Information, Communication and Cyber Security
Area Review

February 2023

What the Information, Communication and Cyber Security (ICCS) Area Does

Performs research and helps utility apply advanced solutions related to integrating Information, Communication and Cyber Security technologies to enable digital transformation, grid flexibility and decarbonization for energy delivery and customer solutions.

Information and Communication Technology Program (161)

The ICT program addresses these challenges by conducting research in six project sets that cut across multiple areas:

- Emerging Technologies and Technology Transfer (161A)
- Distributed Energy Resources (DER) Data and Connectivity (161D)
- Enterprise Architecture and Integration (161E)
- Advanced Metering Systems (161F)
- Telecommunications (161G)
- Geospatial Informatics (161H)

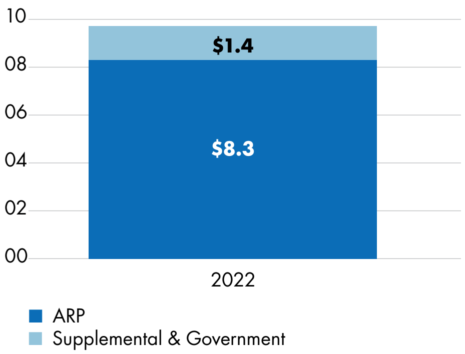
Cyber Security for Power Delivery & Utilization (183)

Focused on performing laboratory assessments of existing, relevant technologies, developing security requirements and creating new security technologies to enhance the current cyber security posture of the grid and increase the security of systems that will be deployed in the future.

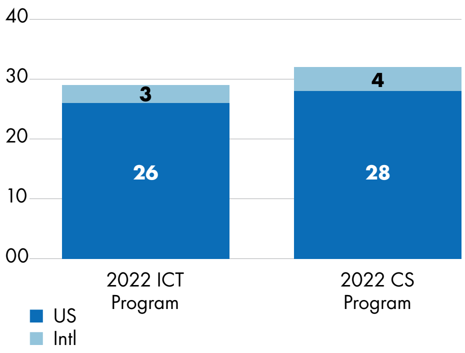
- Knowledge Applications
- Incident and Threat Management
- Cyber Security for Transmission & Distribution
- Cyber Security for DER & Grid-Edge Systems

Contents

ICT & Cyber Security Program Funding (in $ Millions)



ICT (161) and CS (183) Programs Utility Members



Staff	#
Tech	32
Admin	2
Total	**34**

Degree	#
PhD	2
Masters	12
Bachelors	19

What the Information and Communication Technology (ICT) Program Does

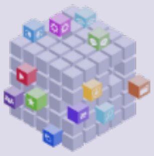
Performs research and development to support members address challenges associated with selecting and integrating communications, computing, information technologies and architectures to enable grid modernization applications, such as wide area monitoring and control, asset management, advanced metering, distribution automation, integration of distributed energy resources (DER) and demand response.

Emerging Technologies and Technology Transfer (161A)

- Provides insights into emerging information and communication technologies and issues that could impact utility investments.
- Provides frequent technology transfer activities to help utility members understand ICT resources and how to use them.

Distributed Energy Resources (DER) Data and Connectivity (161D)

- Supports members with integrating DER by developing resources to aid in the adoption of relevant standards for interoperability and interchangability of DERs.
- Maintains a pipeline of emerging and disruptive technologies to help members sort through an ever-growing set of data and connectivity technologies.
- Evaluates how ICT technologies can help fit into a bigger utility transformation required for meeting DER penetration and clean energy targets.



Enterprise Architecture and Integration (161E)

- Provides tools and techniques that will help enterprise architects better execute their work.
- Provides leading practices on cloud integration and digital transformation.

Advanced Metering Systems (161F)

- Provides information and tools for the deployment of next-generation advanced metering systems.
- Leads the industry toward interoperability between advanced metering systems.

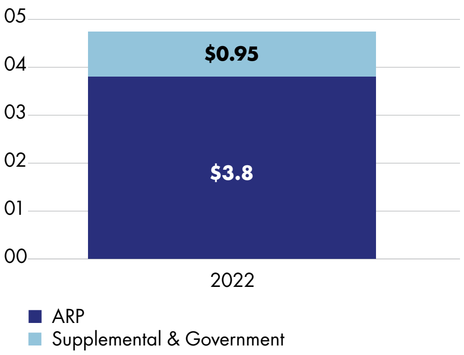
Telecommunications (161G)

- Provides insights into the technology risks and opportunities resulting from regulatory rulings.
- Provides leading practices for transitioning the wide area network to packet technologies and for developing best-in-class telecom network management, visualization, and control systems while maintaining reliability, resilience, and cyber security.

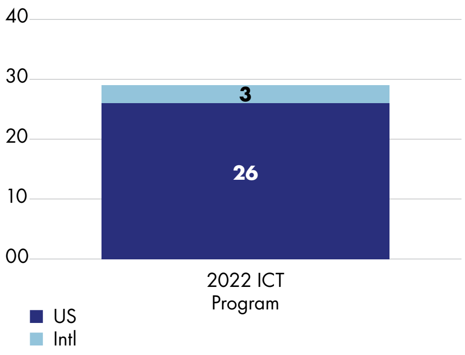
Geospatial Informatics (GIS) (161H)

- Provides leading practices for addressing GIS data quality and data management challenges.
- Enables the next-generation of GIS, including the support of immersive 3D environments and the requirements to support advanced distribution planning and modeling applications.

ICT Program Funding (in $ Millions)



Utility Members



Staff	#
Tech	17
Admin	2
Total	19

Degree	#
PhD	2
Masters	5
Bachelors	12

P161A

Matt Wakefield,
Director ICCS and
ICT Program Manager,
mwakefield@epri.com

Emerging Technologies and Technology Transfer (161A)

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

PROJECT	**2022** Accomplishments & Key Deliverables	**2023** Plan
Smart Grid Standards Tracking and Emerging Information and Communications Technology	The Summary of Interoperability Tracking and Reporting by the ICT Program in 2022 is a compiled list of "3rd Thursday" webcasts that included topics: **DER Data & Connectivity** – 1) FERC Order 2222 & Importance of ICT Standards, 2) IEEE 1547, Action Required: Reading Between the Lines **Enterprise Architecture** – 1) Control Center of the Future Reference Architecture, 2) Optimizing Grid Model Data Management **Advanced Metering** – 1) AMI System Simulation, 2) Next Generation Metering, Distributed Intelligence **Telecommunication** – 1) Value of Shared Private LTE, 2) Satellite & Emergency Communications **Geospatial Informatics** – 1) Enhancing Geospatial Data Performance, 2) GIS Analytics for Resiliency Grid modernization playbook	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:** • 6 GHz Microwave - An Executive Perspective on Managing Business Risk • Developing ICT Networks to Integrate DER Technologies • Modeling Your AMI Network: How and Why You Should • Enhancing GIS Data Quality using Artificial Intelligence Tools • Utilizing a Business Capability Model for Capability, Technology, and Data Assessments • Grid Modernization Playbook • Introduction to Grid Model Data Management (GMDM): A Best Practice Approach to Managing Distribution Grid Model Data • Applying the Grid Model Data Management (GMDM) Information Architecture at the Distribution Utility	Several White Papers that investigate emerging ICT related issues and technologies that may impact utility investments. White paper topics are identified in coordination with advisors from each of the project sets.
Technology Transfer for the ICT Program	The value of the research results developed through the ICT Program is realized when the intended audience uses them. **Webcasts throughout the year** are recorded and provide insights on research in all the ICT Project Sets and guidance on how to apply the research or leverage EPRI Subject Matter Experts to help members apply the results.	Technology transfer of ICT Program resources are combined with monthly "3rd Thursday of the month webcasts, periodic newsletters, Advisory meetings, Supplemental projects and one-on-one engagements with members.

P161D

Ben Ealey,
Sr. Project Manager,
bealey@epri.com

Distributed Energy Resources (DER) Data and Connectivity (161D)

Provides leading resources related to the evolving needs for DER data and connectivity, including tools and technologies, architectures, methodologies, insights, and leading practices to support distributed energy resources (DER) and demand response (DR) technologies integration and data services. A priority is reducing costs and improving efficiency of existing operations today while helping utilities prepare for a 2030 energy system.

PROJECT	**2022** Accomplishments & Key Deliverables	**2023** Plan
Enabling Open, Interoperable DER – Standards, Testability, and Overcoming Barriers to Interoperability	**Protocol Reference Guidebook (PRG)** Your pulse on an ever-changing DER standards landscape. A free version is available and provides an overview of the guidebook and an example brief – the CTA-2045 demand response standard mandated in Washington, Oregon, and California. **IoT Protocols to Integrate DERs** decomposes the buzzword IoT identifying high-priority applications for IoT in utility-centric applications. Identifies high-value applications, existing efforts, and emerging technologies.	As the industry supports utility clean energy targets, information about relevant standards and their maturity become more important in decision-making by utilities, solution providers, and regulators. In 2023 EPRI will perform an annual update of the **Protocol Reference Guidebook** capturing the latest of communications and data standards including adoption, governance, supported technologies, test tools and certification, regulatory requirements, and the utility architecture.
Utility Case Studies on Communicating with DER – Highlighting Experiences, Best Practices and Barriers	**2022 DER Interoperability Guidebook** This annually updated guidebook compiles knowledge, lessons learned, and guidance on achieving DER interoperability. Topics range from testing frameworks, interoperability and cost tests, communication architectures, and more. **Precise Protocol Requirements** DER protocol standards are long and complex. They can include 1000s of optional elements. How do you know which you need and why? This study designed a process to make this easy.	**DER Data and Connectivity Technology Pipeline** EPRI will work with members to establish a pipeline of emerging technologies related to DER data and connectivity. EPRI will perform a deep dive on one or two promising technologies chosen by EPRI to evaluate how these technologies will support the industry, the maturity and what is required for it to be successful.
Bigger Picture – Preparing for End-to-End Integration of DERs	**Training Materials – Information and Communication Technologies (ICT) for Monitoring, Management, and Configuration of DER/DR** This training covers: The Value of a Grid-Connected DER, ICT Fundamentals for DER, ICT Maturity, Private Long-Term Evolution (LTE) Network, Standards to Streamline Grid Interoperability, and Standards and Architectures to Integrate DERs. **Decomposing FERC O2222** evaluates FERC O2222 through an IT/OT lens to develop a model that the industry can reference and build on.	**DER Interoperability Guidebook 2023** The guidebook leverages ten-plus years of work developing and applying standards and each year EPRI revises and adds new sections to reflect the latest industry research needs. **Utility Experiences in DER Integration** EPRI will work with member utilities to capture experiences, use cases, and other information to inform the member collaborative.

Enterprise Architecture and Integration (161E)

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

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

PROJECT	2022 Accomplishments & Key Deliverables	2023 Plan
Enterprise Architecture (EA)	**Top Ten Indicators of Enterprise Architecture (EA) Maturity—2021 Results** The state of EA maturity in the utility industry. **Library of Enterprise Architecture Patterns: LEAPworx 4th Edition** Re-usable elements and diagrams. **Utility Enterprise Architecture Guidebook, 7th Edition** Shift left, getting EA involved sooner. Lessons from the field. **Architectural Impacts of Disruptive Technology** How to select potentially disruptive technologies for your operations or a competitor's.	**Utility Enterprise Architecture Guidebook, 8th Edition** Annual update that incorporates leading research from the EA discipline and best practices and lessons learned from utilities and beyond. **Top Ten Indicators of EA Maturity: 2022 Survey Results** A state of the EA discipline in the utility industry annual survey. **LEAPWorx 5th Edition** Reusable diagrams and elements from the EA teams collaborations across the institute.
Enterprise Systems Integration	**Common Information Model Primer: Eighth Edition** Implementing the CIM at a utility for standards-based integration and semantic understanding. **Cloud Integration Guidebook, 7th Edition: A Guide for Enterprise Architects** Limitations of gov cloud, an overview of cloud managed services and updated cloud related security standards. **Applying the Grid Model Data Management (GMDM) Approach at the Distribution Utility** Laying out the central Grid Model Manager concept, proven in the transmission domain, in distribution. **CIM Support for Distribution Grid Model Data Management** How the CIM supports the additional requirements of the distribution domain. **Distribution Grid Model Data Management (GMDM) A Best Practice Approach** How to use the GMDM approach, proven in the transmission domain, in distribution. **Grid Model Data Management (GMDM) Architecture in Archimate** The GMDM Information architecture captured in the Archimate modeling language. Includes model files for immediate use and extension.	**Cloud Integration Guidebook: A Guide for Enterprise Architects, 7th Edition** Annual update that to enable the adoption of cloud-based services. **Common Information Model (CIM) Primer, 8th Edition** A reference for the IEC CIM; its structure, use, and extension.

continued…

continued...

Enterprise Architecture and Integration (161E)

PROJECT	2022 Accomplishments & Key Deliverables	2023 Plan
Organizational Alignment	**Digital Transformation: Information Technology–Operational Technology Convergence Guidebook: Fifth Edition** A facilitation approach to bridge the cultural gaps and bring IT and OT teams together. **Grid Modernization Playbook** A framework for developing your plan. A joint deliverable with Distribution planning and operations (P200).	**Utility Business Capability Model** Extensions and refinements to the model learned through its application across EPRI and utility projects. **Digital Transformation: Aligning Information Technology and Operations Technology, Sixth Edition** Why, when and how to converge capabilities across teams. **Impacts of Disruptive Technologies 4th Edition** Incorporating disruptive technologies into the innovation practice. Business Capability Model Guidebook 1st Edition - Provides guidance for building and using a business capability model for strategy development, roadmapping, assessments and portfolio optimization. **Grid Modernization Playbook** Provides guidance on road mapping for grid modernization. Joint deliverable with the Distribution Operations and planning (P200).
Technology Innovation	**Diagramming OT Cyber Security Threats, Vulnerabilities, and Impacts** Capturing and visualizing cyber security threats, vulnerabilities, and risks and impacts in utility OT environments. **A Functional Application Architecture for Grid Model Data Management (GMDM)** Defines the Grid Model Data Management (GMDM) application functions and the data objects they produce and consume. **DER Gateway Reference Architecture** The device and application functions associated with DER Gateways and the data they produce and consume.	Reference architectures to support open-source development and adoption in the utility industry. Capture and automatically validate CIM Data exchange rules using graph based technology.

P161F

Advanced Metering Systems (161F)

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

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

PROJECT	**2022** Accomplishments & Key Deliverables	**2023** Plan
Achieving Open, Interoperable Advanced Metering Systems	**Standard Meter Communications Protocols Primer** This primer describes the ANSI C12 and DLMS/COSEM (IEC 62056) series of standards to give interested people an idea of what is included within these important metering communications protocol standards and how they work. Security provisions of the various protocols are also included.	Survey of Currently Used AMI Radiofrequency Protocols that is an investigation of the full stack of protocols currently used in RF-based AMI networks.
Advanced Metering Systems Operations and Management	**Guidebook for Identifying and Mitigating AMI Communications** This document describes the ways of identifying and mitigating AMI communications problems. It describes both inadvertent and malicious interference.	Testing Requirements for AMI Meters that describe current requirements, from both business and regulatory aspects of meter accuracy testing and possible future trends.
Optimizing Advanced Metering System Value and Utilization	**Analyzing and Categorizing Momentary Outages from AMI** AMI data are widely applied in conjunction with outage management systems (OMSs), improving average outage duration by 4–6 min. Offering measurable and significant benefits, such schemes usually rely on outage reports from the meters themselves, either via powerline carrier or radio frequency communications, using so-called "last-gasp messages." This paper considers instead the use of momentary outages that are not long enough for the meter to report an outage or that clear without human intervention within a few seconds.	Business Cases for Replacement AMI Systems report enumerates and analyzes business cases for the replacement of AMI systems. **Advanced Metering Data Analytics Guidebook** Update to 2019 edition, describes how utilities used AMI data analytics and how to organize their employees for that purpose. Also describes free open-source software tools that can be useful in AMI data analytics.
Technology Innovations	**AMI System Simulation Software** Allows utilities, researchers, and the general public to be able to begin modeling their AMI systems. Benefits and Values: • Simulation provides an inexpensive way to assess • Simulator built on well-known ns-3 tool • Simulation can be expanded and modified **AMI System Simulation Users Manual** The purpose of the AMI System Simulation software is to provide software that will allow utilities, other researchers, and the public to be able to begin modeling their Advanced Metering Infrastructure systems. Software modeling is frequently used in utilities today for planning and controlling portions of the grid as diverse as distribution operations and capacity expansion planning for generation. This software is solely concerned with modeling communications and has no provisions for modeling grid or meter functioning beyond the communications on an AMI network.	**High-speed experimental meter front-end** is a mixed hardware and software prototype to experiment with waveform capture and compression techniques.

Tim Godfrey,
Program Manager,
tgodfrey@epri.com

Telecommunications (161G)

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

PROJECT	**2022** Accomplishments & Key Deliverables	**2023** Plan
Wide Area Networks	**Assessment of AFC System Protection of 6 GHz Microwave Links** reviews and provides research on the status of automatic frequency control (AFC) development, which facilitates the unlicensed co-channel use. In addition, computer code is used to perform simulations of AFC FS protection calculations for comparison against actual EPRI test case measurements. Lastly, a demonstration simulation is done for a Wi-Fi Alliance (WFA) AFC test vector. **Wide Area Network (WAN) Modernization Guidebook** WANs have a central place and play a critical role in the utility telecommunications infrastructure and operation, but challenges are brought on by obsolescence of existing solutions. This forces a migration from TDM and serial to packet-based WAN technologies. Cloud computing along with other technology advances, i.e., software defined networking complicates the transition process. This first edition report contains an overview of the topic and content drawn from previous ICT research in the WAN subject area. **Strategic Fiber Guidebook 2022 Edition** Utilities consider constructing private long-term evolution (LTE) telecommunications networks to better meet reliability and resiliency requirements and to support grid modernization programs. The report contains four case studies of utility private long-term evolution (LTE) projects. Ameren's case study captures a project in the pilot stage. Southern Company's Southern Linc case study highlights a mature private LTE network. New York Power Authority highlights a focus on transmission asset inspection as a use case, and San Diego Gas and Electric's case study highlights operation in CBRS spectrum.	**Evaluation of Interference to 6- GHz Microwave** Field testing of interference to 6-GHz microwave links from standard power unlicensed devices using automatic frequency control (AFC) (may include multiple deliverables). **WAN Modernization Guidebook 2023 Edition** Update of this guidebook's 2022 edition. **Strategic Fiber Guidebook 2023 Edition** Annual update of this guidebook.
Field / Neighborhood Area Networks	**Private LTE Guidebook 2022** contains four case studies of utility private LTE projects. Ameren's case study captures a project in the pilot stage. Southern Company's Southern Linc case study highlights a mature private LTE network. New York Power Authority highlights a focus on transmission asset inspection as a use case, and San Diego Gas and Electric's case study highlights operation in CBRS spectrum. **Communication Requirements for DER** introduces the components used in the evaluation of Wi-SUN to support DER communications and discusses prior work on DER protocols and performance expectations, a DER Simulation tool, and network setup methods for executing the study with one vendor.	**Private LTE Guidebook – 2023 Edition** Annual update of this guidebook that provides an overview of the technology and architecture and identifies current and potential spectrum options for private LTE network deployment. **Evaluation of 5G URLLC for Direct Transfer Trip** Ultra-Reliable Low-Latency Communication (URLLC) field testing and evaluation.

continued…

continued…

Telecommunications (161G)

PROJECT	**2022** Accomplishments & Key Deliverables	**2023** Plan
Telecommunications Planning and Management Systems	**Telecom Site Planning and Practices for Resilience and Backup Power** Southern Linc, now with many years of experience operating a private cellular network, shares their experiences designing, deploying, and maintaining a unique backup power scheme involving fuel cells, including features of their topology, reasoning behind their decision to use fuel cells, and some lessons learned. **Approaches for Autonomous Peer to Peer Communication: For Resilient Community Microgrids** The decentralized control architecture is expected to maximize community benefit during normal conditions by interfacing upstream with central systems and isolating and coordinating with peer systems to provide power to local communities during emergency events. **Integration of Device Provisioning into the Network Management System** examines three vendor offerings for device management. Through this assessment, EPRI attempts to identify the systems that may provide a method for SIM management integration into the NMS. This information was obtained through publicly available webcasts and through the companies' websites.	**Network Management Systems** Telecom Network Management Systems **Resilient Networks with Islanded Operation Capability** Resilient networks with islanded operation capability evaluation – update on system-level testing with microgrid scenario. **Satellite and Emergency Communication** Continue evaluation of Starlink and other satellite services for resiliency and availability. Update on technologies and best practices for ensuring communications availability in various scenarios
Telecommunication Standards Engagement	**Standards Guidebook - 2022 Edition** Updates in this 2022 edition include new and revised content in the areas of: Rural broadband, joint builds, partnerships; asset and lifecycle tracking, fiber in distribution and inside the substation and PON technology. **Comms Intelligencer Newsletter, 1H 2022** highlights issues of relevance and interest to utility communications engineers and managers. Focus is on developments in communication technologies and standards. **Comms Intelligencer Newsletter 2H 2022** Many of the wide range of wireless communications technologies that are deployed today, or may be deployed in the future, originate from the standards development activities that are covered in this newsletter.	**Smart Grid Communications Intelligencer 1H 2023 & 2H 2023** This triannual newsletter highlights issues of relevance and interest to utility communications engineers and managers. The focus is on developments in communication technologies and standards, as well as business issues that can affect the design, deployment, or operation of utility communications infrastructure. **Telecom Standards Guidebook Vol 5** Annual update of this guidebook incorporates previous work performed and adds individual utility policies and practices, including placeholders for future research results.
Technology Innovations	**6GHz AFC Protection Innovations** documents progress in developing the tool, most significantly the successful implementation of OpenAFC that is a project under the Telecom Infra Project (TIP) sponsored by Meta. **Analysis of Private LTE and 5G Radio Access Network Data Sets for Performance Optimization** EPRI's AI initiative is a collaborative effort funded by Technology Innovation for developing artificial intelligence (AI) and machine learning (ML) solutions. EPRI's effort is intended to bridge the gap between the electric power industry and AI community by bringing various cutting-edge methodologies and models to the power and energy sector and to utilities.	

P161H

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

Geospatial Informatics (161H)

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

PROJECT	**2022** Accomplishments & Key Deliverables	**2023** Plan
Geospatial Informatics (GIS) Data Practices	**Geospatial Informatics Guidebook: Third Edition** key updates included inventory of data quality software solutions, Key performance indicators template and case study, additions to geolocating underground infrastructure case studies, and geospatial data standards section updates.	• Migrate the Geospatial Informatics Guidebook to an interactive online platform. • New case studies on geospatial data maintenance/data improvement leading practices • Survey of Utility GIS teams • GIS software functionality matrix
Geospatial Informatics (GIS) Applications	**Geospatial Requirements for XR Applications - 2022 Update** Technical update of geospatial requirements for XR applications, especially around digital twin research with guidance on digital twin technology development, mature digital twins, use cases and practical implementation steps.	• Work management systems and GIS, mobile apps • Custom GIS applications and management practices • Geospatial Digital Twins, Machine Learning and Neural Network opportunities
Geospatial Informatics (GIS) Analytics and Visualization	**Dynamic Geospatial Informatics Can Model Grid Operations** Dynamic data for complex geo-analytics supporting grid management, change detection, and future opportunities. **Geospatial Analysis for Site Selection and Grid Managment of DERs** Outlines geospatial analytic techniques and data sources for Solar, Wind and Battery Storage site selection and GIS support in managing DER variable power generation.	• Role of dynamic data in GIS Analytics • Capture Utility GIS analytics practices • Begin compilation of Utility GIS Analytics playbook
Technology Innovations	**Enhancing GIS Data Quality Using Artificial Intelligence Tools** Improving geospatial data quality investigation of available Artificial Intelligence, Machine Learning and Graph database tools. Data quality segments locational accuracy, feature attributes, and network topology are examined.	• Digital Unique Identification of Specialized Equipment • Develop Utility Hazard Zone GIS data services and Story Map for Distribution Resilience

Examples of Member Application of Results

Value Obtained

161A

ConEdison

EPRI ICT Program (161A) - "3rd Thursday" Emerging Technology Webcasts

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

161A

Ameren

EPRI ICT Program (161A) - Technology Transfer Activities

The role of the Emerging Technologies and Technology Transfer (161A) Project Set is to provide insights into ICT standards, issues and insights in a variety of formats from webcasts, white papers and advisory meetings.

"The variety and depth of topics on the ICT Monthly webcasts combined with the technical papers is very helpful and the advisory meetings are my favorite. With my responsibilities changing from metering to telecommunications making the connections to ICT provides a valuable breadth of information."

Kirby Diller, PE, Ameren

161D

Southern California Edison

Advanced Communications, Standards, and Controls of Smart Inverters and Smart Devices to Enable More Residential Solar Energy

Advanced smart-inverter functions defined in California's Rule 21 tariff pave the way for grid supportive DERs. This project assessed the smart inverter behavior of Rule 21 inverters using laboratory and field tests. Tests included successful side-by-side operation of smart inverters and using residential smart loads to enable more solar PV on the grid.

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.

161D

Duke Energy

CTA 2045 Field Pilots Guide a Path Towards Grid-Enabled End-Use Devices

A technology that continues to be at the forefront of demand response enabled products is the standard known as CTA-2045. EPRI has worked intensively with the industry to develop specifications, test tools, and other resources to support utilities and manufacturers to adopt this new, promising demand response technology.

EPRI's work supporting the commercial availability of CTA-2045 enabled appliances and communication modules allowed Duke to test new innovative applications in lab and field settings. This includes flexible two-way communication to appliances, zero-truck-roll implementation, ease of communication upgrades, and maintaining customer comfort during demand response events.

Examples of Member Application of Results

Value Obtained

161E

Ameren, ConEd, Exelon, National Grid, NYPA, PNM, SRP

Business Capability Model Development for IT-OT Investment Alignment

The two-year project created a Utility Business Capability Model with 8 utilities. Each utility applied and refined the business capability model on their own strategic initiatives including customer experience, asset management and the utility of the future. The primary contributors from the eight utilities received a technology transfer award for their work on this project.

"The EPRI Business Capability Model and associated methods and tools helped SRP take the first step toward capability-based planning, shifting the strategic conversation from acquiring things to understanding what capabilities are need to deliver value to your customers."

Shanon Jones, Manager, Architecture & Planning. Salt River Project (SRP).

"The EPRI Business Capability model has added credibility to our NG Capability Model work across internal stakeholders and external partners, validates and improves our approach to standardization and efficiency, and provides a foundation for much needed industry collaboration around utility of the future, transformational shifts, strategic initiatives and more."

Jennifer Cooper, Director, Future of Electric, National Grid.

161E

Distribution Grid Model Data Management Vendor Forum

In support of these efforts, EPRI began its distribution Grid Model Data Management (GMDM) research in 2017. EPRI's strategy is to develop a unified, vendor-agnostic architecture to enable energy providers to better manage their distribution grid data using products that operate and communicate with each other more accurately. The value of this architecture – and its practical application– was demonstrated at the recent EPRI/UCAIug CIM Interoperability event.

More details and value statements from each of the vendors here: https://energycentral.com/o/EPRI/interoperability-event-demonstrates-successful-grid-model-data-exchange

EPRI's GMDM project is a natural alignment with our Energy Digital Twin solution. This IOP event proved that the proposed interoperability works and uncovered an exciting insight and validation from the data exchanges and collaboration of different vendors."

Esen Kacar, Principal Product Manager

"Thanks to EPRI for the leadership in the Grid Modeling and Data Management (GMDM) project. The project created an architecture for utilities to solve the vexing problem of interoperability of several network management applications such as GIS, ADMS, and network analysis. EPRI allowed us to partner with Safe Software to provide the tools to successfully model the Esri GIS into the most up-to-date CIM model. In addition, they facilitated the process to validate that various network management vendors could consume the CIM output from the ArcGIS Utility Network. This process demonstrated the ability of CIM to model the electric network in a standard, detailed and neutral structure."

Bill Meehan, Director, Electric Utility Solutions

161F

Exelon

Applications of Advanced Meter Functionality

Exelon utilities' participation in the Next Generation Smart Meter Vision and Criteria project identified new meter functionality to enhance operations and functionality. PECO chose to focus on downloading applications and configurations to the meter, programming low and high voltage points, and implementing an interval voltage channel based on EPRI's findings.

The utility's project teams leveraged EPRI research as a catalyst to improve the flexibility of our metering system, enhance quality control, and utilize alarms, voltage and other data more effectively. Both PECO and ComEd have a dynamic environment with competing priorities and incentives, and the EPRI project provided clarity in pursuing these initiatives.

161F

Southern California Edison Uses EPRI Guidebook to Improve AMI System Health Monitoring

This document is a guidebook for utilities that details a recommended practice for AMI system prognostics and health management (PHM). The procedures outlined herein are intended to guide utility test procedures that provide insight into the remaining useful service life of AMI systems.

"Going through another mass deployment is not an option, we must proactively understand the long-term reliability of our AMI system."

Jeffery Counseller, Southern California Edison

Examples of Member Application of Results

Value Obtained

161G

FirstEnergy

FirstEnergy 6GHz Additive Interference Study

In 2020, FCC issued Report & Order (R&O) 20-51 that allows unlicensed device operation in the upper and lower licensed 6 GHz fixed service (FS) microwave radio bands. This band has been licensed for exclusive use by utilities and others. Electric utilities continue to be concerned about the possibility of interference that could cause failure of their critical communication links. One open question has been the potential additive impact of many Wi-Fi networks operating in the vicinity of utility microwave links.

FirstEnergy was able to utilize the testing recommendation and knowledge for making decisions about network upgrades and maintenance of existing systems. The results aid in knowing what to look for when troubleshooting interference on their microwave links. Utilities can speak with more credibility about the harm unlicensed Wi-Fi devices may have on critical communications that support grid management and voice services.

161G

New York Power Authority (NYPA) Private LTE Testing and Performance Assessment

A testing platform for Field Area Networks (The FAN Testing Platform) has been developed as part of the Information and Communication Technology project set 161G on Telecom to assist utilities. NYPA applied the FAN Testing Platform to perform an assessment of the performance of the Private LTE pilot that was in operation at the Blenheim-Gilboa pumped hydro facility.

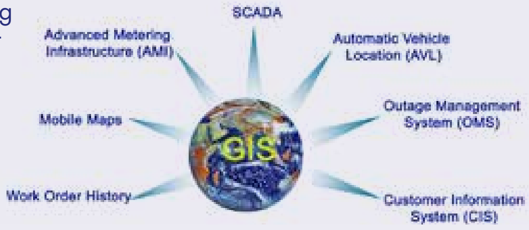
The research revealed the detailed performance characteristics of the Private LTE system, enabling NYPA to better understand the capabilities of the prototype system at the pilot, and plan for future deployments. The testing also revealed new learnings about the overall network architecture that will be essential for integrating the PLTE network into the overall NYPA operational network.

161H

Consolidated Edison

The Geospatial Informatics project set focuses on the science and technology of acquiring, storing, cleaning, modeling, analyzing, producing, presenting, and disseminating geospatial data sets. Collaborative research projects in this area will enable utility geographic information system (GIS) professionals to master GIS data quality and data management challenges and deliver new geodata services for advanced planning and operations applications.

EPRI's Geospatial Informatics research topics are peripheral in relation to ConEds staff's day-to-day work. Looking at our company's GIS through different eyes and seeing the potential to align our work with future GIS development.


SCADA
Advanced Metering Infrastructure (AMI)
Automatic Vehicle Location (AVL)
Mobile Maps
GIS
Outage Management System (OMS)
Work Order History
Customer Information System (CIS)

ICT guidebooks

ICT guidebooks are developed as adaptable go-to reference books to help utilities with development of emerging standards and architectures to enhance interoperability, innovation, marketplace competition; and identify best practices for the support of system operations and monitoring of systems.

161D: Distributed Energy Resources (DER) Data and Connectivity	PID#	YEAR
DER Protocol Reference Guidebook – 6th Edition: Assessment of Information and Protocol Standards for Distributed Energy Resources (DER), Electric Vehicles, and Demand Response Technologies	**3002024179**	**2022**
Distributed Energy Resources Interoperability Guidebook – 2022 Edition: Information and Case Studies to Support Utilities in Achieving Interoperability with Distributed Energy Resources and Demand Response Technologies	**3002024910**	**2022**
Distributed Energy Resources (DER) Protocol Reference Guidebook—5th Edition: Public Version	**3002023419**	**2022**
Demand Response Interoperability Guidebook: A Repository of Information to Support Utilities in Achieving Interoperability in Demand Response Technologies	**3002018543**	**2020**

161E: Enterprise Architecture and Integration	PID#	YEAR
Architectural Impacts of Disruptive Technology	**3002024191**	**2022**
Common Information Model (CIM) Primer: Eighth Edition	**3002024188**	**2022**
Cloud Integration Guidebook, 7th Edition: A Guide for Enterprise Architects	**3002024186**	**2022**
Digital Transformation: Information Technology–Operational Technology Convergence Guidebook: Fifth Edition	**3002024190**	**2022**
Library of Enterprise Architecture Patterns: LEAPworx 4th Edition	**3002024189**	**2022**
Top Ten Indicators of Enterprise Architecture (EA) Maturity—2021 Results	**3002024184**	**2022**
Utility Enterprise Architecture Guidebook, 7th Edition	**3002024183**	**2022**
Introduction to Grid Model Data Management (GMDM): A Best Practice Approach to Managing Distribution Grid Model Data	**3002025384**	**2022**
Common Information Model (CIM) Support for Distribution Grid Model Data Management	**3002025386**	**2022**
Applying the Grid Model Data Management (GMDM) Information Architecture at the Distribution Utility	**3002025387**	**2022**
Distribution Grid Model Manager (GMM) Functional Requirements	**3002025388**	**2022**
A Framework for Relating the Elements of Strategy Development through Implementation	**3002021853**	**2021**
Advanced Metering Infrastructure (AMI) Reference Architecture	**3002021854**	**2021**

ICT guidebooks

161F: Advanced Metering Systems	PID#	YEAR
Standard Meter Communications Protocols Primer	3002024105	2022
Guidebook for Identifying and Mitigating AMI Communications	3002024106	2022
Analyzing and Categorizing Momentary Outages from Advanced Metering Infrastructure (AMI) Data	3002024107	2022
Guidebook for Integrating AMI into Outage Management	3002021413	2021
Program on Technology Innovation: Utilizing AMI Data for Fault Anticipation	3002021414	2021
Revenue Protection Guidebook, Second Edition: Using Advanced Metering Infrastructure	3002018630	2021
Guidebook for Advanced Metering Infrastructure (AMI) Data Analytics	3002015774	2019
Guidebook for AMI System Disaster Preparedness and Restoration, First Edition	3002010502	2017
Guidebook for Advanced Metering Infrastructure Prognostics and Health Management, Second Edition	3002005471	2015

161G: Telecommunications	PID#	YEAR
Private Long-Term Evolution Guidebook	3002023624	2022
Telecommunication Standards Guidebook V4	3002023631	2022
Strategic Fiber Guidebook 2022 Edition	3002023623	2022
FirstEnergy 6 GHz Additive Interference Study – Public	3002025484	2022
Wide Area Network (WAN) Modernization Guidebook: First Edition 2022	3002023622	2022
Teleprotection Over Packet Guidebook: 2020 Edition	3002018509	2020
Utility Telecom Planning Framework and Reference Guide	3002009805	2018

161H: Geospatial Informatics	PID#	YEAR
Geospatial Informatics Guidebook: Third Edition	3002024796	2022
Geospatial Requirements for XR Applications - 2022 Update	3002024797	2022
Enhancing GIS Data Quality Using Artificial Intelligence Tools	3002024798	2022
GIS Leading Practices Guidebook – Data Cleanup Methods with Cost—benefit Analysis Guidance	3002010509	2017
Electric Utility Guidebook for Geographic Information Systems Data Quality: Metadata	3002007921	2016
Electric Utility Guidebook for GIS Data Quality: Conflation	3002006006	2015
Electric Utility Guidebook on Geospatial Information System (GIS) Data Quality	3002003036	2014

What Cyber Security for Power Delivery and Utilization Program (P183) Does:

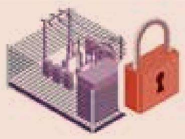
Cyber security has become a critical priority for electric utilities, which are increasingly dependent on information technology and telecommunication infrastructure to ensure the reliability and security of the electric grid. Mitigations to ensure cyber security must be designed and implemented to protect the electric grid from attacks by terrorists and hackers, and to strengthen grid resilience against natural disasters and inadvertent threats, such as equipment failures and user errors.

Incident Management: Improve the electric sector's ability to correlate data and alerts across verticals and respond to threats, and better understand the true risks associated with operating OT networks.

Threat Management: Develop strategies and guidelines for using the latest generation of intrusion detection and prevention systems on the market designed to operate in the OT space, as well as ingest and develop threat intelligence. Utilize advanced technologies such as decoys and AI to improve the overall cyber security posture.

Cyber Security Forensics: Create additional ICS forensics field guides for OT devices and deploy a mobile field guide application for the guides.

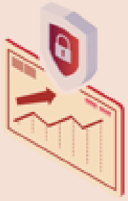
Transmission and Distribution Control Center Security: Develop a comprehensive control center model to determine cyber security requirements and solutions.



Transmission and Distribution Substation Security: Develop a secure IED management guidebook that provides a comprehensive assessment of management requirements for intelligent substation equipment with a recommended substation management strategy.

DER Security: Update the DER Cyber Security Guidebook to include considerations for cyber security engineering approaches for securing DER systems. Develop cyber security guidelines for DERMS to provide security architects and engineers with risk-informed and practical approaches for securing DER management systems.

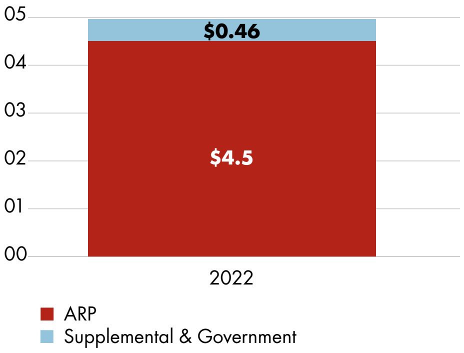
DER Technologies: Provide guidelines for deploying intrusion detection and prevention technologies (IDS/IPS) with DER systems. Develop security reference architectures for microgrids with a focus on the integration of community microgrids.



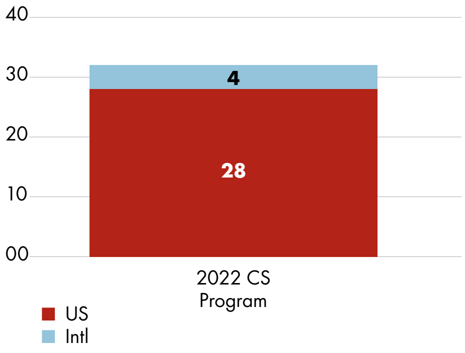
Knowledge Applications: Develop additional cyber security metrics, including resiliency metrics. Support metrics adoption and enabling benchmarks of relevant cyber security program performance. Deliver cyber security program assessments and develop novel training opportunities.

Cyber Security Roadmap for 2030: identifies the critical future states for Cyber Security in the electricity subsector and the action plans that must be adopted to achieve intrinsic Cyber Security.

Cyber Security Program Funding
(in $ Millions)



Utility Members



Staff	#
Tech	15
Admin	2
Total	17

Degree	#
Masters	8
Bachelors	8

Ben Sooter,
Program Manager,
bsooter@epri.com

Incident and Threat Management

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

PROJECT	2022 Accomplishments & Key Deliverables	2023 Plan
Incident Management Ben Sooter ***bsooter@epri.com***	**The Integrated Security Operations Center (ISOC) Guidebook 2022 Update** provides utilities with guidance for the implementation of their incident management program, focusing on monitoring, detection, and response. The update for 2022 includes information on utilizing managed service providers (MSSPs) to augment staff for OT monitoring.	The Integrated Security Operations Center (ISOC) Guidebook 2023 Update - reflects changes in technology and best practices and includes new EPRI research related to incident management. In 2023 we plan to update several of the areas in the guidebook that have undergone change in the past few years.
Threat Management Ben Sooter ***bsooter@epri.com***	**Threat Management Guidebook 2022 Update** describes strategies and guidelines for electric power utilities to design, implement, and operate a Threat Management Program (TMP) for their entire system so they can better protect it against cyber-attacks. A threat management program extends the capabilities of a typical security operations center by integrating and correlating security events from operations technology (OT) networks across the entire kill chain. The 2022 update includes information on cyber threat intelligence and protecting OT assets from ransomware.	Threat Management Guidebook 2023 Update - provides comprehensive guidance based on past EPRI research from 2017 to 2023. The guidebook will be updated annually to reflect changes in technology and best practices and to include new EPRI research related to threat management. In 2023 we plan to explore timing attacks on SIEMSs and decoy technologies in OT environments.
Cyber Security Forensics William Webb ***wwebb@epri.com***	**Automation of Digital Forensics in Operational Technology Environments: Collection, Analysis, and Alerting** aims to investigate the possibility of using automation in the process of collecting and analyzing forensics evidence during an incident response. The goal is to determine whether this approach could improve the efficiency and accuracy of the investigation process. By automating certain tasks, it may be possible to gain a deeper understanding of the incident and identify relevant information more quickly and accurately. **SEL-3530 RTAC Mobile Forensics Field Guide** This product is a mobile application version of report 3002019056, SEL-3530 RTAC Forensics Field Guide, available from the Apple App Store and the Google Play store. These mobile field guides provide a convenient format for analysts to view the content in a more interactive way. These guides can be downloaded to a mobile device and viewed even in areas where cellular reception may be poor or prohibited.	ICS Forensics Guidebook, 1st edition - provides updated guidance on how to use automated forensic harvesting tools with an integrated security operations center. It will also continue to address the manual extraction of forensics artifacts from a variety of industrial control system devices.

John Stewart,
Principal Project Manager,
jstewart@epri.com

Cyber Security for Transmission and Distribution

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

PROJECT	**2022** Accomplishments & Key Deliverables	**2023** Plan
Cyber Security for Substations and Field Devices John Stewart *jstewart@epri.com*	**Secure IED Management Guidebook** provides an overview of various management capabilities that should be included in a comprehensive Intelligent Electronic Device (IED) management program. The focus of this research is on substation networks and systems, since cybersecurity in the transmission and distribution area can present a significant number of challenges to utility personnel. **Cyber Security for Digital Substations** discusses substation cybersecurity, the ongoing transition to digital substation designs, the differences between conventional and digital substations, and recommended actions for security personnel to engage digital substation engineers to develop and an appropriate security strategy. Topics include, Differences in Enterprise IT and Substation OT, Design Lifecycle, Digital Substation Technologies, Cyber and Compliance Impact.	Substation Security Integration Opportunities to influence the substation planning and design workflow to integrate security objectives early in the decision-making process. Cyber Security for Digital Substations - A revised exploration of new substation architectures and emerging cyber security needs
Cyber Security for Control Centers John Stewart *jstewart@epri.com*	**Security Integration for Transmission and Distribution Systems: Collaborative Working Group** The Security Integration Working Group is a collaborative effort focused on the integration of security requirements as early as possible in the utility capital project process. NERC and IEEE initiated the working group effort with the support of EPRI's utility members and other industry subject matter experts.	Modeling and Securing T&D Systems - This report will define a framework and methodology for creating a detailed control system model that can be used to assess alternative cyber security approaches.

Cyber Security for DER and Grid-Edge Systems

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

Cyber Security for DER Integration and Management (CSDIM)

Xavier Francia
xfrancia@epri.com

2022 Accomplishments & Key Deliverables

The Distributed Energy Resources (DER) Cybersecurity Guidebook 2022 Update
This annual guidebook is a reference document for utility cybersecurity architects, cybersecurity engineers, and other stakeholders to assist in securing integration of DER to the grid and provides background information on DERs, standards and regulations, electricity market participants and an overview of cybersecurity risks through the representative DER threat scenario information library.

2023 Plan

Distributed Energy Resources (DER) Cyber Security Guidebook for Utility Architects and Engineers, 3rd Edition is a reference document for Cyber Security Guidelines for DERMS that are intended to provide a key reference for utility cyber security architects and engineers by providing risk-informed and practical approaches for securing DER Management Systems and includes security requirements for both DERMS systems and the various interfaces, ADMS, third-party DERs, aggregator DERMS, and security considerations for DERMS control hierarchies.

Cyber Security for DER Technologies (CSDT)

Sai Ram Ganti
sganti@epri.com

Security Architecture for Microgrid Integration Volume 2 Microgrids present a valuable tool for electric reliability for both electric utilities and customers. This report explores types of microgrid systems, from utility-scale to customer-scale deployments, specifies the components that make up a microgrid system, identifies specific threats against these components, and offers a set of practical cybersecurity controls and recommendations to assist both utilities and customers in their design of these new types of grid systems.

Threat Monitoring Guidance for DER Systems: Phase 1 investigates threat monitoring approaches for DER systems. This project included a testbed development for evaluating various test cases with common DER protocols and IDS/IPS solutions. This report provides architectural guidance for implementing and placement of IDS/IPS solutions for DERs. Phase 1 of this report focusses on evaluating IDS/IPS solutions monitoring DNP3 communications in a master-outstation setup.

Threat Monitoring Guidance for DER Systems, Second Edition - provides better understanding on how threat monitoring technologies may be implemented for DER, including research results from laboratory testing. The second edition includes considerations for implementing threat monitoring technologies for IEEE 1547 DER Integration Data Models supported by DNP3, Modbus, and IEEE 2030.5/SEP2.

Christine Hertzog,
Principal Project Manager,
chertzog@epri.com

Knowledge Applications

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

PROJECT	**2022** Accomplishments & Key Deliverables	**2023** Plan
Cyber Security Data Foundations Christine Hertzog *chertzog@epri.com*	EPRI completed work with three utilities to create performance metrics using a web-based platform, established a working group to develop cyber security resiliency metrics, and surveyed cyber security data governance and management practices and developed and published: • Cyber Security Data Management – Utility Survey Results • Cyber Security Data Management – Data Model Guidelines • Metrics 101 – A Beginners Guide to OT Cyber Security Metrics • Cyber Security Data Management – Utility Gaps and Framework • OT Cyber Security Resiliency Metrics V.1	OT Cyber Security Data Management Guide V1 – provides recommendations for OT cyber security data management to help utilities prepare for AI-enabled applications. Data Governance Guidelines for OT Cyber Security Data will provide guidance on NERC CIP compliance and data usage in advanced analytics and AI-enabled applications. The Cyber Resiliency Technical Update will document progress made in metrics to describe cyber resilient operations.
Cyber Security Assessments Christine Hertzog *chertzog@epri.com*	EPRI established OT-specific assessment services to identify gaps and recommend actions to improve OT cyber security programs and risk postures.	Conduct assessments and develop anonymized benchmarking data to help utilities take corrective actions that effectively mitigate prioritized risks.
Cyber Security Workforce Training Christine Hertzog *chertzog@epri.com*	EPRI created hands-on training to help utilities strengthen practical knowledge and competencies in OT cyber security solutions in addition to CBTs and videos available through EPRI U.	Develop new instructor-led and lab-based courses and CBTs based on utility needs in topics such as IEC 61850 and equipment familiarization.
Industry Collaboration Erica Loveday *eloveday@epri.com*	**Cyber Security Industry Updates: 2022 Edition** This project supports active participation in and contribution to collaborative efforts and interest groups through a monthly email member update to summarize EPRI's industry activities and the status of its research projects.	Cyber Security Industry Updates—2023 Edition (Newsletters) This public report will provide a summary of 2023 industry collaboration effort

Examples of Member Application of Results

Incident and Threat Management

Value Obtained

Southern Company

Next Generation OT Cyber Security Visibility

Detecting and responding to security threats in an operational environment is one of the biggest challenges for utilities. Southern Company (SoCo) worked closely with the Knoxville Cyber Security Research Lab (CSRL) to develop a novel solution. Past government exercises, such as the DOE CYOTE project and the DARPA RADICS project, demonstrated the value of having full packet capture from network data for all traffic combined with other sensor packages. Working with EPRI, Gravwell and Southern Company developed a system that leveraged an open source and high-performance packet-capture capabilities that can be deployed in conjunction with Gravwell data collectors. This enabled the packet capture to take place and be stored at the edge nodes of networks. This solution eases network load on already bandwidth-constrained OT environments; this reduction in bandwidth was critical in realizing the detection, monitoring, and forensic capabilities.

The solution deployed by SoCo demonstrated that flexibility in deploying multiple sensors and creating as much visibility as possible is necessary when responding to advanced attacks. Utilizing the CSRL enables EPRI members to perform proof-of-concept testing of future security technologies and use cases that will provide efficient testing and implementation of new technologies and systems. SoCo utilized the EPRI Lab to demonstrate the effectiveness of the solution prior to deploying it. Besides receiving value from EPRI, SoCo also received a great deal of value from the proposed solution. The previously deployed technologies at SoCo to perform full packet capture, were commercially sourced solutions which were very expensive. As a result, SoCo deployed full PCAP only at specific high-value sites, such as data centers. The cost and bandwidth constraints meant that the existing solution could not be deployed to field sites such as substations. The new system has extensive bandwidth savings, reduces license costs, and leverages open-source technologies. In addition to the savings, the new system can provide full packet capture at field sites, is easy to distribute, and provides fast searching.

Tokyo Electric Power

Artificial Intelligence for Cyber Security

The field of artificial intelligence (AI) has dramatically advanced over the past decades and has found applications in various fields such as robotics, manufacturing, transportation, healthcare, finance, sports, marketing, and many other areas of engineering and science. In recent years, advances in the electric sector have made AI solutions a desirable paradigm for solving data-driven problems that can be automated. The effectiveness of AI has been demonstrated in many power systems applications in the electric sector, such as load forecasting, state estimation, electricity pricing, and optimal power flow. Cybersecurity in the electric industry can significantly benefit from technology advancements in AI. However, broad adoption remains to be seen. There are several reasons for this. Some of the main reasons are a lack of high-fidelity data for training AI models, limited understanding of what is possible with AI, the absence of clearly defined use cases articulating what AI methodologies are applicable, and roadmaps for integrating AI along with difficulty in navigating the AI-based cybersecurity solutions vendor landscape.

In collaboration with Tokyo Electric Power Company (TEPCO), this project examined ten use cases for AI-based cybersecurity and briefly discussed how various well-known algorithms can be applied to the use cases. An AI-based cybersecurity integration roadmap template was also developed, along with guidelines for navigating the complex AI-based cybersecurity solutions vendor landscape. This project enabled TEPCO to assess its readiness to implement AI for cybersecurity solutions, identify crucial use cases, and create an implementation roadmap.

Examples of Member Application of Results

Cyber Security for Transmission and Distribution Operations and Systems

Value Obtained

Louisville Gas and Electric Company and Kentucky Utilities Company

Cyber Security for Digital Substations

A significant amount of money and resources have been deployed over the past twenty years to mitigate cyber risks and meet regulatory requirements in substations. The evolution of control system and communications infrastructure in the substation has accelerated in recent years.

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

The typical pace of change for T&D infrastructure is slow and incremental, but the shift to digital substations involves the replacement of systems that have not been "cyber assets" and did not have an attack surface for remote manipulation.

As utilities continue to expand the focus of cybersecurity and compliance efforts in the power delivery space, new technical and process controls have evolved to address specific risks at transmission and distribution substations. These unique facilities are critical to the safe and reliable operation of the grid and must be protected from emerging cyber risk.

Cyber Security for DER and Grid-Edge Systems

Value Obtained

AEP, SRP

EPRI Security Architecture for the DER Integration Network and DER Cyber Security Workshop

Remote monitoring and control of distributed generation require local devices and sensors to communicate operational status and receive commands from remote systems, via public or private communication networks. In the meantime, the attack surface of the nation's grid is increasing as more and more devices become intelligent and connected. Without adequate cybersecurity protection, energy generation and interconnected systems may be exposed to cyber threats.

Security Architecture for the DER Integration Network provides a clear and practical guideline for network design and introduces a risk-based security approach for DER integration. This includes a detailed implementation guideline with examples of technologies to meet the requirements and a 60-point checklist to verify the compliance with the requirements. Utilities can use the requirements specified in the document for implementing utility managed integration networks or for the procurement of integration services from third parties.

PG&E

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

Grid modernization, renewable generation, and integration of distributed energy resources pose significant challenges to cyber security. EPRI's focus to cyber security for distribution systems in garnered various options and methodologies for understanding and modeling cyber-attacks to these systems for utilities.

EPRI's security reference architectures and attack models provide utility cyber security professionals with critical security information on distribution systems in a simple format. They can be used in the design and deployment of new systems; security augmentation of old systems; architectural review of current systems; vulnerability analysis and attack modeling; and remediation of discovered security vulnerabilities.

Examples of Member Application of Results

Knowledge Applications

Value Obtained

New York Power Authority (NYPA)

Cyber Security Tailored Assessment for Utility Transmission and Distribution Operations

Electric generating utilities are seeking to increase their cyber security program maturity beyond regulatory compliance. Their goals include reducing the likelihood and consequence of cyber attacks. A robust OT cyber security program can mitigate cyber risks that may impact grid operations and cause unplanned outages, reputational damages, lost revenue, and/or personnel safety. EPRI's Power Delivery Cyber Security Tailored Assessment for Utility Transmission and Distribution Operations project delivers focused assessments to help utilities identify opportunities for operational, tactical, and strategic actions that may mitigate cyber risks.

EPRI worked with the New York Power Authority (NYPA) to assess its transient cyber asset, patching and vulnerability management, and training programs. The first two assessment topics focused on how NYPA manages security procedures for specific grid operations. The third assessment topic examined NYPA's cyber security training for all resources and for cyber security professionals. These analyses identified strengths and opportunity areas in the program capabilities and documented actionable recommendations bolstered by EPRI research.

EPRI identified recommendations to improve NYPA's cyber security program. These recommendations were specific, rated by priority, and given estimated timeframes for completion. NYPA tailored the recommendations to meet internal security goals and incorporate them into work plans. In addition to the recommendations, EPRI provided a detailed discussion of the program components, regulatory requirements, industry best practices, and relevant EPRI research. NYPA derived added value from EPRI membership by using the organization's research in targeted action plans.

"Third party assessments are powerful tools to assess the security posture of an organization. EPRI's experience and research in the utility sector and operational technology adds insights that generic cyber assessments may miss or overlook. EPRI's specific and actionable recommendations both showed that NYPA's cyber security program is on the right track and highlighted valuable opportunities for improvement," said Nezir Fetahaj, NYPA's director of Operations Technology.

Cyber Security for PDU guidebooks

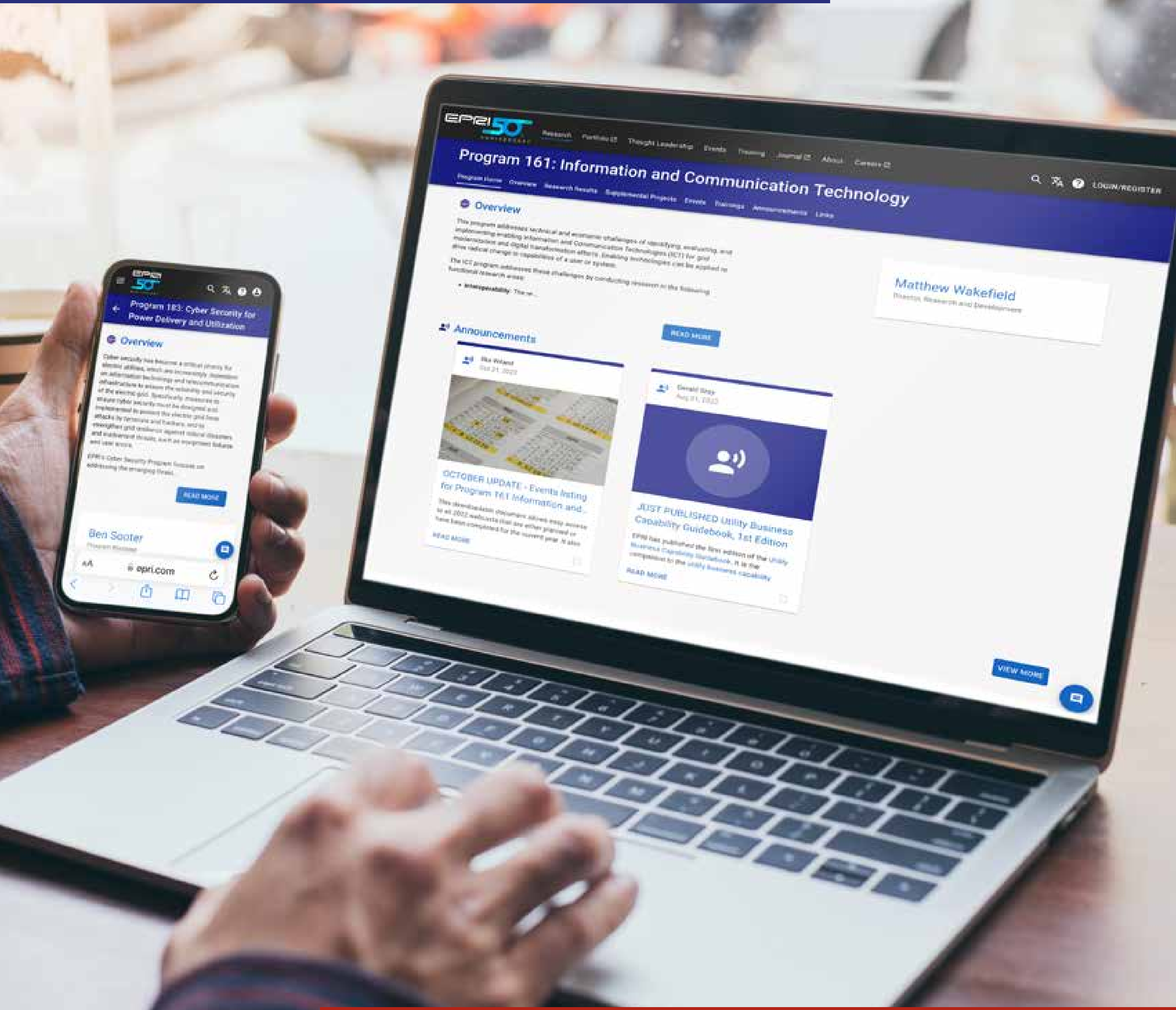
Cyber Security for PDU guidebooks are developed as adaptable go-to reference books to help utilities with development of emerging standards and architectures to enhance interoperability, innovation, marketplace competition; and identify best practices for the support of system operations and monitoring of systems.

TITLE	PID#	YEAR
Automation of Digital Forensics in Operational Technology Environments: Collection, Analysis, and Alerting	3002024151	2022
Cybersecurity Guidebook for Distributed Energy Resources: 2nd Edition	3002024142	2022
Guidebook for a Comprehensive Approach to Secure Intelligent Electronic Device (IED) Management	3002024172	2022
Metrics 101 – A Beginners Guide to OT Cyber Security Metrics	3002024127	2022
OT Cyber Security Resiliency Metrics V1	3002024129	2022
SEL-3530 RTAC Mobile Forensics Field Guide	3002024152	2022
Security Architecture for Microgrid Integration: 2nd Edition	3002024146	2022
Threat Management Guidebook: 2022	3002024203	2022
Threat Monitoring Guidance for DER Systems: Phase 1	3002024149	2022
The Integrated Security Operations Center Guidebook: 2022	3002024202	2022
Cybersecurity Requirements for Utility Owned Energy Storage Systems	3002021386	2021
Cybersecurity Requirements for Utility Electric Vehicle Charging Infrastructure	3002021392	2021
Cyber Security for Grid Connected Devices and Demand Response: Cybersecurity Risks, Threats, and Recommendations	3002021395	2021
EPRI Cyber Security Metrics for the Electric Sector: Cyber Security Metrics Implementation Guidebook	3002021398	2021
EPRI OpenMetCalc User Guide: OpenMetCalc 3.0 User Manual	3002021399	2021
OpenMetCalc 3.0 Tutorial Workbook: A Quick Guide to EPRI OpenMetCalc 3.0	3002021401	2021
AI Based Vulnerability Assessment for Power Distribution Systems Considering Distributed Energy Resources (DERs)	3002021407	2021
Insider Threat Management Program Guidebook for Electric Power Utilities	3002022658	2021
Innovation in Utility Security Automation: Automating Cybersecurity Compliance	3002022196	2021
Cybersecurity for Utility UAS Operations	3002023217	2021
NovaTech OrionLX Mobile Forensics Field Guide	3002019057	2021
EPRI Cyber Security Metrics: Data Point Definition & Collection Guideline	3002019259	2020
Forensics Field Guide: SEL-3530-4 Real-Time Automation Controller	3002019056	2020
Smart Inverter Hardware Security: Utility Procurement Guide	3002019558	2020

Information, Communication and Cyber Security Area Resources

EPRI's website is the place to go for all information about the ICCS Area results, projects, events, announcements and more…

Program 161 www.epri.com/research/programs/062333


Research
Thought Leadership
Events
Training
Journal
About
Careers
LOGIN/REGISTER
Program 161: Information and Communication Technology
Overview
Announcements
READ MORE
Matthew Wakefield
OCTOBER UPDATE - Events listing for Program 161 Information and...
READ MORE
JUST PUBLISHED Utility Business Capability Guidebook, 1st Edition
READ MORE
VIEW MORE
Program 183: Cyber Security for Power Delivery and Utilization
Overview
READ MORE
Ben Sooter
epri.com

Program 183 www.epri.com/research/programs/072143

EPRI 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

Product ID 3002026076