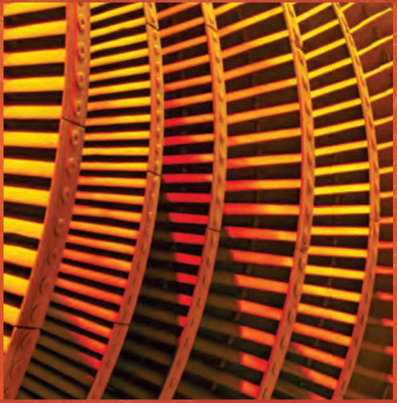
December 2018



Cyber Security Roadmap

ELECTRIC POWER
RESEARCH INSTITUTE

Introduction

Cyber Security Area Research Objective

Conduct research, development, and demonstrations that provide the technical basis and tools to support the management of cyber security risk across the entire utility enterprise. This roadmap describes EPRI's cyber security research in its Power Delivery, Generation, and Nuclear Sectors in support of EPRI's mission to provide a safe, reliable, affordable and environmentally responsible source of electric power for society.

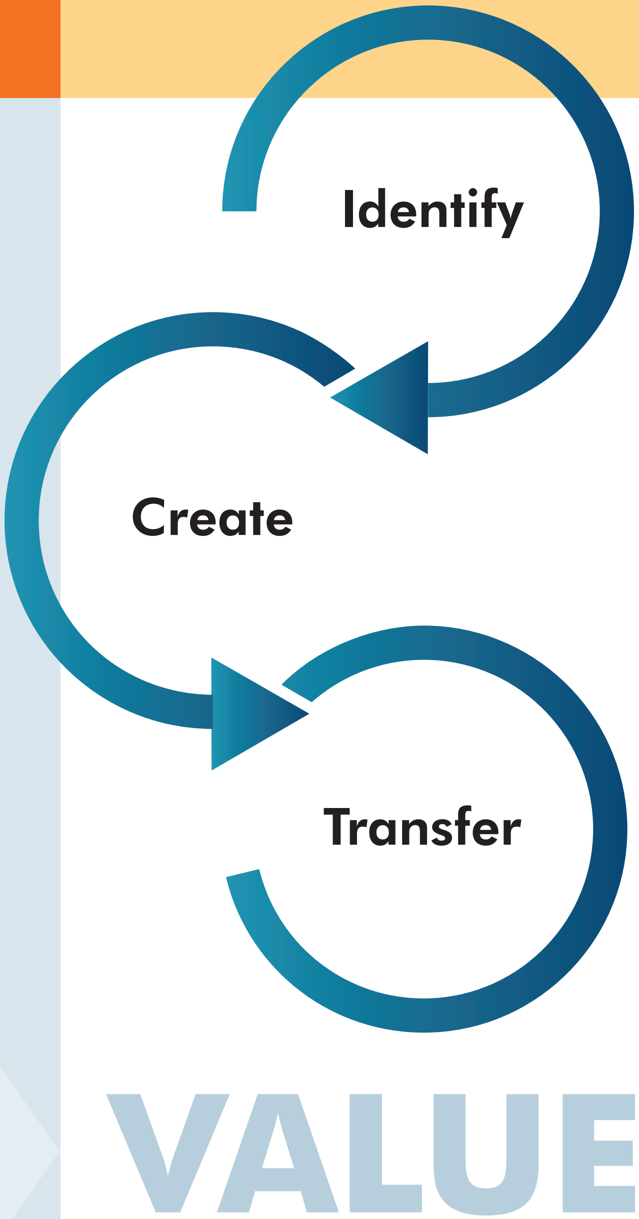
Approach

- We use a collaborative model to Leverage investment, Identify issues, Guide research, and Implement results.
- We execute research using a Portfolio-based approach to provide Short-, Mid- and Long-Term Deliverables to address identified industry issues.
- We utilize a member-driven Roadmap which includes Mission, Drivers, Future States, Gaps, and multi-year Research Plans that document how EPRI is bridging these gaps.
- We utilize continual engagement with members to ensure that the R&D we perform is High Value, Easy to Implement and Likely to Succeed.

Power Delivery and Utilization

Generation Sector

Nuclear Sector



Identify

Create

Transfer

VALUE

How We Do It

- We leverage the shared experience of our utility members, industry engagement, and the expertise of EPRI's Cyber Security Team to ***Identify*** existing research gaps and associated project needs.
- We develop a portfolio of research projects that ***Create*** independent, fact-based results and effective tools to provide members decision support in managing their cyber security risk.
- We ***Transfer*** the research value to members through advisor interactions, topical workshops, user groups, training modules, and direct member support. Research results may be distilled into any of the following forms:

Reports

Reference Guides

Field Guides

Interest/User Groups

Lab/Field Demos

Software Tools

Videos

Training Modules

PROGRAMS DEFINE ACTION PLANS

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identify Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Process	DE.DP
Respond & Recover	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

NIST Cybersecurity Framework Functions and Categories

The U.S. National Institute of Standards and Technology (NIST) released Version 1.1 of the *Framework for Improving Critical Infrastructure Cybersecurity* in April 2018. The NIST Cybersecurity Framework (CSF) Reference Tool provides a "common organizing structure for multiple approaches to cyber security by assembling standards, guidelines, and practices". Since its initial release, the CSF has been adopted by many utilities around the world. The future states of EPRI's Cyber Security Roadmap have been categorized according to the Framework Core's five Functions of Identify, Protect, Detect, Respond, and Recover, providing a clear mapping to utility cyber security activities. The chart above provides the Functions and Categories from the CSF as a reference.

Action Plans and Project Definitions:

What we need to do to bridge the gaps to achieve the Future States

Annual Research Portfolio: EPRI's offering of collaborative, membership funded research work for a given year. All annual research portfolio purchases are based on EPRI's research year (the calendar year). These offerings are made available each June for the subsequent research year.

Supplemental Project: Some research projects are not part of the annual research portfolio, they are executed as supplemental projects. These supplemental projects are done more as one-off projects; they can be single or multiple funder projects.

Technology Innovation Project: Technology Innovation allows members to leverage their long-term investment (10+ years) in collaborative research that may create entirely new markets, products and services, increase the public benefits of efficient, clean affordable energy, and ensure the competitiveness of the energy enterprise.

Pre-Demonstration Project: EPRI program to fund R&D that would enable a large scale demonstration project. For example, a pre-demonstration project that laid the foundation for the multi-year, collaborative was the Field Area Network (FAN) Demonstration project.

Government Project: A project that EPRI has been awarded through a government entity such as the U.S. Department of Energy, California Energy Commission or the New York State Energy Research and Development Authority. Awards are typically made by these organizations through an open, competitive solicitation process.

Workshops and Forums: EPRI meetings, direct interaction with one or more potential customers can take place via face-to-face meetings, workshops, conference calls, or webcasts and are defined as technical deliverables. Forums or interest groups are formed by advisors and stakeholders that also meet on a regular basis throughout the year.

Cyber Security (CS) Roadmap

Future States

Automating Asset and Configuration Management (ACM) Technology For Power Systems

Cyber Security Metrics for The Electric Sector

Compliance Standards Driven Solutions

Cyber Security Process and Integration For Generation Facilities

Technical Assessment Methodology

Hazard Consequence Analysis for Digital Systems (HAZCADS)

Cyber Security Program Guide

Cyber Security in the Supply Chain

Security Architecture for Flexible and Resilient Utility Systems

Protective Measures for Distributed Energy Resources

Protective Measures for Generation Industrial Control Systems

Incident Detection

Threat Management

Cyber Security Forensics for Industrial Control Systems

Respond & Recover Capabilities for Generation Facilities

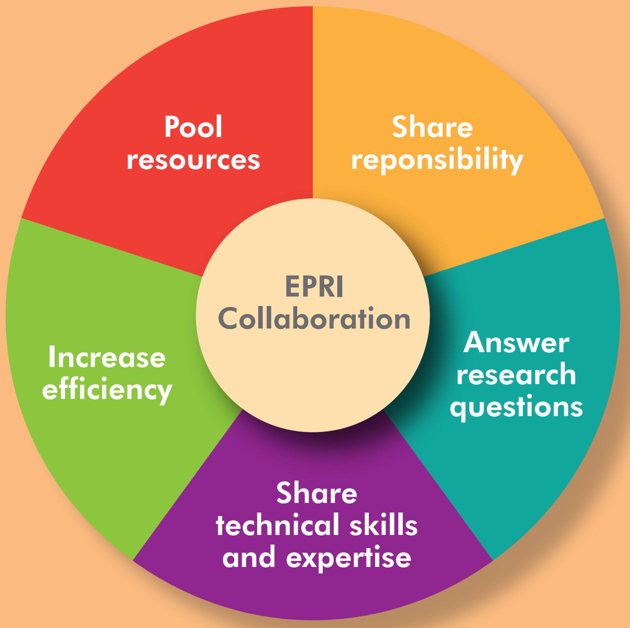
Cyber Security Overview

Overview

Cyber security has become a critical priority for electric utilities across the power delivery, fossil generation, and nuclear power sectors. The evolving electric grid is increasingly dependent on information technology and telecommunications infrastructures to ensure its reliable operation. As generation plants are being required to adapt to the complex demands of an ever increasingly competitive marketplace, each power generation site is deploying more digital Instrumentation and Control assets from a variety of vendors. Additionally, the US Nuclear Industry has spent large sums on regulatory mandated cyber security implementation to date, though it is not certain if these costs have had a commiserate increase in security.

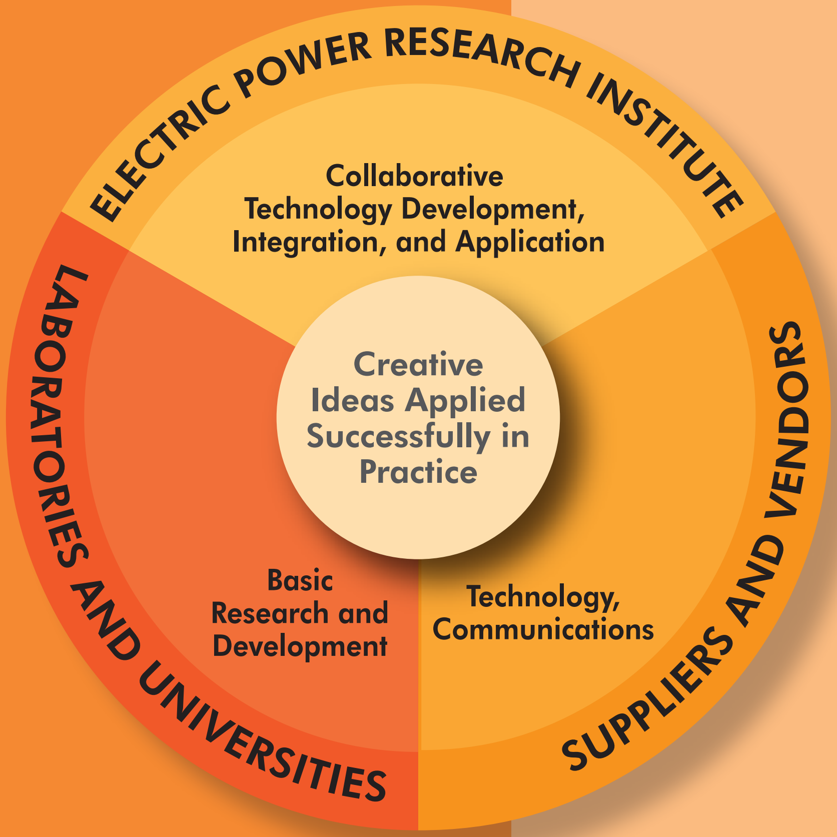
Cyber security measures must be designed and implemented to support grid reliability. These measures must also support grid resilience against attacks by terrorists and hackers, natural disasters, and inadvertent threats such as equipment failures and user errors.

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



One of the goals outlined in the U.S. Department of Energy's Multiyear Plan for Energy Sector Cyber Security focuses on "accelerating game-changing research, development, and demonstration of resilient Energy Delivery Systems". EPRI's Cyber Security Portfolio supports this goal through targeted cyber security research in generation, delivery, and use of electricity that leverages EPRI's in-depth understanding of power systems and utility operating environments.

Cyber Security Research Value


ELECTRIC POWER RESEARCH INSTITUTE
LABORATORIES AND UNIVERSITIES
SUPPLIERS AND VENDORS
Collaborative Technology Development, Integration, and Application
Creative Ideas Applied Successfully in Practice
Basic Research and Development
Technology, Communications

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. To enhance cyber security R&D, EPRI will identify where relevant work is happening—whether it be the national laboratories, manufacturers, or universities. Drawing on our deep expertise in cyber security and diverse aspects of the power system, we will transfer key insights and results of this work to the electric power industry, helping companies to apply them in their operational systems.

EPRI's Cyber Security portfolio can provide:

- A better awareness of industry and government collaborative efforts, where members can "plug in" to current activities;
- Guidance on developing cyber security strategies and requirements for selecting effective technologies;
- Guidance on security metrics;
- Techniques for assessing and monitoring risk;
- Practical approaches to mitigating the risk of operating legacy systems;
- Early identification of security gaps through laboratory assessments of security technologies;
- Technologies which support the management of cyber incidents and increase the cyber security and resiliency of the grid;
- Methodology for integrating cyber security assessment and control methods into the existing facility digital engineering (design, system, and analysis) and operational program to achieve design and implementation efficiency; and
- Technologies which support cyber programmatic management and increase the cyber security posture.

Identify

The NIST Cybersecurity Framework defines the Identify Function as "Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities." Specifically, the activities in this function involve "Understanding the business context, the resources that support critical functions, and the related cyber security risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs."

Categories within this Function include:
- Asset Management;
- Business Environment;
- Governance;
- Risk Assessment;
- Risk Management Strategy; and
- Supply Chain Risk Management

The following Future States support the business processes and technologies required to effectively and efficiently execute activities within the Identify Function's categories:
- Automating Asset and Configuration Management (ACM) Technology for Power Systems
- Cyber Security Metrics for the Electric Sector
- Compliance Standards Driven Solutions
- Cyber Security Process and Integration for Generation Facilities
- Cyber Security Assessment Methods
- Risk Informed Cyber Security Methods
- Cyber Security Program Guide
- Supply Chain Security and Digital Engineering Process Integration

Automating Asset and Configuration Management (ACM) Technology for Power Systems

Future States: Utilities will be able to identify and track field assets and efficiently manage their configurations by integrating automated solutions.

Description: Asset and configuration management is a critical area of interest for the electric sector with multiple significant challenges that must be addressed to ensure the secure and reliable delivery of power. While modern asset management and configuration controls are routinely implemented in a typical business IT environment, this research project focuses on a unique set of conditions presented by cyber systems in an industrial control systems (ICS) environment. For example, relatively long technology refresh cycles lead to situations where legacy hardware and software may remain in place long after vendor support has been discontinued. This scenario leaves utilities with a number of challenges to overcome when trying to manage and secure systems that were not built with security in mind.

Action Plan: Automating Asset and Configuration Management

- Assess commercial solutions for device identification, configuration monitoring, and password management
- Identify key points of interoperability required to integrate solutions and enable the automated discovery and management of field devices
- Pilot an integrated system that enables exchange of information from device discovery through configuration and password management

Major Past Accomplishments	2019	2020	Future
POWER DELIVERY CYBER SECURITY ANNUAL RESEARCH PORTFOLIO (P183)			
Assessed purely passive identification techniques for ICS equipment and explored safe active interrogation	Extend safe active interrogation techniques and explore integration with Intelligent Electronic Devices (IED) management solutions	Demonstrate integrated solution for device identification, configuration monitoring and password management	Expand integrated solution to cover a larger set of devices and explore the use of device information to better coordinate cyber security controls

Gaps Addressed:

- The inconsistency of remote access and access control tools in their ability to securely access and configure power grid devices in a multi-vendor environment
- Significant manual effort required to baseline and manage devices
- Vendor-neutral tools that can seamlessly interface with device configurations in a multi-vendor environment
- Vendor-neutral tools that can parse and manipulate configuration interfaces and files
- Lack a centralized, policy-driven framework for configuration management of field systems that is open and vendor-neutral

MEASURES OF SUCCESS

The integration and testing of an integrated solution that incorporates information from identification systems, configuration management systems, and password management systems

DELIVERABLE TYPE

Software, technical publications

ARP PROJECT

P183.008: Asset and Configuration Management (2018)

TIES TO OTHER PROGRAMS

Substations (P37)

Cyber Security Metrics for the Electric Sector

Future States: Utilities will measure their cyber security performance through a standard set of security metrics. Using these metrics, they will clearly communicate the status of cyber security to various stakeholders and measure the effectiveness of security investment based on data. Utilities will also be able to compare the scores and benchmark through established metrics aggregation framework.

Description: As cyber security threats continue to grow in number and sophistication, utilities will need to evaluate and improve their security postures continuously. Continuous improvement cannot be achieved without accurate performance metrics and clear goals. While mandatory security standards provide the initial goal of compliance, the binary nature of compliance comes short of providing strategic direction for continuously evolving technology and threat landscape. Security Metrics for the Electric Sector is an ongoing research project that EPRI is leading in collaboration with multiple member utilities. It aims to create a common set of metrics that quantify the effectiveness of cyber security controls and promote its wider adoption through standardization. EPRI also is developing a framework for industry-level metric data aggregation to support industry benchmarking and long-term trend analysis.

Action Plan:
In 2017, EPRI developed a common set of sixty security metrics based on 120-150 data points, and pilot tested the set with six utility members. In 2018, we will continue the utility pilot for further refinement of metric formulae and data points. To realize the full value of the study, the metrics must be 1) widely adopted; 2) aggregated for statistical analysis across the industry, and 3) correlated with the threat/breach data for advanced analytics. As the first step to address the gaps, EPRI will promote the common set of metrics through standardization and start the development of a security metrics tool for automated data collection, metric calculation, and dashboard reporting. In parallel to this effort, EPRI will start the background research on issues and solutions related to large-scale data aggregation, including data privacy, data anonymization, and security requirements. In 2019, with the consultation with the members, EPRI will launch a supplemental project where the participants will implement the security metrics tool in their own environment, paving the way to industry-level data aggregation in 2020 and onward. EPRI will also examine piloting the security metrics in Generation and Nuclear operating environments.

Major Past Accomplishments	2019	2020	Future
POWER DELIVERY CYBER SECURITY ANNUAL RESEARCH PORTFOLIO (P183)			
• EPRI Cyber Security Metrics development • Security metrics utility pilot • Metrics calculator tool (MetCalc) development • Study on data anonymization, data security and privacy issues for security	• Establish Metrics Advisory Council for ongoing enhancement of the metrics • Engage vendors and industry partners for data collection automation metrics aggregation • Metrics Hub (metric repository and portal site) development	• Security Metric Aggregation Framework implementation with Metrics Hub • Operationalization of security metrics through the supplemental project	• Operationalization of security metrics through the supplemental project (continue) • Industry statistics based on aggregated data • Data analytics using aggregated data and correlations with other data sets

Gaps Addressed:
- The lack of a common set of metrics for leadership to communicate the security status to stakeholders
- The lack of performance metric to measure the effectiveness of security controls and operations
- The lack of reliable historical data for establishing long-term strategic goals
- The lack of industry-level statistics on cyber security performance for benchmarking
- The lack of large-scale data aggregation framework for industry-level security data accumulation

MEASURES OF SUCCESS

- Utility members contribute to the development of cyber security metrics
- Utility members utilize cyber security metrics through pilot studies
- Other EPRI programs or external parties utilize research results

DELIVERABLE TYPE

Investigative results, software, the establishment of industry advisory group

ARP PROJECT

P183.014: Cyber Security Metrics (2018)

TIES TO OTHER PROGRAMS

Information and Communication Technology (P161)

Compliance Standards Driven Solutions

Future States: Utilities have the capability to transparently and confidently implement technical and procedural solutions that resolve security challenges while effectively complying with mandatory standards. By using the Implementation Guidance process, EPRI will develop solutions that are effective and compliant to address security and regulatory challenges.

Description: Cyber security standards, guidance, and regulations have been developed in response to continual threats to business and process control networks. In recent years, electric utilities that are part of the North American Bulk Electric System (BES) have established cyber security programs to ensure compliance with the critical infrastructure protection (CIP) standards of the North American Electric Reliability Corporation (NERC). New cyber security requirements for critical infrastructure are being introduced in other regions as well, such as the Directive on Security of Network and Information Systems (NIS Directive) of the European Commission. In addition, some states are developing cyber security requirements for the distribution sector of the grid.

Compliance with cyber security regulations and cyber security requirements is non-trivial and requires IT staff and control system engineers to work together to implement and maintain a cyber security program for control systems. In some cases, entities seek regulatory certainty from the regulators to determine if a solution will meet compliance with the standards. EPRI can help provide this certainty by developing Implementation Guidance, which are NERC-approved methods to comply with CIP standards, to help provide our members with confidence that their security solutions will be deemed compliant.

Major Past Accomplishments	2019	2020	Future
POWER DELIVERY CYBER SECURITY ANNUAL RESEARCH PORTFOLIO (P183)			
Lab testing of patch management tools	Implementation Guidance for Cloud Solutions – Encryption of BCSI – Operating BES Cyber Systems Off-premise	Development of Security Architectures for Real-time Operations	Development of Community Based-Cloud Pilot Program

Action Plan: Secure Architecture Methodology

- Become a pre-approved organization that can submit implementation
- Development of guidelines and industry support for critical challenges in cloud-based operations for BES Cyber System and BES Cyber Systems Information

Gaps Addressed:

Lack of NERC-approved solutions to address emerging risks on the Bulk Electric System.

MEASURES OF SUCCESS

- NERC-informed security guidance
- Solutions to address compliance issues with cloud-based operations

DELIVERABLE TYPE

- Security-based Implementation Guidance Considerations
- Technical Architectures

ARP PROJECT

P183.013: Cyber Security Compliance (2018)

TIES TO OTHER PROGRAMS

Substation (P37),
Grid Operations and Planning (P39)

Cyber Security Process and Integration for Generation Facilities

Future States: Cyber security is integrated into other utility and generation plant programs and departments, such as physical security, procurement, design engineering, maintenance, and training.

Description: This future state studies technical approaches to address process and coordination challenges associated with cyber security. Additional research in this area includes IT/OT integration and coordination; technical approaches and strategies to address the conflict between skill requirements and reduced resources; security metrics; integration with physical security and procurement departments; training needs; and risk management.

Action Plan:
EPRI will work with members and utilities to understand the synergies that exist between cyber security programs, practices, procedures, and interdependencies with other utility and plant departments and programs. By benchmarking utilities and assessing their maturity and capability, EPRI will be able to research methodologies to better incorporate cyber security into all applicable plant and utility functions.

Gaps Addressed:

- Research on how to integrate cyber security into generation-specific plant's O&M programs
- Understanding of the integration of cyber security with physical security and the interdependencies
- Research on transitioning workforce, skill gaps, and reduction of overall generation workforce (dedicated cyber security staff)

Major Past Accomplishments	2019	2020	Future
GENERATION INSTRUMENTATION, CONTROLS, AND AUTOMATION CYBER SECURITY SUPPLEMENTAL PROJECT (P68)			
• Cyber Security in the Supply Chain • Generation OT Cyber Security Assessment Methodology • Technical Assessment Methodology	• Transient Cyber Asset and Removable Media Guideline • Supply Chain Case Studies • Renewables Cyber Security Overview • Technical Assessment Methodology – Case Studies		
GENERATION CYBER SECURITY ANNUAL RESEARCH PORTFOLIO (P209)			
		• Cyber Security Design Engineering Integration • Plant Management Cyber Security Review • Workforce Development for Generation Cyber Security	• Workforce Development for Generation Cyber Security • Internal Audit for Generation DCS Cyber Security • Vendor Qualifications • Self-Assessment Tools • Receipt Inspections and Warehousing for Generation Plants

MEASURES OF SUCCESS

- Incorporation of cyber security into plant processes and departments
- Other EPRI programs incorporating cyber security into their process guidance and research deliverables

DELIVERABLE TYPE

Working groups, Technical results (knowledge base, guidance, and application level)

ARP PROJECT

P68 Supplemental, **P209** (2020)

TIES TO OTHER PROGRAMS

Operations (P108), Maintenance and Reliability (P69), Balance of Plant Systems (P104), Instrumentation & Control and Automation (P68), Renewables (P193)

Technical Assessment Methodology

Future States: Consistent, repeatable, regulatory agnostic, risk informed processes are used to assess systems, services, and assets across critical infrastructure facilities, vendors, and suppliers.

Description: A consistent risk informed, graded, technical process is needed to assess systems, assets, and services. This process must be modular, integrated, and able to be incorporated across the supply chain to be performed by different people, at different times, across different organizations.

Action Plan:
EPRI will work with different national laboratories, members, and organizations to develop an engineering-based method that meets these objectives.

Gaps Addressed:

- Develop a repeatable method that is fully bounded, efficient, and repeatable by plant engineers and other technically trained personnel
- Develop a process that is risk informed, allowing threat capability intelligence to inform the process and ensure the appropriate level of protection is achieved
- Improve the detailed subject matter knowledge as skill and knowledge gaps are recognized due to changing technology or insufficient awareness of EPRI methods through detailed field guides as needed
- Develop training materials to reduce skill gaps, and improve technology transfer for the overall workforce

Major Past Accomplishments	2019	2020	Future
EPRI TECHNOLOGY INNOVATION CROSS-CUTTING CYBER SECURITY PROGRAM			
• *Technical Assessment Methodology (TAM) Rev One*	• Technical Assessment Methodology Tech Transfer • TAM Field Guides TAM Case Studies for All Sectors (Generation, Nuclear, PDU) • TAM Classroom Training • EXSIM Database Software Tool Beta • TAM CBT Modules, Classroom, and Distance Learning Environment (DLE) Training Development	• Technical Assessment Methodology Tech Transfer • TAM Field Guides • TAM Classroom Training • TAM Revision 2 • EXSIM Database Software Tool Production	• Technical Assessment Methodology Tech Transfer • TAM Field Guides • TAM Classroom Training

MEASURES OF SUCCESS

- Other EPRI programs incorporating cyber security into their process guidance and research deliverables
- Member use and acceptance of TAM into their facility processes and procedures
- Member engagement with the continued development and update of the TAM
- Vendor acceptance and use of TAM

DELIVERABLE TYPE

Technical reports, field guides, training deliverables including CBT modules

TIES TO OTHER PROGRAMS

Nuclear Instrumentation and Control (41.05.03),
Advanced Nuclear Technology (41.08.01),
Instrumentation & Control and Automation (P68),
PDU - Cyber Security (P183),
P209 (2020)

Hazard Consequence Analysis for Digital Systems (HAZCADS)

Future States: Utilities have tools that allow for understanding the impact hazards that are unique to digital hazards such as EMI/RFI, Common Cause Failures, Cyber Security, Single Point Vulnerabilities, and others have on digital equipment and how they impact plant consequences.

Description: Digital equipment can have almost unlimited configurability and the failure mechanisms of the equipment and how it can impact plant consequences is difficult to determine using traditional PRA and other quantitative risk analysis methods. Using qualitative risk methods, these digital failure mechanisms can be analyzed to inform engineers and owners/operators.

Action Plan:
Work with national laboratories, universities, and research the best hazard analysis methods and how they can be applied to digital equipment and systems. STAMP, STPA, and FTA are all methods that will be researched and determined how they can be utilized effectively to mitigate digital hazards.

Gaps Addressed: Develop a repeatable methodology for identifying causal factors that can lead to plant consequences that are attributable to digital components and systems.

Major Past Accomplishments	2019	2020	Future
EPRI TECHNOLOGY INNOVATION CROSS-CUTTING CYBER SECURITY PROGRAM			
• *Hazard Analysis Methods for Digital Instrumentation and Control Systems* • *Program on Technology Innovation: Cyber Hazards Analysis Risk Methodology – Phase II: A Risk Informed Approach* • *HAZCADS: Hazards and Consequences Analysis for Digital Systems*	• HAZCAD Tech Transfer • HAZCAD Integration with Risk Assessment Software Tool • HAZCAD Case Studies for CCF and Cyber Security • HAZCAD CBT Modules, Classroom, Distance Learning Environment (DLE) Training	• HAZCAD Tech Transfer • HAZCAD Field Guides • HAZCAD Software Tool Training Development • HAZCAD Training	• HAZCAD Integration with other Digital Hazard Research such as SPV, EMI/RFI • HAZCAD Field Guides • HAZCAD Training

MEASURES OF SUCCESS

Methodology to identify causal factors unique to digital equipment and systems that can cause a plant consequence is adopted by utilities and integrators worldwide

DELIVERABLE TYPE

Technical reports, updates, member updates, training deliverables including CBT modules

ARP PROJECT

Technology Innovation Project with Programs (P41, P68, and P183)

TIES TO OTHER PROGRAMS

Nuclear Instrumentation and Control (41.05.03), Advanced Nuclear Technology (41.08.01)

Cyber Security Program Guide

Future States: Utilities have a regulatory agnostic, technically sound, risk informed and performance-based framework for implementing a cyber security program. This guidance document will guide the facility and owner/operator to securing their facility.

Description: This program guide can be used by any facility or owner/operator implementing a risk-informed cyber security program.

Action Plan: Cyber Security Program Guide
Research existing regulatory frameworks such as IEC 62443 and others to provide a risk informed framework that synthesizes existing guidance. The program guide should integrate other risk informed approaches where appropriate such as the EPRI Technical Assessment Methodology for performing assessments, or using the Supply Chain Procurement Methodology and using HAZCADS for determining digital causal factors that can lead to a plant consequence. The program guide should also integrate security metrics to monitor the overall performance of the program as appropriate.

Gaps Addressed:
Develop a regulatory agnostic technical based program that mitigates cyber security threats.

Major Past Accomplishments	2019	2020	Future
NUCLEAR INSTRUMENTATION AND CONTROL PROGRAM ANNUAL RESEARCH PORTFOLIO (P41.05.03)			
Cyber Security Program Guide for Nuclear Facilities	Cyber Security Program Guide Tech Transfer	Cyber Security Program Guide Tech Transfer	Revision of Program Guide that allows for cross-sector use cases and provides additional guidance

MEASURES OF SUCCESS

Program Guide is used by members as needed to assist with implementing a sound cyber security program worldwide

DELIVERABLE TYPE

Technical reports, updates, member updates

ARP PROJECT

Nuclear Instrumentation and Control (41.05.03)

TIES TO OTHER PROGRAMS

Cyber Security in the Supply Chain

Future States: Utilities have the capability to leverage a common supply chain security and procurement methodology across all of their business units that provides a common understanding among all parties in the supply chain and incorporates a risk informed process in the development of the target asset and supply chain integrity cyber security requirements.

Description: The supply chain for existing and new nuclear generating stations, as wells as other generation, transmission, and distribution facilities, represents a significant cyber-attack pathway for digital assets and systems. There are several key issues associated with the supply chain that affect both buyers and suppliers including software/firmware of unknown provenance, unknown hardware development sources, counterfeit hardware and software components that may contain malicious code, lack of universal technical standards for cyber security in the supply chain, regulatory uncertainty, risk transference where buyers and suppliers attempt to transfer cyber security risk to the other entity, uncertainty about where integration occurred and who performed the integration, improperly vetted or managed technical services, commingling of target asset cyber security requirements with supply chain integrity requirements, and lack of visibility into lower tier suppliers and processes.

Action Plan: Security in the Supply Chain
The procurement methodology developed for this future state introduces a supply chain model to establish common understanding among all parties in the supply chain and integrates the EPRI Technical Assessment Methodology (TAM) guidance to assist in the development of target asset and supply chain integrity cyber security requirements. This provides a risk informed process for determining the attack surface of a target asset or system and mitigating the attack surface with engineered or site/shared cyber security control methods. This methodology enables development of cyber security procurement specifications for a target asset by providing a clear division of responsibility between the buyer and supplier using a graded approach, as well as development of supply chain integrity specifications while a target asset is in a supply chain segment or in transition.

Major Past Accomplishments	2019	2020	Future
EPRI TECHNOLOGY INNOVATION CROSS-CUTTING CYBER SECURITY PROGRAM			
• *Cyber Security Procurement Methodology for Power Delivery Systems* • *Cyber Security Procurement Methodology, Rev 2*	• Supply Chain Tech Transfer • Supply Chain Case Studies for All sectors (Generation, Nuclear, PDU) • Supply Chain SDID Guide • Supply Chain Field Guides • Supply Chain CBT Modules, Classroom, Distance Learning Environment (DLE) Training	• Supply Chain Tech Transfer • Supply Chain Field Guides • Digital Procurement Methodology Rev. 3 • Cyber Security Design Engineering	• Vendor Qualifications • Receipt Inspections and Warehousing for Generation Facilities

Gaps Addressed:
The lack of techniques, including strategies, to address potential cyber security vulnerabilities in the supply chain.

MEASURES OF SUCCESS

Methodology to address security in the supply chain adopted by utilities and suppliers

DELIVERABLE TYPE

Technical reports, updates, member updates, training deliverables including CBT modules

ARP PROJECT

Technology Innovation Project with Programs (P41, P68, and P183)

TIES TO OTHER PROGRAMS

P41.05.03 Nuclear Instrumentation and Control,
P41.08.01 Advanced Nuclear Technology,
Instrumentation & Control and Automation (P68),
P183 PDU - Cyber Security
P209 (2020)

Protect

The NIST Cybersecurity Framework defines the Protect Function as "Develop and implement appropriate safeguards to ensure the delivery of critical services." Specifically, the activities in this function involve "the ability to limit or contain the impact of a potential cyber security event."

Categories within this Function include:

- Identity Management and Access Control;
- Awareness and Training;
- Data Security;
- Information Protection Processes and Procedures;
- Maintenance; and
- Protective Technology

The following Future States support the business processes and technologies required to effectively and efficiently execute activities within the Protect Function's categories:

- Security Architecture for Flexible and Resilient Utility Systems
- Protective Measures for Distributed Energy Resources
- Protective Measures for Generation Industrial Control Systems

Security Architecture for Flexible and Resilient Utility Systems

Future State: Flexibility and resiliency have become critical concerns for the OT infrastructure supporting utility systems. Security architecture patterns supporting these characteristics are available to industry for timely analysis of emerging vulnerabilities and establishment of practical risk mitigation strategies.

Description: The rapid changes occurring in the grid demand flexibility and resiliency of the grid, in addition to reliability. The modern technologies adopted to support this demand depend increasingly on digitalization and interconnection, expanding attack surface exponentially. To maintain security in such rapid expansion, cyber security professionals require the ability to design and deploy key security controls quickly and analyze and mitigate emerging vulnerabilities in a timely manner.

Security architecture research aims to identify system architecture patterns for various areas of utility operations and provide multiple reference architectures with built-in security controls. The security reference architectures can be used for:

- Design and deployment of new systems
- Security augmentation of old systems
- Architectural review of current systems
- Remediation of discovered security vulnerabilities

In addition, the research also suggests methodologies for vulnerability analysis and attack modeling, which can be utilized for the configuration of security controls.

Action Plan: Reference Architectures
The project will run as a multi-year effort, addressing different areas of utility OT systems each year. In the past, the focus was given to the transition for legacy, transient, and future substations. In 2018, the project focused on current systems supporting distribution operations – DMS, ADMS, GIS, ORMS, DERMS, etc., and the surrounding infrastructures. To complete the picture, the project collaborated with P200 Distribution Operations and Planning to address cyber security guidelines for distribution operators, who are the main users of this system. The project will leverage the foundational work of 2018 and tackle the challenge of creating reference architectures for distribution grid modernization and large-scale renewable generation.

Especially the following topics will be examined:

- Security Architecture for DER integration
- Cyber security Considerations for Distributed Energy Storage
- Security Architecture using Software Defined Network (SDN)
- Security Architecture for Large-Scale Renewables
- Security Architecture for utility IoT
- Security Architecture for Electric Vehicle Service Equipment (EVSE)
- Updating NESCOR Failure Scenario for grid-edge systems
- Attack modeling for utility OT infrastructure

Gaps Addressed:
The lack of practical security reference architecture that can be modified and applied into a utility OT environment in a short period of time.

Major Past Accomplishments	2019	2020	Future
POWER DELIVERY CYBER SECURITY ANNUAL RESEARCH PORTFOLIO (P183)			
• Attack surface analysis for micro-grid • Security architecture for distribution systems • Cyber security considerations for distribution operators	Attack modeling for utility OT infrastructure	Security Architecture for utility IoT	Security Architecture using Software Defined Network
EPRI TECHNOLOGY INNOVATION CROSS-CUTTING CYBER SECURITY PROGRAM			
	• Security Architecture for DER integration • Cyber security Considerations for Distributed Energy Storage • Updated NESCOR Attack Scenarios for grid-edge systems	• Security Architecture for EVSE • Updated NESCOR Attack Scenarios for Grid-edge systems (continue)	Security Architecture for EVSE (continue)

Continued next page

Security Architecture for Flexible and Resilient Utility Systems/continued

Major Past Accomplishments	2019	2020	Future
GENERATION INSTRUMENTATION, CONTROLS, AND AUTOMATION CYBER SECURITY SUPPLEMENTAL PROJECT (P68)			
• Generation DCS Reference Architectures • Secure Remote Access Reference Architecture			
GENERATION CYBER SECURITY ANNUAL RESEARCH PORTFOLIO (P209)			
		Reference Architecture for Large-Scale Renewables Cyber Security	Reference Architecture for Generation Interdependencies

MEASURES OF SUCCESS

- Utilities contribute to the development of reference architecture and attack models
- Utilities utilize architecture patterns and attack models
- Other EPRI programs or external parties utilize research results

DELIVERABLE TYPE

Investigative reports

ARP PROJECT

P183.012: Cyber Security Architecture
P68 Supplemental and **P209** (2020)

TIES TO OTHER PROGRAMS

Electric Transportation (P18), Energy Storage and Distributed Generation (P94), Information and Communication Technology (P161), Integration of Distributed Energy Resources (P174)

Protective Measures for Distributed Energy Resources

Future States: Effective cyber security strategies are implemented in the multi-party grid where large numbers of distributed energy resources are deployed and managed by utilities, customers and various third parties.

Description: Distributed Energy Resources (DER), including solar photovoltaics, battery storage, electric vehicles, demand response, and axiomatic devices, and sub-systems and systems, are connected to the grid in ever-increasing numbers. Integrated DER can perform advanced grid-supportive services, but in order to enable these services, the devices must be connected; and data must flow among different systems. The growing presence of utility and third-party owned DER has introduced significant challenges for cyber security. Effective cyber security requires utilities to understand potential threats and to implement cyber security governance, architectures, technology solutions, and business processes.

Action Plan:
EPRI will take a multi-pronged approach to address cyber security needs for the fast-changing world of DERs. Multiple studies, tests, and assessments will be conducted in over-lapping time scale, focusing on the risks that are introduced to the reliability of the distribution or even bulk transmission grids.

This action plan includes:

- Survey cyber security leading practices and solutions for management of utility, customer and third-party owned devices, addressing configuration management, patch management, and change management
- Research and test new technologies and approaches for securing communications among DER systems owned by multiple parties
- Further, refine electric sector-specific guidelines for cyber security and data protection for DER integration

Major Past Accomplishments	2019	2020	Future
EPRI TECHNOLOGY INNOVATION CROSS-CUTTING CYBER SECURITY PROGRAM			
	Device Hardening Guide for DER Integration	Communication security guidelines for DER Integration	Utility guidelines for system security management for DER/DERMS

Gaps Addressed:
The lack of commonly accepted cyber security solutions for communication and operational security for customer-, utility- or third-party owned assets/systems.

MEASURES OF SUCCESS

- Utility members contribute to the development of guidelines, requirements, or white paper
- Utility members utilize research results in their current projects or operations
- Other EPRI programs or external parties utilize research results

DELIVERABLE TYPE

Investigative results

ARP PROJECT

TBD

TIES TO OTHER PROGRAMS

Electric Transportation (P18), Energy Storage and Distributed Generation (P94), Information and Communication Technology (P161), Integration of Distributed Energy Resources (P174), Instrumentation & Control and Automation (P68)

Protective Measures for Generation Industrial Control Systems

Future States: Methodologies, process guidance, and technology to protect against a cyber attack in generation facilities are available and widely adopted.

Description: This research focus area concentrates on technical and operational security control methods to protect against an attack. Generation Sector research in this area has included interactive remote access, patch management, hardening, access and identity management. Additional research needs in this area include identity management and governance, cryptography, asset and configuration management, advanced boundary devices, hardware-based decentralized secure remote access, secure architectures and effective personnel awareness programs.

Action Plan: EPRI will conduct research and development on many different aspects of protection against a cyber attack in a generation plant. Because of the unique nature of generation control system networks and interaction with cyber-physical processes, EPRI will focus the research and development efforts working with utility members, industry subject matter experts, and third-party research partners (such as government and university). Depending on the sector and programmatic maturity, research results may be presented as knowledge base documents, generation-specific guidance, or application-type deliverables.

Gaps Addressed:

- Research on how to protect generation-specific equipment from a cyber attack
- Understanding of the methodologies, technologies, and procedures that are appropriate in a generation plant and integrate with legacy existing equipment to provide protective functions against cyber attacks

GENERATION INSTRUMENTATION, CONTROLS, AND AUTOMATION CYBER SECURITY SUPPLEMENTAL PROJECT (P68)

Major Past Accomplishments	2019	2020	Future
• Interactive Remote Access • Configuration Management and Hardening • Patch Management • Access and Permission Management • Technical Assessment Methodology	• Hardening Field Guides • Advanced Vulnerability Grading Tool • Secure Remote Access Pilots		

GENERATION CYBER SECURITY ANNUAL RESEARCH PORTFOLIO (209)

Major Past Accomplishments	2019	2020	Future
		• Network Connectivity and Segmentation • Cryptography and Authentication • Integration of Physical and Cyber Security • DCS Integrated Architecture and Active Directory • Hardening Field Guides	• Secure Wireless • Application White listing • Automated Patch Management and Regression Testing • Hardening Field Guides • Integration of Physical and Cyber Security • Securing non-DCS Assets • Using Advanced Security Techniques in Virtualization • Using and Protecting RTOS • Advanced Boundary Device Architectures • Hardening Field Guides

MEASURES OF SUCCESS

- Increased cyber security posture and readiness levels within the industry
- Integration of process guidance, methodologies, and technology into generation utility cyber security program environments
- Integration of process guidance, methodologies, and technology into other EPRI programs

DELIVERABLE TYPE

Technical results (Knowledge base, process guidance, and application deliverables)

ARP PROJECT

P68 Supplemental, **P209** (2020)

TIES TO OTHER PROGRAMS

Instrumentation & Control and Automation (P68), Maintenance and Reliability (P69), Operations (P108), Renewables (P193)

Detect

The NIST Cybersecurity Framework defines the Detect Function as “Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.” Specifically, the activities in this function “enable timely discovery of cybersecurity events”.

Categories within this Function include:

- Anomalies and Events;
- Security Continuous Monitoring; and
- Detection Processes

The following Future States support the business processes and technologies required to effectively and efficiently execute activities within the Detect Function’s categories:

- Incident Detection
- Threat Management

Incident Detection

Future State: Utilities will have the tools and capabilities to effectively monitor and detect cyber security incidents. They will have solutions in place to integrate event monitoring and response for IT, OT, physical security, power system operations, and external threat information. As part of the incident management response, utilities will have the skills and tools to conduct effective forensics analysis in the OT environment. New solutions will emerge to automatically detect and prioritize security events using machine-learning technology. Additionally, data analytics will be a mainstream tool utilized by utilities to determine trends for cyber security event information and develop decision models for incident monitoring and detection.

Description: The objective of this project is to increase the capabilities and efficiency of incident detection for power delivery and generation systems through innovative monitoring solutions.

Action Plan: The Integrated Security Operations Center (ISOC)

This project provides guidelines and solutions for implementing a security operations center that integrates monitoring and response for IT, OT, physical security, grid operations events, and external threat information. The ISOC will enable power delivery system owners to:

- Enhance incident monitoring and detection capabilities
- Improve incident response times
- Contain incidents
- Reduce operational impact of incidents

Action Plan: Intrusion Detection/Prevention Systems (IDS/IPS) Solutions Analysis and Testing for ICS Environments

This project will provide guidance for the evaluation of IDS/IPS solutions and will evaluate effectiveness of IDS/IPS solutions during various types of cyber-attacks and incidents. The resulting knowledge will help utilities save time and money by eliminating the need to set up their own testing environments, benefit from pooled knowledge, and may improve their vendor selection processes.

Gaps Addressed:

- Situational awareness for the entire utility environment, including IT, OT, physical security, and operations
- Tools needed to analyze the significant amount of data collected for security operations
- Solutions for automating incident detection and prioritization are needed to augment the ISOC capabilities
- Effective application of IDS/IPS tools in the OT environment has not been achieved

Major Past Accomplishments	2019	2020	Future
POWER DELIVERY CYBER SECURITY ANNUAL RESEARCH PORTFOLIO (P183)			
• ISOC Guidebook • Guidelines for planning an ISOC • Guidelines for integrating control center systems into an ISOC • Guidelines for integrating the substation and field domain into an ISOC • IDS/IPS guidelines for power deliver systems • ITAF framework and utility testing	• ISOC Guidebook update • Utilizing artificial intelligence and machine-learning for incident management • Data analytics guidelines for incident management • Review and update the National Electric Sector Cyber security Organization Resource (NESCOR) failure scenarios	• ISOC Guidebook update • Utilizing artificial intelligence and machine-learning for incident management • Data analytics for incident management; utilizing use cases and determining trends for machine-learning	Artificial intelligence for predictive analysis
POWER DELIVERY CYBER SECURITY SUPPLEMENTAL PROJECT – INTRUSION DETECTION/PREVENTION SYSTEMS (IDS/IPS) SOLUTIONS ANALYSIS AND TESTING FOR ICS ENVIRONMENTS (P183)			
Project launched	Interim test results and draft report	Final report published	

Continued next page

Incident Detection/continued

Action Plan: Incident Detection for DER Systems

Enhance utility threat detection and response capabilities by 1) developing and testing new threat detection technologies for DER systems and 2) exploring solutions for monitoring power distribution system behavior for early identification and isolation of cyber security incidents. PDU Program P183: Incident Detection for DER and Grid-Edge Systems

Gaps Addressed:

Accelerating the development and adoption of new technologies that could enable effective threat detection and response for DER assets, systems, or supporting network infrastructure.

Major Past Accomplishments	2019	2020	Future
EPRI TECHNOLOGY INNOVATION CROSS-CUTTING CYBER SECURITY PROGRAM			
		Advanced security event monitoring and threat detection for DER systems – exploring solutions for early detection and isolation	Advanced security event monitoring and threat detection for DER systems – exploring solutions for early detection and isolation

Continued next page

Incident Detection/continued

Action Plan: Incident Detection for Generation Facilities
The Generation Sector's research in this area includes control network scanning and security status event monitoring. Additional research includes monitoring and inspection of control system protocols, network and system level monitoring, real-time detection and notification, data analytics, monitoring devices in the M&D center and plant security integration with Integrated Security Operation Centers (ISOC).

Gaps Addressed:

- Research on how to detect cyber attacks in generation-specific DCS and control system networks
- Understanding of the methodologies, technologies, and procedures that are appropriate in a generation plant and integrate with legacy existing equipment to provide detection mechanism for cyber attacks

GENERATION INSTRUMENTATION, CONTROLS, AND AUTOMATION CYBER SECURITY SUPPLEMENTAL PROJECT (P68)

Major Past Accomplishments	2019	2020	Future
• Real-time Detection Overview • Control Systems Protocols and Scanning • Security Status (Event) Monitoring • ISOC and M&D Integration	• Network and System Monitoring • Data Analytics and Incident Detection		

GENERATION CYBER SECURITY ANNUAL RESEARCH PORTFOLIO (P209)

Major Past Accomplishments	2019	2020	Future
		• Securing DCS and Generation Control System Protocols • Network and Asset Discovery and Visualization • Data Analytics and Incident Detection	• Securing DCS and Generation Control System Protocols • Integrated Event Monitoring Frameworks (ISOC) • Detection and Correlation Across Different OT Networks • Plant Data Analytics for Cyber Incident Detection

MEASURES OF SUCCESS

- Situational awareness is fully achieved for power delivery system owners
- Incident management solutions and processes are available and utilized for power deliver systems
- Artificial intelligence and machine-learning are utilized for incident management
- Data analytics solutions have been applied to the incident management process

DELIVERABLE TYPE

Technical updates, investigative results, working group

ARP PROJECT

183.005: Incident Response (2018)
P68 Supplemental Project, **P209** (2020)

TIES TO OTHER PROGRAMS

Substations (P37), Distribution (P180), Integration of DER (P174), Instrumentation & Control and Automation (P68), Operations (P108)

Threat Management

Future State: Utilities will have the tools and capabilities to manage and mitigate threats.

Description: The objective of threat and vulnerability management is to establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cyber security threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (for example critical, IT, or OT) and organizational objectives. Advanced Threat Management for should:

- Be adaptive to the changing threat environment
- Incorporate threat intelligence into automated response systems
- Rapidly contain cyber incidents
- Provide a better understanding of the impact of decisions on power system operations
- Identify and measure the impact of a cyber security incident

Action Plan: Threat and Vulnerability Management

- Provide visibility into indicators of compromise across the entire enterprise
- Incorporate threat intelligence into automated response systems
- Develop automated threat response systems for utility environments
- Develop guidebooks to contain cyber incidents more rapidly
- Ability to identify and measure the impact of a cyber security incident.
- Develop the capabilities to discover vulnerabilities in a utility ICS environment

Gaps Addressed:

- The lack of utility focused tools to facilitate threat and vulnerability management
- The lack of trained subject matter experts that are capable of performing penetration testing and hunting in a utility environment

Major Past Accomplishments	2019	2020	Future
POWER DELIVERY CYBER SECURITY ANNUAL RESEARCH PORTFOLIO (P183)			
• Investigated and contributed to OT Threat Modeling Language tools for OT systems • Guidelines for threat hunting techniques for OT systems • Three successful Birds of a Feather Threat Management Workshops	Guidelines for integrating threat intelligence feeds for protecting OT systems	Develop automated response to threat intelligence for OT systems	Pilot testing of automated threat response system
POWER DELIVERY CYBER SECURITY SUPPLEMENTAL PROJECT – INTRUSION DETECTION/PREVENTION SYSTEMS (IDS/IPS) SOLUTIONS ANALYSIS AND TESTING FOR ICS ENVIRONMENTS (P183)			
• Identify ICS vulnerabilities and means of exploitation • Investigate vulnerability mitigations and solutions. • Provide training on ICS penetration testing best practices	• Identify more advanced ICS vulnerabilities and mitigations • Build the capabilities to do in house industry training	• Provide on going training to utility members • Provide on going discovery of advanced vulnerabilities in utility focused ICS solutions	

MEASURES OF SUCCESS

- Prioritizing and addressing threats that are considered important (e.g., implement mitigating controls, monitor threat status)
- Threat hunting capabilities for OT systems
- Exchange of threat information for OT protocols, applications, and systems
- Development of tools that enable the effective penetration testing of ICS systems
- Discovery of new, zero day, vulnerabilities in utility focused ICS systems

DELIVERABLE TYPE

Investigative results

ARP PROJECT

P183.006: Threat Management (2018)

TIES TO OTHER PROGRAMS

Substations (P37), Distribution (P180)

Continued next page

Action Plan: Threat Management for Generation Systems

This action plan focuses on understanding and staying apprised of current threats, vulnerabilities, and trends for Generation Systems. Research in this area includes guidance on using multiple information sources to understand and gauge the threat, understanding new emerging threats, evaluating vulnerabilities, and distilling and interpreting threat information by informing the cyber security program and posture to stay ahead of an advancing adversary's sophistication.

Gaps Addressed:

- Understanding of the current threat landscape and trends associated with the Generation Sector
- Understanding the impact of vulnerabilities in Generation-specific industrial control system equipment
- Implementing threat intelligence feeds into risk management approaches

GENERATION INSTRUMENTATION, CONTROLS, AND AUTOMATION CYBER SECURITY SUPPLEMENTAL PROJECT (P68)

Major Past Accomplishments	2019	2020	Future
Quick Briefs/ Analysis on Forming or Impending Cyber Threats to Generation	• Coordination with the Technical Assessment Methodology • Changing Threat Landscape Study		

GENERATION CYBER SECURITY ANNUAL RESEARCH PORTFOLIO (P209)

Major Past Accomplishments	2019	2020	Future
		• Coordination with the Technical Assessment Methodology • Advanced Skills Training: Threat Hunting in DCS Systems • Threat Hunting in DCS Systems	• Threat Information Sharing and Collaboration • Technologies and Services for Threat Discovery/ Mitigation • Indicator Development Techniques, Technologies, and Standards • Distilling Internal and 3rd Party Information • Defense-in-Depth Holistic Protection Measures

MEASURES OF SUCCESS

- Situational awareness of current and evolving threats effecting the generation sector
- Adaptation of threat information used within the generation sector for protection, detection, and response & recovery
- Use of 3rd Party information in generation focused threat protection activities

DELIVERABLE TYPE

Technical updates, working groups, technical results (knowledge base, guidelines, application deliverables)

ARP PROJECT

P183
P68 Supplemental, **P209** (2020)

TIES TO OTHER PROGRAMS

Instrumentation & Control and Automation (P68)

Respond & Recover

The Respond and Recover Functions are grouped together in this Roadmap since they are often developed jointly within organizations. The NIST Cybersecurity Framework defines the Respond Function as "Develop and implement appropriate activities to take action regarding a detected cybersecurity incident." Categories within this Function include:

- Response Planning;
- Communications;
- Analysis;
- Mitigation; and
- Improvements.

The Recover Function is defined as "Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident." Categories within this Function include:

- Recovery Planning;
- Improvements; and
- Communications

The following Future States support the business processes and technologies required to effectively and efficiently execute activities within the Respond and Recover Functions' categories:

- Cyber Security Forensics for Industrial Control Systems
- Respond & Recover Capabilities for Generation Facilities

Cyber Security Forensics for Industrial Control Systems

Future States: Utilities will have the tools and capabilities to conduct effective forensics analysis in an OT environment.

Description: Incident Response is the process of containing and recovering from cyber security events. The objective of this project is to increase the capabilities and efficiency of incident response through innovative forensics solutions and technical tabletop exercises. These capabilities also will aid utilities in understanding the origin of incidents and the impact on power system operations.

Action Plan: Cyber security Forensics for Industrial Control Systems (ICS)
This project provides guidelines and methods for utilities to manage security incidents in the latter stages of the incident management process including response to incidents, recovery and continuity of operations, and post-incident analysis and action. This project will improve the forensics capabilities of power delivery system owners by:

- Providing methods for detection of cyber security incidents in ICS systems
- Identifying tools that support forensics in ICS systems
- Improving processes for sharing information related to ICS cyber security incidents for:
  - – Entities involved in the internal and external forensics process
  - – Peer utilities
  - – Industry partners
  - – Solution providers

Gaps Addressed:
The lack of forensics tools and processes for the industrial control system or OT environment.

Major Past Accomplishments	2019	2020	Future
POWER DELIVERY CYBER SECURITY ANNUAL RESEARCH PORTFOLIO (P183)			
• Guidelines for an ICS forensics program • ICS Forensics Working Group	• ICS Forensics Analysis Guidelines • ICS Forensics Working Group • Power Delivery Forensics Tabletop Testing and Drills Methodology	• ICS Forensics Analysis Guidelines • ICS Forensics Working Group	

MEASURES OF SUCCESS

ICS forensics capabilities are available and utilized for power delivery systems

DELIVERABLE TYPE

Investigative results, working group

ARP PROJECT

183.005: Incident Response (2018)

TIES TO OTHER PROGRAMS

Substations (P37), Distribution (P180), Instrumentation & Control and Automation (P68), Instrumentation & Control (P41)

Respond & Recover Capabilities for Facilities

Future States: Facilities will have the guidelines and processes necessary to efficiently respond and recover from a cyber security attack.

Description: This research area focuses on technical and operational security control methods to respond and recover from an attack. Research needs in this area include identifying a cyber-attack, back-up and recovery, incident classification and response, and industry operating experience and forensic analysis.

Gaps Addressed:

- Research on how to respond and recover from a cyber-attack in DCS and control system networks
- Understanding of the methodologies, technologies, and procedures that are appropriate in a generation plant and integrate with legacy existing equipment to provide response and recovery functions to include augmenting disaster management
- Investigate backups and reconstitution methods for legacy, emerging technologies, and automation, and DCS targeted for critical infrastructure plants

Major Past Accomplishments	2019	2020	Future

GENERATION INSTRUMENTATION, CONTROLS, AND AUTOMATION CYBER SECURITY SUPPLEMENTAL PROJECT (P68)

Major Past Accomplishments	2019	2020	Future
Incident Response Guideline (Generation)	Incident Detection and Classification Field Guide		

Major Past Accomplishments	2019	2020	Future

EPRI TECHNOLOGY INNOVATION CROSS-CUTTING CYBER SECURITY PROGRAM

Major Past Accomplishments	2019	2020	Future
		• Cross Sector Plant Testing and Drills Methodology • Generation Cyber Incident Scenarios • Nuclear Cyber Incident Scenarios • PDU Cyber Security Incident Scenarios	• Playbook Development • Response and Recovery Integration into Disaster Recovery Operations • Plant Response Functions Integration into Corporate ISOCs • Backup and Restoration Best Practices • External Support and Intelligence • Forensics in DCS Incident Response

MEASURES OF SUCCESS

- Incident management solutions and processes are available and utilized for all sectors (Generation, Nuclear, and PDU)
- Incident response and preparedness is improved within the generation sector
- Data analytics and Monitoring and Diagnostics data is used to inform incident response capabilities

DELIVERABLE TYPE

Working groups, technical results (knowledge base, guidelines, application deliverables)

ARP PROJECT

P68 Supplemental, **P209** (2020)

TIES TO OTHER PROGRAMS

Power Delivery Cyber Security (P183), Instrumentation & Control and Automation (P68), P41.05.03 Nuclear Instrumentation & Control

Glossary and Acronym Definitions

A
ACM: Asset and Configuration Management
ADMS: Advanced Distribution Management Systems
AHR: Air-conditioning, Heating, and Refrigeration Institute
AMI: Advanced Metering Infrastructure
ANL: Argonne National Laboratory
ANSI C12.22: American National Standard for Protocol Specification for Interfacing to Data Communication Networks
APPA: American Public Power Association

B
Backhaul: The backhaul portion of the telecommunications network comprises the intermediate links between the core network, or backbone network and the small subnetworks at the "edge" of the entire hierarchical network
BES: Bulk Electric System
Bitcoin: A cryptocurrency and a payment system
BlockChain: A distributed database that maintains a continuously-growing list of ordered records called blocks

C
CBT: Computer Based Training
CCF: Common Cause Failure
CCOMS: Cyber combat simulator
CEC: California Energy Commission
CIM: Common Information Model
CIP: Critical Infrastructure Protection
CM: Configuration Management
COP: Common Operating Picture
COTS: Commercial Off-the-Shelf
CPM: Cyber Security Program Management
CS: Cyber Security
CSF: NIST Cybersecurity Framework (CSF) Reference Tool

D
DCS: Distributed Control System
DER: Distributed Energy Resources
DERMS: Distributed Energy Resource Management System
Distributed Control System
DLE: Distance Learning Environment
DMD: Distribution Modernization Demonstration
DMR: Digital Mobile Radio
DMS: Distribution Management System
DNP3: Distributed Network Protocol
DR: Demand Response
DRAS: Demand Response Automation Server
DRMS: Demand Response Management System

E
EA: Enterprise Architecture
EDM: External Dependencies Management
EEI: Edison Electric Institute
EMI/RFI: Electromagnetic and Radio Frequency Interference
EPIC: California Electric Program Investment Charge
EPRI: Electric Power Research Institute
EVSE: Electric Vehicle Service Equipment

F
FAN: Field Area Network
FCC: Federal Communications Commission
FLISR: Fault location, isolation, and service restoration
FTA: Fault Tree Analysis

G
GIS: Geospatial Information System

H
HAZCADS: Hazard Consequence Analysis for Digital Systems

I
ICS: Industrial control systems environment
ICT: Information and Communications Technology
IDS: Intrusion Detection System
IEC: International Electrotechnical Commission
IED: Intelligent Electronic Devices
IoT: Internet of Things
IOUs: Investor owned utilities
IP: Internet Protocol
IPS: Intrusion Protection System
IR: Incident Response
IRM: Interface Reference Model
ISOC: Integrated Security Operations Center
IT: Information Technology
ITAF: Integrated Threat Analysis Framework
ITIL: Information Technology Infrastructure Library

L
LMR: Land mobile radio

M
M&D: Monitoring and Diagnostic
MG: Microgrid
MOM: Message-oriented middleware
MPLS: Multi Protocol Label Switching
MVNO: Mobile virtual network operator

N
NAN: Neighborhood Area Network
NaN: Stands for not a number, is a numeric data type value representing an undefined or unrepresentable value
NERC: North American Electric Reliability Corporation
NESCOR-Cybersecurity: National Electric Sector Cyber Security Organization Resource
NFV: Network Functions Virtualization
NIS: Network and Information Security
NIST: U.S. National Institute of Standards and Technology
NMS: Network management station
NOC: Network operations center
NRECA: National Rural Electric Cooperative Association
NREL: National Renewable Energy Lab

O
O&M: Operation and Maintenance
ODI: Outage Data Initiative
OFDM: Orthogonal Frequency Division Multiplexing

OMS: Outage Management System
OP: Operations Technology
OpenADR: Open Automated Demand Response
OpenESB: Open Enterprise Service Bus
OpenFMB: Open Field Message Box
OpenWMS: Open Workflow Management System
ORM: Object-relational mapping
OSI: Open Systems Interconnection
OT: Operational Technology

P
P25: Project 25 (or APCO-25) Standards for digital radio communications
PDP: Pre-Demonstration Project
PDU: Power Delivery Utilization
PHY: Is an abbreviation for the physical layer of the OSI model and refers to the circuitry required to implement physical layer functions
PHY: PHYsical Layer
PHY and MAC: PHY chips handle the physical layer (Layer 1 of the OSI model), while MAC chips handle the data link layer (Layer 2 of the OSI model). MAC is Media Access Control which will control the transfer of data from PHY
Physical Layer L1: In the seven-layer OSI model of computer networking, the physical layer or layer 1 is the first and lowest layer. The implementation of this layer is often termed PHY
PLC Network Technology: PLC offers a unique means of communication for a power-supply system, which takes full advantage of the wide coverage of power-line installations without having to lay dedicated cables. Like RF wireless modules, it's easy to embed PLC modules into electrical meters
PMU: Phasor measurement units
PRA: Probabilistic Risk Assessment
PV: Photovoltaics
PVNO: Private virtual network operator

Q
QoS: Quality of service

R
RF: Low-power RF networking refers to the use of 315 MHz/433 MHz/780 MHz/2.4-GHz frequencies with transmit power equal to or less than 50 mW
RF LAN: Radio Frequency-Local Area Network
RM: Risk Management

S
SA: Secure Authentication
SANS: The SANS Institute was established in 1989 as a cooperative research and education organization. SANS is the most trusted and by far the largest source for information security training and security certification in the world
SAS: (previously "Statistical Analysis System") is a software suite developed by SAS Institute for advanced analytics, multivariate analyses, business intelligence, data management, and predictive analytics
SCRAM: Security, cyber, risk assessment methodology
SDN: Software Defined Network
SDO: Standards Development Organization
SME: Subject Matter Expert
SOA: Service-Oriented Architecture
SPN: Supplemental Opportunity
SPV: Single Point Vulnerability
STPA: Systems Theoretic Process Analysis

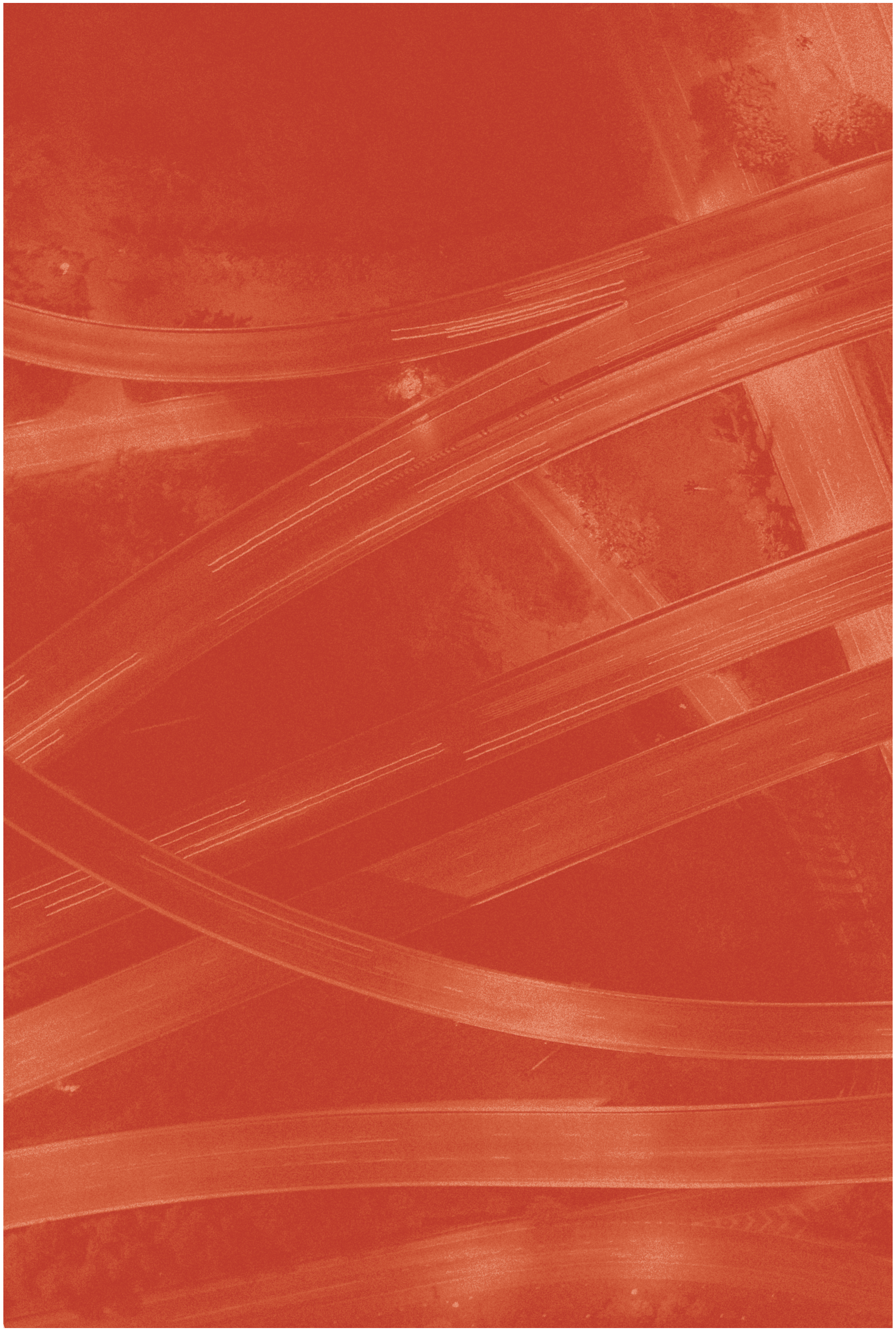
T
T&D: Transmission and Distribution
T&S: Transmission and Substations
TAM: Technical Assessment Methodology
TDM: Time-division multiplexing
TETRA: Terrestrial Trunked Radio
TI: Technology Innovations
Transport Layer L4: Transport layer is a conceptual division of methods in the layered architecture of protocols in the network stack in the Internet Protocol Suite and the Open Systems Interconnection (OSI).
In the OSI model the transport layer is most often referred to as **Layer 4**
TVM: Threat and Vulnerability Management

U
UAS: Unmanned aerial system
UTC: Utilities Technology Council

V
VLAN: Virtual local area network
VoLTE: Voice over **LTE** (Long Term Evolution)
VPP: Virtual Power Plant

W
WAN: Wide Area Network
Wi-Sun: Alliance promoting open interoperable industry standards for smart utility network communications
WSDL: An XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are described abstractly, and then bound to a concrete network protocol and message format to define an endpoint

X
XSD: (XML Schema Definition), a recommendation of the World Wide Web Consortium (W3C)



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's members represent approximately 90 percent of the electricity generated and delivered in the United States, and international participation extends to more than 30 countries. EPRI's principal offices and laboratories are located in Palo Alto, CA; Charlotte, NC; Knoxville, TN; and Lenox, MA.

3002014536

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

To join, contact:
Power Delivery and Utilization Sector: Galen Rasche, 650.855.8779, *grasche@epri.com*
Generation Sector: Jason Hollern, 704.595.2579, *jhollern@epri.com*
Nuclear Sector: Michael Thow, 704.595.2967, *mthow@epri.com*