EPRI

Information, Communication and Cyber Security

Area Review 2026

MARCH 2026

AT A GLANCE

Information and Communication Technology (ICT) Program 161

Research Value

- **Interoperability** – Accelerate industry's migration toward interoperable protocols, standards, and architectures.
- **Data-Centricity** – Leading the industry towards enterprise-wide data management and domain specific best practices for defining, measuring, sharing and utilizing data.
- **Telecommunications** – Advancing ubiquitous, standardized and resilient networks to enable secure connectivity for the grid of the future.
- **Strategy** – Measuring and quantifying the benefits of scalable, standardized ICT approaches and architectures with tools, resources, and guidance to develop and apply an actionable roadmap.

Member Benefits

- **Identify and understand emerging Information and Communication Technologies and how they may impact utilities** – AI, Geospatial information, AR/ VR, Edge Computing, IT/OT Convergence, Cloud, 5G/6G, device and enterprise Standards and Protocols.
- **Annual Reference Guidebooks** – Providing tools, strategies and references related DER Protocols, Enterprise Architecture, Advanced Metering, Telecommunications, and Geospatial Informatics.
- **Thought Leadership Insights** – Strategic planning and execution, Roadmapping tools, impact assessments and proven best practices.
- **Case Studies** – Learning from Actual Deployments.

Promote innovation by identifying, evaluating, and applying emerging Information and Communication Technologies for grid modernization and digital transformation efforts.

This program addresses technical and economic challenges of identifying, evaluating, and implementing and enabling

- Information and Communication Technologies (ICT) for grid modernization and digital transformation efforts.
- Tools and resources including Artificial Intelligence (AI) to enable adoption of emerging ICT and the development of strategies to prioritize IT/ OT Investments.
- Emerging and potentially disruptive technologies insights to inform decision makers of potential impacts and opportunities.
- Technology and standards evaluation, laboratory testing, and field demonstrations, interpreting results into opportunities and challenges to achieve interoperable, scalable, cost-effective solutions and maximizing the sharing.
- Industry case studies, best practices, and guidebook development. Experiences are captured through utility immersions, interviews, and case studies.
- Technology transfer with a variety of approaches to share and apply research results, including technical reports, white papers, software tools, webcasts, workshops, and application of ICT program resources directly for utilities.

EPRI CONTACT

SEAN CRIMMINS, *Program Manager*
650.855.7901, scrimmins@epri.com

Research Highlights

Emerging Technologies and Technology Transfer (161A)

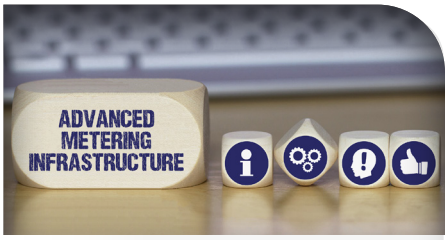
- Delivers strategic insights into emerging information and communication technologies.
- Develops white papers that investigate and analyze emerging ICT issues that could enable innovation, future proofing,efficiencies, cost savings, and a better customer experience.

DER Data and Connectivity (161D)

- Research about interoperability and interchangeability standards that help you integrate with increasingly diverse sets of DERs
- Assess the continuously flowing pipeline of new data and connectivity solutions for DERs and how Artificial Intelligence (AI) can unlock insights and opportunities in DER data.
- Best practices and peer perspectives to help utilities support investments in the ICT technologies needed to support DER integration.

Enterprise Architecture (EA) and Integration (161E)

- Guidebooks and resources for EA practitioners to increase maturity, influence, and impact to become an integral part of the business from strategy development to technology evolution.
- Research on aligning business and technology including capability modeling, digital transformation, and modernization.
- Resources on standards-based integration and interoperability to enable faster application and feature implementation.
- Research on Data Management, helping all participants in the enterprise have access to the information and toolsets necessary to maximize data utilization.



Advanced Metering Systems (161F)

- Assists utilities in designing, selecting, integrating, and deploying AMI systems based on standards, to reduce lifetime costs and improve performance.
- Provides insights into all aspects of AMI systems operation and management life cycles.
- Optimizes the use and value of AMI and the full range of applications that can be supported.
- Help utilities to prepare for newer AMI systems that employ AI in both the headend system and the metering devices.

Telecommunications (161G)

- Identify and mitigate interference to 6-GHz systems.
- Identify, analyze, including AI and quantify business cases for fiber and broadband service opportunities.
- Understand standards-based FAN technologies – Private LTE, 5G, and IoT networks, and their configuration and optimization for utility purposes.
- Develop insights for utility telecom network management.
- Engagement in Telecom Standards development.

Geospatial Intelligence (161H)

- Optimizing geospatial data performance for electric utilities.
- Provides insights into innovative geospatial applications electric utilities can leverage to optimize the value of their geospatial investments.
- Develops innovative geospatial analysis techniques to support multiple utility business processes.

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

© 2026 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ENERGY are registered service marks of the Electric Power Research Institute, Inc.

Emerging Technologies and Technology Transfer (161A)

Provides insights into emerging ICT standards and issues that could impact utility investments and accelerates technology transfer.

Sean Crimmins,
Program Manager,
scrimmins@epri.com

PROJECT

Emerging ICT and Technology Transfer

Technology Innovation

2025 Accomplishments & Key Deliverables

The "3rd Thursday" of the Month ICT Program Webcasts provide tracking and analysis on key standards development activities provides up-to-date information on standards development and an analysis of the impact that these activities can have on electric utilities. Each month, members provide input on future topics.

Summary of Interoperability Tracking and Reporting by the ICT Program in 2025 – 3rd Thursday Webcasts

2025 Schedule (epri.com log in is required to access presentations)

January 16th - DER Data and Connectivity

February 20th - Enterprise Architecture

March 20th - Advanced Metering - AMI 2.0 - Further Advancements in Metering Systems

April 17th - Telecommunications

May 15th - Geospatial Informatics

June 19th - ICT Mid-Year Update

July 17th - DER Data & Connectivity

August 21st - Enterprise Architecture Value Proposition

September 18th - Grid Edge Applications

October 16th - Telecommunications pLTE/5G Spectrum Options Update

November 20th - Geospatial Informatics Digital As-built Technologies

December 18th - ICT End of Year Review

ICT Program Newsletter – Periodic newsletter (typically bi-monthly) with brief articles on program activities and research project results.

Implemented the ICCS Online Forum - The Information, Communication and Cyber Security (ICCS) Forum is a utility member-only discussion forum.

Annual Reviews deliverables have been incorporated into the Smart Grid Standards Tracking and Emerging Information and Communications Technology Project Set for 2025.

AI Readiness in Utilities: Turning Data into Strategic Advantage (Public) AI has the potential to rapidly transform the utility sector to enhance efficiency, decision-making, and customer experience. A significant gap remains between AI ambition and execution due to challenges in data management. To unlock AI's full potential, utilities must prioritize data readiness.

2026 Plan

Monthly Technology Transfer webcasts that provide strategic insights on emerging ICT, program updates, and the opportunity for impromptu discussions on emerging topics. ("Third Thursday of the month").

ICT Program Newsletter – Bi-monthly newsletter with the latest on on program activities and research project results.

ICCS Online Forum – Discuss the latest challenges with EPRI and your peers in a secure, member only forum.

Annual Program Area Review – Digital Summary that provides a summary of the research results produced by the ICT program during the current year, what is planned for the next year and success stories on how members have used and benefited from program results.

© 2026 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ENERGY are registered service marks of the Electric Power Research Institute, Inc. 800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

P161 D

Distributed Energy Resources (DER) Communication and Data Integration (161D)

It focuses on tools, technologies, architectures, methodologies, insights, and best practices. The main goals are to reduce costs, improve operational efficiency, and help utilities prepare for the energy system of 2030.

Ben Ealey,
Principal Team Lead,
bealey@epri.com

PROJECT

Distributed Energy Resources (DER) Standards – Interoperability, Information, Protocol, and Connectivity Standards

Emerging Topics, Technologies, and Techniques

Integration Experiences and Practices

2025 Accomplishments & Key Deliverables

DER Non-Interoperability and How We Fix It: EPRI Findings and Action Plan (Public). EPRI launched the DER Interoperability Lab initiative to identify, test, and address communication issues with DERs through a public working group. This paper summarizing the issues found and EPRI's response plan.

EPRI Protocol Reference Guidebook - 9th Edition: Annual Assessment of Protocols and Profiles for Achieving Grid Flexibility from DER, Electric Vehicles, and Demand Flexibility Technologies is a reference document for stakeholders working with DER and demand response technologies who want to learn more about the different options for application-layer protocols.

Interoperability Guidance for Utility Technical Interconnection Requirements covers key aspects of IEEE 1547-2018 Clause 10 implementation — from version management, gateway roles, coordinated communications, protocol selection, and PKI trust management to unlock code policies — providing utilities with structured guidance for secure, scalable, and interoperable DER integration.

IoT Technologies for DER - 4th Edition: Information, Case Studies, and Lab Evaluations of IoT-Based Connectivity, Distributed Messaging, and Integrated Platform-As-A-Service Solutions provides a high-level presentation of prevalent IoT protocols, including hardware, software, and messaging technologies, to build a baseline for understanding the potential of IoT protocols.

Smart Meters with Internal Wi-Fi for DER Integration Challenges and Research Needs for DER-Ready AMI Platforms focuses on a recent evolution in AMI technology: smart meters with internal Wi-Fi.

Distributed Energy Resources Interoperability Guidebook - 2025 Edition an annually updated guide that outlines how to achieve interoperability and cost-efficiency in demand response (DR) and distributed energy resource (DER) programs.

Interoperability at Scale: The Hidden Complexity of IEEE 2030.5 Certificates summarizes the distinctive PKI structure of IEEE 2030 centered on the SERCA root — contrasting it with traditional PKI models and outlining the resulting interoperability, trust-chain, and lifecycle challenges for DERs, utilities, and DERMS, while offering guidance on PKI governance, architectural considerations, and scalable trust strategies for secure DER integration.

Where Small Worlds Collide: Navigating the EV Protocol Universe examines how EVs are evolving into grid-interactive DERs and highlights the need for interoperable architectures, shared communications standards, and coordinated stakeholder ecosystems to enable scalable, secure smart charging and V2G integration.

2026 Plan

EPRI Protocol Reference Guidebook 10th Edition is a concise, stylized, digest-like overview of communication protocols that allows readers to make 1:1 comparisons of specific aspects of information and protocol standards. Previous editions have covered protocols such as: EcoPort (ANSI/CTA-2045:2018), OpenADR, SunSpec Modbus, , IEEE 2030.5, OCPP, Matter, and more. The report content spans across demand response, EVs, energy storage, smart inverters, and DER group management. New protocols are considered annually.

DER Data and Connectivity — Technology Pipeline Technical Update — EPRI will work with members to establish a pipeline of emerging technologies related to DER data and connectivity.

Study Results Tech Update from one or two Promising Technologies — Each year, EPRI selects one or two promising technologies for further study. EPRI will evaluate how these technologies will support the industry, the maturity of the technology, and what is required for it to be successful. The results will be shared with members at task force meetings for further discussion about next steps for EPRI research on each topic.

Utility Experiences in DER Integration works with member utilities to capture experiences, use cases, and other information to inform the member collaborative. This includes member task force meetings twice a year to discuss ongoing EPRI and utility research efforts in the industry.

DER Interoperability Guidebook leverages 10+ years of work developing and applying standards. The 2026 version of the guidebook includes the following sections: Industry Requirements for DER Interoperability & Protocols, How to Validate Conformance: EPRI & Industry Test Tools, Example DERMS Communication Architectures, Cloud-Based Architectures to Support DR Programs and more.

© 2026 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ENERGY are registered service marks of the Electric Power Research Institute, Inc. 800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

P161 E

Enterprise Architecture and Integration (161E)

Establishing and improving Enterprise Architecture that is committed to strategic alignment, information availability and an optimized application portfolio.

Bijan Hosseininejad,
Principal Technical Leader
bhosseininejad@epri.com

PROJECT

2025 Accomplishments & Key Deliverables

Enterprise Architecture (EA)

Library of Enterprise Architecture Patterns: LEAPworx, 7th Edition is a repository of Enterprise Architecture diagrams for the electric utility industry, updated to include Distributed Energy Resource Management (DERM) Reference Architecture and Telecom Network Reference Architecture.

Utility Enterprise Architecture Guidebook, 10th Edition provides comprehensive guidance and strategies for EA practitioners to implement standards such as The Open Group Architecture Framework (TOGAF) in an electric utility context, including a recent update on leveraging Generative AI to develop and test the value message of EA.

Enterprise Systems Integration

Common Information Model Primer: 11th Edition (Public) helps readers understand how the Common Information Model (CIM) is used at electric utilities, including the basics of Unified Modeling Language (UML) as well as guidance and examples on implementing CIM.

Cloud Integration Guidebook, 10th Edition: A Guide for Enterprise Architects was created to synthesize resources from the relevant literature, regulatory guidance, and the experiences of utility practitioners who have been on the leading edge of migrating applications to the cloud.

Organizational Alignment

Utility Business Capability Model 2026 is an electric utility-specific model of capabilities that define what the business may focus on, including new capabilities for data management and asset management domains. This is a complete version with four levels of depth for most capabilities. A Public Version is also available.

Utility Business Capability Guidebook, 4th Edition is a reference for understanding business capabilities and models, and how they support strategy execution through capability based planning.

Digital Transformation: Information Technology-Operational Technology Convergence Guidebook, 8th Edition aims to define key IT OT concepts, explain convergence drivers, outline three convergence levels, offer approaches for overcoming cultural barriers, present updatable EPRI research, guide capability selection, and highlight future research needs.

Data Management

Data Management Guidebook: 1st Edition consolidates EPRI research in data management, including data quality, business capability, and semantic modeling. This guidebook outlines why data management is particularly important, as well as particularly challenging in the current environment, and provides resources to assess and improve data management maturity.

2026 Plan

Utility Enterprise Architecture Guidebook, 11th Edition will be updated to include the latest EA research and practices in the electric utility industry, including adoption of product model-inspired methodologies. model-inspired methodologies.

Top Ten Indicators of EA Maturity: 2026 Survey Results will be published, providing insight on the state of the EA discipline in the utility industry.

Common Information Model Primer: 12th Edition (Public), along with the accompanying microsite, will be updated to include the latest developments around the CIM standard.

Utility Business Capability Guidebook, 5th Edition will include new research and guidance, including value-based delivery.

Digital Transformation: Information Technology-Operational Technology Convergence Guidebook, 9th Edition will include new insights gained from across the electric utility industry, including maturity model updates.

Data Management Guidebook: 2nd Edition will include the latest developments in the domain, providing a foundation to support data-driven decision-making and insights driven by advanced analytics capabilities.

Data Management Maturity Model 2026 will be updated in conjunction with the Data Management Guidebook to provide a resource for assessing Data Management maturity and planning a roadmap for maturity growth.

© 2026 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ENERGY are registered service marks of the Electric Power Research Institute, Inc. 800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

P161 F

Advanced Metering Systems and SCADA (161F)

Leading industry efforts to develop open, interoperable AMI systems combined with practical guidance and analytics for today.

Daniel Quarells,
Technical Leader II
dquarells@epri.com

PROJECT	2025 Accomplishments & Key Deliverables	2026 Plan
Achieving Open, Interoperable Advanced Metering Systems	ANSI Meter Standards Utilization, 2nd Edition analyzes a sample of twenty meters, both old and new, to assess their compliance with the ANSI C12.18 Standard (optical port protocol) and the ANSI C12.19 Standard (data table standard). While some quirks and anomalies were discovered, it appears that the level of compliance with these two standards is sufficient to read enough data in a standard form that would allow for the creation of a bill.	***Metering Engineering Tutorial*** describes the current state of metering engineering, with particular attention to applications and standards of practice.
Advanced Metering Systems Operations and Management	The Evolution of Advanced Metering Infrastructure System Functions traces the evolution of AMI and Head-End Systems, explains their role as the operational backbone of modern metering, and offers a maturity model to guide utilities in advancing toward a fully digital, intelligent grid.	***Edge Artificial Intelligence (AI) for Metering Applications*** describes some of the machine learning capabilities, distributed intelligence applications, for edge nodes in AMI systems and analyzes some of the implications of these functions. ***Meter Services Operations Overview*** defines the purposes, methods, equipment, personnel, and training for a modern meter services department?
Optimizing Advanced Metering System Value and Utilization	Advanced Metering Data Analytics Guidebook (AMI-Data-Analytics) 3rd Edition this web application explains how successful utilities organize their AMI data, systems, and staff to support analytics, outlines key use cases and architectures, and reviews eight open-source tools plus new machine-learning methods for AMI data analysis. To access AMI-Data-Analytics v3.0, click here: https://ami-data-analytics.epri.com (log in required)	***Advanced Metering Data Analytics Guidebook, 4th Edition*** is an update of the 2025 version to include the latest developments, including the use of machine learning in metering data analytics.
SCADA Protocols	Considerations for Incorporating Substation Meters into Advanced Metering Infrastructure Platforms this report outlines how integrating substation meters into AMI can expand operational capabilities, improve reliability, and strengthen grid resilience beyond traditional billing functions.	***SCADA vs. AMI Protocols: A Comparison*** describes some of the defining characteristics of both SCADA and AMI protocols to help utility personnel from either realm to better understand commonalities and differences.

© 2026 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ENERGY are registered service marks of the Electric Power Research Institute, Inc. 800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

EPRI

P161 G

Telecommunications (161G)

Communication technology analysis thru laboratory and field tests to help utilities effectively plan and design their communication networks.

Tim Godfrey,
Program Manager,
tgodfrey@epri.com

PROJECT

Wide Area Networks

Field / Neighborhood Area Networks

Telecommunications Planning and Management

Telecommunication Standards Engagement

Technology Innovations

2025 Accomplishments & Key Deliverables

6 GHz AFC Protection: Field Test Results - 2025 summarizes EPRI's work in the WInn Forum 6 GHz AFC specifications group, the resulting consensus to address WINNER2 under-protection issues, findings from DOE-funded AFC field tests at a Southern Company microwave site, and the investigation of real-world unlicensed interference to an SRP fixed-service link.

Strategic Fiber Guidebook: 2025 Edition focuses on electric utility specific fiber optic networks. Several research questions arise when a utility considers deploying or expanding a fiber optic network.

Wide Area Network (WAN) Modernization Guidebook: 2025 Edition introduces telecom wide-area networking for electric utilities, explaining why WANs are needed, how their technologies have evolved, and best practices learned from utility network migrations.

Low-Latency Testing of 5G for Utility Use Cases documents the testing methods, testing results, and the future work planned for this area of research.

Private Long-Term Evolution Guidebook - A Guidebook on Cellular Communications for Utilities: 7th Edition provides an overview of the technology and architecture and identifies current and potential spectrum options for private LTE network deployment.

Network Management Systems Guidebook introduces the audience to the field of telecom network management with a focus on the field's evolution, including the more recent role of artificial intelligence (AI)/machine learning (ML), and its relevance for the utility industry.

Satellite and Emergency Communication: Phase 3 evaluates LEO satellite communications — through Starlink performance testing, MPLS failover trials, and new NTN phone-based connectivity — as a promising low-latency, lower-cost solution for extending reliable utility communications to remote grid assets and workers.

Security and Resiliency of Utility Critical Communications Infrastructure for Microgrids assesses the security and resilience of microgrid communications using private LTE, evaluating LTE's protections against Zero Trust principles and offering guidance to help utilities build secure, pLTE-enabled microgrids that mitigate cyber-physical risks.

Smart Grid Communications Intelligencer 1H 2025 and 2H 2025 biannual newsletters that highlight issues of relevance and interest to utility communications engineers and managers.

Telecom Standards Guidebook 7th Edition focuses on the purpose and relevance of the standards as well as the development status and roadmap of the standards development organizations.

Telecommunication Simulator provides a repeatable testbed that lets utility engineers assess grid application performance under realistic wireless network impairments such as asymmetric latency, packet loss, and bandwidth limitations.

2026 Plan

Evaluation of Interference to 6 GHz Microwave analyzes and field tests interference impacts on licensed microwave links arising from increased consumer adoption of WI-Fi 7 and new types of unlicensed devices, including VLP and GVP.

Strategic Fiber Guidebook: 2026 Edition Annual Guidebook Update.

WAN Modernization Guidebook 2026 Edition updates on SDN, SD-WAN, and Segment Routing, Requirements Engineering and Planning, and AI tools to assist in project and resource scheduling.

Guidebook on Cellular Communications for Utilities this *2026 version* expands on the previous Private LTE edition, covering private, public, and hybrid cellular technologies, with insights on architecture and spectrum options.

Evaluation of Low-Latency Wireless Technologies is ongoing testing and evaluation of 5G URLLC technologies in labs and real-world environments.

Network Management Systems Guidebook 2026 update of the telecom network management guidebook, including training on automation-friendly protocols/algorithms, expanding the role of AI/ML.

4G and 5G Architecture Approaches for Resilient Networks 4G and 5G research and technology evaluation to enhance security and resiliency of utility critical infrastructure.

Satellite and Emergency Communication 2026 is an update on best practices for ensuring communications availability in emergency scenarios, assessment of new technologies for non-terrestrial networks, and longer-term test results for existing and new suppliers of Low Earth Orbit satellite systems.

Smart Grid Communications Intelligencer 2026 is an annual newsletter for utility communications professionals covering tech, standards, and business trends impacting smart grid infrastructure.

Telecom Standards Guidebook Vol 7 (2026) annual update of this guidebook incorporates a high-level description of current and historical telecom and communications standards, their roadmap, utility applications, and interrelationships.

© 2026 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ENERGY are registered service marks of the Electric Power Research Institute, Inc. 800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

P161 H

Geospatial Intelligence (161H)

Advancing the use and value of geospatial data sets to deliver new geodata services utility applications.

Kevin Gorham,
Principal Technical Leader,
kgorham@epri.com

PROJECT	**2025** Accomplishments & Key Deliverables	**2026** Plan
Geospatial Informatics Data Practices	Geospatial Informatics Guidebook: 6th Edition is an annual update of a digital reference for best practices in geospatial data management. This prepares electric utility GIS professionals to deliver improved geodata services to an expanding spectrum of utility individuals and systems. It intends to help GIS professionals understand how geospatial industry trends affect their management of geospatial information and investments.	***Geospatial Informatics Guidebook: 7th Edition*** is a digital reference for best practices in geospatial data management, updated annually.
Geospatial Informatics Innovation Engine	Digital Twin Case Studies and Takeaways from Industrial Immersive 2025. The integration of digital twins, AI, and immersive technologies like AR/VR is revolutionizing operational efficiency across industries. Case studies from Industrial Immersive 2025 highlight applications in energy, urban planning, and training, showcasing evolving uses from grid resiliency to XR-enhanced inspections. GIS Data Quality State-of-the-Art: Machine Learning and Artificial Intelligence highlights how digital twins combined with AI and immersive AR/VR technologies are being used across industries — illustrated through multiple case studies — to show current operational applications and emerging directions for digital twin evolution.	***Geospatial Innovations Lab Strategy*** outlines the Lab's strategic direction for extending current GIS technologies.
Geospatial Informatics Analytics and Visualization	Geospatial Intelligence Adds New Dimensions to Utility Situational Awareness helps utilities operate more safely and efficiently by integrating GIS with utility systems and new data sources, and the EPRI Geospatial Innovations Lab supports utilities in unifying these tools to turn data into actionable insights.	***2026 Geospatial Innovations Lab Demonstration*** presentation on GIS graph network and machine learning research results.

© 2026 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ENERGY are registered service marks of the Electric Power Research Institute, Inc. 800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

Success Stories
Information and Communication Technology (ICT)

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.

Topic

Data Science Model to Correct Customer Linking using AMI Voltage Correlation: Alabama Power Company (2025)
Alabama Power implemented a data science model using AMI voltage data to accurately link customer meters to transformers. This improved GIS accuracy and outage management, enabling faster fault isolation, better grid reliability, and proactive customer communication. The approach converts underused voltage data into actionable insights, delivering efficiency, resilience, and a scalable solution for industry adoption.

Grid Model Data Management (GMDM) for Distribution: Puget Sound Energy (2025)
GMDM for Distribution addresses the challenge of centralizing distribution grid model data to support planning and operations amid increasing DERs, flexible loads, and advanced services. The project applied EPRI's GMDM Information Architecture to define the problem domain and deliver actionable recommendations for Puget Sound Energy to improve data collection, management, and model exchange. These improvements reduce engineering workload, enhance model quality and synchronization, and enable advanced distribution management capabilities for faster, more accurate system analysis.

Grid Edge Communications Evaluation and Unified Fixed-Access Service (UFAS) Gateway: Taiwan Power Company (TPC) (2025)
The UFAS Gateway initiative creates a unified communications platform combining Power Line Communication (PLC), WiFi HaLow, and cellular for flexible, cost-effective connectivity across utility assets. It reduces vendor dependency, supports legacy and future systems, and enables scalable, global deployment. TPC, with EPRI and ITRI, is advancing from concept to design and deployment based on evaluations of Broadband over power lines (BPL) and low-cost hardware.

5G Evaluation and Low Latency Network Performance Testing: Consolidated Edison of New York (2025)
Low-latency, high-reliability communications are critical for integrating growing DERs. EPRI research enables Con Ed to make confident design decisions, supporting scalable, efficient connectivity for protection and operations. This work accelerates DER adoption, optimizes resources, and strengthens grid resilience

EPRI 2025 Technology Transfer Award Winner

Voice Assistant and Artificial Intelligence (AI): Southern Company, FirstEnergy, NYPA (2025)
Voice Assistant and AI enables hands-free workflows for utilities by integrating voice technologies into IT/OT systems for work order creation, data retrieval, and safety communication. Field tests showed reduced admin burden, improved data accuracy, and enhanced safety in high-noise environments, providing a scalable framework for broader adoption.

Available Fault Current (AFC) Simulation and Risk Analysis, Southern California Edison(SCE) (2024)
Teleprotection is essential for the safe operation of transmission lines, and this work supports SCE's ability to continue providing reliable service to customers. The analysis of 6 GHz band sharing, which requires an understanding of Federal Communications Commission (FCC) rules, AFC methodologies, and obstructions, will set a precedent for future band sharing plans for both federal and non-federal spectrum.

Success Stories
Information and Communication Technology (ICT)

Available Fault Current (AFC) Simulation and Risk Analysis, Southern California Edison(SCE) (2024)
Teleprotection is vital to transmission safety, and this work supports SCE reliability while informing future federal and non-federal 6 GHz spectrum sharing.

Enterprise Architecture, Alliant Energy (2024)
Alliant Energy used EPRI's Capability Model and the Gartner T-I-M-E framework to identify redundant applications, align with stakeholders on migration and elimination plans, and reduce technical debt while cutting O&M costs by more than $1 million.

Enterprise Architecture Maturity Assessment, Salt River Project (SRP) (2024)
The research delivered a maturity model that assesses SRP's current state and guides continuous improvement, identifying actions to support IT/OT convergence and digital transformation with Enterprise Architecture as a key enabler.

Grid Model Data Management, American Electric Power (AEP) (2024)
Distribution Grid Model Management is essential to enable DER integration and advanced distribution management by addressing data complexity and fragmentation, centralizing models to reduce engineering effort, improve model quality and synchronization, and support faster, higher-confidence planning and interconnection decisions.

Grid Network Model Management, Ameren (2024)
The Ameren INMM EPRI project extended EPRI's grid model management architecture using IEC CIM standards to secure funding and implement Cimphony, a CIM-based platform now managing over 6,000 feeder models with daily GIS updates to support ADMS and planning applications.

Low-Latency Wireless Communications, Consolidated Edison (ConEd)(2024)
EPRI's research supports the growing need for low-latency, high-reliability distribution communications by enabling confident grid planning and advanced protection designs that support scalable DER integration and a more resilient, sustainable energy system.

Emerging Information, Communication Technology (ICT) and Technology Transfer - PECO, an Exelon Company (2023)
The Emerging Technologies and Technology Transfer Project Set shares ICT standards, issues, and peer-utility insights to keep utilities informed of EPRI research and emerging trends supporting an advanced electric grid.

"3rd Thursday of the Month" Emerging Technology Webcasts and ICT Program White Papers - American Electric Power (AEP) (2023)
The 161A "3rd Thursday of the Month" webcast series provide regular updates on emerging trends and insights of the entire program with topics determined based on member input."The 10 technical "3rd Thursday of the Month" webcasts and the White Papers produced in this project set are timely and good assessments of the covered topics and are helpful in providing useful talking points to others across member utilities business units at AEP.", Ron Cunningham, IT Enterprise Architect, AEP.

Advanced Communications, Standards, and Controls of Smart Inverters and Smart Devices to Enable More Residential Solar Energy - Southern California Edison, Pacific Gas and Electric (2023)
The project evaluated advanced smart inverter functions and interoperable communication architectures under California Rule 21, demonstrating through lab and field testing that combining smart inverters with PV-optimized load management can significantly increase solar integration and grid performance.

Economically Feasible, Secure DER Network Gateways for Control Integration of Smart Inverters - New York Power Authority, Consumers Energy, North Carolina Electric Membership Corporation, Électricité de France, Salt River Project, Evergy, Southern Company, Exelon, Tennessee Valley Authority, KEPCO (2023)
Utilities are adopting DERMS to manage diverse DERs, with the DER Gateway—supported by EPRI research and the emerging IEEE 1547.10 standard—providing a secure, standards-based platform to handle utility-specific integration needs and guide utility RFPs and market development.

Utility Business Capability Model for Investment Optimization - National Grid USA (2023)
The Utility Business Capability Model enables strategic capability-based planning, with National Grid leading its advanced application internally and across the industry to support its utility-of-the-future initiatives.

To read more Success Stories click at this link or use the QR code

Supplemental Project Offerings
Information and Communication Technology (ICT)

Supplemental projects are member-funded, quickly initiated EPRI research efforts led by EPRI staff to address targeted needs, with shared scope, defined deliverables, and EPRI-owned results licensed for internal use by participants.

Applied Grid Model Data Management (GMDM) for Distribution or GMDM for Transmission
The Applied GMDM project helps utilities implement EPRI's grid data architecture to streamline model updates, improve accuracy and traceability, reduce labor costs, and better support grid simulation needs.

Assessment of DER-Ready Meter Forms
This project evaluates voice-enabled technologies for utility maintenance, operations, and construction to improve productivity, safety, and satisfaction while addressing IT/OT integration, cybersecurity, and workflow impacts

Assessment of MATTER Protocol for Utility Applications
The Matter protocol aims to improve secure, cloud-independent interoperability among smart devices and could enable tighter utility integration with systems like SCADA and AMI, though utility use cases have yet to emerge

Data Management Collaborative: Surviving the Data Avalanche
This collaborative project helps utilities improve data management maturity by sharing best practices, strengthening data literacy, and applying assessment frameworks to enable AI-driven insights, better decisions, and sustained competitiveness.

Ensuring That DER Are Grid-Equipped (EDGE)
EPRI developed a Common File Format to electronically exchange DER settings and prevent grid violations, but the format currently lacks cybersecurity protections and can be easily altered.

Enterprise Architecture Maturity Assessment
This project helps utility enterprise architecture teams assess and improve EA maturity through surveys and a practical guidebook that aligns leading frameworks like TOGAF with business strategy.

EPRI U - Information, Communication Technology and Cyber Security (ICCS)
This project addresses utility workforce turnover and digital transformation by delivering foundational ICCS training and implementing a system to track and manage employee skill development to maintain agility and competitiveness.

Evaluation of Automated GIS Data Cleanup Methods
This project evaluates emerging technologies to automate GIS data cleanup and asset inventorying using vehicle-based, aerial, and satellite mapping approaches.

Field Evaluation of Digital As-Built Technology Solutions
This research examines digital, scalable alternatives to manual GIS as-built processes to improve data accuracy, speed, and resilience, strengthening grid operations and outage response.

FLEXIT: Flexible Interoperable Technologies Initiative: VPP/DER Registry and Integration Interface
This project provides utilities with a common framework and guidance for integrating DER through aggregators, simplifying requirements, improving utility–aggregator interactions, boosting customer confidence, and informing regulatory discussions.

GIS Migration Data Requirements: Investigating Data Readiness
As the grid shifts to a hybrid, DER-rich model, utilities must modernize data-intensive systems and migrate GIS to better support asset management, maintenance, and outage response.

Grid Model Data Management (GMDM) Vendor Forum Phase II: An EPRI-Sponsored Vendor-Funded Collaborative Initiative
This initiative develops a lifecycle asset tracking system using durable QR-based unique identifiers and industry standards to improve visibility, traceability, and inventory management of electric grid assets from manufacture to retirement.

Supplemental Project Offerings
Information and Communication Technology (ICT)

Grid Model Manager (GMM) for Distribution Interest Group
This interest group defines an industry vision and architecture for Distribution Grid Model Managers by aligning utility and vendor perspectives to support accurate, analysis-ready distribution grid models.

Grid Modernization Strategic Roadmapping
Rising customer expectations, policy changes, extreme weather, and DER integration are driving widespread regulatory action and multi-year, commission-mandated grid modernization plans across U.S. utilities.

NextWave AMI: Riding the Current, Powering the Future - Maximizing AMI Now and for the Future
As AMI systems reach end of life, utilities have a strategic opportunity to move beyond basic billing and outage uses to unlock advanced capabilities that support DER integration, grid modernization, and greater customer value.

Renewables Communications: Use Cases, Communications Technologies, and Implementation Considerations
This project examines communication use cases, technologies, and protocols at remote renewable sites to support expanding solar and wind assets through member collaboration and EPRI research

Utility Digital Worker Collaborative
This project advances digital worker technologies by evaluating impact, sharing case studies, and convening an annual forum to help utilities safely and effectively deploy applications that improve field and plant work performance.

For a more detailed listing click Information and Communication Technology Program161Supplemental Project Offering Summaries.

AT A GLANCE

Cyber Security for Energy Delivery and Customer Solutions Program 183

Research Value

- **Enhanced Resilience Against Cyber Threats** – Develops and implements strategies for advanced cyber security measures.
- **Multidisciplinary Approach to Emerging Challenges** – Addresses the rapidly evolving cyber security threats to interconnected electric sectors with collaborative and multidisciplinary research.
- **Expert Insight and Analysis** – Leverages a team of cyber security experts who offer in-depth insights and analyses on security tools, architectures, and guidelines.
- **Proactive and Comprehensive Cyber Security Strategies** – Identify, address, and adapt to both current and future cyber security challenges, developing roadmaps and strategies to safeguard critical infrastructure.

Member Benefits

- **Access to Cutting-edge Research** – Gain exclusive access to the latest cyber security technologies and research findings to proactively safeguard infrastructure.
- **Expert Guidance and Support** – Benefit from direct support and insights from top cyber security experts, enhancing the ability to respond to and manage threats.
- **Collaborative Network Opportunities** – Engage with industry peers, sharing best practices and learning from collective experiences in cyber security challenges.
- **Tailored Cyber Security Strategies** – Receive customized advice and strategies for specific infrastructure needs, ensuring robust and effective cyber security measures are in place.

Focus on addressing the emerging threats to an interconnected electric sector through multidisciplinary, collaborative research on cyber security technologies, standards, and business processes.

The Cyber Security for ED&CS program focuses on the following issues:

- Strategic Intelligence and Emerging Issues: Focused on providing insights and guidance on strategic cyber security issues relevant to electric utilities.
- Incident and Threat Management: Develops comprehensive cyber security approaches encompassing incident management, threat analysis, and forensics.
- Cyber Security for Transmission and Distribution: Addresses specific challenges in digital substations and control centers, integrating cyber security into utility processes.
- Cyber Security for DER and Grid Edge Systems: Concentrates on risk management and secure integration of distributed energy resources (DER) with grid systems.
- Cyber Security Data Applications: Involves innovative data management strategies and the use of advanced analytics and AI for threat identification and mitigation.

EPRI CONTACT

MATT WAKEFIELD, *Director, Research and Development • ICCS*
865.218.8087, mwakefield@epri.com

Research Highlights

Strategic Intelligence and Emerging Issues (183A)

- Explore how Artificial Intelligence (AI) strengthens cybersecurity and secures AI systems across the enterprise. Provides current threat intelligence and actionable guidance on emerging vulnerabilities to help organizations stay ahead in an AI-driven security landscape.
- Dynamic Program Monitoring and Evolution: Offers guidance for OT cybersecurity programs, alongside developing strategic roadmaps for adapting to emerging threats and technological advancements.

Incident Management and Threat Management (183B)

- Comprehensive Incident and Threat Management: Build systems for monitoring, detection, and response to cybersecurity events, with procedures for threat management and research in AI and machine learning (ML).
- In-depth ICS Forensics: Focuses on conducting detailed forensic analysis of industrial control systems (ICS) devices.

Cyber Security for Transmission and Distribution (183C)

- Targeted Security for Digital Substations and Control Centers: Addresses unique cyber security challenges in digital substations and control centers.
- Integrating Cyber Security into Utility Processes: Focuses on integrating cyber security into utility planning, design, and operations, and developing best practices for long-term security standards in grid infrastructure.

Cyber Security for DER and Grid Edge Systems (183D)

- Cybersecurity for DER Integration: Develops cybersecurity strategies, frameworks, and engineering guidelines to secure grid systems with DER, including evaluation of AI, machine learning, and post-quantum cryptography for both attack and defense.
- Practical Tools and Collaboration: Delivers engineering tools, reference architectures, and field demonstrations to support resilient DER integration.

Cyber Security Data Applications (183E)

- Empowering utilities to maximize the value of cyber security data across transmission, distribution, and the grid edge through practical data and analytics approaches that transform grid operational data into trusted, actionable intelligence. Partner with utilities to establish secure, scalable data foundations AI, and analytics capabilities through resilient data pipelines, sound governance, meaningful metrics and benchmarking, cybersecurity assessments, and applied AI and advanced analytics.

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

© 2026 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ENERGY are registered service marks of the Electric Power Research Institute, Inc.

P183 A

Strategic Intelligence and Emerging Issues (183A)

This project set aims to help utilities proactively identify, address, and adapt to both current and emerging cybersecurity challenges in order to ensure the ongoing protection and resilience of their critical infrastructures.

Matt Wakefield,
Director, Research and Development, ICCS
mwakefield@epri.com

PROJECT

Strategic Intelligence and Emerging Issues

2025 Accomplishments & Key Deliverables

Cyberjoule 2.0 - An Agentic Approach to Cyber Security Metrics and Data Analysis Cyberjoule 2.0 uses agent-orchestrated Agentic AI integrated with the EPRI metrics framework to automate data ingestion, produce defensible cybersecurity metrics, and deliver actionable reporting that helps utilities overcome data-complexity challenges and demonstrate cyber risk reduction across operational, tactical, and strategic levels.

Defending Against Cyber Attacks - A Human-Centric Approach for the Energy Sector: A 2025 Cyber Security Landscape Overview outlines a cybersecurity strategy for the energy sector that blends Zero Trust, AI-driven analytics, and OT-focused resilience while underscoring the vital role of human expertise amid escalating, high-impact cyber threats exemplified by attacks like the 2022 Industroyer2 incident.

Insider Threat Detection: New Findings, Threats, and Advancements Insider threat risks are rising across IT and OT environments due to remote work, workforce turnover, and increased interconnectivity, and this report highlights how utilities can counter them through AI-enhanced detection tools, cross-department collaboration, privacy-aware monitoring, and formalized insider risk programs that strengthen security culture while maintaining workforce trust.

Securing Operational Technology in an IoT-Connected World: Cybersecurity Risks, Best Practices, and Strategic Guidance for OT Systems, OT and IoT systems, once isolated, now face expanding cybersecurity risks due to IT integration, legacy vulnerabilities, and weak device security, requiring a layered defense strategy to safeguard critical infrastructure and operational continuity.

Transforming Schematics Into Intelligence: Artificial Intelligence (AI) Pipelines for Power System Modeling describes how EPRI is using computer vision and knowledge-graph techniques to automatically convert traditionally static, non-searchable single-line diagrams into structured digital models, enabling utilities to overcome a major barrier to automation and support advanced applications such as network validation, asset analytics, and digital-engineering workflows.

2026 Plan

Emerging Issues in Cyber Security for Transmission and Distribution (T&D) highlights emerging issues in the T&D space.

Emerging Issues in Cyber Security for DER and Grid Edge Systems highlights emerging issues in the DER and Grid-edge space.

Emerging Issues in Incident and Threat Management (IMTM) highlights emerging issues in the IMTM space.

Emerging Issues in Cyber Security for Data Analytics highlights emerging issues in the data analytics space.

Emerging Issues in Cyber Security for Artificial Intelligence highlights emerging issues in AI.

© 2026 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ENERGY are registered service marks of the Electric Power Research Institute, Inc. 800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

P183 B

Incident and Threat Management (183B)

Technical solutions and guidelines to increase the capabilities and efficiency of incident and threat management tools and processes for power delivery systems.

Chuck Moran,
Technical Leader III,
cmoran@epri.com

PROJECT

Incident Management

Threat Management

Cyber Security Forensic

2025 Accomplishments & Key Deliverables

The Integrated Security Operations Center Guidebook: 2025
Provides comprehensive guidance for utilities on designing and operating an Integrated Security Operations Center (ISOC) which unifies IT, OT, and physical security monitoring and response, incorporating best practices and lessons learned from more than a decade of EPRI research and utility implementations.

Threat Management Guidebook: 2025 Update
Electric power utilities need a coordinated, system-wide Threat Management Program that integrates OT security events across the full kill chain, and this guidebook provides comprehensive strategies based on a decade of EPRI research for designing, implementing, and operating such programs to better protect critical infrastructure from cyberattacks.

OT Network Visibility Guidebook 2025 Update
EPRI assessed the deployment of OT Network Visibility tools (IDS/IPS) at substations, evaluating configuration, placement, and gaps. This research supports CIP-005-5, CIP-007-6, and forward-looking CIP-015-01 INSM conformance through technical design, testbed development, and lab testing.

Substation Logging for Cybersecurity: EPRI P183B / P183C
Electric utility OT systems face advanced cyber threats to substation protection and control equipment, and this report presents a comprehensive RTAC-based logging and detection architecture that maps relay- and device-level events to MITRE ATT&CK for ICS, enabling actionable SIEM-integrated monitoring that closes key visibility gaps and strengthens CIP conformance and resilience against sophisticated adversaries.

Forensics Guidebook: 2025 Edition
This research outlines methods for quickly and accurately collecting and analyzing forensic data from ICS devices in OT environments to support incident response, offering step-by-step guidance, attack-vector insights, and field procedures that help utilities enhance investigations and understand the scope of potential compromises.

2026 Plan

The Integrated Security Operations Center (ISOC) Guidebook (2026 Update)
Planned annual update incorporating evolving best practices in unified IT/OT/physical security monitoring and new technology integrations.

Threat Management Guidebook (2026 Update)
Planned update to address AI-enabled adversary techniques, living-off-the-land tactics, and emerging nation-state campaigns targeting energy delivery. Reflects current threat intelligence, detection strategies, and OT-specific response considerations.

OT Network Visibility (2026 Research)
Continue evaluation of emerging monitoring technologies providing both network traffic analysis and OT process context, moving beyond traditional IDS/IPS toward converged cybersecurity and operational awareness.

Substation Logging for Cybersecurity (2026 Update)
Expansion of component-specific analysis and MITRE ATT&CK for ICS mapping to additional substation equipment types based on member feedback, supporting CIP-015-01 INSM conformance.

AI, Advanced Analytics, and Security Orchestration for OT
Laboratory validation of AI-driven detection capabilities, natural language security data querying, automated threat intelligence operationalization, and OT-tailored SOAR workflows. Emphasis on practical, deployable options for resource-constrained, air-gapped utility environments.

Forensics Field Guide (2026 Update)
Expanded device coverage and planned development of the Forensics Toolkit Framework (Beta) for integrated forensic readiness, automated evidence preservation, and standardized artifact collection.

© 2026 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ENERGY are registered service marks of the Electric Power Research Institute, Inc. 800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

P183 C

Cyber Security for Transmission and Distribution (183C)

Technical solutions and guidelines to improve the security posture of transmission and distribution systems.

John Stewart,
Principal Technical Leader,
jstewart@epri.com

PROJECT

Cyber Security for Substations and Field Devices

Cyber Security for Control Centers

2025 Accomplishments & Key Deliverables

Multi-Vendor IED Management Challenges: Protocol Adapters and Unified Management Architecture proposes a vendor-agnostic architectural approach — adapted from the Home Assistant IoT model — to help utilities integrate and manage diverse IED populations by separating protocol handling from application logic, enabling standardized management across key use cases and improving interoperability, scalability, and modernization of substation automation systems.

Substation Security Guidebook: 2025 Revision
This updated edition of the guidebook has been reorganized into a more modular format, making it easier for utilities with limited security resources or less mature security programs to apply substation security controls and processes. Beyond structural improvements, the revision adds practical guidance in two key areas: navigating the transition from legacy substation architectures to modern digital protocols and communication systems, and implementing zero trust security strategies adapted for OT environments. These architectural patterns are designed to balance cyber risk mitigation with operational priorities—identifying approaches that benefit both security and operations teams.

Leveraging Grid Design Documentation for Security Modeling
This research provides utilities with a framework and maturity model for developing digital twins that enhance preparedness for cyber attacks, disasters, and equipment failures, offering both leadership-level justification and technical implementation guidance validated through real-world demonstrations of improved security and risk reduction.

2026 Plan

Security at the Intersection of Control Systems and Communication Networks.
This white paper is intended to provide an overview of evolving control system applications and the resulting impacts to utility communication networks. Security strategies will be assessed to help balance cyber risk with operational benefits.

Substation Security Guidebook 2026 Revision is an updated version of the substation security guidebook that incorporates multiple years of transmission and distribution security project findings across multiple areas including secure management, remote access, and security integration.

Developing Long-Term Security Strategies for Digital Substations helps utility cybersecurity teams plan long-term security strategies for digital substations by mapping IEC 61850 adoption stages, emerging architectures, and communications choices to evolving attack surfaces, while drawing lessons from other safety-critical industries to anticipate future software-defined, virtualized protection systems.

Applying a Conceptual Framework for Grid Security
This technical report will explore potential approaches to evaluating risk from a grid reliability and resilience perspective by incorporating dependencies across major grid subsystems including power assets, control systems, and communication networks.

The AI Arms Race for T&D Security
This white paper explores how AI is reshaping T&D security by accelerating both adversarial attacks and utility defenses, identifying emerging AI-driven attack surfaces, and outlining collaborative research and actionable strategies to help utilities deploy AI-enabled security faster than threat actors.

© 2026 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ENERGY are registered service marks of the Electric Power Research Institute, Inc. 800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

P183 D

Cyber Security for DER and Grid-Edge Systems (183D)

Security requirements, solutions, and reference architectures for the deployment and integration of distributed generation and Grid-Edge technologies.

Xavier Francia,
Sr. Principal Technical Leader,
xfrancia@epri.com

PROJECT

Cyber Security for DER Integration and Management (CSDIM)

Xavier Francia
xfrancia@epri.com

2025 Accomplishments & Key Deliverables

[Cyber Security for DER Integration — Guidebook for Utility Cyber Security Architects and Engineers: 5th Edition (2025)] provides utility stakeholders with comprehensive guidance for securing distributed energy resource integration by outlining DER fundamentals, key standards, threat scenarios, reference architectures, and practical engineering approaches for protecting DER communications and technologies at grid scale.

[Cyber Security Guide for DER Technical Interconnection and Interoperability Requirements (TIIR) 1st Edition]

This report provides utilities with a standardized set of cybersecurity interconnection and interoperability requirements for DER systems, offering guidance on applying industry frameworks, inserting security reviews into TIIR processes, using a DER cybersecurity self-assessment, and adopting consistent requirement language to align customers, developers, and utility stakeholders.

2026 Plan

Cyber Security for DER Integration: Guidebook for Utility Cyber Security Architects and Engineers, 6th Edition — Annual update of the guidebook that includes the latest development in industry standards, protocols, and state-of-the-art with respect to DER interoperability, integration, and cyber security.

The DER Cyber Security Protocol Guide, 1st Edition offers utilities comprehensive technical insights aimed at enhancing the security and understanding of communication protocols for DERs. This guide thoroughly examines key IEEE 1547 protocols, including IEEE 2030.5, MESA-DER (DNP3), and Sunsec Modbus, providing detailed assessments of their architectural frameworks and their associated cyber security challenges.

Cyber Security for DER Technologies (CSDT)

Sai Ram Ganti
sganti@epri.com

[The State of Cyber Security for Grid-Edge DER Technologies, 2nd Edition] includes updates on the latest security challenges and industry security best practices as it related to DER technologies.

This new edition of the guidebook will include:

- Discussion on applicable cyber security standards for electric vehicle supply equipment (EVSE).
- Expanded guidance on security risks and mitigation approaches for energy storage systems (ESS).
- Considerations for performing threat monitoring on DER communication networks.

The State of Cyber Security for Grid-edge DER Technologies, 3rd Edition will include updates on the latest security challenges and industry security best practices as related to DER technologies.

The white paper, Cyber Security Considerations for AMI 2.0, offers an in-depth analysis of the emerging challenges related to grid reliability and data privacy that are poised to accompany new AMI 2.0 use cases, including use of meter Wi-Fi for behind-the-meter DER management.

© 2026 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ENERGY are registered service marks of the Electric Power Research Institute, Inc. 800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

P183 E

Cyber Security Data and Analytics (183E)

Transforming grid operational data into trusted, actionable intelligence across transmission, distribution, and the grid edge.

Esther Amullen,
Technical Leader III,
eamullen@epri.com

PROJECT

Cyber Security Data Foundations and Metrics

2025 Accomplishments & Key Deliverables

Operational Technology Cybersecurity Metrics: 5th Edition continuing a decade-long body of work focused on helping the electric sector move from compliance-based reporting toward more quantitative, repeatable, and data-driven measurement. This edition reflects the continued evolution of EPRI's cybersecurity metrics framework and highlights a new era of measurement shaped by artificial intelligence, advanced analytics, and increasing IT/OT convergence. In addition to strengthening the foundation for protection, detection, response, and resilience measurement, the report also introduces emerging approaches for evaluating the performance, trustworthiness, and operational value of AI-enabled cybersecurity systems.

IT/OT Cyber Security Operations and Organization: Benchmarking Cyber Security Operations, Budgets, and Workforce . In collaboration with Program 209, the 2025 survey provides an updated view of how utilities structure, fund, and staff cybersecurity across IT and OT. With 49 responses from 40 organizations, the survey highlights trends such as increased executive-level prioritization, more centralized governance, rising cybersecurity budgets, and growing investment in OT security. These benchmarks help utilities evaluate their organizational maturity and guide future planning.

Artificial Intelligence (AI)/ Machine Learning (ML) and Advanced Analytics in Cyber Security

Operational Technology Cybersecurity Data and Analytics Guidebook: 1st Edition a practical reference designed to help utilities safely design, implement, and govern cybersecurity analytics in OT environments. The guidebook provides a structured framework for moving from raw operational telemetry to actionable security insight, covering safe data movement architectures, a five-stage OT analytics pipeline, detection development, and validation approaches tailored to industrial systems. By translating standards and best practices into implementable analytics patterns, the guidebook gives utilities a blueprint for building data-driven cybersecurity capabilities that improve visibility, support compliance, and preserve operational safety and reliability.

Artificial Intelligence (AI) and Advanced Analytics for OT Cybersecurity Operations: 2nd Edition
Examines how utilities are beginning to apply AI in practical, operationally relevant ways across OT cybersecurity. Organized around the NIST Cybersecurity Framework, the report explores how AI and advanced analytics can strengthen governance, asset visibility, access control, and anomaly detection while maintaining the transparency, human oversight, and regulatory defensibility required in critical infrastructure environments. Rather than positioning AI as a replacement for existing practices, the report frames it as an augmentation layer that can improve efficiency, enhance context, and support more adaptive cybersecurity operations when deployed responsibly.

2026 Plan

Operational Technology Cybersecurity Metrics: 6th Edition.
This edition will place particular emphasis on Zero Trust-oriented metrics, scalable KPI calculation, and methods for improving the integrity, consistency, and operational relevance of cybersecurity measurement across diverse data sources.

CyberJoule 2.0 Leverages AI to accelerate and simplify OT cybersecurity measurement by orchestrating discovery, analysis, triage, and metrics generation across diverse utility data sources.

Artificial Intelligence and Advanced Analytics for OT Cybersecurity Operations Use Cases 3rd Edition extends prior NIST-aligned work by exploring additional cybersecurity functions and use cases not covered in the second edition. The report will continue to show how AI and advanced analytics can be applied in practical, utility-relevant ways to strengthen cybersecurity operations, while emphasizing transparent, defensible, and operations-aware adoption.

AI Governance, Privacy, and Regulatory Readiness for Utilities, this new deliverable will help utilities navigate the growing governance and compliance challenges associated with adopting AI in cybersecurity and operational environments. The report will examine key issues related to AI privacy, data governance, model transparency, accountability, and emerging regulatory expectations, translating a fast-changing landscape into practical guidance for the electric sector.

© 2026 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ENERGY are registered service marks of the Electric Power Research Institute, Inc. 800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

Success Stories
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.

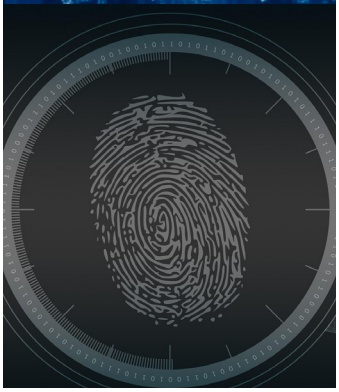
Cybersecurity Strategy Assessment and Program Alignment (CSAPA) Framework CSAPA-Report-05182025 - Tennessee Valley Autority (TVA) (2025)
Researchers evaluated cybersecurity maturity across Tennessee Valley LPCs and delivered a unified, standards-aligned framework—combining metrics, roadmaps, and templates—that 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.

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.

EPRI 2025 Technology Transfer Award Winner



Success Stories
Cyber Security for Energy Delivery & Customer Solutions

Advanced Grid Analytics and Visibility Engine - Southern Company (2024)
Southern Company, working with EPRI and partners, deployed a scalable internal network security monitoring solution that strengthened OT cybersecurity by improving traffic visibility, threat detection, and regulatory compliance while advancing industry practices.

Cybersecurity Decision Framework for Utility Scale Energy Storage Systems - Southern Company, CPS Energy, CenterPoint Energy, Southern California Edison (SCE) (2024)
As utilities rapidly deploy energy storage, EPRI's cybersecurity decision framework helps leaders like Southern Company, CPS Energy, CenterPoint, and SCE, apply NIST-based, risk-prioritized security controls across procurement, interconnection, and operations to strengthen system reliability and safety.

Operational Technology Equipment Technology Transfer Workshop - Consolidated Edison (2024)
Con Edison partnered with EPRI to create a hands-on, OT-specific cybersecurity workshop that closed training gaps, improved cross-team incident response, and strengthened alignment with industry standards.

Power Delivery Cyber Security Tailored Assessment for Utility Transmission and Distribution Operations - New York Power Authority (NYPA) (2024)
EPRI partnered with NYPA to deliver risk-based recommendations beyond compliance that strengthened OT cybersecurity practices, improved asset and patch management, enhanced training, and supported NYPA's VISION2030 goals.

Xcel Energy Staff Benefits from Remote Cyber Security Operational Technology Equipment Familiarization Course (2023)
An EPRI OT equipment familiarization course gave Xcel Energy cybersecurity professionals a realistic, hands-on learning experience that significantly improved their understanding of grid technologies, strengthened operational skills, and built valuable industry relationships. 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, NYPA (2023)
An open-source, NYSERDA-funded automated forensics tool was developed to enable real-time artifact collection from ICS devices in OT environments, improving incident response and paving the way for future SOAR integration and automated threat detection.

Dedicated Power Delivery Cybersecurity Program (PD CSP) - Southern Company (2023)
Southern Company's updated Power Delivery Cybersecurity Program, developed with EPRI, proactively strengthens OT security, modernizes legacy systems, builds customer trust through transparency, and sets a scalable, cost-effective model adopted across the energy sector.

Cybersecurity for KEPCO's Distributed Energy Resource (DER) Integration Architectures - Korea Electric Power Company (2023)
KEPCO partnered with EPRI to apply by-design DER cybersecurity guidelines, establishing secure end-to-end grid communications and a reusable architecture that supports resilient, decentralized grid modernization.

Next Generation OT Cyber Security Visibility - Southern Company (2022)
Southern Company, with Cyber Security Research Lab (CSRL) and EPRI, developed a cost-effective, open-source packet-capture solution that enables full visibility and efficient threat detection across OT field sites while reducing bandwidth and licensing costs.

Artificial Intelligence for Cyber Security - Tokyo Electric Power (2022)
In collaboration with TEPCO, this project identified AI-based cybersecurity use cases and provided readiness, integration, and vendor-selection guidance to help utilities plan practical AI adoption for power system security.

To read more Success Stories click at this link or use the QR code

Supplemental Project Offerings
Cyber Security for Energy Delivery & Customer Solutions

Supplemental projects are member-funded, quickly initiated EPRI research efforts led by EPRI staff to address targeted needs, with shared scope, defined deliverables, and EPRI-owned results licensed for internal use by participants.

Creating Effective Analytics to Monitor Operation Technology (OT)
This project improves OT cybersecurity by using advanced analytics to distinguish normal from abnormal behavior, enabling earlier threat detection, faster response, and stronger protection of critical utility infrastructure.

Cyber Security Incident Response and Recovery Tabletop Exercise
This project delivers tailored tabletop exercises to help utilities test and improve OT incident response and recovery capabilities to meet NERC CIP requirements amid rising cyber risks.

Cyber Security Operational Technology Equipment Familiarization Course
This hands-on training equips utility OT cybersecurity professionals with practical knowledge of power delivery systems and supporting networks so they can more effectively protect grid operations.

Cyber Security Program Assessment for Utility Transmission and Distribution Operations
This offering uses NIST or DOE maturity assessments and EPRI benchmarking metrics to deliver utility-specific, actionable insights and plans for strengthening OT cybersecurity readiness and risk reduction.

Cyberjoule™ Platform Implementation for Utility Cyber Security Metrics
This supplemental project helps utilities implement effective cybersecurity metrics using EPRI expertise and the Cyberjoule™ platform to enable data-driven performance assessment, avoid common pitfalls, and clearly communicate value to stakeholders.

EPRI U - Information, Communication Technology and Cyber Security (ICCS)
This project delivers foundational ICCS training and a structured system for tracking employee development to help utilities address workforce turnover, cybersecurity demands, and digital transformation while remaining competitive.

Integrated Cyber-Physical Security for Distribution Automation
EPRI developed a prototype cyber-physical security system that integrates low-cost sensors, orchestration software, and facial recognition to help utilities detect and mitigate real-time cyber and physical threats to distribution assets.

NextWave AMI: Riding the Current, Powering the Future - Maximizing AMI Now and for the Future
As AMI systems reach end of life, utilities have a strategic opportunity to move beyond basic billing and outage functions to unlock advanced capabilities that support DER integration, grid modernization, and increased customer value.

Operational Technology Data 101: Cultivating Data Literacy and Stewardship in Utilities
The "OT Data 101" project builds utility data literacy by teaching core analysis, management, and decision-making skills to turn OT data into actionable insights and strategic value.

OT Cyber Risk Assessments for Transmission and Distribution Operations
EPRI experts help utilities quantify cyber risks across operational, financial, safety, and reputational impacts to prioritize mitigations and guide informed cybersecurity investments.

Supplemental Project Offerings
Cyber Security for Energy Delivery & Customer Solutions

OT-INSIGHT (Operational Technology Intelligence-Driven Security, Investigation, and Guided Hardening Through Tactic Emulation)
OT INSIGHT provides an energy-sector framework that links threat actor behaviors to OT assets and protocols, using AI to make cybersecurity guidance more actionable and improve threat response and resilience.

Power Delivery Cyber Security Tailored Assessment for Utility Transmission and Distribution Operations
EPRI experts provide targeted assessments of utility cybersecurity programs to identify priority risks and deliver tailored improvement plans with clear goals and timelines.

Responding to High Impact Cyber Security Events (RHISE)
This project strengthens utility OT incident response by using tabletop exercises, operational playbooks, and best practices to improve recovery from high-impact ransomware and malware attacks.

Secure IED Management Strategies
This project helps utilities assess IED management challenges and develop a tailored, integrated strategy to improve OT visibility, compliance efficiency, procurement, and security controls across power delivery systems.

Utility Red Team Collaborative
This project uses collaborative red team simulations to help utilities identify vulnerabilities, strengthen response and recovery, and build cyber resilience through shared, anonymized insights and best practices.

Zero Trust for Operation Technology (OT): Balance Competing Objectives on the Road to a Zero-Trust Mindset
The ZT4OT project advances zero-trust security for operational technology by developing protocol authentication, reference architectures, and a roadmap—validated with digital twins—to reduce cyber risk while meeting NERC CIP-015 requirements.

For a more detailed listing click Cyber Security for Energy Delivery and Customer Solutions Program 183

Supplemental Project Offering Summaries.