# Cyber Security (CS) Program (P183)

Sr. Program Manager—Galen Rasche, 650.855.8779, grasche@epri.com

## Overview

Cyber security has become a critical priority for electric utilities. The evolving electric sector is increasingly dependent on information technology and telecommunications infrastructures to ensure the reliability and security of the electric grid. Cyber security measures must be designed and implemented to support grid reliability. These measures must also support grid resilience against attacks by terrorists and hackers, natural disasters, and inadvertent threats such as equipment failures and user errors.

The Cyber Security Program of the Electric Power Research Institute (EPRI) focuses on addressing the emerging threats to the electric sector through multidisciplinary, collaborative research on cyber security technologies, standards, and business policies and processes.

## Research Value

The rapid pace of change in the electric sector creates a challenging environment for asset owners and operators to monitor the activities of industry and standards organizations, develop an understanding of the security impacts of new technologies, and assess and monitor cyber security risks. 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.

Participation in EPRI's Cyber Security Program can provide:

- Technologies which support the management of cyber incidents and increase the cyber security and resiliency of the grid
- Guidance on developing cyber security strategies and requirements for selecting effective technologies;
- Early identification of security gaps through laboratory assessments of security technologies; and
- Techniques for assessing and monitoring risk;
- Guidance on security metrics;
- A better awareness of industry and government collaborative efforts, where members can "plug in" to current activities.

## 2018 Research Areas:

- Industry Collaboration and Technology Transfer
- Integrated Security Operations Center (ISOC)
- Cyber Security Forensics for Industrial Control Systems
- Threat Management
- Passive and Safe Active Identification of Substation Devices
- Advanced Processes and Technologies for Cyber Security Compliance
- Flexible and Resilient Security Architecture
- Cyber Security Metrics
- Cyber Security Risk Management

## Looking Ahead:

**In 2019,** the Cyber Security Program has the following research priorities:

- Collaboration: Track industry and government activities and provide technical contributions to key working groups;
- Incident Management: Improve the electric sector's ability to detect, respond, and recover from cyber incidents and continue technical development of the Integrated Security Operations Center;
- Threat Management: Develop guidelines and use cases for security automation;
- Asset, Change, and Configuration Management: Develop a proof of concept system that exchanges relevant configuration and asset data between network security solutions and configuration management systems;
- Security Compliance: Identify technology-driven solutions to aid member's compliance to the Critical Infrastructure Protection(CIP) standard;
- Cyber Security Architecture: Extend the security architecture methodology to include new components for grid modernization and DER integration; and
- Cyber Security Metrics: Create a methodology supporting metrics, and framework to evaluate the effectiveness of implemented security controls within power delivery systems and operational environments.

## Industry Updates

**Issue:** The cyber security landscape is complex, with a large number of resources and activities to track. Maintaining an up-to-date and comprehensive view of trends, technologies, and standards requires a significant expenditure of time by over-subscribed utility resources.

**R&D Objective:** This research activity provides monthly updates on cyber security activities and events. It covers the activities of industry groups, government organizations, regulatory bodies, and research groups from around the world, including the Institute of Electrical and Electronics Engineers (IEEE), CIGRE, the Council on Large Electric Systems, and numerous electric industry conferences and workshops.

**Target Audience:** Cyber security architects and analysts, threat and incident response personnel, power delivery system security staff and stakeholders.

**2018 Research Results:**

- Cyber Security Industry Updates: 2018 Edition **(3002014707)**
- Key Deliverables from Previous Years:
  - Cyber Security Industry Updates: 2016 Edition (**3002007701**)
  - Cyber Security Industry Updates: 2017 Edition (**3002010337**)

**Next Steps:** The project will continue to monitor, analyze and document industry activities for utilities.

**Project Lead:** Erica Loveday, *egloveday@epri.com*

## Integrated Security Operations Center (ISOC)

**Issue:** Incident response includes detecting cyber security events, establishing criteria for event prioritization, and correlating multiple cyber security events. Utilities must establish and maintain plans, procedures, and technologies to detect, analyze, appropriately respond to cyber security events, and sustain operations through cyber security events. These criteria should align with the organization's cyber security risk management strategy and ensure consistent assessment of events. This project covers four primary areas of incident response:

- Detection of events
- Escalation of events and declaration of incidents
- Response to incidents and escalation of prioritized events
- Planning for recovery and continuity

**R&D Objective:** This research provides prescriptive guidance on the planning, design, implementation, and operation of ISOCs for electric utilities.

**Target Audience:** Chief Information Security Officers, Power Systems Operations Managers, Cyber Security Program Directors, Security Operations Managers, Cyber Security Architects, Cyber Security Engineers, Cyber Security Analysts, Physical Security Program Directors.

**2018 Research Results:**

- The Integrated Security Operations Center (ISOC) Guidebook (**3002013903**)
- The ISOC Seminar was delivered at the PDU Fall Advisory Meeting
- Key Deliverables from Previous Years:
  - Guidelines for Integrating Substation and Field Domain Events into an ISOC (2015; **3002005946**)
  - Implementing Intrusion Detection/Prevention Systems for Power Delivery Systems (2016; **3002009369**)
  - Implementing Intrusion Detection/Prevention Systems for Power Delivery Systems: Phase 2 (2017; **3002010595**)
  - Integrating Cyber and Physical Security for Power Delivery Systems – An NEC Case Study (2017; **3002010593**)

**Next Steps:**

- Build an ISOC environment in the EPRI Cyber Security Research Lab for use by various projects and by utility members for technology and use case testing.
- Produce annual update for the ISOC Guidebook.
- Introduce data analytics, artificial intelligence and machine learning tools into the ISOC to manage security incidents for power delivery systems.

**Project Lead:** Ralph King, *reking@epri.com*

## Cyber Security Forensics for Industrial Control Systems

**Issue:** A comprehensive cyber security program not only implements defensive measures, but also investigates successful attacks for response and remediation and unsuccessful attacks to improve their defensive posture. A key component of investigation, response, and remediation of attacks is forensic analysis. While forensic capabilities are widely available for typical information technology environments, they are limited for industrial control systems (ICS) found in power delivery systems. This capabilities gap impedes utilities responses, remediations, and investigations of cyber incidents.

**R&D Objective:** This research intends to improve the availability and capability of forensic tools, procedures, techniques and processes for ICS.

**Target Audience:** Chief Information Security Officers, Power Systems Operations Managers, Cyber Security Program Directors, Security Operations Managers, Cyber Security Architect, Cyber Security Engineers, Cyber Security Analysts, Physical Security Program Directors.

**2018 Research Results:**

- ICS Forensics Working Group
  - o Completed cyber security forensics tabletop exercises at three electric power utilities.
  - o Cyber Security Forensics for Industrial Control Systems: Summary of Utility Tabletop Exercises (**3002013991**)

**Next Steps:**

- Continue to lead a multi-sector ICS Forensics Working Group and develop new knowledge.
- Complete additional cyber security forensics tabletop exercises at electric power utilities.
- Develop prescriptive guidance for utilities to implement effective ICS cyber security forensics.

**Project Lead:** Ralph King, *reking@epri.com*

## Threat Management

**Issue:** Cyber security threats are dynamic and constantly attempting to overcome existing security defenses. Modern utility cyber security programs need to detect, protect, and remediate these threats at higher velocities. Automating work flows will be necessary to keep pace with the massive data volumes currently available for analyses and improve response times to stop threats.

**R&D Objective:** This research project will identify opportunities for automation in utility cyber security operations and demonstrate improved detection and response times.

**Target Audience:** Chief Information Security Officers, Power Systems Operations Managers, Cyber Security Program Directors, Security Operations Managers, Cyber Security Architect, Cyber Security Engineers, Cyber Security Analysts, Physical Security Program Directors operations center managers and operators, threat-hunting analysts.

**2018 Research Results:**

- Guidelines for Enhancing Threat Intelligence Programs for Power Delivery Systems (**3002013701**)
- Key Deliverables from Previous Years:
  - o Guidelines for Implementing a Threat Hunting Program for Power Delivery Systems (**3002010601**)

**Next Steps:**

- Develop utility-specific security automation use cases.
- Engage in pilot projects with utilities to demonstrate the effectiveness and potentials of security automation.

**Project Lead:** Ben Sooter, *bsooter@epri.com*

## Passive and Safe Active Identification of Substation Devices

**Issue:** Asset and configuration management is a critical area of interest for the electric sector with multiple challenges that must be addressed to ensure the secure and reliable delivery of power. In the substation environment, long technology refresh cycles and proprietary device interfaces have driven most utilities toward manual solutions that may be labor intensive.

**R&D Objective:** This project explores and categorizes substation devices based on available configuration and asset management interfaces. Building on past research involving device identification techniques, the project proposes a potential solution where network security solutions such as intrusion detection systems can be leveraged to assist with automating aspects of the asset and configuration management process.

**Target Audience:** Power delivery system owners and operators, cyber security analysts, compliance specialists, substation engineers.

**2018 Research Results:**

- Automating Asset and Configuration Management (**3002014136)** 2018/TBC 3/2019)
- Key Deliverables from Previous Years:
  - Passive and Safe Active Identification of Substation Devices (**3002010336**)

**Next Steps:** Future work will focus on the development of a proof of concept system that exchanges relevant configuration and asset data between network security solutions and configuration management systems. Additionally, the use of detailed asset configuration information for improved network security control will be explored.

**Project Lead:** John Stewart, *jstewart@epri.com*

## Cyber Security Compliance

**Issue:** Managing the large volume of vendor-supplied software patches is a challenging issue for utilities that are required to be compliant with NERC CIP standards. To maintain compliance, each utility must test and document all vendor patches prior to deployment. Current practices involve a series of steps to capture potential post-patch changes to the security posture of an application or device.

**R&D Objective:** This project introduces a patch testing approach that leverages patch regression analysis. By performing an exhaustive analysis of a large number of variables that can be observed or measured and comparing these variables before and after the patch is deployed, a more detailed understanding of the patch impact can be documented and its relevance to utilities can be assessed.

**Target Audience:** Power delivery system owners and operators, cyber security analysts, compliance specialists.

**2018 Research Results:**

- Patch Regression Testing Tool Analysis (**3002014137**)
- Key Deliverables from Previous Years:
  - Patch Management Guidelines (**3002010601**)

**Next Steps:** This project will identify technology-driven solutions to aid member's compliance to the CIP standards.

**Project Lead:** John Stewart, *jstewart@epri.com*

## Security Architecture

**Issue:** The rapid changes occurring in the grid demand flexibility and resiliency of power delivery systems, in addition to reliability. The modern technologies that support this capability increasingly depend on digitalization and interconnection, significantly expanding the grid's attack surface. In order to maintain security in such rapid expansion, cyber security professionals need to design and deploy key security controls quickly and analyze and mitigate emerging vulnerabilities in a timely manner.

**R&D Objective:** This project is a part of a multi-year effort that addresses a different area of utility OT systems each year. This year's research focuses on systems supporting distribution operations including DMS, ADMS, GIS, OMS, and DERMS and their supporting infrastructures. The outcomes will contain reference security architectures for the systems and infrastructure supporting distribution operations, primary attack modeling methodologies, and five generic attack models for distribution systems.

**Target Audience:** Power delivery system owners and operators, cyber security architects.

**2018 Research Results:**

- Security Architecture for Distribution Systems – Reference Architectures and Attack Modeling (2018; **3002013697**)
- Key Deliverables from Previous Years:
  - Substation Security Architecture Reference Diagrams Version 2.0 (2018; **3002012484**)
  - Substation Attack Surface Analysis (2017; **3002010417**)
  - Microgrid Attack Surface Analysis (2017; **3002010418**)
  - Cyber Security Architecture Methodology for the Electric Sector, Version 2 (2016; **3002007887**)

**Next Steps:**

- Extend the reference architecture to include new components for grid modernization and DER integration.

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

## Risk Management – Cyber Security Implications for an Integrated Grid

**Issue:** With the rise in customer-owned grid-connected DER, it is essential to understand the communication and control strategies and cyber vulnerabilities to effectively mitigate attack risks.
**R&D Objective:** This project identifies cyber security risk and key challenges associated with the deployment of distributed energy resources (DER), Electric vehicle infrastructure and microgrids.
**Target Audience:** Utility risk management, utility security management, security architects.

**2018 Research Results:**
- Cyber Security Implications for an Integrated Grid (**3002013699**)

**Next Steps:** EPRI will develop a publicly available Integrated Grid Risk Management software tool to highlight the various components of an integrated grid and match related security requirements and standards with stakeholders needs.
**Project Lead:** Tobias Whitney, *twhitney@epri.com*

## Cyber Security Metrics

**Issue:** There are several challenges with implementing effective, actionable cyber security metrics, specifically how utilities can accurately measure cyber security risks and the effectiveness of cyber security controls based on quantitative, repeatable data. The sector lacks accepted industry-wide metrics and benchmarks.
**R&D Objective:** The project focuses on developing, testing, and refining a set of metrics to quantify the effectiveness of cyber security controls. Once operationalized, the metrics can provide meaningful and actionable cyber security information to various stakeholders.
**Target Audience:** Utility risk management, utility security management, security architects, security operation center personnel, security engineering personnel.

**2018 Research Results:**
- Cyber Security Metrics for the Electric Sector, Volume 4 (2018; **3002013690**)
- Key Deliverables from Previous Years:
  - Creating Security Metrics for the Electric Sector (2015; **3002005947**)
  - Creating Security Metrics for the Electric Sector, Version 2 (2016; **3002007886**)
  - Cyber Security Metrics for the Electric Sector, Version 3 (2017; **3002010426**)

**Next Steps:**
- Operationalize security metrics – enable adoption of security metrics for security operations and risk management.
- Standardize security metrics – develop an industry standard based on these metrics for wider adoption across various critical infrastructure sectors.
- Enable industry comparisons – develop ways to securely aggregate the metrics from various organizations to produce industry statistics and enable benchmarking.

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



## ACRONYMS

| | |
|---|---|
| **ADMS** | Advanced Distribution Management System |
| **CIGRE** | International Council for Large Electric Systems |
| **CIP** | Critical Infrastructure Protection |
| **DERMS** | Distributed Energy Resource Management System |
| **DMS** | Distribution Management System |
| **GIS** | Geographical Information System |
| **IEEE** | Institute of Electrical and Electronics Engineers |
| **ICS** | Industrial Control Systems |
| **ISOC** | Integrated Security Operations Center |
| **NEC** | The National Electrical Code |
| **OMS** | Outage Management System |

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 longrange research and development planning, and supports research in emerging technologies.EPRI members represent 90% of the electricutility revenue in the United States with international participation in 35 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

**TO JOIN, CONTACT ANY OF THE FOLLOWING TECHNICAL ADVISORS:**

***West:*** *Christine Hertzog, Senior Technical Advisor, 650.314.8111; chertzog@epri.com*
***East:*** *Chris Kotting, Technical Advisor, 980.219.0146; ckotting@epri.com*
*Annette Mosley, Technical Advisor, PDU, 972.556.6507; amosley@epri.com*
***International:*** *Kevin East, International Director, +44 (1925) 450.207; keast@epri.com*

For more information, contact the EPRI Customer Service Center at 800.313.3374 or askepri@epri.com

*3002015126*

**January 2019**

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

SUCCESS STORY

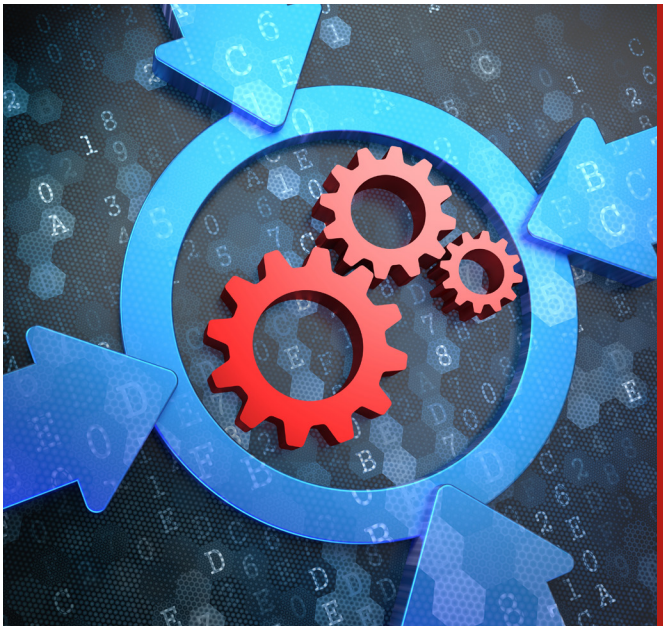
# Cyber Security Architectures and Attack Modeling Methodologies Help Analyze and Mitigate Emerging Risks for Utility Distribution Grids

The rapid changes occurring in the grid demand flexibility and resiliency of power delivery systems, in addition to reliability. The modern technologies that support this capability increasingly depend on digitalization and interconnection, significantly expanding the grid's attack surface. In order to maintain security in such rapid expansion, cyber security professionals need to design and deploy key security controls quickly and analyze and mitigate emerging vulnerabilities in a timely manner.

EPRI's extensive research on security architecture addresses a different area of utility Operations Technology (OT) systems each year. The 2018 research focused on systems supporting distribution operations – DMS, ADMS, GIS, OMS, DERMS, etc., and their underlying infrastructures. The research included a detailed study on five closely related topics: distribution system components, network topology and zoning, cyber security controls for distribution systems, attack modeling methodology for distribution systems, and attack models for a generic distribution system.

Using this analysis, reference architectures were developed based on North America's distribution utility companies' IT/OT systems and network topologies. The in-depth examination of the current systems and existing security controls allowed the research team to carry out a cyber-attack modeling exercise where potential vulnerabilities and corresponding attack techniques were identified.

Recommended cyber security controls for distribution systems were developed based on the NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 and the Centre for Internet Security (CIS) Controls Version 7. The attack modeling provided five generic models based on NESCOR failure scenarios related to the distribution grid. These can be used to understand possible attack paths; identify security gaps; configure security tools; train incident response personnel or perform incident response exercise.



**"PG&E is facing many changes to the distribution grid. Grid modernization, renewable generation, and integration of distributed energy resources - all pose significant challenges to cyber security, by increasing attack surfaces and introducing unknown vulnerabilities to the systems supporting the distribution grid operations. EPRI's focus on distribution systems in 2018 garnered the timely attention to cyber security within PG&E and provided various options and methodologies for understanding and modeling cyber-attacks to these systems."**

*According to Xavier Francia, Cybersecurity Risk Advisor, Pacific Gas and Electric Company*

**Leadership/Innovation Demonstrated:**
This research significantly advances industry comprehension about tactics and techniques that can be used against the distribution grid by the adversaries. There have been previous studies on distribution systems, system architectures, and attack modeling methodologies. However, in most cases the studies were done in isolation within their own domains and therefore it took a significant amount of time for cyber security professionals to identify, analyze, and correlate the information. By listing the key system components, key security controls and examples of attack models, the study provides an effective tool to protect the nation's grid and to prepare for the significant changes coming in the near future.

**Value Realized:**
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.

**Key findings:**
- Distribution systems should be separated into several network zones or security enclaves based on the risk their compromise poses to the utility, the users who need to access them, and other networked systems
- People, processes, and technologies controlling cyber security risks must be developed and implemented to protect distribution grid operations from internal and external cyber threats
- Various attack modeling methodologies can be utilized for finding and mitigating security vulnerabilities in distribution system architecture

Project Set Lead: Candace Suh-Lee, 650.855.8513, csuh-lee@epri.com

**TO JOIN, CONTACT ANY OF THE FOLLOWING TECHNICAL ADVISORS:**

***West:*** *Christine Hertzog, Senior Technical Advisor, 650.314.8111; chertzog@epri.com*

***East:*** *Chris Kotting, Technical Advisor, 980.219.0146; ckotting@epri.com*
*Annette Mosley, Technical Advisor, 972.556.6507 amosley@epri.com*

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

For more information, contact the EPRI Customer Service Center at 800.313.3374 or askepri@epri.com

*3002015250* **January 2019**

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

SUCCESS STORY

# Industrial Control System Forensic Tabletop Exercises Aid in Developing Incident Response Playbooks


The potential for malicious cyber incidents to occur in operational technology (OT) systems increases with the burgeoning usage of processor-based operational and communications infrastructure. It is critical for utilities to continually evaluate and exercise their capabilities to effectively respond to events in their operational environments to determine if their processes satisfy requirements. The incident response process for a cyber-attack includes detection, analysis, mitigation, recovery, and post-incident activities. A critical component of the incident response process is forensic investigation. The EPRI Cyber Security Team worked with three electric power utilities in 2018 to evaluate their forensic investigation process by conducting tabletop exercises that test their response to cyber events in their unique operational technology environments.

A tabletop exercise is a facilitated, scenario-based discussion that tests an organization's ability to respond to a potential scenario in a practice environment. It enables participants to review and discuss in detail the actions they would take to validate operational processes, procedures, and reporting structures. The key outputs of the exercise are an identification of people, process, or technology gaps and recommendations to resolve them.

A planning meeting was held with each utility prior to the 1-day exercise workshop to identify the appropriate utility staff that would attend and to determine logistics of the meeting. Utility resources responsible for the processes to be evaluated attended the workshop along with EPRI's Cyber Security team members and staff from MITRE. The exercise evaluated the roles and responsibilities, processes and procedures, and technologies supporting cyber event response and forensics investigations for those events in an OT environment.

The objectives of the exercises were:

- Identify how to address a non-obvious cyber event normally attributed to a maintenance problem.
- Refine the OT processes and procedures following a cyber event, including actions taken by operators in the field.
- Document roles, responsibilities, and authorities, to answer:
  - Who is the primary authority?
  - Who performs cyber-related analysis of the operational environment?
  - Who are the stakeholders?
  - How is information shared?

**"Overall the engagement was very informative and has assisted us as we are on our journey of improving capabilities of incident response. At the time of the exercise we were actively engaged in developing playbooks, communication channels, and escalations paths for our Integrated Security Operations Center. The exercise allowed us to pause and adjust some of the playbooks that were developed to be more in line with the practices that were discussed as part of the exercise."**

*Lance Howard, Senior Manager of Security Assurance and Information Risk Management at Portland Gas and Electric*

Each scenario focused on addressing different aspects of incident response and the forensics process in the OT environment. The participating utility then received a report documenting how cyber security and operational resources currently respond to cyber events. The report also included the scenarios, findings, and recommendations.

The tabletop exercises for incident response and forensics were a valuable process for the participating utilities. The exercises also provided value to utilities through an anonymized report that provides a baseline summary of the process, scenarios, findings, and recommendations resulting from all workshops.

Key points from the workshops include the following:

- The coupling of IT and OT infrastructure components requires coordination, collaboration, and knowledge-sharing between the IT and OT organizations.
- It is critical to have clear processes and procedures in place to avoid conflicts between the forensics functions and operations restoration.
- The incident response and forensics processes should be routinely tested.
- Organizations should develop internal forensics talent and reduce reliance on vendors to perform these evaluations.

It is important to build upon this baseline analysis of the incident response and forensics capabilities of utilities, particularly for the industrial control system components of the OT infrastructure. Forensic capabilities for industrial control systems are not mature and represent knowledge gaps within utilities and technology vendors. Therefore, EPRI will continue research to further the incident response and forensic investigative processes for industrial control systems in our 2019 roadmap.

Program Manager: Ralph King, *reking@epri.com*

**TO JOIN, CONTACT ANY OF THE FOLLOWING TECHNICAL ADVISORS:**

***West:*** Christine Hertzog, Senior Technical Advisor, 650.314.8111, chertzog@epri.com

***East:*** Chris Kotting, Technical Advisor, 980.219.0146; ckotting@epri.com
Annette Mosley, Technical Advisor PDU, 972.556.6507 amosley@epri.com

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

For more information, contact the EPRI Customer Service Center at 800.313.3374 or askepri@epri.com

3002015311 **January 2019**

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

# Cyber Security Deliverables

## 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** (2018/TBC 3/2019)

*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: 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

*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

*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

*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)

# Cyber Security Deliverables

*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

*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)

## 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

*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)

**TO JOIN, CONTACT ANY OF THE FOLLOWING TECHNICAL ADVISORS:**

***West:*** *Christine Hertzog, Senior Technical Advisor, 650.314.8111; chertzog@epri.com*
***East:*** *Chris Kotting, Technical Advisor, 980.219.0146; ckotting@epri.com*
*Annette Mosley, PDU Technical Advisor, 972.556.6507; AMosley@epri.com*
***International:*** *Kevin East, International Director, +44 (1925) 450.207; keast@epri.com*

For more information, contact the EPRI Customer Assistance Center at 800.313.3374 or askepri@epri.com

*3002015251* **January 2019**

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

## BIOGRAPHIES

# Cyber Security (183) Team Members

**Matt Wakefield** is Director of Information and Communication Technology (ICT) and Cyber Security (183) at the Electric Power Research Institute (EPRI). With over 25 years of energy industry experience, his research area responsibilities include furthering the development of a modernized grid with a strong focus on leveraging emerging information and communication technologies that can be applied to the electric grid infrastructure. He received his BS in Technology Management from the University of Maryland University College.
*mwakefield@epri.com*

**Galen Rasche** is a Senior Program Manager in the Power Delivery and Utilization (PDU) Sector at the Electric Power Research Institute (EPRI), managing the P183 Cyber Security Program. He is experienced in the areas of cyber security, Smart Grid security and the penetration testing of embedded systems. Prior to joining EPRI, Galen led the Embedded and Application Security Group at Southwest Research Institute (SwRI). He received a Master of Science in electrical engineering degree from the University of Illinois at Urbana-Champaign and a Master of Business Administration and Bachelor of Science in electrical engineering from the University of Kentucky.
*grasche@epri.com*

**Ralph King** is a Program Manager in P183. With over 30 years in the electric power industry he manages cyber security projects focused on technology advancements in situational awareness, threat management, and incident response and provided guidance to electric power utilities in the development of the Integrated Security Operations Center (ISOC). He holds a BS in mathematics and computer science, a MS in computer science, an MBA, and has completed the Exe. Dev. Prg. at the Wharton School of Business. He also holds industry certifications in Lean Sigma and is a Project Management Professional.

*reking@epri.com*

**Candace Suh-Lee** is a Principal Technical Leader in the Cyber Security Program. Candace leads cybersecurity metrics R&D and the taskforce for cybersecurity of DER and grid-edge systems. Her research focuses on collaboration across different R&D programs to design cybersecurity into the emerging technologies. Prior to EPRI, Candace worked for various electric and gas utilities, specializing in industrial control system security, compliance, and risk management. Candace holds a M.Sc. Computer Science from the University of Nevada, Las Vegas and Hon. B.Sc., Computer Science from the University of Toronto, Canada
*csuh-lee@epri.com*

**Ivan Dragnev** is a Principle Technical Leader in the Cyber Security Program. He has nine years of information and technology experience and four years of Cyber Security experience in the energy sector. His current focus includes security metrics, secure architecture, and the Integrated Security Operations Center (ISOC). Prior to EPRI, Ivan worked at an electric utility with the main focus on Cyber Program implementation and development. Ivan holds a BS in Hydraulics and Pneumatics and a BS in Business Administration.
*idragnev@epri.com*

**Tobias Whitney** is a Technical Executive in P183. He has over 20 years of experience in cyber security and regulatory policy for the electric sector and begam his career at PricewaterhouseCoopers. He also worked as the Security Practice Leader at Burns and McDonnell Engineering and worked at GE Energy's Smart Grid Center of Excellence. Most recently he led the Critical Infrastructure Protection (CIP) program at North American Electric Reliability Corporation (NERC). He holds an undergraduate degree from the Uni. of Missouri and a MBA from the Wash. University Olin Business School.
*twhitney@epri.com*

**John Stewart** is a Senior Technical Leader in the Power Delivery and Utilization (PDU) sector at EPRI. Some of his current work includes passive device identification, tunneling legacy protection communications over packet networks, and supporting the development of an architecture for improving substation security. Prior to joining EPRI, John spent over fifteen years working with grid communications and control systems and advised multiple DOE projects focused on securing critical power delivery systems.
*jstewart@epri.com*

**William Webb** is a Technical Leader in the Cyber Security Program in the PDU sector. His current research activities focus on incident response and threat management. Prior to joining the Cyber Security Program, he spent 10 years working with EPRI's Critical Power Program. William received a MS degree in electrical and computer engineering from the Georgia Institute of Technology in Atlanta, Georgia, and a BS degrees in electrical engineering and computer engineering from North Carolina State University in Raleigh, North Carolina.
*wwebb@epri.com*

**Gerardo Trevino** is a Technical Leader in the Cyber Security Program. His current research focus is on Microgrid systems, Electric Vehicle Supply Equipment (EVSE), Global Positioning System (GPS) dependent power applications, and Distributed Energy Resources (DER) technologies. His past work included using embedded systems expertise to develop and improve Smart Grid technologies, assess system security for commercial and government clients, and architect test equipment for different space missions.He received a Master's and a BS in Electrical Engineering from the University of Texas at San Antonio.
*gtrevino@epri.com*

**Ben Sooter** is a Sr. Project Manager in P183. In addition to managing the Cyber Security Research Lab (CSRL) in Knoxville, TN, he is responsible for cyber security projects in the areas of threat management and incident response. Prior to joining the Cyber Security team, Ben managed EPRI's Knoxville lab and lab network for over nine years. Prior to EPRI, Ben worked at Oak Ridge National Laboratory in their Power Systems group. He holds a MS in Electrical Engineering from the University of Tennessee and a BS in Electrical Engineering from the University of Texas at Austin.
*bsooter@epri.com*

# Cyber Security (183) Team Members

**Greg Drewry** is an Engineer/Scientist II in the Cyber Security Program in the PDU sector. His current research focus is on security monitoring. Greg's past responsibilities included product development and implementation of Voice Over Internet Protocol (VOIP) services, maintaining the Class 5 phone switch, tertiary generators for critical sites, fraud prevention, and fiber management and supporting cable, phone, and internet services. Greg received his BS in Electrical Engineering from the University of Tennessee in Knoxville, Tennessee.
*gdrewry@epri.com*

**Alekhya Vaddiraj** is an Engineer/Scientist II in the Cyber Security Program in the PDU sector of EPRI. Her work focuses on Security Architecture of Microgrids and Demand Response in Electrical Vehicles and California Independent System Operator (CAISO) Energy Markets. She has experience in design-simulation of power systems with Real-Time Simulators and DOE C2M2 model. Alekhya graduated with a Masters in Electrical and Computer Engineering from University of North Carolina Charlotte.
*avaddiraj@epri.com*

**Chris Stapler** is an Engineer/Scientist II in Program 183. His current work is focused on research and development associated with cyber security and information communications technologies for the electric sector. His main areas are maturing the Information Security Operations Center (ISOC) and developing a holistic threat model interface via the Integrated Threat Analysis Framework (ITAF) initiative. Chris has previous experience in RADAR systems engineering, Autonomous Underwater Vehicle R&D, and Chemical, Biological, Radiological and Nuclear Defense (CBRNE) threat detection.
*cstapler@epri.com*

**Larry Burnette** is an Engineer/Scientist II in P183. He has over 35 years of experience in information technology and cyber security. Larry is responsible for the operations of the Cyber Security Research Lab (CSRL). His focus is on threat frameworks, intrusion detection, and lab testing. Prior to joining the Cyber Security team, Larry was a senior engineer in the EPRI Knoxville Lab and a group leader in EPRI's corporate information technology team. Larry worked at CTI Molecular Imagining and was responsible for help desk operation and cyber security. He has an Electronics Specialist Degree and multiple certifications in the computer industry.
*lburnette@epri.com*

**Alekhya Avadhanula** is an Engineer/Scientist I in the Cyber Security Program in the PDU Sector. Her work focuses on research and software development for Cyber Security Metrics for the Electric Sector, and Security Data Analytics and Cloud Security for Utility Oriented Applications. Alekhya's past responsibilities included research, vendor analysis, and demo architecture design for Security Data Analytics. Alekhya received her Master of Science degree in Software Engineering from San Jose State University in San Jose, CA.
*aavadhanula@epri.com*

**Luke Varner** is an Engineer/ Scientist I for the Cyber Security Program in the PDU sector. His current research focus is on network security and threat detection. In the past, he has worked on research and development of security software and frameworks for IT/ OT environments and was a key developer in engineering the WAMPAC C37.118 man-in-the-middle attack. Luke has worked at EPRI since 2016 as a student employee.
*lvarner@epri.com*

**Sai Ram Ganti** is an Engineer/Scientist II in the Cyber Security Program in the PDU sector at EPRI. His work focuses on security in Electric Vehicle Supply Equipment (EVSE) and Distributed Energy Resources (DER). He has a experience with hardware simulations and embedded systems. Sai Ram graduated with a Masters in Computer Science from the University of Nevada Las Vegas, Nevada
*sganti@epri.com*

**Erica Loveday** is the Technical Assistant III for the Cyber Security Program in the PDU sector of EPRI. She coordinates P183 program logistics for the bi-annual advisory meeting, annual program workshops, and lab visits to the Knoxville Cyber Security Research Lab. Prior to joining EPRI, she worked as an Operations Analyst and in IT Operations. Erica has an educational background in both Information Technology and design.
*egloveday@epri.com*

**Christine Hertzog** is a Senior Technical Advisor for ICT and Cyber Security at EPRI. She was previously the founder of a consulting firm focused on Smart Grid ecosystems and has an extensive telecommunications background. She authored the *Smart Grid Dictionary*, and co-authored *Data Privacy for the Smart Grid*. She has also served in an advisory capacity to innovators, industry associations, and publications. She has a MS in Telecommunications from the University of Colorado–Boulder.
*chertzog@epri.com*

**Chris Kotting** is a Technical Advisor II for ICT and Cyber Security at the Electric Power Research Institute. He was previously engaged as a consultant and author on the development of communication standards for the electric industry, working with SGIP, NAESB, and other industry alliances. Earlier in his career he was on staff at the Public Utilities Commission of Ohio, working in numerous policy and regulatory roles, in both the energy and telecommunications industries, including work in critical infrastructure protection. He has an BA in Communications from the Ohio State University.
*ckotting@epri.com*

**Annette Mosley**
is a Technical Advisor in the Power Delivery and Utilization Sector and supports the Information, Communication and Cyber Security (ICCS) programs.
*AMosley@epri.com*

**Laura McLemore**
is the Project Operations Coordinator for the Information, Comm-unications Technology and Cyber Security Programs within the PDU sector. She has 20+ years of experience in executive administrative support and meeting planning in a variety industries including engineering, consulting, medical, television, and radio.

*lmclemore@epri.com*

**Ilka Wiland**
is the Leader, Product Development and Administration for programs 161 and 183 in PDU. Her responsibilities include technical assistance in the administration of the Annual Research Portfolio, includng Operations and Marketing task management. Her experience includes large trade show execution in the high-tech business and the planning, preparation, and organization of technical conferences. Ilka has an educational background in project management, graphic production, and hotel business administration.
*iwiland@epri.com*

**Linda Dabbs**
Is the Senior Administrative Assistant for the Information, Communications and Cyber Security Programs within the PDU sector. Linda has 25+ years of experience providing executive administrative support. Linda is responsible for member communications, webcast support, tracking advisor engagement, managing program cockpits and event planning.
*ldabbs@epri.com*

EPRI | ELECTRIC POWER RESEARCH INSTITUTE

BIOGRAPHIES

# Cyber Security (183) Team Members

**TO JOIN, CONTACT ANY OF THE FOLLOWING TECHNICAL ADVISORS:**

***West:*** *Christine Hertzog, Senior Technical Advisor, 650.314.8111; chertzog@epri.com*
***East:*** *Chris Kotting, Technical Advisor II, 980.219.0146; ckotting@epri.com*
*Annette Mosley, Technical Advisor PDU, 972.556.6507; AMosley@epri.com*
***International:*** *Kevin East, International Director, +44 (1925) 450.207; keast@epri.com*

Staff listing by job titles

For more information, contact the EPRI Customer Assistance Center at 800.313.3374 or askepri@epri.com

**3002015440** **January 2019**

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