EPRI

Information, Communication and Cyber Security

Area Review

February 2022

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

Performs research and development to support electric utility digital transformation, decarbonization and grid flexibility for transmission, distribution and customer behind the meter technologies and solutions.

Information and Communication Technology Program (161)

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

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

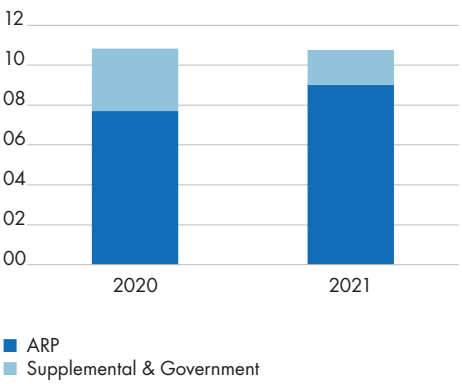
Cyber Security for Power Delivery & Utilization (183)

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.

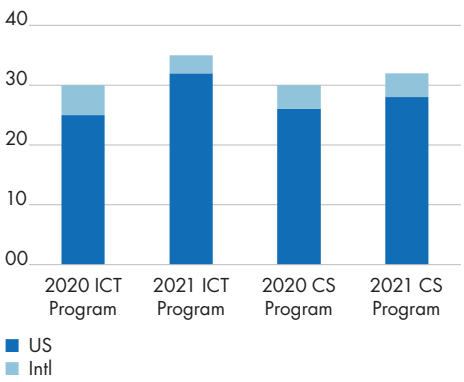
- Incident and Threat Management
- Cyber Security Forensics
- Transmission & Distribution Control Center & Substation Security
- Distributed Energy Resources Security Technologies
- Knowledge Applications

Contents

ICT & Cyber Security Program Funding (in $ Millions)



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



Staff	#
Tech	35
Admin	2
Total	**37**

Degree	#
PhD	2
Masters	13
Bachelors	21

What the Information and Communication Technology (ICT) Program Does

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

Emerging Technologies and Technology Transfer (161A)

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

Information and Communication Technology for DER & Demand Response (161D)

Advancing interoperable technologies and standards to enable integration of solar, storage, electric vehicles, and appliances.

Enterprise Architecture and Integration (161E)

Creates practical artifacts and guides to improve the state of the art in enterprise architecture standards-based systems integration.

Advanced Metering Systems (161F)

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

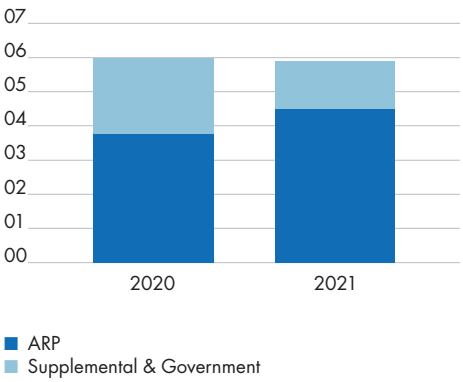
Telecommunications (161G)

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

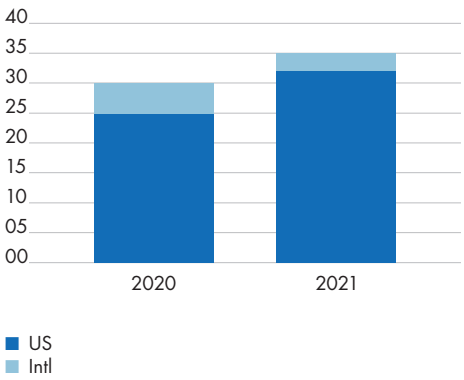
Geospatial Informatics (161H)

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

ICT Program Funding (in $ Millions)



Utility Members



Staff	#
Tech	18
Admin	2
Total	20

Degree	#
PhD	1
Masters	4
Bachelors	14

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

Emerging Technologies and Technology Transfer (161A)

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

PROJECT	2021 Accomplishments & Key Deliverables	2022 Plan
Smart Grid Standards Tracking and Analysis	The **Summary of Interoperability Tracking and Reporting** by the ICT Program in 2021 is a compiled list of 2021 webcasts that included topics: Distributed Energy Resources (DER) Protocol Reference Guidebook. How Advanced Metering Infrastructure (AMI) Standards Save you Time, Money, and Aggravation. Distributed Energy Resources (DER) Standards Harmonization. CTA-2045 Standard Update. A Framework for Relating the Elements of Strategy Development Through Implementation.	Tracking and analysis on key standards development activities. Results will be presented through monthly interoperability webcasts that will focus on a specific technology or application and provide members with a forum for exchanging priorities and ideas with their peers.
White Papers on Emerging Information and Communication Technology	Three white papers: **Leading the Digital Transformation in the Electric Utility Industry** describes how digital technologies may transform the electricity sector. **Exploring a Data Centric Approach for Digital Utilities: Why Getting Data "Right" Matters** highlights key technical/organizational components to initiate data centrism. **Mastering the Critical Role of GIS in Modeling DER** highlights further research on how to position GIS in their grid modernization roadmaps.	White Papers that investigate emerging ICT related issues and technologies that may impact utility investments. White paper topics are identified in coordination with advisors in early 2022.
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.	The value of the research results developed through the ICT Program is realized when the intended audience uses them. Technology transfer of ICT Program resources are combined with monthly Interoperability webcasts as well as periodic newsletters.

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

Applied Information and Communication Technology for Distributed Energy Resources and Demand Response (161D)

Advancing interoperable technologies and standards to enable integration of solar, storage, electric vehicles, and appliances.

PROJECT

	2021 Accomplishments & Key Deliverables	2022 Plan
Enabling Open, Interoperable DER – Standards, Testability, and Overcoming Barriers to Interoperability	**The EPRI Protocol Reference Guidebook (PRG) V5** is a reference document for stakeholders working with DER and DR technologies who want to learn more about the different options for application-layer protocols. In 2021 EPRI increased the number of protocols to eleven, introduced historical maturity tracking, and added a new section focused on key changes in the past year.	Analysis of barriers and maturity of communications and data standards including adoption, governance, supported technologies, test tools and certification, regulatory or industry requirements, the standards' placement in the DER/DR control architecture. • Data models over communication protocols • Testing of DER/DR on the market • Tracking regulations requiring standards (e.g. IEEE 1547-2018, California, Washington, Oregon) • Evolving IT practices with increase of DER/DR
Utility Case Studies on Communicating with DER – Highlighting Experiences, Best Practices and Barriers	**EPRI's DER Interoperability Guidebook** compiles knowledge, lessons learned, and guidence on achieving DER interoperability. In 2021 the report was expanded to cover eleven topics. This includes Key Attributes of DER Interoperability, DER Standards Landscape, Templates for Protocol Requirements, Validating Conformance, Protocol Mapping, Example Architectures, Cloud-Based Architecture for DR Programs, Integrating with Third-Parties, Common Interoperability Failures, and Telecommunications for DERs.	DER and DR deployment is increasing. Utilities are making both business and technical decisions and learning how these are impacting their utility's DER/DR architecture. This project will support this by researching: • State of art-development and case studies • Existing and planned DER/DR architecture • Best practices and barriers • Impact of communications metrics (bandwidth and latency), choice of protocol, and intended control application
Bigger Picture – Preparing for End-to-End Integration of DERs	EPRI developed information and protocol requirements for eight high-priority energy storage applications, identified gaps in both DER protocols and grid codes, and defined the steps to fill them. Key product - **Energy Storage Management Functions to Address Grid and Customer Services: Phase 2 – Information and Communication Capabilities** EPRI completed year three of a multi-year effort focused on reducing the communications costs for DERs. Specifically, reducing hardware costs and complexity, time required for installation, and on-going network charges. Key product - **Connecting to Smart Inverters: Opportunities and Limitations of Using Power Over Ethernet and Advanced Metering Infrastructure Networks**	Understand DER/DR roadmap components (incl. communicating DER/DR); technologies, processes, and systems that streamline the end-to-end automation and integration and reduce long-term O&M costs. Examples: • Integration of DER/DR with aggregation platforms, microgrid and advanced energy communities, building or campus management systems, DERMS • Security and telecom technologies • Communication capabilities requirements (customer-owned or utility networks) • Response to grid transformation, training of digital workers

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	2021 Accomplishments & Key Deliverables	2022 Plan
Enterprise Architecture (EA)	**The Top Ten Indicators of EA Maturity: 2020 Results** captures the state of EA maturity in the utility industry. **LEAPWorx 3rd Edition** The Library of Enterprise Architecture Patterns. **Utility EA Guidebook 6th Edition** The resource for utility specific guidance for enterprise architects.	• New version of EA maturity survey that includes latest best practices • Create the network model reference architecture • Apply and refine AMI and Control Center reference architectures for roadmapping and maturity models • Proven approaches to increase the influence, effectiveness, and scope of the EA capability • Enhance LEAPWorx with latest guidance for effective modeling
Enterprise Systems Integration	**Common Information Model Primer: 7th Edition** Tools and processes to create extended CIM-based interfaces (English & Spanish versions). **Cloud Integration Guidebook, 6th Edition:** A Guide for Enterprise Architects. **Transmission Network Data Management:** Best Practice for Meeting European Requirements. **Advanced Metering Infrastructure (AMI) Reference Architecture** The functions and data required to implement 12 of the most important AMI use cases.	• A guide to the new CIM standard and updates for DER • Managed adoption of cloud services • OT Data Reference Architecture • Capability Specific Data Management
Organizational Alignment	**Utility Business Capability Model** Utilities collaborated to create a model for the industry. **A Framework for Relating the Elements of Strategy Development through Implementation** Utilizing capability-based planning to capture and communicate strategy through execution. **Grid Modernization Playbook** (joint with Distribution Operations) A Framework for Developing Your Plan. **IT/OT Convergence Guidebook: 4th Edition** A business capability-based approach.	• Incorporate and extend the EPRI Utility Business Capability Model • Extend the relationship framework to include roadmaps and maturity models • Case studies for IT-OT alignment • Playbook updates with latest lessons learned from roadmapping projects
Technology Innovation	A **Reference Architecture for the Control Center of the Future** describes the results of a multidisciplinary effort between two project sets to develop a reference architecture for the control center of the future (CCOTF) that identifies the 5–10-year system risks and corresponding system requirements. 161E has focused on use and development of reference architectures or models for several utility domains. **A Reference Architecture for the Control Center of the Future: Model Files** contains the model files for the Control Center of the Future Reference Architecture. **Work Order Management Business Analysis and Testing (WOMBAT)** The WOMBAT tool in order to 1) address capabilities associated with implementing augmented reality (AR) within a work order and maintenance context, 2) address data integration preferences, and 3) develop new application integration testing capabilities.	

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

Advanced Metering Systems (161F)

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

PROJECT	2021 Accomplishments & Key Deliverables	2022 Plan
Achieving Open, Interoperable Advanced Metering Systems	Created open source software and hardware to read meters via optical port using a Raspberry Pi Zero W or other inexpensive computer. Obtained a collection of meters and tested them for compliance with ANSI C12.18 and ANSI C12.19. **ANSI Meter C12 Communications Compliance** **ANSI Meter C12 Communications Compliance Software (c12test) v1.0.4.6** **ANSI C12 Compliance Testing Software Public Video**	Create a Standard Meter Comm. Protocols Primer for the ANSI C12 and IEC 62056 (DLMS/COSEM) standards. Lab and field evaluations are conducted to assess the performance and interoperability of emerging system components in collaboration with Power Quality (P1) and Distribution Systems (P180).
Advanced Metering Systems Operations and Management	Created report on sensor integration including detailed case study of gas leak detectors at ConEd. **Integrating Non-meter Sensors and Devices into AMI**	Create a report that describes current practice in identifying and resolving AMI system communications, including RF mesh and PowerLine Carrier (PLC) technologies. • Ways to reduce time and cost in operating and maintaining advanced metering systems • Streamlining AMI system procurement, deployment, and integration • Mitigating risks by providing insights into the system's health and remaining useful service life • Mitigating risk by proactively identifying and correcting meter issues
Optimizing Advanced Metering System Value and Utilization	This research describes the essential characteristics of a successful Advanced Metering Infrastructure (AMI) to Outage Management System (OMS) integration. It synthesizes some of the currently known best practices to assure the success of such a project and gives practical examples. **Guidebook for Integrating AMI into Outage Management**	Develop data processing algorithms and simulation tools to help utilities and vendors implement new AMI functionality in an optimal way and to process AMI data for maximum benefit. Create Analyzing and Categorizing Momentary Outages from AMI Data report describing methods for analyzing momentary outages reported by AMI meters and how to interpret and categorize the results.

Tim Godfrey,
Program Manager,
tgodfrey@epri.com

Telecommunications (161G)

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

PROJECT	2021 Accomplishments & Key Deliverables	2022 Plan
Wide Area Networks	Completed field testing of **6 GHz interference to utility microwave Low Power Indoor Wi-Fi 6E** equipment: • **Southern Company in Columbus, GA** • Ameren in Peoria, IL **Completed Lab Testing of Wi-Fi 6E interactions with 6 GHz Microwave Radios.** Completed update of **Strategic Fiber Guidebook** Completed Integrating and Orchestrating WAN Services.	Research • Evaluate AFC effectiveness in preventing interference to 6 GHz microwave systems from higher power unlicensed equipment • Develop WAN Modernization Guidebook, addressing private and leased WAN circuits, requirements for teleprotection and precision time synchronization, SDN and SD-WAN, and ways to improve WAN reliability/availability • Update Strategic Fiber Guidebook with business cases for expanded fiber deployment, sharing and partnerships, IT/OT convergence, and rural broadband
Field / Neighborhood Area Networks	**Annual Update of Private LTE Guidebook 2021** Completed Frequency Planning and Interference Management for Licensed Spectrum FANs. Conducted studies **LTE Shared Spectrum and Flexible Frequency Operations** highlighting challenges of deploying and operating in CBRS spectrum. Evaluated equipment capabilities and requirements for LTE Inter-Network Operation and Roaming. Conducted lab testing on using commercial Cellular for Direct Transfer Trip protection.	• Define tradeoffs between private wireless networks and commercial cellular • Achieve interoperability, reliability/ resilience, and QoS in multi-technology wireless networks • Understand communication requirements for DER and related protection such as Direct Transfer Trip (DTT) • Understand options for licensed and shared spectrum for LTE and NB-IoT networks • Use of unlicensed spectrum current capacity limits and future

continued...

Tim Godfrey,
Program Manager,
tgodfrey@epri.com

Telecommunications (161G) *continued*

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

PROJECT	**2021** Accomplishments & Key Deliverables	**2022** Plan
Telecommunications Planning and Management Systems	Completed presentation deliverable Design and Planning of a Scalable IT, highlighting telecom changes to support remote workforce. Project on Multi-Tier networks was tied to DOE project which had delayed start - project will move into 2022. Developed case studies **Integration of the Telecom NMS with GIS.**	• Best practices for utility telecom network management • Techniques to optimize the process of quickly, easily, and securely provisioning field devices • Leverage service-oriented architecture, the infrastructure technology information library, and best practices from carriers • Tools for automation and documentation (logical network inventory as well as physical), including identification of naming conventions from carrier best practices • Planning Communications Sites for resilient operation and backup power
Telecommunication Standards Engagement	Comms Intelligencer Newsletter 1H 2021 published in June. Comms Intelligencer Newsletter 2H 2021 published in December. **Telecommunication Standards Guidebook V3** 2021 Edition was published in October. Pandemic continues to have a significant impact on standards progress in all SDOs.	• Participation and leadership in IEEE 802, IEEE PES, and 3GPP standards development organizations • Smart Grid Communications Intelligencer newsletters that highlight issues of relevance and interest to utility communications engineers and managers. Focus on developments in communication technologies and standards • Telecom Standards Guidebook annual update that incorporates previous work performed and adds individual standards status, roadmaps, schedules, and maturity metrics

Randy Rhodes,
Technical Executive,
rrhodes@epri.com

Geospatial Informatics (161H)

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

PROJECT	2021 Accomplishments & Key Deliverables	2022 Plan
Geospatial Informatics (GIS) Data Practices	Reviewed 2020 content for updates and developing new material based on input from 161H funders for publishing update of **Geospatial Informatics Guidebook**.	Research • Immature data, incomplete system models, and insufficiently accurate modeling • Inability to visualize and evaluate data sets • Immature standards and vendor lock-in • Duplicate data and incomplete metadata • Difficulty with quickly and accurately onboarding precise asset data • Inability to accurately establish a valuation of information assets over time • Geospatial Informatics Guidebook annual update for best practices in geospatial data management
Geospatial Informatics (GIS) Applications	• Participated as a member of The Open Geospatial Consortium (OGC) to learn from OGC Testbed 17 activities. • Principal investigator attended three virtual conferences and consulted with leaders in the fields of AR, MR, VR, digital twins, and spatial computing. • Published executive-focused white paper Digital Twin is Today's Utility GIS Opportunity mid-year. • Launched digital twin SPN project in September, which helped consolidate our findings. • Panel presentation at Nov Augmented World Expo.	• Enabling rapid technology adoption by understanding data needs through monitoring and contributing expertise to a real-world pilot and testbed • Encourage sharing of expertise and development resources, providing early market insight • Reduce technology risk through development and testing of interoperability standards • Influence market development toward choices that fit well with existing electric utility GIS environments, providing a transition path to the future • Geospatial Requirements for XR Applications annual update with development of digital twin frameworks and application roadmaps
Geospatial Informatics (GIS) Analytics and Visualization	• Conducted survey with161H funders on data validation, verification, tracking and collaboration approaches across GIS and distribution planning. • Ongoing coordination has been maintained with P200E and the Grid Model Data Management project. • 161H has support the P200E development of a CIM-based interface for OpenDSS and preparation for the GMDM interop in 2022. • Review of P200E content and finalized joint deliverable publication Enhanced Grid Modeling Data for Planning and Operations.	• Identify requirements and best practices for GIS data management in support of advanced planning and operations requirements • Enhanced Grid Modeling Workshop • Enhanced Grid Modeling for Advanced Planning Analytics expanding on distribution application requirements not addressed in 2020

Examples of Member Application of Results

Value Obtained

161A Seattle City Light

Outage Data Standard to Improve Customer Engagement and Assist First Responders

EPRI led an industry effort to create standardized outage management status messages that have since been contributed to International Electrotechnical Commission (IEC) Standard 61968-3 as well as Multi-Speak. And has resulted in a growing international adoption referred to as the Outage Data Initiative.

"The Outage Data Initiative enabled Seattle City Light to share outage data so that other utilities and emergency management organizations can see it on their preferred platform. Together, we can create a common operating picture and improve our response when storms, fires, earthquakes or other disasters strike."

Scott Thomsen, Sr. Strategic Advisor, Seattle City Light

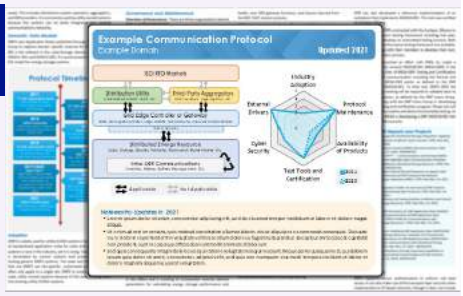
161D Salt River Project

EPRI's Protocol Reference Guide Organizes Information for Utility Use Now and In Future Editions

The Protocol Reference Guide answers frequently asked questions about information and protocol standards for distributed energy resources and demand response technologies. It is an important tool for stakeholders working with DER/DR technologies who want to learn more about the different options for standard protocols, information, and data models.

"EPRI's Protocol Reference Guide is helpful in communicating and educating the various departments within SRP on the many different attributes of DER protocols. This information helps all stakeholders get on the same page to better define requirements and next steps for DER integration."

Kyle Cormier, Salt River Project

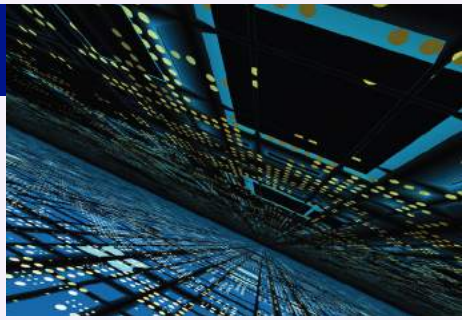


161D Ameren Services

EPRI Test Tools Support Advanced Testing

IEEE 1547 and California Rule 21 is breaking new ground by requiring standardized communications interfaces in devices. Utilities need tools to evaluate these products and their capabilities to ensure they meet requirements. EPRI created test-tools to support implementation and testability of open protocols in solar, storage, and demand response technologies.

EPRI helped Ameren establish the Dorsett Inverter validation facility by defining priority use cases for utility and customer. Ameren also used the EPRI's openDERMS platform to conduct testing on virtual and physical DER assets in their lab. This allowed Ameren to achieve learn and demonstrate capabilities with minimal capital investment.



161E American Electric Power

Enterprise Architecture Collaboration Group (EACG) Addresses Standards-based Integration

Do standards-based interfaces (SBI) reduce operations and maintenance costs? It seems like SBI should reduce costs. As the EACG explored this topic they also compared SBI against other types of integration techniques, such as proprietary point-to-point, or using "adapters". Because the development norms may vary by organization, the EACG did not seek to be definitive, but rather to create a framework so that any utility could compare their own development costs, expectations, and patterns to compare the different integration approaches.

"This framework will provide a meaningful public benefit for architecture practitioners looking for tools to help quantify architecture debt, better understand where various integration techniques are cost effective, and help align the thinking of other interoperability efforts, such as the Grid Modernization Laboratory Consortium – Interoperability Project."

Enterprise Architect at American Electric Power (AEP)

Examples of Member Application of Results

Value Obtained

161E Salt River Project

Digital Transformation: An Information Technology and Operations

EPRI has been conducting research on information technology and operations (IT&O) convergence since 2014. The work has looked at strategy, critical success factors, cost-benefit analysis, portfolio management, and has been involved in conversations with thought leaders at the highest level of utility organizations. The model attempts to identify those attributes that a utility can invest in to see improved execution across IT&O domains, leveraging the leading practices of each, to achieve better outcomes related to projects and investments. Domains coincide with the categories of people, process, technology, and governance, and use a common "five tiers" maturity model that evolves from Level 1 – ad hoc, to Level 5, Industry Leading. EPRI, coordinating with utility subject matter experts (SMEs), and leveraging their prior maturity model experience, conducted three workshops:

- 1st workshop hosted by SRP
- 2nd workshop as part of the Enterprise Architecture Collaboration Group task force meeting hosted by AEP
- 3rd session at the EPRI advisor meeting in Nashville.

This model is reflected in the deliverable, Digital Transformation: Aligning Information Technology and Operations, 2nd Edition.

"After a lively discussion at an advisory meeting on IT/OT convergence challenges, EPRI took the lead in facilitating the creation of a digital transformation maturity model. This model is the result of a collaboration of numerous utilities and will be hugely valuable in helping us understand our maturity as an integrated IT/OT organization, and what we need to do to improve."

Dawn Jurgensmeier, Information Technology Services Grid Modernization Services (ITS GMS) Salt River Project (SRP)

161F EPRI Wi-SUN Meter Test Tool Helps Xcel Energy and Ameren Test AMI Systems

Perfect interoperability is, so far, an unrealized ideal for the RF mesh devices used in Advanced Metering Infrastructure (AMI) networks. The Wi-SUN Alliance is trying to do for AMI communications what the Wi-Fi Alliance has done for Wi-Fi. Both are based on an underlying IEEE standard; IEEE 802.11 for Wi-Fi and IEEE 802.15.4g for Wi-SUN. EPRI has been helping to drive this effort through multiple projects.

"EPRI's participation in the Wi-SUN Alliance and the development of the reference implementation of the Wi-SUN stack are examples of EPRI's leadership in advancing standards-based solutions."

Dan Nordell, Xcel Energy

161F Utilities Enhance Revenue Protection Processes Through the EPRI Leading Practice Guidebook

This guidebook is aimed at helping utilities establish and improve revenue protection practices. *Revenue protection* refers to the broad set of processes that utilities employ to prevent, detect, and respond to energy theft and other energy unaccounted for. With the introduction of advanced "smart" metering technology more than a decade ago, utilities have been required to modify and broaden the methods and procedures they use to protect themselves from energy theft. A process that previously relied on physical visits, human labor, and training in inspection techniques is being replaced by one that is primarily based on digital sensors, remote readings, and analytic algorithms.

"The opportunity to discuss revenue protection best practices with other utilities on a weekly basis encouraged Exelon to explore and utilize new methods and techniques to finding power theft."

Paul Unruh, Exelon

Examples of Member Application of Results

Value Obtained

161G

Ameren

EPRI Field Area Network Research Project – Private LTE Guidebook and FAN Testing Platform

Results from the Private LTE Guidebook provided insights on technology, spectrum options, and use cases to support business case development and investment decisions. Once the pilot project was underway, EPRI's FAN Testing Platform provided quantitative results to asses and verify the network performance.

EPRI's in-depth research helped us not only to make a decision to pursue private LTE, but during our pilot provided above and beyond support for doing unbiased bandwidth and latency testing that was critical for us to understand.

161G

Southern Company

EPRI Wide Area Network Research Project – 6 GHz Microwave Interference

Results from field testing collaboration between EPRI and Southern Company have been instrumental in identifying and quantifying the issues posed by the FCC allowance of unlicensed operation in the 6 GHz band.

EPRI contributed immensely to the planning and execution of the testing, use-case parameters, and the results aided our regulatory filings. EPRI's expertise, knowledge and ingenuity made our real-world testing of unlicensed 6 GHz interference with licensed microwave possible. Their ability to sort out the immature Wi-Fi 6E technology and create working 6E networks for testing not only supported Southern Company but is also contributing to the entire microwave industry's testing and reporting in this area. Because of the partnership with EPRI, Southern Company is well positioned to have a deep knowledgebase and bench strength in areas we need assistance for years to come.

161H

Salt River Project & Lincoln Electric System (LES)

Geodata Informatics Guidebook Second Edition

The GIS guidebook aims to prepare electric utility GIS professionals to deliver improved geodata services to an expanding spectrum of utility individuals and systems. The project is also intended to help GIS professionals understand how trends in the geospatial industry are affecting their management of geospatial information and investments.

GIS Guidebook – provides high value in operational point of view. Joint project work that is GIS related with P200 Distribution Operations & Planning. A lot of value if EPRI can successfully work with vendors and influence industry standards so that products are more off the shelf today. Successfully standing up new ADMS system and a test environment with our GIS data handler.

161H

NYPA, Ameren and Exelon

Digital Twin is Today's Utility GIS Opportunity White Paper

Decarbonization and grid modernization require digital transformation at electric utilities. Readers of the Digital Twin is Today's Utility GIS Opportunity white paper will gain insights they can share and apply to realize the organizational benefits to help accelerate their utility's digital transformation.

Valuable to see more VR implementation in GIS and providing virtual tours, therefore moving forward creating a virtual twin. Also, very valuable to see what other companies are doing in this space. Digital Twin Whitepaper applicability of this research and this new technology and the analysis that is performed in this research.

ICT Technology Transfer Award Winners & Nominees

Each year EPRI recognizes the leaders and innovators who transfer research into applied results. The people and companies honored with Technology Transfer Awards exemplify the collaboration and leadership that drive progress in the industry and benefit society. Nominees are an individual or group of individuals from our member companies who have championed the successful use of EPRI-sponsored research results over the 2021 time period. Awards were selected in the Fall of 2021 and are presented at the following year 2022 Winter Advisory Meetings.

Nominees are judged on the following criteria:

- Successful application of research results,
- Magnitude of the problem solved,
- Impact and quantifiable benefits of the application to the company, customers, and/or society at large, and
- Leadership, innovation, and initiative demonstrated.

Winners	Technology	How Research was Applied
Ameren Corporation David Bruemmer (Retired), Brian Hartman, Imran Khan Martin Welge **Southern Company** Larry Butts, John Holmes, Randall Watkins, Al Whitley	**Assessment of Interference to 6 GHz Microwave links from Unlicensed Wi-Fi Devices**	Collaboration to demonstrate and prove theoretical issues of the Federal Communications Commission Report & Order 20-50 which allows unlicensed device operation in the upper and lower licensed 6GHz fixed service microwave radio bands.

Nominees	Technology	How Research was Applied
Southern California Edison Pacific Gas & Electric	**Advanced Communications, Standards, and Controls of Smart Inverters and Smart Devices to Enable More Residential Solar Energy**	Two methods assessed the smart inverter behavior using lab and field tests: (1) successful side-by-side operations; and (2) using residential smart loads to enable more solar PV on the grid. The lab testing and research applications by PG&E and SCE, allowed power quality (PQ)functions, 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 lab, including PQ changes and other factors induced by load-changes. 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.
New York Power Authority	**Assessing Augmented Reality in Electric Utilities**	Augmented Reality (AR) is an enabling visualization technology that overlays computer graphics on a live video rendering over part of an interface of a user's environment. Virtual Reality (VR) replaces all of the user's natural environment with rendered graphics. Collectively, these technologies may be referred to as Extended Reality (XR). This research explored the use of XR to help facilitate data entry, digital training, monitoring, and other applications at utilities as well as benchmark before and after measurements of time on task during its use. AR has improved worker efficiency in mobile application prototypes that integrate sensor data. It also indicates that VR training may provide safe and remote training access to work environments that require increased situational awareness or otherwise.

Supplemental Projects

These projects are research, development or demonstration projects offered outside of the annual research portfolio. They can be started anytime and are often spearheaded in response to an immediate need by an individual or group of members. Supplementals are supported either through Tailored Collaboration or pooled member funds. **For details click here.**

Guidebooks

These deliverables 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.

For further details click on the 2021 ICT Guidebook Listing.

Technology Transfer Activities

For additional details click here.

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

The Cyber Security for Power Delivery and Utilization Program focuses 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.

Incident & Threat Management:
Technical solutions, guidelines, and guidebooks to increase the capabilities and efficiency of incident and threat management tools and processes for power delivery systems.

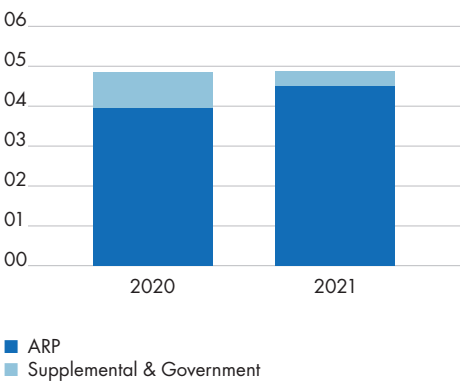
Cyber Security for Transmission & Distribution Operations and Systems:
Technical solutions and guidelines to improve the security posture of transmission and distribution systems.

Cyber Security for DER and Grid-Edge Systems:
Security requirements, solutions, and reference architectures for the deployment and integration of distributed generation and grid-grid technologies.

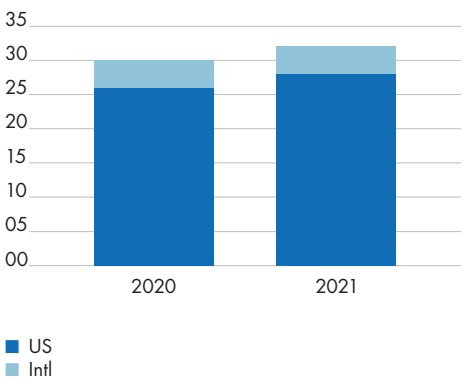
Knowledge Applications:
Improve cyber security programs through quantitative and qualitative performance assessments and specialized workforce training.

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

Cyber Security Program Funding
(in $ Millions)



Utility Members



Staff	#
Tech	17
Admin	2
Total	19

Degree	#
PhD	1
Masters	9
Bachelors	7

Ben Sooter,
Program Manager,
bsooter@epri.com

Incident & Threat Management

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

PROJECT

Incident Management

Ben Sooter
bsooter@epri.com

2021 Accomplishments & Key Deliverables

The **Integrated Security Operations Center (ISOC) Guidebook V4** provides utilities guidance for the implementation of their incident management program, focusing on monitoring, detection, and response. The update for 2021 includes detailed attack scenarios for power delivery systems to provide technical specifications for utilities to successfully monitor and detect the attacks.

2022 Plan

Updates to the ISOC Guidebook 2022 will focus on Artificial Intelligence (AI) for the Information Security Operations Center (ISOC). AI projects are gaining maturity and may be used to eliminate Tier 1 analyst tasks. New solutions will be explored to provide strategies for how to implement these new systems.

Threat Management

Ben Sooter
bsooter@epri.com

The **Threat Management Guidebook V1** describes strategies and guidelines for electric power utilities to design, implement, and operate a Threat Management Program (TMP) for their entire system so they can better protect it against cyber-attacks. A threat management program extends the capabilities of a typical security operations center by integrating and correlating security events from operations technology (OT) networks across the entire kill chain.

The annual update for the Threat Management Guidebook will provide comprehensive guidance base on past EPRI research from 2017 to 2021. In 2022 the Threat Management Guidebook will add information on threat intelligence sharing in the utility industry.

Cyber Security Forensics

William Webb
wwebb@epri.com

The **Mobile Forensics Field Guide: NovaTech OrionLX** substation automation controller forensics field guide was published to the EPRI Mobile Field Guides app. Members may download the app and view the mobile field guide.

The Forensics Field Guide, **SEL-751 feeder protection relay field guide** has also been published to the mobile platform and is available for download at the appropriate link for your mobile device: iOS/iPadOS , Android.

Cyber Security Forensic Guidebook - This deliverable will provide guidance on how to develop process and procedures for obtaining forensics from embedded devices. It will also include how to use automated forensic harvesting tools to simplify the forensic collection process.

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

Cyber Security for Transmission and Distribution Operations and Systems

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

PROJECT

Cyber Security for Substations

John Stewart
jstewart@epri.com

2021 Accomplishments & Key Deliverables

Guidebook: A Comprehensive Approach to Secure IED Management provides an overview of various management capabilities that should be included in a comprehensive Intelligent Electronic Device (IED) management program. The focus of this research is on substation networks and systems, since cybersecurity in the transmission and distribution area can present a significant number of challenges to utility personnel.

2022 Plan

Develop a Cyber Security for Digital Substations document - An exploration of new substation

Support member efforts to securely manage the wide range of systems and technologies deployed in existing substations.

Identify opportunities to leverage information between different management systems to automate cross-checking and validation of systems.

Annual update of the IED Management guidebook

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

Cyber Security for DER and Grid-Edge Systems

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

PROJECT

Cyber Security for DER Integration and Management (CSDIM)

Xavier Francia
xfrancia@epri.com

2021 Accomplishments & Key Deliverables

The **Distributed Energy Resources (DER) Cybersecurity Guidebook** is a reference document for utility cybersecurity architects, cybersecurity engineers, and other stakeholders to assist in securing integration of distributed energy resources to the grid. It provides background information on DERs, an overview of cybersecurity risks, reference architectures are provided to assist in cybersecurity architecture development, and practical approaches towards securing DER technologies.

The **Cybersecurity for Grid Connected Devices and Demand Response: Cybersecurity Risks, Threats, and Recommendations** overview of DR programs, use cases, and the systems involved. Cybersecurity threat modeling is performed against DR reference architectures, and associated security control recommendations are presented.

2022 Plan

Update to 2nd Edition of DER Cyber Security Guidebook with a focus on cyber security engineering approaches including identify and access management, cloud integration, data diodes, and distributed energy resource management systems

Cyber Security for DER Technologies (CSDT)

Sai Ram Ganti
sganti@epri.com

The **Cybersecurity Requirements for Utility Electric Vehicle Charging Infrastructure** report identifies various utility models for EV charging and investigates cyber security risks associated with each of these.

The **Cybersecurity Requirements for Utility Owned Energy Storage Systems** report investigates cyber security aspects for energy storage systems models for utilities based on ownership, services provided by ESS, access level, and point of interconnection. Potential cyber risks across their energy storage systems have been identified and security requirements to mitigate those risks are detailed.

Develop Threat Monitoring Guidance for DER Systems

Update of Cybersecurity Architecture for Microgrid Integration with a focus on security architecture for connected communities

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

Knowledge Applications

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

PROJECT	2021 Accomplishments & Key Deliverables	2022 Plan
Cyber Security Metrics Christine Hertzog *chertzog@epri.com*	EPRI worked with three utilities to automate data collection, calculations, and reporting with a web-based platform and established the CyberNabu metrics interest group to facilitate cyber security data governance and management best practices. **Developed and published:** **Cyber Security Metrics Implementation Guidebook** **OpenMetCalc 3.0 User Guide** **OpenMetCalc 3.0 Workbook**	Develop a Beginners Guide and use cases to OT Cyber Security Metrics - Provides data collection, management, and governance guidelines for OT cyber security metrics. Create Cyber Security Resiliency Metrics V1 - Includes description of data points, systems, and formulas to calculate resiliency. Continue CyberNabu webcasts to develop cyber security data models and build foundation for AI applications.
Cyber Security Assessments Christine Hertzog *chertzog@epri.com*	EPRI established general and tailored assessment services to help utilities understand their OT cyber security and risk postures.	Conduct assessments and develop anonymized benchmarking data to help utilities take corrective actions that effectively mitigate prioritized.
Cyber Security Workforce Training Christine Hertzog *chertzog@epri.com*	EPRI created role-based CBTs and videos to help utilities strengthen resource knowledge and competencies in OT cyber security skills available through EPRI U.	Develop new instructor-led and lab-based courses and CBTs based on utility needs in topics such as 61850 for Cyber Security Resources and OT Familiarization.
Industry Collaboration Erica Loveday *eloveday@epri.com*	This project supports active participation in and contribution to collaborative efforts and interest groups by providing a monthly email member update to summarize EPRI's industry activities and the status of its research projects. • Reduce time to track industry efforts and reduce risks resulting from not tracking key activities in cyber security. • Increase the efficacy of information from industry working groups delivered to the electric sector. • Cyber Security Industry Updates: 2021 Edition	Continued support for participation and contribution to collaborative efforts and interest groups by providing a monthly email member update to summarize EPRI's industry activities and the status of its research projects.

Examples of Member Application of Results

Incident & Threat Management

Value Obtained

Alliant Energy, FirstEnergy, ConEd, Cooperative Energy, New York Power Authority, Southern Company, Xcel Energy

Insider Threat Management Guidebook

This guidebook is the de facto standard for Insider Threat Management Programs for electric power utilities. The guidebook provides (1) detailed guidance for starting, maturing, and running a program, (2) the use of behavioral psychology for development of critical personas associated with insider threats, and (3) technical guidance for monitoring and detecting suspicious activity.

Each utility is applying the research in their own way and needs. For example, one utility currently has an insider threat management program in place and focuses on using the research to mature and run their program. Another utility has just initiated their program und using the research to build their program based upon the guidance and practices outline in the guidebook.

Southern Company (SoCo)

Operational Technology (OT) Visibility and Response Pilot

Cyber-attacks, such as the SolarWinds and Colonial Pipeline attacks, have shown a critical need for more in-depth detection, monitoring, and forensic capabilities, especially in the electricity industry.

Southern Company worked with EPRI's Cyber Security Research Lab to develop OT visibility and response capabilities that are not only industry-leading but have already been proven to effectively respond to recent high-profile cyber events such as SolarWinds.

Consolidated Edison Company

Cyber Security Forensics

The role of cyber security forensics and having the ability to extract forensics information from device has become increasingly important. ConEdison has used EPRI's cyber security research to enhance their Cyber Security Forensics Program, which is a critical component of their cyber incident response process.

NYSERDA forensics harvester and forensics working group are providing Con Edison with the tools and knowledge to effectively respond to cyber incidents and protect our customers. The ConEdison Forensics Team has extended their capabilities by developing an innovative Mobile Forensics Unit that consists of a vehicle that is customized with the necessary equipment to quickly respond to cyber incidents and perform field forensics investigations.

Examples of Member Application of Results

Cyber Security for Transmission and Distribution Operations and Systems

Value Obtained

American Electric Power (AEP), Dominion Energy

EPRI Cyber Security Technical Assessment Methodology (TAM) on Substation Digital Equipment

Understanding cyber security vulnerabilities and mitigations to maintain a strong security posture for critical infrastructure as described in Executive Order (EO) 13920, Securing the United States bulk-power system (BPS) and are important to help understand opportunities to improve the security posture of digital equipment on the BPS, particularly in transmission substations.

By using the first application of the EPRI TAM on substation equipment systems and using Cyber Security Data Sheets (CSDSs) on the individual equipment to document vulnerabilities, AEP & Dominion were as able to leverage the TAM CSDSs to compare existing controls vs recommended controls and as a result validated existing security controls as well as identified additional attack pathways to consider for potential future mitigations.

Korea Electric Power Corporation (KEPCO)

Cyber Security Compliance Automation

Regulatory standards for electric power systems vary widely around the world, it is a significant concern for almost all utilities. Over time regulators have expanded their role to establish new requirements for cyber security controls. To manage the growing regulatory compliance burden, utilities are looking to EPRI for innovative solutions that lower compliance costs without increasing risk.

KEPCO applied EPRI's cybersecurity research to optimize the compliance process around critical systems such as the Distribution Management System (DMS) and studied, researched, and developed use cases and tools to comply with the national infrastructure protection laws such as North America Electric Reliability Corporation – Critical Infrastructure Protection (NERC-CIP).

Examples of Member Application of Results

Cyber Security for DER and Grid-Edge Systems

Value Obtained

AEP, SRP

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

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

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

PG&E

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

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

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

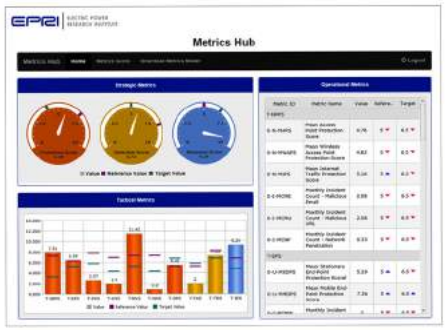
Cyber Security Metrics

ConEd, AECC and TVA, FirstEnergy, NYPA, PG&E, and ConEd

EPRI Cyber Security Metrics Operationalization Pilot

Quantification of cyber security has been a challenge that comes from the fact that there have not been comprehensive security metrics widely adopted by the industry. If such metrics existed, a utility could easily calculate and understand the value of security investments in concrete terms.

Eight utilities piloted EPRI security metrics and used them to quantitatively evaluate security programs. Key learnings from these pilots indicated a need for automated data collection, metrics visualization and root cause analysis capabilities for EPRI security metrics. 120 data points have been identified that can be used to calculate 60 metric scores that quantitatively reflect an organization's security posture in a consistent and repeatable way.



Cyber Security Technology Transfer Award Winners & Nominees

Each year EPRI recognizes the leaders and innovators who transfer research into applied results. The people and companies honored with Technology Transfer Awards exemplify the collaboration and leadership that drive progress in the industry and benefit society. Nominees are an individual or group of individuals from our member companies who have championed the successful use of EPRI-sponsored research results over the 2021 time period. Awards were selected in the Fall of 2021 and are presented at the following year 2022 Winter Advisory Meetings.

Nominees are judged on the following criteria:

- Successful application of research results,
- Magnitude of the problem solved,
- Impact and quantifiable benefits of the application to the company, customers, and/or society at large, and
- Leadership, innovation, and initiative demonstrated.

Winners	Technology	How Research was Applied
Alliant Energy Travis Brown, Lisa Moller **FirstEnergy** Donna Bursick, Shannan Garrett, Thomas Kostura, Christopher Talaski **Consolidated Edison Co. of New York, Inc.** Raul Cabrera, Steve Kim, Serena Lee **Cooperative Energy** Scotty Barron, Mark Dodd **New York Power Authority** Vic Costanza, Tom Savin, Jeffrey Staten **Southern Company** Brittany McBride, Brad Stephenson, Xcel Energy, Jeff Imsdahl, Jamey Sample	**Insider Threat Management Guidebook**	Collaboration and participation in development of the Insider Threat Management Guidebook to support the start, maturation, and operation of insider threat management programs.

Nominees	Technology	How Research was Applied
Korea Electric Power Corporation (KEPCO)	**Cyber Security Compliance Automation**	KEPCO has worked with EPRI and presented to members on projects such as: automated testing of patches for security vulnerabilities, integration of siloed systems that generate artifacts used to demonstrate compliance, optimizing the compliance process DMS, developed use cases and tools to comply with NERC-CIP to obtain knowledge/understanding of U.S. rules and regulations.
Lower Colorado River Authority	**Cyber Security Metrics for the Electric Sector: Vol. 3**	By adapting EPRI's Cyber Security Metrics for the Electric Sector: Volume 3 to create a Cyber Risk Quantification Tool that is used by leadership to understand the effectiveness of applied security controls and architecture LCRA has strengthened the company's cyber security program and is facilitating continuous improvement of NERC-CIP compliance of risk posture for both IT and OT needs.
Southern Company	**OT Visibility and Response Pilot**	Working with EPRI and Gravwell, Southern Co. developed a system that leveraged an open source and high-performance packet-capture capabilities that can be deployed in conjunction with Gravwell data collectors. This enabled the packet capture to take place and be stored at the edge nodes of networks.

Supplemental Projects

These projects are research, development or demonstration projects offered outside of the annual research portfolio. They can be started anytime and are often spearheaded in response to an immediate need by an individual or group of members. Supplementals are supported either through Tailored Collaboration or pooled member funds. **For details click here.**

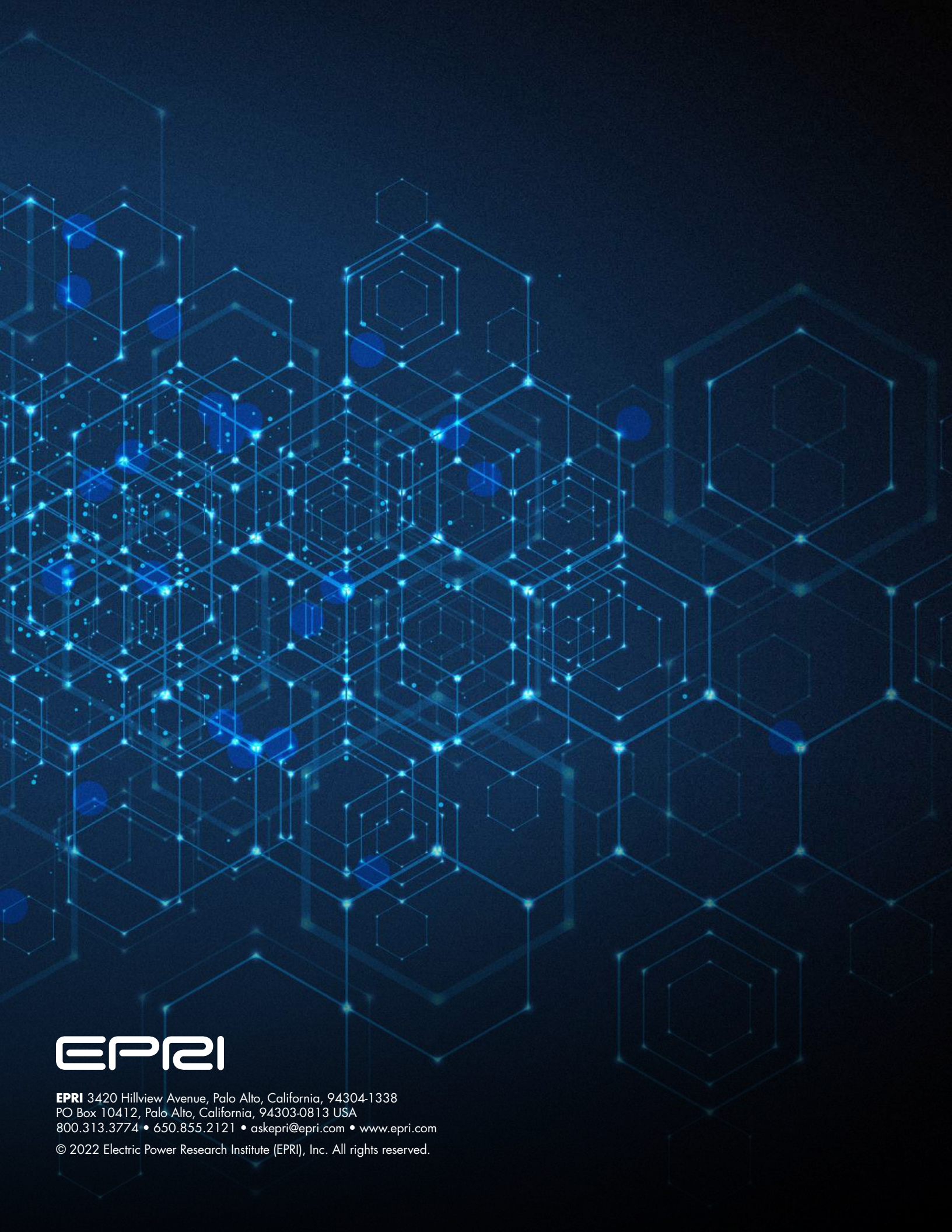
Guidebooks

These deliverables 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.

For further details click on the 2021 CS Guidebook Listing.

Technology Transfer Activities

For additional details click here.



EPRI 3420 Hillview Avenue, Palo Alto, California, 94304-1338
PO Box 10412, Palo Alto, California, 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com