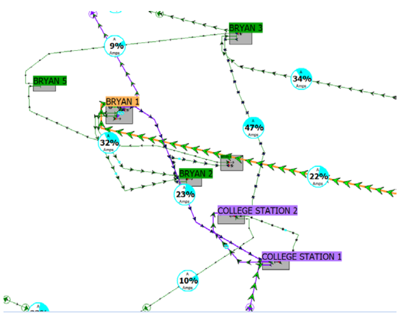
TEEX Cyber Readiness Summit Tabletop Handout

RESLab Power Company

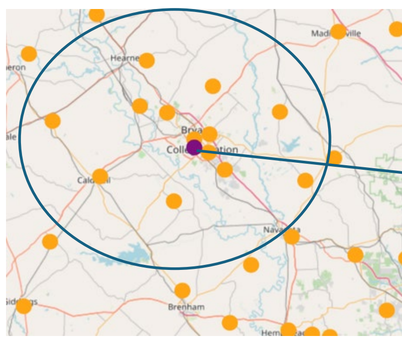
Building a Smarter, Stronger Grid for Bryan–College Station

RESLab Power Company is a synthetic utility for the tabletop. It is designed for research, education, and testing of cyber-physical resilience strategies for power systems.

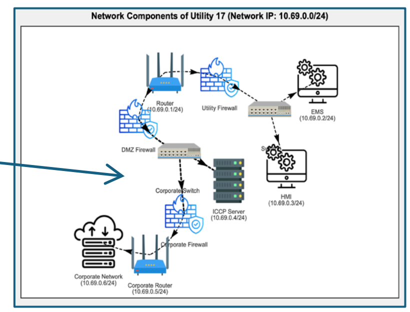
- **Mission:** To enhance grid resilience through advanced monitoring, optimal response, and integration of cybersecurity practices.
- **Service Area:** The simulated RESLab Power Company serves the Bryan, College Station and surrounding counties with a mix of residential, commercial, and industrial loads.



One-line Diagram of Synthetic 2000-Bus System around Bryan Area



Cyber System of Synthetic 2000-Bus System with DesTinE Tool



Cyber Assets in Utility Control Center

Acronyms

Acronym	Definition
CORE	Common Open Research Emulator
CPS	Cyber-Physical Systems
CYPRES	Cyber-Physical Resilient Energy Systems
DMZ	Demilitarized Zone
DNP3	Distributed Network Protocol 3
DOE	U.S. Department of Energy
EMS	Energy Management System
ERCOT	Electric Reliability Council of Texas
FERC	Federal Energy Regulatory Commission

HMI	Human-Machine Interface
ICCP	Inter-Control Center Communications Protocol
ISO	Independent System Operators
IT	Information Technology
N-1 / N-2 Secure	Power system resilience to the failure of one or two critical elements (e.g., lines, transformers)
NERC	North American Electric Reliability Corporation
OT	Operational Technology
RESLab	Resilient Energy Systems Lab
SCORE	Scalable Cyber-Physical Optimal Response Engine
SCADA	Supervisory Control and Data Acquisition
TCP	Transmission Control Protocol

Definitions

- **Transmission system**: System for moving bulk electric power from generating stations to substations over high-voltage lines, essential for transporting electricity efficiently over long distances. **Components** include buses, substations, transformers, etc.
- **SCADA Systems** are responsible for **remote control**, **data acquisition**, and **automation** of substations, plants, and grid assets
- **Human-Machine Interface (HMI)**: Graphical interfaces used to monitor and control systems
- **Firewall (FW)**: Network security device that monitors and filters incoming and outgoing traffic based on defined security rules, protecting critical assets from cyber threats.
- **Router:** A device that directs data packets between different networks.
- **Ethernet switch:** A network device that connects multiple devices within a **Local Area Network (LAN)** at substations, control centers, or plants.
- **Physical components:** Transmission lines, substations, transformers, etc. that handle the generation, transmission, and distribution of electricity
- **Cyber components** HMI, router, firewall, etc. and other devices that enable communication, control, and protection across the grid's IT and OT environments
- **Cyber-physical components** are key components that bridge the physical and cyber layers
- **Relays** and **Intelligent Electronic Devices (IED)**: Cyber-physical devices include microprocessor-based assets to monitor and control physical grid parameters (e.g., current, voltage), execute protection algorithms (e.g., overcurrent protection), and issue control commands (e.g., trip circuit breakers) while communicating with SCADA over secure networks.

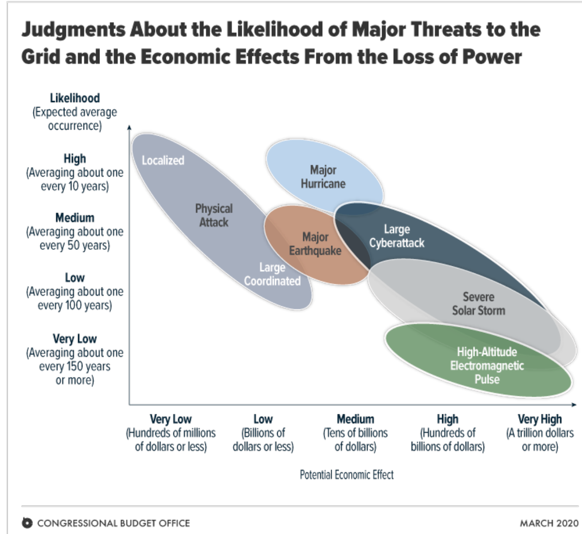
- ## Four Broad Categories of Incidents on Grid Infrastructure

Natural Incidents – Weather, Solar Storm

Physical Attacks – Shootings, break-ins, site damage

Cyber Attacks – Ransomware, Business E-Mail Compromise, Phishing

Cyber-Physical Attacks – Cybersecurity breaches with targeting at grid systems



- ## Natural and Physical Attacks

Often involve the physical destruction of equipment, reducing grid resilience

Lower risk of sustained intrusion

Lower complexity of attacks

Remediation methods are typically well understood and executed.

- ## Cyber and Cyber-Physical Attacks

December 2015
Ukraine Power Grid Attack

December 2016
Industroyer Malware Attack in Ukraine

2021
Colonial Pipeline Ransomware Attack

April 2022
Sandworm's Industroyer2 Attempt

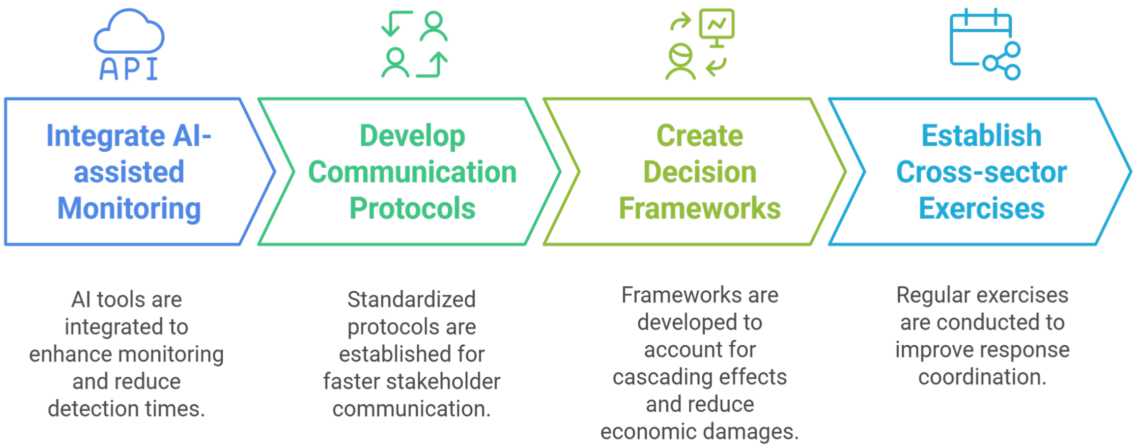
2024
Surge in Cyberattacks Against Utilities

May involve systemic risk outside of the typical utility sphere of control.

Attackers may be in a system without detection for extended periods of time.

Attacks can be novel and require extensive work into root cause investigation and prevention, eradication and recovery efforts.

Decision Making and Response



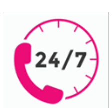
10 Steps to Develop a Cyber Incident Response Plan

1. Establish a Cyber Incident Response Team

Cyber Incident First Response Team
- Cyber Incident Response Manager
- IT Technical Response Team
- IT/OT Power Operations Team

Roles:
- Conducts initial investigation of alerts
- Declares a cyber incident
- Mobilizes the full response team resources
- Oversees plan development and updates after the incident

2. Develop a 24/7 Contact List for Response Personnel and Partners



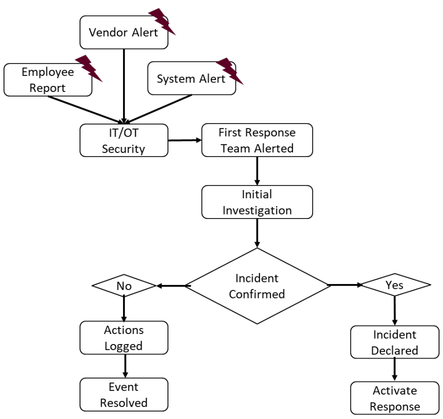
Contact lists can include:
- Internal stakeholders
- Support contacts for all software and equipment vendors and contracted service providers
- Key contacts or liaisons

3. Compile Key Documentation of Business-Critical Networks and Systems
4. Identify Response Partners and Establish Mutual Assistance Agreements
5. Develop Technical Response Procedures for Incident Handling
6. Classify the Severity of Cyber Incidents
7. Develop Strategic Communication Procedures
8. Develop Legal Response Procedures
9. Obtain CEO or Senior Executive Buy-In and Sign-off
10. Exercise the Plan, Train Staff, and Update the Plan Regularly

Response Life Cycle

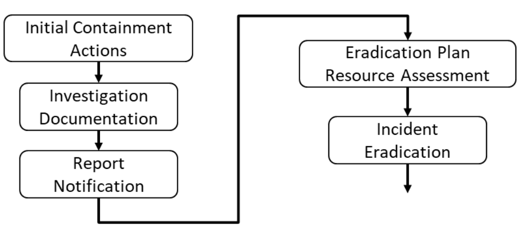
Detection	Containment	Eradication	Recovery
Detect based on cyber and physical alerts and reports	IT and OT teams collaborate to quickly contain the intrusion	Power system experts probe into the threats Mitigate while ensuring system function	Take short- and long-term actions Develop & deploy resilience hardening strategies

Detection



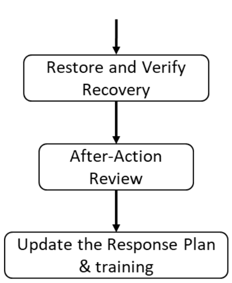
IT	OT
▪ **Monitor** for intrusions, unauthorized access, or malware on substation IT networks. ▪ **Detect** anomalous logins or command injections, e.g., from alerting systems. ▪ **Identify** phishing emails or ransomware attempts targeting substation IT systems.	▪ Detect **unexpected SCADA commands** or anomalous control signals. ▪ **Identify** abnormal changes, e.g., voltage changes, sudden breaker operations. ▪ Use network monitoring tools to check for **unauthorized protocol usage** (e.g., unexpected Modbus/TCP traffic).

Containment & Eradication



IT	OT
▪ **Block** malicious IP addresses and disable compromised accounts ▪ **Isolate** affected substation remote access points ▪ **Contain** the spread of malware by disabling unnecessary network connections	▪ **Segregate** affected SCADA systems to diagnose the intrusion ▪ Implement **manual control** mode if necessary ▪ **Disable remote access,** to prevent adversarial command execution

Response & Recovery



IT	OT
▪ **Remove** malware, reset credentials, and patch vulnerabilities in IT networks ▪ **Verify** no suspicious persistence mechanisms (e.g., accounts) ▪ **Reinforce** network segmentation and firewalls between IT and OT environments	▪ Revalidate **control system integrity** by checking all SCADA setpoints and relay settings ▪ **Patch vulnerabilities,** e.g., in RTUs and HMI software ▪ Ensure **redundancy measures** (e.g., backup control centers)

Resources and References:

[1] U.S. Department of Energy, “Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector,” Office of Electricity, Energy.gov, 2023. [Online]. Available: https://energy.gov/epsa/downloads/cyber-threat-and-vulnerability-analysis-us-electric-sector.

[2] P. W. Parfomak, “Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations,” Congressional Research Service, Report R43604, 2014. [Online]. Available: https://sgp.fas.org/crs/homesec/R43604.pdf.

[3] Cybersecurity and Infrastructure Security Agency (CISA), “Sector Spotlight: Electricity Substation Physical Security,” CISA.gov, 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-02/Sector%20Spotlight%20Electricity%20Substation%20Physical%20Security_508.pdf.

[4] "Texas power outages: Nearly half the state experiencing water disruptions as power grid operator says it's making progress," *The Texas Tribune*, Feb. 18, 2021. [Online]. Available: https://www.texastribune.org/2021/02/18/texas-winter-storm-power-outage-ercot/.

[5] North American Electric Reliability Corporation (NERC), CIP-008-6: Cyber Security — Incident Reporting and Response Planning, NERC, Feb. 6, 2019. [Online]. Available: https://www.nerc.com/pa/stand/reliability%20standards/cip-008-6.pdf.

[6] North American Electric Reliability Corporation (NERC), “GridEx VII Report,” NERC, 2024. [Online]. Available: https://www.nerc.com/pa/CI/ESISAC/GridEx/GridEx%20VII%20Report.pdf.

[7] American Public Power Association, “Public Power Cyber Incident Response Playbook,”2025. [Online]. Available: https://www.publicpower.org/resource/public-power-cyber-incident-response-playbook

|8] Takepoint Research: 80% of industrial cybersecurity professionals favor AI benefits over evolving risks,” *Industrial Cyber,* Oct. 24, 2024. [Online]. Available: https://industrialcyber.co/ai/takepoint-research-80-of-cybersecurity-professionals-favor-ai-benefits-over-evolving-risks/

[9] “AI and Cybersecurity: A New Era,” Morgan Stanley, 11 Sept. 2024. [Online]. Available: https://www.morganstanley.com/articles/ai-cybersecurity-new-era

[10] National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, Jan. 17, 2025: https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

[11] The National Cybersecurity Strategy, March 2023: https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/

[12] DOE Multiyear Plan for Energy Sector Cybersecurity*,* 2018: https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf

[13] NERC CIP Standards: https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf

[14] Electricity Information Sharing and Analysis Center (E-ISAC): https://www.eisac.com/s/

[15] Electric Reliability Organization (ERO), “Cyber Informed Transmission Planning,” 2023: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/ERO_Enterprise_Whitepaper_Cyber_Planning_2023.pdf

[19] Idaho National Laboratory, "Cyber-informed Engineering," 2025: https://inl.gov/national-security/cie/

[20] A. Sahu, K. Davis, H. Huang, A. Umunnakwe, S. Zonouz, A. Goulart, "Design of Next-Generation Cyber-Physical Energy Management Systems: Monitoring to Mitigation," *IEEE Open Access Journal of Power and Energy*, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10024808

[21] A. Sahu, Z. Mao, P. Wlazlo, H Huang, K. Davis, A. Goulart, "Multi-Source Data Fusion for Cyberattack Detection in Power Systems," *IEEE Access*, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9521204

[22] K. Davis, C. Davis, S. Zonouz, R. Bobba, R. Berthier, L. Garcia, P. Sauer, "A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures," *IEEE Trans. Smart Grid*, 2015. [Online]. Available: https://ieeexplore.ieee.org/document/7103368

[23] H. Huang, H. Vincent Poor, K. Davis, T. Overbye, A. Layton, A. Goulartm, S. Zonouz, "Toward Resilient Modern Power Systems: From Single-Domain to Cross-Domain Resilience Enhancement," in Proceedings of the IEEE, vol. 112, no. 4, pp. 365-398, April 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10556785

[24] A. Umunnakwe, S. Sun, K Davis, "Toward Proactive Cyber-Physical-Human Risk Assessment in Power Systems," IEEE Texas Power and Energy Conference (TPEC), Feb 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10472174

[25] S. Sun, S. Hossain-McKenzie, L. Al Homoud, K. Haque, A. Goulart, K. Davis, "An AI-based Approach for Scalable Cyber-physical Optimal Response in Power Systems," IEEE Texas Power and Energy Conference (TPEC), Feb. 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10472265

[26] T.J. Overbye, K.R. Davis, A.B. Birchfield, "The Electric Grid and Severe Resiliency Events," *National Academy of Engineering Bridge Journal*, issue on Engineering the Energy Transition, vol. 53, no. 2, Summer 2023, pp. 73-79. [Online]. Available: https://www.nae.edu/294939/The-Electric-Grid-and-Severe-Resiliency-Events

[27] L. Al Homoud, V. Bobato, A. Goulart, K. Davis, M. Rice, "Analyzing a Multi-Stage Cyber Threat and Its Impact on the Power System," *IET Cyber-Physical Systems: Theory and Applications*, January 2025. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/cps2.12107

[28] S. Sun, H. Huang, E. Payne, S. Hossain-McKenzie, N. Jacobs, H. V. Poor, A. Layton, K. Davis, "A Graph Embedding-Based Approach for Automatic Cyber-Physical Power system Risk Assessment to Prevent and Mitigate Threats at Scale," *IET Cyber-Physical Systems: Theory and Applications*, June 2024. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/cps2.12097

[29] NIST SP-800 Publications are Relevant to Conducting Cyber Security Risk Assessment: https://csrc.nist.gov/publications/sp800

Phishing & Credential Theft (MITRE T1566)
Ransomware Attacks (MITRE T1486)
Supply Chain Attacks (MITRE T1195)
Man-in-the-Middle (MitM) in SCADA Communication (MITRE T0830)
Firmware Manipulation in Substation Devices (MITRE T0851)
Denial-of-Service (DoS) on ICS Components (MITRE T0814)

To get involved, and for more information and resources, please visit our website https://score.engr.tamu.edu/ or contact us. Dr. Katherine Davis: katedavis@tamu.edu

Discussion Notes: