EPRI



# Information, Communication and Cyber Security

Area Review 2024





FEBRUARY 2024



# What the Information, Communication and Cyber Security (ICCS) area does

This program addresses technical and economic challenges of identifying, evaluating, and implementing enabling Information and Communication Technologies (ICT) for grid modernization and digital transformation efforts.

## Information and Communication Technology Program (161)

The ICT program addresses these challenges by conducting research in six project sets that cut across three functional research 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.

### 2023

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

### Changes for 2024

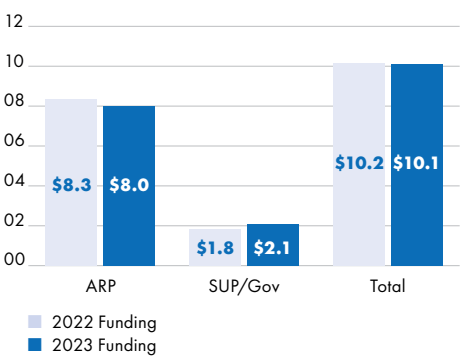
**Cyber Security for Energy Delivery and Customer Solutions**

- Strategic Intelligence & Emerging Issues (PS183A)
- Incident & Threat Management (PS183B)
- Cyber Security for Transmission & Distribution (PS183C)
- Cyber Security for DER & Grid-Edge Systems (PS183D)
- Cyber Security Data Applications (PS183E)

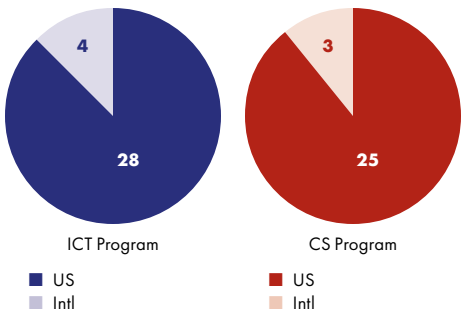
**Contents**


3 What We Do
4 ICT Program (161) What We Do
5 ICT Emerging Technologies (161A)
6 ICT for DER (161D)
7 Enterprise Architecture (161E)
9 Advanced Metering (161F)
10 Telecommunications (161G)
12 Geospatial Informatics (161H)
13 Examples of Member Application Results (161)
16 Supplementals (161)
21 Guidebooks (161)
24 Cyber Security Program (183) What We Do
25 Strategic Intelligence and Emerging Issues (183A)
26 Incident and Threat Management (183B)
27 Cyber Security for Transmission and Distribution (183C)
28 Cyber Security for DER and Grid-Edge Systems (183D)
29 Cyber Security Data Applications (183E)
30 Examples of Member Application Results (183)
33 Supplementals (183)
38 Guidebooks (183)
40 Cyber Security Training
42 Cyber Security Laboratory Knoxville


**ICT & Cyber Security Funding (in $ Millions)**




**2023 Utility Members**




| 2024 Staff | # |
|---|---|
| Tech | 30 |
| Admin | 2 |
| **Total** | **32** |

| Degree | # |
|---|---|
| PhD | 2 |
| Masters | 13 |
| Bachelors | 16 |

## What the Information and Communication Technology (ICT) Program does

The program is designed to promote innovation by discovering new and more effective solutions to current problems through interoperability, thereby guiding the industry towards highly connected, interoperable future grid value streams. The program is organized into six project sets to enable digital transformation and provide the following benefits to members and the public:



### Emerging ICT and Technology Transfer (161A)

Provides insights into emerging information and communication technologies and issues that could impact utility investments; also enables technology transfer to personnel who can use and benefit from it.



### DER Data and Connectivity (161D)

This project set provides resources related to the evolving needs for DER data and connectivity tools and technologies, architectures, methodologies, insights, and leading practices to support DER technologies integration.



### Enterprise Architecture and Integration (161E)

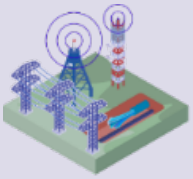
Four primary areas of focus include

1) Organizational Alignment,
2) Information Availability,
3) Application Portfolio Optimization, and
4) Enterprise Architecture (EA) Maturity.



### Advanced Metering Systems (161F)

Provides information and tools for the deployment of next-generation advanced metering systems while aiding utilities in optimizing existing system utilization and in discovering the full value of AMI-collected data.



### Telecommunications (161G)

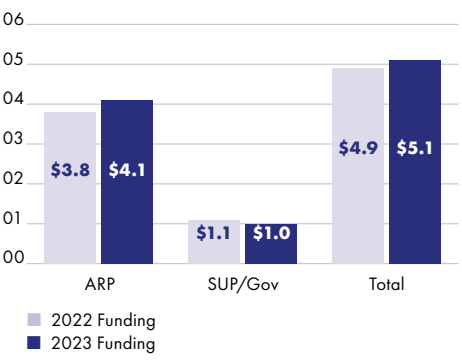
Provides insights, guidance, and tools to help utilities develop telecommunications strategies and apply emerging technologies and standards that play an increasingly critical role in the operation of the integrated grid.



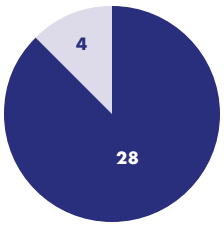
### Geospatial Informatics (GIS) (161H)

Provides leading practices for optimizing GIS system value and innovative uses of geospatial data in emerging applications such as augmented reality and digital twins.

**ICT (P161) Funding (in $ Millions)**




**2023 Utility Members**




| 2024 Staff | # |
|---|---|
| Tech | 15 |
| Admin | 2 |
| **Total** | **17** |

| Degree | # |
|---|---|
| PhD | 2 |
| Masters | 6 |
| Bachelors | 9 |



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

# Emerging Technologies and Technology Transfer (161A)

Designed to promote innovation by providing strategic insights into emerging information and communication technologies (ICT) that may drive radical change in the capabilities of the grid by enabling interoperability, pervasive telecommunications, and data-centricity. The project set also promotes technology transfer for the entire ICT program



## PROJECT

| | **2023** Accomplishments & Key Deliverables | **2024** Plan |
|---|---|---|
| Smart Grid Standards Tracking and Emerging Information and Communications Technology | The Summary of Interoperability Tracking and Reporting by the ICT Program in 2023 is a compiled list of "3rd Thursday" webcasts that included topics:<br>Summary of Interoperability Tracking and Reporting by the ICT Program in 2023 | 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 | The State of DER Interoperability - 2023 Edition summary of annual maturity study, monitoring changes in technical standards, best practices, utility programs, testing and certification program landscape, and the DER product landscape.<br>IT-OT Convergence: Why, When and How to Converge summarizes why IT-OT convergence is important to the utility industry, when it is best applied and presents strategies for how it can be achieved.<br>The Long Road to AMI Interoperability AMI interchangeability would mean that any meter could be substituted and different meters could still be used to send information to a head-end system using a different data format.<br>A Telecom Primer for Utility Industry Executives familiarizes readers with the issues surrounding telecom investment decisions to enable grid decarbonization and decentralization.<br>GIS Tools for Visualizing the Net Zero Grid Transition discusses GIS workflows that illustrate the vision for the Net Zero Grid of the Future.<br>The Invisible Network: Telecom's Vital Role in Power System Decarbonization<br>Strategic Alignment of Power System Telecom Modernization with Grid Decarbonization: The Invisible Network White Paper Series, Part 2<br>**Toolkit for Augmented Reality Rapid Prototyping (TARRP) –** Video **and** Technical Report<br>Leveraging the Standards in Formalizing EMS Alarms Data Structure<br>Artificial Intelligence for Distribution Analysis Using Advanced Metering Infrastructure Data | 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. Yearly Annual Reviews reviewing delivered results and future research for the following year. Example 2022-23 Area Review: Information, Communication and Cyber Security.<br>2023-24 Area Review: Information, Communication and Cyber Security (this document) | 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. |



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

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

This project set can help utilities at any stage of DER/DR deployment and integration. This includes industry leaders targeting full integration (control and monitoring) of both in-front and behind-the-meter DER/DR or utilities more focused on reducing costs and improving efficiency of existing operations, such as the monitoring and operation of large-scale storage or solar plants and DR programs. The project set has activities that support both the immediate future (existing plans) and longer-term (strategic vision) value streams.

This project set has three recurring areas of focus: Interoperability, Information, Protocol, and Connectivity Standards; Emerging Technologies; Integration Experiences and Practices.



| PROJECT | **2023** Accomplishments & Key Deliverables | **2024** Plan |
|---|---|---|
| DER Standards – Interoperability, Information, Protocol, and Connectivity Standards | **EPRI Protocol Reference Guidebook (PRG) – 7th Edition** summarizes the state of the art of 15 different information and protocol standards that support interoperability and interchangeability of DERs in the energy system. | **EPRI Protocol Reference Guidebook – 8th Edition** will provide an overview of communication protocols that allows readers to make 1:1 comparisons of specific aspects of information and protocol standards. New protocols are considered annually. |
| Emerging Topics, Technologies, and Techniques | **The ICTs Behind Group Management of DERs** explores protocols and practices for managed aggregated DERs through both ADMS-DERMS and Utility-Aggregator interfaces. | **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 conduct deeper research on one of two promising technologies to understand how these technologies support the industry, their maturity, and what is required for it to be successful. |
| Integration Experiences and Practices | **DER Interoperability Guidebook** received a new chapter on information interoperability in OT systems and how utilities can take advantage of this rising trend for DERs.<br>EPRI evaluated the state of DER interoperability testing and suggest **new best practices and expanded test procedures for enhanced interoperability** in the industry.<br>EPRI published **training materials** to prepare utilities for new products certified through UL1741SB/IEEE 1537-2018. | EPRI adds chapters annually to the DER Interoperability Guidebook to support utility DER adoption. Example topics include trends in industry mandates, validating interoperability, cloud-based architectures, telecommunication requirements for DERs, and preparing for IEEE 1547-2018.<br>EPRI will host DER Data and Connectivity task force meetings to help members stay up to date with the latest **Utility Experience in DER Integration.** |
| Technology Innovations | **DER Data Needs for 2030 Energy System** provides a summary of today's state of the art for DER interoperability, key barriers today, and EPRI's planned approach to proactively solve interoperability issues. | To be determined. |



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

# Enterprise Architecture and Integration (161E)

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




## PROJECT

Enterprise Architecture (EA)



Enterprise Systems Integration

## 2023 Accomplishments & Key Deliverables

**Utility Enterprise Architecture Guidebook, 8th Edition** - guidebook synthesizes information relevant to practitioners of enterprise architecture in the utility industry. Recent updates have included an overview of the "Shift Left" concept leading utilities are using to better engage business partners. The 8th edition includes updates on the use of the new common maturity model framework for capability assessments.

**Top Ten Indicators of EA Maturity: 2022 Survey Results** - The annual survey measures the evolution of the EA practice at utilities. The latest edition highlights the increasing adoption of enterprise class Enterprise and Business Architecture tools.

**LEAPWorx 4th Edition** - Re-usable elements and diagrams for enterprise and solution architects. The 4th edition includes diagrams used in DER and business architecture projects.

**Cloud Integration Guidebook: A Guide for Enterprise Architects, 7th Edition** – guides reader through concepts; considers cloud-based solutions from a variety of perspectives, technical, financial, and change management; how to evaluate any given solution for technical, business, and information risk.

**Common Information Model (CIM) Primer, 9th Edition** – annual update on how the CIM supports the additional requirements of the distribution domain.

## 2024 Plan

**Utility Enterprise Architecture Guidebook, 9th Edition** annual update with leading research from the EA discipline and best practices, lessons learned from utilities.

**Top Ten Indicators of EA Maturity: 2023 Survey Results** 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.

**Utility Business Capability Model 3rd Edition** updated with refinements from the latest round of applying the model to utility strategic initiatives.

**Business Capability Model Guidebook 3rd Edition** describes how to use the model for capability-based planning, roadmapping, investment optimization, portfolio rationalization, and more.

**IT-OT Convergence Guidebook 8th Edition** - Why, when, and how to converge functions from the IT and OT domains for more effective and efficient operations.

**Grid Modernization Playbook 6th Edition** – a joint deliverable between P200/P161 is a framework to help utilities develop strategies to meet the evolving requirements of a modern grid. Best practices and lessons learned from grid modernization strategy development and roadmap review at utilities.

**Cloud Integration Guidebook: A Guide for Enterprise Architects, 9th Edition** – describes how to utilize and connect to cloud-based services, securely utilize public clouds, and manage capital expenditures/operating expenses (CAPEX/OPEX) considerations.

**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.

**Enterprise Information Management (EIM) Maturity Model 2nd Edition** - Specifies maturity levels of the components of an Enterprise Information Management capability and a corresponding assessment.

*continued...*

*continued...*

# Enterprise Architecture and Integration (161E)




| PROJECT | **2023** Accomplishments & Key Deliverables | **2024** Plan |
|---|---|---|
| Organizational Alignment | **Aligning Information Technology and Operations Technology, Sixth Edition** details the benefits and approaches to IT-OT Convergence.<br>**Impacts of Disruptive Technologies 4th Edition** describes criteria and techniques for evaluating a disruptive technology.<br>**Business Capability Model Guidebook 2nd Edition** outlines how to create and use a business capability model for strategy development and execution, for IT and OT alignment and management. The second addition includes an overview of the new common maturity model framework and all level 2 diagrams from the 2023 model.<br>**EPRI Utility Business Capability Model 2023 Edition** is the latest edition of the model with significant updates in data management and DER management related capabilities. | **Utility Business Capability Model** a guide that contains extensions and refinements to the model learned through its application across EPRI and utility projects.<br>**Digital Transformation: Aligning Information Technology and Operations Technology, 6th Edition** explores the critical success factors, organizational maturity, and drivers of the convergence of information technology and operations technology.<br>**Impacts of Disruptive Technologies 4th Edition** defines a process for selecting and assessing the potential impact of modern technology to a utility.<br>**Business Capability Model Guidebook 2nd Edition** provides guidance for building and using a business capability model for strategy development, roadmapping and assessment.<br>**Grid Modernization Playbook** provides guidance on roadmapping for grid modernization. Joint deliverable with the Distribution Operations program. (joint deliverable with home program P200 Distribution Operations and Planning). |
| Technology Innovation | **Enhanced Grid Model Validation** Shapes Constraint Language (SHACL) Primer report discusses methodologies for data validation, specifically in the context of grid data, but generalizable to other domains.<br>**Digital Transformation Maturity Model Guide** describes what the maturity model is and how to use the model itself which is an attached spreadsheet to be filled out by interested parties.<br>**Impacts of Disruptive Technology: Organizational Structures and Resources** identifies how decisions regarding disruptive technology are primarily made. Evaluates maturity of organizational structure/processes to deal with rapid technology change. Identifies resources (people and technology) needed to integrate disruptive technology. | To be determined. |





# 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 | 2023 Accomplishments & Key Deliverables | 2024 Plan |
|---|---|---|
| Achieving Open, Interoperable Advanced Metering Systems | **Survey of Currently Used AMI Radiofrequency Protocols** is an investigation of the full stack of protocols currently used in RF-based AMI networks. | **DLMS/COSEM for North American Utilities** is a report on the use of the DLMS/COSEM metering protocols for use in North America. |
| Advanced Metering Systems Operations and Management | **Testing Requirements for AMI Meters** this report describes current requirements, from both business and regulatory aspects of meter accuracy testing and possible future trends. | **Introduction to DC Metering for Utilities** catalogs the current state of dc revenue metering, including use cases, equipment provider, relevant standards, and challenges/gaps in the industry. |
| Optimizing Advanced Metering System Value and Utilization | **Business Cases for Replacement AMI Systems** report enumerates and analyzes business cases for the replacement of entire AMI systems<br>**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. | **Continuous Meter Replacement in Heterogenous Systems** describes the future state of metering in which meters exist in heterogenous systems and where meter replacements do not require system replacement. |
| Technology Innovations | **High-speed Experimental Meter Front-end** is a mixed hardware and software prototype to experiment with waveform capture and compression techniques. | To be determined. |



**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

### Wide Area Networks

**2023** Accomplishments & Key Deliverables

**AFC Protection - Field Test Results** a detailed analysis of responses of AFC operators for locations of EPRI field tests and other paths with concerns. These results highlight potential discrepancies in the operation of the AFC systems.

**WAN Modernization Guidebook 2023 Edition** an annual guidebook update with a focus on packet-based technologies and increasing reliance on software, plus project execution challenges.

**Strategic Fiber Guidebook 2023 Edition** describes fundamentals of fiber technology, strategic opportunities for joint build and fiber sharing, update case studies.

**2024** Plan

**Evaluation of Interference to 6- GHz Microwave** 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

**WAN Modernization Guidebook 2024 Edition** Annual Guidebook Update

**Strategic Fiber Guidebook 2024 Edition** Annual Guidebook Update .

### Field / Neighborhood Area Networks

**Private LTE Guidebook – 2023 Edition** that includes a new chapter on network configuration and optimization to support low-latency use cases.

**Communication requirements for DER** is an analysis and test results of WI-SUN RF-Mesh networks and their ability to support the communications traffic resulting from DER use cases.

**Low-Latency Cellular Network Field Study** field testing results of latency performance of commercial LTE, 5G, and private LTE.

**Private LTE Guidebook – 2024 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 Low Latency Wireless technologies for Direct Transfer Trip** Ongoing evaluation of the development of wireless technologies leading up the availability of 5G Ultra-Reliable Low-Latency Communication (URLLC), including lab and field testing as technologies become available.

### Telecommunications Planning and Management Systems

**Network Management Guidebook** Telecom network management guidebook with a focus on the impact of network programmability and softwarization plus latest updates on network operation frameworks prevalent in the telecom industry.

**Satellite and Emergency Communication** – overview of new satellite technologies and their application to utility WAN augmentation and emergency backup. Test Plans for Starlink Evaluation are highlighted.

**Network Management Systems** Telecom network management guidebook with a focus on the impact of network function virtualization

**Resilient Networks with Islanded Operation Capability** Resilient networks with islanded operation capability evaluation – Field Demonstration Results

**Emergency/Black Sky Communications Resilience and Planning** is an update on best practices for ensuring communications availability in various scenarios, development of new standards and technologies for satellite, and longer-term test results.

*continued...*

*continued...*

# Telecommunications (161G)



| PROJECT | 2023 Accomplishments & Key Deliverables | 2024 Plan |
|---|---|---|
| Telecommunication Standards Engagement | **Telecom Standards Guidebook Vol 5** Insights and updates from active participation in telecom standardization. Many of the wide range of wired and wireless communications technologies that are deployed today, or may be deployed in the future, originate from the standards development activities that are covered in these reports.<br>**Smart Grid Communications Intelligencer 1H 2023**<br>**Smart Grid Communications Intelligencer 2H 2023**<br>The Intelligencer newsletters provide timely updates between the annual Telecom Standards Guidebook editions. | **Smart Grid Communications Intelligencer 1H 2024** biannual newsletter highlights issues of relevance and interest to utility communications engineers and managers.<br>**Telecom Standards Guidebook Vol 6** annual update of this guidebook incorporates previous work performed and adds individual utility policies and practices, including placeholders for future research results.<br>**Smart Grid Communications Intelligencer 2H 2024** 2nd issue for 2023. |
| Technology Innovations | **Communications and Connectivity Technology Newsletter, September 2023** This 13th issue highlights key insights technologies with a high potential for strategic impact on the electric utility industry. This issue focuses on emerging direction for 6G technology.<br>**Telecom the Nitrogen (part 1 of 2)** **and** **Strategic Alignment of Power System Telecom Modernization with Grid Decarbonization (part 2 of 2)** whitepapers for utility executives and regulators, that highlight the critical role of power system telecom in a decarbonized grid and argues for the need to strategically align the transformation of this infrastructure with that of the power grid.<br>**Evaluation of Amazon Sidewalk IOT** is an evaluation of the Amazon Sidewalk IoT network that is available across the US, considering appropriate utility applications and use cases where it could provide unique opportunities.<br>**Utility Owned Satellite Analysis** describes satellite solution alternatives pros and cons, innovative approach of shared private network to address the cons, innovative approach of shared private network to address the cons, feasibility analysis of the innovative approach.<br>**Mobile Base Stations** examines the current state of rapidly deployable types of mobile cellular communication systems as well as the feasibility of moveable base stations. In addition, it covers some challenges for deploying moveable cellular base stations. | To be determined. |



# Geospatial Informatics (161H)

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

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



| PROJECT | **2023** Accomplishments & Key Deliverables | **2024** Plan |
|---|---|---|
| Geospatial Informatics (GIS) Data Practices | **Geospatial Informatics Guidebook 4th Edition** this guidebook provides an industry resource for geospatial data practices and begin to lay the groundwork for the development of a maturity model for geospatial data management. The 2023 edition is available for the first time in a microsite format and as a PDF version. | **Geospatial Informatics Guidebook: Fifth Edition** is an interactive digital reference guide for best practices in geospatial data management, updated annually. |
| Geospatial Informatics (GIS) Innovation Engine | **Geospatial Applications and Management** is an overview of leading practices for leveraging geospatial technology with work management systems.<br>**Geospatial XR Demonstration** is intended to provide EPRI members with a high-level demonstration of how digital twins can be leveraged for managing utility assets. | **Geospatial Innovations** is an innovative applications leveraging GIS technologies within electric utilities. Geospatial digital twins, Augmented Reality, Virtual Reality, and Geospatial Artificial Intelligence. |
| Geospatial Informatics (GIS) Analytics and Visualization | **Modeling and Visualizing the Utility of the Future** a hypothetical utility proposal demonstrating the incremental investments needed to meet the challenge of increasing extreme weather events and the rapid migration to distributed energy resources. Story Map presentation that is stored on the EPRI organization page for ESRI ArcGIS online. | **Geospatial Analytics Use Cases** is an update to 2023 pilot demonstration extending geo-analytics into new use case areas. Delivered via interactive Web-based format (Story Maps). |
| Technology Innovations | **Digital Unique Identification of Specialized Equipment** Identity management across utility systems for AI, machine learning and digital twins.<br>**Geographic Hazard Zones for Utilities** is a Story Map presentation that is stored on ESRI ArcGIS online. | To be determined. |

# Examples of Member Application of Results

## Value Obtained

161A

### PECO, an Exelon Company

EPRI ICT Program – Emerging Technology and Technology Transfer Activities

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

161A

### American Electric Power (AEP)

"3rd Thursday of the Month" Emerging Technology Webcasts and ICT Program White Papers




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

161D

### Southern California Edison, Pacific Gas and Electric

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



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, PG&E 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.

161D

### New York Power Authority, Consumers Energy, North Carolina Electric Membership Corporation, Électricité de France, Salt River Project, Evergy, Southern Company, Exelon, Tennessee Valley Authority, KEPCO

Economically Feasible, Secure DER Network Gateways for Control Integration of Smart Inverters



Today, utilities are deploying DER management systems (DERMS) that intend to connect with DER, making them an integral part of system operations. However, this remains a challenge due to the revolving mix of DER types and capabilities that will be continuously interconnected and retired over time. Standardization efforts like IEEE 1547-2018 make the integration possible by specifying simple functions to the DER and leaving many utility-specific functions to the integration systems. The DER Gateway is designed to address these management-specific functions. It serves as a local platform housing features and logics important to the utility. It also performs several other important functions including translation of the DER's communication protocol to the protocol used in the communication network and enabling secure integration with utility operations.

The DER Gateway requirements document provides a reference set of requirements for DER gateways and is useful for utilities to develop RFPs. It covers a broad set of potential use cases of a DER gateway and can also be used by commercial entities to better understand market needs. Additionally, an IEEE standard 1547.10 for "Recommended Practices for DER Gateway Platforms" was also launched under EPRI leadership to reach various stakeholders to create a standard document for DER gateways.

# Examples of Member Application of Results

## Value Obtained

### 161E National Grid USA

Utility Business Capability Model for Investment Optimization

The Utility Business Capability Model is an important tool in the ability to perform strategic business capability-based planning—that is, planning that prioritizes a focus on capabilities that meet the stated strategic initiatives of a company.

National Grid led the advanced application in the capability-based planning domain both internally and with other project participants. The project owner led the impact of the business capability model across National Grid and inspired its application at other utilities. The recognition of the capability-based planning within National Grid and strategic initiatives is related to the National Grid utility of the future.




### 161F Exelon Family of Companies (PECO Energy Company (PECO) and Commonwealth Edison (ComEd)

Next Generation Metering Requirements

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 metering system, utilize alarms better, and utilize 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.




### 161F Consolidated Edison Company (ConEd)

Remote Operation of AMI meter disconnect in Natural Gas environment

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 end-use 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.

ConEd's electric franchise is coincident with the ConEd's NYC and Westchester Country natural gas franchise and National Grid's NYC natural gas franchise. The natural gas franchise operating areas have had instances of natural gas accumulating inside buildings from a multitude of reasons that include broken and leaking natural gas piping. For these events, the immediate elimination of electric power sources of ignition of the natural gas that accumulates in the building are paramount for the safety of building occupants, emergency responders, and the general public. ConEd has completed a system wide installation of Automated Metering Infrastructure (AMI), and electric meter AMI capability that includes the ability to remotely turn off the electric meter from ConEd's AMI Control Center. The EPRI project evaluated the risk of operating an AMI electric meter in an environment that contains a combustible concentration of natural gas and confirmed under the full range of electric meter operating amperages that turning off of an electric meter installed in a combustible gaseous environment does not serve as a source of ignition. The EPRI testing results are directly transferable by now providing remote electric meter turn-off for safety on events when natural gas accumulates inside a building thus avoiding the risk of fire and/or explosion from building electrical sources.



# Examples of Member Application of Results

## Value Obtained

### 161G Nebraska Public Power District

6GHz testing

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**



### 161G Salt River Project (SRP) and FirstEnergy

6GHz testing

**SRP:** This work has benefited SRP through mitigation of risk associated with potential interference around the 6GHz band. SRP has over 25 point to point microwave paths that utilize 6GHz spectrum which can now be used for lower power indoor devices for WiFi and eventually, standard power outdoor devices as well. Impacts to these microwave paths could impact the reliability of SRP's Wide Area Networks (WAN) which in turn could impact reliability of other services including SRP's ability to operate generation facilities.

**FirstEnergy:** The issue of interference to utility-owned licensed microwave links from unlicensed devices is ongoing and has many nuances. One open question was the potential for additive impact of many Wi-Fi networks operating in the vicinity of utility microwave links. This research conducted field testing and found a measurable additive impact effect on microwave links, which reduces their reliability. It provides the first quantitative test data to counter simulation studies that claimed additive interference would not occur.

**SRP:** Additional understanding of the risk was gained which allowed SRP to proactively produce a plan to help mitigate that risk.
**FirstEnergy:** The research provides data to quantify the impact of multiple unlicensed devices to utility communications systems. EPRI and FirstEnergy worked together to conduct real-world testing with multiple unlicensed networks to provide the first utility testing and impact analysis of the additive contribution to interference. Utilities can utilize this knowledge of increasing interference when 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, and how to prioritize microwave upgrades, re-banding, and fiber replacement projects.



### 161H Salt River Project

Data Quality Project Case Study

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.



# Supplementals and Project and Contact Information

## Applied Grid Model Data Management (GMDM) for Distribution and Transmission

The objective of the Applied Grid Model Data Management (GMDM) project is to help a utility apply the data management architecture developed by EPRI's Grid Model Data Management research. The AGMDM project will analyze a utility's requirements and develop strategies for integrated grid model management that will enable faster and more seamless model updates across multiple utility business domains.



**Sean Crimmins** • 865.227.1991 • scrimmins@epri.com

Scan QR code for GMDM for Distribution

Scan QR code for GMDM for Transmission

## Business Capability-based Investment Optimization (BCM Phase II)

Strategic objectives often do not align with where the dollars end up being spent. Firefighting, local challenges and strong personalities can draw attention away from the long-term goals of the organization. It is important to create a clear connection between strategic objectives and the investments undertaken.




**Sean Crimmins** • 865.227.1991 • scrimmins@epri.com

Scan QR code for two-page summary of project

## Enhanced Surveillance Over Wireless

The project objectives are to evaluate systems and solutions for supporting physical security video over bandwidth-constrained communications networks. In addition to conventional video compression technology the project will examine innovative event-based sensors that enable motion reduction.



**Tim Godfrey** • 650.855.8584 • tgodfrey@epri.com

Scan QR code for two-page summary of project

# Supplementals and Project and Contact Information



## Enterprise Architecture Maturity Assessment

Benefit Enterprise Architecture teams at utilities to address gaps in EA as Strategy, the Business-IT relationship and business architecture. It is a direct result of two deliverables that are updated each year:

**1. Top Ten Indicators of Enterprise Architecture Maturity**
A survey of questions to uncover the maturity level at a utility and collects attributes of a mature EA practice at utilities and industry at large, ranked in a maturity model format.

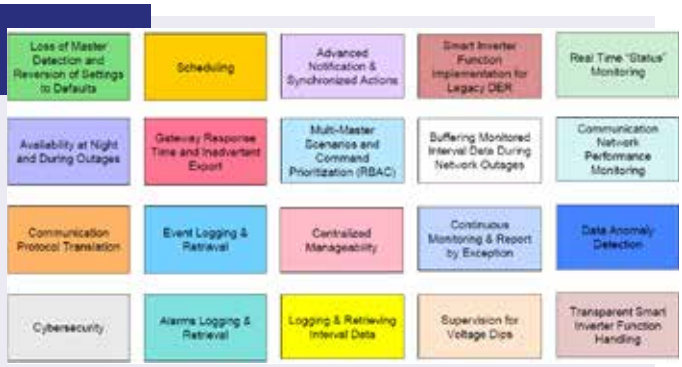
**2. The Utility Enterprise Architecture Guidebook**
This guidebook seeks to address a gap between reading a leading enterprise architecture reference such as The Open Group Architecture Framework (TOGAF) and being able to apply it.

**Sean Crimmins** • 865.227.1991 • scrimmins@epri.com

Scan QR code for two-page summary of project

## Evaluation and Economic Feasibility Analysis of Commercial DER Gateways – Phase II

The initial project addressed some of the gaps in the first phase (2021-2022) by developing technical requirements and documenting specifications and produced an open-source reference implementation of a gateway, however focused only on solar-type DER. With renewed focus on integrating energy storage and solar plus storage type DER, the second phase of this project will be tasked to address this gap.




**Ben Ealey** • 865.218.5938 • bealey@epri.com
**Xavier Francia** • 650.855.2883 • xfrancia@epri.com
**Ajit Renjit** • 614.620.3154 • arenjit@epri.com

Scan QR code for two-page summary of project

## Evaluation of Automated GIS Data Cleanup Methods

This project attempts to examine emerging technologies and methodologies to automate GIS data cleanup and asset inventorying. The project will evaluate multiple data collection approaches such as:

- Street Vehicle-based mobile mapping
- Aerial Vehicle-based mobile mapping
- Satellite-based mapping



**Kevin Gorham** • 704.595.2397 • kgorham@epri.com

Scan QR code for two-page summary of project

# Supplementals and Project and Contact Information

## Field Asset Unique Identification System

Tracking of electric grid (transmission and distribution) assets, especially field assets across their lifecycle (cradle to grave) has become more important over the past several decades. QR Code coupled with industry consensus catalog ID would form the necessary asset make/model and configuration information, to create a unique identifier for all electric grid assets.



**Kevin Gorham** • 704.595.2397 • kgorham@epri.com
**Sean Crimmins** • 865.227.1991 • scrimmins@epri.com

Scan QR code for two-page summary of project

## Grid Model Data Management (GMDM) Vendor Forum Phase II: An EPRI-Sponsored Vendor-Funded Collaborative Initiative

EPRI's Distribution Grid Model Data Management project is defining functional capabilities for managing network models. To support future success of this effort, EPRI wants to engage vendors of distribution domain software products that supply, manage, or consume grid model data in the conversation.



**Sean Crimmins** • 865.227.1991 • scrimmins@epri.com
**Varun Perumalla** • 650.855.1051 • vperumalla@epri.com

Scan QR code for two-page summary of project

## Grid Model Data Management Interest Group

While Grid Model Manager applications have been deployed by transmission operators; distribution operators and the vendor community are racing to meet the rapidly evolving need for accurate, detailed models of the current and future distribution grid to enable the many kinds of power flow analysis.



**Sean Crimmins** • 865.227.1991 • scrimmins@epri.com
**Varun Perumalla** • 650.855.1051 • vperumalla@epri.com

Scan QR code for two-page summary of project

# Supplementals and Project and Contact Information

## Next Generation Metering – Distributed Intelligence

Multiple meter vendors are now touting the benefits of the ability of new devices to accommodate the development, testing and distribution of applications that can be created and downloaded to meters. Other vendors claim that there is no real benefit in doing so, and that centralized data processing is a superior model in all cases. These are obviously diametrically opposed viewpoints, that independent and objective EPRI research can help resolve. The purpose for this research is to investigate use cases to which distributed intelligence might be put, to understand the process by which the development, testing, deployment, and retirement of applications can be done in the current environment.

**Ed Beroset** • 919.901.2652 • eberoset@epri.com



Scan QR code for two-page summary of project

## Next Generation Wireless Local Area Network (WLAN)

Wireless LAN technology has made significant advancements with the completion of Wi-Fi™ 6 (IEEE 802.11ax), and Wi-Fi™ 7 (IEEE 802.11be) nearing completion. These include the latest security standard, WPA3, and new Wi-Fi Location capabilities. For existing and emerging wireless use cases, this next generation WLAN offers a significant improvement. Capabilities can match/exceed 5G in most aspects and at lower cost. While Wi-Fi 6 provides notable improvements in data throughput, the most significant advancements are improvements in efficiency. It enables new utility use cases, from wireless sensors to augmented/virtual reality (AR/VR), delivers value in the generation plant, in the substation, and across the enterprise.

**Tim Godfrey** • 650.855.8584 • tgodfrey@epri.com




Scan QR code for two-page summary of project

# Supplementals and Project and Contact Information

## Utility Digital Worker Collaborative

Digital Worker is defined as "integrating technology and applications to provide field and plant workers with the information and capability to perform their jobs safer and more effectively." This cross-sector project focuses on performing case studies to accelerate understanding opportunities and challenges of emerging technologies for digital workers including smart phones, head-worn devices, wearable computers, mobile applications, augmented and virtual reality, autonomous data gathering, artificial intelligence, location mapping, computer vision, drones, robotics, and other emerging technologies.

**Julia Uhr** • 972.556.6556 • juhr@epri.com



Scan QR code for two-page summary of project

## Utility Integration with Third-Party DER Aggregators

Given the expected growth of distributed energy resources (DER), including generation, storage, and manageable load, some type of visibility and control of these devices will be needed. There are a growing number of commercial entities offering systems and services in this area (often referred to as a type of third-party DER management system or DERMS). In some instances, integrating with third parties may be desirable due to economics, a lack of available utility communication infrastructure, a need for more flexible business plans, and the general difficulty of customer engagement and acquisition.

**Brian Seal** • 865.456.3586 • bseal@epri.com
**Ajit Renjit** • 614.620.3154 • arenjit@epri.com



Scan QR code for two-page summary of project

# Information, Communication Technology (ICT) Guidebooks 2023

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:** Applied Information and Communication Technology for Distributed Energy Resources (DER) Data and Connectivity | PID# | YEAR |
|---|---|---|
| DER Interoperability Guidebook | 3002026700 | 2023 |
| EPRI Protocol Reference Guidebook – 7th Edition | 3002026697 | 2023 |
| IoT Technologies for Distributed Energy Resources – 2023 Guidebook: Information, Case Studies, and Lab Evaluations of IoT-Based Connectivity, Distributed Messaging, and Integrated Platform-As-A-Service Solutions | 3002026699 | 2023 |
| 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 (see QR code on page 23) | 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 |
|---|---|---|
| Cloud Integration Guidebook: A Guide for Enterprise Architects, 7th Edition | 3002026851 | 2023 |
| Common Information Model (CIM) Primer, 9th Edition (see QR code on page 23) | 3002026852 | 2023 |
| Digital Transformation: Aligning Information Technology and Operations Technology, 6th Edition | 3002026853 | 2023 |
| Impacts of Disruptive Technologies 4th | 3002026854 | 2023 |
| Utility Enterprise Architecture Guidebook, 8th Edition | 3002026848 | 2023 |
| Utility Business Capability Model Guidebook 2nd Edition | 3002028279 | 2023 |
| 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 |

*continued...*

# Information, Communication Technology (ICT) Guidebooks 2023 *continued...*

| **161F:** Advanced Metering Systems | PID# | YEAR |
|---|---|---|
| Advanced Metering Data Analytics Guidebook (see QR code on page 23) | **3002026784** | **2023** |
| 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** |
| Advanced Metering Infrastructure (AMI) Reference Architecture | **3002021854** | **2021** |
| 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 |
|---|---|---|
| Network Management Systems Guidebook | **3002027107** | **2023** |
| Private LTE Guidebook – 2023 Edition | **3002027090** | **2023** |
| Strategic Fiber Guidebook 2023 Edition | **3002027080** | **2023** |
| Telecom Standards Guidebook Vol 5 (see QR code on page 23) | **3002027156** | **2023** |
| WAN Modernization Guidebook 2023 Edition | **3002027068** | **2023** |
| 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** |

*continued...*

# Information, Communication Technology (ICT) Guidebooks 2023 *continued...*

| **161H:** Geospatial Informatics | PID# | YEAR |
|---|---|---|
| Geospatial Informatics Guidebook 4th Edition (quick access via QR code below) | **3002026827** | **2023** |
| 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** |

**DER Protocol Reference Guidebook 5th Edition Public Version (161D)**

**Common Information Model (CIM) Primer 9th Edition (161E)**

**Guidebook for AMI Data Analytics 2nd Edition (161F)**

**Telecommunication Standards Guidebook V5 2023 (161G)**

**Geospatial Informatics Guidebook 4th Edition (161H)**

## What Cyber Security for Energy Delivery and Customer Solutions (ED&CS) 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. Specifically, measures 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.

EPRI's cyber security program focuses on addressing the emerging threats to an interconnected electric sector through multidisciplinary, collaborative research on cyber security technologies, standards, and business processes.

**Collaboration:** Track industry and government activities and provide technical contributions to key working groups.



**Incident Management:** Improve the electric sector's ability to scan for devices and vulnerabilities in OT areas and better understand the true risks associated with those activities.

**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.



**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.



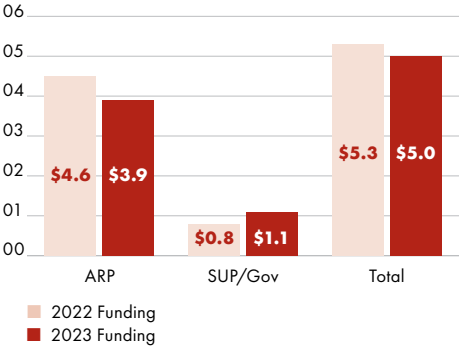
**DER Technologies:** Provide guidelines for deploying intrusion detection and prevention technologies (IDS/IPS) with DER systems. Develop security reference architectures for microgrids with a focus on the integration of community microgrids.

**Data Applications:** Develop additional cyber security metrics, including resiliency metrics. Support metrics adoption and enabling benchmarks of relevant cyber security program performance. Develop data management strategies and strategies for utilizing machine learning and artificial intelligence.

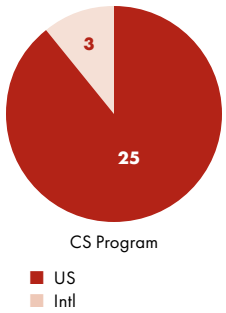


**Cyber Security Roadmap for 2030** identifies the critical future states for Cyber Security in the electricity subsector and the action plans that must be adopted to achieve intrinsic Cyber Security.

**CS (P183) Funding (in $ Millions)**




**2024 Members**




| 2024 Staff | # |
|---|---|
| Tech | 15 |
| Admin | 2 |
| **Total** | **17** |

| Degree | # |
|---|---|
| Masters | 8 |
| Bachelors | 8 |



**Ben Sooter,**
Program Manager,
*bsooter@epri.com*

# Strategic Intelligence and Emerging Issues (183A) **(NEW for 2024)**

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.




## PROJECT

**P183.021**
Strategic Intelligence andf Emerging Issues

Ben Sooter
*bsooter@epri.com*

## 2023 Accomplishments & Key Deliverables

**New project set for 2024**.

Post Quantum Cryptography in Operational Technology

De-Risking Cyber Insurance for Utilities – Video and Presentation and White Paper

Quantum Science and Technology: Energy System Applications and Future Opportunities

Quantum Challenge Results: Quantum Technologies for AI-Enhanced Utility Cybersecurity

Cyber Security Operations Security (OPSEC) Awareness Posters

Cyber Security Platform and Certification Framework Development for Extreme Fast Charging (XFC)-Integrated Charging Ecosystem

## 2024 Plan

- Building OT Cyber Security Program Roadmaps describes how to build a roadmap for an OT cyber security program at an electric utility.
- Emerging Issues in Incident and Threat Management (IMTM) highlights emerging issues in the IMTM space.
- Emerging Issues in Cyber Security for Transmission and Distribution highlights emerging issues in the T&D space.
- Emerging Issues in Cyber Security for DER and Grid Edge Systems highlights emerging issues in the T&D space.
- Emerging Issues in Cyber Security Data Applications (183E) highlights emerging issues in the DER and grid edge space.

**P183.022**
Security Newsletters

Erica Loveday
*egloveday@epri.com*

**In 2023 - Industry Collaboration** 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**

The EPRI Cyber Security Program provides email updates to program members 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 updates.

P183 Cyber Security Newsletter Compendium is a public summary Public Summary of 2024 Newsletters.



**Ben Sooter,**
Program Manager,
*bsooter@epri.com*

# Incident and Threat Management (183B)

The objective of the Incident and Threat Management Project is to develop a comprehensive approach to cybersecurity that encompasses incident management, threat management, and forensics. This project aims to enhance utilities' and organizations' ability to detect, analyze, respond to, and recover from cyber security events; manage and mitigate cyber threats; and conduct in-depth forensic analysis of industrial control systems (ICS) devices.



## PROJECT

### Incident Management

Ben Sooter
*bsooter@epri.com*

## 2023 Accomplishments & Key Deliverables

**The Integrated Security Operations Center (ISOC) Guidebook** provides comprehensive guidance based on past EPRI research from 2013 to 2022. In addition, it draws upon contributions from five electric power utilities that are members of the EPRI Cyber Security Research Program and have implemented the ISOC as part of their cyber security program. EPRI conducted in-depth interviews with the five utilities to determine best practices and lessons learned for planning, designing, implementing, and operating an ISOC.

## 2024 Plan

**The ISOC Guidebook 2024** update that will include 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.

This project can help improve the following incident response capabilities for power delivery systems:

- Incident containment
- Reducing operational impact to the power system
- Identification and measurement of holistic impact

### Threat Management

Ben Sooter
*bsooter@epri.com*

**Threat Management Guidebook 2023 Update** provides comprehensive guidance based on past EPRI research from 2017 to 2022. The guidebook will be updated annually to reflect changes in technology and best practices and to include new EPRI research related to threat management.

**Threat Management Guidebook 2024 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.

### Cyber Security Forensics

William Webb
*wwebb@epri.com*

**Forensics Field Guide: SEL 421 Protection Relay** provides a step-by-step approach on how to collect forensics-relevant data from a SEL-421 protection relay in support of a cyber incident response investigation.

**Forensics Field Guide 2024** 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.



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

# Cyber Security for Transmission and Distribution (183C)

The objective of the Cybersecurity for Transmission & Distribution Systems Project is to collaboratively develop security strategies for critical T&D systems. As the industry transitions toward more intelligent grid monitoring and control systems, the utility attack surface expands and emerging risks must be mitigated. Conventional enterprise security practices may not be appropriate for the operations technology environment, so this task force leverages domain expertise from multiple perspectives to minimize cyber risk without negatively impacting other objectives.



## PROJECT

### Cyber Security for Substations and Field Devices

John Stewart
*jstewart@epri.com*

## 2023 Accomplishments & Key Deliverables

The **Substation Security Guidebook** is a collection of findings and recommendations for utility personnel who are focused on the security of T&D substations and field systems. These facilities typically contain a range of critical systems that have been engineered to respond to events in a predictable and reliable manner. The potential impacts of any security controls deployed in that environment should be well understood prior to commissioning. Utility engineers select equipment from multiple vendors to integrate into the utility's monitoring and control systems. Since each individual device is a proprietary hardware/software platform the specific techniques for monitoring and management a given device may vary widely. These device-specific limitations and characteristics must be factored into an effective substation security program.

## 2024 Plan

**Multi-Vendor Secure Management Framework** project leverages lessons learned from community-developed management tools from the home automation industry to explore potential solutions for utility engineers tasked with the security of critical systems. This effort will propose an industry framework to support the integrated management of security controls spread across various systems in a multi-vendor substation environment.

**Cyber Security for Digital Substations** is a revised exploration of new substation architectures and emerging cyber security needs. The adoption of new substation protection and control standards such as IEC-61850 presents a range of new cyber security and compliance challenges. As substation design practices shift away from analog wiring towards network coordination, new security controls must be developed to ensure reliable operation of critical systems. This project will focus on practical approaches to these emerging security issues associated with digital substations.

### Cyber Security for Control Centers

John Stewart
*jstewart@epri.com*

**Integrating Security in the T&D Lifecycle** documents industry efforts to shift from the use of "bolt-on" security solutions and toward controls that are deeply embedded in the utility infrastructure lifecycle. In the past, early utility efforts were focused on the security of existing grid monitoring and control systems. As security programs have matured, security discussions should be introduced as early as possible in the project planning process. To address these concerns EPRI has coordinated with NERC and IEEE on the Security Integration Working Group to develop recommendations for utilities to integrate security objectives into planning, design, operations and maintenance workflows. This deliverable provides guidance for utilities who are focused on deeply embedding security into their infrastructure lifecycle.

**All-Hazard Risk Assessment of T&D Systems** This report will define a framework and methodology to create a detailed grid infrastructure model that can be used to assess alternative cyber security approaches. While many utilities rely on power system modeling to prepare for potential grid scenarios or events, these models are primarily focused on representing the flow of power. To fully understand the security implications of different scenarios or events a more detailed understanding of all three major grid layers is required (power, controls, communications). This project will explore the potential for modeling and simulation of each layer as well as dependencies between layers.



# 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-grid technologies. The project set will provide electric utilities with a robust set of risk narratives, frameworks, engineering guidelines, tools, and reference architectures to safeguard their grid systems and ensure secure communications and interoperability with distributed energy resources (DER).

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



## PROJECT

Cyber Security for DER Integration and Management (CSDIM)

Xavier Francia
*xfrancia@epri.com*

### **2023** Accomplishments & Key Deliverables

**Distributed Energy Resources (DER) Cyber Security Guidebook for Utility Architects and Engineers, 3rd Edition**

The DER Cyber Security Guidebook 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. The 3rd Edition update includes cyber security guidance related to connected community integrations, as well as updates to emerging cyber security standards and certifications for DER systems.

### **2024** Plan

**Distributed Energy Resources (DER) Cyber Security Guidebook for Utility Architects and Engineers, 4th Edition**

With the recent publication of the IEEE 1547.3 Cyber Security Guidance for DER Systems, the 4th edition of the guidebook will include 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 will also include expanded guidance related to electric vehicle integration, as well as utility considerations for developing a cyber security for DER strategy.

Cyber Security for DER Technologies (CSDT)

Sai Ram Ganti
*sganti@epri.com*

**Threat Monitoring Guidance for DER Systems, 2nd Edition**

This guide 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 WAF technologies and IEEE 1547 DER Integration Data Models supported by DNP3, Modbus, and IEEE 2030.5/SEP2.

**Cybersecurity Requirements for Utility-Owned Energy Storage Systems, 2nd Edition**

The 2nd Edition will include updated requirements for utility-owned energy storage systems (ESS), including a risk-decision framework for selecting appropriately commensurate security controls for utility ESS projects as well as for third-party ESS integrating with utility electric delivery systems. The update will also include ESS archetypes and their associated cyber security reference architectures and requirements.



# Cyber Security Data Applications (183E)

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

**Christine Hertzog,**
Principal Technical Leader,
*chertzog@epri.com*



| PROJECT | 2023 Accomplishments & Key Deliverables | 2024 Plan |
|---|---|---|
| Cyber Security Data Foundations/Cyber Security Data Applications<br>Christine Hertzog<br>*chertzog@epri.com* | **OT Cyber Security Data Management Guide V1**<br>This guidebook helps develop forward-thinking approaches to managing data used for cyber security situational awareness.<br>**OT Cyber Security Resiliency Metrics V2**<br>The research identifies metrics that can help quantify the cyber resiliency and data resiliency postures. Cyber resiliency metrics may improve cyber security postures and programs.<br>**Benchmarking Utility Cyber Security**<br>This document explains the value of benchmarks in strategic decisions.<br>**Utility Cyber Security and Artificial Intelligence Challenges and Opportunities**<br>This deliverable identifies major challenges to secure AI data and platforms and leverage AI for defensive security postures. | **OT Cyber Security Data Management Guide V2** provides recommendations for OT cyber security data management to help utilities prepare for AI-enabled applications.<br>**OT Cyber Security Resiliency Metrics V3** continues research into data points, systems, and formulas to calculate resiliency.<br>**Machine Learning Applications for OT Cyber Security Operations V1** documents knowledge and experiences with commercially available and custom machine learning tools for utility use cases. |
| Cyber Security Assessments<br>Christine Hertzog<br>*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<br>Christine Hertzog<br>*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. | Develop new instructor-led and lab-based courses and CBTs based on utility needs in topics such as IEC 61850 and equipment familiarization. |

# Examples of Member Application of Results

## Incident and Threat Management

## Value Obtained

### Xcel Energy

Staff Benefits from Remote Cyber Security Operational Technology Equipment Familiarization Course

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**

### 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

Industrial Control Systems Automated Digital Forensics Harvester

With the rapidly changing cyber security threat, the ability to collect critical forensics artifacts quickly and accurately from Industrial control systems (ICS) devices in operational technology (OT) environment is a crucial component in an organization's incident response process. The analysis of such forensics data may help investigators identify the mechanisms by which one or more devices became compromised along with the attack vectors that were used to compromise these devices. The embedded nature of the majority of ICS devices, which often function in custom operating systems, can make it difficult to perform these analyses. In this project, the team successfully developed an automated forensics collection tool to enable routine and automated collection of critical forensic artifacts earlier in the incident response process.



This research effort developed a unique forensics harvester tool that allows utility employees to extract important forensics information from a device in real time. The harvester communications protocol is an extension of an existing and supported communications protocol and is demonstrated to be an effective method of interacting with a device.

The harvester, in addition to its protocol and the method by which data received is stored in a logical and structured format, accomplishes the project's primary goals of supporting forensics automation.

A NYSERDA funded project, the harvester prototype has been released as an open-source tool to encourage product manufacturers to incorporate and to provide forensics collection capabilities to end users in the industry.

The harvester prototype developed in this project is well-suited for future research extensions -
(1) to be integrated in security orchestration and automation (SOAR) tools,
(2) to continuously monitor devices for potentially malicious activities
(3) to support automated threat detection and, perhaps in the future,
(4) for supporting automated threat mitigation.

# Examples of Member Application of Results

## Cyber Security for Transmission and Distribution Operations and Systems

### Southern Company

Dedicated Power Delivery Cybersecurity Program (PD CSP)

Operational technology cybersecurity programs are a critical piece of the protection of electric utility networks. Southern has a dedicated Power Delivery Cybersecurity Program (PD CSP) that focuses on securing many of their OT networks. Southern' s PD CSP partnered with EPRI to update and extend their program strategy and have rolled out those changes with great success. Implementing a robust power delivery cybersecurity program provides a crucial shield against potentially crippling cyber attacks, ensuring the continuous, efficient, and secure operation of essential utility services. Ultimately, these measures contribute to business continuity, customer trust, and the overall resilience of the national infrastructure against evolving cybersecurity threats.

### Value Obtained



PD CSP's updated strategy is setting new standards for the industry. Its comprehensive and multi-faceted approach to cybersecurity not only fortifies their systems but also instills a culture of proactive vigilance, aligning with industry best practices. The enhanced support provided to their customer base has considerably increased customer satisfaction and trust, reinforcing their reputation as a reliable and secure partner.

This strategy's popularity is not just confined within Southern; it's also influencing the cybersecurity landscape in the energy sector at large. Other cybersecurity programs at Southern are adopting similar models, acknowledging the value derived from the streamlined, cost-effective, and comprehensive structure of the PD CSP. This is a testament to the effectiveness and innovation of their program, leading the way in corporate cybersecurity strategies. Furthermore, the emphasis on regular communication, including quarterly updates and executive messaging, fosters a transparent environment that keeps stakeholders informed about progress and developments. This practice strengthens relationships with partners and stakeholders, enhancing trust and collaboration across the board.

The commitment to internal and external engagement, as seen in the adoption of advanced technologies and collaborations with commercial and governmental organizations, further amplifies the impact of the PD CSP. This approach keeps Southern at the forefront of cybersecurity trends, ensuring they are well-equipped to navigate and respond to an ever-evolving landscape of threats.

Lastly, the PD CSP's focus on modernizing legacy systems and supporting digital transformation processes positions Southern as a pioneer in the energy sector's digital age. This not only enables them to maintain a competitive edge but also allows them to make significant contributions to the broader industry and society. By securing advanced digital systems and distributed energy resources, they are helping to ensure the safety and reliability of future energy infrastructures.

Overall, the new strategy for the Power Delivery Cybersecurity Program at Southern is revolutionizing their cybersecurity approach, bringing substantial benefits to their customers, stakeholders, and the broader energy industry.

## Cyber Security for DER and Grid-Edge Systems

### Korea Electric Power Company (KEPCO)

Cybersecurity for KEPCO's Distributed Energy Resource (DER) Integration Architectures

DER integration presents a major paradigm shift in grid operations and the architectures of a utility's grid communication system. As energy systems shifts towards more decentralized architectures with higher reliance on distributed sources, cyber risks, security implementation challenges, and architectures must all be considered to ensure a safe and reliable DER-dependent grid. KEPCO is one of the first utilities to holistically review EPRI's cybersecurity guidelines for DER integration to determine what security strategies can be applied towards KEPCO's DER architectures that achieve end-to-end secure communications across a hostile threat landscape. During the project, KEPCO and EPRI researchers of P183 teamed together to provide one of the first case-studies for DER cybersecurity architectures, providing significant techn transfer value for other utilities facing similar challenges.

### Value Obtained



Strong cybersecurity practices underpins every facet of a utility's business, and these practices are especially important for realizing the strategic objectives for grid modernization. KEPCO utilized EPRI's cyber security research to develop secure reference architectures and strategies to prepare them for an emerging grid with extensive DER integration. The public benefit of this project includes providing the industry with a case-study of how pro-active approaches, as outlined by EPRI's DER cyber security guidelines, can help ensure that a utility's cyber security program and developed grid architectures can be strategically ready to support integration of DERs. By addressing cyber security through by-design approaches, as KEPCO has done, utilities and their DER projects are better positioned to protect themselves from cyber-attacks that could disrupt the flow of electricity to the public.

# Examples of Member Application of Results

| Cyber Security Data 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.



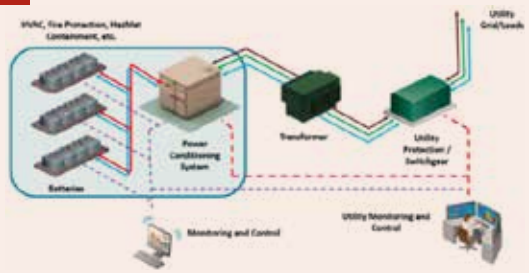

EPRI identified recommendations to improve NYPA's cyber security program. These recommendations were specific, rated by priority, and given estimated timeframes for completion. NYPA tailored the recommendations to meet internal security goals and incorporate them into work plans. In addition to the recommendations, 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.

# Supplementals and Status

## Cyber Security Decision Framework for Utility-Scale Energy Storage Systems

As more utility-scaled energy storage systems (ESS) are utilized for grid support, their reliance on digital components and off-site analytics raise cyber security concerns. This supplemental project opportunity will investigate security risks related to energy storage and the impact to grid operations, identify mitigation approaches for security hazards and develop decision framework for utilities to prioritize mitigation related to energy storage cyber security risks.



**Sai Ram Ganti** • 650.269.6799 • sganti@epri.com

Scan QR code for two-page summary of project

## Cyber Security Incident Response and Recovery Tabletop Exercise

It is critical for utilities to continually evaluate and exercise their capabilities to effectively respond to cyber security events in their operational environments to determine if their processes satisfy detection, response, and recovery requirements. With the increased inclusion of and dependence on processor-based power delivery and communications infrastructure, the potential for attacks by malevolent cyber agents also increases. In addition, NERC CIP-008 and CIP-009 require utilities to test their Incident Response and Recovery plans. This project provides tailored tabletop exercises to utilities to exercise their incident response plans and identify areas for improvement.



**Ben Sooter** • 865.218.8108 • bsooter@epri.com

Scan QR code for two-page summary of project

## Cyber Security Operational Technology Equipment Familiarization Course

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



**William Webb** • 865.218.8132 • wwebb@epri.com

Scan QR code for two-page summary of project

# Supplementals and Status

## Cyber Security Program Assessment for Utility Transmission and Distribution Operations

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



**Christine Hertzog** • 650.314.8111 • chertzog@epri.com

Scan QR code for two-page summary of project

## Cyberjoule™ Platform Implementation for Utility Cyber Security Metrics

This supplemental project aids utilities in designing and deploying cyber security metrics to quantitatively measure performance of their cyber security program. It leverages EPRI's experience in metrics development and implementation to avoid common project pitfalls and accelerate the benefits of cyber security metrics.




**Christine Hertzog** • 650.314.8111 • chertzog@epri.com

Scan QR code for two-page summary of project

## Evaluation and Economic Feasibility Analysis of Commercial DER Gateways

The initial project addressed some of the gaps in the first phase (2021-2022) by developing technical requirements and documenting specifications and produced an open-source reference implementation of a gateway, however focused only on solar-type DER. With renewed focus on integrating energy storage and solar plus storage type DER, the second phase of this project will be tasked to address this gap.




**Ben Ealey** • 865.218.5938 • bealey@epri.com
**Xavier Francia** • 650.855.2883 • xfrancia@epri.com
**Ajit Renjit** • 614.620.3154 • arenjit@epri.com

Scan QR code for two-page summary of project

# Supplementals and Status

## Integrated Cyber-Physical Security for Distribution Automation

It is critical that utilities protect their assets from both cyber and physical security threats, including remote monitoring and control locations throughout the distribution system. This includes the ever-increasing addition of distribution automation equipment such as reclosers. EPRI has developed a prototype cyber-physical security system that uses low-cost sensors in conjunction with state-of-the-art security orchestration platform and facial recognition to facilitate the detection of physical security threats in real time and provide options to mitigate potential cyber security threats. This platform has been developed over a two-year period in EPRI's laboratories and is available for utilities to evaluate the capabilities and benefits of having both cyber and physical security for distribution field equipment.

**William Webb** • 865.218.8132 • wwebb@epri.com




Scan QR code for two-page summary of project

## OT Cyber Risk Assessments for Transmission and Distribution Operations

Use EPRI experts to examine utility risk management consideration of threats and cyber security mitigations and quantify the likelihood and impacts of existing and emerging threats in reputational, environmental, financial, safety and operational categories.

A comprehensive understanding of all cyber risks enhances utility decision-making about investments and prioritization of controls to effectively manage risk, appropriately protect utility infrastructure, and avoid potential threat impacts.

**Christine Hertzog** • 650.314.8111 • chertzog@epri.com



Scan QR code for two-page summary of project

# Supplementals and Status

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

Use EPRI experts to examine specific areas of your cyber security program such as transient cyber asset management, remote access, engineering design process, or a customized assessment scope. Results include recommendations for improvements with suggested goals, plans, and timelines.



**Christine Hertzog** • 650.314.8111 • chertzog@epri.com

Scan QR code for two-page summary of project

## Responding to High Impact Cyber Security Events (RHISE)

With ransomware perpetrators carrying out over 4,000 attacks daily, companies of all shapes and sizes are being significantly affected by this new scourge of malware. Critical infrastructure appears to be targeted more than ever before as ransomware groups recognize the pressure these organizations feel to recover from attacks as fast as possible. This project aims to improve the response and recovery capabilities of participating utilities when dealing with a cyber incident that potentially affects operations.



**Ben Sooter** • 865.218.8108 • bsooter@epri.com

Scan QR code for two-page summary of project

# Supplementals and Status

## Utility Red Team Collaborative

In the ever-evolving realm of cyber threats, electric utilities find themselves at the crossroads of technological advancement and increasing vulnerabilities. This project aims to leverage a Red Team Collaborative approach to provide read team services to the electric industry. By simulating genuine cyber threats in a controlled environment, these assessments will provide utilities with an unparalleled perspective into their existing vulnerabilities, response mechanisms, and recovery protocols.

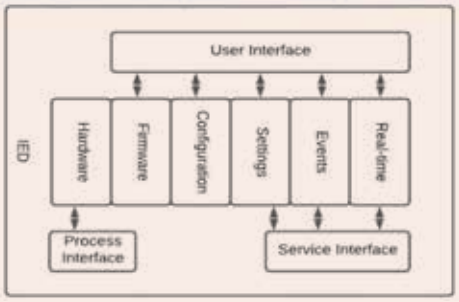



**Ben Sooter** • 865.218.8108 • bsooter@epri.com

Scan QR code for two-page summary of project

## Secure IED Management Strategies

This project will provide participants with a framework to assess management challenges associated with individual Intelligent Electronic Devices (IEDs) and recommend a comprehensive, integrated management strategy that is optimized for the unique fleet of IEDs installed in their power delivery infrastructure.




**John Stewart** • 865.279.1447 • jstewart@epri.com

Scan QR code for two-page summary of project

# Cyber Security for Power Delivery and Utilization Guidebooks 2023

Cyber Security for Power Delivery and Utilization 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 |
|---|---|---|
| Building an OT Cyber Lab Guidebook | 3002028549 | 2023 |
| Distributed Energy Resources (DER) Cyber Security Guidebook for Utility Architects and Engineers, 3rd Edition (see QR code page 39) | 3002027325 | 2023 |
| OT Cyber Security Data Management Guide V1 (see QR code page 39) | 3002027173 | 2023 |
| Substation Security Guidebook (see QR code page 39) | 3002027332 | 2023 |
| The Integrated Security Operations Center (ISOC) Guidebook (2023 Update) | 3002026798 | 2023 |
| Threat Management Guidebook (2023 Update) (see QR code page 39) | 3002027168 | 2023 |
| Threat Monitoring for DERs – Phase II: Enabling WAF Technologies | 3002027167 | 2023 |
| OT Cyber Security Data Management Guide: Version 1) (see QR code page 39) | 3002027173 | 2023 |
| 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 |

| TITLE | PID# | YEAR |
|---|---|---|
| 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 |

DER Cyber Security Guidebook for Utility Architects and Engineers 3rd Edition

OT Cyber Security Data Management Guide Version 1

Substation Security Guidebook 2023 Edition

Threat Management Guidebook 2023 Edition



## Self-Led Cyber Security Training

### Developing a Cyber Security Culture in the Operational Technology (OT) Environment

This software computer-based training provides an overview of OT cyber security culture and its importance in the energy industry. It covers recent cyber attacks targeting OT equipment to impact infrastructure. Students will gain a better understanding for the importance of developing a OT cyber security culture.

### Cyber Security Technical Assessment Methodology Revision 1

Cyber security vulnerabilities and exploits are a digital hazard and reliability consideration that is best addressed using an engineering method. The Cyber Security Technical Assessment Methodology (TAM) guides the user through a methodical process that efficiently converges the assessment and mitigation activities to achieve an effective result. The TAM identifies and mitigates the actual vulnerabilities of digital systems, enabling advanced digital implementations at a sustainable cost and incorporates risk informed elements to balance the cost of protection against the actual risk to the facility, such as reputational risk, lost generation, equipment damage, chemical release, or radiological release.

### Cyber Security Fundamentals for Procurement Professionals –Role-based Training

Maintaining a robust cybersecurity posture relies on both security technology tools and administrative controls. This relies on facility personnel to each perform specific roles in ensuring these tools and controls are implemented, operated, and maintained effectively. This training course introduces and reinforces fundamental cybersecurity knowledge areas applicable to supply chain specialists and related roles in the energy sector. It can be used to supplement initial training and company-specific qualification. It can also be incorporated into periodic refresher training and qualification renewal.

### Incident and Threat Management (ITM) 1116: How to plan an Integrated Security Operations Center (ISOC)

This course is designed for utility resources who are responsible for integrating Information Technology (IT), Operations Technology (OT) and physical Security Operations Centers or SOCs into Integrated Security Operations Centers or ISOCs. It is also useful for new managers of ISOCs to help build background knowledge that enables continuous people, process, and technology improvements of ISOCs.



### Secure Remote Access – A Functional Architecture for Grid Operations Procurement Decisions

This course describes unique remote substation communications requirements and apply EPRI's functional architecture in identifying the capabilities that deliver secure communications to substations. This knowledge will aid in evaluations of vendor products and in developing specifications that enable more consistent evaluations.

### OT Cyber Security Basics in Power Delivery Systems for IT Cyber Security Resources

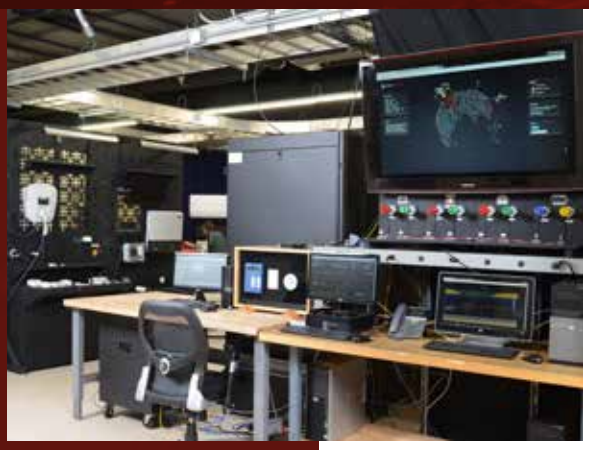
This course is designed for utility IT cyber security professionals interested in OT cyber security from the transmission grid all the way to the meter. It serves as a good foundation to cross train IT cyber security professionals in utility OT environments to help support OT cyber security roles and ISOC responsibilities. It is also a good course for IT professionals in advance of IT/OT convergence projects.

### Integrated Security Operations Center (ISOC) Human Assets Impacts

This course is designed for utility Human Resources professionals involved in utility initiatives that integrate Information Technology (IT), Operations Technology (OT), and physical Security Operations Centers (SOCs) into Integrated Security Operations Centers (ISOCs). It is also useful for ISOC managers to help build background knowledge about people and process change management regarding ISOCs. Students will gain practical information and tools to support their utility's ISOC initiatives.



SECURING POWER DELIVERY



## EPRI's Cyber Security Research Laboratory (CSRL), Knoxville, Tennessee

### R&D IN ACTION

EPRI labs are staffed by accomplished researchers, many with advanced degrees in energy and engineering fields.

More importantly, EPRI ensures that laboratory staff earn and maintain critical certifications for work performed.

**At EPRI's Cyber Security Research Laboratory Research investigations include:**

- **Integrated Security Operations Center Project**
- **Integrated Threat Analysis Framework Project**
- **Network Management Systems Project**
- **Open Enabling Platform Project**
- **Intrusion Detection System and Intrusion Prevention System Project**



EPRI's Cyber Security Research Laboratory (CSRL) addresses the security challenges of mission-critical utility operations. Part of the Smart Grid Substations Lab, it bridges the gap between the longer-term perspectives of National Laboratories and university research activities, and the more immediate solutions needed by utilities.

Our research investigates architectural options for substations or field area networks; the recommended use and placement of firewalls and intrusion detection systems (IDS); incorporating network management systems (NMS) into security operations and deployment of security information and event management (SIEM) tools.

The CSRL lab has the only multi-vendor "end-to-end" environment supporting the testing of communications, security and standards-based integration for the enterprise, control center, substation, field, and customer environments.

The CSRL lab supports Cyber Security program funder research needs too. Lab facilities are available for utility tests of vendor solutions, benefitting members by accelerating demonstrations without costs incurred in building individual test environments. EPRI's Cyber Security Research Lab is an important research tool to address and resolve utility cyber security challenges.

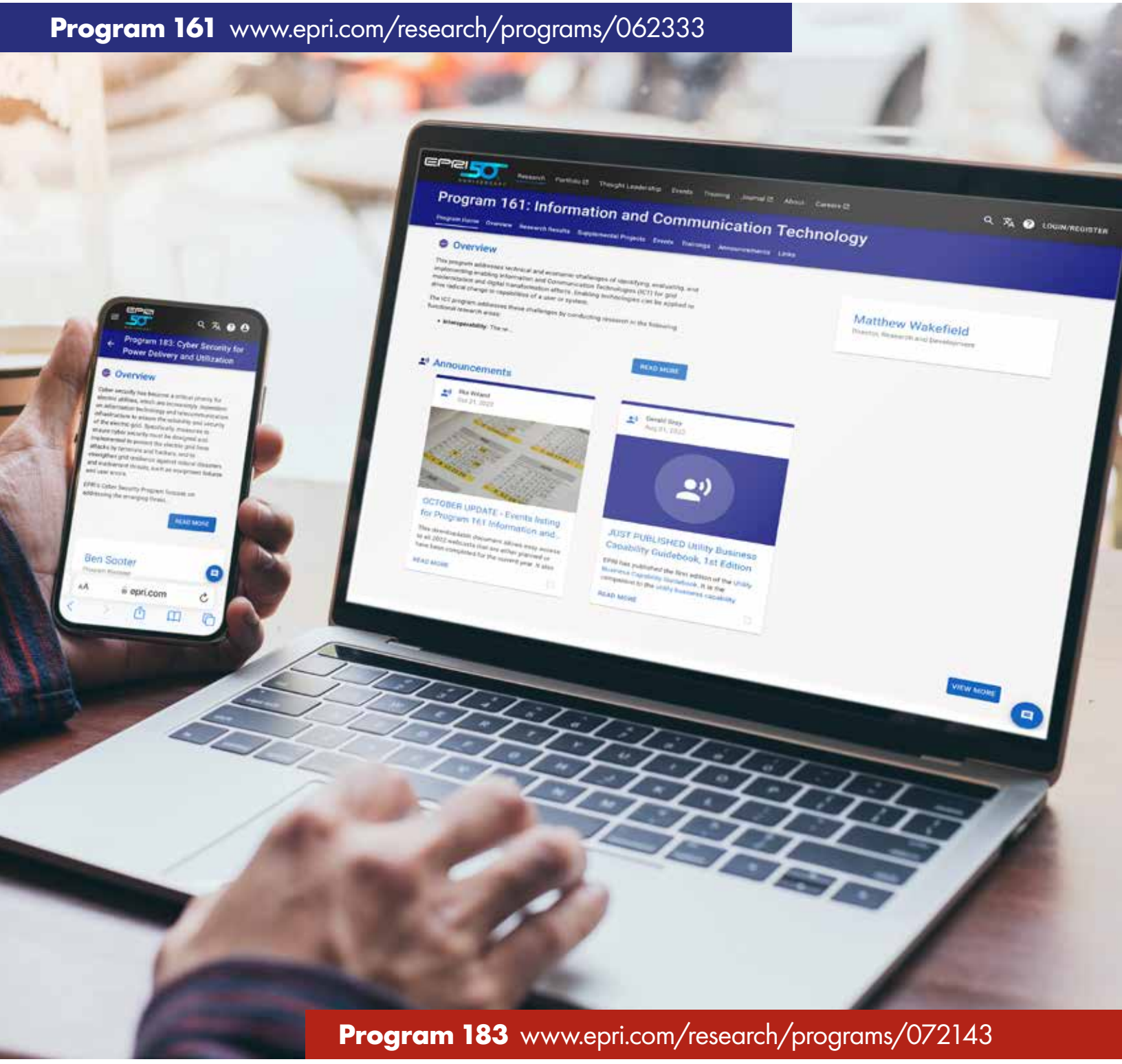




## Information, Communication and Cyber Security Area Resources

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




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



**EPRI**

3420 Hillview Avenue, Palo Alto, California, 94304-1338 USA
800.313.3774 • 650.855.2121 • askepri@epri.com •
www.epri.com

© 2024 Electric Power Research Institute (EPRI), Inc. All rights reserved.

3002028935