EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Cyber Security for Power Delivery and Utilization

Annual Program Review

January 2020

Contents

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Electric Power Research Institute

3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA

800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

The 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.

Cyber and physical security have become critical priorities 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.

Research Value

The rapid pace of change in the electric sector creates a challenging environment for asset owners and operators to monitor the cyber security activities of industry groups, develop an understanding of how new technologies affect security, and maintain the right internal resources for assessing those technologies. EPRI employs a team of experts with comprehensive backgrounds in cyber security who address these challenges by providing insight and analyses of various security tools, architectures, guidelines, and results of testing to program participants.

The purpose of this research area review is to help members stay informed of our research activities, quickly review research highlights from the year, and identify valuable results to apply at their utility.

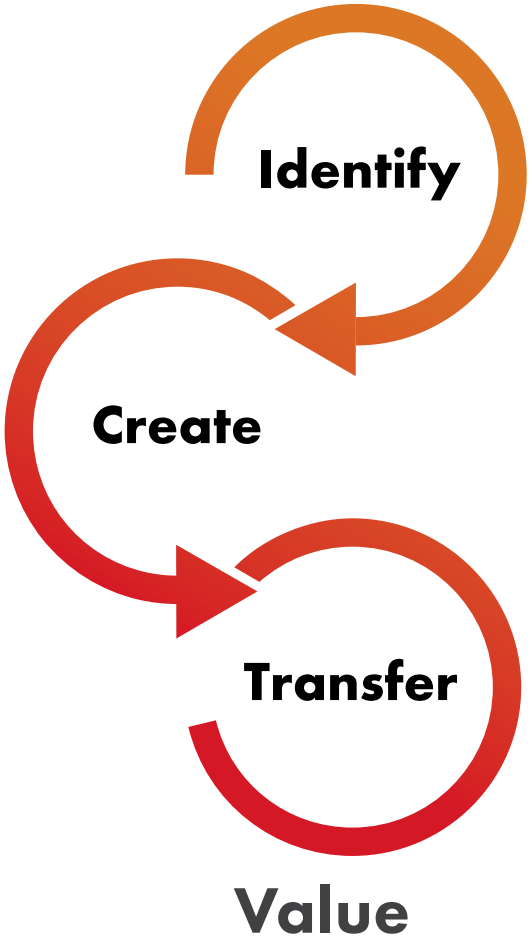
Approach

The Cyber Security Program focuses on developing security requirements, creating new security technologies, and performing laboratory assessments of existing, relevant technologies. The products may be used to enhance the current cyber security posture of the grid and increase the security of systems that are deployed in the future.

Key deliverables in this program include:

- Newsletters and whitepapers to address high-impact issues;
- Guidance and tools for security metrics;
- Security architecture templates for distribution systems;
- Guidance on assessing and monitoring risk;
- Tools to support improved incident and threat management; and
- Tools and techniques for assessing grid security, resiliency, and cyber security posture

Galen Rasche
Sr. Program Manager
Cyber Security for
Power Delivery & Utilization
email: grasche@epri.com



Cyber Security for PDU Program Review 1

EPRI Cyber Security Strategic Initiative

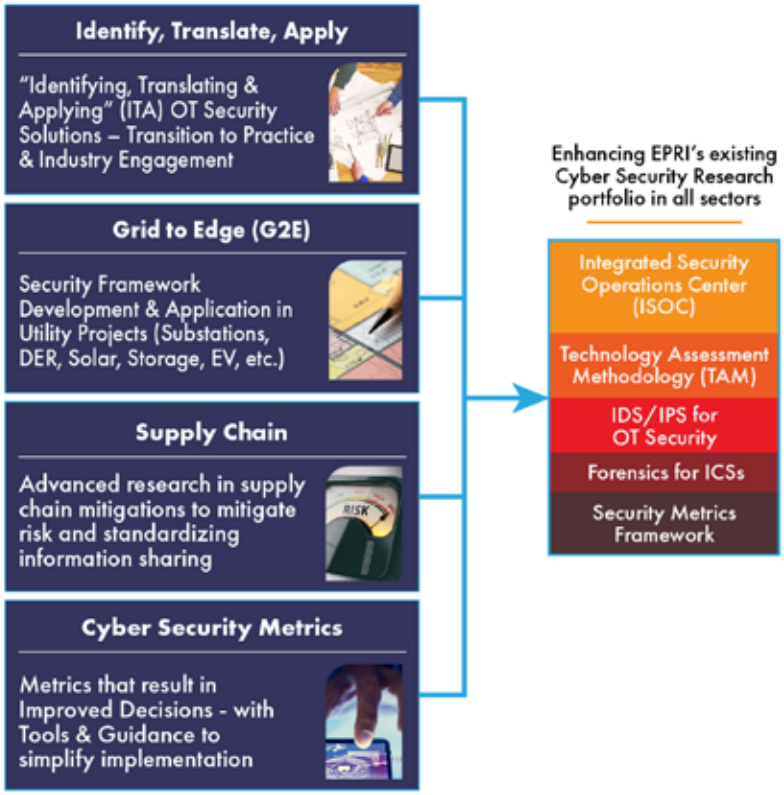
Matt Wakefield
Director ICCS
Cyber Security Strategic Initiative
email: mwakefield@epri.com

The Cyber Security Strategic Initiative (CSSI) is a 3-year (2019-2021) investment approved by the EPRI Board Initiative to build technical capabilities, industry engagement, and a self-sustaining business model that engages utilities, government stake-holders, universities, to harden existing infrastructure while enabling future integrated grid technologies.

The initiative is addressing cyber security gaps identified by utility executives that will enhance the strong foundation of our cyber security research as well as improve executive and industry engagement to help facilitate awareness and transfer of research results to industry.

The four areas of focus for the initiative are shown in the graphic

The CSSI executive committee provides guidance on this research and is made up of mostly CISO's identified by CEO's on EPRI's Board of Directors along with other key industry executives. Research accomplished in this initiative will migrate into the associated research programs – Cyber Security for Power Delivery (183) Cyber Security for Generation (209) and the Nuclear sector cyber security research.



Some of the deliverables and projects incude:

3002016153	Cybersecurity Considerations for Distributed Energy Storage
3002017753	Developing a Cyber Security Culture in the Operational Technology (OT) Environment, Training
3002016796	EPRI Cyber Security Metrics Operationalization and Benchmarking Pilot
3002016154	Grid Security of Connected Devices: Communications and Cybersecurity Assessment report
3002017455	Data Foundations for Operations Technology Cyber Security Analytics, Artificial Intelligence and Other Data Intensive Applications
3002017720	Low-Cost, Secure DER Network Gateways for Control Integration of Smart Inverters
3002017578	PRE-SW: Supply Chain Security Exchange (SCSE) v1.0 (http://scse.epri.com)
3002016781	Security Architecture for DER Integration report
3002017149	SEL 487E Protective Relay Reference Cyber Security Data Sheet (CSDS): Cyber Security Technical Assessment Methodology Use Case Study
3002017754	Training Survey and Gap Analysis: Electric Sector Cyber Security Initiative
	Integrated Security Operations Center (ISOC) buildout for Automated Threat Research in Knoxville Security Lab

Training:

3002017753	Developing a Cyber Security Culture in the Operational Technology (OT) Environment

Cyber Security for PDU Program Review 2

Industry Collaboration and Technology Transfer

The landscape of cyber security activities in the electricity sector involves numerous industries, government, and regulatory groups. Although tracking these groups can be a daunting effort, it is critical for utilities to be up-to-date on key industry activities. This research area provides members with an up-to-date view of industry activities and supports technical contribution to these groups. It also supports white papers and working groups on key cyber security topics.

Industry Collaboration and Technology Transfer

Erica Loveday
Technical Assistant III
email: **egloveday@epri.com**

Project Number and Namer	**2019 ACCOMPLISHMENTS**	**2020 PLAN**
P183.001 **Industry Collaboration**	**3002015870** Cyber Security Industry Updates: 2019 Edition summarizes monthly updates provided to utilities on cyber security activities and events that are impacting the electric sector. The goal is to cover the activities of industry groups, government organizations, regulatory bodies, and research groups from around the world.	The reports developed during this project will provide a single reference point for members to track the detailed efforts of several industry groups. This project may also increase the relevance and utility of the security reports, controls, and technologies that are being developed by these groups. Cyber Security Industry Updates – The 2020 Edition will provide a summary of the 2020 industry collaboration activities.

Cyber Security for PDU Program Review 3

Cyber Security for Incident and Threat Management Task Force

The electric power sector continues to be a high-value target for cyber-attacks. While the frequency and complexity of attacks continue to increase, the attack vectors and attack surface for electric power utilities have also expanded, introducing greater risk to the power grid. It is important for utilities to establish plans, procedures, and technologies to address and manage these risks. The Incident and Threat Management Task Force focuses on research to improve the capabilities of utilities to detect, identify, analyze, manage and respond to cyber security threats and vulnerabilities as early in the Cyber Kill Chain® as possible.

Ralph King
Program Manager
email: reking@epri.com

Project Number and Name	**2019 ACCOMPLISHMENTS**	**2020 PLAN**
P183.005: **Incident Management**	Members can apply the results of this project to guide the implementation of their incident management program, focusing on monitoring, detection, response, and forensics analysis. **3002017690** The Integrated Security Operations Center (ISOC) Guidebook V2 describes strategies and guidelines for electric power utilities to design, implement, and operate ISOCs	The Integrated Security Operations Center (ISOC) Guidebook Update. Cyber Security Attack Scenario Library adds attack scenarios for distribution to the library. Automation for the Integrated Security Operations Center (ISOC) provides strategies and technical specifications for automating ISOC functions, utilizing tools such as machine learning.

Cyber Security for PDU Program Review 4

Cyber Security for Incident and Threat Management Task Force

Project Number and Name	**2019 ACCOMPLISHMENTS**	**2020 PLAN**
P183.017: **Cyber Security Forensics**	**3002016504** Forensics Analysis Guidelines for Power Delivery Systems – provides guidelines for implementing forensics analysis capabilities for industrial control systems within power delivery systems.	Members can apply the results of this forensics project to guide the development of their cyber security forensics program, which will serve as a key component of their incident management program. Forensics next steps 2020: • Perform additional device use case studies • Draw conclusions across findings from multiple devices • Document abstracted common processes, best practices, and analysis approaches in general forensics guidebook

Cyber Security for PDU Program Review 5

Cyber Security for Incident and Threat Management Task Force

Project Number and Name	**2019 ACCOMPLISHMENTS**	**2020 PLAN**
P183.006: **Threat Management**	Results of this project can be used to effectively design, deploy, and maintain threat management systems. Completed Playbooks - A Collection of steps that allow an organization to complete tasks in their policies and procedures **3002017582** Threat Automation Playbooks: Cyber Security. By using force multiplier threat automation tools can be used to automate tasks that security analysts might otherwise have to work through manually. Focus is on the considerations and requirements for ICS or OT threat automation including the following: • Threat automation for OT playbook recommendations • Threat automation for OT playbook examples 2019 Birds of a Feather Workshop for Threat Management	Identify and address challenges to applying Security Orchestration and Automation Response (SOAR) tools in a utility system. Security Orchestration and Automation Response (SOAR) Tool OT Gap Analysis report will evaluate the use of Security Orchestration and Automation Response (SOAR) tools in an OT environment. It will help articulate and plan how to address gaps in SOAR tools that are preventing OT integration.

Cyber Security for PDU Program Review 6

Cyber Security for Transmission and Distribution Task Force

The Cyber Security for Transmission and Distribution Task Force focuses on three individual domains that each have a distinct set of challenges and opportunities that will be explored through individual projects. The first domain is focused on both transmission and distribution control centers. At most utilities, system monitoring and control is performed from a small number of primary and backup facilities with connections to neighboring utilities. The second domain is targeted at both transmission and distribution substations. Each utility will typically have a significant number of substations located around their service territory, and most will have the control systems protected with buildings and perimeter fencing. Finally, there are a large number of geographically dispersed control systems within pole-top cabinets or similar enclosures along the power line right-of-way. The field systems domain was developed to address cybersecurity needs of these assets.

John Stewart
Principal Technical Leader
email: jstewart@epri.com

Project Number and Name	**2019 ACCOMPLISHMENTS**	**2020 PLAN**
P183.008: **Asset and Configuration Management**	Identify new assets through passive mechanisms, then using that preliminary ID to direct active device management measures in safe manner. To accommodate the variety of legacy devices with proprietary interfaces, additional focus will be given on using flexible tools to drive the vendor configuration and management tools directly. This will allow utilities to bridge the gap to address intelligent electronic device (IED) management of devices that will remain in service with legacy interfaces for a long period of time. **3002014136** Automating Asset and Configuration Management: Substation Devices. The typical ICS environment may use a wide range of devices that are managed through proprietary vendor configuration tools and device interfaces. These proprietary tools and legacy technologies combine to present utility engineers with several challenges for those attempting to effectively manage ICS infrastructure.	Leverage approaches for the exchange of information between passive monitoring systems (IDS) and active device management systems. Standardization through the development of an information model that describes relevant device characteristics. An Integrated Solution for Monitoring and Managing Substation Devices (Technical Update) - This report will leverage past research focused on asset identification and management to evaluate potential integrated solutions for automating the substation device management process from commissioning through operations and maintenance. Additional plans for 2020 research include the following Securing Control Centers: • Cybersecurity Training for Grid Operators (Supplemental) • Distribution Operations Cybersecurity Drill (Collaboration-P200) • Emergency Control Center Network Isolation Technology and Processes • DNP Secure Authentication v6: Interoperability Plugfest (Supplemental) Securing Field Systems: • Remote IED Management for Field Systems (Collaboration-P180) • Field Management of Cyber and Physical Security for Distribution Automation (Collaboration-P180) • LTE Security Assessment (Supplemental-P161)

Cyber Security for PDU Program Review 7

Cyber Security for Transmission and Distribution Task Force

Project Number and Name	**2019 ACCOMPLISHMENTS**	**2020 PLAN**
P183.013 **Cyber Security Compliance/ Policy-Driven Cyber Security Research**	Enable EPRI members and industry to identify, research and resolve technology challenges that may impede security or operational practices without modifying the CIP standards. Implementation Guide: Registered Entities are using virtualized systems for networking, servers or storage. Given its use, the industry has been working diligently to assess whether the NERC standards should be modified to address the various use cases of virtualization. This project will examine the NERC CIP implications of the virtualization and develop Implementation Guides to address effectivesecurity practices while managing compliance to the NERC Standards. Reference Architecture: Operating CIP Applicable Assets in the Cloud - The CIP standards present challenges for members in their pursuit of outsourcing security or operations to a 3rd party. EPRI, through collaboration with our members will develop a series of Implementation Guides and reference architectures to address the various scenarios of leveraging cloud operations.	Enable EPRI members and industry to identify, research and resolve technology challenges that may impede security or operational practices without modifying the CIP standards. Cloud-Based Reference Architecture for CIP Applicable Assets –This Technical Resource will include the development of white papers on reference architectures for low-impact BES cyber systems, and reference architectures for high- and medium-impact BES cyber systems in a cloud environment. CIP-Compliant Compliance Automation Reference Model – EPRI's study to identify practices to help improve utilities' ability to secure their environment and at the same time effectively demonstrate compliance to cyber security regulation.

Cyber Security for PDU Program Review 8

Cyber Security for DER and Grid-Edge Systems Task Force

Rapid, disruptive changes are happening in electric grids around the world. In many states and countries, initiatives are underway to integrate small, renewable generation into the distribution grid, to meet the local demand for electricity, while reducing the dependency on large, central generation facilities and long-distance transmission. This integration requires new technologies, connectivity, and intelligence which inherently exposes the grid to cyber security risks. Through its collaborative, independent R&D, EPRI is examining these emerging risks in more detail and researching solutions that can prevent, detect, and respond to the possible cyber incidents with DER and grid-edge systems.

Candace Suh-Lee
Principal Project Manager
email: csuh-lee@epri.com

Project Number and Name	**2019 ACCOMPLISHMENTS**	**2020 PLAN**
P183.012: **Cyber Security Architecture**	The objective of this project is to create a set of reference security architectures for the systems supporting the power grid. In 2019, the project focused on the network security architecture for DER integration. **3002016781** EPRI Security Architecture for the Distributed Energy Resources Integration Network: Risk-Based Approach for Network Design - provides a practical set of cybersecurity requirements pertaining to the network components supporting distributed energy resources (DER) communications.	Continuing the effort to create reference security architectures, the project will focus on security architecture for microgrid integration. The system components and characteristics specific to microgrid will be closely examined and security recommendations will be offered for both utility-owned and operated systems and systems in the customer site. Planned deliverable: Security Architecture for Microgrid Integration.

Cyber Security for PDU Program Review 9

Cyber Security for DER and Grid-Edge Systems Task Force

Project Number and Name	**2019 ACCOMPLISHMENTS**	**2020 PLAN**
P183.018 **Cyber Security for DER & Grid-Edge Systems**	New project for 2020	This project examines various topics related to the cyber security of DER and grid-edge systems. The topics may include • Security engineering topics (smart inverter security, secure communication, cryptography, etc.) • Security application areas (cyber security for PV integration, energy storage, EV, microgrid, etc.) In 2020, the project will focus on communication protocol security. Through in-depth examination of IEEE 2030.5 (one of the three mandatory protocols for smart inverter communication according to IEEE1547-2018), the project will discuss the requirements, issues, and recommendations for secure DER communication. The analysis will not only suggest the path forward for enhancing the security of IEEE 2030.5, but also help the development of security options for other protocols widely used in DER integration. Planned deliverable: Security Assessment of IEEE 2030.5 for DER integration.

Cyber Security for PDU Program Review 10

Cyber Security Metrics

Standardized security metrics are currently not widely adopted by the electricity industry. If such metrics would exist, a utility could easily calculate and understand the value of security investments in concrete terms. EPRI's Cyber Security Metrics for the Electric Sector addresses these needs by developing a practical set of security metrics that represents the status of a utility's security posture. The EPRI research project is expected to deliver a full set of proposed metrics that will provide measures of the effectiveness of security controls.

Candace Suh-Lee
Principal Project Manager
email: csuh-lee@epri.com

Project Number and Name	**2019 ACCOMPLISHMENTS**	**2020 PLAN**
P183.014 **Cyber Security Metrics**	Quantification of cyber security has been a challenge in the utility industry, coming from the fact that there have not been comprehensive, standardized security metrics widely adopted by the industry. With metrics, a utility could easily calculate and understand the value of security investments in concrete terms. **3002013691** OpenMetCalc v1.0: EPRI Security Metrics Calculator - MetCalc is a stand-alone Windows application that allows users to load data, calculate EPRI metrics and adjust metric parameters Cyber Security Metrics for the Electric Sector report discusses the operationalization of EPRI security metrics, including the strategy to roll-out security metrics and efficiently collect data for the calculation of metrics	In 2020, the project will focus on the following areas: EPRI Cyber Security Metrics Operationalization Guideline discusses the operationalization of EPRI security metrics, including the strategy to roll-out security metrics and efficiently collect data for the calculation of metrics. Public release of MetCalc (EPRI Metrics Calculator tool) and Metrics Hub (Metrics Benchmarking Platform). Industry adoption and continued improvement of metrics and the tools through the International Metrics Advisory Council (MAC).

Cyber Security for PDU Program Review 11

Technology Innovation (TI)

TI projects generally have longer-term goals (greater than five to ten years out) and have higher research risks. Learnings from TI projects can inform and inspire future Research Portfolio (ARP) projects and provide thought leadership for EPRI, its members and other relevant stakeholders. All TI deliverables in a given year are available to all EPRI members investing in an EPRI research program in that year.

Project Number and Name	**2019 ACCOMPLISHMENTS**	**2020 PLAN**
Cyber Security Technology Innovation Projects	**3002015657** Program on Technology Innovation: Managing Cloud Storage and BES Cyber System Information - addresses third-party, cloud-based hosting of sensitive utility data. It examines the various methods of cloud-based data storage and strategies for securing the data off the utility's premises. The paper also explores the implications of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards on cloud-based storage of utility data, especially bulk electric system (BES) cyber system information (BCSI). **3002017577** Technology Innovation Program: Secure Cloud Reference Architecture for Real-Time Utility-Based Applications - introduces cloud concepts and security approaches that are unique to off-premise cloud implementation and provides foundational considerations for reference architectures to manage cloud service provider deployments for grid-edge applications, low-impact BES Cyber Systems located in the cloud and managed security services for low impact BES Cyber Systems.	EPRI's Technology Innovation projects examines the problems with broader industry implication with long-term perspective. In 2020, the following three projects will provide the additional security insights for DER, grid-edge systems and cloud based architectures. Smart Inverter Hardware Security provides technical guidelines on how to secure the hardware elements for secure communication of smart inverters. The project will provide guidelines for inverter procurement, as well as secure design of microcontrollers within smart inverter communication modules. Grid Cyber Security for Automated Demand Response (DR) Ready Buildings investigates the cybersecurity gaps, potential cyber-risks by the grid-connected buildings. Cloud-based Reference Architectures for Low Impact BES Cyber Systems, Control Centers and Grid-Edge Applications testing and implementation. The results will be further analyzed and shared.

Cyber Security for PDU Program Review 12

GPS Cyber Security Assessment Help Understand Risks for Transmission Applications

As critical infrastructure end-users deploy more automated technologies in their applications, they will become increasingly reliant on time synchronization. These applications have different timing requirements and sensitivities, including mechanisms to enable time synchronization. Examples of widely used methods and technologies used to provide and distribute time synchronization data include U.S. Global Positioning System (GPS), Russia's GLONASS, IEEE's 1588 Precision Time Protocol (PTP), eLOng-Range Navigation (eLORAN) and others. But these technologies also introduce cybersecurity vulnerabilities and timing uncertainties.

The US Department of Homeland Security (DHS) has confirmed vulnerabilities in precision timing that may pose risks to applications used in operations that rely upon highly accurate timing. With the lack of clarity for potential risks created by precision timing vulnerabilities, there is also an absence of field-tested and proven mitigations for many of these vulnerabilities. Existing research on mitigations for vulnerabilities in applications that depend upon precision timing, for the most part, has not been widely adopted, and their effectiveness in utility environments has not been widely established.

In order to address these issues, EPRI launched a Timing Security Assessment Supplemental project. EPRI worked closely with utility asset owners to identify specific time synchronization dependent devices used in the industry and to select applications that could demonstrate the downstream effects of cyber security attack exploits. EPRI, utility asset owners and experts in the industry created a test procedure and test environments at different laboratories to perform real time hardware in the loop (RT-HiL) testing.

Project Lead:
Gerardo Trevino
gtrevino@epri.com

Cyber Security for PDU Program Review 13

"EPRI's research brought to light credible concerns, and is now moving toward actionable solutions. Vulnerabilities involving Positional Navigation Timing (PNT) are an issue in numerous industries around the world. Everyone is a stakeholder and is impacted when it relates to timing and the power industry; as they are common dependencies woven into the fabric of modern society. EPRI's research will help us communicate and work together on solving problems in an area that has been underestimated or misunderstood. I am impressed by how swiftly and effectively EPRI can take expertise from outside the electric power industry and apply it to this endeavor. I anticipate the findings and deliverables from this research will have influence beyond the electric power industry."

William Vesely
Project Specialist
Consolidated Edison Company of New York

The objective for the testing was to recreate applications deployed in the field and to evaluate their performance against the attack vectors described in the test procedure. EPRI has also identified a preliminary list of mitigation technologies available in the market that are intended to be evaluated in a second phase supplemental project.

Key Recommendations for utilities include:

- Developing a time synchronization modernization roadmap to include IEEE 1588, new GPS receivers, detection technologies and architecture best practices.
- Monitoring GNSS/GPS devices to understand if they enter in error states such as "unlocked".Understanding GPS satellites power level behavior may also provide a mechanism of detection for spoofing attacks
- Leveraging modern network monitoring technologies to identify possible signatures of GPS attacks. These technologies can provide automatic anomaly detection if implemented properly.

The EPRI Cyber Security Team will continue to work with industry and members that are part of the research project that has been launched for 2019-2020. In addition, EPRI has launched a Technology Innovation (TI) funded interest group, the Resilient Time Synchronization for Energy Sector group intends to create a virtual forum for stakeholders to share experiences, talk about tools and techniques and explore research topics while maintaining impartiality, independence, and vendor neutrality. EPRI provides this forum without charge as a service to the industry and to promote the importance of reliable time synchronization data in the energy sector.

The abstract information for the phase I and phase II projects can be found in the documents, **3002008952** and **3002016546**.

The final report for the phase I project is reflected in the deliverable, Timing Security Assessment and Solutions: Supplemental Project Report, **3002017347**.

The new Resilient Time Synchronization for Energy Sector Interest Group will have a kick-off meeting in March 10-11, 2020 at EPRI's office in Dallas, Texas.

EPRI Security Architecture for the DER Integration Network and 2019 DER Cyber Security Workshop

As distributed energy resources (DERs) expand rapidly as a major source of electricity generation and interconnect with the grid, the ability to securely monitor and control the operations of the resources in a large geographical area becomes increasingly important to maintain safety, reliability, and resiliency of the nation's grid. 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.

EPRI Security Architecture for the DER Integration Network 3002016781 provides a practical set of cybersecurity requirements pertaining to the network components supporting distributed energy resources (DER) communications. The requirements specified in the report can be used by utilities, DER integrators or aggregators to reduce the cybersecurity risk to the distribution grid to which various DERs
are connected.

The report has been produced with a collaborative effort with EPRI Cyber Security Task Force for DER and Grid-Edge Systems and was reviewed by industry interest groups during the 2019 EPRI DER Cyber Security Workshop (July 16, 2019, Palo Alto).

Project Lead:
Candace Suh-Lee
csuh-lee@epri.com

EPRI DER Cyber Security Workshop (Palo Alto, CA)

Value Realized:
In the general absence of comprehensive cyber security requirements in DER-related industry standards, EPRI 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. The report also 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.

Leadership/Innovation Demonstrated:
The report outlines the methodology where,

- DERs are categorized into high-impact, medium-impact, and low-impact systems;
- The network is designed in the way that high-impact systems require more strict security controls; and
- Implementation and maintenance cost for security is reduced with the risk-based strategic allocation of security measures

This approach demonstrates the very first adaptation of the risk-based security principles to the DER integration area. The requirements and the underlying methodology have become an important influence on the IEEE 1547 community and stimulated an active discussion on the needs for cybersecurity for the DER integration network.

"EPRI's security architecture for DER network integration provides simple and practical guidelines that all utilities can implement. It provides key security guidance that should be considered when connecting myriad devices, systems, and microgrids that will be connecting to the distribution power grid in the near future".

Mark Johnson-Barbier
Sr. Principal Analyst
Salt River Project (SRP)

"EPRI is leading the charge to help electric utilities understand cybersecurity risks affecting Distributed Energy Resources (DERs). In particular, their annual DER Architecture Workshops are very helpful in bringing together operators, engineers and architects from across the globe to discuss relevant security issues that directly impact grid modernization efforts, thus helping utilities improve reliability and resiliency of the electric grid in a more consistent fashion."

Jason Hill
Security Architect Lead
American Electric Power (AEP)

Cyber Security for PDU Program Review 16

Supplemental Projects

Supplemental Projects are research, development or demonstration projects offered outside of the annual research portfolio. These projects 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.

Status

Cyber Security Incident Response and Recovery Tabletop Exercise 3002017679
Ralph King, *rking@epri.com*

With inclusion/dependence on processor-based power delivery/ communications infrastructure, attacks by malevolent cyber agents increase. NERC CIP-008 and CIP-009 require utilities to test their Incident Response

Each tabletop exercise is designed for a specific utility and is independent of other members.

Cloud Security Reference Architecture for Real-time Utility-Based Applications 3002017697
Tobias Whitney, *twhitney@epri.com*

This project identifies how utilities can remain CIP standards compliant while using cloud-based operational technology services.

Project start expected early 2020.

EPRI Cyber Security Metrics Operationalization and Benchmarking Pilot 3002016796
Candace Suh-Lee;*csuh-lee@epri.com*

This project aims to provide tools, processes, guidance, and training necessary to measure the performance of security investments through standardized metrics and benchmark security performance anonymously and securely.

Project start expected early 2020.

Industrial Control Systems Penetration Testing 3002013989
Ralph King, *rking@epri.com*

The project discovers vulnerabilities in utility owned ICS equipment and compile tools and methods to assist with the detection of vulnerabilities in utility owned ICS equipment.

Training class held in Knoxville that covered a variety of methods to be used to perform penetration and vulnerability testing of embedded systems. Penetration Testing performed on Novatech Orion LX and SEL 421

Intrusion Detection Systems/Intrusion Prevention Systems Solutions Analysis and Testing for ICS Environments 3002012235
Ralph King, *rking@epri.com*

Provide guidance on assessing solution selection for IDS/IPS solutions and will evaluate effectiveness of IDS/IPS solutions during various types of cyber-attacks and incidents.

Second round testing complete on Nozomi, Claroty, and ForeScout IDS, Dragos installed and under test in the Knoxville lab, reporting wrapping up for tested IDS systems.

Cyber Security for PDU Program Review 17

Status

Insider Threat Management 3002017819

Ralph King, *rking@epri.com*

This project will provide information and prescriptive guidance to build and implement an Insider Threat Management Program that will result in more secure utility operations.

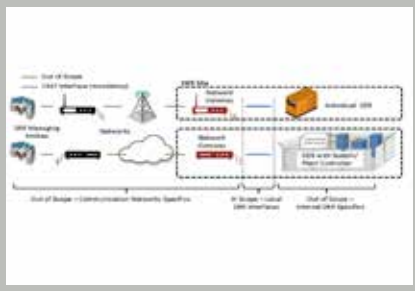
Project start expected early 2020.

Low-Cost, Secure DER Network Gateways for Control Integration of Smart Inverters 3002017720

Xavier Francia, *XFrancia@epri.com*

This project will identify key DER gateway capabilities to supplement requirements in California Rule 21 and IEEE 1547-2018. Evaluate technical and economic feasibility of DER gateway platforms and associated features.

Project start expected early 2020.



Timing Security Assessment and Solutions 3002008952

Gerardo Trevino, *gtrevino@epri.com*

Progressive approach for addressing cyber security vulnerabilities in precision timing systems used in mission-critical utility operations. The results will provide significant power industry and public benefits, particularly focused on improved power grid reliability and resiliency.

Identified 4 vulnerabilities related to GPS spoofing. Progress to identify additional equipment and start identification of specific applications to be tested. Early project adopters are in the process of determining which applications are of interest for testing. Two have been determined and are moving forward with steps needed to test differential relay protection, new communication systems (MPLS) and PMU susceptibility/impact related to the vulnerabilities identified to date. The final 2019 report for Phase I is Timing Security Assessment and Solutions: Supplemental Project **3002017347**

Timing Security Assessment and Solutions: Phase II 3002016546

Gerardo Trevino, *gtrevino@epri.com*

2nd Phase of this project will explore different mechanisms to be used as a basis for this synchronization or precision timing. Some widely used methods include Global Positioning Satellite (GPS) signals, Network Time Protocol (NTP), and IEEE's 1588 Precision Time Protocol (PTP).

Working with industry stakeholders to create an EPRI funded Interest Group, the new Resilient Time Synchronization for Energy Sector Interest Group will have a kick-off meeting on March 10-11,2020 at the EPRI Dallas office in Texas. The Interest Group will help identify mitigation technologies available in the market to be evaluated and tested under the second phase of this supplemental project.

Cyber Security for PDU Program Review 18

Cyber Security Technology Transfer Activities January - December 2019

2 Advisory Meetings	**3343 Deliverables Downloads (includes public downloads)**	**7 Deliverables Overview Videos**
8 Workshops/Conferences	**7,148 Member Center Visits**	**18 Technical Advisor Member Visits**
19 Webcasts	**12 Task Force Meetings/webcasts**	**Steve Sanders/Southern Company Program Utility Chair**

Cyber Security Technology Transfer Award Winners

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 2018 - 2019 time period. Awards were selected in the Fall of 2019 and are presented at the following year February 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 Lisa Moller, John Kotolski	Integrated Security Operations Center (ISOC) (2019)	Implemented and demonstrated the application of EPRI cyber security research providing requirements and design considerations for an Integrated Security Operation Center (ISOC). Valuable feedback and information sharing for the entire industry.
Consolidated Edison Company of New York Arman Shiplu, Selena Ley, William Vesely **FirstEnergy Service Company** Scott Hipkins, M. Scott Poley, Marcus Noel **New York Power Authority** Paul Silba, Jeffrey Staten, Kenneth Carnes **Pacific Gas & Electric** Xavier Francia, Joe Sagona, Fernando Medrano	Cyber Security Metrics for the Electric Sector (2017)	The participating utilities and EPRI worked closely together to ensure that the calculated metrics reflect the security status of sampled systems. Once the 58 metrics were successfully calculated and tuned, the project team held the metrics review session with the various stakeholders within the company to review the metrics calculated.
Mississippi Power Company Joseph Stewart **SCANA Corporation** Mukesh Maisuria, Andrew Bowden, Will Hayden **Southern Company** Steve Sanders , Christopher Taylor, Guy Palmer	The Integrated Security Operations Center (ISOC) (2017)	ISOC is a platform to detect, alert and respond to cyber security threats. Southern Company and SCANA Corporation have taken EPRI's ISOC framework and implemented it within their organizations and proactively shared results with members.

Cyber Security for PDU Program Review 19

Cyber Security Research Laboratory (CSRL)

Ben Sooter
Principal Project Manager
email: bsoooter@epri.com

Cyber Security is rapidly evolving and through collaboration, research, and strategic partnerships EPRI hopes to provide utilities the tools to protect their networks and assets for years to come. The CSRL is made up of a collection of different types of utility equipment and cyber security defense systems. The research performed in the lab identifies how to integrate new technologies and architectures and measure their effectiveness, so intelligent decisions can be made about new cyber security solutions deployed into a utility environment. The lab has a library of utility focused cyber security use cases that can be run against test beds to demonstrate the effectiveness of architectural changes or the introduction of new technologies.

Research investigations include:
- Integrated Security Operations Center Project (ISOC)
- Integrated Threat Analysis Framework Project (ITAF)
- Network Management Systems Project
- Open Enabling Platform Project
- Intrusion Detection System and Intrusion Prevention System Project

Past research and testing statistics: Over $2.5 million worth of hardware, software, and other equipment
- 172 devices from over 30 manufacturers
- Over 295 Terabytes of storage connected to 108 virtual machines and servers by 1.5 miles of network cable
- Configured to support multiple SCADA protocols
- 9 Cyber Security engineers and managers
- Evaluation of new technologies and architectures
- Penetration testing and forensic analysis of embedded systems

Specialized Exploits Available
- Advanced a man-in-the-middle (MITM) attacks against DNP3 utilizing ARP spoofing and IP hijacking
- Advanced MITM manipulation of C37.118 PMU data streams manipulation via ARP spoofing
- IEC 61850 (GOOSE) message replay attacks
- CrashOverride / Industroyer, Havex, Black Energy and DragonFly malware

Penetration Testing: Fuzzing, Vulnerability Scanning, Attack Surface Evaluation

Vendor Testing:
- ISOC Lab: SIEMs, splunk, IBM, Rada, LogRhythm, Elastic, Gravwell, Graylog, Alien Vault
- Physical Security: Honeywell Security
- Security Orchestration, Automation and Response (SOAR): Phantom, Demisto
- Substation Lab: Schweitzer Engineering Laboratories, GE Power, ABB, Siemens, NovaTech, Schneider Electric, Cooper Power Systems, OMICRON, AREVA
- IDS/IPS: Fortinet, Q-Net Security, CyberX, Dragos, Claroty, Nozomi Networks, Forescout, Sierra Nevada Corporation
- Testbed Example - Test bed data networks available: DNP3, IEC 61850, C37.118, Sunspec Modbus

IT Networking Equipment
Level 1 Switches: MRV
Level 2 Switches: Cisco, RuggedCom, ABB
Level 3 Switches/Routers: Cisco

Serial Analysis

2019 ACCOMPLISHMENTS

Development of a full Integrated Security Operations Center (ISOC) lab containing the integration of security information across IT, OT, and physical. Additionally, a complete threat automation environment was stood up to evaluate how automation can be applied to OT.

2020 PLAN

Expand the cyber security research lab (CSRL) DER and grid edge capabilities to include an end to end DER test area that can evaluate technologies from end points, such as inverters, to distributed energy resource management systems (DERMS), and everything in between.

Cyber Security for PDU Program Review 20

Guidebooks

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

Title	PID#	Year
Operational Technology Forensics Guidebook Use Case: NovaTech OrionLX	3002016504	2019
The Integrated Security Operations Center Guidebook: Version 2	3002017690	2019
The Integrated Security Operations Center (ISOC) Guidebook	3002013903	2018
Guidelines for Enhancing Threat Intelligence Programs for Power Delivery Systems	3002013701	2018
Guidelines for Deploying Application Whitelisting	3002003919	2018
Guidelines for Implementing a Threat Hunting Program for Power Delivery Systems	3002010601	2017
Guidelines for Integrating Substation and Field Domain Events into an Integrated Security Operations Center	3002005946	2015
Risk Management in Practice: A Guide for the Electric Sector	3002003333	2014
DNP3 (IEEE Std 1815TM) Secure Authentication: Implementation and Migration Guide and Demonstration Report	3002003736	2014
Guidelines for Integrating Control Center Systems Into an Integrated Security Operations Center	3002003739	2014
Guidelines for Justifying Risk-Based Cyber Security Control Projects for Utility Business Units	3002000391	2014
Guidelines for Planning an Integrated Security Operations Center	3002000374	2013
Lemnos Implementation Guide for IPsec: Device Configuration Examples	3002000375	2013
Secure ICCP Implementation Guide	1024420	2012
AMI Cyber Security Incident Response Guidelines	1026554	2012

Cyber Security for PDU Program Review 21

Onsite Training

Title	DATE
Cyber Security Procurement Methodology Revision 2 Workshop, Charlotte	October 7- 8, 2019
Cyber Security Technical Assessment Methodology (TAM) Revision 1 Workshop	October 8-11, 2019

Videos

2019 Deliverable Overview Videos are available for viewing and download on the **member center program home page**

Cloud Based Security Solutions
Cyber Security Analysis of Electric Vehicle Extreme Fast Charging Infrastructure
Embedded Device Forensics & Penetration Testing
EPRI Threat Automation
Grid Flexibility using OpenADR
How secure is Cyber Security Data Protection with Transport Layer Security (TLS) Encryption?
Physically Unclonable Functions (PUF)

Software

Software products to support member companies address complex issues

Title	PID#	Year
OpenMetCalc v1.0	3002013691	2019
PRE-SW: Security Metrics Calculator (MetCalc), version 0.1 – Beta	3002010413	2017
Security, Cyber, Risk Assessment Methodology (SCRAM), version 3.0	3002010421	2017
Security Testing Tool for End-User Devices (PT2) Version 2.0	3002005804	2015

Cyber Security for PDU Program Review 22

AMI

Secure Integration of Advanced Metering Infrastructure (AMI) into Substation Networks, **1025469** (2015)

Advanced Metering Infrastructure (AMI) Cyber Security Risks, **300200389** (2013)

Advanced Metering Infrastructure Common Alarms and Events, **1026552** (2012)

Advanced Metering Infrastructure Security Objects, **1024427** (2012)

Cryptographic Key Management (CKM) Design Principles for the Advanced Metering Infrastructure (AMI), **1024431** (2012)

AMI Cyber Security Incident Response Guidelines, **1026554** (2012)

Intrusion Detection System for Advanced Metering Infrastructure, **1026553** (2012)

Asset and Configuration Management

Asset Discovery and Configuration Management for Substation Devices, **3002014136** (2019)

Patch Regression Analysis Testing, **3002014137** (2018)

Exploring an Open Model for Control Systems Device Fingerprinting for Passive Identification, **3002010336** (2017)

Patch Management Guidelines, **3002011187** (2017)

Passive Identification of Substation Assets, **3002010418** (2016)

Industry Collaboration

Cyber Security Industry Updates: 2019 Edition, **3002015870** (2019)

Cyber Security Industry Updates: 2018 Edition, **3002014707** (2018)

Cyber Security Industry Updates: 2017 Edition, **3002010337** (2017)

Cyber Security in the Energy Sector – Recommendations for the European Commission, **3002010341** (2017)

Cyber Security Industry Updates: 2016 Edition, **3002007701** (2016)

Incident Management

Modernization of the Cybersecurity Program and Implementation of the Integrated Security Operations Center at the Tokyo Electric Power Corporation, **3002016738** (2019)

The Integrated Security Operations Center (ISOC) Guidebook: Version 2, **3002017690** (2019)

Operational Technology Forensics Guidebook Use Case: NovaTech OrionLX **3002016504** (2019)

Cyber Security Forensics for Industrial Control Systems: Summary of Utility Tabletop Exercises, **3002013991** (2018)

The Integrated Security Operations Center (ISOC) Guidebook, **3002013903** (2018)

Integrating Cyber and Physical Security for Power Delivery Systems: An NEC Case Study, **3002010593** (2017)

Implementing Intrusion Detection/Prevention Systems for Power Delivery Systems: Phase 2, **3002010595** (2017)

Implementing Intrusion Detection/Prevention Systems for Power Delivery Systems, **3002009369** (2016)

Guidelines for Integrating Substation and Field Domain Events into an Integrated Security Operations Center, **3002005946** (2015)

Guidelines for Integrating Control Center Systems Into an Integrated Security Operations Center, **3002003739** (2014)

Guidelines for Planning an Integrated Security Operations Center, **3002000374** (2013)

Implementation and Migration

Timing Security Assessment and Solutions: Supplemental Project Report, **3002017347** (2019)

Secure Remote Substation Access: Supplemental Project Report, **3002014132** (2018)

Timing Security Assessment and Solutions, **3002010336** (2016)

DNP3 Security Evolution 2016, **3002010417** (2016)

Configuration Management and North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) v5, **3002010601** (2015)

Deployment Options and Considerations for Substation Security Gateways: P183A Working Group White Paper, **3002010595** (2015)

Distributed Network Protocol (DNP3) Security Interoperability Activities 2015, **3002005945** (2015)

Security Implications and Considerations for Serial to IP-Based SCADA Migration Revisited, **3002006492** (2015)

DNP3 (IEEE Std 1815TM) Secure Authentication: Implementation and Migration Guide and Demonstration Report, **3002003736** (2014)

Intelligent Electronic Device Password Management Strategies, **3002000372** (2013)

Security Implications and Considerations for Serial to Internet Protocol-Based Supervisory Control and Data Acquisition Migration, **1025674** (2012)

Secure ICCP Implementation Guide, **1024420** (2012)

Substation Intelligent Electrical Devices (IED) Password Complexity and Capabilities Study, **1025675** (2012)

Substation Security and Remote Access Implementation Strategies, **1024424** (2012)

National Electric Sector Cybersecurity Organization Resource (NESCOR)

Analysis of Selected Electric Sector High Risk Failure Scenarios– Version 2.0 (2015)

Electric Sector Failure Scenarios and Impact Analyses–Version 3.0 (2015)

Electric Sector Failure Scenarios Common Vulnerabilities and Mitigations Mapping–Version 2.0 (2015)

Guidelines for Leveraging NESCOR Failure Scenarios in Cyber Security Tabletop Exercises (2014)

Attack Trees for Selected Electric Sector High Risk Failure Scenarios – Version 2.0 (2013)

NESCOR Guide to Penetration Testing for Electric Utilities (2013)

Smart Energy Profile (SEP) 1.x Summary and Analysis, Version 1.0 (2011)

Network and System Management

Systems and Security Monitoring: KEPCO Implementation of the IEC 62351-7 Standard, **3002010587** (2017)

Network and System Management: Advanced Application of the IEC 62351-7 Standard and Utility Pilot Project, **3002005944** (2015)

Network System Management: Implementations and Applications of the IEC 62351-7 Standard, **3002003738** (2014)

Network System Management: End-System-Related International Electrotechnical Commission (IEC) 62351-7 Object Definitions, **3002000373** (2013)

Securing Cell Relay Networks, **3002000390** (2013)

Network and System Management for Reliability and Cyber Security, **1024418** (2012)

Network Security Management for Transmission Systems, **1024421** (2012)

Procurement

Potential for Blockchain Technology Application in Electric Power Industry Supply Chain Security, **3002010433** (2017)

Cyber Security Procurement Requirements Traceability for the Electric Sector, **3002003331** (2014)

Cyber Security Procurement Methodology for Power Delivery Systems, **1026562** (2012)

Risk Management and Assessment

Cybersecurity Considerations for Distributed Energy Storage, **3002016153** (2019)

Cyber Security Risk Management for the Multi-Party Grid, **3002013699** (2018)

Cyber Security Risk Management Database Update–Security, Cyber, Risk Assessment Methodology Database (SCRAM) v2.0, **3002010419** and **3002010421** (2017)

Cyber Security Risk Management Database Overview: Security, Cyber, Risk Assessment Methodology Database (SCRAM) Version 3.0, **3002010419** (2017)

Security, Cyber, Risk Assessment Methodology (SCRAM), Version 3.0, **3002010421** (2017)

The Common Operating Picture for Power Delivery Systems, **3002010590** (2017)

*Cyber Security Compliance Database Overview,***3002010419** (2016)

Security, Cyber, Risk Assessment Methodology (SCRAM Database) Version 2.0, **3002007889** (2016)

Cyber Security Risk Management in Practice: Comparative Analyses Tables, **3002004712** (2014)

Guidelines for Justifying Risk-Based Cyber Security Control Projects for Utility Business Units, **3002000391** (2014)

*Risk Management in Practice: A Guide for the Electric Sector***, 3002003333** (2014)

Security Posture using the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), **3002003332 (**2014)

Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology, **3002001181** (2013)

Cyber Security Strategy Guidance for the Electric Sector, **1025672 (**2012)

Electric Sector Cyber-Physical Attack Scenarios to Support Risk Assessment Models, **1025842** (2012)

Security Architecture and Security Metrics

EPRI Security Architecture for the Distributed Energy Resources Integration Network: Risk-Based Approach for Network Design **3002016781** (2019)

EPRI Cyber Security Metrics – A Continuous Process Driving Decisions to Reduce Risk, **3002017501** (2019)

Cyber Security Metrics for the Electric Sector: Volume 4, **3002013690 (**2018)

Security Architecture for Distribution Systems: Reference Architectures and Attack Modeling, **3002013697** (2018)

Substation Security Architecture Reference Diagrams Version 2.0. **3002012484** (2018)

Cyber Security Metrics for the Electric Sector: Volume 3, **3002010426** (2017)

*Microgrid Attack Surface Analysis***, 3002010418** (2017)

PRE-SW: Security Metrics Calculator (MetCalc), Version 0.1 – Beta, **3002010413** (2017)

Substation Attack Surface Analysis, **3002010417** (2017)

Creating Security Metrics for the Electric Sector Version 2.0, **3002007886 (**2016)

Security Architecture Methodology for the Electric Sector, Version 2.0, **3002007887** (2016)

Substation Security Architecture Reference Diagrams, **3002009519** (2016)

Creating Security Metrics for the Electric Sector, **3002005947** (2015)

Cyber Security Architecture Methodology for the Electric Sector, **3002005942** (2015)

Tabletop Exercises

Cyber Security Tabletop Exercise Facilitation Plan and Master Scenario Event List, **3002004722** (2015)

Cyber Security Tabletop Exercise After Action Report and Improvement Plan, **3002004725** (2015)

Cyber Security Tabletop Exercise Player Handbook, **3002004723** (2015)

Multi-Year Cyber Security Tabletop Exercise Plan, **3002004721** (2015)

Technology Innovation

Technology Innovation Program: Secure Cloud Reference Architecture for Real-Time Utility-Based Applications **3002017577** (2019)

Program on Technology Innovation: Managing Cloud Storage and BES Cyber System Information **3002015657** (2019)

Deception Technology – Emerging Cyber Security Technology for Utilities, **3002017417** (2019)

Testing

Security Testing Tool for End-User Devices (PT2) Version 2.0, **3002005804** (2015)

Security Resiliency Testing, **3002001187** (2013)

Distributed Network Protocol (DNP3) Security Interoperability Testing 2012, **1026561** (2012)

Security Testing Techniques for End-User Devices, **1024428** (2012)

Threat Management

Integrated Threat Analysis Framework Project: FirstEnergy Testing Report **3002009875** (2019)

Integrated Threat Analysis Framework Project: SCANA Testing Report **3002009877** (2019)

Threat Automation Playbooks: Cyber Security, **3002017582** (2019)

The Integrated Threat Analysis Framework, **3002017341** (2019)

Guidelines for Enhancing Threat Intelligence Programs for Power Delivery Systems **3002013701** (2018)

Guidelines for Implementing a Threat Hunting Program for Power Delivery Systems, **3002010601** (2017)

Technical Leads

Contact Name	Title	email
Matt Wakefield	Director, Information Communication Technology and Cyber Security for Power Delivery and Utilization	mwakefield@epri.com
Galen Rasche	Sr. Program Manager	grasche@epri.com
Tobias Whitney	Technical Executive	twhitney@epri.com
Christine Hertzog	Pricipal Technical Leader	chertzog@epri.com
Ivan Dragnev	Pricipal Technical Leader	Idragnev@epri.com
Ralph King	Program Manager	reking@epri.com
Ben Sooter	Principal Project Manager	bsooter@epri.com
Erica Loveday	Technical Assistant III	egloveday@epri.com
John Stewart	Principal Technical Leader	jstewart@epri.com
William Webb	Technical Leader	wwebb@epri.com
Candace Suh-Lee	Principal Project Manager	csuh-Lee@epri.com
Alekhya Avadhanula	Engineer/Scientist I	aavadhanula@epri.com
Alekhya Vaddiraj	Engineer/Scientist II	avaddiraj@epri.com
Esther Amullen	Engineer/Scientist II	eamullen@epri.com
Gerado Trevino	Technical Leader	gtrevino@epri.com
Sai Ram Ganti	Engineer/Scientist II	sganti@epri.com
Xavier Francia	Sr. Technical Leader	xfrancia@epri.com
Ben Sooter*	Principal Project Manager	bsooter@epri.com
Chris Stapler	Engineer/Scientist II	cstapler@epri.com
Greg Drewry	Engineer/Scientist III	gdrewry@epri.com
Larry Burnette	Engineer/Scientist II	lburnette@epri.com
Luke Varner	Engineer/Scientist I	lvarner@epri.com

(Ben Sooter listed twice to show reporting structure for lab staff)*

Contact Name	Title	email
Annette Mosley	Technical Advisor II, WEST	amosley@epri.com
Chris Kotting	Technical Advisor II, EAST	ckotting@epri.com
Sujit Mandal	Sr. Manager, Member and Technical Services	smandal@epri.com

Cyber Security Program Review 25

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI members represent 90% of the electricity generated and delivered in the United States with international participation extending to nearly 40 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; Dallas, Texas; Lenox, Mass.; and Washington, D.C.

Together...Shaping the Future of Electricity

TO JOIN OR FOR MORE INFORMATION, CONTACT THE FOLLOWING TECHNICAL ADVISORS:

West: *Annette Mosley, 972.556.6507; amosley@epri.com*

East: *Chris Kotting, 980.219.0146; ckotting@epri.com*

International: *Kevin East, International Director, +44 (1925) 450.207; keast@epri.com*

Product ID 3002017938 January 2020

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