EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Roadmap

Cyber Security

January 2020

INTRODUCTION

EPRI's Cyber Security 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.

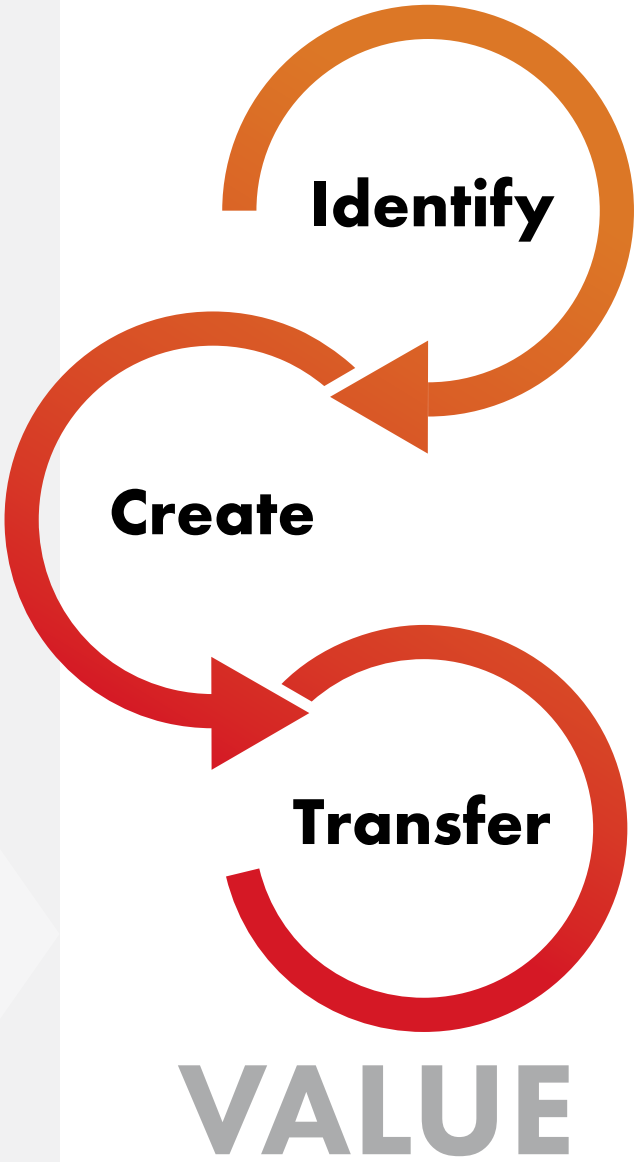
Approach

- 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 of High Value, Easy to Implement and Likely to Succeed

Power Delivery and Utilization

Generation Sector

Nuclear Sector



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

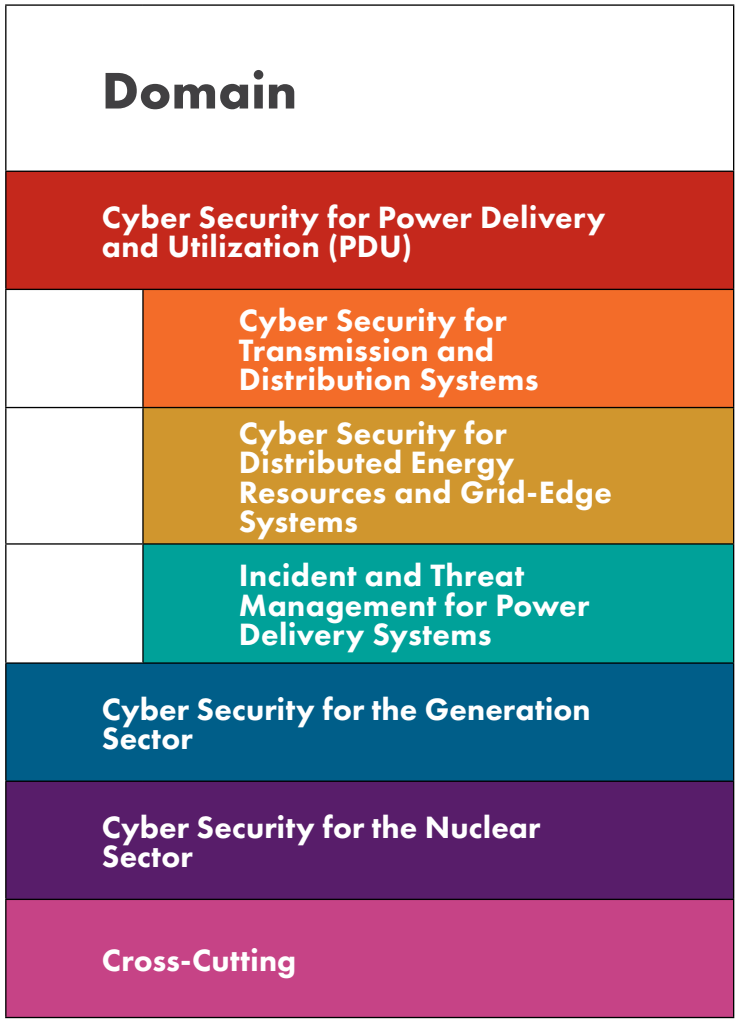
Lab/Field Demos

Software Tools

Videos

Training Modules

PROGRAMS DEFINE ACTION PLANS



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 Roadmap

Future State

- Securing Grid Control Centers
- Securing Substations
- Securing Field Systems
- Taskforce for Cyber Security for Distributed Energy Resources and Grid-Edge Systems
- DER Technology Application Area & Demand Response and Connected Loads
- Incident Detection
- Threat Management
- Cyber Security Forensics for Industrial Control Systems
- Cyber Security Process and Integration for Generation Facilities
- Protective Measures for Generation Industrial Control Systems
- Incident and Threat Management for Generation Facilities
- Respond and Recover Capabilities for Generation Facilities
- Cyber Security Program Guide
- Hazard Consequence Analysis for Digital Systems (HAZCADS)
- Cyber Security Metrics
- Technical Assessment Methodology
- Cyber Security for the Supply Chain

Cyber Security 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 U.S. 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.

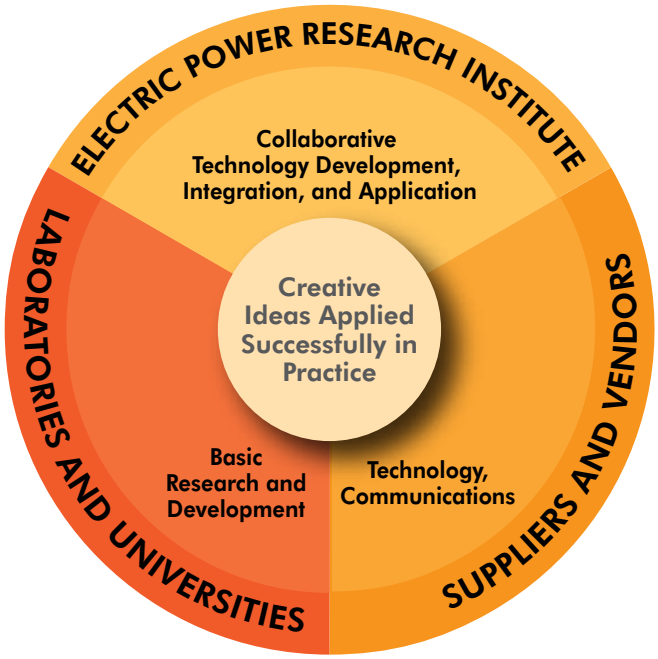
Cyber security measures must be designed and implemented to support grid reliability. These measures must also support grid resilience against attacks by terrorists and hackers, natural disasters, and inadvertent threats such as equipment failures and user errors.

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 Multi-year 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 Roadmap



Cyber Security 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
- Technologies which support cyber programmatic management and increase the cyber security posture

CYBER SECURITY FOR TRANSMISSION AND DISTRIBUTION

Power delivery systems are designed to safely and reliably connect generation sources to utility customers. Electric power is a unique commodity in that it must be generated and used instantaneously due to the lack of deployed grid-scale storage. Utilities also interconnect their power delivery systems with neighboring utilities to achieve diversity and increased system reliability. These factors combine to create a large-scale system that must be continuously balanced while utilities serve their own customers and support neighboring utilities.

To monitor and control this complex power delivery infrastructure, customized grid control systems have been designed and deployed. These control systems help support the grid by protecting key infrastructure, enabling remote switching, and tracking grid measurements. Unique performance and integration requirements have driven control system vendors toward the use of proprietary solutions that rely on embedded software. This approach has produced a wide range of different hardware and software solutions that require specialized tools and knowledge for configuration and maintenance.

Additionally, the system upgrade or replacement cycle is relatively long with utilities relying on control systems that may have been designed twenty or more years in the past. Within a single utility, the combination of proprietary devices installed at different times can be very challenging for those tasked with operating and maintaining the system.

In this complex control systems environment, utility personnel responsible for the Cyber Security of these systems are confronted with significant challenges. In addition to the range of technology in operation, utility processes and culture may preclude the use of conventional security measures. Each security control must be studied to balance the mitigation of cyber risks against negative operational impacts. EPRI's Cyber Security for Transmission and Distribution Task Force was launched in 2019 to facilitate utility collaboration and direct research to find optimal security solutions for securing transmission and distribution systems.

Within the task force, three individual domains have emerged during the roadmap development process. Each area has a distinct set of challenges and opportunities that will be explored through individual projects. The first domain is focused on both transmission and distribution control centers. At most utilities, system monitoring and control is performed from a small number of primary and backup facilities with connections to neighboring utilities.

The second domain is targeted at both transmission and distribution substations. Each utility will typically have a significant number of substations located around their service territory, and most will have the control systems protected with buildings and perimeter fencing. Finally, there are a large number of geographically dispersed control systems within pole-top cabinets or similar enclosures along the power line right-of-way. The field systems domain was developed to address Cyber Security needs of these assets.

Future States

- Transmission and Distribution control centers will be driven by evolving business models to adopt new processes and technology. These changes will force a reassessment of security controls and procedures that are applied in the control center environment
- Transmission and Distribution substations will continue to transition away from analog wiring towards digital communication systems to lower cost and increase reliability. This transition will expand the attack surface in the substation and will require new cyber security solutions
- As increasingly intelligent control systems are installed along transmission and distribution lines, new security approaches will be necessary to protect these dispersed assets and the communications systems they rely on for monitoring and coordination

The advisors for this task force should have expertise in one or more of the following areas:

- Power Transmission Control Systems
  - » Engineering
  - » Operations
  - » Maintenance
- Power Distribution Control Systems
  - » Engineering
  - » Operations
  - » Maintenance
- NERC CIP Compliance
  - » Transmission Substations
  - » Transmission Control Centers

Securing Grid Control Centers

Future State: Transmission and Distribution control centers will be driven by evolving business models to adopt new processes and technology. These changes will force a reassessment of security controls and procedures that are applied in the control center environment.

Description: Transmission and distribution control centers play a critical role in the safe and reliable operation of the power grid. These facilities host a wide range of applications used to make real-time operational decisions and execute control actions. Looking forward, system operations will need to adapt to the changing power delivery business model.

In addition to incorporating monitoring and control of customer and third-party energy systems, evolving regulatory requirements will heavily influence control center architecture and processes. In parallel, a number of technology advancements in the IT domain have provided utilities a transition path to a more modular environment using techniques like virtualization to abstract operations applications from the underlying infrastructure. While there are strong financial and system resiliency advantages that can be realized by virtualizing control center infrastructure, regulatory compliance and security will be a significant part of the overall strategy.

Action Plan: Securing Grid Control Centers

- Identify industry trends toward emerging technology
- Recognition of cost implications for researched solutions
- Researched solutions will consider NERC CIP Standards

Major Past Accomplishments	2020	2021	Future
• Distributed Network Protocol (DNP3) Secure Authentication v5: Facilitated development and interoperability testing. DNP3 Secure Authentication **3002010607** • Policy-Driven Cyber Security: Interpret and comply with CIP while maximizing efficiency	• Cyber Security Training for Grid Operators (Supplemental) • Distribution Operations Cyber Security Drill (Collaboration P200) • Emergency Control Center Network Isolation Technology and Processes • DNP Secure Authentication v6: Interoperability Plugfest (Supplemental) • Managed Security Services: How can it be leveraged in today's NERC CIP world • Super Encapsulating Security Payload (ESP): Integrating primary and backup control center capabilities	• DNP3 Secure Authentication: Vendor requirements and deployment best practices • Zero Trust Control Center Application Environment: Re-architecting SCADA network • Off-Prem SCADA Architecture Security: Pilot Implementation and Lessons Learned	• Emergency Control Center Network Isolation Technology and Processes • Find, Rip and Replace: Action steps to mitigate after a complete compromise

MEASURES OF SUCCESS

Utilities have the ability to easily implement secure Supervisory Control and Data Acquisition (SCADA) protocols and advanced security architectures in their control centers. SCADA operators have sufficient training and knowledge to recognize and respond to cyber incidents if they occur.

DELIVERABLE TYPE

Software, technical publications

ARP PROJECT

Cyber Security for PDU (P183)

TIES TO OTHER PROGRAMS

Transmission Operations (P39), Distribution Operations (P200)

Securing Substations

Future State: Transmission and Distribution substations will continue to transition away from analog wiring towards digital communication systems to lower cost and increase reliability. This transition will expand the attack surface in the substation and will require new cyber security solutions.

Description: Transmission and distribution substations provide a challenging environment for individuals tasked with managing cyber and compliance risk. Substation technology continues to trend away from physical configuration of individually wired contacts toward logical configuration defining digital data over protocol links. In the future, communication networks that are currently confined in the switch house will be extended out into the switch yard to replace existing analog wiring and instrument transformer circuits. This increase in device intelligence and communication capabilities will enable more flexible and resilient control systems, but the associated risk will require creative cyber security controls.

Additionally, existing challenges associated with the monitoring and management of proprietary embedded control systems will continue to provide obstacles to securing the substation. Since these systems are not general-purpose computing platforms, many of the traditional IT security approaches that rely on standard system interfaces will not be viable. Relatively long technology refresh cycles will require utilities to accommodate microprocessor-based systems that may have been developed over twenty years in the past. These substation characteristics will require a unique approach to security.

Action Plan:

- Identify industry trends toward emerging technology
- Assess security challenges and opportunities associated with emerging technology
- Explore security solutions that minimize cyber risk without negatively impacting operations

Major Past Accomplishments	2020	2021	Future
• Assessed passive fingerprinting and safe-active interrogation techniques for substation devices. Passive Identification of Substation Devices: Exploring Opportunities and Challenges **3002009417** • Explored options for automated asset tracking and configuration management. Automating Asset and Configuration Management **3002014136**	• Intelligent Electronic Devices (IED) Access Control and Management Approaches: Focused on existing IEDs • Timing Security Phase 2: Evaluate timing solutions for relevant vulnerabilities (supplemental)	• Leveraging device configuration data to customize security controls • Explore evolving communications requirements and emerging network technologies like Software Defined Network (SDN) as a layer 2 replacement • Develop a modular framework to interpret vendor configuration files and extract parameters relevant to security	• Security Solutions for Switchyard Systems: protecting the process bus without impacting operations • Perform a security assessment of the proposed centralized protection architecture

MEASURES OF SUCCESS

Utilities have tools and processes to secure digital substations, efficiently manage IEDs, and be resilient to timing security attacks

DELIVERABLE TYPE

Software, technical publications

ARP PROJECT

Cyber Security for PDU (P183)

TIES TO OTHER PROGRAMS

Substations (P37), Transmission Operations (P39), Distribution Operations (P200), Distribution Assets (P180)

Securing Field Systems

Future State: As increasingly intelligent control systems are installed along transmission and distribution lines, new security approaches will be necessary to protected these dispersed assets and the communications systems they rely on for monitoring and coordination.

Description: Utilities deploy a range of assets in the field beyond the substation fence. These systems may be located to support the efficient delivery of power through reactance control or enable line segmentation to isolate distributed generation or load. Typically, these systems are deployed in pole-mounted cabinets or enclosures at various points along the line. While the control system components are similar to those deployed within substations, field systems have unique security needs due to their geographic distribution and communication systems.

Additionally, the relative lack of physical protective measures at field sites may drive utilities to develop combined cyber-physical security controls that help mitigate the upstream risk from relatively accessible cabinets.

Action Plan: Securing Field Systems

- Identify risks and unique challenges associated with distributed field systems
- Explore technology and process solutions that address challenges and mitigate risks
- Test and document results to assist members in developing a comprehensive security strategy for field assets

Major Past Accomplishments	2020	2021	Future
• Serial to Packet Transition for Teleprotection Communication: Security and reliability of virtual circuits over Multi-Protocol Label Switching (MPLS) Serial to Packet Protection Workshop: Test Results **3002009783** • Open Field Message Bus (OpenFMB)	• Remote IED Management for Field Systems (Collaboration P180) • Field Management of Cyber and Physical Security for Distribution Automation (Collaboration P180) • Long Term Evolution (LTE) Security Assessment (Supplemental P161)	• Cloud Architecture for Distribution Systems • Security Solutions for Utility Managed LTE Networks • Spread-Spectrum Radio Security Assessment	• Spread-Spectrum Radio Security Assessment • Integrating Work Management Systems with Field Systems Security

MEASURES OF SUCCESS

Utilities have adopted EPRI-recommended approaches for improving the cyber and physical security of field systems. Cloud security architectures have reduced the risk of leveraging cloud services with distribution systems, leading to more widespread adoption.

DELIVERABLE TYPE

Software, technical publications

ARP PROJECT

Cyber Security for PDU (P183)

TIES TO OTHER PROGRAMS

Distribution Assets (P180), Distribution Operations (P200)

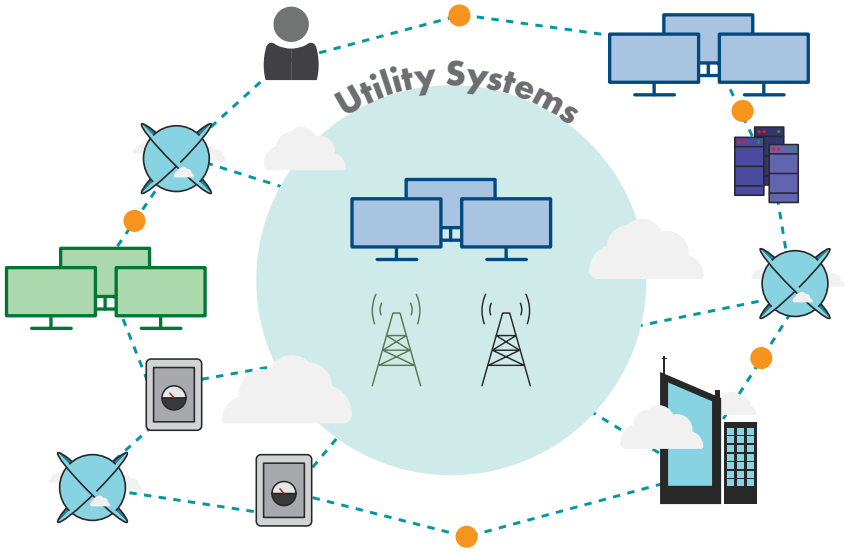
CYBER SECURITY FOR DISTRIBUTED ENERGY RESOURCES AND GRID-EDGE SYSTEMS

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

To organize the complex landscape of different technologies and associated risks effectively, the projects are categorized into 4 major research areas:

1. Secure DER (Distributed Energy Resource) Integration – The projects under this category cover the common technologies and infrastructures that support the secure integration of DER. Cyber security engineering concerns for smart inverters, communication protocols, telecommunications, crypto-key management, and embedded systems are investigated in the perspective of reliability and resiliency of the power distribution grid
2. Security Operations for DER – The projects under this category deals with the identification, protection, detection, response and recovery of utility assets related to DER, from the perspective of the utility security operations. The vulnerability and security patch management, threat detection, incident response, and information sharing are topics under this research area
3. DER Technology Application Area – This area covers the unique characteristics of different DERs in terms of cyber security. Cyber security concerns for solar energy, energy storage, microgrid, electric vehicle, and electric vehicle service equipment are investigated separately as well as their impact on the reliability and resiliency of the power system
4. Demand Response and Connected Loads – The projects under this area covers the cyber security concerns for devices, infrastructure, standards, communications used to manage the electricity demand. Considering advanced technologies and market development enabling large-scale aggregated controls on these systems, their impact on the reliability cannot be overlooked

In the next sections, the future states and EPRI's action plans for each of the four research areas are mapped out for a three-year horizon.



Taskforce for Cyber Security for Distributed Energy Resources and Grid-Edge Systems

Future State: Cyber security (CS) issues related to DER will be better understood by utilities and industry stakeholders intending to adopt and integrate these technologies to the grid. With this knowledge, utilities will be able to develop and implement effective cs threat detection and prevention strategies as industry standards are refined with more robust security requirements. Utilities will be able to update their incident response strategies to consider scenarios which stem from compromised DER assets and develop playbooks that require coordination with DER aggregators and owning customers. As more advanced use cases are developed by industry to optimize the management of DER, utilities will be able to consider inherent risks introduced by these apps and where security requirements are needed in standards, protocols, and architecture.

Description: CS requirements in current DER standards and interoperability protocols, such as IEEE 1547 and IEEE 2030.5, have known deficiencies. Despite this, high penetration of DER exists today and utilities must monitor and manage these new and rapidly expanding energy resources. Utilities are currently addressing risks by including cs requirements in their interconnection handbooks and focusing their attention to developing effective detective and responsive controls while security updates to DER standards are being drafted, debated, and released. New emerging players, including aggregators and DER-owning customers, will become significant players in the multi-party grid, and utilities will need to extend threat response strategies to consider roles and responsibilities of these third-parties for incident response planning and coordination.

Action Plan:

- Identifying and evaluating threat detection technologies for DER communication
- Initiating and facilitating collaborative discussions regarding information sharing among utilities and incident response plans for 3rd parties and customers
- Deepening the understanding of DERMS technology and determining cyber security requirements for threat detection capability and coordinated, multi-party incident response
- Following and contributing to industry efforts for the standardization of cyber security for DER, including revisions to the IEEE 1547 base standard to include secure communications natively to the smart inverter interface.

Gaps Addressed:

- Deficiencies in cyber security requirements in DER interoperability protocols, such as IEEE 2030.5, and DER standards, such as IEEE 1547.
- Lack of security reference architectures, requirements, and best practices to guide utilities on secure implementation of DER.
- Complexity and lack of defined roles and security responsibilities for incident response in a multi-party grid.

CYBER SECURITY FOR PDU ANNUAL RESEARCH PORTFOLIO (P183)

Major Past Accomplishments	2020	2021	Future
• EPRI Security Architecture for DER Integration Network • Security Architecture for Distribution Systems: Reference Architectures and Attack Modeling • Technology Innovatoin Program: Secure Cloud Reference Architecture for Real-Time Utility-Based Applications	• Incident Response and Information Sharing for DER & Grid Edge Systems • Cyber security assessment of IEEE 2030.5 for DER Integration • DER Utility Gateway Cyber Security Requirements (Supplemental, joint with P161, P174) • Smart Inverter Hardware Security Considerations (Technology Innovation) • Cloud Security Reference Architectures for DER and Grid Edge Systems	• EPRI Security Architecture for DER Integration with Utility Gateway • Security Monitoring and Threat Detection for DER and Grid Edge Systems • The Next Generation Secure DER Protocol Requirements • Public Key Infrastructure and Crypto-key Management for Secure DER Communication	• ISOC Integration of Grid Edge Systems • DER Testbed: IDS/IPS, SIEM, and Other Security Solutions • Vulnerability and Patch Management for DER and Grid Edge Systems

MEASURES OF SUCCESS

- Utilities leverage developed cyber security reference architectures and protection and detection strategies for DER
- Extension of utility incident response strategies and playbooks to DER applications and 3rd parties

DELIVERABLE TYPE

Industry Groups, Lab Demos, Technical Reports, Software, Reference Guides

ARP PROJECT

Cyber Security for PDU

TIES TO OTHER PROGRAMS

DER Integration (P174), Information Communication Technology (P161), Bulk Power System Integration of Variable Generation (P173)

DER Technology Application Area & Demand Response and Connected Loads

Future State: Utilities will better understand the cyber security risks and potential grid-impact scenarios associated with grid-edge technologies, including microgrids, demand response programs, battery storage, and electric vehicles (EVs). With insights into potential attack vectors and their implications to grid safety and reliability, utilities will be able to implement practical mitigation strategies and leverage secure architecture patterns specifically designed for grid-edge applications.

Description: New innovations and state government programs will continue to drive demand for emerging grid support technologies and services. These include microgrid for local grid resiliency, energy storage and demand response for load balancing, and electric vehicles (EVs) for state carbon-reduction initatives. Influx of these new technologies, many of which incorporate cloud services, and the slow-pace of cyber security adoption through industry standardization predict an increasing number of cyber incidents in the area of grid-edge technologies, if utilities do not adequately address cyber security as they adopt and integrate these applications. Utility incident response plans must be revisited and active industry discussions should include OEMs, aggregators, and customers to discuss standardization of cyber security requirements.

Action Plan:

- Continue the collaboration with the experts in the different technology areas to understand the attack vectors, risks and impacts of a cyber attack to grid-edge applications
- Collaboratively develop cyber security technical requirements with particular attention in minimizing attack vectors
- Understand the cyber security posture of major vendors who provide grid-edge technologies
- Review cyber security procurement language for grid-edge systems and incident response plans

Gaps Addressed:

- No established cyber security reference architectures specific to microgrids, demand response, electric vehicles and battery storage
- Lack of commonly accepted or defined cyber security controls and standards for grid-edge technologies

Major Past Accomplishments	2020	2021	Future
CYBER SECURITY FOR PDU ANNUAL RESEARCH PORTFOLIO (P183)			
• Cyber security Considerations for Distributed Energy Storage **3002016153** • Grid Security of Connected End-Use Devices **3002016154**	• Cyber security for Microgrid Integration • Cyber security Considerations for Building Management System (Technology Innovation) • Incident Response and Information Sharing for DER & Grid Edge Systems • Cloud Security Reference Architectures for DER and Grid Edge Systems	• Cyber Security Considerations for Electric Vehicle Service Equipment (EVSE) and V2G • Security Monitoring and Threat Detection for DER and Grid Edge Systems	• DER Testbed: IDS/IPS, Security Information and Event Management (SIEM), and Other Security Solutions • Vulnerability and Patch Management DER and Grid Edge Systems

MEASURES OF SUCCESS

- Utilities leverage developed cyber security reference architectures and protection and detection strategies for their implementations of microgrids, demand response programs, and management of electric vehicles and battery storage
- Extension of utility incident response strategies and playbooks consider grid-impact scenarios related to grid-edge technologies

DELIVERABLE TYPE

Industry Groups, Lab Demos, Technical Reports, Reference Guides

ARP PROJECT

Cyber Security for PDU (P183)

TIES TO OTHER PROGRAMS

Energy Storage and Distributed Generation (P94), End-Use Energy Efficiency and Demand Response (P170), Electric Transportation (P18), Information Communication Technology (P161)

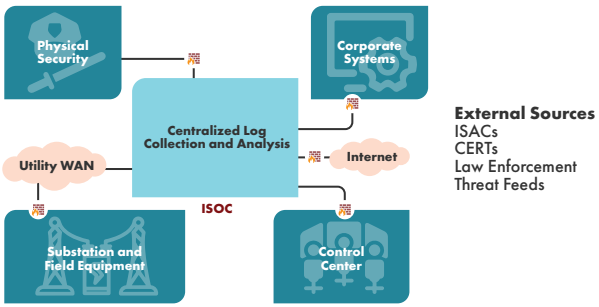
INCIDENT AND THREAT MANAGEMENT FOR POWER DELIVERY SYSTEMS

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

The task force consists of three research tracks:

- The Integrated Security Operations Center (ISOC)
- Threat Management
- Cyber Security Forensics for Industrial Control Systems (ICS)

An ISOC unifies the incident response functions, such as monitoring and detection, for the information technology (IT), operational technology (OT) and physical security (PS) environments. The ISOC track provides a comprehensive ISOC Guidebook, an EPRI ISOC lab, and a cyber-attack scenario library for utilities.



National ASOC Architecture

Cyber Kill Chain®

The ISOC serves five high-level functions:

1. Prevention of unauthorized activity
2. Monitoring, detection, and analysis of relevant security information in the environment to detect suspicious activity
3. Response and recovery procedures to mitigate threats and restore normal system operations
4. Situational awareness so that stakeholders and relevant constituents are informed about the system's current health and status
5. Security Operations Center (SOC) engineering to operate and maintain toolsets to perform SOC functions and develop new SOC capabilities

The ISOC can provide utilities with significant value including:

- Unified security incident management for both corporate and OT systems
- Optimization of security resources
- Improved threat analysis across utility domains
- Unified configuration and patch management
- More efficient forensics and root-cause analysis

The Threat Management research track seeks to identify how threat automation can be used to enhance cyber security programs that must protect ICS, SCADA, and OT equipment. The Security Orchestration Automation and Response (SOAR) framework is employed to help security teams respond to and manage the countless alarms coming into the ISOC at machine speeds. SOAR platforms enable organizations to implement sophisticated enrichments and responses by combining case management, data aggregation, workflow, and analytics. Orchestration can act as a force multiplier in an organization by making individual analysts capable of handling more incidents faster and more efficiently.

The Cyber Security Forensics for ICS research track seeks to 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 track includes guidebooks for forensic analysis, solutions for forensic data harvesting, and the leadership and management for the EPRI ICS Forensics Working Group.

The future states and corresponding projects for the task force and the research tasks are listed and described on the following pages.

Incident Detection

Future States: 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
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

CYBER SECURITY FOR PDU ANNUAL PORTFOLIO (P183)

Major Past Accomplishments	2020	2021	Future
• 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 delivery systems • Integrated Threat Analysis Framework (ITAF) framework and utility testing	• ISOC Guidebook update • Develop framework for cyber security attack scenario library • Build an ISOC in the Cyber Security Research Lab	• ISOC Guidebook Update • Develop cyber security attack scenario library for the transmission and distribution domains • Provide strategies to improve the economics for storage of large cyber security data sets used in incident monitoring and detection • Utilizing apply artificial intelligence and machine-learning technology to the ISOC for incident management • Data analytics for incident management; utilizing use cases and determining trends for machine-learning	• ISOC Guidebook Update • Develop cyber security attack scenario library for the transmission and distribution domains • Apply artificial intelligence and machine-learning • Provide strategies to improve the economics for storage of large cyber security data sets used in incident monitoring and detection

Power Delivery Cyber Security for PDU Annual Research Portfolio (P183)

Major Past Accomplishments	2020	2021	Future
CYBER SECURITY FOR POWER DELIVERY SUPPLEMENTAL PROJECT – INTRUSION DETECTION/PREVENTION SYSTEMS (IDS/IPS) SOLUTIONS ANALYSIS AND TESTING FOR ICS ENVIRONMENTS (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 delivery systems • ITAF framework and utility testing • ISOC Guidebook Version 2 • Developed framework for cyber security attack scenario library • Built the ISOC Lab as part of the Cyber Security Research Lab	• ISOC Guidebook Version 3 • Develop cyber security attack scenario library for the transmission and distribution domains • Provide strategies to improve the economics for storage of large cyber security data sets used in incident monitoring and detection	• ISOC Guidebook Version 4 • Utilizing apply artificial intelligence and machine-learning technology to the ISOC for incident management • Data analytics for incident management; utilizing use cases and determining trends for machine-learning	• ISOC Guidebook Update • Develop cyber security attack scenario library for the transmission and distribution domains • Apply artificial intelligence and machine-learning • Provide strategies to Improve the economics for storage of large cyber security data sets used in incident monitoring and 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 delivery 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

Cyber Security for PDU (P183)

TIES TO OTHER PROGRAMS

Substations (P37), Distribution (P180), Integration of DER (P174), Instrumentation & Control and Automation (P68), Operations (P108), Cyber Security for Generation (P209)

Threat Management

Future States: 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 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

- 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
- Create the capabilities to discover vulnerabilities in a utility ICS environment
- Develop a guidebook for developing an insider threat management program

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

CYBER SECURITY FOR PDU ANNUAL PORTFOLIO (P183)

Major Past Accomplishments	2020	2021	Future
• Investigated and contributed to OT Threat Modeling Language tools for OT systems • Guidelines for threat hunting techniques for OT systems • Four successful Birds of a Feather Threat Management Workshops • Guidelines for integrating threat intelligence feeds for protecting OT systems • Threat Automation Playbooks	• Threat Automation Playbooks	• Develop automated response to threat intelligence for OT systems • Develop strategies, tools, and processes for an insider threat management program for utilities	• Pilot testing of automated threat response system • Develop strategies, tools, and processes for an insider threat management program for utilities

Threat Management

Major Past Accomplishments	2020	2021	Future
CYBER SECURITY FOR PDU 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 ongoing training to utility members • Provide ongoing discovery of advanced vulnerabilities in utility focus	• Provide ongoing training to utility members • Provide ongoing 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

Cyber Security for PDU (P183)

TIES TO OTHER PROGRAMS

Substations (P37), Distribution (P180)

Cyber Security Forensics for Industrial Control Systems

Future State: 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
- Automate the process of ICS forensic harvesting
- Develop prototype tools for automated harvesting of ICS forensic artifacts
- Collaborate with ICS device vendors to improve the ability to harvest and preserve forensic artifacts through automation and capabilities embedded in the devices.
- 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	2020	2021	Future
CYBER SECURITY FOR PDU ANNUAL PORTFOLIO (P183)			
• Guidelines for an ICS Forensics Program • ICS Forensics Working Group	• ICS Forensics Field Guides • ICS Forensics Working Group • Power Delivery Forensics Tabletop Testing and Drills Methodology	• ICS Forensics Field Guides • ICS Forensics Working Group	• Automated ICS Forensic Artifact Harvesting

MEASURES OF SUCCESS

ICS forensics capabilities are available and utilized for power delivery systems

DELIVERABLE TYPE

Investigative results, working group

ARP PROJECT

Cyber Security for PDU (P183)

TIES TO OTHER PROGRAMS

Substations (P37), Distribution (P180), Instrumentation & Control and Automation (P68), Instrumentation & Control (P41), Cyber Security for Generation (P209)

CYBER SECURITY FOR THE GENERATION SECTOR

Industrial control systems used in generation plants (fossil, renewable, and equipment that can impact overall generation) are designed to safely and reliably operate equipment to produce energy and deliver it to the grid. The Generation Cyber Security Program uses a defense-in-depth, best practices approach to cyber security risk reduction for the generation fleet.

Generation control systems, communications equipment, instrumentation, and sensors that are used in fossil generation, renewable plants, and ancillary dependent utilities (interdependencies) have been targeted by sophisticated threat actors for exploitation. For example, the 2017 TRISIS attack showed that adversaries are willing to target dedicated safety instrumented systems that are also used in generation plants. Other threat actors have developed exploits and compromised other controls equipment. As the threat landscape continues to evolve, threat actors continue to grow in sophistication, understanding and using new tactics, tools, and procedures. The generation sector will need to implement best practices to ensure less sensitivity to the changing threat landscape and reduce the overall risk of a cyber compromise.

Meanwhile, the risk associated with a cyber compromise continues to grow. Risk is the product of the likelihood of a cyber compromise and the consequence of a cyber attack. A cyber attack doesn't need to be successful to have a consequence. Overall, however, the consequences of a cyber attack have been steadily increasing. Utilities are no longer able to keep cyber breaches confidential.

A cyber compromise can have internal and external consequences from changes in internal leadership structure, decreased consumer confidence, shareholder implications, credit or insurance ratings changes, equipment damage, to even employee or public safety implications.

Distributed Control Systems (DCS) equipment manufacturers and utilities are installing and using more digital equipment within generation plants. This equipment, if not properly engineered, architected, installed, and configured could open additional attack surfaces that adversaries can exploit. This is especially true as a lot of equipment is not developed as secure by design. As vendors, supplier, and engineers are implementing new digital equipment, sound engineering approaches and best practices should be used to evaluate vulnerabilities and allocate security controls that are appropriate. These security controls must be studied to balance the mitigation of cyber risks against negative operational impacts.

Utilities are being confronted with significant fleetwide challenges across the sector on reducing costs, increasing efficiency, becoming more flexible, mitigating a transitioning workforce, and navigating a changing regulatory cycle. The generation cyber security program is researching best practices to ensure that cyber security is an enabler to address the challenges that utilities are facing today and to be better equipped to be less sensitive to the changes and challenges of tomorrow.

Future States

- Generation utilities are building capability and maturity to reduce overall cyber risk by protecting, detecting, and responding and recovering from a cyber compromise. The capability and maturity will require the adoption of best practices that are applied in the OT environment
- As adversaries continue to increase in sophistication and target generation sector equipment, utilities will continue to reduce the sensitivity to a changing threat landscape by employing new, emerging technologies, increasing overall cyber security implementation maturity, and implementing effective cyber security controls
- As increasingly intelligent control systems are installed in the generation OT environment, new security approaches will be necessary to protect these assets to ensure this will not expand the attack surface
- Generation utilities will continue to work with IT and OT organizations to integrate cyber security practices, roles, and responsibilities to ensure that the entire fleet is able to meet the economic, workforce, and regulatory challenges of the future

The typical advisor has experience in one or more of the following areas:

- Generation OT Control Systems
  - » Engineering
  - » Operations
  - » Maintenance
- OT Cyber Security
- NERC CIP Compliance

Cyber Security Process and Integration for Generation Facilities

Future State: 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: Reference Architectures
EPRI will work with members and utilities to understand the synergies that exist between cyber security programs, practices, procedures, and interdependencies with other utility 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 a 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)

GENERATION CYBER SECURITY ANNUAL RESEARCH PORTFOLIO (P209)

Major Past Accomplishments	2020	2021	Future
• Technical Assessment Methodology – Case Study **3002015337** • Utilizing Reference Architectures for Securing Power Generation Facilities **300201544** • Connected Component Reference Architectures: Securing Connected Components in Power Generation **3002011542**	• Generation cyber security program and integration guide • Asset and configuration management field guide • Asset identification and configuration tools analysis	• Design engineer – secure by design • Generation workforce needs • Cyber risk management guidance, techniques, and tools • Securing specific renewable technologies • Supply chain and procurement specifications • Vendor qualifications • Workforce development • Internal audit review	• Cyber risk management guidance, techniques, and tools • Securing specific renewable technologies • Supply chain and procurement specifications • Vendor qualifications • Workforce development • Internal audit review • Managed services • Self-assessment tool • Receipt inspection and warehousing – cyber security best practices

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

P209 (2020)

TIES TO OTHER PROGRAMS

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

Protective Measures for Generation Industrial Control Systems

Future State: 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 integration with legacy existing equipment to provide protective functions against cyber attacks

GENERATION CYBER SECURITY ANNUAL RESEARCH PORTFOLIO (P209)

Major Past Accomplishments	2020	2021	Future
• Hardening Field Guides **3002017094**, **3002017095** • Advanced Vulnerability Grading Tool **3002015336** • Interactive Remote Access Guidance **3002011541** • Digital Instrumentation and Control (I&C) Configuration Management and Hardening Guideline **3002011904** • Patch Management Guideline **3002011187** • Access Control and Permission Management Guideline **3002014368**	• Hardening field guides • Advanced vulnerability grading tool	• Integration of physical and cyber security • Using and protecting Real-Time Operating System (RTOS) • Network segmentation best practices • Identity management and governance	• Integration of Physical and Cyber Security • Securing non-DCS Assets • Advanced boundary devices and architectures • Cryptography best practices and use Cases • Cloud based industrial controls • Application white listing • Using advanced security techniques in virtualization • Secure wireless

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

P209 (2020)

TIES TO OTHER PROGRAMS

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

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 generation systems through innovative monitoring solutions.

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 Monitoring and Diagnostics (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 CYBER SECURITY ANNUAL RESEARCH PORTFOLIO (P209)

Major Past Accomplishments	2020	2021	Future
• Real-time detection in Power Generation: Overview of Current State of Technology **3002011543** • Control System Protocols and Scanning Guideline **3002014369** • Security Event Monitoring Guideline **3002014367** • ISOC + M&D Integration Whitepaper **3002014509** • Incident Discovery and Classification Field Guide **3002015261**	• Data analytics, incident detection and integration with M&D • Cyber-physical tamper indication overview	• Securing DCS and generation control system protocols • Integrated Event Monitoring Frameworks (ISOC) • Network discovery and visualization • Data Analytics, incident detection and integration with M&D	• Securing DCS and generation control system protocols • Detection and correlation across different OT • Data analytics, incident detection and integration with M&D • Event collection and analysis tools • Automated threat modeling tools

DELIVERABLE TYPE

Technical updates, investigative results, working group

ARP PROJECT

P209 (2020)

TIES TO OTHER PROGRAMS

Cyber Security for PDU (P183), 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 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 CYBER SECURITY ANNUAL RESEARCH PORTFOLIO (P209)

Major Past Accomplishments	2020	2021	Future
• Coordination with the technical assessment methodology • Changing threat landscape study **3002015259**	• Coordination with the technical assessment methodology • Indicators of compromise guideline • Renewables cyber landscape whitepaper	• Coordination with the technical assessment methodology • Threat information sharing and collaboration • Defense-in-depth holistic protection measures	• Coordination with the technical assessment methodology • Threat information sharing and collaboration • Defense-in-depth holistic protection measures • Technologies and services for threat discovery/ mitigation • Distilling internal and 3rd party information • Indicator development techniques, technologies, and standards • Threat hunting in generation – advanced skills training

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 and 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

P209 (2020)

TIES TO OTHER PROGRAMS

Cyber Security for PDU (P183), Instrumentation & Control and Automation (P68)

Respond & Recover Capabilities for Generation Facilities

Future State: 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.

Action Plan:

- 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

Gaps Addressed: Lack of detailed scenarios and technical guidance to support efficient response and recovery functions for plants.

Major Past Accomplishments	2020	2021	Future
GENERATION CYBER SECURITY ANNUAL RESEARCH PORTFOLIO (P209)			
Incident Response Guideline **3002014147** (Generation)	Backup and restore best practices	• Generation testing and drills guidance • Generation cyber incident scenarios • Plant response functions integration into Corporate ISOCs	• Generation testing and drills guidance • Generation cyber incident scenarios • Plant response functions integration into Corporate ISOCs • Forensics in DCS incident response • Playbook development • Response and recovery integration into disaster recovery operations • External support and intelligence

MEASURES OF SUCCESS

- Incident management solutions and processes are available and utilized for generation facilities
- 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

P209 (2020)

TIES TO OTHER PROGRAMS

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

CYBER SECURITY FOR THE NUCLEAR SECTOR

A significant amount of work has been performed by the nuclear industry to protect their facilities from cyber-attack. Regulatory agencies and nuclear facilities across the world are under increasing scrutiny to ensure that critical infrastructure is protected, and public needs are met. International and US regulations to date have been similar in their approach.

Digital I&C hazards, such as common cause failures, electrical magnetic interference, cyber security concerns, etc., must have efficient, technically sound, cost effective, risk informed engineering processes that allows a user to come to a consistent resolution for implementation and long-term operability.

Nuclear Cyber Security Program cost has a nexus with overall O&M cost reductions and has become its own imperative. EPRI is working with international organizations like the International Atomic Energy Agency (IAEA) and reaching out to our international members to ensure that efficient and effective cyber security engineering methodologies are developed to help the global nuclear industry.

Drivers

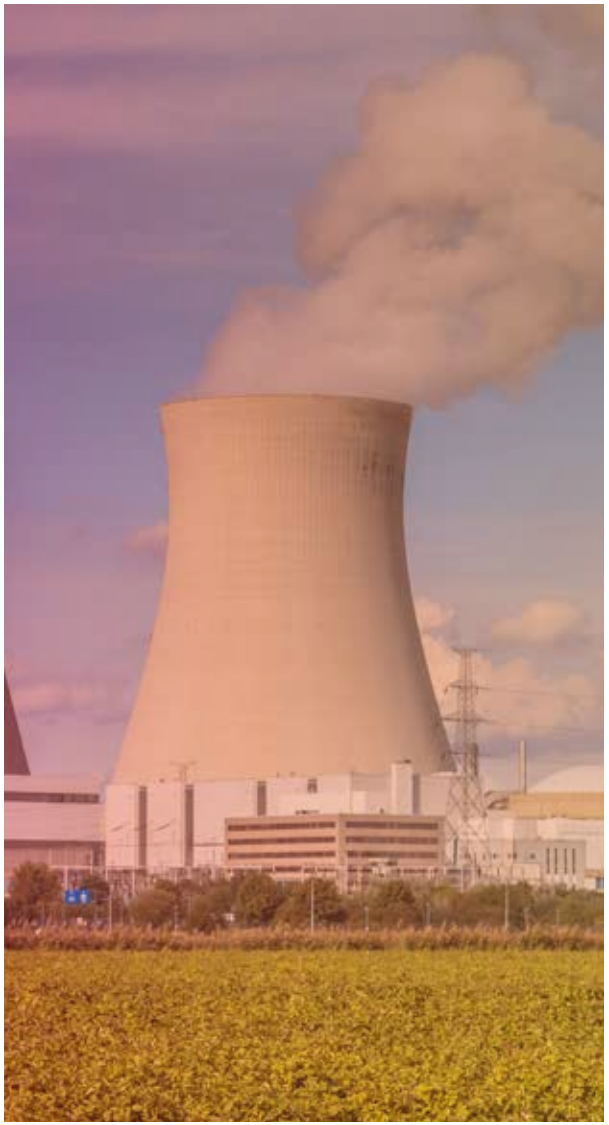
Securing a nuclear power facility effectively and at reasonable costs requires the integration of processes and technologies that establish what should be done vs. what can be done. Reducing the cost to implement and sustain Nuclear Cyber Security Programs while ensuring that nuclear safety and operational goals are met is paramount to sustain and reinvigorate the nuclear industry.

Barriers

The US Nuclear Industry has reported that it has spent over $1.2B on establishing their regulatory driven cyber security programs. These escalating costs are being driven by the requirement to evaluate thousands of components within each plant and assess hundreds of cyber security controls based on the ability of the control to be implemented for each of those devices. This assessment is independent of plant impact or any measurable security benefit. The industry needs to enable the secure expansion of communications and integration capabilities of digital technologies. The international nuclear industry is also facing similar challenges, particularly relating to regulatory uncertainty and lack of strong technical basis and methodologies to help deal with digital I&C hazards, such as cyber security.

Opportunities

As the supply chain continues to mature with digital technologies, it is imperative that the nuclear industry take advantage of the benefits that digital technologies can provide to the industry while maximizing value, reducing costs, improving reliability, and gaining efficiencies.



Hazard Consequence Analysis for Digital Systems (HAZCADS)

Future State: Utilities have tools that allow for understanding the impact hazards that are unique to digital hazards such as Electromagnetic Interference (EMI)/ Radio-Frequency Interference (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 Probabilistic Risk Assessment (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. System-Theoretic Accident Model and Processes (STAMP), System-Theoretic Process Analysis (STPA), and Fault Tree Analysis (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.

EPRI TECHNOLOGY INNOVATION CROSS-CUTTING CYBER SECURITY PROGRAM

Major Past Accomplishments	2020	2021	Future
• Hazard Analysis Methods for Digital Instrumentation and Control Systems **3002000509** • Program on Technology Innovation: Cyber Hazards Analysis Risk Methodology – Phase II: A Risk Informed Approach **3002004997** • HAZCADS: Hazards and Consequences Analysis for Digital Systems **3002012755** • HAZCAD Case Studies for Common-cause Failure (CCF) and Cyber Security	• HAZCAD technology transfer • HAZCADS: hazards and consequences analysis for digital systems, revision 1 • HAZCAD topical guides • HAZCAD integration with risk assessment software tool • HAZCAD software tool training development • HAZCAD classroom/ distance learning environment (DLE) training	• HAZCAD technology transfer • HAZCAD topical guides • HAZCAD Integration with other digital hazard research such as single point vulnerability (SPV), EMI/RFI • HAZCAD training	• HAZCAD integration with other digital hazard research such as SPV, EMI/RFI • HAZCAD topical 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

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 State: Utilities have a regulatory agnostic, technically sound, risk informed and performance-based framework for implementing a cyber security program. This 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	2020	2021	Future
NUCLEAR INSTRUMENTATION AND CONTROL PROGRAM ANNUAL RESEARCH PORTFOLIO (P41.05.03)			
Cyber Security Program Guide for Nuclear Facilities **3002012754**	Cyber Security Program Guide Phase II	Cyber Security Program Guide Technology 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

None

CROSS-CUTTING FUTURE STATES

This section focuses on security challenges that affect multiple operations domains, such as developing effective security metrics for the electric sector, leveraging risk-informed processes to assess systems, service, and assets, and creating common supply chain security templates, processes, and technologies.

Future States

- Cyber Security Metrics for the Electric Sector
  - » As cyber security threats continue to grow in number and sophistication, utilities will need to evaluate and improve their security postures continuously. This 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.
- Technical Assessment Methodology
  - » 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.
- Cyber Security in the Supply Chain
  - » The supply chain 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
  - » Comingling of target asset cyber security requirements with supply chain integrity requirements
  - » Lack of visibility into lower tier suppliers and processes

Cyber Security Metrics for the Electric Sector

Future State: 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 have tools, process and people to run metrics program as a part of security operation.

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 aims to create a common set of metrics that quantify the effectiveness of cyber security controls, and thus enable utilities to set the security target for the continuous improvement. In order to avoid human bias and to enable automation, metrics are calculated using the data collected from the systems. A utility can sub-divide their systems and calculate metrics by business units, IT versus OT, or geographical units for internal benchmarking and 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. To realize the full value of the study, the metrics must be:

1. Widely adopted
2. Aggregated for statistical analysis across the industry
3. Correlated with the threat/breach data for advanced analytics

As the first step to address the gaps, EPRI developed a commercial grade security metrics tool for automated data collection, drill-down metric score analysis, and dashboard reporting. A supplemental project was launched where EPRI implements the security metrics tool in a utility's environment. In 2020, EPRI will continue the operationalization of security metrics through the supplemental project.

In parallel to this effort, EPRI will organize an international metrics advisory council (MAC) to spearhead the standardization of the metrics through vendor engagements.

Gaps Addressed:

- The lack of common set metrics for leadership to communicate the security status to stakeholders
- The lack of performance metrics 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

EPRI TECHNOLOGY INNOVATION CROSS-CUTTING CYBER SECURITY PROGRAM

Major Past Accomplishments	2020	2021	Future
• EPRI Cyber Security Metrics for the Electric Sector **3002010426** • Metrics Calculator (OpenMetCalc) public release **3002013691** • Executive Briefing: EPRI Cyber Security Metrics – A Continuous Process Driving Decisions to Reduce Risk **3002017501**	• Operation-alization of security metrics through the supplemental project **3002016796** • Establish Metrics Advisory Council (MAC) for ongoing enhancement of the metrics • Engage vendors and industry partners	• Operation-alization of security metrics through the supplemental project (continued) • Metrics Operation-alization Guidebook • International expansion of Metrics Advisory Council (MAC)	• Security Metrics Standardization • Public release of Metrics Hub (Cloud-based Metrics Calculator) • Industry statistics and data analytics of metrics

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

TIES TO OTHER PROGRAMS

None

Technical Assessment Methodology

Future State: 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 topical guides as needed
- Develop training materials to reduce skill gaps, and improve technology transfer for the overall workforce

EPRI TECHNOLOGY INNOVATION CROSS-CUTTING CYBER SECURITY PROGRAM

Major Past Accomplishments	2020	2021	Future
• Cyber Security Technical Assessment Methodology, Rev 1 **3002012752** • TAM Overview Computer based training (CBT) (Module 1) **3002016907** • DCS Domain Controller Cybersecurity Data Science (CSDS) Topical Guide **3002015759** • Risk Informed Target Level Topical Guide **3002015760** • Cyber Security Baseline Configuration Topical Guide **3002015794** • Exploit Sequence Identification and Mitigation (EXSIM) Database Software Tool **3002015737**	• Technical Assessment Methodology (TAM) Technology Transfer Workshops • TAM Topical TGuides • TAM Classroom Training on EPRI U • Additional TAM CBT Modules • Developing the installed configuration and data flow topical guide	• TAM Topical Guides • TAM Implementation • TAM Training via EPRI U • TAM Revision 2	• TAM Revision 2 • TAM Training via EPRI U

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, topical guides, training deliverables including CBT modules

ARP PROJECT

Technology Innovation Project with programs (P41, P209, and P183)

TIES TO OTHER PROGRAMS

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

Cyber Security in the Supply Chain

Future State: Utilities have the capability to leverage a common supply chain security and procurement templates, process and technologies 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 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, comingling 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
Developing a centralized clearinghouse of information regarding industry supply chain practices, standards and effective approaches will be the central focal point of EPRI's research activities for the near future. Through coordination with various stakeholder groups such as the NERC technical committees, North American Transmission Forum, Edison Electric Institute and other key forums, EPRI is developing a series of research solutions that can be immediately used to help inform, manage and coordinate suppliers and buyers within the electric grid community.

The central platform that will be the catalyst for this capability will be EPRI's Supply Chain Security Information Exchange (Hub). The Hub will be a central repository for industry's best practices, EPRI's Technical Assessment Methodology related approaches and secure access system that hosts supplier information about the security capabilities of the company's and products.

Gaps Addressed:
The lack of techniques and centralized accessible information to address potential security vulnerabilities in the supply chain.

Major Past Accomplishments	2020	2021	Future
EPRI TECHNOLOGY INNOVATION CROSS-CUTTING CYBER SECURITY PROGRAM			
• Cyber Security Procurement Methodology for Power Delivery Systems **1026562** • Cyber Security Procurement Methodology, Rev 2 **3002012753** • Secure Development, Integration, and Delivery (SDID) Audit Topical Guide **3002015793** • Supply Chain CBT Modules, Classroom, Distance Learning Environment (DLE) Training	• EPRI's Supply Chain Security Information Exchange (Hub) Beta/Full Release • Supply Chain Technology Transfer • Supply Chain Case Studies for all sectors (Generation, Nuclear, PDU) • Supply Chain Topical Guides • Supply Chain CBT Modules, Classroom, Distance Learning Environment (DLE) Training • Establishing Cyber Security Division of Responsibility Topical Guide	• EPRI's Supply Chain Security Information Exchange (Hub) Version 2.0 • Buyer support modules for Asset and Configuration Management interfaces • Supply Chain Technology Transfer • Supply Chain Topical Guides	• EPRI's Supply Chain Security Information Exchange (Hub) Version 3.0 • Vendor Qualifications and Certification Process Automation • Digital Procurement Methodology Rev. 3 • Receipt inspections and warehousing for generation facilities

MEASURES OF SUCCESS

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

DELIVERABLE TYPE

Web portal, technical reports, member updates, training deliverables including CBT modules

ARP PROJECT

Technology Innovation Project with programs (P41, P209, and P183)

TIES TO OTHER PROGRAMS

P41.05.03 Nuclear Instrumentation and Control, P41.08.01 Advanced Nuclear Technology, Cyber Security for PDU (P183), P209 GEN – Cyber Security (2020)

Glossary and Acronym Definitions

C

CBT: Computer Based Training
CCF: Common-cause Failure
CERT: Computer Emergency Response Team
CS: Cyber Security
CSDS: Cybersecurity Data Science
Cyber Kill Chain: A kill chain is used to describe the various stages of a cyberattack as it pertains to network security. The actual steps in a kill chain trace the typical stages of a cyberattack from early reconnaissance to completion where the intruder achieves the cyber intrusion.

D

DCS: Distributed Control Systems
DER: Distributed Energy Resources
DLE: Distance Learning Environment
DNP3: Distributed Network Protocol
DR: Demand Response
DRAS: Demand Response Automation Server
DRMS: Demand Response Management System

E

EMI/RFI: Electromagnetic Interference (EMI)/Radio-Frequency Interference (RFI)
EPRI: Electric Power Research Institute
ESP: Encapsulating Security Payload
EVSE: Electric Vehicle Service Equipment
EXIM: Exploit Sequence Identification and Mitigation

F

FTA: Fault Tree Analysis

H

Hub: EPRI's Supply Chain Security Information Exchange

I

IAEA: International Atomic Energy Agency
ICS: Industrial control systems environment or Cyber Security Forensics for Industrial Control Systems
IDS: Intrusion Detection System
I&C: Instrumentation and Control
IEC: International Electrotechnical Commission
IEDs: Intelligent Electronic Devices
IPS: Intrusion Protection System
ISAC: Information Sharing and Analysis Center
ISOC: Integrated Security Operations Center
IT: Information Technology
ITAF: Integrated Threat Analysis Framework

L

LTE: Long Term Evolution

M

MAC: Metrics advisory council
M&D: Monitoring and Diagnostics
MPLS: Multi-Protocol Label Switching

N

NERC CIP: The NERC CIP (North American Electric Reliability Corporation critical infrastructure protection) plan is a set of requirements designed to secure the assets required for operating North America's bulk electric system.

O

OEM: Original Equipment Manufacturer
OpenFMB: Open Field Message Box
OT: Operational Technology

P

PDU: Power Delivery Utilization
PRA: Probabilistic Risk Assessment

Q

QoS: Quality of service

R

RTOS: Real-time Operating System

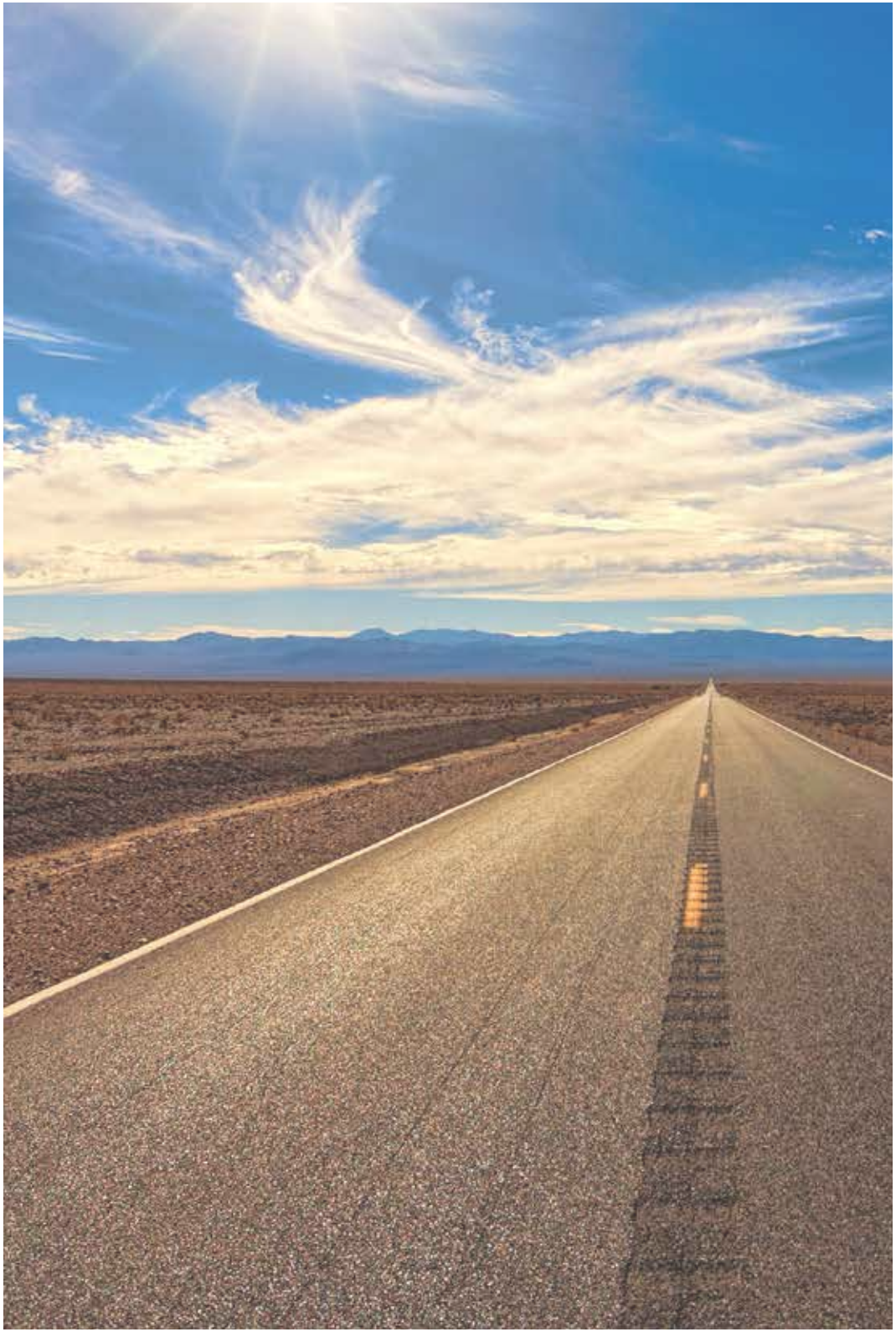
S

SCADA: Supervisory control and data acquisition
SCRAM: Security, cyber, risk assessment methodology
SDN: Software Defined Network
SDID: Secure Development, Integration, and Delivery
SIEM: Security Information and Event Management
SME: Subject Matter Expert
SOAR: Security Orchestration Automation and Response
SOC: Security Operations Center
SPN: Supplemental Opportunity
SPV: Single Point Vulnerability
STAMP: System-Theoretic Accident Model and Processes
STPA: Systems Theoretic Process Analysis

T

TAM: Technical Assessment Methodology
TRISIS: the fifth ever publicly known ICS-tailored malware following STUXNET, HAVEX, BLACKENERGY2, and CRASHOVERRIDE. It is the first ever publicly known ICS-tailored malware to target safety instrumented systems.
TI: Technology Innovations


EPRI
ELECTRIC POWER
RESEARCH INSTITUTE



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

3002017884

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 the Information, Communication, and Cyber Security Technical Advisors.
West: Annette Mosley, 972.556.6507, AMosley@epri.com
East: Chris Kotting, 980.219.0146, ckotting@epri.com