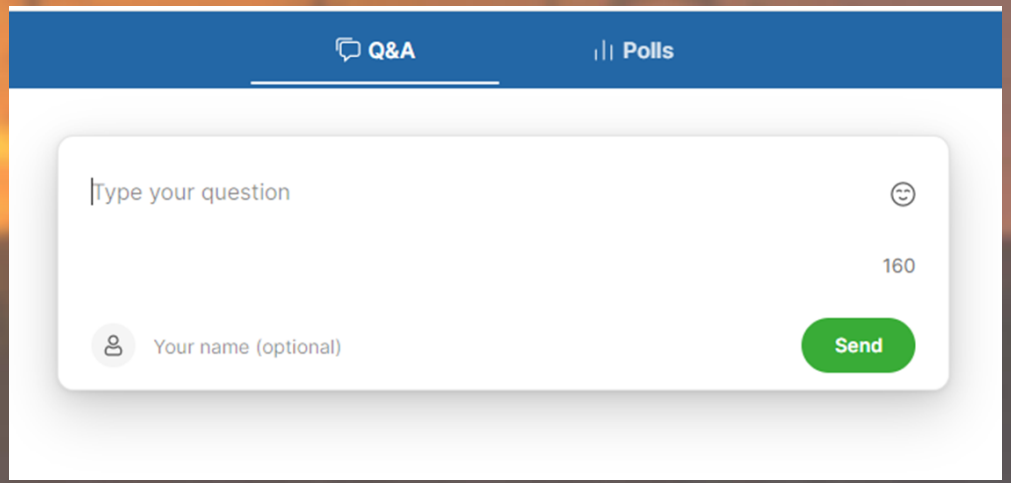
# Texas RE Fall Standards, Security, & Reliability Workshop

November 4, 2026

## AGENDA

- Resilience Through Protected Communication (CIP-012)
- Walking the Line of Defense (CIP-003, CIP-006, CIP-014)
- Inside Threats, Inside Visibility (CIP-015)
- Ask the Hard Questions: Computational Loads, Ride-through, and Grid Compatibility
- Mitigating Misoperation Risk and Finishing the Fix
- Ride-through Ready (PRC-028, PRC-029, PRC-030)
- Closing the Facility Ratings Gap (FAC-008)

To submit questions during the workshop, please visit **slido.com** and enter today's participant code: **TXRE**



# Welcome & Instructions

**Diana Burger**
Texas RE
Manager, Communications & Training



STANDARDS, SECURITY, & RELIABILITY
FALL WORKSHOP

# Antitrust Admonition

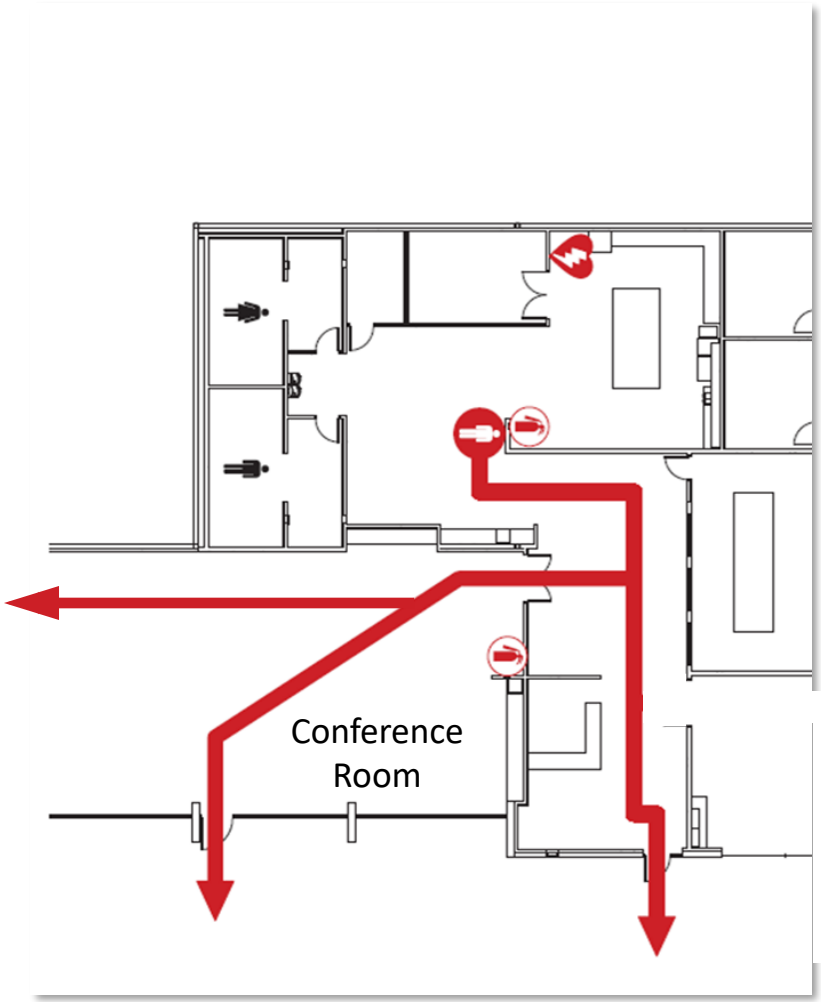
**Because this event brings together market participants who may be viewed as actual or potential competitors, we must be mindful to conduct it in a manner that is consistent with the antitrust and competition laws. Participants should not disclose non-public, proprietary, or competitively sensitive information.**

**Attendees should exercise independent judgment and avoid even the appearance of discussions of agreements or concerted actions that may be viewed as restraining competition. Any questions on Texas RE's Antitrust Compliance Corporate Policy may be directed to Texas RE's General Counsel.**

# Safety Moment

**In case of emergency, evacuate through the nearest door**

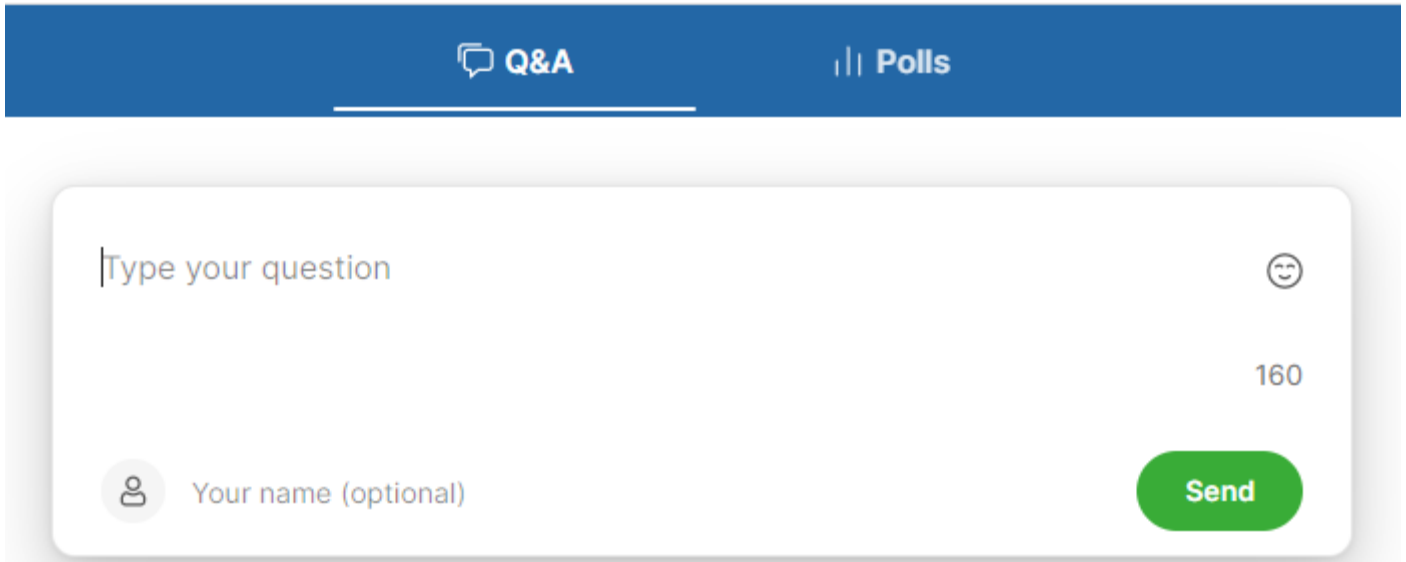
**Rally point is in the front parking lot**



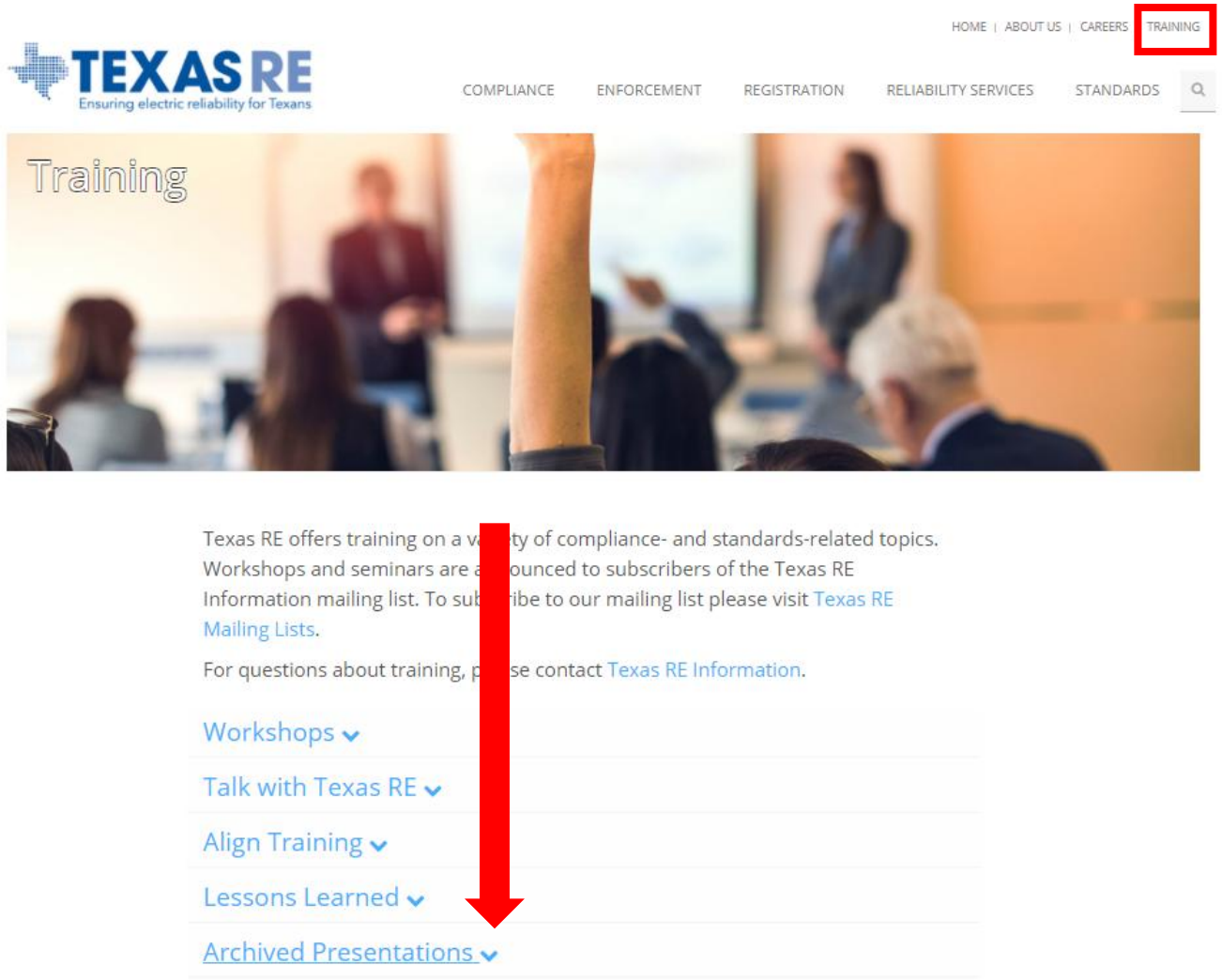
# Questions

To submit questions during the workshop, please visit **slido.com** and enter today's participant code: **TXRE**

slido



# Training Page




## Archived Presentations

All of Texas RE's outreach activities are free and open to the public. Past presentations delivered by Texas RE staff are available here. Please be aware that presentations will not be available indefinitely, and may be removed to comply with Texas RE's document retention policy.

ALIGN

Align Release 1 Training | Recording

Align Release 2 Periodic Data Submittal Training | Recording

Align Release 2 TFE and Self-Certification Training | Recording

Align Release 3 Training | Recording

Align Release 4 & 4.5 Training | Recording

### Workshops

Women's Leadership in Grid Reliability and Security Conference | Recording

Understanding New Generator Obligations | Recording

**Fall Standards, Security, and Relia**

Fall Standards, Security, and Reliability Workshop

**Spring Standards, Security, and Reliability Workshop**

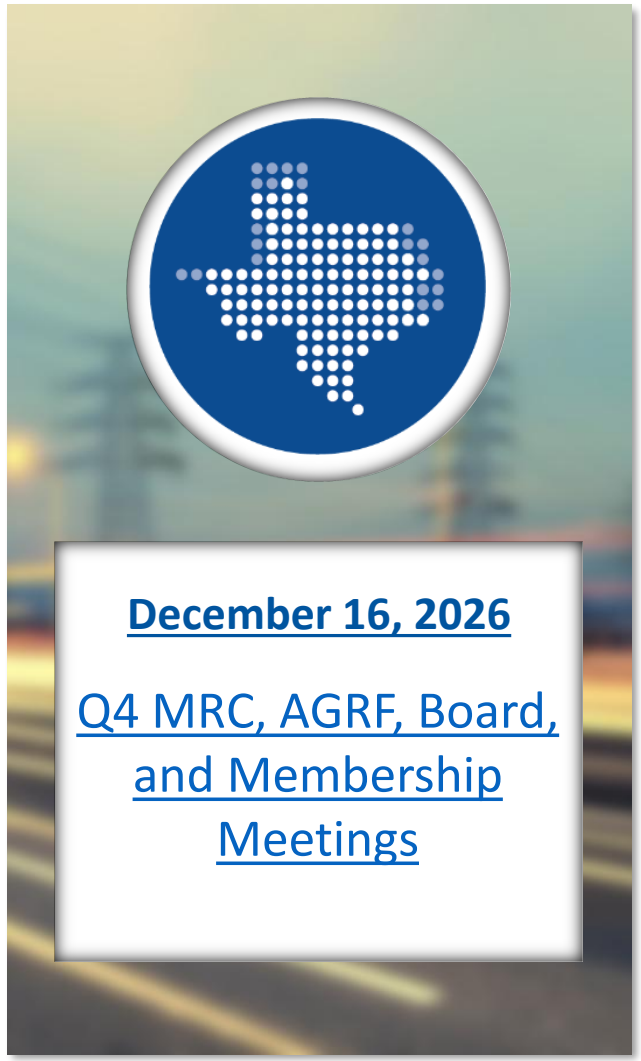
Spring Standards, Security, and Reliability Workshop

# Upcoming Events at Texas RE









# Social Media




## /texas-reliability-entity-inc

# Executive Welcome

**Joseph Younger**
Texas RE
Senior Vice President & Chief Operating Officer



STANDARDS, SECURITY, & RELIABILITY
FALL WORKSHOP



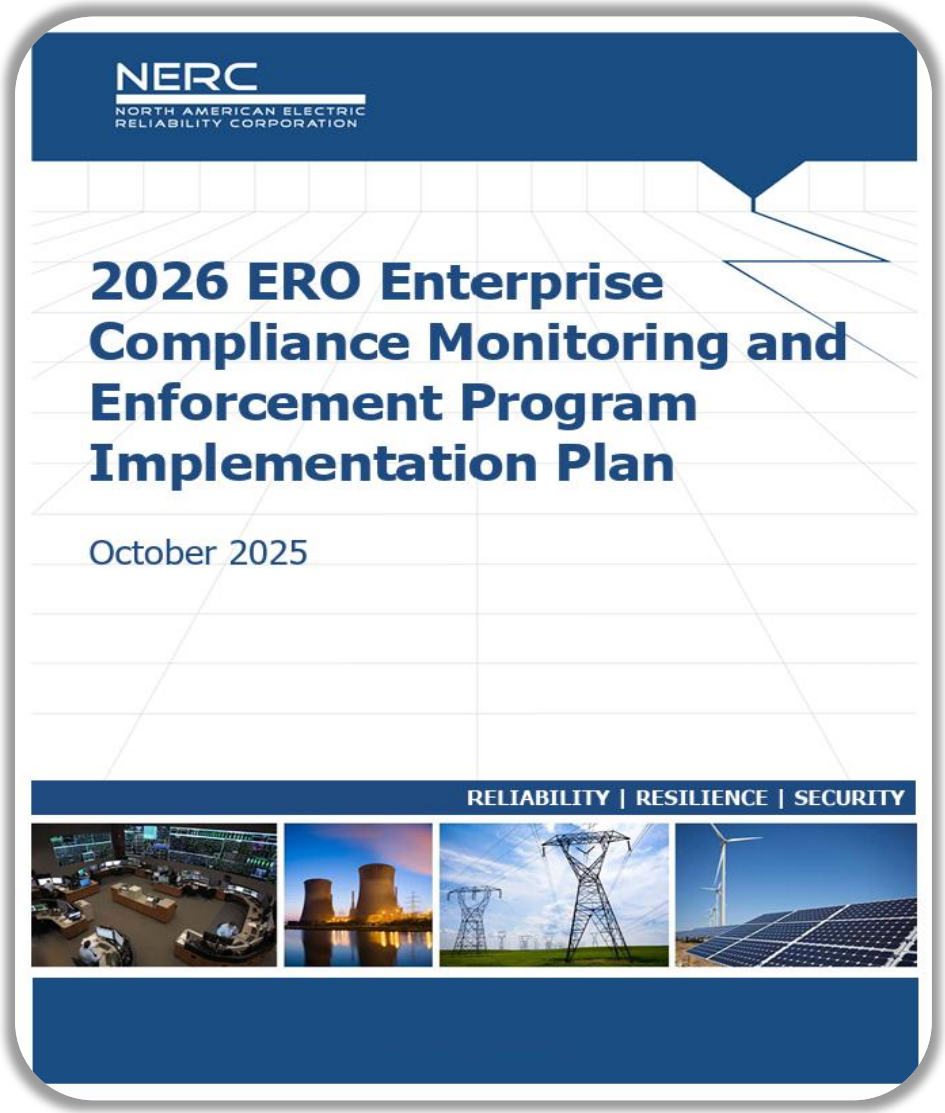

# Resilience Through Protected Communications

**Gabriela Barragan**
**CIP Cyber & Physical Security Analyst**

# Agenda

- Risk Element Areas of Focus: Remote Connectivity
- CIP-012-2 Requirement 1 & Version Changes
- ERCOT Implementation
- Internal Controls, Evidence, & Resources

# Risk Focus & CMEP IP Risk Factor




| Risk Elements |
| --- |
| Remote Connectivity |
| Supply Chain |
| Physical Security |
| Grid Transformation |
| Facility Ratings |
| Extreme Weather Response |

# CIP-012-2 Requirement 1

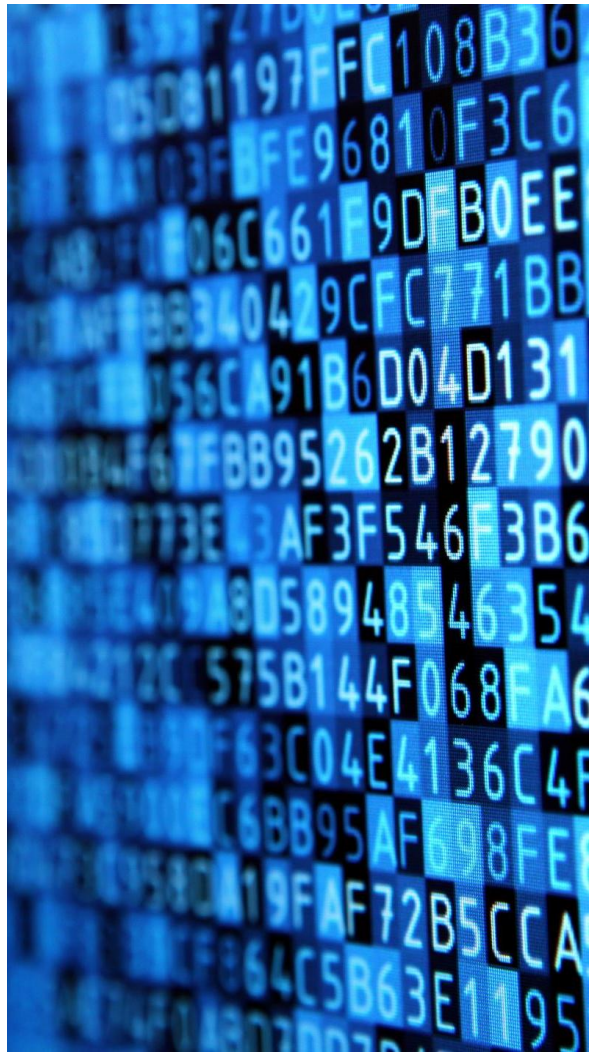



**Unauthorized Disclosure**

**Unauthorized Modification**

**Loss of Availability**

# Part 1.1

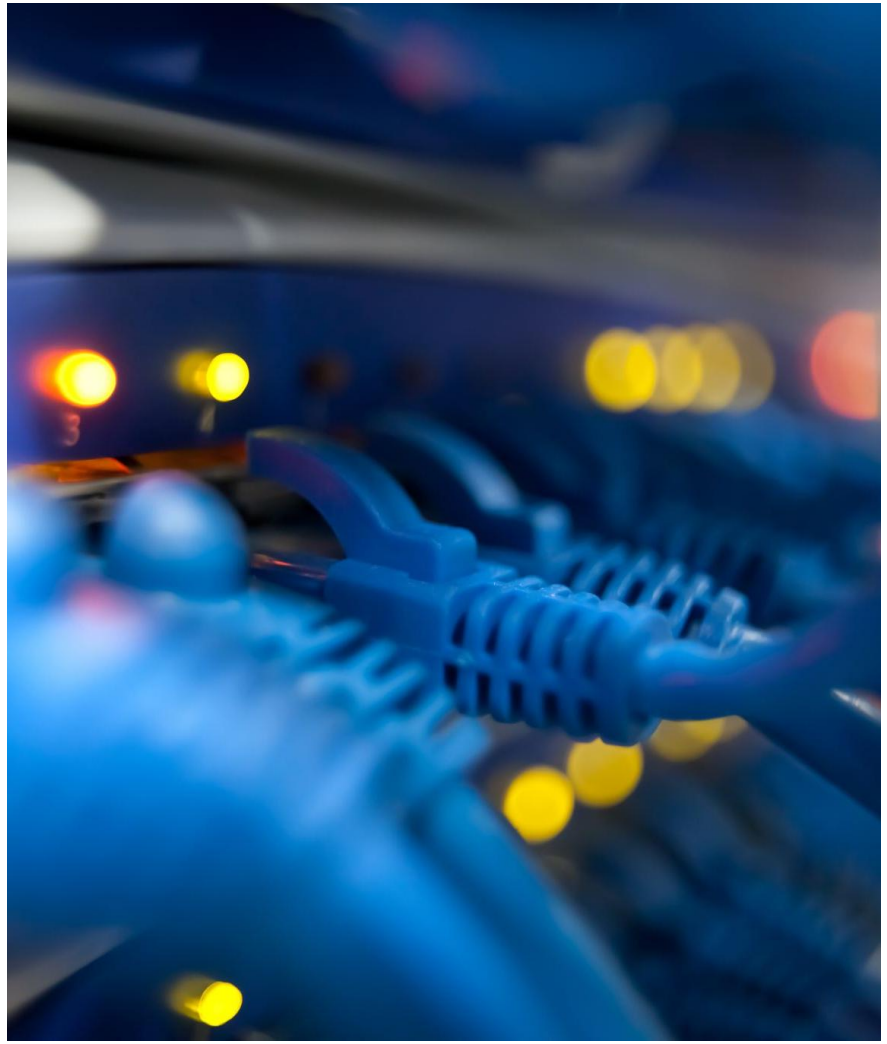


Identification of **method(s) used** to mitigate the risk(s) posed by unauthorized disclosure and unauthorized modification of data used in Real-time Assessment (RTA) and Real-time monitoring while such data is being transmitted between Control Centers.

## Considerations

- Identifying RTA and Real-time monitoring data

# Part 1.2



Identification of **method(s) used** to mitigate the risk(s) posed by the **loss of the ability** to communicate Real-time Assessment and Real-time monitoring data between Control Centers

## Considerations

- How processes address loss of availability

# Part 1.3

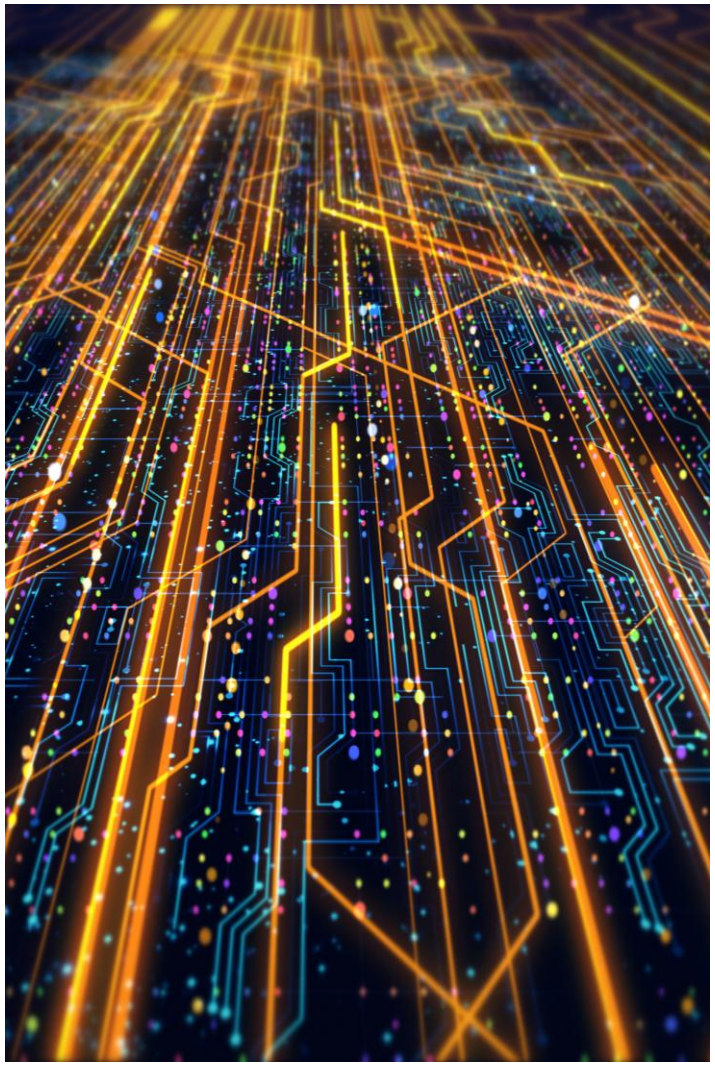


Identification of **method(s) used to initiate recovery of communication links** used to transmit Real-time Assessment and Real-time monitoring data between Control Centers

## Considerations

- Incident response & restoration playbooks

# Part 1.4

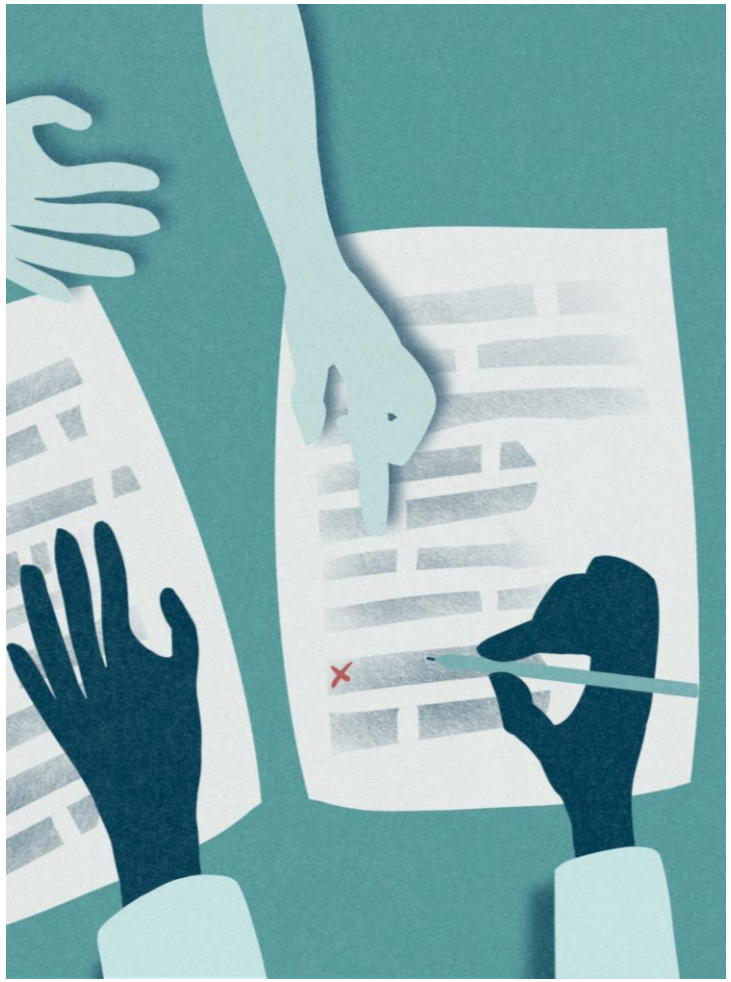


Identification of where the Responsible Entity **implemented method(s)** as required in Parts 1.1 and 1.2

## Considerations

- Control Center as a NERC defined term

# Part 1.5

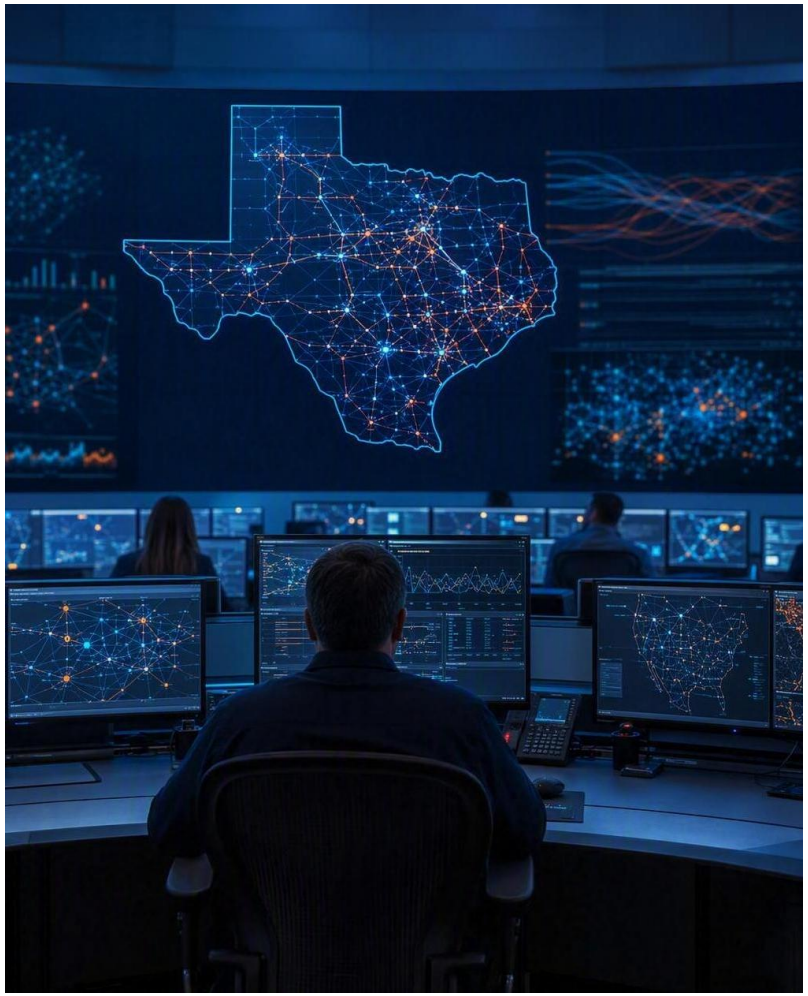


If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for **implementing method(s)** as required in Parts 1.1, 1.2, and 1.3

## Considerations

- Shared responsibility model

# ERCOT Interconnection Implementation



- ERCOT Nodal Operating Guide Section 7.1
- The Demarcation Handoff
- ERCOT Shared Responsibilities

# Internal Controls



Logical & Physical Controls



Up-to-Date Security Protocols



Consistent Inspection & Maintenance



Real-Time Alert & Incident Monitoring



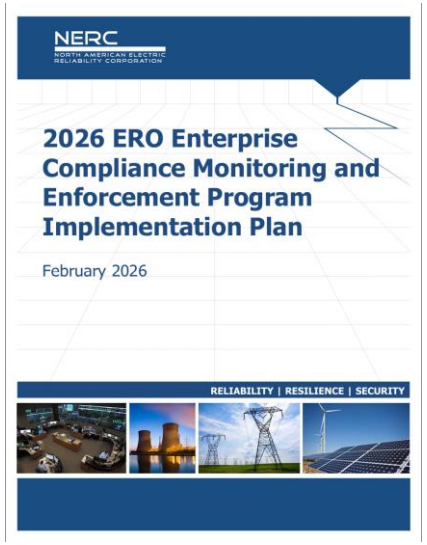
Configuration Backups & Recovery Verification

# Possible Evidence



- Methods of mitigation used (e.g., data masking, encryption/decryption)
- Identification of alternative communication links
- Process to restore systems that provide communications
- Logical diagrams indicating where implemented methods reside
- Agreement outlining responsibilities of each entity

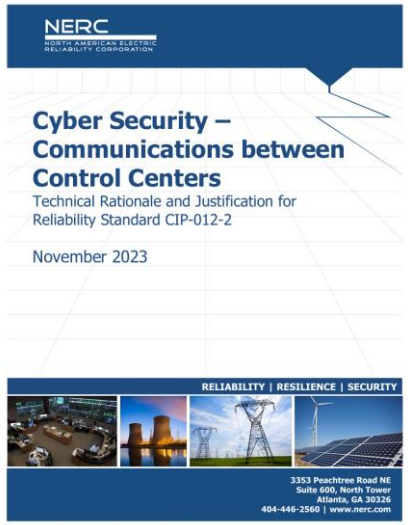
# Resources




[CMEP IP]

NIST

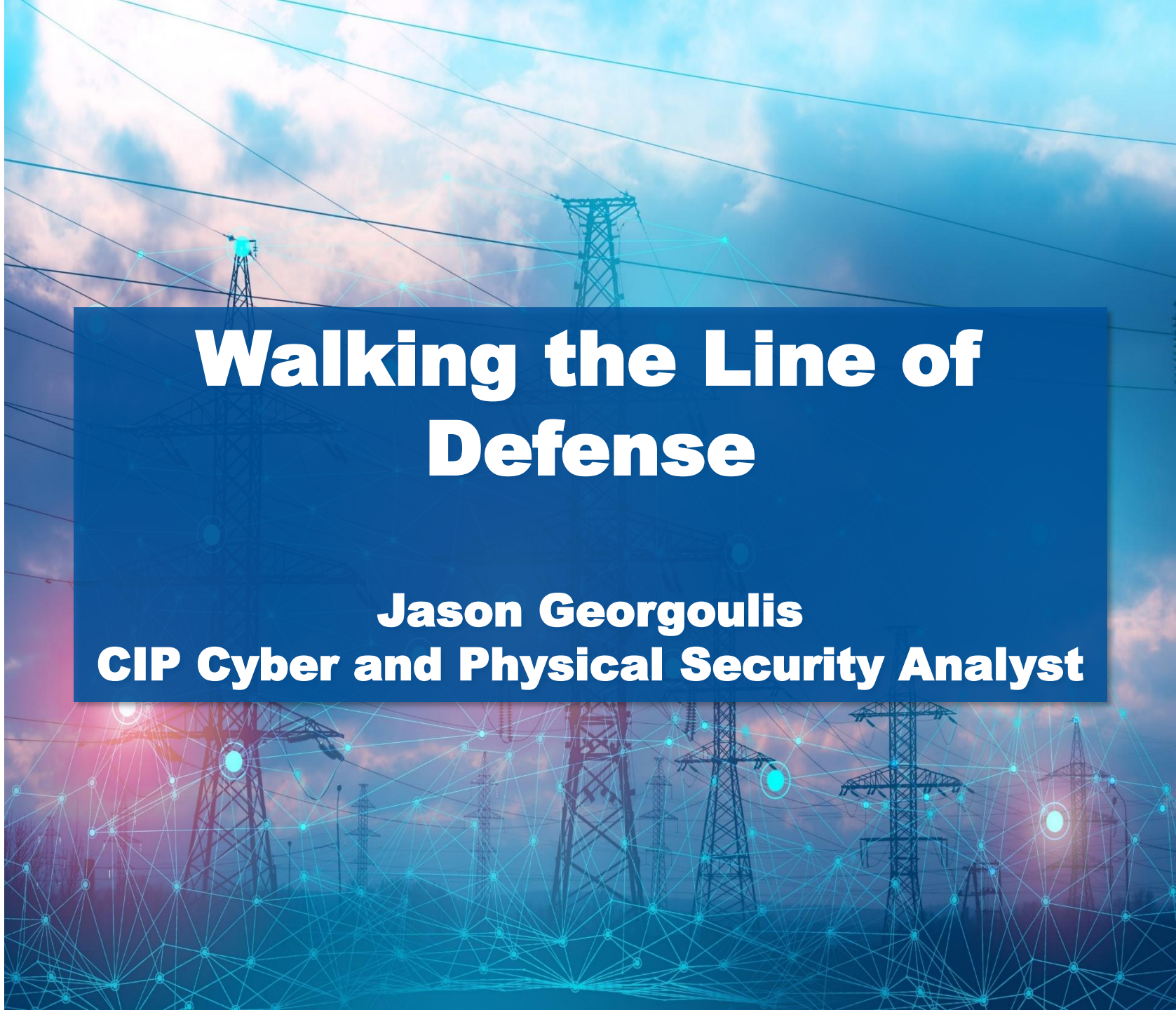
[NIST SP 800-47]




[Technical Rationale]

# Questions?

TEXAS RE
Ensuring electric reliability for Texans

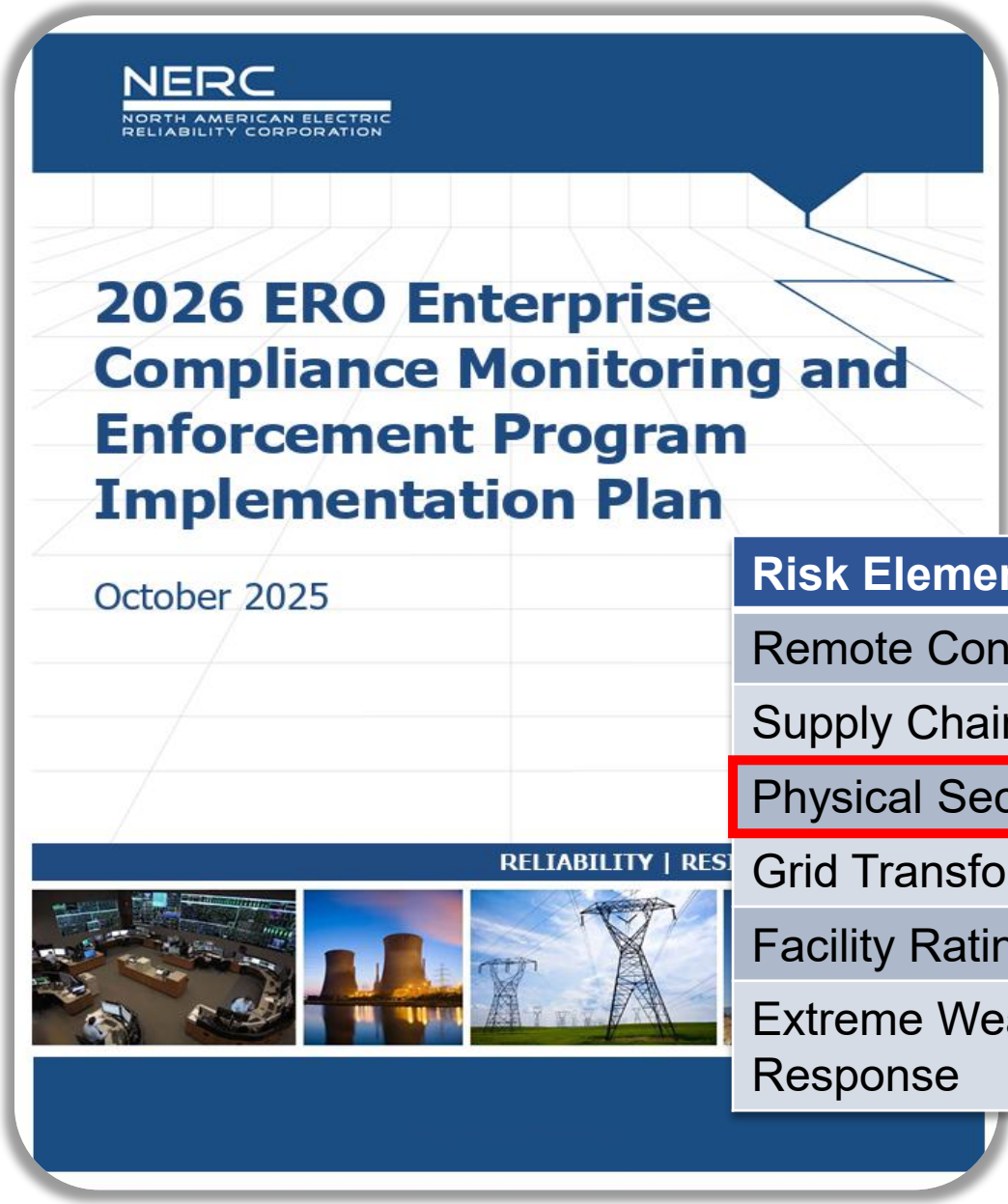


# Walking the Line of Defense

**Jason Georgoulis**
**CIP Cyber and Physical Security Analyst**

# Risk Focus & CMEP IP Risk Factors




| Risk Elements |
| --- |
| Remote Connectivity |
| Supply Chain |
| Physical Security |
| Grid Transformation |
| Facility Ratings |
| Extreme Weather Response |

# Agenda

## What is physical security?

- Define at a high level

## CIP-003-9

- Low impact Requirements

## CIP-006-6

- Medium and high impact Requirements

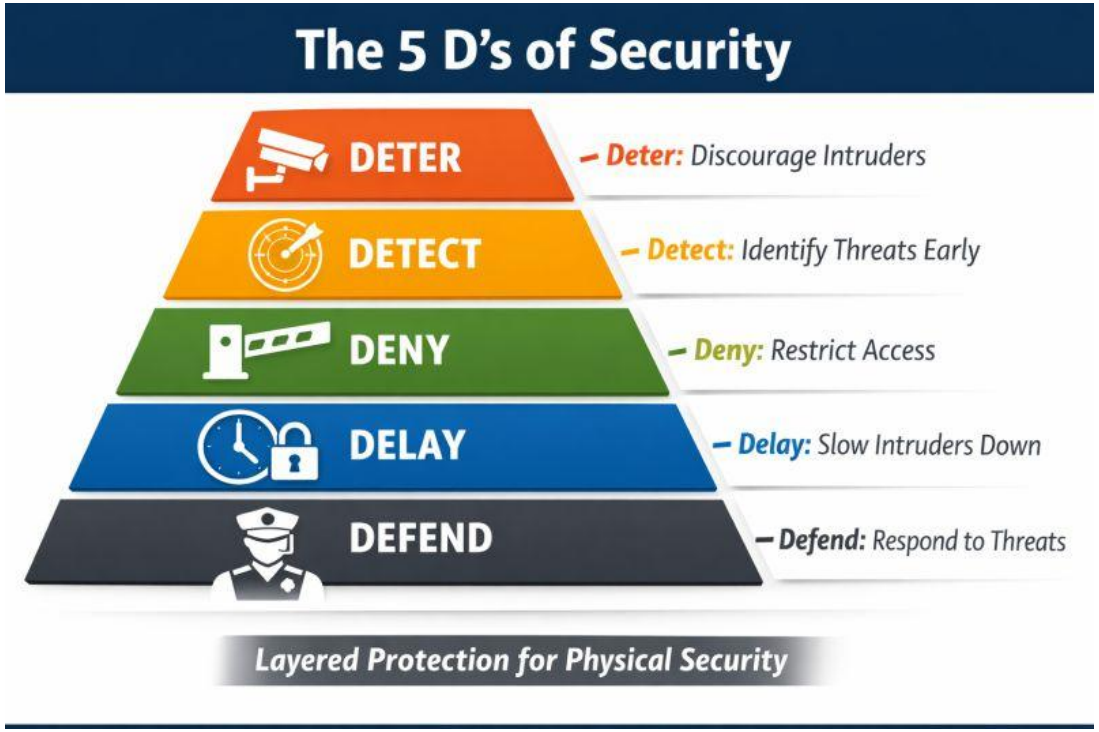
## CIP-014-3

- Transmission stations and substations



# What is Physical Security?

**Physical security is that part of security concerned with active and passive measures, designed to prevent unauthorized access to personnel, equipment, installations, materials, and information; and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity. (CDSE)**



# CIP-003-9 R2 Section 2 – Physical Security Controls

**R2**. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.

**Attachment 1:** Include each of the sections in the cyber security plan(s) required under Requirement R2. Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Develop each plan either by BES Cyber System or BES Cyber Asset.

**Section 2: Physical Security Controls:** Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.



# Considerations

**What**

- What are you controlling physical access to?
- Will you be controlling access to the BES asset, the BES Cyber Systems, or both?

**How**

- How will you control physical access?
- What methods do you intend to implement?

**Who**

- Who will be authorized for physical access?
- Will authorization be based on need?



# CIP-003-9 R2 Section 2

## Control physical access to:

| Asset containing a low impact BES Cyber System | Low impact BES Cyber System within the asset | Cyber Assets, as specified by the Responsible Entity, that provide electronic access control(s) implemented for 3.1 |
|---|---|---|
| • Physical barriers/fencing<br>• Gates with physical access controls<br>• Security signage indicating restricted access<br>• Lighting and motion sensors<br>• Closed-circuit television cameras (CCTV)<br>• Operational and procedural controls | • Control house with access control for ingress<br>• Physical Access Control Systems (PACS)<br>• Authentication systems<br>• Physical intrusion detection systems (IDS)<br>• Video management systems (VMS)<br>• Padlocks protecting cabinet access<br>• Locked relay panels, cabinets or racks | • Control house physical access controls<br>• Locked cabinets<br>• Other types of enclosures with physical access controls |

# Best Practices

## Identity and authorization management

- Track who is allowed access and why the access is needed

## Layered access controls

- Perimeter fencing supplemented by a locked control house will help deny and/or delay unauthorized access

## Periodic physical walkdowns

- Ensure that all access controls are maintained and working effectively

## Physical key management

- Document and implement a key management process to help maintain accountability, reduce unauthorized physical access risks, and support the effectiveness of the physical security plan



# CIP-006-6 Table R1 – Physical Security



**R1:** Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan.

## R1 Key Definitions

**Physical Security Perimeter (PSP):** The physical border surrounding locations in which Bulk Electric System (BES) Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

**Physical Access Control System (PACS):** Cyber Assets that control, alert, or log access to the Physical Security Perimeters(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms and badge readers.

# CIP-006-6 Physical Protections

**Part 1.2** Utilize at least one physical access control to allow only individuals who have authorized unescorted physical access into the Physical Security Perimeter (PSP)

**Part 1.3** Utilize at least two or more different physical access controls

**Part 1.10** Restrict physical access to cabling and nonprogrammable communication components outside of the PSP or encrypt/monitor the status of the link and issue an alarm or alert within 15 minutes of detection, or equal logical protection

**Part 2.1** Require continuous escorted access of visitors within each PSP, except during CIP Exceptional Circumstances

**Part 3.1** Maintenance and testing of each Physical Access Control System (PACS) and locally mounted hardware or devices at the PSP at least once every 24 calendar months to ensure they function properly

# CIP-006-6 Monitoring, Reporting and Logging

**Part 1.4** Monitor for unauthorized access into a PSP

**Part 1.5** Issue an alarm or alert in response to detected unauthorized access through a physical access point to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection

**Part 1.6** Monitor each PACS for unauthorized physical access

**Part 1.7** Issue an alarm or alert of detected unauthorized physical access of a PACS to personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection

**Part 1.8** Log entry of everyone with authorized unescorted physical access into each PSP

**Part 1.9** Retain physical access logs for at least 90 days

**Part 2.2** Require manual or automated visitor logging

**Part 2.3** Retain visitor logs for at least 90 days

# Best Practices

## Proactive Testing

- Test your controls regularly

## Layered access controls

- Perimeter fencing supplemented by a locked control house will help deny and/or delay unauthorized access

## Periodic physical walkdowns

- Ensure that all access controls are maintained and working effectively

## Physical key management

- Document and implement a key management process to help maintain accountability, reduce unauthorized physical access risks, and support the effectiveness of the physical security plan



# CIP Physical Walkthroughs during your Engagement

- Inspect perimeter fencing, gates, and barriers to ensure they are adequate to deter unauthorized access
- Check surveillance systems, including cameras and sensors, to verify their functionality and coverage
- Test access control measures, such as card readers, alarms/alerts, and security personnel to ensure only authorized individuals can enter secure areas
- Review access logs, and visitor logs to ensure continuous escorted access of visitors within the PSP
- Review environmental controls for Control Centers and associated datacenters, redundancy and diversely routed - avoiding single points of failure



# CIP-014-3 R4 – Physical Security

**R4.** Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following:

**4.1** Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s)

**4.2** Prior history of attack on similar Facilities including frequency, geographic proximity, and severity of past physical security related events

**4.3** Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO) Enterprise, the Electricity Information Sharing and Analysis Center (E-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors

# CIP-014-3 R5 – Physical Security

**R5.** Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes:

**5.1** Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4

**5.2** Law enforcement contact and coordination information

**5.3** A timeline for executing the physical security enhancements and modifications specified in the physical security plan

**5.4** Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s)

# Best Practices

Consider testing the security controls for efficacy

Familiarization with local law enforcement

Calendar reminders, notification system

Leverage public resources (i.e., CISA.gov, NERC Security Guideline)



# Questions?

TEXAS RE
Ensuring electric reliability for Texans

# Texas RE Fall Standards, Security, & Reliability Workshop

November 4, 2026

## AGENDA

- Resilience Through Protected Communication (CIP-012)
- Walking the Line of Defense (CIP-003, CIP-006, CIP-014)
- **Inside Threats, Inside Visibility (CIP-015)**
- Ask the Hard Questions: Computational Loads, Ride-through, and Grid Compatibility
- Mitigating Misoperation Risk and Finishing the Fix
- Ride-through Ready (PRC-028, PRC-029, PRC-030)
- Closing the Facility Ratings Gap (FAC-008)

## Break

Will Return at: 10:30

To submit questions during the workshop, please visit **slido.com** and enter today's participant code: **TXRE**




# Inside Threats, Inside Visibility (CIP-015-1)

**Devin Ferris**
**Manager, CIP Compliance Monitoring**

# Federal Energy Regulatory Commission (FERC) Order No. 887




"…North American Electric Reliability Corporation (NERC) to develop …. new or modified Reliability Standards that require internal network security monitoring within a trusted Critical Infrastructure Protection networked environment for all high impact bulk electric system (BES) Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity."

# Cybersecurity Threats

## Volt Typhoon

- CISA Alert AA24-038A
  - February 2024

## ELECTRUM

- Cyber Attack on Poland
  - December 2025

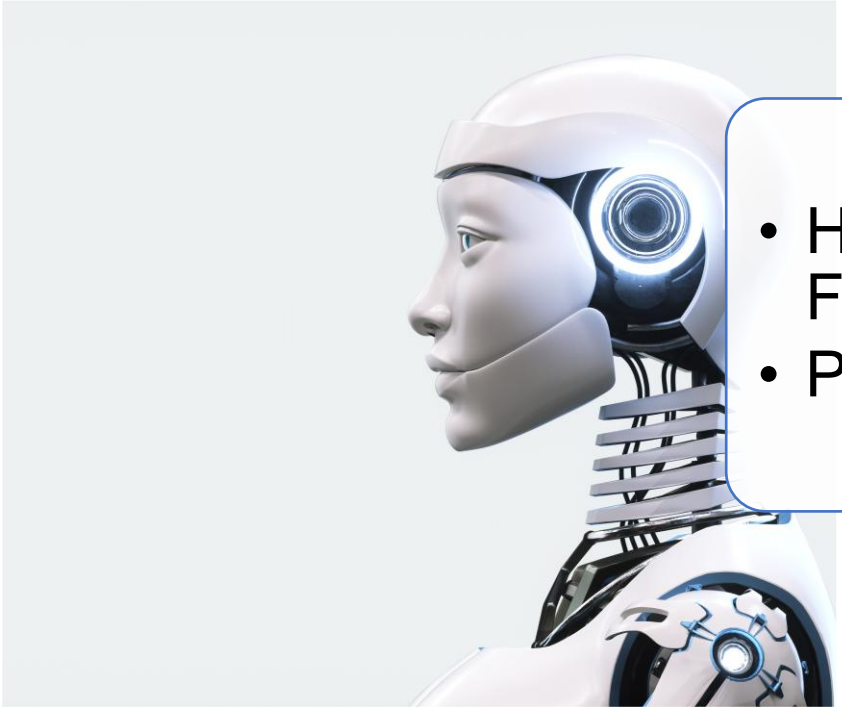
## CyberAv3ngers

- CISA Alert AA26-097A
  - April 2026

## CyberAv3ngers

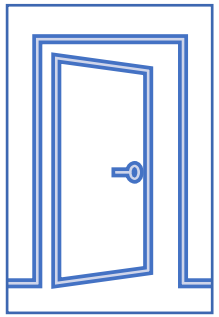
- CISA Alert AA26-097A
  - July 2026

## AI Threats



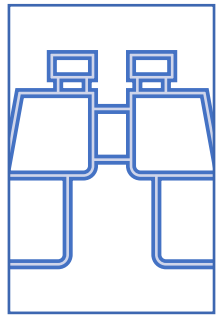
- Hugging Face
- PHP Flaw

# Cyberattack on Poland's Energy Sector



## Initial Access

- Vulnerable Edge Device



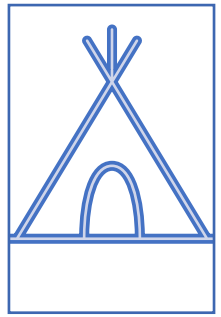
## Reconnaissance

- Native Tools



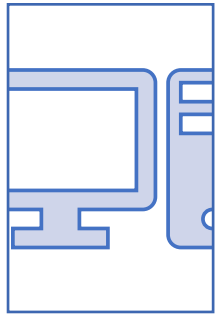
## Escalation of Privilege

- Rubeus



## Persistence

- Living Off The Land (LOTL)



## Affected IT & OT

# CIP-015-1 – Internal Network Security Monitoring (INSM)

## Purpose

- To improve the probability of detecting anomalous or unauthorized network activity in order to facilitate **improved response and recovery** from an attack.

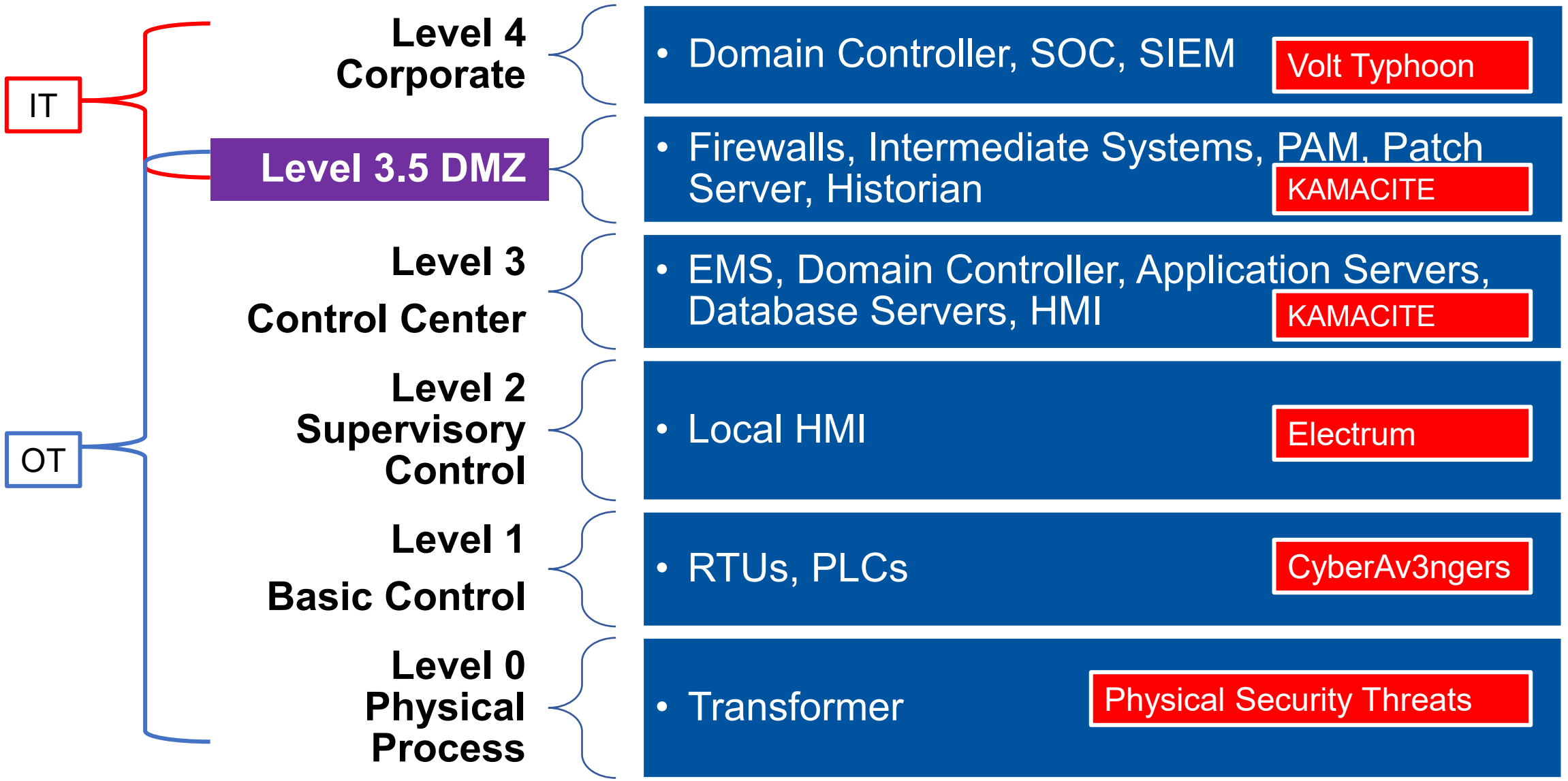
## R1

- Each Responsible Entity shall **implement one or more documented process(es)** for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with **External Routable Connectivity** to provide methods for detecting and evaluating anomalous network activity.

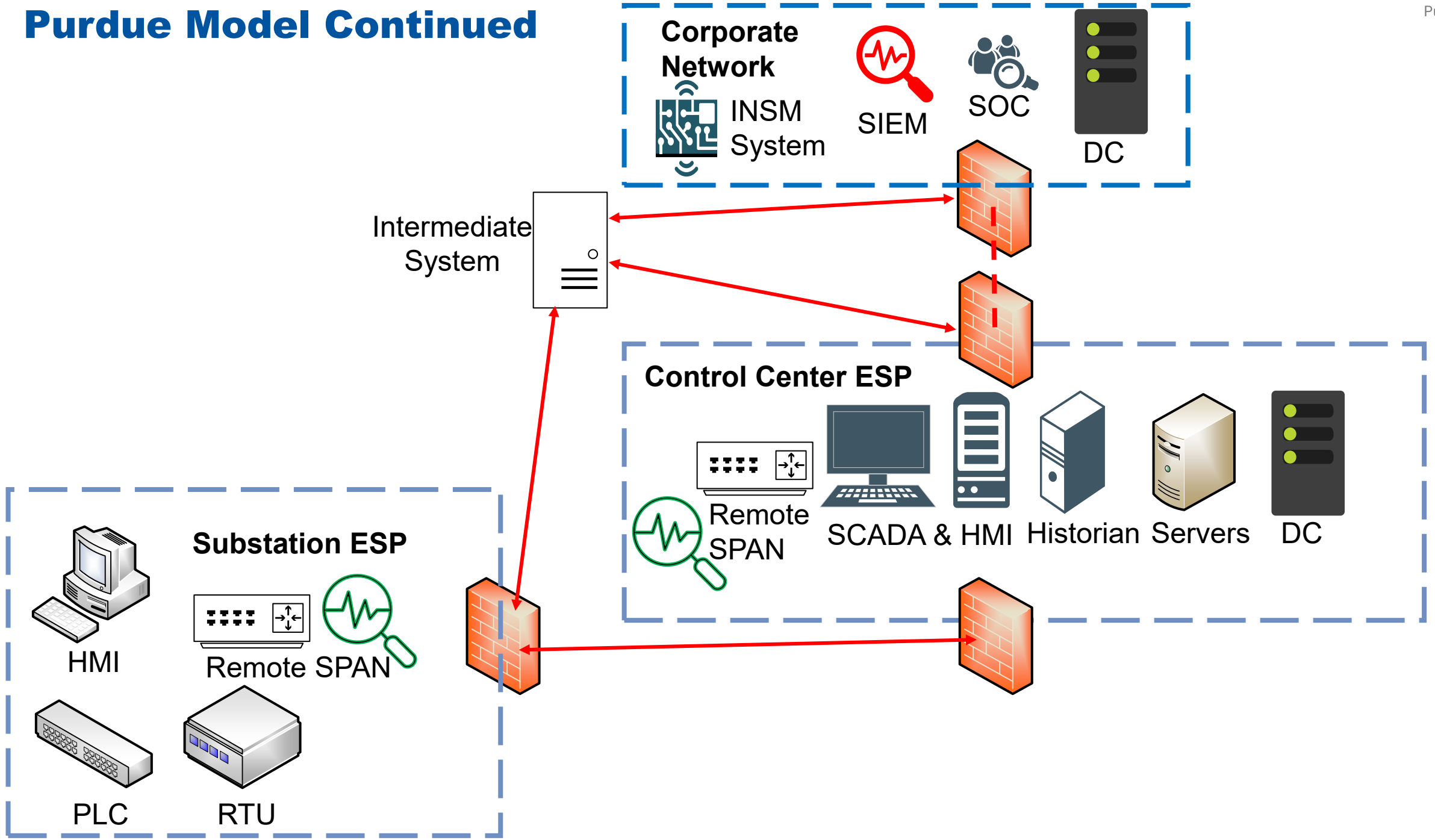
# CIP-015-1 R1, Parts 1.1 – 1.3

| | |
|---|---|
| **Part 1.1** | Implement, using a **risk-based rationale**, network data feed(s) to monitor network activity; including connections, devices, and network communications |
| **Part 1.2** | Implement one or more method(s) to detect **anomalous network activity** using the network data feed(s) from Part 1.1 |
| **Part 1.3** | Implement one or more method(s) to **evaluate anomalous** network activity detected in Part 1.2. to determine further action(s) |

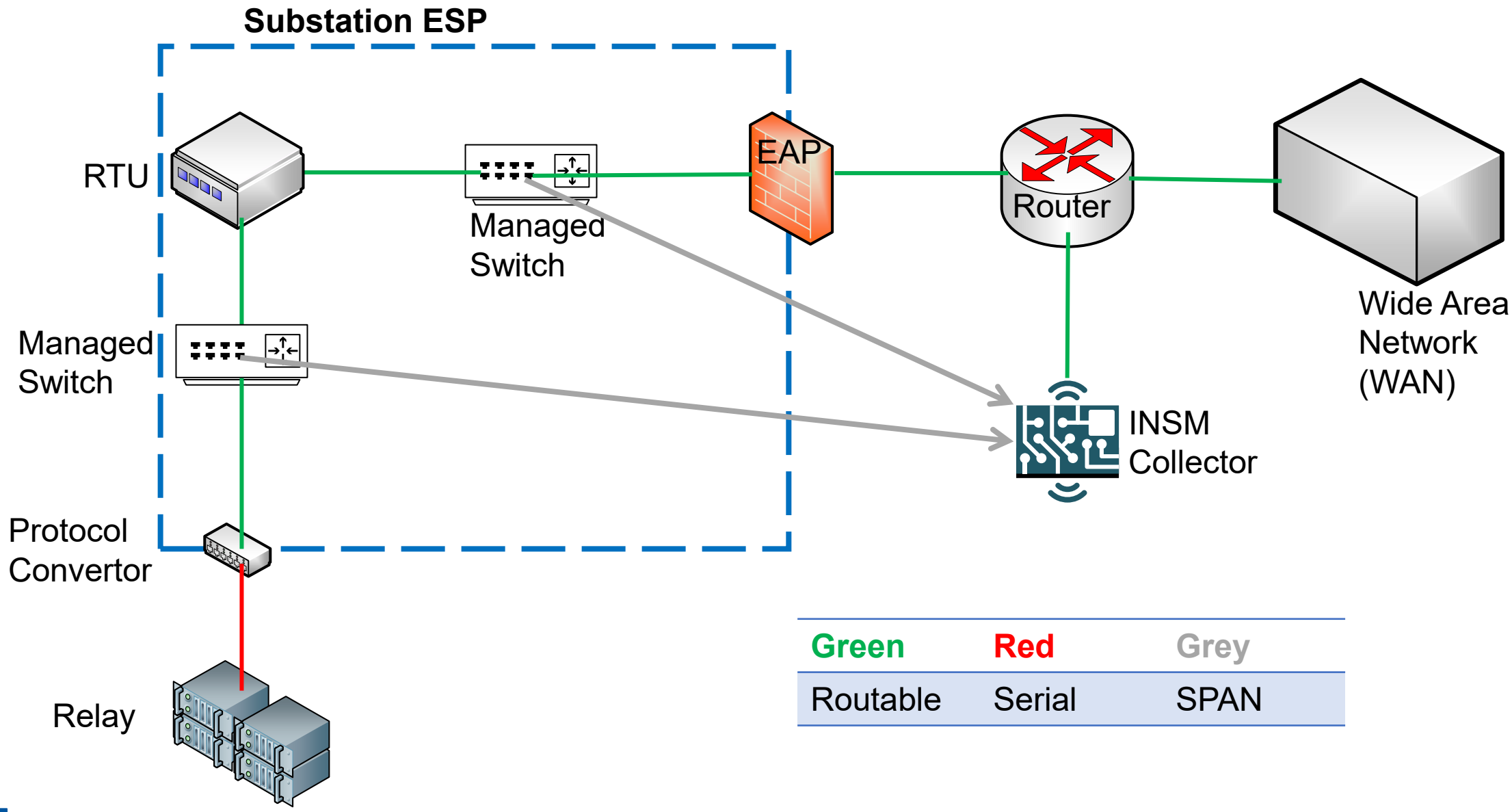
# Purdue Model



# Purdue Model Continued

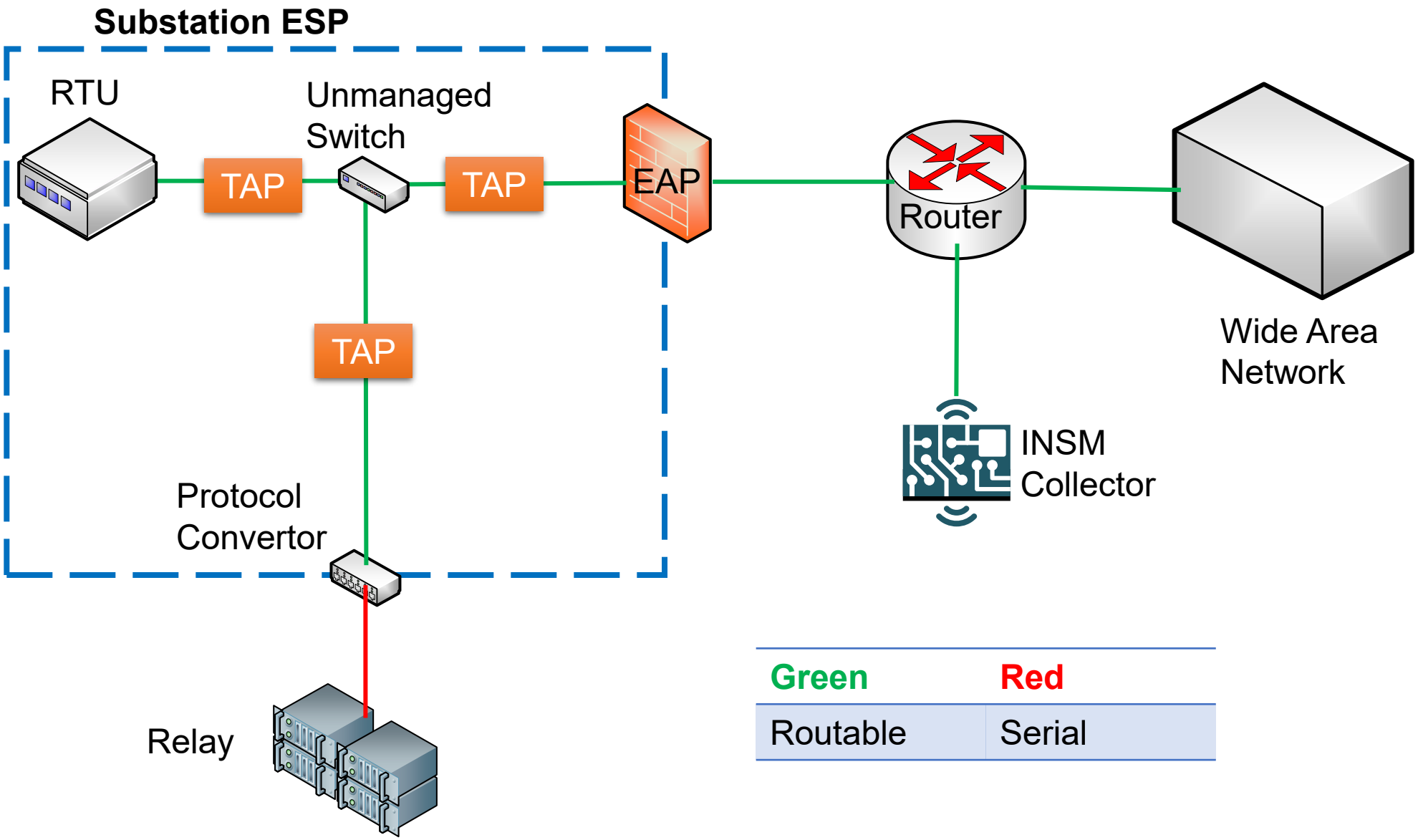


# Managed Switch Example




| Green | Red | Grey |
|---|---|---|
| Routable | Serial | SPAN |

# Unmanaged Switch Example




| Green | Red |
|---|---|
| Routable | Serial |

# Next Level Detection



Indicators Of Compromise (IOC's)



Tactics, Techniques, And Procedures (TTP's)

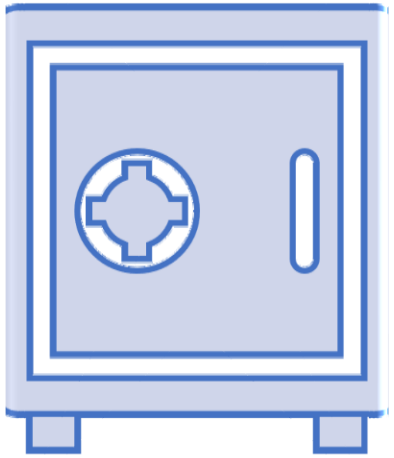


ICS Protocol Analysis



Cyber Asset Level Integration

# CIP-015-1 R2



## R2

- Each Responsible Entity shall implement, except during **CIP Exceptional Circumstances**, one or more documented process(es) to retain internal network security monitoring data associated with network activity **determined to be anomalous** by the Responsible Entity at a minimum until the action is complete in support of Requirement R1, Part 1.3.

| Data Retention | CIP-008-6 R2 | Anomalous Activity |
|---|---|---|
| • Retention Timeframes<br>• Number of Events | • Reportable Cyber Security Incident<br>• Cyber Security Incident<br>• “attempt to compromise” | • What does that mean to you? |

# CIP-015-1 R2



## R3

- Each Responsible Entity shall implement, except during **CIP Exceptional Circumstances**, one or more documented process(es) to **protect** internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of **unauthorized deletion or modification**.

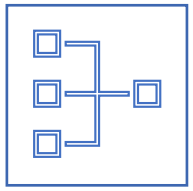
| Segment | Restrict | Control |
| --- | --- | --- |
| • INSM data separate from BCS? | • Least Privilege | • MFA<br>• Increased Authentication and Authorization Controls |

# CIP-015-1 & CIP-015-2 Implementation Plans

| CIP-015-1 Approved | High & Medium Control Centers w/ERC | All other Medium BCS w/ERC |
|---|---|---|
| $T_0$ | $T_{+36}$ | $T_{+60}$ |
| June 26, 2025 | October 01, 2028 | October 01, 2030 |

| CIP-015-2 Phase 1 | CIP-015-2 Phase 2a | CIP-015-2 Phase 2b |
|---|---|---|
| October 01, 2029 | October 01, 2030 | October 01, 2031 |

# Practical Steps for CIP-015-2 Implementation



Network Architecture Considerations



Asset Management



Engage Early



Cross Functional Team



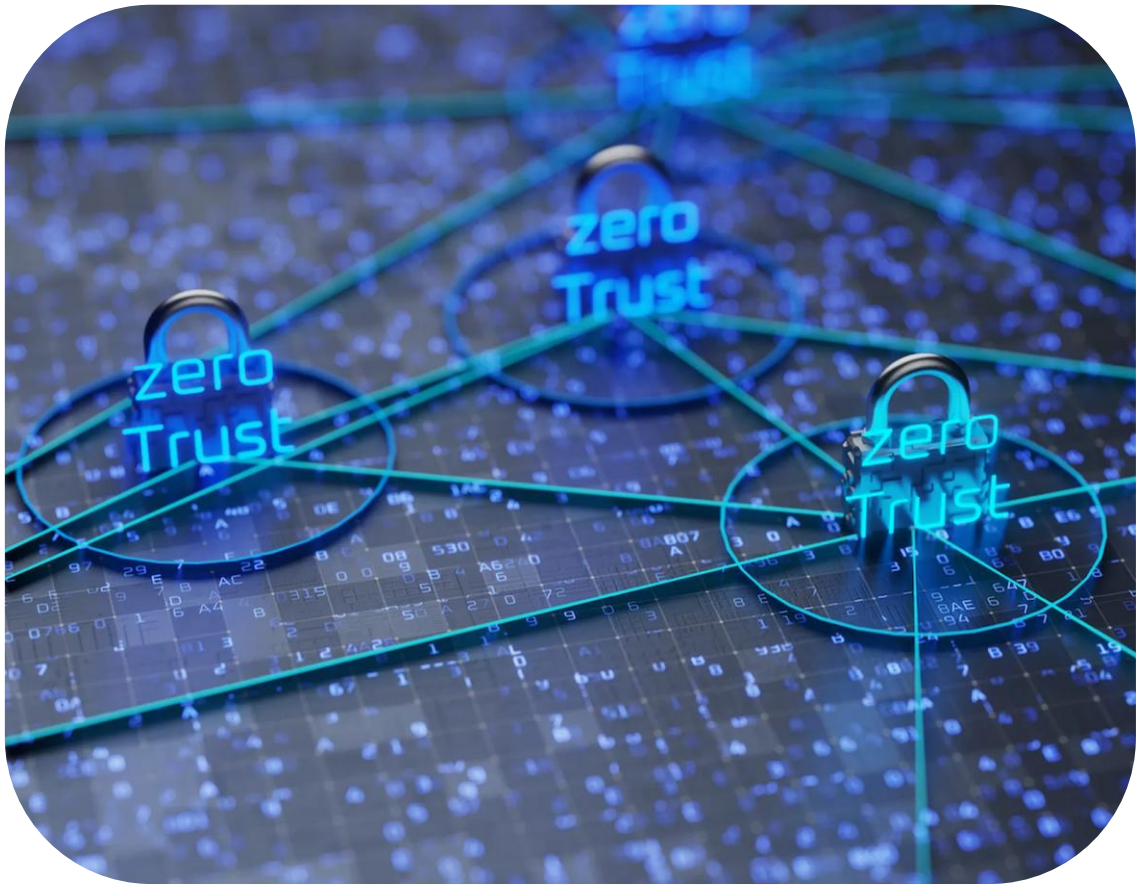
**Effective Date: 10/01/2029**

# Resources

CMEP practice guide-network-monitoring-sensors

SP 800-207, Zero Trust Architecture | CSRC

MITRE ATT&CK®



# Questions?

TEXAS RE
Ensuring electric reliability for Texans

AIONTRACKS

*Linking data centers to stranded electrons™*

# Ask the Hard Questions

## Computational Loads, Ride-Through, and Grid Compatibility

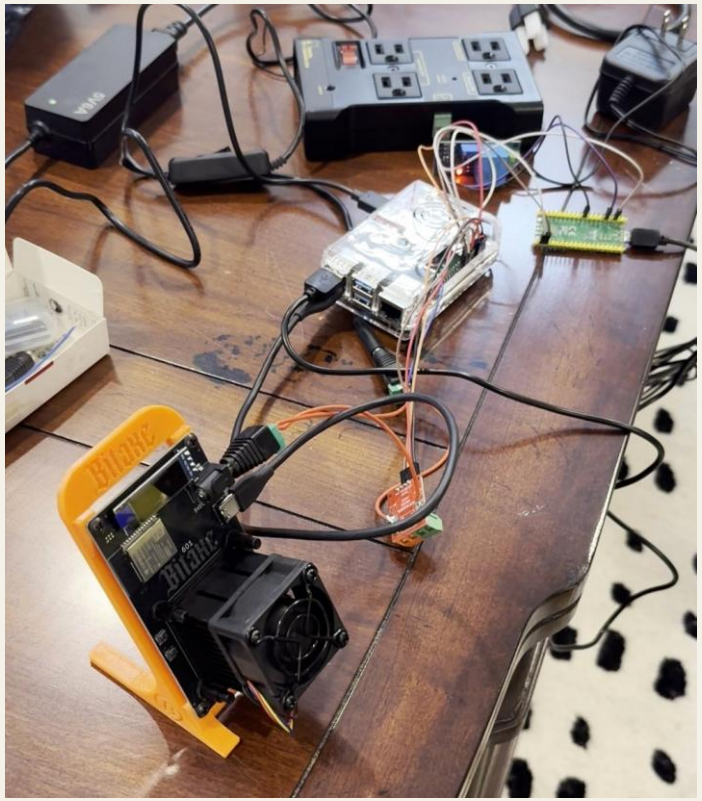
*“You don’t have to swing hard to hit a home run. If you’ve got the timing, it’ll go.” — Yogi Berra*

Praneet K. Sharma, M.D. · Founder and CEO, AIONTRACKS, Inc. · Austin, 4 November 2026

# What I read, built and measured since January

| | |
|---|---|
| **Read** | The ERCOT Nodal Operating Guide, NOGRR282 as approved, PRC-024 through PRC-029, and the NERC incident reviews. |
| **Built** | A facility model from the service delivery point to the chip, and a bench where a production mining chip is driven through programmed voltage sags. |
| **Measured** | Seventy sags on production accelerator workloads, an independent electromagnetic transient study, and the first bench results on mining hardware. |

I am an interventional cardiologist. In January I did not know what a per-unit voltage was.



The bench, September 2026

# John Crowley and Pompe disease, 1998

## 1998

Two of his children were diagnosed with Pompe disease. No treatment existed.

He left his job, founded a biotechnology company, and drove an enzyme replacement therapy through development.

His children are alive today because of that treatment.

## What made the difference

Money and connections helped. Many families with both did not get this result.

He worked on one problem full time for years, with many failed attempts along the way.

The treatment was developed by a parent of patients, with specialists he recruited, outside the established research programs.

Source: CNBC, 1 July 2026, “How my kids’ rare disease drove me to find a cure.”

# $I = P / V$

When power is held constant, current rises as voltage falls.

**A load that holds its power constant reaches 150% of normal current at 0.667 retained voltage. Below that, an unmodified load exceeds any 150% limit.**

Facility voltage is set by the grid. Facility power is set by the load.

# ERCOT reliability concern: 3,200 MW of large-load loss

A fault occurs, loads without ride-through trip or transfer to backup, the load loss drives frequency up, and 60.4 Hz risks cascading outages.

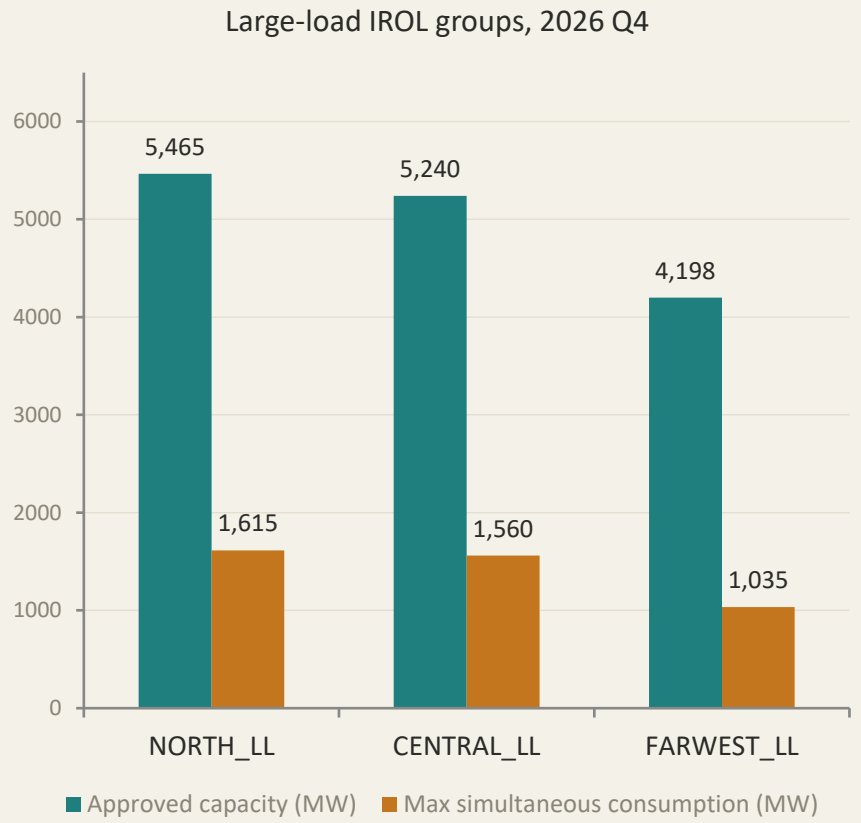
## The quarterly stability assessment

Four-cycle three-phase faults at 147 buses at 345 kV; six-cycle faults at 19 buses at 138 kV.

About 22 GW of large load in the case.

Trip groups are sets of loads that one disturbance can take down together. Any group above 3,200 MW becomes an IROL.

Mitigation plans activate near 2,500 MW and hold each group at 85% of the limit, 2,720 MW, through not-to-exceed limits per TSP and QSE.




## Findings from the Q4 assessment

In West Texas, updated models showing ride-through capability removed loads from the trip group.

Several loads sat on the edge of a voltage sag just below 0.7 pu.

0.7 pu is close to the 0.667 pu at which constant-power current passes 150%.

Pending NOGRR289 would give cooling equipment a 365-day ride-through extension. ERCOT's stated concern: exempted load raises the risk of impending IROL conditions.

Sources: P. Gravois, QSA Results and Large Load IROL Mitigation Plans, ERCOT LLWG, 17 September 2026; ERCOT LLWG 15 October 2026 on NOGRR289.

# The facility from the service delivery point to the chip

NERC reviewed 26 large-load ride-through events on this system in under three years. One lost 19% of a facility at 0.844 pu; recovery took five minutes to two hours.

**1**

### Service delivery point

Where the rule is scored: worst phase, against 150% of that phase's own maximum

**2**

### Transformer

Delta-wye steps change what the UPS actually sees

**3**

### UPS rectifier and DC link

Current limit, undervoltage cessation, battery transfer, walk-in

**4**

### Cooling plant

Chiller motors stall under sag; drives trip on their own DC link

**5**

### Server power supply

Input current limit; bulk capacitor hold-up of 10 to 20 ms

**6**

### Accelerator

The stage where power is set

**Each threshold is set to protect its own equipment. Across a region, these thresholds produce the load loss in ERCOT's assessment.**

Source: NERC Event Analysis, Incident Review: Voltage-Sensitive Crypto Load Reductions, 9 January 2026.

# Properties of computational load under a voltage sag

Five properties that make the load different from motor and lighting load, and one that makes it controllable.

| | |
|---|---|
| **Constant power** | The power supply regulates its output. As input voltage falls, input current rises to keep power constant. |
| **No stored energy of its own** | Bulk capacitors hold up for 10 to 20 ms. Beyond that, the only energy is in the UPS. |
| **Synchronized** | Thousands of machines run the same program in step. They reach their thresholds together. |
| **Protected locally** | Each power supply, UPS and drive trips on its own setting to protect its own equipment. |
| **Fast** | Current rise, DC-link drain and trip all complete within tens of milliseconds. |
| **Controllable** | Power is set by the chip's operating point, which can be changed in milliseconds without disconnecting. |

The first five properties are why computational load trips where other load rides through. The sixth is why it does not have to.

# Miners and AI data centers fail at different places

## Mining facility, no UPS

The supply sits directly on the grid with an integrated power supply.

Field data from a large public miner: ride-through lost near 0.6 to 0.65 pu within 6 to 8 ms, minutes to return.

At 0.65 pu on 240 V service the input is about 156 V, far above the supply's own undervoltage comparator. The failure is delivery-side and depends on load.

Vendor firmware power commands respond in seconds. The window is milliseconds.

## AI data center, behind a UPS

The UPS turns the sag into a rectifier current-limit problem.

The limit caps real power. The shortfall drains the DC link. The link leaves its window. The unit transfers to battery and grid draw falls to zero.

Then the walk-in. Published defaults often ramp back over 15 seconds against a 2 second rule.

The uncontrolled supply has no equilibrium, only a clock.

# NOGRR282 §2.15 on one page: five bands, one ceiling, three clocks

Measured as RMS worst-phase voltage at the service delivery point. In force since 1 August 2026.

| Voltage, pu | Minimum ride-through | What the load may do while connected |
|---|---|---|
| **1.10 to 1.20** | 1.0 s | Consume at the pre-disturbance level |
| **0.90 to 1.10** | Continuous | Consume at the pre-disturbance level |
| **0.80 to 0.90** | 2.0 s | May reduce in proportion to the voltage drop |
| **0.50 to 0.80** | 0.5 s | May reduce as needed to remain connected |
| **0.35 to 0.50** | 0.25 s | May reduce as needed; cooling may trip below 0.35 |
| **Below 0.35** | 0.15 s | May reduce as needed; cooling may trip |

## One ceiling

Current at or below 150% of the facility's normal maximum, per phase, and only during the transient, never beyond 0.5 s.

## Three clocks

Reduce while still drawing: back to 90% within 2 s of voltage recovery.

Cease as a declared transfer or control scheme: begin returning within 0.25 s, 90% within 0.5 s, one action per device per event.

**Cease because the equipment could not ride through: a failure, with root cause in 90 days and a fix in 180. No recovery deadline rescues it.**

Source: ERCOT Nodal Operating Guide §2.15, established by NOGRR282, approved by the PUCT 9 July 2026. Six sags in 90 seconds must be withstood; no trip scheme may key on sag count.

# Measured load reduction against the four tests

Measured accelerator load applied to an independent model of a 9 MW facility on a 69 kV bus. Seven sag depths, ten repetitions each.

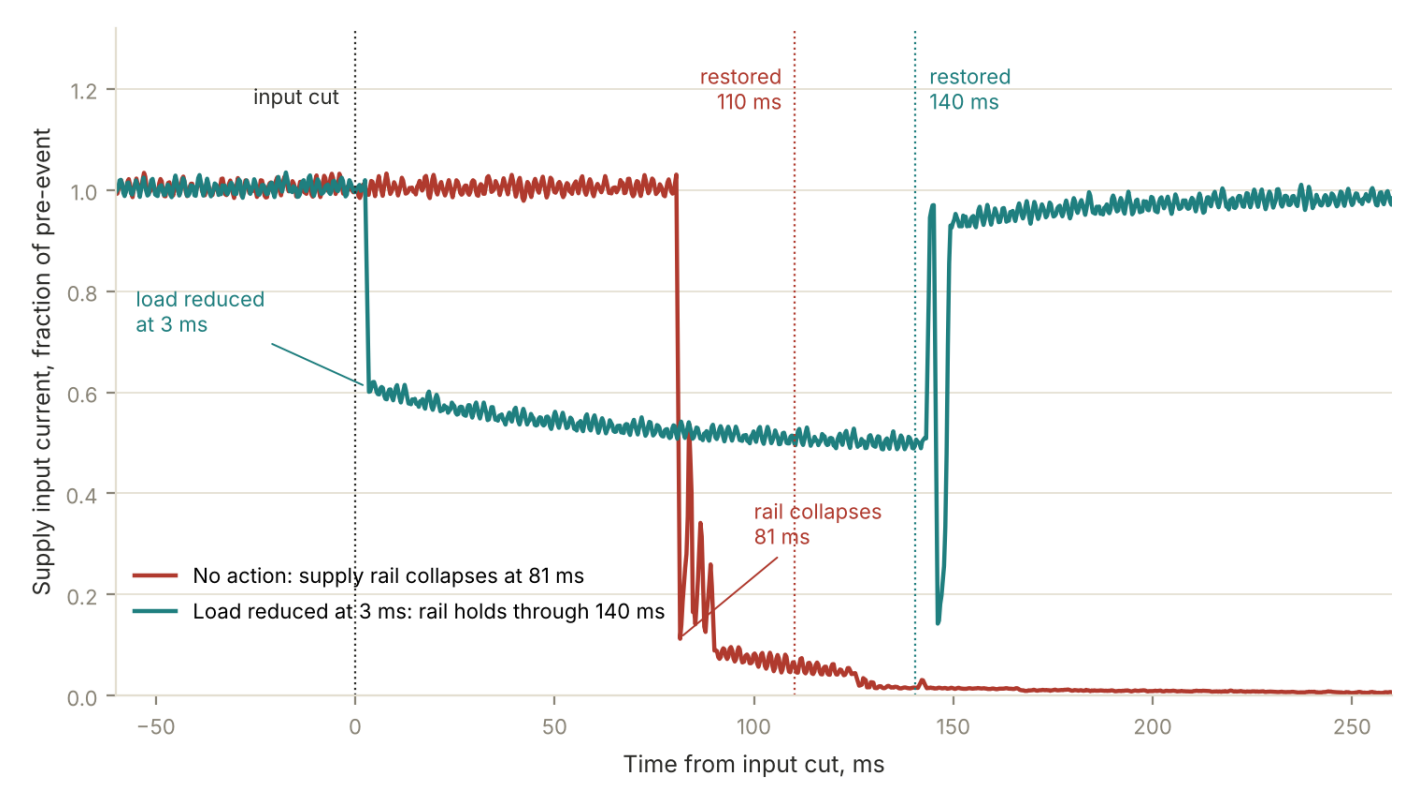
| | |
|---|---|
| ✓ Stay connected and consuming for the Table A durations | **Met at all seven depths** |
| ✓ Current at or below 150% of normal, per phase | **Met to 0.45 retained voltage** |
| ✓ Return to at least 90% within 2 seconds of recovery | **0.41 s median, 0.49 s worst case** |
| ✓ Withstand at least six sags in 90 seconds | **Seven sags in 64 seconds** |

Stored energy sized for the deepest sag is 44% smaller when the load takes part. Stored energy does not lower the current at the meter; reducing the load does.

Source: AIONTRACKS, ERCOT Large Load Working Group, 21 August 2026 (posted at ercot.com). Independent PSCAD/EMT evaluation; the model's protection elements were disabled by design, so it reports current, not trips.

# Mining bench, September 2026

A large public miner asked in September whether its fleet could ride through. A bench on production mining silicon was built and measured within three weeks. The loaned production units are on it now.




### Reduction

One step, about one millisecond from command to the meter.

### Return

90% of pre-disturbance draw within 24 ms median, 48 ms at the 99th percentile.

### Vendor firmware, same chip

565 ms to first change, a 36-step staircase over 3.7 s, 90% at 3.6 s.

### Interruption

No action: rail collapses at 81 ms. Reduced at 3 ms: holds through 140 ms, 90% within 4 ms of restore.

### Sag ladder

420 rungs, 21 injected profiles: ceiling and 2 s return met on every rung.

Bench, Phoenix, 22 September 2026: one production mining chip, 3.2 kHz shunt logger, two interruption cycles from one session at the same baseline. Current is the measured quantity; the decline after the step is the supply rail sagging, not the chip drawing less. Partial-depth sags were injected over a recorded envelope; the hardware-in-the-loop lab supplies them at the input.

# Evidence to date, from model to site

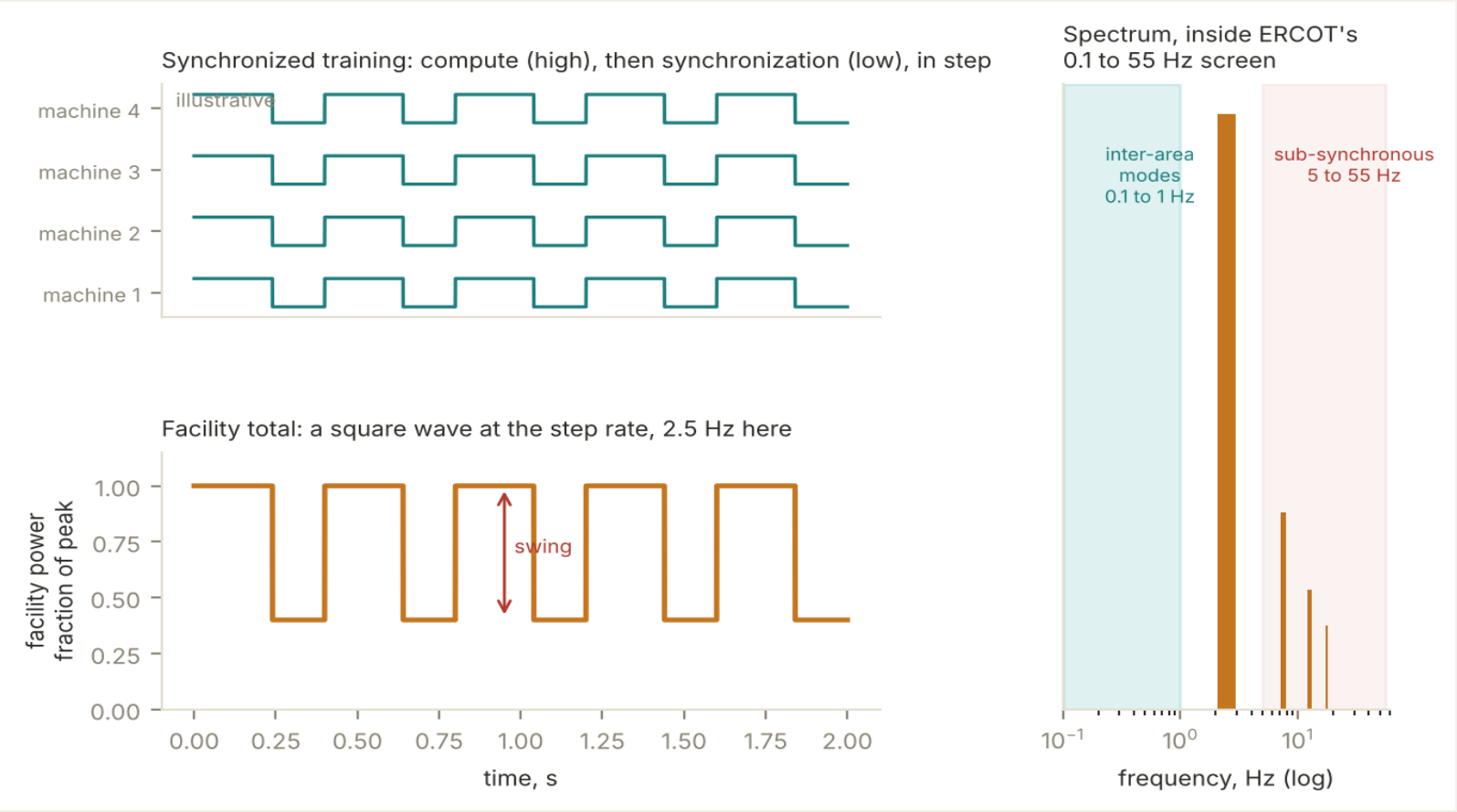
Every figure on these slides traces to a sealed record.

| | | |
|---|---|---|
| **Open-loop electromagnetic transient study** | Independent national-laboratory engineer, open PSCAD model library, 9 MW on 69 kV | **Done** |
| **Silicon measurement** | Four accelerator families from two vendors, production workloads, seventy sags | **Done** |
| **Production mining chip on a bench** | Real actuation under programmed sag; vendor-firmware baseline captured first | **In progress** |
| **Controller hardware-in-the-loop** | RTDS platform at an independent power-electronics laboratory; paired baseline and controller arms | **Starting** |
| **Site** | Facility-level test under a transmission provider's dynamic model review | **Next** |

The facility model predicts that at a 0.55 pu sag the uncontrolled server supply drains its store and trips near 114 ms, and the controlled supply does not. The hardware-in-the-loop run is the test of that prediction.

# How computational load oscillates

Distributed training runs in steps: a compute phase at high power, then a synchronization phase at low power, with every accelerator in the job in step.




Step time is tens to hundreds of milliseconds, so the swing sits at roughly 0.2 to 3 Hz with harmonics above.

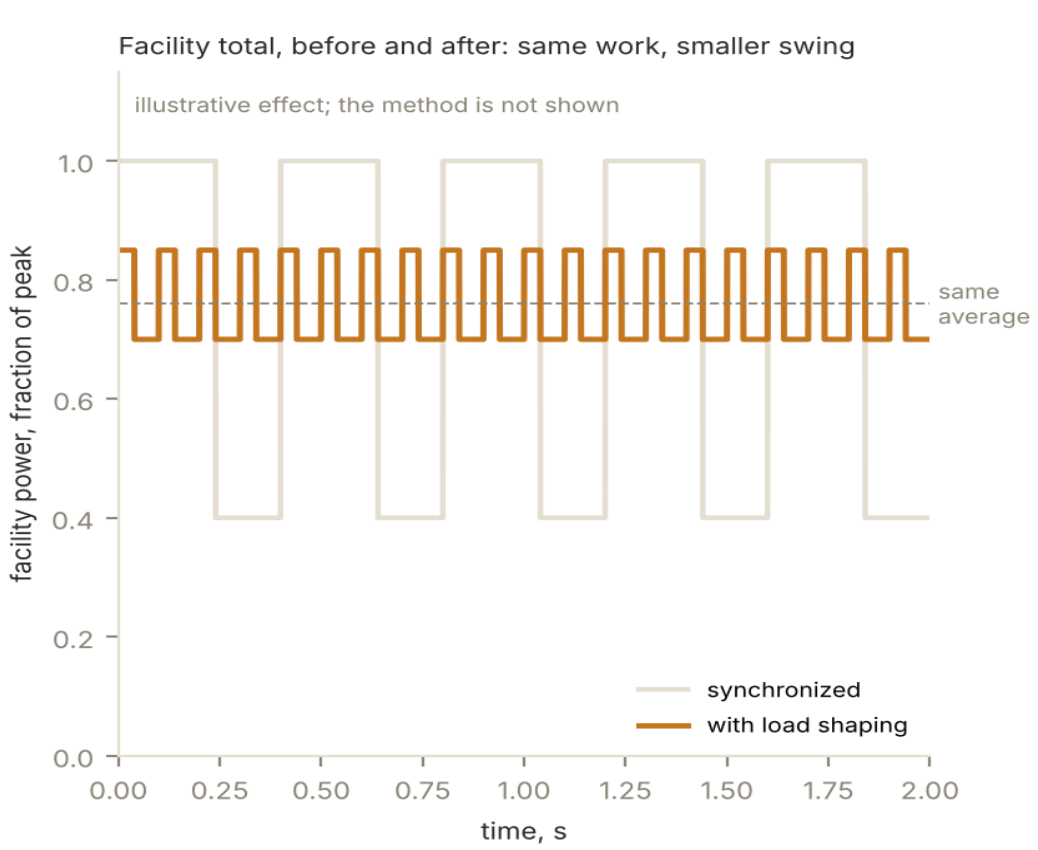
At tens of thousands of accelerators the swing is tens to hundreds of megawatts, documented in published hyperscale measurements.

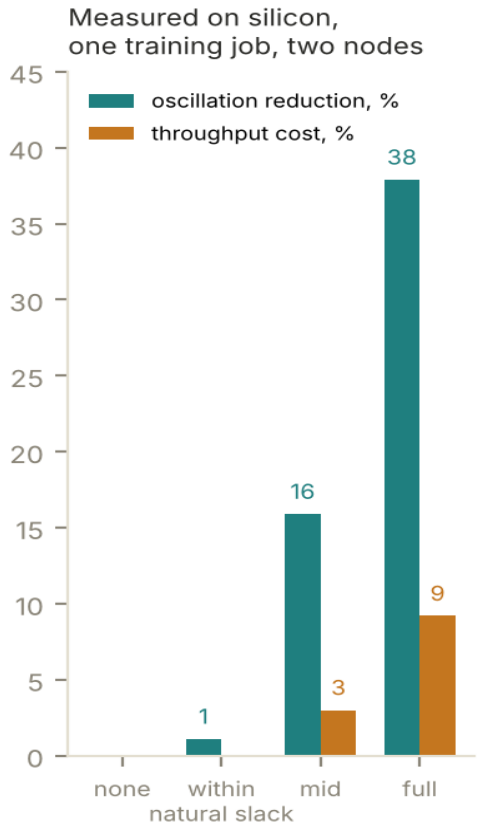
A slower swing, seconds to minutes, comes from jobs starting and stopping and from inference following demand. Planners read it as ramp rate.

ERCOT's draft screen: 10 MW peak-to-peak over a rolling 5 s, 0.1 to 55 Hz, on instantaneous active power. A 100 ms power sensor cannot see the fast band.

Sources: ERCOT LLWG, proposed evaluation of active power variation for Large Computational Loads, June 2026; Microsoft, OpenAI and NVIDIA, power stabilization for AI training datacenters, 2025. Waveforms illustrative.

# Mitigating the oscillation: hardware and load shaping




## Hardware

Batteries, flywheels or capacitors absorb the swing. A power floor keeps the low phase from going low. Both add capital and act on the swing after it exists.

## Load shaping

Acts on the timing of the work rather than on the power. The facility total is smoothed while the work completed is unchanged, and idle phases can carry other useful work.

The two are complementary: shaping reduces how much hardware a site needs; hardware covers what shaping cannot reach. Fleet-scale behavior not yet measured.

Left: illustrative effect only; the method is not depicted. Right: sealed measurement, one training job across two nodes, training result unchanged. Timing-based approaches are published (Michigan State, step-period shifting; Microsoft, OpenAI and NVIDIA, 2025); the approach measured here is a pending patent application and is not described.

# One fault, seven sags: Dominion, 22 July 2026

A fault on a 230 kV line is not one sag. The line's protection recloses into the fault from both ends, and every facility on the line sees each attempt as another sag.




## Why this is the test

Sags 2 and 3 arrive while a UPS that transferred on sag 1 is still walking back in. Settings that survive one sag do not survive three in 400 ms.

Dominion: settings work cut sustained transfer from 1,500 MW in July 2024 to 500 MW in April 2026. In July, customers responded to the first sag and 17 of 20 transferred.

This sequence, with one sag below 0.4 pu added, is the hardware-in-the-loop test case.

Sources: Dominion Energy, ERCOT LLWG 14 October 2026; PJM Planning Committee 8 September 2026. Reclose times and the count of seven sags are as reported; the assignment of sags to the 20 s and 80 s recloses is inferred and not shown.

# Which layers change the current at the service delivery point

| 1 Service delivery point | 2 Cooling and losses | 3 Transformer | 4 UPS front end | 5 Distribution and server supply | 6 Accelerator |
|---|---|---|---|---|---|
| scores | survives | decides | caps, then leaves | survives | sets P(t) |

### Reduce the power at the chip

Removes the deficit. Current at the meter falls with it.

### Cap it at the rectifier

Converts the shortfall into stored-energy drain and a deadline. Then battery, and grid draw goes to zero.

### Leave

Battery transfer or supply trip. This is what puts a facility in an IROL group.

Walk-in, reconnection delay and protection thresholds change when the facility comes back and whether it survived. They do not change the current it drew.

**Oversizing the UPS does not change facility current at the delivery point by one amp.**

# PJM's draft applies ERCOT's 2028 regime to existing sites

| | ERCOT NOGRR282 §2.15 | PJM draft, Planning Committee 6 Oct 2026 |
|---|---|---|
| **Status** | In force since 1 August 2026 | FERC filing planned November 2026 |
| **Scope** | Large Computational Loads under the Nodal Operating Guide | 50 MW or more aggregate; 25 MW or more through power electronics |
| **Below 0.50 pu** | 0.25 s to 0.35 pu; 0.15 s below 0.35 | Single band, 0.25 s |
| **0.50 to 0.90 pu** | Before 2028: reduce as needed to remain connected. After 1 Jan 2028: continue consuming, proportional reduction allowed | Continue consuming; proportional reduction allowed. No phase-in |
| **Recovery, ceiling, sag count** | 90% within 2 s; 150% per phase; six sags in 90 s | Same |
| **Existing facilities** | New agreements | Facilities under construction or in operation: comply by the later of January 2028 or one year after commercial operation |
| **Backup as compliance** | Transfer to battery is the load rejection the rule forbids | Substitution by other resources does not count unless approved in writing on technical infeasibility |

NERC Project 2026-02: the first phase collects ride-through capability data at every 50 MW site and requires dynamic models where available; ride-through performance numbers are expected in 2027. Dominion's 22 July 2026 event: of 20 data centers on a 230 kV line with seven sags and unsynchronized recloses, 3 rode through and 17 transferred.

Sources: ERCOT NOG §2.15; PJM PC 6 Oct 2026 LCL ride-through presentation and redline; NERC CLO-001-1 Draft 1; Dominion Energy, ERCOT LLWG 14 Oct 2026.

# Frequency response: a proposal submitted to ERCOT RIPE

## Frequency ride-through today

NOGRR282 §2.6.4(5) requires a passive hold through frequency excursions; the low edge is 57.5 Hz.

Meeting it is mostly equipment settings: UPS and drive frequency trip points. Load control plays a small part.

§2.6.4(3) reserves space for a dispatched ancillary service that reduces load. For computational load it is not yet defined.

## A coordinated load-reduction service, later

Measured on two vendors' silicon: a 58.7 Hz excursion held within 7 ms with no autonomous shedding; two facilities acting together with simultaneity under one millisecond.

Submitted to ERCOT's Research and Innovation Partnership Engagement program as a joint proof of concept; under review.

Separate from the ride-through work. Offered as a later option, not a current product.

# ERCOT as an island

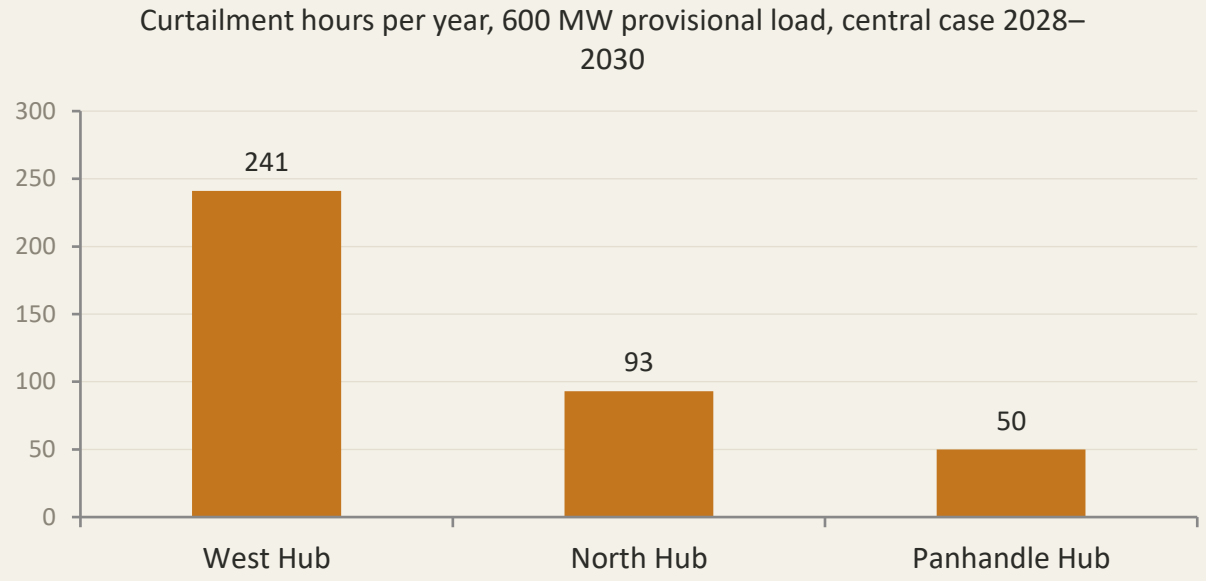
## Isolation and 3,200 MW

ERCOT stands apart from the Eastern and Western Interconnections. The DC ties are small against the system.

Load loss that a continental grid absorbs overshoots frequency here.

The only decorrelation available is inside the island: Panhandle, West, North and Houston have different congestion, weather and reserve dynamics.

Power cannot cross a binding 345 kV constraint. Computational work can move between facilities over fiber in milliseconds.




Aurora: local curtailment events arrive with as little as five minutes' notice, which limits shifting computing loads. A co-sited battery provides hours of lead time. Moving the compute within that lead time is the complementary step.

Source: Aurora Energy Research for Google and V-Wire, Curtailment Mitigation for PCLRs, ERCOT LLWG, September 2026.

# Evidence a facility can show under NOGRR282 and the NERC drafts

| | | |
|---|---|---|
| **Capability declaration** | Parameters, settings and capabilities for cessation, tripping, ride-through and recovery, declared at interconnection. | NOGRR282 §2.15; CLO-001 draft R8.1.1 |
| **Commissioning test** | A sag test at energization with recorded current per phase at the service delivery point, against Table A and the 150% ceiling. | CLO-001 draft R2.4; ERCOT LLIS |
| **Disturbance recording** | Point-on-wave or PMU capture at the delivery point for every event, with the 2 s recovery measured from it. | CLO-003 draft; PRC-028 practice |
| **Dynamic model and verification** | A model whose parameters come from measurement, re-verified within 180 days of any hardware, software, firmware or setting change that alters the response. | PGRR144 model quality testing; CLO-001 draft R11.2.2 |
| **Event performance** | On a failure: root cause within 90 days, a plan within 90 days, implementation within 180. | NOGRR282 §2.15(8) |

The NERC draft treats software and settings as part of the dynamic response. A load controller is therefore part of the model, and its evidence belongs in the same file.

# Five open problems

| | | |
|---|---|---|
| 1 | **Per-phase detection under real facility noise** | Needs recorded three-phase point-on-wave data from an operating site. |
| 2 | **The composite response when levers fire together across a hundred-chip chain** | Completion skew is unmeasured. |
| 3 | **The fast oscillation band** | No common instrument resolves it at the meter. |
| 4 | **A dynamic model block that passes PGRR144 model quality testing** | Parameters from measurement, not assumption. |
| 5 | **Ride-through for facilities already in service** | Which failures are fixed by settings, and which need load control. Dominion's April and July events show both. |

# Thank you

*“If you ask me anything I don’t know, I’m not going to answer.” — Yogi Berra*

Praneet K. Sharma, M.D. · praneet@aiontracks.com · AIONTRACKS, Inc., Phoenix

August 2026 ERCOT LLWG study: AIONTRACKS_LLWG_2026-08-21_FINAL_v3.pdf at ercot.com. The independent EMT evaluation is acknowledged there as printed.

# Reserve: the cooling plant under sag

| | |
|---|---|
| **Chiller** | Direct-on-line induction motor. Stalls under deep sag, draws locked-rotor current, re-accelerates over hundreds of milliseconds. |
| **Air handlers** | Variable-frequency drives with their own DC link: a short hold-up and an undervoltage trip. |
| **The rule** | Cooling may trip below 0.35 pu and its share is subtracted from the recovery base. Above 0.35, a cooling trip is compliant if facility total consumption returns to 90% within 2 s. That is one shared 10% budget. |
| **Arithmetic** | At PUE near 1.25 cooling is about 15% of total. If all of it stays off the facility fails the 90% test. Liquid-cooled sites with cooling under 10% pass. |

# Reserve: the UPS cap-and-wait sequence

1. Sag begins
2. Rectifier reaches its current limit; real power is capped
3. Shortfall is drawn from the DC link
4. DC link leaves its window
5. Transfer to battery; grid draw goes to zero
6. Sag clears; rectifier walks back in
7. 90% reached, or not, by 2 s

The limit does not remove the deficit. It finances the deficit from storage and starts a timer. Only the step from 1 to 2 can be avoided, and only by lowering power before the limit binds.

Walk-in is a settings item inside vendors' adjustable range. Published defaults are often 15 s.

# Reserve: provisional load curtailment exposure by site

| Site | Hours per year | Events per year | Average severity | Curtailed energy |
|---|---|---|---|---|
| West Hub | 241 | 31.7 | 25% | 0.87% |
| North Hub | 93 | 17.3 | 75% | 0.83% |
| Panhandle Hub | 50 | 10.3 | 80% | 0.47% |

600 MW provisional controllable load per site, 2028–2030, 2013-style weather year. Across weather years: 35 hours in the mildest, 550 in the most extreme. A netted 4-hour battery cut hours by 83% on average; without netting, 53%.

Source: Aurora Energy Research for Google and V-Wire, September 2026, posted to the ERCOT LLWG.

# Reserve: the NERC January 2026 incident review

**26**

large-load ride-through events reviewed on this system in under three years

**150 to 160%**

of pre-fault current at facilities studied; some tripped their own breakers on overcurrent during a 50 ms dip

**19%**

of one facility's load lost from a dip to 0.844 pu

**5 min to 2 h**

recovery range

Source: NERC Event Analysis, Incident Review: Voltage-Sensitive Crypto Load Reductions, 9 January 2026. The facilities reviewed largely lack UPS.

# Texas RE Fall Standards, Security, & Reliability Workshop

November 4, 2026

## AGENDA

- Resilience Through Protected Communication (CIP-012)
- Walking the Line of Defense (CIP-003, CIP-006, CIP-014)
- Inside Threats, Inside Visibility (CIP-015)
- Ask the Hard Questions: Computational Loads, Ride-through, and Grid Compatibility
- **Mitigating Misoperation Risk and Finishing the Fix**
- Ride-through Ready (PRC-028, PRC-029, PRC-030)
- Closing the Facility Ratings Gap (FAC-008)

## Break

Will Return at: 1:00

To submit questions during the workshop, please visit **slido.com** and enter today's participant code: **TXRE**



# Mitigating the Risks of Misoperations and Finishing the Fix

Allie Huey – O&P Compliance Eng.
Jeff Hargis – Risk Assessment Eng., Sr.

# Agenda

- Misoperation Rates and Trends
- Review of Risk
- PRC-004-6 Standard and Supplemental Material
- Requirements R1 and R5 – Engagement Ready
- Common Issues
- Internal Controls

# The Good News

"The overall count of misoperations in 2025 was the lowest over the past five years."

NERC's 2026 State of Reliability

# Why might Protection System Misoperations still be considered an ongoing risk?



Join at Slido.com
Use the code TXRE

# So, why is Texas RE talking about PRC-004-6?

Rapid addition of entities responsible for Protection System performance

Practices remain that indicate residual risk

Rise in Misoperation impact score and misoperation-related events

Misoperations may complicate future events

# Misoperation Impact Score

The **misoperations impact score** measures the estimated impact of each misoperation on the BES, which is then aggregated to assess overall performance.

The Texas Region's increase was primarily driven by misoperations reported by **new Generator Owners (GOs)**, **increasing misoperations on 345 kV equipment** (the highest voltage in the Region), and the **use of the "unknown" cause code**.

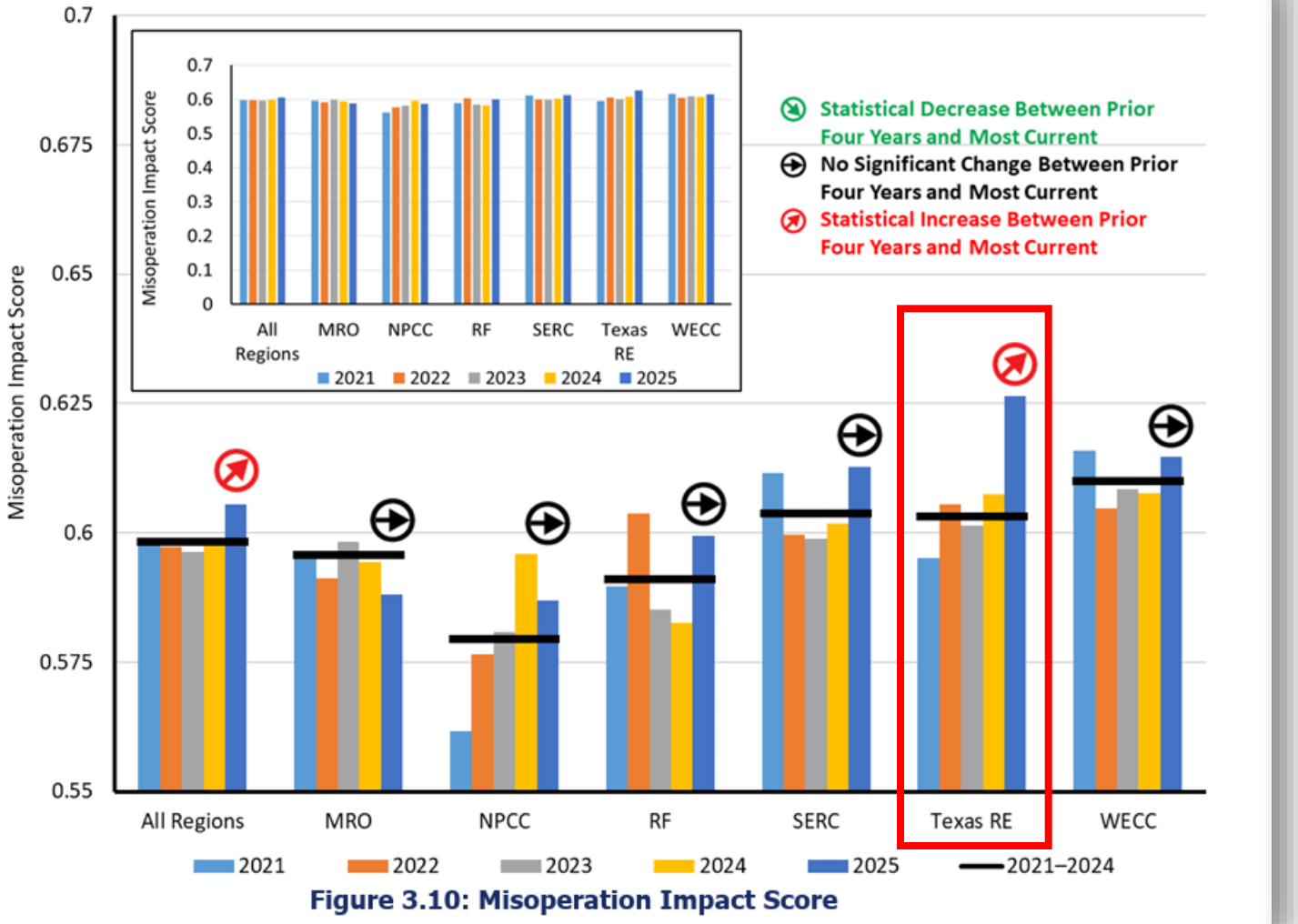



Figure 3.10: Misoperation Impact Score

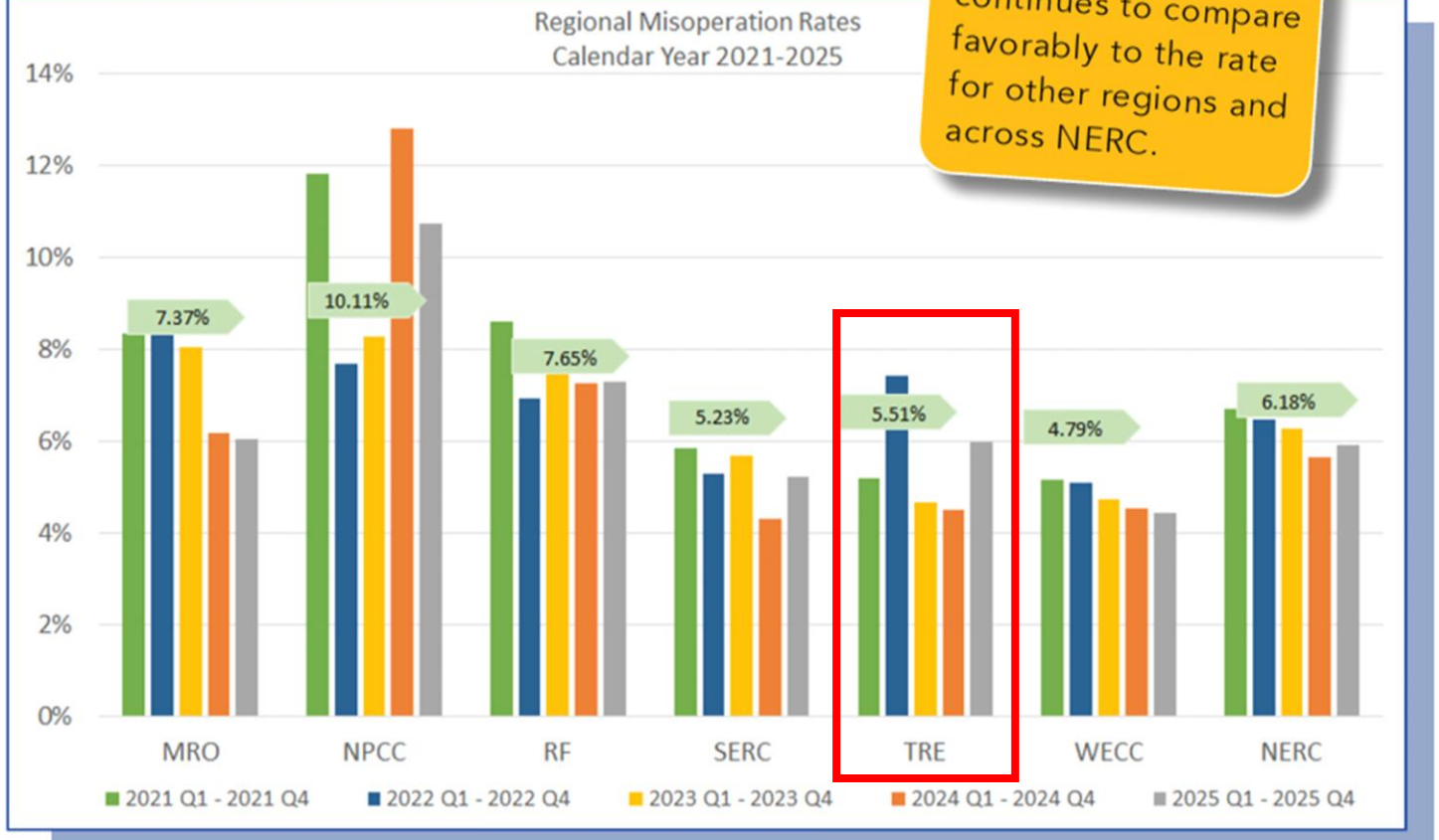
NERC's 2026 State of Reliability

# Texas RE & Misoperations

**AREAS TO MONITOR INCLUDE:**

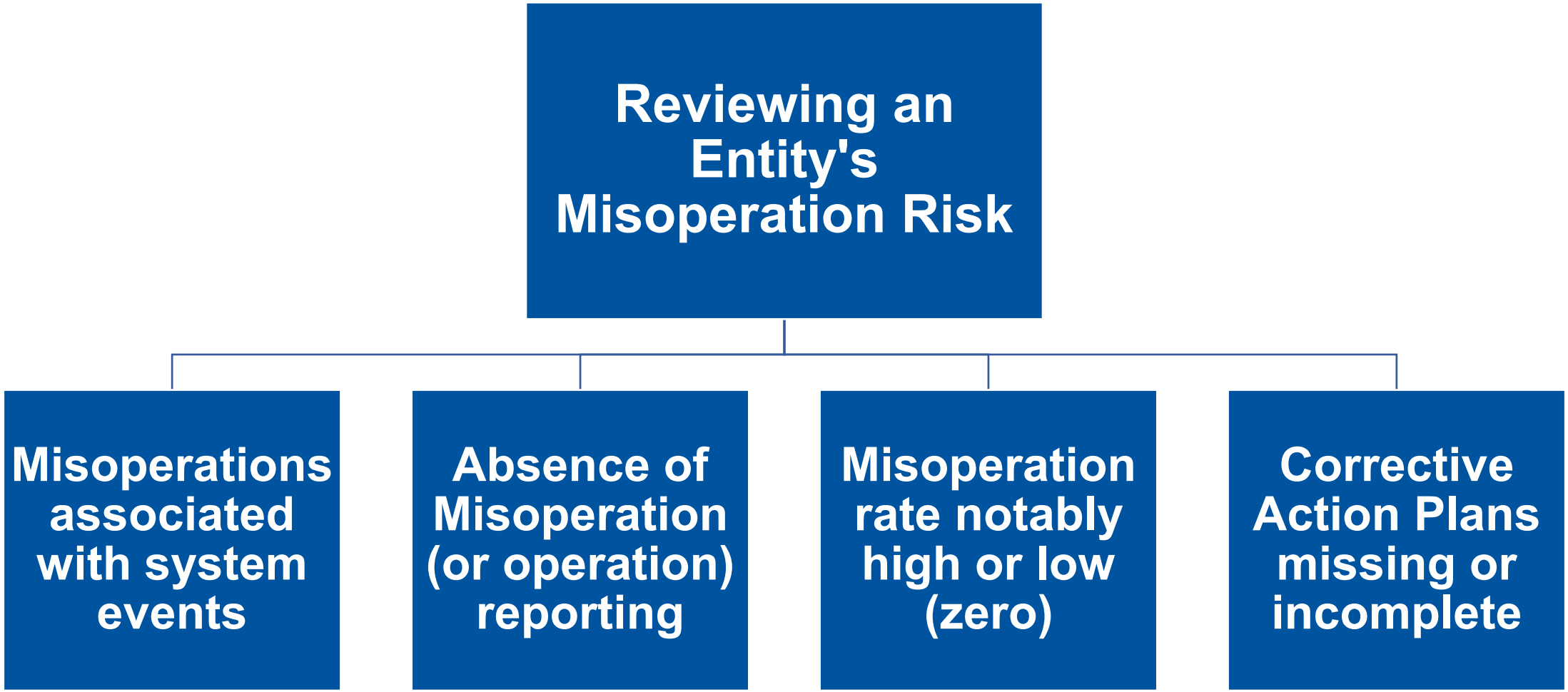
- Incorrect settings, logic, and design errors remained the largest cause of Misoperations, accounting for 26 percent of Misoperations in 2025.
- Misoperations with an unknown cause continued to increase in 2025, which warrants additional monitoring.

The Texas RE Region Protection System Misoperation rate continues to compare favorably to the rate for other regions and across NERC.




**Texas RE's 2025 Assessment of Reliability Performance**

# Risk Review


Reviewing an Entity's Misoperation Risk
Misoperations associated with system events
Absence of Misoperation (or operation) reporting
Misoperation rate notably high or low (zero)
Corrective Action Plans missing or incomplete

# PRC-004-6 Protection System Misoperation Identification and Correction

## Purpose

- Identify and correct the causes of Misoperations of Protection Systems for Bulk Electric System (BES) Elements.

## Functional Entities

- Transmission Owner
- Generator Owner
- Distribution Provider

## Facilities

- Protection Systems for BES Elements (see Standard for exclusions)
- Underfrequency load shedding (UFLS) that is intended to trip one or more BES Elements
- Undervoltage load shedding (UVLS) that is intended to trip one or more BES Elements

# Supplemental Material: Guidelines and Technical Basis

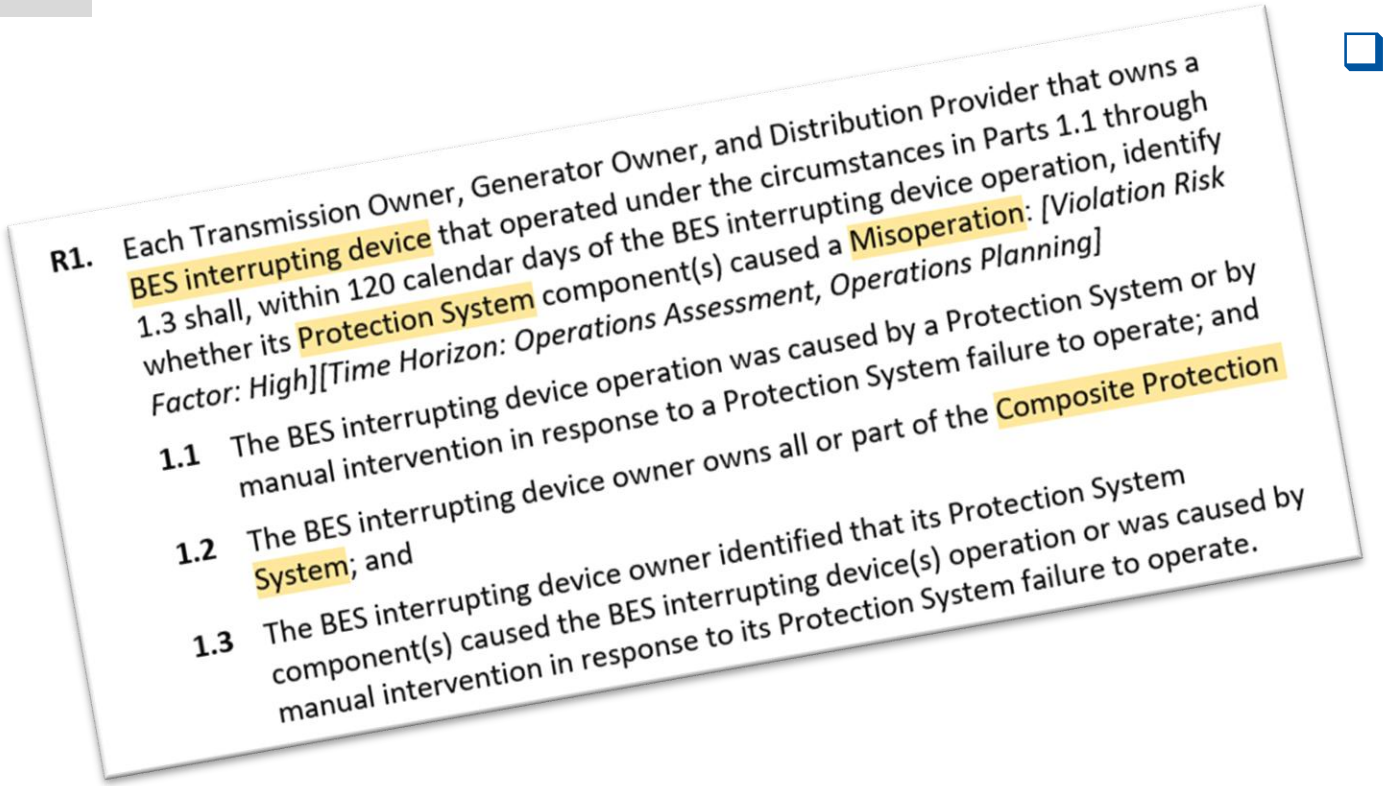
Definitions and Examples

Special Cases

CAPs and Declarations

Time Periods and Flow Charts

# PRC-004-6 Requirement R1



**R1.** Each Transmission Owner, Generator Owner, and Distribution Provider that owns a BES interrupting device that operated under the circumstances in Parts 1.1 through 1.3 shall, within 120 calendar days of the BES interrupting device operation, identify whether its Protection System component(s) caused a Misoperation: *[Violation Risk Factor: High][Time Horizon: Operations Assessment, Operations Planning]*

**1.1** The BES interrupting device operation was caused by a Protection System or by manual intervention in response to a Protection System failure to operate; and

**1.2** The BES interrupting device owner owns all or part of the Composite Protection System; and

**1.3** The BES interrupting device owner identified that its Protection System component(s) caused the BES interrupting device(s) operation or was caused by manual intervention in response to its Protection System failure to operate.

## ❑Protection System

- Protective relays which respond to electrical quantities,
- Communications systems necessary for correct operation of protective functions,
- Voltage and current sensing devices providing inputs to protective relays,
- Station dc supply associated with protective functions (including station batteries, battery chargers, and non-battery-based dc supply), and
- Control circuitry associated with protective functions through the trip coil(s) of the circuit breakers or other interrupting devices.

## ❑BES interrupting device

- A BES Element, typically a circuit breaker or circuit switcher that has the capability to interrupt fault current.

## ❑Composite Protection System

- The total complement of Protection System(s) that function collectively to protect an Element.

# PRC-004-6 Requirement R1 cont'd

**Misoperation** – The failure of a Composite Protection System to operate as intended for protection purposes. Any of the following is a Misoperation:

1. ***Failure to Trip – During Fault*** – A failure of a Composite Protection System to operate for a Fault condition for which it is designed. The failure of a Protection System component is not a Misoperation as long as the performance of the Composite Protection System is correct.
2. ***Failure to Trip – Other Than Fault*** – A failure of a Composite Protection System to operate for a non-Fault condition for which it is designed, such as a power swing, undervoltage, overexcitation, or loss of excitation. The failure of a Protection System component is not a Misoperation as long as the performance of the Composite Protection System is correct.
3. ***Slow Trip – During Fault*** – A Composite Protection System operation that is slower than required for a Fault condition if the duration of its operating time resulted in the operation of at least one other Element's Composite Protection System.
4. ***Slow Trip – Other Than Fault*** – A Composite Protection System operation that is slower than required for a non-Fault condition, such as a power swing, undervoltage, overexcitation, or loss of excitation, if the duration of its operating time resulted in the operation of at least one other Element's Composite Protection System.
5. ***Unnecessary Trip – During Fault*** – An unnecessary Composite Protection System operation for a Fault condition on another Element.
6. ***Unnecessary Trip – Other Than Fault*** – An unnecessary Composite Protection System operation for a non-Fault condition. A Composite Protection System operation that is caused by personnel during on-site maintenance, testing, inspection, construction, or commissioning activities is not a Misoperation.

# PRC-004-6 Requirement R5

**R5.** Each Transmission Owner, Generator Owner, and Distribution Provider that owns the Protection System component(s) that caused the Misoperation shall, within 60 calendar days of first identifying a cause of the Misoperation: [*Violation Risk Factor: High*] [*Time Horizon: Operations Planning, Long-Term Planning*]

- Develop a Corrective Action Plan (CAP) for the identified Protection System component(s), and an evaluation of the CAP's applicability to the entity's other Protection Systems including other locations; or
- Explain in a declaration why corrective actions are beyond the entity's control or would not improve BES reliability, and that no further corrective actions will be taken.

**Corrective Action Plan (CAP):** A list of actions and an associated timetable for implementation to remedy a specific problem.

# PRC-004-6 Requirement R5 CAP Example

**Issue**

The following is an example of a CAP for a relay Misoperation that was applying a standing trip due to a failed capacitor within the relay. An evaluation of the cause at similar locations determined capacitor replacement was not necessary elsewhere.

**CAP**

**Actions:** Remove the relay from service. Replace capacitor in the relay. Test the relay. Return to service or replace by 12/31/2025.

Applicability to other Protection Systems: Tests of similar relays at other locations have not shown any similar issues. Therefore, it is assessed that replacement of capacitors in this type of relay does not need to be established for the system.

**Completed CAP**

**Actions:** The impedance relay was removed from service on 09/02/2025 because it was applying a standing trip. A failed capacitor was found within the impedance relay and replaced. The impedance relay functioned properly during testing after the capacitor was replaced. The impedance relay was returned to service on 11/02/2025.

CAP completed on 11/02/2025

# Engagement Ready – PRC-004-6 R1 & R5

## R1

- [ ] Evidence that demonstrates the Owner identified the Misoperation within the allotted time period
- [ ] A list of BES interrupting device operations
- [ ] Templated analysis/investigation form
- [ ] Process document
- [ ] Task reminders to ensure that 120 calendar days is met

## R5

- [ ] Evidence that demonstrates a CAP was developed and an evaluation of the CAP's applicability to other Protection Systems and locations was performed
- [ ] A list of Misoperations
- [ ] Templated CAP form
- [ ] Process document
- [ ] Task reminders to ensure that 60 calendar days is met

# Common Issues

- Failure to identify whether the Protection System component caused a Misoperation
- Not including all requirement language in process document
- Incomplete CAP and not tracking through completion
- Maintenance of MIDAS records
- Failure to clearly define and communicate timeframes
- Lack of a peer review process

# Internal Controls



## Ensure accurate identification of Misoperations

- Documented process/procedure for PRC-004-6
  - Definitions
  - Roles & responsibilities
  - Establish periodic reviews
- Track/list Misoperations
- Templated form



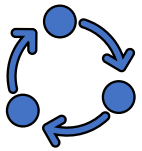
## Manage Corrective Action Plans

- Templated form for capturing CAP details
- Automated task reminder for deadlines
- Perform peer reviews for completeness



## Complete MIDAS reporting with accuracy

- Reminders to complete MIDAS
- Document roles & responsibilities
- Perform peer reviews



## Support full compliance with PRC-004-6

- Documentation
- Record keeping
- Automated task reminders for deadlines

# References

- PRC-004-6
- Misoperation Information & Data Analysis System
- Misoperations Impact Score
- NERC's 2026 State of Reliability
- Texas RE's 2025 Assessment of Reliability Performance
- System Protection and Control Working Group (SPCWG)

# Questions?

TEXAS RE
Ensuring electric reliability for Texans



# Ride-through Ready: PRC-028-1, PRC-029-2, & PRC-030-1

**Blake Ianni**
**O&P Compliance Team Lead**

# Agenda

- Protection Settings Overview
- PRC-028-1 & PRC-029-2: Requirements & Implementation Plans (IPs)
- Enforcement Discretion & Periodic Data Submittal (PDS) Processes
- Best Practices & Controls
- PRC-030-1 Requirements & Implementation Plan



# Protection Settings Objectives



Ensure settings are properly calculated for applicable frequency and voltage protections



Analyze the effects of frequency and voltage excursions on the system protection



Set frequency and voltage protection to prevent trips and momentary cessation within the “no trip zone”

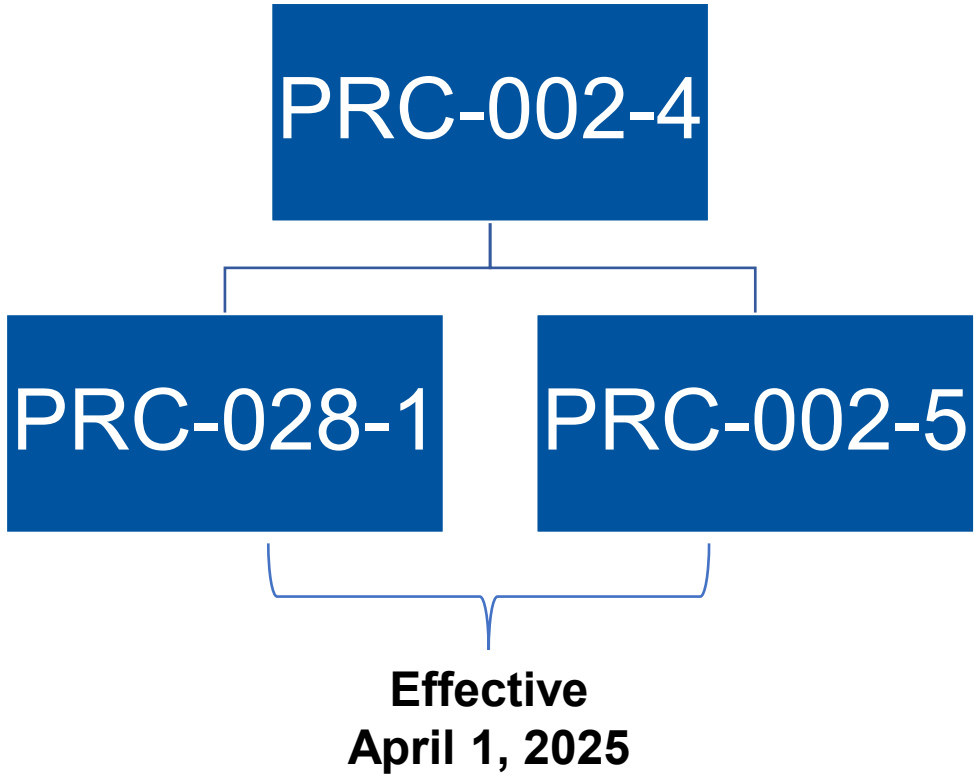
# Background of PRC-028-1

## PRC-002-5 Applicability

- Reliability Coordinator
- Transmission Owner
- Generator Owner excluding inverter-based resources (IBRs)

## PRC-028-1 Applicability

- Generator Owner
  - Facilities:
    - Bulk Electric System (BES) IBRs
    - Non-BES IBRs with:
      - Aggregate nameplate ≥ 20 mVA **and**
      - Connected to common point of connection ≥ 60 kV



# PRC-028-1 Disturbance Monitoring and Reporting for IBRs

## Purpose

- To have adequate data available from IBRs to evaluate IBR Ride-through performance during system disturbances and to provide data for IBR model validation

## Requirements

- R1 – Sequence of event recording (SER) data
- R2 & R3 – Fault recording (FR) data
- R4 & R5 – Dynamic Disturbance Recording (DDR) data
- R6 – Time synchronization
- R7 – Providing requested SER, FR, and DDR data
- R8 – Restore recording capability or submit CAP

# PRC-028-1 Implementation Plan

## *BES IBRs

### Commercial Operations Date (COD) on/before 4/1/2025

- ❑ 12/31/2028-50% of BES IBRs comply with R1-R7
- ❑ 1/1/2030-100% of BES IBRs comply with R1-R7

### COD after 4/1/2025 but within 15 calendar months of Effective Date**

- ❑ 100% of BES IBRs comply with R1-R7 within 15 calendar months-7/31/2026 COB

### COD after 15 calendar months of Effective Date

- ❑ 100% of BES IBRs comply with R1-R7 by COD

### BES IBRs (Regardless of COD)

- ❑ R8—comply by 1/1/2026

## Non-BES IBRs (Category 2)

### Commercial Operations Date (COD) on/before 5/15/2026

- ❑ 1/1/2030-100% of non-BES IBRs comply with R1-R7

### COD after 5/15/2026 but within 15 calendar months of Effective Date**

- ❑ 100% of non-BES IBRs comply within 15 calendar months-7/31/2026 COB

### COD after 15 calendar months of Effective Date

- ❑ 100% of non-BES IBRs comply with R1-R7 by COD

### Non-BES IBRs (Regardless of COD)

- ❑ R8—comply by 4/1/2027

**Effective Date: April 1, 2025*

***Refer to CMEP Practice Guide: Implementation of "Annual" and "Calendar Month(s)"*

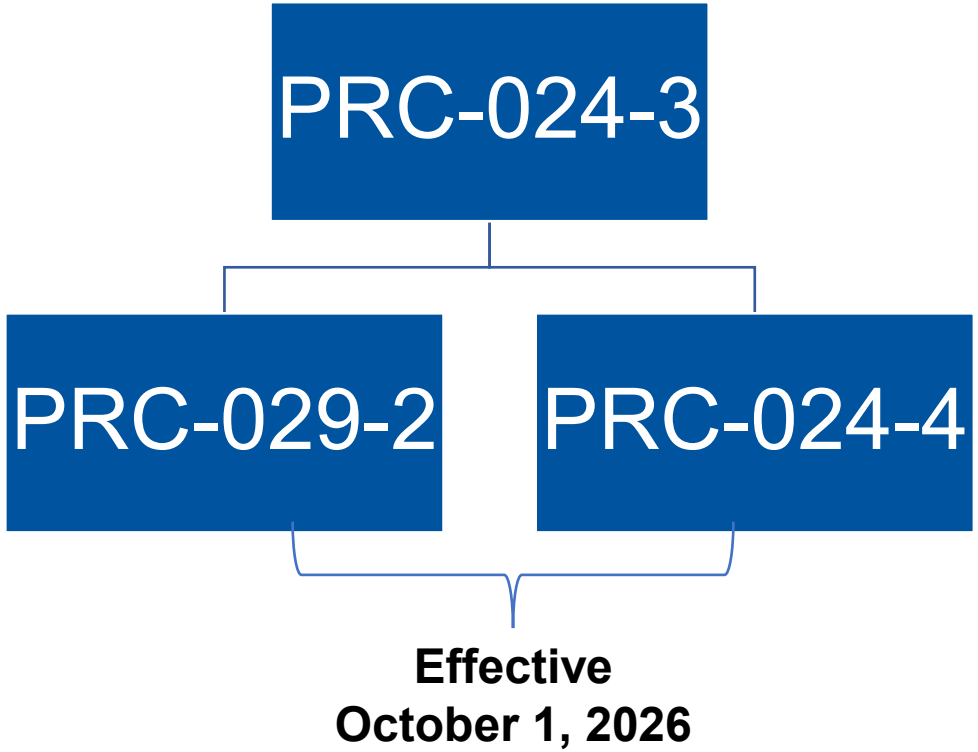
# Background of PRC-029-2

## PRC-024-4 Applicability

- Synchronous generators
- Type 1 and type 2 wind resources
- Synchronous condensers

## PRC-029-2 Applicability

- BES IBRs
- Non-BES IBRs with:
  - Aggregate nameplate ≥ 20 mVA **and**
  - Connected to common point of connection ≥ 60 kV



# PRC-029-2 Frequency and Voltage Ride-through for IBRs

## Purpose

- To ensure that IBRs Ride-through to support the BPS during and after defined frequency and voltage excursions.

## Requirements

- R1 & R2 – Voltage Ride-through capabilities
- R3 – Frequency Ride-through capabilities
- R4 –Hardware limitations

# PRC-029 Implementation Plan—Design vs. Operations

## The Implementation Plan (IP) for PRC-029 bifurcates the capability-based (design) elements & the performance-based (operation) elements for PRC-029 for R1-R3

### Design Elements for Voltage and Frequency Ride-through

- Capability-Based, see Enforcement Discretion Practice Guide
- From R1, Measure 1: “Each Generator Owner shall have evidence to demonstrate the design of each IBR will adhere to Ride-through requirements, as specified in Requirement R1.”
  - Examples of evidence: dynamic simulations, studies, plant protection settings, and control settings design evaluation.

### Operations Elements for Voltage and Frequency Ride-through

- Performance-Based
- From R1, Measure 1: “Each Generator Owner shall retain evidence of actual disturbance monitoring (i.e., sequence of event recorder, dynamic disturbance recorder, and fault recorder) to demonstrate that the operation of each IBR did adhere to Ride-through requirements, as specified in Requirement R1.”

# PRC-029-2 Implementation Plan

## *BES IBRs

### Commercial Operations Date (COD) on/before Effective Date

- ❑ 10/1/2026—100% of BES IBRs comply with R1, R2, & R3 ***design***

### COD after Effective Date

- ❑ Immediately comply with R1, R2, & R3 ***design*** by COD

### BES IBRs (Regardless of COD)

- ❑ Comply with R1, R2, and R3 ***operations*** aspect
- ❑ Date depends on PRC-028-1 deadlines (when entity establishes Disturbance Monitoring Equipment (DME) capabilities)

## Non-BES IBRs (Category 2)

- ❑ 1/1/2027-100% of non-BES IBRs comply with R1, R2, & R3 ***design***

### Non-BES IBRs (Regardless of COD)

- ❑ Comply with R1, R2, and R3 ***operations*** aspect
- ❑ Date depends on PRC-028-1 deadlines (when entity establishes DME capabilities under PRC-028-1)

**Effective Date: October 1, 2026*

# PRC-029-2 IP for Requirement R4

## BES IBRs & Applicable Non-BES IBRs

### In-Service & Subject to Compliance with NERC Standards on or before 10/01/26:

- ❑ R4 Limitations due by 10/01/27

### In-Service on or before 10/01/26 but not yet Subject to Compliance with NERC Standards:

- ❑ R4 Limitations due by later of: (1) 90 calendar days after the date the GO is required to comply with NERC Standards for the applicable IBR; or (2) the effective date of PRC-029-2*

### In-Service after 10/01/26:

- ❑ R4 Limitations due by later of: (1) 90 calendar days after the date the GO is required to comply with NERC Standards for the applicable IBR; or (2) the effective date of PRC-029-2*

*Effective Date: October 1, 2026*

# Enforcement Discretion & Additional Context for PRC-029-2

## CMEP Practice Guide: PRC-029 Enforcement Discretion

- Acknowledges the current OEM/vendor backlog to support GOs implementing setting modifications by compliance dates
- Clarifies that “design” requires the physical implementation of settings on active units
- Entities shall seek Enforcement Discretion prior to their compliance dates (10/01/26 for BES IBRs and 01/01/27 for non-BES IBRs)

## PRC-029-2 Context

- Project 2025-05 Ride-Through Revisions: Directed by FERC Order 909
- PRC-029-2 was approved by FERC on 09/30/2026 and became effective 10/01/2026
- Now accounts for:
  - (1) Limited exemptions for High-Voltage Direct Current (HVDC)-connected IBRs that pose thermal damage risk to equipment (see Item 12 in Attachement 1 of the Standard); and
  - (2) Long-lead time between adopting IBR design specifications and placing the IBR in-service

# Protection Settings—Best Practices & Controls



- Periodically perform an evaluation of Ride-through capability
- Collaborate closely with equipment manufacturer on settings & any firmware upgrades, or parameter changes needed after installation
- Base settings on equipment capability & leave a buffer zone between trip settings & the must Ride-through zone

# Periodic Data Submittals (PDSs) Overview

## PDSs for PRC-028-1

- R1 through R8—Requesting extension of compliance dates
- R8-Corrective Action Plan (CAP) after failure of recording capability

## PDS for PRC-029-2

- R4—Hardware Limitations (exemption from Ride-through criteria)



# PRC-028-1 PDS for Compliance Date Extension




## Overview of PRC-028-1 Compliance Date Extension

- Based on the Implementation Plan for PRC-028-1
- GOs may request an extension from the compliance dates for Requirements R1-R8
- For IBRs that were COD before the April 1, 2025, effective date
- For circumstances beyond GO's control that prevent installation of Disturbance Monitoring Equipment on its IBRs
- Due at least 3 months prior to compliance date for which extension is being requested

# PRC-028-1 PDS for Compliance Date Extension (Cont.)

## PDS extension request via Align

## Includes a spreadsheet to download, complete, and upload to SEL

## Supporting info listed on pg. 4 of IP

- **1.1.** Identification of the inverter-based resource(s) for which the entity requests the extension
- **1.2.** A plan for installing the Disturbance Monitoring Equipment and a timetable for completion
- **1.3.** A description of the circumstances precluding the timely installation of Disturbance Monitoring Equipment and how those circumstances are beyond the control of the entity
- **1.4.** Any other information the entity deems relevant to the Compliance Enforcement Authority's (CEA) consideration of its request

# PRC-028-1 R8 Event-driven PDS for CAP

**R8.** Each Generator Owner shall, upon the discovery of a failure of the recording capability for the SER, FR, or DDR data: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

- Restore the recording capability within 90 calendar days, or
- Submit a Corrective Action Plan (CAP) to the Regional Entity within 90 calendar days and then implement it according to CAP timeline.

## ❑PRC-028-1 R8 CAP Process

- Will submit within 90 calendar days through Align Period Data Submittal section
- Submit supporting documentation via ERO Secure Evidence Locker (SEL)
  - Include the CAP itself & evidence of implementation per CAP timeline
- Evidence can include:
  - Dated reports of discovery of a failure
  - Documentation with the date the data recording was restored
  - SCADA records
  - Dated CAP
- Able to submit within Align currently

# PRC-029-2 R4 Hardware Limitation PDS

**PDS is currently available in Align**

**Due 12 months after effective date of Standard (October 1, 2027)**

- Deadline applies to BES and Non-BES IBRs In-Service & Subject to Compliance with NERC Standards on or before 10/01/2026

**Align PDS and accompanying spreadsheet & evidence to SEL**

**Evidence should include all information in R4.1.1 through 4.1.3**

- IBR info, which specific aspects of Ride-through requirements IBR is unable to meet
- ID the hardware piece(s) with limitation, relevant technical documentation

**Cannot be a software limitation**

# PRC-029-2 R4 Hardware Limitation (Cont.)

## R4.1 Detailed information for documentation

## R4.2 Provide copy of R4.1 information to associated entities

- R4.2—Copy to Planning Coordinator (PC), Transmission Planner (TP), Transmission Operator (TOP), Reliability Coordinator (RC), and Texas RE as CEA
  - R4.2.1—Respond to an entity's request for additional info within 90 days
- R4.2.2—Copy of CEA's acceptance of hardware limitation to associated entities
  - Within 90 days of acceptance

## R4.3 Replacement of hardware limitation

- Communicate and provide documentation of change to PC/RC, TP, & TOP within 90 days (prior exemption becomes not applicable)

## Acceptance of PDS-Texas RE verifies GO submits all info in sub-requirements of R4.1 (footnote 15 of PRC-029-2)

# PRC-030-1 IBR Event Mitigation



## ❑Purpose

- Mitigate Unexpected IBR Change in Power Output

## ❑Applicability

- BES IBRs
- Non-BES IBRs with:
  - Aggregate nameplate ≥ 20 mVA **and**
  - Connected to common point of connection ≥ 60 kV

## ❑Implementation Plan Deadlines

- Effective Date: 10/01/2026
- BES IBRs: 10/01/2026, 100% compliant R1-R4
- Non-BES IBRs: 01/01/2027, 100% compliant R1-R4

# PRC-030-1 Requirement R1

- **Implement documented process to identify changes in Real Power output (within a 4 second period):**
  - Complete facility loss of output; **OR**
  - Changes ≥20 MVA and ≥10% of plant's gross nameplate
- **Changes in Real Power excluded:**
  - Due to intermittent primary energy source availability (e.g., change in wind speed and solar irradiance)
  - Resource dispatch or ramping, planned outages or planned resource testing
  - Transmission or collection system loss configured to disconnect the IBR generator; or
  - Due to Misoperation being analyzed and corrected under PRC-004 Standard



# PRC-030-1 Requirement R2



## Requirement R2

- Within 90 calendar days of an R1 Real Power change event or following a request from the Reliability Coordinator (RC), Balancing Authority (BA), or Transmission Operator (TOP) that identified a change
- R2.1: Analyze the IBR facility performance during the event
  - Root cause(s) (R2.1.1)
  - Document Ride-through performance (including Reactive Power) (R2.1.2)
  - Assess issues identified and if corrective action needed (R2.1.3)
  - Applicability to other IBR facilities (R2.1.4)
- R2.2: Provide analysis results to RC, BA, or TOP, if requested

# PRC-030-1 Requirements R3 & R4

## Requirement R3

- If corrective actions were identified in R2.1.3, within 60 days of completing analysis:
  - Develop Corrective Action Plan (CAP), including all other applicable IBR facilities of the GO, **or**
  - Technical justification for why corrective actions won't be implemented
- Provide to RC, BA, and TOP

## Requirement R4

- For each CAP developed per R3:
  - Implement CAP (R4.1); update as needed (R4.2)
  - Notify RC(s) of any CAP changes and when completed (R4.3)

# Resources

- **Standards & RSAWs**
  - PRC-028-1 Standard
  - PRC-029-2 Standard
  - PRC-030-1 Standard
  - PRC-028-1 RSAW
  - PRC-029-1 RSAW
  - PRC-030-1 RSAW
- **Implementation Plans & PDS**
  - PRC-028-1 Implementation Plan
  - PRC-029-2 Implementation Plan
  - PRC-030-1 Implementation Plan
  - 2026 Periodic Data Submittal Schedule
  - Align Templates for PDS
- **Project Pages**
  - 2020-02 Modifications to PRC-024 (Generator Ride-through)
  - 2021-04 Modifications to PRC-002 - Phase II
  - 2023-02 Analysis and Mitigation of BES Inverter-Based Resource Performance Issues
- **Technical Rationale**
  - PRC-028-1 Technical Rationale
  - PRC-029-1 Technical Rationale
  - PRC-030-1 Technical Rationale
- **Compliance Guidance**
  - ERO Enterprise Endorsed IG: PRC-029-1 R4
  - Proposed IG: PRC-029-1 R1-R3 (Design Evaluation)
  - CMEP Practice Guide on Annual & Calendar Months
  - CMEP Practice Guide: PRC-029-1 Enforcement Discretion
    - Enforcement Discretion Template
  - NERC IBR Small Group Advisory Session (August 2026)

# Questions?

TEXAS RE
Ensuring electric reliability for Texans

# Texas RE Fall Standards, Security, & Reliability Workshop

November 4, 2026

## AGENDA

- Resilience Through Protected Communication (CIP-012)
- Walking the Line of Defense (CIP-003, CIP-006, CIP-014)
- Inside Threats, Inside Visibility (CIP-015)
- Ask the Hard Questions: Computational Loads, Ride-through, and Grid Compatibility
- Mitigating Misoperation Risk and Finishing the Fix
- Ride-through Ready (PRC-028, PRC-029, PRC-030)
- **Closing the Facility Ratings Gap (FAC-008)**

## Break

Will Return at: 2:30

To submit questions during the workshop, please visit **slido.com** and enter today's participant code: **TXRE**



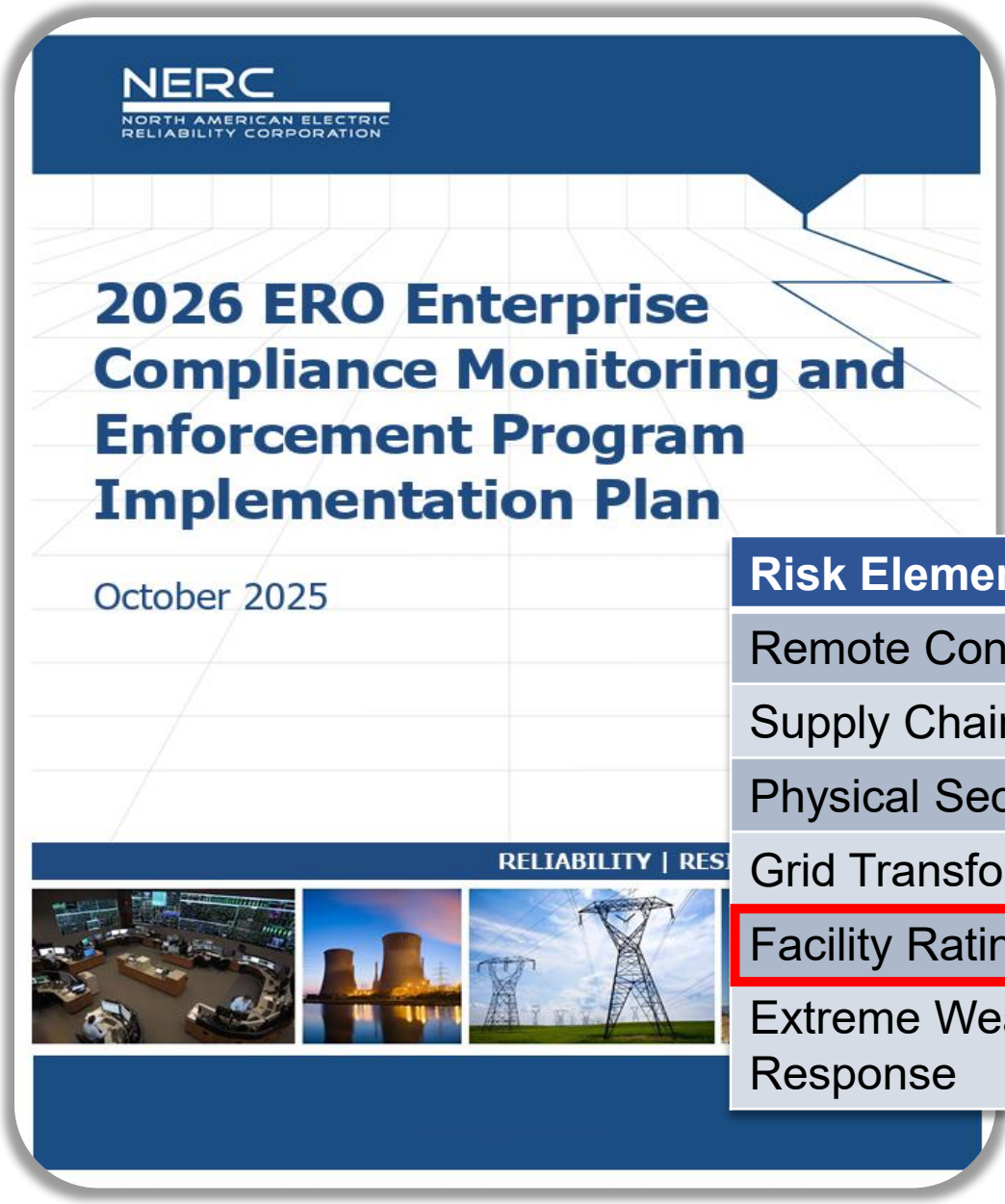

# Closing the Facility Ratings Gap (FAC-008-5)

**Stephen Bradford**
**O&P Compliance Analyst**

**November 4, 2026**

# FAC-008-Facility Ratings – Why?

- The 2026 CMEP Implementation Plan identified Facility Ratings as a Risk Element
- Continues to remain on the list of NERC's most violated standards
- Static nature of the standard leads to complacency
- Lack of internal controls
- Accountability



# The “Gap”

## Gap: a break in space in an object or between two objects

## Where the gaps lie for FAC-008:

- Facility Ratings changes
- Who has the authority to make changes?
- Who provides quality control?
- What if a neighboring entity has changes?
- Who notifies the other departments of a change?
- If the use of CMMS is incorporated, who updates?
- Are periodic walkdowns performed and how are they documented?
- Who is trained and when?



# Standard at a Glance

## Three requirements anchor the control environment

| | | |
|---|---|---|
| R1 | GENERATOR OWNER<br>**Rating documentation** | Assumptions + technical or operational basis + the most limiting applicable Equipment Rating. |
| R2 | GENERATOR OWNER<br>**Documented methodology** | A repeatable method for applicable solely and jointly owned Facilities within the GO scope. |
| R3 | TRANSMISSION OWNER<br>**Documented methodology** | A repeatable method for applicable solely and jointly owned Facilities within the TO scope. |

# The Chain

## A reliable rating depends on the entire chain




**COMPLETENESS**
All in-scope assets and components

**VALIDITY**
Inputs and assumptions are supportable

**ACCURACY**
Method executes as approved

**AUTHORIZATION**
Qualified review before release

**TIMELINESS**
Changes reach downstream users

**CONTROL PRINCIPLE**

**The calculation can be correct while the control still fails—through stale inputs, an unclear boundary, an unapproved change, or a broken handoff.**

# The Trace

| | |
|---|---|
| **1 OWNERSHIP + BOUNDARY** | Identify the Facility, equipment, and terminal boundary covered by the rating. |
| **2 ASSUMPTIONS** | State the conditions that make the rating valid and reproducible. |
| **3 TECHNICAL BASIS** | Design/construction information or operational information, supported by analysis where needed. |
| **4 LIMITING ELEMENT** | Show why the Facility Rating does not exceed the most limiting applicable Equipment Rating. |

## R1

**The evidence test**

**Can a qualified reviewer recreate the rating decision—without relying on memory or the original preparer?**

**If not, the control is person-dependent.**

# Roles and Responsibilities

| ROLE | DEFINE + CALCULATE | REVIEW | PUBLISH | MONITOR | JOINT-OWNER HANDOFF |
|---|---|---|---|---|---|
| Engineering | R | R | C | R | PROVIDE BASIS |
| Asset data | C | C | R | R | CONTROL MASTER |
| Planning / operations | C | C | I | R | CONFIRM USE |
| Compliance | C | R | C | R | TEST EVIDENCE |
| **Control owner** | A | A | A | A | ACCEPT HANDOFF |

R = Responsible A = Accountable C = Consulted I = Informed

ONE OWNER FOR EACH RELEASE

# NERC FAC-008-5 Scenario: Equipment Replacement and Facility Rating Update

Keeping Facility Ratings Accurate Through Change Management

*Right Data. Right Ratings. A More Reliable Grid.*

## 1 Existing Equipment and Facility Rating

A 230/115 kV power transformer (T1) is in service at the Maple Substation. It is included on the company's Facility Ratings spreadsheet with a Normal rating of 300 MVA.




**Facility Ratings Spreadsheet (Excerpt)**

| Facility ID | Facility Name | Equipment | Voltage (kV) | Normal Rating (MVA) | Emergency Rating (MVA) |
|---|---|---|---|---|---|
| MAPLE-T1 | Maple | Power Transformer T1 | 230/115 | 300 | 360 |

## 2 Equipment Requires Replacement

During a routine inspection, significant insulation degradation is found. The transformer must be replaced due to end-of-life condition.




## 3 New Equipment Installed – Different Rating

The existing 300 MVA transformer is replaced with a new 250 MVA transformer (T1). The change affects the facility ratings and must be evaluated and updated in accordance with FAC-008-5.




## 4 Change Management Process

The company follows its internal change management process to evaluate the impact on Facility Ratings.

**Initiate Change Request**
Replacement of T1 (300 MVA → 250 MVA)

↓

**Perform Impact Assessment**
Evaluate effects on Facility Ratings, system studies, and interconnections

↓

**Engineering Review**
Confirm equipment specifications and applicable rating methodology

↓

**Management Approval**
Approve rating updates and implementation

↓

**Implement and Update**
Update Facility Ratings spreadsheet and supporting documentation

## 5 Update Facility Ratings

After engineering analysis and approval, the Facility Ratings spreadsheet is updated to reflect the new 250 MVA transformer.

**Facility Ratings Spreadsheet (Excerpt)**

| Facility ID | Facility Name | Equipment | Voltage (kV) | Normal Rating (MVA) | Emergency Rating (MVA) |
|---|---|---|---|---|---|
| MAPLE-T1 | Maple | Power Transformer T1 | 230/115 | 250 | 300 |




## 6 Result – Compliance with FAC-008-5

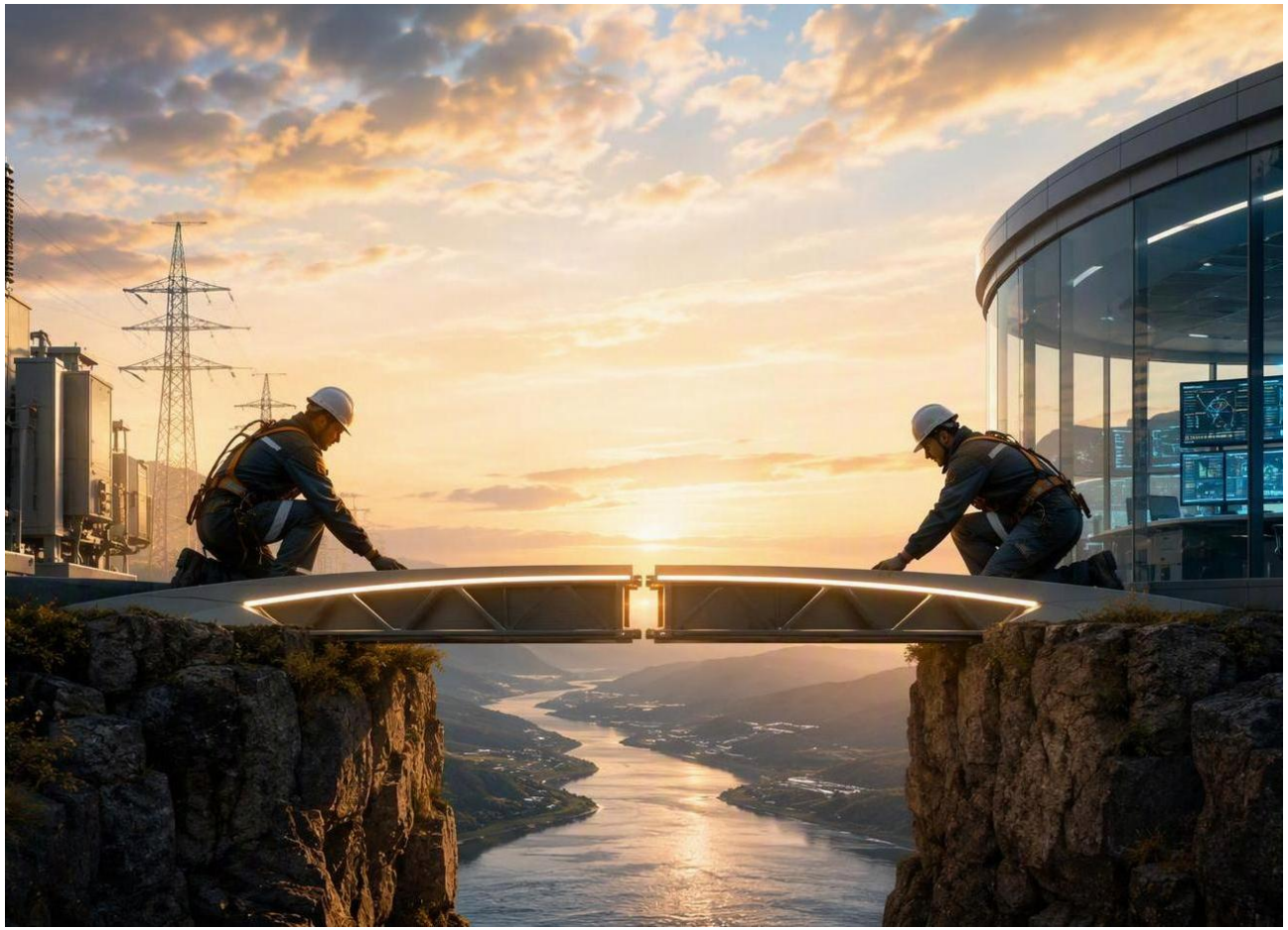
The company has:

- ✓ Followed a documented change management process
- ✓ Evaluated the impact on Facility Ratings
- ✓ Updated the Facility Ratings spreadsheet
- ✓ Retained supporting evidence
- ✓ Maintained accurate and reliable Facility Ratings

This ensures ongoing compliance with FAC-008-5 and supports the reliability of the Bulk Electric System.



# Closing the Gap



**Bring field conditions and operational information together.**

**Closing the gap is not one person's task. It requires engineering, asset management, operations, planning and compliance to complete the connection.**

# Questions?

TEXAS RE
Ensuring electric reliability for Texans

# Wrap-Up

Thank you for coming!

Remote participants will receive a short survey via e-mail. Please complete the workshop survey to help Texas RE develop future outreach.

Remote participants will receive the survey via e-mail.