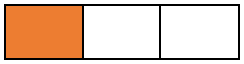
Cyber Security for Power Delivery and Utilization (P183)
Supplemental Projects

Creating Effective Analytics to Monitor Operation Technology (OT)

This project aims to improve situational awareness in operations technology (OT) environments by differentiating between normal and abnormal behaviors, enhancing preemptive threat detection and response. It focuses on strengthening the cybersecurity of electric utilities' OT systems through advanced analytic monitoring to identify potential threats and improve incident response, safeguarding critical infrastructure.

Price	Status	More Info	
$150,000 per utility	 Started	Chuck Moran, 650.855.8521 cmoran@epri.com Scan QR code for two-page summary of project	

Cyber Security Incident Response and Recovery Tabletop Exercise

Utilities must regularly assess and test their ability to respond effectively to cybersecurity events in their operational environments, ensuring their processes meet detection, response, and recovery requirements. With the growing reliance on processor-based power delivery and communications infrastructure, the risk of cyberattacks increases, and NERC CIP-008 and CIP-009 mandate that utilities test their Incident Response and Recovery plans. This project offers customized tabletop exercises to help utilities evaluate and improve their incident response plans.

Price	Status	More Info	
$57,500 Joint project with P94	 Ongoing	Chuck Moran, 650.855.8521 cmoran@epri.com Scan QR code for two-page summary of project	

Cyber Security Operational Technology Equipment Familiarization Course

Utility OT cyber security analysts must be familiar with the systems they are tasked to protect, which can be quite different than enterprise IT environments. This training course provides utility cyber security engineers, analysts, and managers with hands-on exercises and discussions for a variety of components commonly used to monitor and protect both power delivery systems and the networks that support grid operations.

Price	Status	More Info	
$30K	 Ongoing	Greg Drewry, 865.218.5916, gdrewry@epri.com Scan QR code for two-page summary of project	

Cyber Security for Power Delivery and Utilization (P183)
Supplemental Projects

Cyber Security Program Assessment for Utility Transmission and Distribution Operations

Use comprehensive assessment based on NIST Cybersecurity Framework or DOE Cybersecurity Capability Maturity Model to understand current cyber security posture and prioritize recommendations and actions to enhance security program.

- **Gain actionable information and insights to improve OT cyber security posture and attack readiness.**
- **Enact cyber security objectives and project plans based on utility-specific recommendations.**
- **Access to EPRI's metrics portal to benchmark important utility cyber security readiness parameters and inform risk reduction priorities.**

Price	Status	More Info	
Based on scope	∞ Ongoing	Esther Amullen, 650.855.1027, eamullen@epri.com Scan QR code for two-page summary of project	

Cyberjoule™ Platform Implementation for Utility Cyber Security Metrics

This supplemental project helps utilities design and implement cybersecurity metrics to assess the performance of their cybersecurity programs, leveraging EPRI's expertise to avoid common pitfalls. It includes deploying EPRI's Cyberjoule™ platform, offering tools for data-driven metrics, and providing guidance on optimizing implementation strategies and communicating with stakeholders.

Price	Status	More Info	
$40K	Started	Esther Amullen, 650.855.1027, eamullen@epri.com Scan QR code for two page summary of project	

EPRI U - Information, Communication Technology and Cyber Security (ICCS)

Utilities are confronted with ongoing training demands due to the retirement of experienced staff and new challenges in digital transformation and cybersecurity, prompting this project to focus on foundational technical training in ICCS topics. Additionally, it aims to establish a system for tracking and managing employees' professional development to enhance their skills and ensure the organization remains agile and competitive.

Price	Status	More Info	
Tier 1: $15k/year Tier 2: $25k/year Tier 3: $35k/year	Started	Greg Drewry, 865.218.5916, gdrewry@epri.com two-page summary of project	

Cyber Security for Power Delivery and Utilization (P183)
Supplemental Projects

Integrated Cyber-Physical Security for Distribution Automation

Utilities must protect their assets from both cyber and physical security threats, particularly with the increasing use of distribution automation equipment like reclosers. EPRI has developed a prototype cyber-physical security system that combines low-cost sensors, a security orchestration platform, and facial recognition to detect and mitigate both physical and cyber threats in real time and offers utilities the opportunity to evaluate its capabilities and integration into their systems.

Price	Status	More Info	
5 sites: $90K 10 sites: $130K 20 sites: $190K	Started	Greg Drewry, 865.218.5916, gdrewry@epri.com Scan QR code for two-page summary of project	

NextWave AMI: Riding the Current, Powering the Future - Maximizing AMI Now and for the Future

Advanced Metering Infrastructure (AMI) is widely deployed but often underused, with most utilities leveraging only basic functions like billing and outage detection. As AMI systems reach end-of-life, utilities have a strategic opportunity to unlock advanced capabilities—such as DER visibility, load insights, and enhanced grid control—that drive modernization and customer value.

Price	Status	More Info	
(over 3 years) Tier 1: $150k Tier 2: $225k Tier 3: $300k	Started	Matt Wakefield, 865.218.8087 mwakefield@epri.com two-page summary of project	

Operational Technology Data 101: Cultivating Data Literacy and Stewardship in Utilities

This project, "OT Data 101," aims to help utilities strengthen data literacy so they can better transform operational technology data into actionable insights. By building core skills in data analysis, management, and decision-making, the course equips utility professionals to fully harness data as a strategic asset.

Price	Status	More Info	
$50,000 for a virtual option and $100,000 for an in-person	Started	Esther Amullen, 650.855.1027, eamullen@epri.com Scan QR code for two-page summary of project	

Cyber Security for Power Delivery and Utilization (P183)
Supplemental Projects

OT Cyber Risk Assessments for Transmission and Distribution Operations

EPRI experts will help utilities assess risks from existing and emerging cyber threats, quantifying their potential impacts across reputational, environmental, financial, safety, and operational categories. This comprehensive risk understanding will guide utility decision-making, prioritization of mitigations, and investment in controls to protect infrastructure and manage cyber threats effectively.

Price	Status	More Info	
Based on scope	∞ Ongoing	Esther Amullen, 650.855.1027, eamullen@epri.com Scan QR code for two-page summary of project	

OT-INSIGHT (Operational Technology Intelligence-Driven Security, Investigation, and Guided Hardening Through Tactic Emulation)

OT-INSIGHT introduces a framework that maps threat actor behaviors to specific OT assets and protocols, making cybersecurity guidance more actionable for the energy sector. Powered by the FM-EDSEC AI Assistant, it enhances adversary emulation, speeds threat response, and strengthens cyber resilience across energy delivery systems.

Price	Status	More Info	
$100K	Started	Chuck Moran, 650.855.8521 cmoran@epri.com Scan QR code for two-page summary of project	

Power Delivery Cyber Security Tailored Assessment for Utility Transmission and Distribution Operations

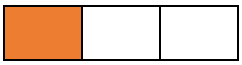
EPRI experts will evaluate specific areas of a utility's cybersecurity program, such as asset management, remote access, or engineering design, providing tailored recommendations for improvements, goals, and timelines. The results will help identify priority cyber risks, build a baseline plan for addressing cyber-physical threats, and develop action plans to strengthen the cybersecurity program.

Price	Status	More Info	
Based on scope	∞ Ongoing	Esther Amullen, 650.855.1027, eamullen@epri.com Scan QR code for two-page summary of project	

Cyber Security for Power Delivery and Utilization (P183)
Supplemental Projects

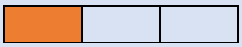
Secure IED Management Strategies

This project will help participants assess management challenges related to Intelligent Electronic Devices (IEDs) and develop an integrated strategy tailored to their specific fleet of IEDs in power delivery infrastructure. The initiative focuses on closing OT visibility gaps, managing compliance risk efficiently, optimizing IED procurement, and enhancing security controls through IED management systems.

Price	Status	More Info	
$75K	 Started	John Stewart at 865.279.1447, jstewart@epri.com Scan QR code for two-page summary of project	

Utility Red Team Collaborative

This project uses a Red Team Collaborative approach to provide electric utilities with simulated cyber threat assessments, offering insights into vulnerabilities, response mechanisms, and recovery protocols. By participating, utilities can enhance cyber resilience, gain valuable red team experience, and learn from industry trends and best practices through anonymized, non-proprietary assessment results.

Price	Status	More Info	
$35,000 per utility annually	 Beginning	Chuck Moran, 650.855.8521 cmoran@epri.com Scan QR code for two-page summary of project	

Zero Trust for Operation Technology (OT): Balance Competing Objectives on the Road to a Zero-Trust Mindset

The Zero Trust for OT (ZT4OT) project aims to implement zero-trust security in operational technology environments by developing authentication solutions for key protocols, conceptualizing architectures for substations and DER systems, and ensuring NERC CIP-015 compliance. The project will also use digital twin modeling to assess security options and create a roadmap for adopting zero-trust capabilities while balancing operational resilience and cyber-risk reduction.

Price	Status	More Info	
$100K	 Ongoing	John Stewart, 865.279.1447, jstewart@epri.com Scan QR code for two-page summary of project	