Information, Communication and Cyber Security

Area Review 2025

JANUARY 2025

AT A GLANCE

Information and Communication Technology (ICT)

Program 161

Research Value

- **Interoperability** – Accelerate industry's migration toward interoperable protocols, standards, and architectures and challenges of proprietary solutions.
- **Data-Centricity** – Leading efforts towards enterprise-wide extensible data models to facilitate data sharing among devices, systems, and stakeholders.
- **Telecommunications** – Advancing ubiquitous, standardized resilient networks to enable secure data exchanges 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

- **Cutting Edge Updates on Emerging Information & Communication Technologies and how they may impact utilities** – AI, Geospatial information, AR/VR, Edge Computing, IT/OT Convergence, Cloud, 5G/6G, Emerging Standards and Protocols.
- **Annual Reference Guidebooks** – Providing tools, strategies and references related DER Protocols, Enterprise Architecture, Advanced Metering, Telecommunications, Data Management, and Geospatial Informatics
- **Thought Leadership Insights** – Strategies, Roadmap tools, Business Capability Models, Impacts of Disruptive Technology
- **Case Studies** – Learning from Actual Deployments

This program involves several strategies to address technical and economic challenges of identifying, evaluating, and implementing enabling Information and Communication Technologies (ICT) for grid modernization and digital transformation efforts, including:

- Tools and resources to enable adoption of emerging ICT including the development of strategies to prioritize IT/OT Investments.
- Insights on Emerging and potentially disruptive technologies
- Technology and standards evaluation, laboratory testing, and field demonstrations that interpret results into opportunities and challenges to achieve interoperable, scalable, cost-effective solutions and maximizing the sharing.
- Industry case studies, best practices, and guidebook development to help utilities plan for, design, deploy, and maintain new technologies or applications.
- 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.

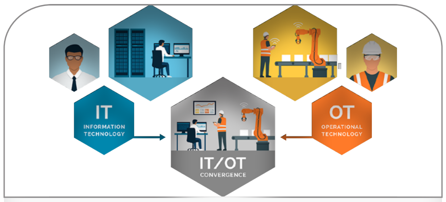
Research Highlights

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 Communication and Data Integration (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.
- 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)

- Increases the maturity, influence, and impact of EA practitioners at utilities.
- Pursues semantics of data and of available standards-based data exchange standards as a key to enable innovative applications.
- Provides Architects and strategic planners with frameworks, tools, and processes to align current and future strategic objectives.

Advanced Metering Systems and SCADA (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.

Telecommunications (161G)

- Identify and mitigate interference to 6-GHz systems.
- Identify, analyze, 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.

EPRI Technical Contact

SEAN CRIMMINS, *Program Manager*
865.227.1991, scrimmins@epri.com

For more information, contact:

EPRI Customer Assistance Center
800.313.3774 • askepri@epri.com

3002031018 September 2024

EPRI

3420 Hillview Avenue, Palo Alto, California 94304-1338 USA • 650.855.2121 • www.epri.com

P161 A

Emerging Technologies and Technology Transfer (161 A)

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	**2024** Accomplishments & Key Deliverables	**2025** Plan
Smart Grid Standards Tracking and Emerging Information and Communications Technology	**The Summary of Interoperability Tracking and Reporting by the ICT Program in 2024** is a compiled list of "3rd Thursday" webcasts that included these topics: • January – Coming Soon to a Customer Near You: Overview of the Mandates for ICT Standards and What to Expect • February – Enterprise Architecture and Integration - Data Management for the Utility of the Future • March – Continuous Meter Replacement in Heterogenous AMI Systems • April – Telecommunications – Evolution of Utility Private LTE Towards 5G - Roadmap, Benefits, and Pre-Requisites • May – Telecommunications Management with GIS and Extended Reality (XR) Updates • June – ICT Program Mid-Year Update – 2025 Annual Research Portfolio Overview • July – DER Impact on Telecommunications Systems • August – Assessing Enterprise Architecture Maturity • September – SCADA Protocols – DNP3 Tutorial • October – Telecommunications Management with GIS and Extended Reality (XR) Updates • November – Geospatial Informatics • December – P161 End of Year Review	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 .
White Papers on Emerging Information and Communication Technology	**White Papers:** 1. A DER Dilemma: Achieving Coexistence of Interoperability and Cyber Security 2. Application Portfolio Management with Business Capabilities 3. Elevating Geospatial Insights: A Case Study on the Strategic Implementation of 3D Geospatial Design 4. Empowering Tomorrow's Grid: The Vital Role of Telecommunications in Enabling Decarbonization, Electrification, and Resilience 5. Meter Socket Adapters for DER Devices 6. Power System Telecommunications Reliability – An Analytical Deconstruction 7. The Future of XR in the Electric Power Industry	White paper deliverables will be produced within individual project sets for 2025.
Technology Transfer for the ICT Program	The value of the ICT Program's research is realized when the intended audience uses the findings, with recorded webcasts offering insights and guidance, and annual reviews evaluating delivered results and future research. **2025 Area Review: Information, Communication and Cyber Security.**	Annual Reviews deliverables have been incorporated into the Smart Grid Standards Tracking and Emerging Information and Communications Technology Project Set for 2025.

Success Stories

Emerging Information, Communication Technology (ICT) and Technology Transfer - PECO, an Exelon Company (2023)

The role of the Emerging Technologies and Technology Transfer (161A) Project Set is to provide insights into ICT standards, issues and learnings from peer utilities across a broad range of interoperability, data-centricity and telecommunications topics for an advanced electric grid infrastructure.

"The information sharing and networking with EPRI and my peer utilities on a variety of Information and Communication Technology (ICT) topics keeps me informed of the EPRI research and abreast of emerging trends." *Glenn Pritchard, Senior Manager,Advanced Grid Operations & Technology, PECO.*

"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 161A 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.*

"3rd Thursday" Emerging Technology Webcasts - ConEdison (2022)

In 2022, the ICT Program started the Emerging Technologies, Interoperability & Technology "Third Thursday" of the month webcast series to provide a more regular and member driven technology transfer of the entire program. The webcasts provide insights from all 6 projects sets twice per year and the topic for each month is selected by webcast participants.

"With all the industry priorities and needs, the ICT program is doing a great job to emphasize the strategic importance of data-centricity, telecommunications and interoperability. I really like the "3rd Thursday of the Month" webcasts that provide bite-size research updates on emerging information and communication technologies. This combined with the advisory and task force meetings provide good opportunities to learn and where to go to get additional EPRI support to get value from our EPRI investment." *Steve Go, ConEdison.*

List of Supplementals

These are standalone supplemental project opportunities that are not linked to this project set.

- EPRI U - Information, Communication Technology and Cyber Security (ICCS)
- FLEXIT: Flexible Interoperable Technologies Initiative: VPP/DER Registry and Integration Interface
- Utility Digital Worker Collaborative

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

P161 D

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

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

DER Standards – Interoperability, Information, Protocol, and Connectivity Standards

Emerging Topics, Technologies, and Techniques

Integration Experiences and Practices

2024 Accomplishments & Key Deliverables

The EPRI Protocol Reference Guidebook – 8th Edition provides stakeholders with detailed briefs on various application-layer protocols used in distributed energy resources and demand response technologies, offering insights into their maturity, applicability, and updates, with contributions from industry leaders like AEP, Duke Energy, and SRP.

IoT Technologies for DER Guidebook – 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. The paper also defines the relationship between IoT protocols and existing DERs protocols assessed in the DER Protocol Reference Guidebook as well as deeper dives on protocols like Amazon Sidewalk and LoRaWAN for DERs.

2024 Emerging Technology Studies & Task Force Meetings – In 2024 EPRI investigated four emerging technologies and conducted 10+ task force meetings for member discussion. Example topics included:

+ Understanding the Difference in DER Gateways and Plant Controllers: Key differences between these platforms & why you should care.

+ Integrating DERs via Utility AMI: Three Required Integrations for Success & Common Challenges Experienced by Utilities.

+ A DER Dilemma: Achieving Coexistence of Interoperability and Cyber Security.

+ How to Integrate Vehicle-to-Grid EVs: Navigating the standards and conformance landscape for V2G EVs.

DER Interoperability Guidebook 2024 is based on over a decade of standards development, includes updated sections on industry requirements, validation tools, communication architectures, cloud support, third-party integration, telecom choices, common failures, IEEE 1547-2018 application, DER gateways, profiles, and the value of information models. Newest edition in 2024 includes Protocols to Support ADMS-DERMS & Utility-Aggregator.

2025 Plan

EPRI Protocol Reference Guidebook 9th Edition – This guidebook 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. The 2025 update will reflect the latest changes in the rapidly changing standards landscape.

2025 Emerging Technology Studies & Task Force Meetings – EPRI will work with members to establish a pipeline of emerging technologies in the data and connectivity domain. These technologies will be characterized by technology readiness for the DER domain. Each year, EPRI will select 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. This 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 – EPRI collaborates with member utilities to document experiences and use cases in DER integration and will host task force meetings to discuss ongoing research and utility efforts in the industry. Findings will be incorporated into respective guidebooks.

Success Stories

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 allows an understanding of advanced smart-inverter functions, as defined in California's Rule 21 tariff and communication systems to manage them. The following two methods assessed the smart inverter behavior using laboratory and field tests: (1) successful side-by-side operation of smart inverters; and (2) using residential smart loads to enable more solar PV on the grid. Specific test procedures for smart inverters and smart loads, and distributed energy resource (DER) management algorithms and communications architecture were developed and applied for smart loads and inverters to enable higher penetration of solar energy. The smart inverter functions, together with smart (PV-optimized) use of their loads, have shown that more solar PV capacity, and more PV total production in the distribution grid can be achieved by application of the project results.

The laboratory testing and research applications by the two largest California utilities, Pacific Gas & Electric Company (PG&E) and Southern California Edison (SCE) allowed power quality functions (e.g., voltage, frequency), solar variability and consumer activity to be varied in a controlled fashion, thereby evaluating the full range of conditions. Field testing brought-in real-world conditions that might be overlooked in the laboratory, including power quality changes and other factors induced by load-changes. Another key aspect of the testing was the communication and controls architecture that reflected the real-world conditions and leveraged the interoperability standards-based approaches such as CTA-2045.

List of Supplementals

- Assessment of the Matter Protocol for Utility Applications
- Evaluation and Economic Feasibility Analysis of Commercial DER Gateways

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

P161 E

Enterprise Architecture and Integration (161 E)

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

Sean Crimmins,
Principal Program Manager,
scrimmins@epri.com

PROJECT	**2024** Accomplishments & Key Deliverables	**2025** Plan
Enterprise Architecture (EA)	**Utility Enterprise Architecture Guidebook, 9th Edition,** incorporates leading research from the EA discipline and best practices and lessons learned from utilities to expand the effectiveness, scope, and influence of EA teams and those who share their objectives. **Top Ten Indicators of EA Maturity: 2023 Survey Results** is a yearly survey on the state of the EA discipline in the utility industry. **LEAPWorx 6th Edition** Reference architectures, metamodels, and other modeling accelerators.	*Utility Enterprise Architecture Guidebook, 9th Edition* is incorporating leading research and best practices to enhance the impact and scope of EA teams in utilities. *Top Ten Indicators of EA Maturity: 2024 Survey Results* is a yearly survey on the state of the EA discipline in the utility industry. *LEAPWorx 5th Edition* is a reference for architectures, metamodels, and other modeling accelerators.
Enterprise Systems Integration	**Cloud Integration Guidebook: A Guide for Enterprise Architects, 8th Edition** covers the basics of cloud archetypes, portfolio management evaluation criteria, capital expenditures/operating expenses (CAPEX/OPEX) considerations, and integration patterns/models. **Common Information Model (CIM) Primer, 10th Edition** is a reference for the IEC common information model, the associated data exchange standards, extending the model and building services as well as using the CIM and an Enterprise Information Model for semantic understanding.	*Cloud Integration Guidebook: A Guide for Enterprise Architects, 9th Edition*, for enterprise architects on securely connecting to cloud services, managing CAPEX/OPEX, and integrating IT/OT systems in the cloud. *Common Information Model (CIM) Primer, 11th Edition* is a reference guide for the IEC Model (CIM) model and data exchange standards. *Grid Model Data Management Functional Architecture 2nd Edition* outlines a reference framework for grid model data, emphasizing CIM-based tool interoperability and detailing DERMS/DMS and AMI integration for DER management.
Organizational Alignment	**Digital Transformation: Aligning Information Technology and Operations Technology, 7th Edition** aims to clarify IT-OT concepts, offer context on convergence challenges, define convergence levels, share strategies to bridge cultural gaps, present research, guide capability selection, and highlight future research areas. **Architectural Impacts of Disruptive Technologies, 5th Edition** defines a process for selecting and assessing the potential impact of new technology to a utility.	*Utility Business Capability Model* contains extensions and refinements to the model learned through its application across EPRI and utility projects. *IT-OT Convergence, 8th Edition* explores the drivers, the benefits, types and approaches for the convergence of information technology and operations technology.
Data Management	This project is new for 2025	*Data Management (DM) Maturity Model 2nd Edition* specifies maturity levels of the components of Enterprise Information Management capability. *DM Guidebook 1.0* helps utilities optimize data management by aligning strategy with capability. *Grid Model Data Management (GMDM) Guidebook 1.0* offers a structured framework and best practices for efficient grid model data management in T&D utilities.
Technology Innovations 2024	**Data Management Maturity Model** introduces a data management maturity model developed using the EPRI common maturity model framework.	

Success Stories

Enterprise Architecture, Alliant Energy (2024)
Alliant Energy used EPRI's Capability model to map business capabilities to software applications across all portfolios. The software applications were then placed under the Gartner T-I-M-E model to understand what applications needed to migrate or eliminated. The EPRI capability model provided the view of multiplication software applications used at Alliant Energy for one business capability which created technical debt. Alliant Energy is meeting with their business stakeholders to create a plan on migrating and eliminating the software applications. Eliminating or migrating these applications will reduce technical debt and reduces O&M cost by more than a million dollar.

Enterprise Architecture Maturity Assessment, Salt River Project (SRP) (2024)
The research developed a maturity model that not only assessed SRP's current maturity level but also provides a framework for ongoing evaluation and improvement. It identified key actions to enhance maturity, supporting SRP's efforts as IT and OT converge and digital transformation progresses, with Enterprise Architecture playing a crucial role in driving the energy transformation.

Grid Model Data Management, American Electric Power (AEP) (2024)
Distribution Grid Model Management (GMDM) is increasingly critical for the energy transition to plan and operate a grid with Distributed Energy Resources and for Advanced Distribution Management services like volt/var optimization (VVO), fault location isolation and repair (FLISR) and Distribution Automation (DA). GMDM is especially problematic in the Distribution domain because of the variety of applications, their roles, the complexity of data and the lack of standardization. Getting distribution grid model management in order is essential to further integrate T&D modeling and planning. Centralizing grid model management will reduce the data processing workload for power system engineers, increase model quality and synchronization and enable advanced distribution management services. It will also enable much more automated analysis of the distribution system, allowing for faster response times and higher fidelity and confidence in results when customer interconnection requests are received.

List of Supplementals

- Applied Grid Model Data Management (GMDM) for Distribution
- Applied Grid Model Data Management (GMDM) for Transmission
- Business Capability-Based Investment Optimization (BCM Phase II)
- Data Management Collaborative: Surviving the Data Avalanche
- Enterprise Architecture Maturity Assessment
- Grid Model Data Management (GMDM) Vendor Forum Phase II: An EPRI-Sponsored Vendor-Funded Collaborative Initiative
- Grid Model Manager (GMM) for Distribution Interest Group

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

P161 F

Advanced Metering Systems and SCADA (161 F)

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

Ed Beroset,
Sr. Principal Technical Leader,
eberoset@epri.com

PROJECT	**2024** Accomplishments & Key Deliverables	**2025** Plan
Achieving Open, Interoperable Advanced Metering Systems	**Device Language Message Specification and Companion Specification for Energy Metering for North American Utilities** describes the DLMS/COSEM (IEC 62056) standard that defines a communication protocol for metering systems, enabling interoperability between devices for data exchange. It outlines how data is collected, stored, and transmitted between meters and external systems. The standard supports various metering applications, including electricity, gas, water, and heat meters, and ensures secure, reliable communication for utility management.	*ANSI Meter Standards Utilization, 2nd Edition* describes the current state of the utilization of the American National Standards Institute (ANSI) standards in advanced metering systems available today and recent changes to the ANSI metering standards.
Advanced Metering Systems Operations and Management	**Advancements and Applications of Direct Current Metering in Modern Energy Systems** survey explores the progress in development and use cases involving DC metering equipment, highlighting its growing necessity for modern energy systems.	*Head-end System Overview: Functions and Interfaces* describes the functions and interfaces of modern Head-End Systems (HES) and analyzes some of the implications of these functions.
Optimizing Advanced Metering System Value and Utilization	**Continuous Meter Replacement in Heterogenous Systems** describes the future of metering that involves meters integrated into diverse systems, allowing for replacements without overhauling the entire infrastructure.	*Advanced Metering Data Analytics Guidebook, 3rd Edition* updates the 2023 version to include the latest developments, including the use of machine learning in metering data analytics.
SCADA Protocols	This project is new for 2025	*DNP Tutorial* is a short, modern tutorial that describes the operation and features of the DNP protocol.

Success Stories

Next Generation Metering Requirements - Exelon Family of Companies (PECO Energy Company (PECO) and Commonwealth Edison (ComEd) (2023)

This work is a great example of how EPRI and Exelon can collaborate to investigate new opportunities for AMI and Smart Meters to advance the functionality of the distribution grid and continue to meet customer expectations of high quality reliable electric service.

The project team leveraged EPRI knowledge as a catalyst to improve the flexibility of the metering system, utilize alarms better, voltage and other data more effectively. Exelon has a dynamic environment with competing priorities and incentives, and the EPRI project provided clarity in pursuing these initiatives.

Remote Operation of AMI meter disconnect in Natural Gas environment - Consolidated Edison Company (ConEd) (2023)

The use and usefulness of having remote electric service connect/disconnect switches integrated into electric meters has been well established. One new potential use case is to employ the electric service disconnect in meters when the operator receives notification of a natural gas leak from gas inside a building. By disconnecting the electric service, the potential for equipment to cause a spark is eliminated, but the question is what effect the disconnect itself might have in this situation. This research addressed that question.

List of Supplementals

- Assessment of DER-Ready Meter Forms
- Next Generation Metering – Distributed Intelligence

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

P161 G

Telecommunications (161 G)

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	**2024** Accomplishments & Key Deliverables	**2025** Plan
Wide Area Networks	**Strategic Fiber Guidebook 2024 - Annual update** focuses on electric utility specific fiber optic networks. **Wide Area Network (WAN) Modernization Guidebook 2024** focuses on why WANs are needed by utilities, and the rationale behind the evolution of the underlying technologies. **6 GHz AFC Protection: Field Test Results** is an analysis and field testing of interference to 6-GHz microwave links from increasing consumer adoption of unlicensed devices, including impacts of the new Wi-Fi 7 standard.	*Evaluation of Interference to 6- GHz Microwave* is an analysis and field testing of interference to 6-GHz microwave links from increasing consumer adoption of unlicensed devices, including very-low-power (VLP) devices and increased adoption of Wi-Fi 7. *WAN Modernization Guidebook 2025 Edition* —Annual Guidebook Update *Strategic Fiber Guidebook 2025 Edition* —Annual Guidebook Update.
Field / Neighborhood Area Networks	**Private LTE Guidebook – 2024 Edition** provides an overview of the technology and architecture and identifies current and potential spectrum options for private LTE network deployment. **Low-Latency and Performance Assessment of 5G for Utility Use Cases** is an ongoing evaluation of the development of wireless technologies leading up the availability of 5G Ultra-Reliable Low-Latency Communication (URLLC).	*Private LTE Guidebook – 2025 Edition* provides an overview of the technology and architecture and identifies current and potential spectrum options for private LTE network deployment. *Evaluation of Low Latency Wireless Technologies* is an ongoing evaluation and assessment of the 5G predecessor technologies Ultra-Reliable Low-Latency Communication (URLLC), including lab and field testing as technologies become available.
Telecommunications Planning & Management	**Network Management Systems, Annual Update** introduces the audience to the field of telecom network management with a focus on the field's evolution and relevance for the utility industry. **Integrating Islandable Communications Networks into Resilient Microgrids: Lab Test Results** the final phase of the Islandable Communications task in the SECURE project integrated an islandable communications network into a simulated microgrid at NREL, comparing performance between commercial cellular and Private LTE networks. This highlighted the need for further research on microgrid behavior in real-world or impaired communication environments. **Satellite and Emergency Communication 2024 Update: Additional Testing of Starlink for Utility Use Cases** Low Earth Orbit (LEO) satellite communications offer a promising solution to address communication gaps in remote areas of the electricity T&D networks, with lower latency, reduced costs, and higher throughput compared to traditional geostationary satellites..	*Network Management Systems Guidebook* Telecom network management guidebook annual update. *4G and 5G Architecture Approaches for Resilient Networks* is a Research and Technology Evaluation to Enhance Security and Resiliency of Utility Critical Infrastructure. *Satellite and Emergency Communication Phase 3 and Planning* on best practices for ensuring communications availability in emergency scenarios, assessment of new technologies for non-terrestrial networks, and longer-term test results for Low Earth Orbit satellite systems.
Telecommunication Standards Engagement	**Smart Grid Communications Intelligencer 1H 2024 and 2H 2024** is a biannual technical newsletter that focuses on developments in communication technologies, standards, and business issues affecting utility communications infrastructure. **Telecom Standards Guidebook Vol 6** provides an overview of standards relevant to telecommunications in the electric power industry.	*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* updates to current status of new and developing standards, highlighting relevance to utility telecommunications networks and technology roadmaps.

Success Stories

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.

Low-Latency Wireless Communications - Consolidated Edison (ConEd) (2024)
Low-latency, high-reliability communications are becoming increasingly critical in electric distribution as the number of DER sites grows, creating a need for more advanced protection systems. EPRI's research has been instrumental in guiding the planning and engineering of the company's distribution grid, enabling confident design decisions that support the scalable and efficient integration of DERs. This research facilitates widespread DER adoption by providing a more robust framework for connectivity, optimizing resource allocation, and fostering innovation, ultimately contributing to a more sustainable and resilient energy ecosystem.

6GHz testing - Nebraska Public Power District (2023)
The Federal Communications Commission (FCC) issued a Report and Order (R&O) in April 2020 that allows unlicensed devices (such as Wi-Fi) to operate in 6 GHz microwave radio bands that were previously exclusively licensed. This regulatory change introduces the possibility of harmful interference to existing microwave systems, including those used by utilities for SCADA, system control, and teleprotection. These microwave systems were not designed to deal with interference from unlicensed devices.
"Our big takeaway from the EPRI 6GHz testing is the interference testing and the results we have access to. We are also engaged with EPRI testing in private Long-Term Evolution (LTE) space in case we need to go down that road for leased Remote Terminal Units (RTUs). Future plans include having the Telecommunications Operations Center (TOC) evaluate the EPRI Network Monitoring Guidebook to determine value and implement on our network if appropriate." *Matt Holthe, Telecommunications Manager.*

List of Supplementals

- Enhanced Surveillance Over Wireless
- Nationwide Resilient Communications System (NRCS): Phase 1: Requirements Definition and Design Specification
- Next Generation Wireless Local Area Network (WLAN)
- Renewables Communications: Use Cases, Communications Technologies, and Implementation Considerations

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

P161 H

Geospatial Intelligence (161 H)

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	**2024** Accomplishments & Key Deliverables	**2025** Plan
Geospatial Informatics Data Practices	**Geospatial Informatics Guidebook: Fifth Edition** aims to prepare electric utility GIS professionals to deliver improved geodata services to an expanding spectrum of utility individuals and systems. The project is also intended to help GIS professionals understand how trends in the geospatial industry are affecting their management of geospatial information and investments. **Geospatial Guidebook: User Training Video** provides a high-level overview of the Geospatial Informatics Guidebook: 4th Edition.	*Geospatial Informatics Guidebook: Sixth Edition* is an annual update of a digital reference for best practices in geospatial data management.
Geospatial Informatics Innovation Engine	**Geospatial Innovations** provides exposure to a few of the latest technologies that have potential for a positive impact for the electric utility industry. The first chapter researches the benefits of combining Artificial Intelligence techniques with geospatial intelligence. There is much attention paid to Artificial Intelligence due to its high potential for the industry. The second chapter focus is on dynamic and streaming data within GIS. GIS was not originally designed for handling streaming data and the paper discusses a few of the leading technology solutions today. The third article discusses leading technologies for locating underground utility structures and the final chapter is a report on the 2024 ESRI Infrastructure Management and GIS conference.	*Geospatial Innovations* - Leading practices for leveraging GIS technologies within electric utilities.
Geospatial Informatics Analytics and Visualization	**EPRI Geospatial Intelligence Develops Innovation Lab – The Path Forward.** Utility GIS organizations serve as the foundation of modern utility operations, supporting key functions like outage management, distribution management, inspection and maintenance planning, construction design, and customer communications. However, their full potential remains untapped, as GIS is primarily used as a repository for asset location and connectivity data. This research aims to push the boundaries of utility GIS by incorporating geospatial intelligence (GEOINT) to better support field and control room operations.	*Geospatial Analytics Use Cases* - Presentation Update to the 2023 pilot demonstration that will be extending geo-analytics into new use case areas. Delivered via interactive Web-based format (Story Maps).

Success Stories

GIS Standards and Centralized Database - Los Angeles Department of Water and Power (LADWP) (2024)

The LADWP Environmental Affairs team manages environmental compliance over a five-state region. It is a daunting task ensuring compliance requirements from multiple jurisdictions as well as managing vendor workload. Geographic data is a critical resource for this use case. EPRI developed GIS standards for optimizing their process and developed a centralized GIS system to provide visibility into potential environmental impacts on utility projects. The GIS is synchronized with their internal Environmental review application and is shared with multiple departments at LADWP.

Data Quality Project Case Study - Salt River Project (2023)
Salt River Project GIS Data Improvement for ADMS. At Salt River Project ADMS guides the implementation of GIS data improvement effort development. The group was formed from across distribution to develop a framework that merged two existing GIS Databases. Data errors were identified and prioritized, and the lessons learned will be incorporated into next steps that are summarized in a case study.

List of Supplementals

- Evaluation of Automated GIS Data Cleanup Methods
- Field Asset Unique Identification System

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

EPRI

AT A GLANCE

Cyber Security for Energy Delivery and Customer Solutions (ED&CS)

Program 183

Research Value

- **Enhanced Resilience Against Cyber Threats** – Develop and implements strategies for advanced cyber security measures.
- **Multidisciplinary Approach to Emerging Challenges** – Address the rapidly evolving cyber security threats to interconnected electric sectors with collaborative and multidisciplinary research.
- **Expert Insight and Analysis** – Leverage 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.

The Cyber Security for Energy Delivery and Customer Solutions program is a comprehensive initiative designed to fortify the electric grid against cyber threats.

Focusing on electric utilities, the program incorporates multidisciplinary research and expert collaboration to develop and implement advanced cyber security measures.

Members benefit from access to pioneering research, expert guidance, collaborative networks, and tailored strategies to address evolving cyber threats, ensuring the reliability and security of their infrastructure against a backdrop of rapid technological change.

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.

Research Highlights

Strategic Intelligence and Emerging Issues (183A)

- **Guidance on Emerging Threats and Vulnerabilities:** Provides up-to-date intelligence and recommendations on newly emerging cyber security vulnerabilities, threats, and issues.
- **Dynamic Program Monitoring and Evolution:** Offers guidance for OT cybersecurity programs, alongside developing strategic roadmaps for adapting to emerging threats and technological advancements.

Incident and Threat Management (183B)

- **Comprehensive Incident and Threat Management:** Develops systems for monitoring, detection, and response to cyber security events, alongside procedures for managing and responding to threats.
- **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)

- **Robust Cyber Security for DER Integration:** Develops comprehensive cyber security strategies, including risk narratives, frameworks, and engineering guidelines, to secure grid systems with distributed energy resources.
- **Practical Tools and Collaborative Efforts**: Creates practical engineering tools, reference architectures, and conducts field demonstrations, for resilient integration.

Cyber Security Data Applications (183E)

- **Innovative Data Management and Analytics:** Develops advanced data management strategies and integrates machine learning for proactive cyber threat identification and mitigation.
- **Collaborative Cyber Security Advancements:** Focuses on collaborative efforts and continuous improvement in cyber security data applications, promoting industry-wide knowledge sharing.

EPRI Technical Contact
BEN SOOTER,
Program Manager
865.218.8108,
bsooter@epri.com

For more information, contact:

EPRI Customer Assistance Center 800.313.3774 • askepri@epri.com

Product ID 3002031015

January 2025

EPRI

3420 Hillview Avenue, Palo Alto, California 94304-1338 USA • 650.855.2121 • www.epri.com

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.

Ben Sooter,
Program Manager,
bsooter@epri.com

PROJECT

Strategic Intelligence and Emerging Issues

2024 Accomplishments & Key Deliverables

Ransomware as a Service (RaaS): The Rise of AI-assisted Threats and AI-assisted Mitigation. The integration of AI into Ransomware as a Service (RaaS) has intensified attacks through automation, AI-driven phishing, advanced malware, and deepfakes, requiring organizations to adopt comprehensive security measures.

Building an OT Cyber Lab: 2024 Edition provides lessons learned on building an OT (Operational Technology) Cyber Security Lab.

Leveraging Open Source Software in Cyber Security for Operational Technology (OT) aims to help IT professionals and cybersecurity experts integrate OSS while addressing associated risks and best practices.

Emerging Issues in Cyber Security for Data Analytics provides an overview of several critical resources developed to enhance cybersecurity for operational technology (OT) in electric utilities. As digital threats to OT systems grow, these deliverables offer practical tools and insights to improve data management, resilience, and readiness through advanced analytics.

2025 Plan

In 2025, our focus sharpens on pioneering cyber resilience across multiple facets of operational technology. Each initiative is designed not just to confront emerging threats but to redefine how we understand, react to, and preempt cyber challenges:

Incident and Threat Management Evolution: We'll delve into advanced methodologies and technologies that redefine incident response and threat anticipation, setting new industry benchmarks in proactive cyber defense.

Transmission & Distribution Cyber Frontiers: Explore groundbreaking cyber resilience strategies specific to the T&D sphere, enhancing our grid's ability to resist, recover, and evolve in response to digital threats.

Innovating at the Grid Edge: As DER systems become increasingly integrated, our efforts will focus on pioneering cyber strategies that ensure these complex ecosystems are not just secure, but resilient against sophisticated threats.

Data Analytics: The Next Cyber Battleground: Harnessing the power of big data, we will unveil cutting-edge analytic techniques that enhance visibility and predictive capabilities, turning data into one of our strongest allies against cyber threats.

Through these initiatives, we aim to not only protect our critical infrastructures but also to empower them to thrive in the face of cyber adversity. Emerging Issues in Incident and Threat Management. This deliverable will highlight emerging issues in the IMTM space.

Security Newsletters

Cyber Security Newsletter
The EPRI Cyber Security Program provides monthly updates to utilities on cyber security activities and events that are impacting the electric sector. The goal is to cover the activities of industry groups, government organizations, regulatory bodies, and research groups from around the world. This document provides highlights from these monthly updates.

Cyber Security Newsletter

Success Story

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

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

List of Supplementals

These are standalone supplemental project opportunities that are not linked to this project set:

- Creating Effective Analytics to Monitor Operation Technology (OT)
- Cyber Security Operational Technology Equipment Familiarization Course
- Operationalizing Software Bill of Materials (SBOMS)
- Cyber Security Incident Response and Recovery Tabletop Exercise
- Utility Red Team Collaborative
- Zero Trust For Operational Technology (ZT4OT)

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

P183 B

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

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.

PROJECT	**2024** Accomplishments & Key Deliverables	**2025** Plan
Incident Management	**The ISOC Guidebook 2024** includes work that can benefit the public by improving the overall security posture of the electric sector and reducing the possibility of a successful cyber-attack that could cause an interruption to the operation of the power grid and includes incident containment, reducing operational impact to the power system, identification and measurement of holistic impact.	Proposed research for 2025 supporting the *Integrated Security Operations Center (ISOC) Guidebook* include integration of new technologies and their valuable context data and leveraging AI/ML to increase alert fidelity and time to detection and response.
Threat Management	**Threat Management Guidebook 2024** This guidebook provides comprehensive guidance based on past EPRI research from 2017 to 2024. The guidebook will be updated annually to reflect changes in technology and best practices and to include new EPRI research related to threat management. **OT Network Visibility Guidebook 2024** evaluates the deployment of Network Visibility tools, such as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), at substations to identify configuration, usage, and gaps. The research supports compliance with Critical Infrastructure Protection (CIP) requirements, including CIP-005-5, CIP-007-6, and CIP-015-01, and includes technical design, testbed development, and testing scenarios.	*2025 Update of Threat Management Guidebook* provides comprehensive guidance based on past EPRI research from 2017 to 2025. Proposed research supporting the Threat Management Guidebook includes continued focus on detecting threats, value from new to market technologies, and best practices related to threat management in the ever changing threat landscape.
Cyber Security Forensic	**Forensics Guidebook 2024** Cyber attacks on industrial control system (ICS) devices have risen, making it critical to quickly and accurately collect forensics data from these devices for incident response. This research identifies approaches for forensic analysis on ICS devices, offers guidance on extracting key forensics indicators, and provides a step-by-step use case for field personnel to capture and preserve data, aiding cybersecurity teams in investigating and responding to attacks.	*2025 Update of the Forensics Field Guide* provides a step-by-step approach on how to collect forensics-relevant data from a relay or RTU in support of a cyber incident response investigation. Proposed research supporting the Forensic Field Guide includes continued focus on identifying valuable data for functional and cyber incidents and automation to ensure valuable data is capture to support Incident Response efforts.

Success Story

Industrial Control Systems (ICS) Automated Digital Forensics Harvester - Consumers Energy, North Carolina Electric Membership Corporation, Électricité de France, Salt River Project, Evergy, Southern Company, Exelon, Tennessee Valley Authority, KEPCO, New York Power Authority (2023)

As cyber security threats evolve, rapid and accurate forensic data collection from ICS devices in OT environments is essential for incident response. This project developed an automated forensics tool that enables real-time extraction of critical artifacts from devices, overcoming challenges with ICS devices' custom operating systems. Using an extended, supported communications protocol, the harvester tool collects and stores data in a structured format, enhancing forensics automation. Funded by NYSERDA, the tool is open-source, encouraging manufacturers to adopt it. Future extensions include integration with security orchestration, automation, and response (SOAR) tools, continuous monitoring, automated threat detection, and potentially automated threat mitigation.

List of Supplementals

- Cyber Security Incident Response and Recovery Tabletop Exercise
- Creating Effective Analytics to Monitor Operation Technology (OT)
- Utility Red Team Collaborative
- Integrated Cyber-Physical Security for Distribution Automation
- Operationalizing Software Bill of Materials (SBOMs)
- Zero-Trust for OT (ZT4OT)

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

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 Leaderr,
jstewart@epri.com

PROJECT	**2024** Accomplishments & Key Deliverables	**2025** Plan
Cyber Security for Substations and Field Devices	**Substation Security Guidebook 2024** incorporates research results and recommendations from multiple years of base-funded projects that address a range of common T&D cybersecurity challenges. The 2024 revision has been expanded and reorganized providing references for: typical control system and communications network architectures, secure remote access options, and potential approaches to modeling or simulation of complex systems. **Zero Trust Challenges for Operational Technology (OT) Systems** white paper explores the unique challenges of adopting a Zero Trust philosophy in OT environments or facilities. Much of existing zero trust guidance available was developed for typical enterprise IT applications with distinct security priorities and objectives relative to utility OT. Recommendations are provided for utilities to assist members with adapting zero trust concepts for both grid core (substations) and grid edge (DER) applications.	The 2025 update of this *Substation Security Guidebook* will incorporate emerging cybersecurity challenges associated with new technologies and standards that will impact future substation design practices. The shift from traditional architectures towards IEC-61850 designs should drive a reassessment of existing security control standards to align with the expanded attack surface. Additional information will also be included on potential security benefits that can be realized by leveraging standardized engineering or configuration data to inform intrusion detection systems. *Security at the Intersection of Control Systems and Communication Networks* is intended to provide an overview of key utility control system applications and their emerging reliance on telecommunication networks for regular operation. Future security challenges will be addressed to help align security efforts with new telecommunications technologies.
Cyber Security for Control Centers	**A Conceptual Framework for Grid Security: Modeling Power, Control, and Communication Dependencies** report presents a conceptual framework for modeling and securing transmission and distribution (T&D) systems within the electric grid. Designed to evaluate and strengthen cybersecurity strategies, the framework provides a detailed methodology for creating a control system model that incorporates critical dependencies across power assets, control systems, and communication networks. By integrating reliability and resilience perspectives, this framework allows utilities to assess the impact of alternative security approaches on grid stability and recovery.	In 2025, the conceptual framework will be expanded and developed further with the goal of creating an example model or digital twin of a single grid facility or substation from the component level up through integration of critical operational and support systems. This effort will leverage information from multiple sources including vendor documentation, device configuration files, and utility diagrams to model relationships and expected behavior.

Success Story

Operational Technology Equipment Technology Transfer Workshop - Consolidated Edison (ConEd) (2024)

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

Digital Substation Workshop (Multiple) (2024)

EPRI Cybersecurity program advisors from multiple utilities identified a common challenge associated with their ongoing transition from traditional substation design practices toward digital substations that leveraged the IEC-61850 standard. This transition involves replacement of point-to-point legacy technologies with new control systems and multiple real-time networks expanding the substation attack surface significantly in exchange for operational benefits and flexibility. To support this transition, utility cybersecurity organizations must engage with control system and communications personnel to better understand each utilities digital substation roadmap and develop new practices for securing digital substations. The Digital Substation Workshop is an annual cross-program event that brings together industry experts to explore different approaches to the transition and highlight best-practice strategies to secure the next generation of digital substations.

List of Supplementals

- Integrated Cyber-Physical Security for Distribution Automation
- OT Cyber Risk Assessments for Transmission and Distribution Operations
- Power Delivery Cyber Security Tailored Assessment for Utility Transmission and Distribution Operations
- Zero Trust for Operation Technology (ZT4OT)

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

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. Technical Leader,
xfrancia@epri.com

PROJECT

2024 Accomplishments & Key Deliverables

2025 Plan

Cyber Security for DER Integration and Management (CSDIM)

Xavier Francia
xfrancia@epri.com

Cyber Security for DER Integration: Guidebook for Utility Cyber Security Architects and Engineers, 4th Edition includes expanded engineering guidance on technical strategies that can be implemented by utilities to meet IEEE 1547's recommended set of cyber security controls. This publication also includes expanded guidance related to electric vehicle integration.

Enhancing DER Integration: Exploring the Application of Cloud-Based Secure Access Service Edge (SASE) Distributed Energy Resources (DERs) are crucial to the smart grid transformation, enabling competition and enhanced grid services, but their expansion introduces cybersecurity risks such as communication vulnerabilities, supply chain threats, and remote access exploitation. Cloud-based Secure Access Service Edge (SASE) capabilities offer a potential solution for addressing these risks by providing consistent security management and supporting scalable security approaches as DER integration grows.

Distributed Energy Resources (DER) Cyber Security Guidebook for Utility Architects and Engineers, 5th Edition is a reference document for utility cyber security architects, cyber security engineers, and other stakeholders to assist in securing integration of distributed energy resources and demand response technologies to the grid.

Cyber Security for DER Technical Interconnection and Interoperability Requirements (TIIR) is a reference document to assist utilities in identifying approaches towards including and enforcing cyber security requirements for third party DER systems. This guidance report will provide a baseline of cyber security requirements currently included in utility TIIRs and reference language utilities may consider including in their third-party aggregator and DER interconnection agreeements.

Cyber Security for DER Technologies (CSDT)

Sai Ram Ganti
sganti@epri.com

The State of Cyber Security for Grid-Edge Distributed Energy Resource (DER) Technologies, 1st Edition guidebook aims to equip readers with the knowledge necessary to navigate the complexities of DER technologies and their associated cyber security risks. This document provides a background on various DERs and their technologies like Energy Storage, EV Charging Infrastructure, Smart Inverters and PV Systems.

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.

Success Story

Cybersecurity Decision Framework for Utility Scale Energy Storage Systems - Southern Company, CPS Energy, CenterPoint Energy, Southern California Edison (SCE) (2024)

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

List of Supplementals

- Evaluation and Economic Feasibility Analysis of Commercial (DER) Gateways

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

P183 E

Cyber Security Data Applications (183E)

Improve cyber security programs through quantitative and qualitative performance assessments and specialized workforce training.

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

PROJECT	**2024** Accomplishments & Key Deliverables	**2025** Plan
Cyber Security Data Foundations/Cyber Security Data Applications	**OT Cyber Security Data Management Guide V2** underscores the importance of comprehensive data management and governance in protecting critical infrastructure. It provides actionable recommendations for utilities to adopt proactive, data-driven cybersecurity strategies, leveraging advanced analytics and machine learning to enhance situational awareness and streamline security operations. **OT Cyber Security Resiliency Metrics V3 Guide** helps utilities measure and enhance their resilience against cyberattacks by providing clear objectives and actionable metrics aligned with industry frameworks like the NIST Cybersecurity Framework. It includes research-supported use cases, real-world examples, and best practices to develop robust processes for ensuring continuity and security in a rapidly evolving threat landscape. **Machine Learning Applications for OT Cyber Security Operations V1 Guide** details how actionable metrics can enhance the operational performance of cybersecurity programs in OT environments, based on pilot tests from 2018 to 2021. It also introduces the Cyberjoule™ software application, which aids utilities in tracking and communicating cyber risks and performance to stakeholders at all maturity levels.. **Metrics 101 – A Beginners Guide to OT Cyber Security Metrics** discusses integrating machine learning into OT cybersecurity for threat detection and intelligence, covering data preprocessing, feature engineering, and ML algorithms. It emphasizes AI governance and collaboration, providing a roadmap for leveraging AI and ML to enhance OT security, while also detailing enhancements in metrics calculation, automated data collection, and customizable reporting.	The *OT Cybersecurity Data Management & Governance Guide V3* will offer updated best practices for managing OT cybersecurity data, preparing for AI-driven security solutions. It emphasizes safeguarding data integrity and ensuring compliance throughout its lifecycle, helping utilities confidently adopt advanced analytics and machine learning. *Metrics to Evaluate Advancements in Cybersecurity Operations* introduces a unified framework to assess the impact of AI-based and advanced analytics solutions on cybersecurity operations. It defines key performance indicators for AI-driven threat detection and incident response, addresses adversarial risks, and incorporates research from OT Cyber Security Resiliency Metrics V.3 and Metrics 101 to help utilities track progress effectively. *AI and Advanced Analytics Use Cases for OT Cybersecurity Operations* showcases real-world examples of machine learning and AI applications in OT environments, highlighting how productionalized AI can streamline threat detection and response. It builds on previous work to provide practitioners with clear guidance on leveraging ML capabilities while maintaining security and operational integrity. *Tooling & Support for Cybersecurity Metrics Calculation Initiative* provides ongoing support for tools like Cyberjoule™ to simplify data collection, reporting, and continuous improvement of security metrics. It combines fixed benchmarks and adaptive metrics to help utilities respond to evolving threats, along with documentation and training resources for long-term metrics management.
Cyber Security Assessments	Conduct assessments and develop anonymized benchmarking data to help utilities take corrective actions that effectively mitigate prioritized risks.	
Cyber Security Workforce Training	Develop new instructor-led and lab-based courses and Computer Based Trainings (CBTs) based on utility needs in topics such as IEC 61850 and equipment familiarization.	

Success Story

Power Delivery Cyber Security Tailored Assessment for Utility Transmission and Distribution Operations - New York Power Authority (NYPA) (2024)

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

List of Supplementals

- Cyber Security Program Assessment for Utility Transmission and Distribution Operations
- Cyberjoule™ Platform Implementation for Utility Cyber Security Metrics
- Power Delivery Cyber Security Tailored Assessment for Utility Transmission and Distribution Operations

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