

Technology Innovation Project



Project Brief

TIP 420: EPRI P183 - Cyber Security for Power Delivery and Utilization

Context

The landscape of cyber security activities in the electricity sector involves numerous industry, 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.

With increased attention focused on securing the electric sector, numerous industry groups and public-private partnerships have been created to develop new security requirements and technologies. Additionally, working groups of organizations such as the North American Electric Reliability Corporation (NERC), International Council on Large Electric Systems (CIGRE), Institute of Electrical and Electronics Engineers (IEEE), and the International Electrotechnical Commission (IEC) will continue to have a direct impact on utility operations.

These groups are addressing specific needs in the industry; however, utility personnel are often unavailable to support all of these efforts. This lack of availability can lead to two key issues. First, utilities are less aware of changes that might impact the industry. Second, manufacturers of security products may lack the perspective of the electric sector.

2020 Key Activities

In 2020, this program expects to accomplish the following objectives:

- **Collaboration** - Track industry and government activities and provide technical contributions to key working groups;
- **Incident Management** - Improve the electric sector's ability to efficiently detect cyber incidents through the application of AI and machine learning techniques. The program will also continue technical development of the Integrated Security Operations Center (ISOC);
- **Cyber Security Forensics** - Create additional ICS forensics field guides for OT devices and begin the initial phase of tool development to facilitate automated collection of forensics data;
- **Threat Management** - Develop guidelines for security orchestration automation and response (SOAR) for power delivery systems;

- **Asset and Configuration Management** - Develop guidelines for effective field device management;
- **Policy-Driven Cyber Security** - Pilot EPRI's compliance automation reference model. The program will also create a Cloud Security Reference Architecture for real-time utility-based applications that incorporates high and medium impact CIP applicable environments;
- **DER Security** - Develop guidelines for key aspects of DER system security, including smart inverter hardware security, public key infrastructure for secure DER communication, and cyber security for microgrid integration; and
- **Security Metrics** - Create a Cyber Security Metrics operationalization guideline and release EPRI's MetCalc and Metrics Hub solutions.

This program provides monthly email updates to the members to summarize EPRI's industry activities and the status of its research projects.

Why It Matters

The reports developed by this program will provide BPA a reference point to track the detailed efforts of several industry groups. This program also increases the relevance and utility of the security reports, controls, and technologies that are being developed by these groups.

Goals and Objectives

BPA will use its membership in this program to gain a better awareness of industry and government collaborative efforts, where members can "plug in" to current activities; evaluate techniques for assessing and monitoring risk; evaluate tools and metrics to better assess security posture and return on investment; identify practical approaches to mitigating the risk of operating legacy systems; study early identification of security gaps through laboratory assessments of security technologies; and obtain technologies which support the management of cyber incidents and increase the cyber security and resiliency of the grid.

Deliverables

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;
- Tools to support improved automation of incident and threat management processes;
- Security forensics field guides for industrial control systems;
- Integrated solution for device identification, configuration monitoring, and password management;
- Cloud security reference architectures for real-time applications;
- NERC CIP automation reference model;
- Security tools and guidelines for Distributed Energy Resources (DER) smart invertors, secure communications, and microgrid integration; and
- Guidance and tools for operationalizing EPRI's security metrics and Metrics Hub.

TIP 420: EPRI P183 - Cyber Security for Power Delivery and Utilization

Project Start Date: January 2020

Project End Date: December 2020

Links

[EPRI Program 183: Cyber Security for Power Delivery and Utilization](#)

Leverage

BPA's contributions are leveraged at a ratio of 37:1. This annual membership provides BPA access to reports and results of EPRI Cyber Security projects.

For More Information Contact:

Technology Innovation Program Manager:

Cynthia Polsky
chpolsky@bpa.gov

Sean Barry, Lead IT Cybersecurity Specialist
spbarr@bpa.gov

EPRI P183 Program Manager

Galen Rasche
grasche@epri.com

EPRI P183 Research Portfolio - 2020

P183.001: Industry Collaboration - 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 cybersecurity topics.

P183.005: Incident Response - Incident response includes detecting cyber security events, establishing criteria for event prioritization, and correlating multiple cybersecurity events. Utilities need to establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event.

P183.008 Asset & Configuration Management - Asset and configuration management is a critical area of interest for the electric sector, with many significant challenges that must be addressed to ensure the secure and reliable delivery of power. This research project focuses on a unique set of conditions presented by cyber systems in an industrial control systems (ICS) environment.

P183.017: Cyber Security Forensics - Incident management and response includes detecting cybersecurity events, establishing criteria for event prioritization, and correlating multiple cybersecurity



Technology Innovation Project



Project Brief

events. Utilities need to establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event.

P183.013: Policy-driven Cyber Security Research - The power industry developed the Critical Infrastructure Protections (CIP) standards, which address many topics of cyber security for electric power companies. While the standards have improved the security posture of most organizations, they have impeded certain adoptions of technology or practices for others due to ambiguity or compliance risk avoidance.

P183.014 Cyber Security Metric - Key research questions for this project can be summarized in the following three areas:

- How can the electric power industry scientifically measure cyber security risks and the effectiveness of cyber security controls based on quantitative, repeatable data?
- What metrics should be calculated and what data is required to calculate the metrics?
- Is there a way to standardize the metrics for industry-level data aggregation and benchmarking?