIP-014 – Physical Security Standard
- **2021 – Colonial Pipeline Cyber Attack, physical impact**
  - Disruption of fuel supplies to Southeastern U.S.
- **December 2022 – Substations attacked with gunfire (Moore County, NC)**
  - Approximately 45,000 people impacted
- **December 2022 – Substations in Washington state vandalized**
  - $3 million in damage
- **Early 2023 – San Jose, CA substation attacks, others plotting to destroy Baltimore area infrastructure**

FERC Order – Physical Security

Due to an increase in reports of physical attacks on electric substations, the Commission issued the December 2022 Order directing NERC to evaluate the effectiveness of the Physical Security Reliability Standard (CIP-014) in mitigating the risks to the Bulk-Power System ("BPS") associated with physical attacks.

- FERC directed NERC to conduct a study evaluating
  - (1) the adequacy of the Applicability criteria set forth in the Physical Security Reliability Standard;
  - (2) the adequacy of the required risk assessment set forth in the Physical Security Reliability Standard; and
  - (3) whether a minimum level of physical security protections should be required for all BPS substations and their associated primary control centers.

NERC Findings

- **CIP-014 Applicability adequate**
  - Additional discussion at FERC/NERC Technical Conference
- **A bright line set of minimum physical security protections for all substations not an effective approach**
  - Additional discussion at FERC/NERC Technical Conference
- **Recommending Reliability Standards Development Project for clarifications**

E-ISAC

E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

Mission: *The E-ISAC reduces cyber and physical security risk to the electricity industry across North America by providing unique insights, leadership, and collaboration*

- The E-ISAC is the primary cyber and physical security communications channel for the electricity industry
- Collaborates with U.S. and Canadian governments and intelligence communities
  - Gathers, analyzes, and shares voluntary security information provided by members and partners
  - Information shared with the E-ISAC is protected from government regulator compliance monitoring and enforcement

Eligibility

- All electricity asset owners and operators and select government and cross-sector partners in North America
- Intended audience: security directors, cyber and physical security analysts, and general managers

Membership Benefits

- Members receive customized situational awareness on:
  - ✓ Security threats (including immediate notifications)
  - ✓ Physical security and cyber security bulletins

Website: www.eisac.com

Key Products and Services

- **Critical Broadcast Program (CBP)**
  - ✓ CBP Call: Rapid-convening call for industry and government to provide information and context on imminent and emergent security issues
  - ✓ All-Points Bulletin (APB): Bulletin providing additional information and context on emergent issues facing industry, that do not necessitate a call
- **Monthly Briefings**
  - ✓ E-ISAC and partner updates, threat overviews, and guest speakers
- **Grid Security Exercise (GridEx)**
  - ✓ GridEx is an unclassified exercise designed to simulate a cyber/physical attack on electric and other critical infrastructures across North America
- **Grid Security Conference (GridSecCon)**
  - ✓ Conference for cyber and physical security experts from industry and government to share emerging security trends and lessons learned

Resources

- NERC Report on CIP-014

  https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/NERC%20Report%20on%20CIP-014-3.pdf
- NERC IBR Strategy

  https://www.nerc.com/comm/Documents/NERC_IBR_Strategy.pdf
- NERC Standards page

  https://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States
- EISAC Page

  https://www.eisac.com/
- Supply chain information

  https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx

Questions and Answers