Success Stories 2025-2020
Cyber Security for Energy Delivery & Customer Solutions

EPRI member application success stories showcase research insights addressing specific issues, offering potential solutions, and delivering valuable knowledge transfer, thereby adding significant value to member organizations. For a more detailed listing click here.

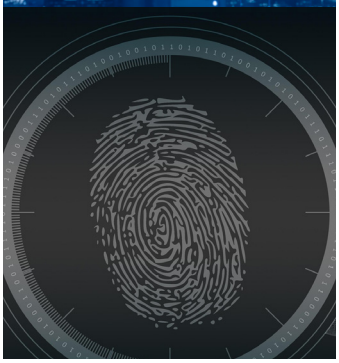
Cybersecurity Strategy Assessment and Program Alignment (CSAPA) Framework CSAPA-Report-05182025 - Tennessee Valley Autority (TVA) (2025)
Researchers evaluated cybersecurity maturity across Tennessee Valley LPCs and delivered a unified, standards-aligned framework—combining metrics, roadmaps, and templates—that reduced compliance burden, strengthened grid-wide resilience, and gave both small and large utilities access to standardized, cost-effective security practices. The value delivered was leveling the playing field, easier compliance and grid-wide resilience.

EPRI 2025 Technology Transfer Award Winner

Creating Effective Analytics to Monitor Operation Technology (OT) - Alabama Power, a Southern Company (APC), Mississippi Power, a Southern Company (MPC), Salt River Project (SRP), Southern Company (SCS) (2025)
This initiative strengthened cybersecurity visibility in energy delivery OT environments by translating behavioral detection concepts into validated, field-tested capabilities through multi-utility and EPRI collaboration. Proof-of-concept testing and the LE2024 live-fire exercise improved early threat detection, incident response, and monitoring logic while introducing new operational data sources and reinforcing host- and application-level logging. The effort also supported evolving regulatory requirements, informed risk-based monitoring architectures, and delivered industry-wide benefits in resilience, flexibility, and cost efficiency.

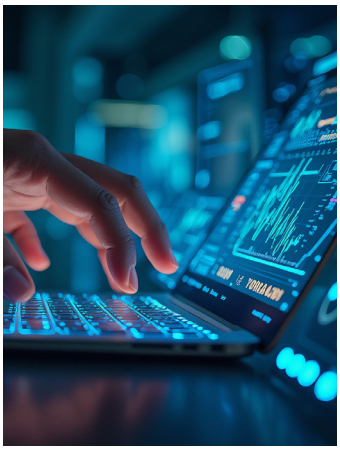
Electric Vehicle Supply Equipment (EVSE) Cyber Security Gap Analysis – Southern California Edison (2025)
P183D researchers worked with Southern California Edison (SCE) to conduct a comprehensive cybersecurity gap and consequence analysis of EVSE systems deployed under California's Investor-Owned Utilities (IOU) Transportation Electrification (TE) programs. This work, commissioned by Southern California Edison (SCE) and the California Public Utilities Commission (CPUC), considers cybersecurity threat scenarios resulting from known exploits used against EV charging systems, gaps in cybersecurity vetting processes, and limitations in industry standards and protocols. Gaps were assessed to develop a key set of recommendations that CA IOUs and industry can consider adopting to include more specified cyber security requirements and approaches for securing EVSE systems and future V2G ecosystems.

Tabletop Implementation – New York Power Authority (NYPA) Cybersecurity Exercise (2025)
In March 2025, NYPA took part in an OT-focused cybersecurity tabletop exercise to strengthen resilience by applying EPRI research on incident response, ICS forensics, and insider threat detection. Using EPRI frameworks, the exercise helped NYPA clarify escalation thresholds, improve coordination between OT and cybersecurity teams, and test manual operations and backup communication strategies under advanced threat scenarios. As a result, NYPA enhanced its incident response readiness, identified gaps in forensic data collection and detection practices, and refined containment and evidence-retention protocols. The exercise also validated continuity strategies for severe disruptions and generated feedback that improved EPRI guidance, translating research into practical, sector-wide cybersecurity improvements for electric utilities.



Cybersecurity Strategy Assessment and Program Alignment (CSAPA) Framework CSAPA-Report-05182025 (2025)
Researchers assessed cybersecurity maturity across Tennessee Valley LPCs using surveys, audits, and policy reviews, combining quantitative metrics (e.g., patch latency, intrusion detection coverage) with qualitative workforce and governance insights. These findings informed tailored roadmaps, scalable reference architectures, and policy templates aligned with NIST CSF, DOE C2M2, and IEC 62443, enabling utilities to adopt standardized, resilient security practices. The value delivered was **Leveling the Playing Field:** Smaller LPCs gained access to expert-vetted tools and templates without costly consultants, while larger LPCs advanced toward unified, standardized solutions. **Easier Compliance:** A single streamlined framework simplified regulatory readiness, reducing audit prep time and costs, and even lowering insurance premiums for some LPCs. **Grid-Wide Resilience:** Common cybersecurity practices across all LPCs reduced systemic risk, protecting over 10 million residents and strengthening public trust in grid security.

Creating Effective Analytics to Monitor Operation Technology (OT) - Alabama Power, a Southern Company (APC), Mississippi Power, a Southern Company (MPC), Salt River Project (SRP), Southern Company (SCS) (2025)
This initiative addresses the critical need for enhanced cybersecurity visibility in energy delivery environments by converting behavioral detection concepts into practical, field-tested capabilities. Through collaboration among Research Lab, SCS, APC, MPC, and EPRI, the project validated analytics effectiveness before production deployment and demonstrated measurable improvements during the LE2024 live-fire exercise.The value that was received was Earlier Threat Detection and Improved Response: Proof-of-concept testing and live exercises enhanced detection fidelity and incident triage workflows, reducing response times for advanced threats. Operational Insights and New Data Sources: Introduced additional log sources (e.g., time synchronization issues) and leveraged operational data for actionable improvements in monitoring logic. Regulatory Alignment and Strategic Justification: Supported compliance with evolving standards (e.g., CIP-015 INSM) and reinforced the need for host- and application-level logging beyond network data. Risk-Informed Monitoring Architecture: Established internal guidance shaping procurement, deployment, and scaling decisions—bridging compliance and real-world cybersecurity effectiveness. Industry-Wide Impact: Shared lessons learned promote flexibility, cost savings, and improved resilience across Energy Delivery OT environments.



Tabletop Implementation – New York Power Authority (NYPA) Cybersecurity Exercise (2025)
In March 2025, NYPA participated in a cybersecurity tabletop exercise focused on OT resilience, applying EPRI research in incident response, ICS forensics, and insider threat detection. Using EPRI-developed frameworks, NYPA assessed escalation thresholds, coordinated across OT and cyber teams, and validated manual operations and backup communication strategies. The value delivered was Improved Incident Response Readiness: Clearer escalation thresholds and enhanced OT–cyber team coordination strengthened NYPA's ability to respond to advanced threats like firmware manipulation and insider activity. Operational Forensics and Detection Enhancements: Applied forensic data collection, log correlation, and insider threat principles to uncover gaps and refine containment protocols and artifact retention practices. Validated Continuity Strategies: Confirmed effectiveness of manual operations and backup communications for severe disruptions, ensuring operational resilience. Industry-Wide Impact: NYPA's feedback refined EPRI guidance and advanced best practices, turning research into actionable improvements for utilities sector-wide.

Advanced Grid Analytics and Visibility Engine; Southern Company (2024)
Southern Company developed an advanced cybersecurity solution to counter growing threats to operational technology (OT). Collaborating with EPRI, the Knoxville Cyber Security Research Lab, and vendors like Gravwell, they implemented an Internal Network Security Monitoring (INSM) system to meet regulatory requirements and enhance cybersecurity defenses. This system focused on monitoring internal network traffic, optimizing data collection, and reducing bandwidth strain, ultimately improving detection and response to cyber threats. Their innovative, scalable solution not only strengthened their own infrastructure but contributed to industry-wide advancements in cybersecurity.

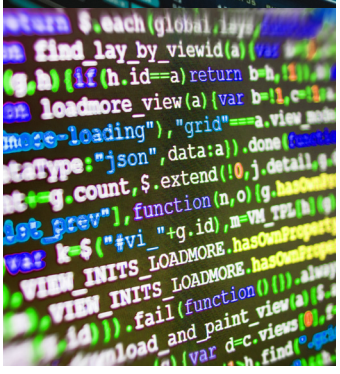
Cybersecurity Decision Framework for Utility Scale Energy Storage Systems; Southern Co., CPS Energy, CenterPoint Energy, SCE (2024)
As energy storage infrastructure expands, ensuring cybersecurity is crucial for reliability and safety. Utilities like CPS Energy, CenterPoint Energy, SCE, and Southern Company are leading efforts to deploy energy storage systems, with EPRI developing a cybersecurity decision framework to guide them. This framework helps utilities prioritize security controls based on risk profiles, applying NIST guidelines to procurement, interconnection agreements, and ongoing operations such as monitoring and incident response. The framework has provided utilities with valuable insights into securing energy storage systems, improving their cybersecurity posture for future deployments, despite the complexities of large-scale renewable integration.

Operational Technology Equipment Technology Transfer Workshop; ConEd (2024)
Con Edison identified a gap in OT-specific cybersecurity training, which was largely generic and IT-centric, and collaborated with EPRI to address this need in 2020. Together, they developed a tailored OT Familiarization Workshop utilizing EPRI's Cyber Security Research Lab, providing hands-on, interactive training specific to Con Edison's technologies and operations. The workshop was expanded in 2023 for a broader audience, fostering cross-team engagement and improving incident response capabilities across various departments. This partnership helped Con Edison enhance OT cybersecurity knowledge, strengthen vendor relationships, and align with industry standards for cybersecurity architecture and response.

Power Delivery Cyber Security Tailored Assessment for Utility Transmission and Distribution Operations; NYPA (2024)
EPRI conducted research to help NYPA enhance its cybersecurity procedures beyond regulatory compliance, focusing on transient cyber assets, patch and vulnerability management, and cybersecurity training. The research provided NYPA with recommendations to strengthen security measures, such as improving transient cyber asset handling, refining patch management procedures, and elevating training standards with a focus on operational technology (OT). Short-term, intermediate, and long-term recommendations were offered to address security gaps and enhance NYPA's ability to respond to cyber threats. The collaboration between EPRI and NYPA aligned with NYPA's VISION2030 goals and strengthened its cybersecurity posture across operations.

Xcel Energy Staff Benefits from Remote Cyber Security Operational Technology Equipment Familiarization Course (2023)
This training course provided Xcel Energy utility cyber security engineers, analysts, and managers with hands-on exercises and supporting discussions for a variety of components commonly used to monitor and protect both the power delivery networks and the network infrastructures that support grid operations.
"I was privileged to be chosen to participate as one of eight Xcel Energy students in a six-day EPRI Operational Technology (OT) Equipment Familiarization Course. Although conducted remotely, we were immersed in a realistic, hands-on experience by connecting to equipment in the EPRI Cyber Security Research Lab (CSRL). The instructor facilitation was superb; they encouraged us to learn and explore in a safe, yet realistic environment, which was available between and after classes as well. My understanding of substation architecture, communication protocols and hardware and software in use at Xcel Energy was dramatically improved. The course also provided a splendid opportunity for me to engage and build relationships with my classmates and the exceptional industry professionals at EPRI; if I have specific technical questions, I know exactly who to call."
- Taylor Cox Sr. Consultant, Business Continuity Enterprise Security and Emergency Management Xcel Energy.
Link to Supplemental Project Offering.

Industrial Control Systems Automated Digital Forensics Harvester - Consumers Energy, North Carolina Electric Membership Corporation, Électricité de France, Salt River Project, Evergy, Southern Company, Exelon, Tennessee Valley Authority, KEPCO, New York Power Authority (2023)
As cybersecurity threats evolve, rapid and accurate forensic data collection from ICS devices in OT environments is essential for incident response. This project developed an automated forensics tool that enables real-time extraction of critical artifacts from devices, overcoming challenges with ICS devices' custom operating systems. Using an extended, supported communications protocol, the harvester tool collects and stores data in a structured format, enhancing forensics automation. Funded by NYSERDA, the tool is open-source, encouraging manufacturers to adopt it. Future extensions include integration with SOAR tools, continuous monitoring, automated threat detection, and potentially automated threat mitigation.



Southern Company - Dedicated Power Delivery Cybersecurity Program (PD CSP) (2023)
Southern Company's Power Delivery Cybersecurity Program (PD CSP) strengthens the cybersecurity of its operational technology (OT) networks, enhancing resilience against cyber threats to ensure uninterrupted utility services. In collaboration with EPRI, Southern updated the PD CSP to adopt a comprehensive, proactive approach, setting new industry standards in cybersecurity. This program has increased customer trust and satisfaction through consistent communication and transparency, with quarterly updates to stakeholders. Other Southern cybersecurity programs are adopting PD CSP's cost-effective, streamlined model, reinforcing its success and influence across the energy sector. By modernizing legacy systems and supporting digital transformation, PD CSP not only positions Southern as a cybersecurity leader but also contributes significantly to advancing secure energy infrastructure for the future.

Korea Electric Power Company (KEPCO) - Cybersecurity for KEPCO's Distributed Energy Resource (DER) Integration Architectures (2023)
DER integration shifts grid operations towards decentralized, distributed energy sources, raising cybersecurity challenges. KEPCO, working with EPRI, conducted a comprehensive review of EPRI's DER cybersecurity guidelines to establish secure, end-to-end communication across the grid. This collaboration provided a foundational case study on DER cybersecurity architectures, benefiting other utilities facing similar risks. Using EPRI's research, KEPCO developed secure architectures to support grid modernization with DER integration, demonstrating that proactive, by-design cybersecurity approaches strengthen utilities against disruptions and protect electricity flow to the public

Southern Company - Next Generation OT Cyber Security Visibility (2022)
Detecting and responding to security threats in operational environments is a key challenge for utilities. Southern Company (SoCo), in collaboration with the Knoxville Cyber Security Research Lab (CSRL), developed a solution that leverages open-source, high-performance packet-capture capabilities integrated with Gravwell data collectors. This system captures and stores network data at edge nodes, reducing bandwidth load on OT networks and enabling enhanced detection, monitoring, and forensic capabilities.

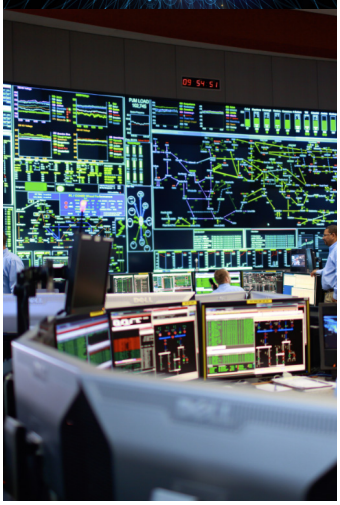
SoCo's solution enables flexible sensor deployment and maximizes visibility, allowing more effective responses to advanced threats. Testing with EPRI at CSRL validated the solution's effectiveness, proving it more cost-effective and bandwidth-efficient than previous, commercially sourced packet-capture systems. Unlike older systems limited to high-value sites, this solution allows full packet capture at field sites, reduces license costs, saves bandwidth, and provides fast data searchability.

Tokyo Electric Power - Artificial Intelligence for Cyber Security (2022)
AI has rapidly advanced and found applications across diverse sectors, including power systems, where it aids in load forecasting, state estimation, pricing, and power flow. AI also holds promise for electric industry cybersecurity, though adoption has been slow due to challenges like limited high-fidelity data, unclear use cases, and a complex vendor landscape. In collaboration with Tokyo Electric Power Company (TEPCO), this project explored ten AI-based cybersecurity use cases, provided an integration roadmap template, and guidelines for vendor selection, enabling TEPCO to assess its readiness for AI in cybersecurity and develop a tailored implementation plan

Louisville Gas and Electric Company and Kentucky Utilities Company (2022)
A significant amount of money and resources have been deployed over the past twenty years to mitigate cyber risks and meet regulatory requirements in substations. The evolution of control system and communications infrastructure in the substation has accelerated in recent years.

EPRI's Cybersecurity for Transmission and Distribution Task Force has hosted multiple working sessions with utilities like LG&E and KU to explore the security and compliance implications associated with a transition from traditional substations to digital substations.

The typical pace of change for T&D infrastructure is slow and incremental, but the shift to digital substations involves the replacement of systems that have not been "cyber assets" and did not have an attack surface for remote manipulation. As utilities continue to expand the focus of cybersecurity and compliance efforts in the power delivery space, new technical and process controls have evolved to address specific risks at transmission and distribution substations. These unique facilities are critical to the safe and reliable operation of the grid and must be protected from emerging cyber risk.

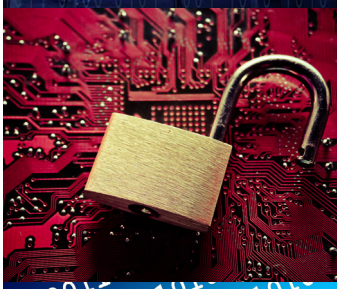


Alliant Energy, FirstEnergy, ConEd, Cooperative Energy, New York Power Authority, Southern Company, Xcel Energy - Insider Threat Management Guidebook (2021)

This guidebook is the de facto standard for Insider Threat Management Programs for electric power utilities. The guidebook provides (1) detailed guidance for starting, maturing, and running a program, (2) the use of behavioral psychology for development of critical personas associated with insider threats, and (3) technical guidance for monitoring and detecting suspicious activity. Each utility is applying the research in their own way and needs. For example, one utility currently has an insider threat management program in place and focuses on using the research to mature and run their program. Another utility has just initiated their program and using the research to build their program based upon the guidance and practices outlined in the guidebook.

Southern Company (SoCo) - Operational Technology (OT) Visibility and Response Pilot (2021)

Cyber-attacks, such as the SolarWinds and Colonial Pipeline attacks, have shown a critical need for more in-depth detection, monitoring, and forensic capabilities, especially in the electricity industry.
Southern Company worked with EPRI's Cyber Security Research Lab to develop OT visibility and response capabilities that are not only industry-leading but have already been proven to effectively respond to recent high profile cyber events such as SolarWinds.



Consolidated Edison Company - Cyber Security Forensics (2021)

The role of cyber security forensics and having the ability to extract forensics information from device has become increasingly important. ConEdison has used EPRI's cyber security research to enhance their Cyber Security Forensics Program, which is a critical component of their cyber incident response process.
NYSERDA forensics harvester and forensics working group are providing Con Edison with the tools and knowledge to effectively respond to cyber incidents and protect our customers. The ConEdison Forensics Team has extended their capabilities by developing an innovative Mobile Forensics Unit that consists of a vehicle that is customized with the necessary equipment to quickly respond to cyber incidents and perform field forensics investigations.

American Electric Power (AEP), Dominion Energy - EPRI Cyber Security Technical Assessment Methodology (TAM) on Substation Digital Equipment (2021)

Understanding cyber security vulnerabilities and mitigations to maintain a strong security posture for critical infrastructure as described in Executive Order (EO) 13920, Securing the United States bulk-power system (BPS) and are important to help understand opportunities to improve the security posture of digital equipment on the BPS, particularly in transmission substations.
By using the first application of the EPRI TAM on substation equipment systems and using Cyber Security Data Sheets (CSDSs) on the individual equipment to document vulnerabilities, AEP & Dominion were as able to leverage the TAM CSDSs to compare existing controls vs recommended controls and as a result validated existing security controls as well as identified additional attack pathways to consider for potential future mitigations.

Korea Electric Power Corporation (KEPCO) - Cyber Security Compliance Automation (2021)

Regulatory standards for electric power systems vary widely around the world, it is a significant concern for almost all utilities. Over time regulators have expanded their role to establish new requirements for cyber security controls.

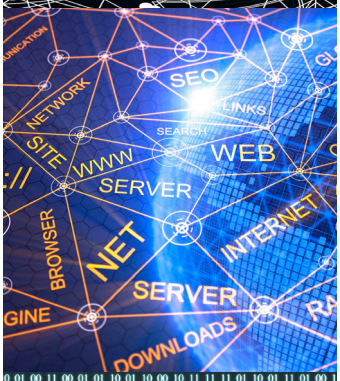
To manage the growing regulatory compliance burden, utilities are looking to EPRI for innovative solutions that lower compliance costs without increasing risk.
KEPCO applied EPRI's cybersecurity research to optimize the compliance process around critical systems such as the Distribution Management System (DMS) and studied, researched, and developed use cases and tools to comply with the national infrastructure protection laws such as North America Electric Reliability Corporation – Critical Infrastructure Protection (NERC-CIP).

American Electric Power (AEP), Salt River Project (SRP) - EPRI Security Architecture for the DER Integration Network and DER Cyber Security Workshop (2021)

Remote monitoring and control of distributed generation require local devices and sensors to communicate operational status and receive commands from remote systems, via public or private communication networks. In the meantime, the attack surface of the nation's grid is increasing as more and more devices become intelligent and connected. Without adequate cybersecurity protection, energy generation and interconnected systems may be exposed to cyber threats. Security Architecture for the DER Integration Network provides a clear and practical guideline for network design and introduces a risk-based security approach for DER integration. This includes a detailed implementation guideline with examples of technologies to meet the requirements and a 60-point checklist to verify the compliance with the requirements. Utilities can use the requirements specified in the document for implementing utility managed integration networks or for the procurement of integration services from third parties.

Pacific Gas & Electric (PG&E) - Cyber Security Architectures and Attack Modeling Methodologies Help Analyze and Mitigate Emerging Risks for Utility Distribution Grids (2021)

Grid modernization, renewable generation, and integration of distributed energy resources pose significant challenges to cyber security. EPRI's focus to cyber security for distribution systems in garnered various options and methodologies for understanding and modeling cyber-attacks to these systems for utilities.
EPRI's security reference architectures and attack models provide utility cyber security professionals with critical security information on distribution systems in a simple format. They can be used in the design and deployment of new systems; security augmentation of old systems; architectural review of current systems; vulnerability analysis and attack modeling; and remediation of discovered security vulnerabilities



New York Power Authority (NYPA) - Cyber Security Tailored Assessment for Utility Transmission and Distribution Operations (2021)
Electric utilities aim to enhance cybersecurity maturity beyond compliance, focusing on reducing cyber-attack risks. EPRI's Power Delivery Cyber Security Assessment project provides targeted evaluations to help utilities like the New York Power Authority (NYPA) identify improvements in key areas, including transient cyber assets, patching, vulnerability management, and training. EPRI's assessments identified strengths and provided actionable, prioritized recommendations that NYPA adapted into its work plans. By leveraging EPRI's research and tailored guidance, NYPA gained valuable insights that aligned with its cybersecurity goals and advanced its operational resilience Link to Supplemental Project Offering (SPN

Cyber Security Forensics (2020)
ConEdison has used EPRI's cyber security research to enhance their Cyber Security Forensics Program, which is a critical component of their cyber incident response process. The ConEdison forensics team has shown industry leadership in cyber forensics and has been active in EPRI's cyber forensics research projects.
"EPRI is leading the industry to recognize that cyber security forensics is a critical component of an effective cyber incident response program and brought all the relevant stakeholders to collaborate on this research. The work on investigation, response, and remediation of attacks is enhancing the industry's cyber forensics capabilities. The forensics field guides, NYSERDA forensics harvester and forensics working group are providing Con Edison with the tools and knowledge to help us effectively respond to cyber incidents and protect our customers." Serena Lee, Project Manager Cyber Security Consolidated Edison Company of New York, Inc.

EPRI Cyber Security Metrics Operationalization Pilot with ConEd, AECC and TVA (2020)
Eight utilities piloted EPRI security metrics between 2017 and 2018 and used them to quantitatively evaluate security programs. Key learnings from these pilots indicated a need for automated data collection, metrics visualization and root cause analysis capabilities for EPRI security metrics. 120 data points have been identified that can be used to calculate 60 metric scores that quantitatively reflect an organization's security posture in a consistent and repeatable way. "The EPRI security metrics have the potential to provide detailed insight into the performance of ConEd's cyber security programs through the EPRI Metrics Hub. This tool will add tremendous value to our operations by allowing us to make data-driven decisions on what areas of our cyber operations can be improved and how. ConEd is looking forward to the completion of the metrics operationalization project and integrating metrics into our operations."Mikhail Falkovich, Director-Information Security, ConEdison. Link to Supplemental Project Offering.

GPS Cyber Security Assessment Help Understand Risks for Transmission Applications (2019)

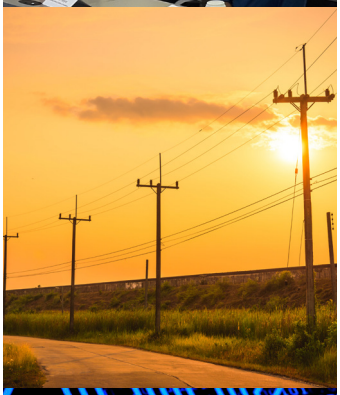
As critical infrastructure increasingly relies on automated technologies, time synchronization becomes essential but introduces cybersecurity vulnerabilities. EPRI's Timing Security Assessment project, in collaboration with utility asset owners, identified time-dependent devices and applications vulnerable to cyberattacks, highlighting potential downstream impacts. EPRI also identified initial mitigation technologies for further evaluation in a second project phase. Consolidated Edison emphasized the importance of EPRI's work in addressing Positional Navigation Timing (PNT) vulnerabilities, noting its broad impact across industries and the power sector's reliance on precise timing for secure operations.

EPRI Security Architecture for the DER Integration Network and 2019 DER Cyber Security Workshop (2019)

The 2019 EPRI cyber security initiative addressed a major gap in the industry: the lack of comprehensive cybersecurity requirements for distributed energy resources (DER). EPRI's report, Security Architecture for the DER Integration Network (3002016781), provides practical, actionable cybersecurity guidelines for the network components that support DER communications.
The document became a valuable resource for utilities by offering straightforward, implementable security requirements to help protect the growing ecosystem of devices, systems, and microgrids connecting to the distribution grid. The report and workshops strengthened the industry's ability to secure DER systems and support grid modernization.

Cyber Security Architectures and Attack Modeling Methodologies Help Analyze and Mitigate Emerging Risks for Utility Distribution Grids (2018)

Grid modernization, renewable generation, and integration of distributed energy resources pose significant challenges to cyber security. EPRI's focus to cyber security for distribution systems in 2018 garnered various options and methodologies for understanding and modeling cyber-attacks to these systems for utilities.
"PG&E is facing many changes to the distribution grid. Grid modernization, renewable generation, and integration of distributed energy resources - all pose significant challenges to cyber security, by increasing attack surfaces and introducing unknown vulnerabilities to the systems supporting the distribution grid operations. EPRI's focus on distribution systems in 2018 garnered the timely attention to cyber security within PG&E and provided various options and methodologies for understanding and modeling cyber-attacks to these systems." According to Xavier Francia, Cybersecurity Risk Advisor, Pacific Gas and Electric Company

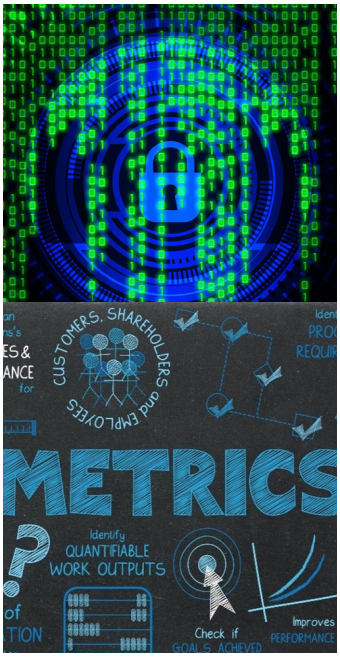


Industrial Control System Forensic Tabletop Exercises Aid in Developing Incident Response Playbooks (2018)

The EPRI Cyber Security Team worked with three electric power utilities in 2018 to evaluate their forensic investigation process by conducting tabletop exercises that test their response to cyber events in their unique operational technology environments. A tabletop exercise is a facilitated, scenario-based discussion that tests an organization's ability to respond to a potential scenario in a practice environment. It enables participants to review and discuss in detail the actions they would take to validate operational processes, procedures, and reporting structures. The key outputs of the exercise are an identification of people, process, or technology gaps and recommendations to resolve them.
"Overall the engagement was very informative and has assisted us as we are on our journey of improving capabilities of incident response. At the time of the exercise we were actively engaged in developing playbooks, communication channels, and escalations paths for our Integrated Security Operations Center. The exercise allowed us to pause and adjust some of the playbooks that were developed to be more in line with the practices that were discussed as part of the exercise." Lance Howard, Senior Manager of Security Assurance and Information Risk Management at Portland Gas and Electric. Link to Supplemental Project Offering

SCANA Corporation - SCANA's Integrated Threat Analysis of Serialized Communications (2017)

As electric grids integrate routed and switched networks with older OT systems, including serialized communications to remote devices, cybersecurity risks increase due to the shift from local to hybrid access methods. Utilities need technologies to detect, analyze, and manage these emerging threats. SCANA Corporation addresses these risks through its Integrated Security Operations Center (ISOC), a centralized, real-time incident response system that integrates cyber and physical security data across substations, field devices, control centers, and external sources. The 24/7 ISOC team enhances SCANA's security posture, supported by collaboration with EPRI and other utilities to refine and advance OT security strategies.



FirstEnergy, NYPA, PG&E, and ConEd - Metrics Pilot: Security Metrics for the Electric Sector (2017)
Quantification of cyber security has been a long-standing challenge in the utility industry. This challenge comes from the fact that there have not been comprehensive security metrics widely adopted by the industry. If such metrics existed, a utility could easily calculate and understand the value of security investments in concrete terms. A utility could definitively state, "the change improved the Protection Score by 10.4% and overall security metric by 6.2%." EPRI's Cyber Security Metrics for the Electric Sector project addresses these needs by developing a practical set of security metrics that represents the status of utility's security posture.
"I did not know what to expect when I first volunteered for the pilot. Once we loaded the data and MetCalc tool showed our numbers, I realized how much of our preconception needed to be adjusted. There is tremendous value in reviewing the metrics and having an in-depth discussion with my staffs." M. Scott Hipkins, Director, Security, and Infrastructure Operation, FirstEnergy.

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com