EPRI

2024 TECHNICAL UPDATE

Cyber Security Newsletter Compendium

2024 Update

Cyber Security Newsletter Compendium

2024 Update

3002030015

Technical Update, November 2024

EPRI Project Manager
Ben Sooter

EPRI
3420 Hillview Avenue, Palo Alto, California 94304-1338 USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE FOLLOWING ORGANIZATION(S), UNDER CONTRACT TO EPRI, PREPARED THIS REPORT:

EPRI PREPARED THIS REPORT.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

Together…Shaping the Future of Energy®

ACKNOWLEDGMENTS

The following organizations, under contract to EPRI, prepared this report:

EPRI prepared this report.

Principal Investigator
Ben Sooter

This report describes research sponsored by EPRI.

This publication is a corporate document that should be cited in the literature in the following manner: *Cyber Security Newsletter Compendium: 2024 Update.* EPRI, Palo Alto, CA: 2024. 3002030015.

ABSTRACT

The EPRI Cyber Security Program provides monthly updates to utilities on cyber security activities and events that are impacting the electric sector. The goal is to cover the activities of industry groups, government organizations, regulatory bodies, and research groups from around the world. This document provides highlights from these monthly updates.

Keywords

Cyber security
Industry updates
Newsletter

CONTENTS

LIST OF FIGURES

1 INTRODUCTION

A wide range of industry groups and public-private partnerships have emerged to address the growing need for enhanced security within the electric sector. These collaborations aim to establish new security standards and develop cutting-edge technologies tailored to protect critical infrastructure. While these initiatives target specific challenges in the industry, two significant obstacles persist.

Firstly, due to limited availability, utility personnel often cannot fully engage with all of these efforts. As a result, utilities may be less informed about evolving security requirements or technological advancements that could affect their operations. This knowledge gap can hinder timely adaptation to emerging threats and compliance with new standards.

Secondly, manufacturers of security solutions may lack direct insight from electric utility stakeholders. Without consistent input from those working within the sector, security technologies may not fully align with the unique operational needs and vulnerabilities of electric utilities. This disconnect risks the development of products that are less effective or impractical for real-world application.

To bridge these gaps, the Electric Power Research Institute's (EPRI) Strategic Intelligence and Emerging Issues project played a crucial role. It delivered monthly email briefings to Cyber Security Program members, summarizing key developments in industry activities, emerging threats, and the status of EPRI's ongoing research projects. This report serves as a comprehensive highlight of those monthly updates, offering a clear overview of the latest trends and insights impacting cyber security in the electric sector.

2 INDUSTRY UPDATE HIGHLIGHTS

P183 Updates and Opportunities (January Update)

The January 2024 EPRI Cyber Security Program newsletter includes updates on upcoming events such as the Winter and Fall 2024 Energy Delivery & Customer Solutions Advisory meetings, with details on dates, locations, and registration. It announces the availability of the 2023 P183 Technology Transfer Workshop materials and a list of 2023 deliverables for members. The newsletter also highlights industry events like Distributech 2024 and Electrification 2024, providing essential information for attendees and members interested in the electric sector's cyber security initiatives.

2023 P183 Deliverables List

A PDF list of all currently available 2023 P183 deliverables is now downloadable through this Box link. The deliverables are also linked on the P183 Member Center. EPRI members will need to log into the website with their user account and be a member of the deliverable's funding utility to be able to view the materials.

Meeting Materials Available: 2023 P183 Technology Transfer Workshop

There are two ways to insert figure captions.

The presentations and recordings from the 2023 P183 Technology Transfer Workshop held on December 5th-7th are now available on the P183 program page. EPRI members will need to log into the website with their user account to be able to view the materials (under Attachments).

Red Team Collaboration and Winter Advisory (February Update)

The February 2024 EPRI Cyber Security Program newsletter highlights key upcoming events, including webcasts and workshops, such as the Red Team Collaborative Working Group and Birds of a Feather Threat Management Workshop. It also provides updates on research projects and program documentation for 2024, including the annual research portfolio and ICCS Area Review. The newsletter outlines the agenda for the EPRI Winter 2024 Energy Delivery & Customer Solutions Advisory, focusing on cyber security sessions and strategic planning for future grid challenges.

Red Team Collaboration

In the ever-evolving realm of cyber threats, electric utilities find themselves at the crossroads of technological advancement and increasing vulnerabilities. The proliferation of smart grids, the adoption of renewable energy sources, and the integration of storage solutions, while ushering in an era of energy efficiency and sustainability, also present an expanded cyber-attack surface. What's more, as cyber adversaries recognize the critical nature of utility services, these vital

infrastructures are witnessing an unprecedented surge in targeted attacks, with potential ramifications ranging from financial setbacks to widespread power outages.

Recent global events underline the emphasis adversaries are placing on critical infrastructure. The alarming rise in attacks underscores the need for electric utilities to bolster their cyber defenses. While the industry continues its strides in prevention, a parallel focus on efficient and informed response mechanisms to potential breaches is indispensable. This project aims to leverage a Red Team Collaborative approach to provide read team services to the electric industry. By simulating genuine cyber threats in a controlled environment, these assessments will provide utilities with an unparalleled perspective into their existing vulnerabilities, response mechanisms, and recovery protocols.

The Red Team Collaborative's projects goals are twofold: firstly, to enhance the cyber resilience of electric utilities by identifying and addressing latent vulnerabilities; and secondly, to delineate and promote industry best practices that encompass both preventive measures and responsive strategies.

Benefits

With the rapidly changing threat landscape, the Red Team Collaborative provides a proactive defense for electric utilities. By marrying technological innovation with rigorous cybersecurity testing, this project aims to provide:

- Realistic Understanding through Simulated Threats: We don't just tell you about potential threats; we help facilitate simulated real-world attacks to pinpoint vulnerabilities, offering a tangible assessment that goes beyond theory.
- Robust Defense Mechanism Evaluation: The project is not designed to just identify vulnerabilities; it's also about testing your fortifications and understanding how well your defenses hold up against genuine cyber attacks.
- Elevated Incident Preparedness: In the event of a cyber intrusion, swift and effective incident response is paramount. Insights from tests will strengthen incident response mechanisms, equipping utilities with the tools they need to mitigate damage and recover rapidly.
- Fostering a Proactive Cybersecurity Culture: By helping to facilitate assessments against cyber defenses, we instill a forward-thinking mindset that prizes anticipation and preparedness over reactive measures.
- Maximizing Return on Security Investments: The resources invested in cybersecurity are substantial. Through these kind of assessments, utilities can validate that their investments are being directed most cost effectively.

- Continuous Learning and Skill Enhancement: Beyond identifying gaps, this project is a potent tool for training. It provides hands-on experience, enabling utilities to develop the skills necessary to confront and repel real-world ever-changing threats.

Project Approach and Summary

The Red Team Collaborative project is focused on advancing the ability for utilities to protect and recover from cyber attacks. The approach taken will include:

- Develop and Instantiate a Red Team Assessment Environment: This task intends to develop and build out an environment that is remotely accessible by funding utilities for their use during assessments.
- Red Team Assessment Guidebook: Annually, advisors will prioritize guidebook content that may include, but are not limited to: Anonymous assessment lessons learned, Best Practices, Rules of Engagement, Training, Guidance on protecting against threats.
- Information Sharing Webcasts: Periodic webcasts will share learnings, get information on member priorities, practices to address emerging threats.
- Provide Red Team Matchmaking Services: Facilitate matching utilities that would like to be assessed and utilities that may do the assessment. Assessment scope and costs will be agreed upon by the participating the utilities and are not included in this scope.

ICCS Forum and New Projects (March / April Update)

The March/April 2024 EPRI newsletter announces upcoming events, including the EPRI European Workshop Week, Birds of a Feather Threat Management Workshop, and Cross-Sector Cyber Security Technology Transfer Event. It introduces the ICCS Forum for utility discussions, a revised "Metrics 101" guide for OT cybersecurity, and new projects on integrated cyber-physical security and OT analytics. The newsletter also provides updated materials for the Winter 2024 Advisory meeting and promotes various industry events scheduled for later in the year.

ICCS Forum Now Online

Utility-only Discussion Forum

We are pleased to announce that the ICCS Forum is now online at http://iccsforum.epri.com. This is a new utility-only discussion forum where our members can ask questions for one another and EPRI, share experiences, and find answers. The development of this tool was motivated by two main factors:

1. Email dialogue is lost shortly after it occurs and is not archived. Great dialogue takes place by email with questions, answers and many participants,

but when others have similar questions or you want to find it later, it is lost. The ICCS Forum makes threads of discussion searchable.

2. Inquires to the EPRI staff often regard established practices and what other utilities are doing. The ICCS Forum provides a direct means for peer-discussion among utility personnel.

Who Should Participate: All ICCS advisors. Questions to both EPRI staff and other utility members is encouraged.

Discussion areas are by P183 and P160 PSET but all areas are available to advisors.

Metrics 101 – A Beginners Guide to OT Cyber Security Metrics

The Metrics 101 Guidebook has been recently republished with revised and enhanced content. This includes streamlined Cyberjoule software installation instructions and updated visuals to improve comprehension.

Who Should Download: The document delivers significant value for anyone interested in cyber security data, particularly Cyberjoule system administrators, end users, and data governance professionals.

Creating Effective Analytics to Monitor Operational Technology (OT)

This project seeks to bridge existing gaps in situational awareness within operations technology (OT) environments. By distinguishing between normal and abnormal behavior, it aims to furnish cyber defenders with enhanced tools for preemptive threat detection and rapid response. The research aims to elevate the cybersecurity posture of electric utilities' OT systems through the deployment of advanced analytic monitoring. Drawing on established methodologies and insights, the project aims to discern patterns indicative of potential threats, thereby fortifying incident response capabilities and mitigating risks to critical infrastructure.

Who Should Join: Utilities that want to gain a greater understanding into their own current capabilities to monitor and detect cyber security attacks in OT.

Integrated Cyber-Physical Security for Distribution Automation

Based on feedback from member utilities, EPRI identified a need to develop an integrated approach to cyber-physical security for field deployed controls used for distribution automation. Utilities must protect these important assets from malicious actors along with protecting against a potential cyber attacker who may attempt to use the control as location to gain access to the utility's network for malicious purposes. This project builds on the results of laboratory testing and seeks to apply and refine the approach in the field.

Who Should Join: Distribution utilities who actively deploy communicating line devices that could demonstrate technologies to strengthen both their physical and cyber security.

2024 ICCS Quick Reference Guide

Updated for 2024, the Information, Communication and Cyber Security (ICCS) Quick Reference Guide features information about program funding, Advisory and the Advisory structure, and staff contact information.

Who Should Read: All P183 funders.

2024 Winter Advisory Meeting Materials

The meeting materials for the EPRI ED&CS Transmission, ICCS & ESCA Advisory & Sector Council Meeting - Winter 2024 held Monday, March 25th- Thursday, March 28th, 2024, are now available for download on EPRI.com. To access the materials, follow these steps:

1. Click on this link
2. Log-in to your EPRI ID account
3. Select the Attachments tab

P183E Task Force Update (May Update)

The May 2024 EPRI newsletter highlights key upcoming events, including the Cyber Security Data/Knowledge Applications Task Force webcast on May 15th and the Birds of a Feather Cyber Security Workshop in June. It announces a new Red Team Collaborative project, a deliverable on cybersecurity for energy storage, and shares insights from a recent visit to Powerlink Transmission Utility in Australia. The newsletter also promotes the Fall 2024 ED&CS Advisory and the Cross-Sector Cyber Security Technology Transfer Event later in the year.

EPRI P183E Cyber Security Data / Knowledge Applications Task Force Webcast

The Data Foundations for Cyber Security Task Force supports the research activities for Pset 183E and helps inform project direction and deliverables for funders. This inaugural Task Force webcast features a presentation from Paul Agbabian, VP and Distinguished Engineer at Splunk and a principal driver of the Open Cybersecurity Schema Framework (OCSF) open-source project.

Cybersecurity Decision Framework for Utility Scale Energy Storage

This report provides insights on commonly used architectures that utilities use to deploy energy storage systems and investigates cyber security risks for each of those architectures. Cyber risks applicable to generic energy storage system have been identified and security requirements to mitigate those risks are detailed. Four architectures have been identified based on participating utility's interests. Storage systems are promulgating throughout utility systems and are slated to become a prevalent grid support tool. Given the increasing reliance on these new storage technologies and the expanding focus on ensuring the cyber security of the grid, it is necessary

to research how cyber security approaches can be best applied to energy storage. This report provides a high-level risk analysis and security controls covering all the four architectures.

P183 Staff Visit Powerlink Transmission Utility in Australia

EPRI resources John Stewart and Christine Hertzog recently visited new P183 member Powerlink, a transmission utility in Queensland, Australia. The team met with over 20 resources in the areas of OT and IT cyber security, telecommunications, protection & control, and senior management for control centers and technology projects.

Figure 2-1. John Stewart and Christine Hertzog visiting Powerlink's Headquarters

The company serves two local distribution utilities and is growing as the population of Brisbane and outlying areas expands. Powerlink currently provides service to more than five million Queenslanders and 253,000 businesses. Their network extends 1,700 kilometers (km) from Cairns to the New South Wales border, which is roughly equivalent to the distance between New York City and Tallahassee, FL. Power is delivered through 15,345 circuit km of transmission lines and 147 substations with both metrics scaling rapidly to meet demand.

This utility has embarked on an ambitious 10-year initiative to refresh critical infrastructure including a new EMS system, a new GIS system, a new OMS solution with a new control center planned to support operations. Some of the challenges Powerlink shared include the complex

integration of legacy technologies with modern systems and the scarcity of skilled resources to help design operate and maintain the grid.

Additionally, Powerlink has developed some creative solutions to address these challenges by standing up a variety of organizations that are focused on different business capabilities. The use of separate IT and OT security teams enables Powerlink to leverage dedicated resources who are familiar with the unique requirements found in both environments. Past EPRI work on the "Security Integration" topic has highlighted the need for early coordination between the substation design and security organizations. Powerlink has developed a comprehensive substation design standard that is version controlled for different vintages of equipment which allows the security team to understand the technology within a station by referencing the specific version of standard that was used for the design. To ensure alignment, appropriate security controls have been designated for each version and can be applied in a repeatable manner. For more information about the solutions used by Powerlink, contact John Stewart, jstewart@epri.com.

Task Force Updates and Forum Highlight (June Update)

The June 2024 EPRI newsletter highlights upcoming events such as the Birds of a Feather Cyber Security Workshop (June 12-13) and the Cyber Security Program ARP Rollout Webcast (July 30). It covers discussions from the P183E Task Force, focusing on AI's role in OT cybersecurity, and introduces a new article on quantum cybersecurity. The newsletter also promotes the ICCS Forum, details from recent meetings, and shares insights from the Energy Storage Cyber Security Webcast. Additionally, it encourages registration for fall industry events like Black Hat USA.

P183E Task Force Meeting Summary and Call for Members

In our very first PS183E Taskforce meeting, held on May 15th, 2024, (meeting materials here) the pivotal role of machine learning (ML) in enhancing OT cybersecurity operations was delved into. With the rise of AI-powered cyber threats, securing our critical infrastructure has never been more crucial. The importance of data proficiency was emphasized, highlighting that clean, well-managed data is the cornerstone of effective cybersecurity.

The challenges we face, including a shortage of expertise and manpower, were discussed, and advanced AI techniques like supervised and unsupervised learning, NLP, and generative AI for threat detection and anomaly hunting were introduced. The session underscored the need for secure AI implementation and continuous education to prepare our teams for the evolving threat landscape.

It was concluded that by investing in data management and advanced AI solutions, we can stay ahead of emerging threats and optimize our cyber defense strategies. The meeting wrapped up with our guest speaker, Paul Agbabian, VP and Distinguished Engineer from Splunk, who discussed the growing importance of the Open Cybersecurity Schema Framework (OCSF).

ICCS Forum Q&A Highlight

Defining DER/DERMS

ICCS Forum Q&A Highlight

Defining DER/DERMS

A great question was added to the ICCS Forum by Alexander Waitkus from Southern Company Services, Inc.

Question: "I am currently reading a draft paper and the DER definition is different from definitions I have seen from FERC and other orgs, in your opinions, how would you define distributed energy resources? The definition I am asking about is below as is a comment from someone on our Generation team and I am trying to make my own assessment, but I would like your thoughts as well. Thanks for your time!"

Distributed Energy Resource (DER) – Any Source of Electric Power located on the Distribution System. *Note: Loads and Demand Response do not produce electric power and are therefore not included in the definition of DER.

"Comment that I find a tad odd," "The DER definition which, based on how broad it is stated, includes emergency house generators if they're serving more than 1 metered household (which could be the case at farms, family neighborhoods, etc.)."

Answer: (Xavier Francia, P183 Cyber Security)

"Hi Alex, Great question! I think the most important part is that each utility agrees internally on what's in scope when using the term DER. If the term is used in requirements, say an RFP released to candidate vendors, the utility would likely want to adopt specific industry language and normative references such as IEEE to describe what exactly they mean. For example, the 1547-2018 language for interconnection requirements. For us in P183D, we tend to use the California definition for our scope as we do include demand response aa part of our own research. But typically when we talk/present, we use the 1547 definition for DERs and if we intend to include Demand Response/Demand Flexibility and EVs, we say so explicitly for clarity."

Ben Ealey and Brian Seal, P161 also posted their thoughts and definitions. The post is available here, we'd love to hear from other advisors on their definition of DER/DERMS, or any other questions they might want to share with other utilities.

New Article from the P183 Knoxville Lab

Quantum Cyber Security: Fortifying Digital Defense Against Quantum Threats

In the rapidly evolving landscape of cyber threats, quantum computing looms as both a promise and a peril. While heralded for its potential to revolutionize computation, quantum technology poses a significant challenge to conventional cryptographic methods, threatening the security

of digital information and communication systems worldwide. In response, the burgeoning field of quantum cyber security is harnessing the unique properties of quantum mechanics to develop innovative cryptographic solutions capable of withstanding the power of quantum computers.

At the forefront of this endeavor is quantum key distribution (QKD), a cutting-edge cryptographic protocol that utilizes quantum principles to establish secure keys for encrypting and decrypting sensitive data. Unlike traditional cryptographic methods, which rely on the difficulty of solving complex mathematical problems, QKD leverages the fundamental laws of quantum mechanics, including the Heisenberg uncertainty principle and the no-cloning theorem, to ensure the security of the critical exchange process.

Central to QKD is the principle of quantum entanglement, which allows for the creation of shared keys between distant parties in an inherently secure manner against eavesdropping attempts. By exploiting the delicate correlations between quantum particles, QKD enables the generation of cryptographic keys with provably secure levels of randomness, offering unparalleled protection against interception and decryption by malicious actors, including quantum computers.

Moreover, quantum cyber security encompasses the development of quantum-resistant cryptographic algorithms designed to withstand attacks from classical and quantum computers. These algorithms, built upon mathematical structures resistant to quantum algorithms such as Shor's algorithm, represent a crucial line of defense in safeguarding digital communication and data storage against emerging quantum threats.

As the race to develop practical quantum computers intensifies, the imperative to fortify our digital defenses against quantum-enabled attacks has never been more urgent. Quantum cyber security stands poised at the vanguard of this endeavor, pioneering innovative solutions grounded in the intricate principles of quantum mechanics. By leveraging the power of quantum technology, we can confidently navigate the complexities of the quantum era, ensuring the integrity and confidentiality of our digital infrastructure for generations to come.

Energy Storage Cyber Security Webcast

Held on May 22nd, 2024, the Energy Storage Cyber Security Webcast featured staff from both the Cyber Security and Energy Storage programs who presented an overview of security risks, supply chain security concerns, and shared insights from the Energy Storage Cyber Security Decision Framework supplemental project.

Program Rollout and Forum Highlight (July Update)

The July 2024 EPRI newsletter highlights upcoming events, including webcasts on Distributed Energy Resources (July 9) and the 2025 Cyber Security Program ARP Rollout (July 30). It also announces the Fall 2024 ED&CS Advisory meeting (September 16-19) and the Cross-Sector Cyber Security Technology Transfer Event (December 9-12). The newsletter shares insights from the Energy Storage Cyber Security Decision Framework webcast and introduces a Q&A from the

ICCS Forum on network resiliency. Additionally, Chuck Moran, the new Principal Technical Leader, discusses his background and thoughts on cyber security.

EPRI P183 Cyber Security Program 2025 ARP Rollout Webcast

The P183 Cyber Security Program 2025 Advanced Research Portfolio (ARP) Rollout webcast was held on Tuesday July 30th, 2024. Cyber security has become a critical priority for electric utilities, which are increasingly dependent on information technology and telecommunication infrastructure to ensure the reliability and security of the electric grid. Specifically, measures to ensure cyber security must be designed and implemented to protect the electric grid from attacks by terrorists and hackers, and to strengthen grid resilience against natural disasters and inadvertent threats, such as equipment failures and user errors. EPRI's Cyber Security Program focuses on addressing the emerging threats to an interconnected electric sector through multidisciplinary, collaborative research on cyber security technologies, standards, and business processes.

The 2025 ARP information is available to download in PDF format from the program Member Center site under Projects - Project Overview & Updates.

ICCS Forum Q&A Highlight

Network Resiliency for Major Electric Substations

Question: "Are there any best practices or guidelines regarding having technology diversity for building transport networks such as fiber and microwave to support major substations with higher voltages such as 220k and 500kV? This type of design will provide network resiliency in case of natural disasters so that one technology will survive more than the other...the WECC guideline for critical protection circuits is avoid a single point of failure, and this requires a N-1 design for two diverse routes. Sometimes utilities use N-2 or three diverse routes to avoid long-term outages on any one of the routes. Any thoughts on what other utilities feel about N-2 design?"

Answer: (Christine Hertzog, P183 Cyber Security)

"From a general resiliency perspective, yes, having two different network options from different vendors and different technologies is the best practice. I consulted with clients in a previous role that created distinctly different physical access points for network connections to buildings to address scenarios like partial building destruction."

Answer: (Ishaq Mian, P161 Information Communication Technology) "Two point answer:

Part 1-Classic answer is "it depends". Two diverse routes are usually sufficient. But yes, as you alluded to, there are situations (albeit rare) where more than two diverse routes are preferred...I remember one situation relating to a 500kv line connecting a large nuclear power plant to the grid. The line was protected via a SONET ring - two diverse routes. A small section of the fiber in a different part of the ring needed replacement, which meant taking a scheduled outage on one route. The ISO in this case required a 90 day advance outage notification. The

outage had to be re-scheduled three times (270 days) as the ISO did not provide a green signal on the day of the outage, based on system level risk. The telecom team was in a difficult situation as the fiber needed replacement due to perceived degradation, which was a risk in itself. The outage was eventually granted, and the fiber cable eventually replaced almost a year after originally planned. The utility learnt the lesson though and availed a shield wire replacement opportunity to add OPGW on another line which provided a third route and converted the SONET ring into a semi-mesh in that specific region. Part 2-Note that resilience goes beyond just things like route diversity (or the ability to withstand a disruptive event). It also includes the capability to rapidly recover from such events. In my experience, telecom engineers tend to prioritize the former (e.g., protection via diversity) over the later (network recovery via rapid response capabilities that go beyond just the equipment). I have been guilty of doing the same as well. But have learnt over the years that the later is equally important for resilience and at times even more complex to engineer."

Further discussion continued in the post. We'd love to hear from other advisors with an answer, or who want to provide any other questions to share with other advisors.

New Article from P183 Knoxville Lab

Welcome to Chuck Moran

Recently, P183 Cyber Security welcomed Chuck Moran as Principal Technical Leader. We posed a series of questions to him to help our members better understand his thoughts on cybersecurity and to help get to know him.

Question: Your background included a start in wireless telecommunications. How did you end up in cyber security?

It has been a journey! I have always had a couple different passions, automotive and technology with a focus on exploitable weaknesses (e.g. cybersecurity). Early on, formal education and careers in technology were not well defined. With that, I had an opportunity presented to pursue one of my passions – automotive, becoming an ASE certified automotive technician. Having different roles in the automotive field including work as a technician, restorer, and a warranty claims adjuster allowed me to build my skillset that continues to support my hobby.

As formal education and careers matured in the technology field, I moved forward with additional formal education. First with a degree in Computer Networking. During that journey, I had an opportunity to visit Auburn University. I was impressed with the new joint Electrical and Computer Engineering (ECE) and Computer Science (CS) developed program for Wireless Engineering. While pursuing this degree my initial focus was heavily within cybersecurity but later, I switched to a more ECE focus. My senior capstone project focused on wireless networks – cybersecurity detection and monitoring.

Question: Your research focus is on project set 183B – Threat Management and Incident Response. What is your vision for where EPRI's research should impact this important topic area?

With the many challenges of investment in ICS/OT cybersecurity, the research focus in P183B must continue to provide short-, medium-, and long-term value to our Members. Short-term research goals include driving value from cybersecurity investments by researching ways to operationalize ICS/OT cybersecurity data as a business intelligence tool (ask me about our OT Dashboard Supplemental Project) and examining the fidelity of ICS/OT cybersecurity alerts for earlier detection of threats and to prevent analyst fatigue. Medium- and longer-term goals include researching how Artificial Intelligence (AI) and Machine Learning (ML) may provide economies of scale for Threat Management and Incident Response.

Question: You just returned from the Birds of a Feather workshop. What did you think about your first EPRI workshop and was there anything about it that surprised you?

I think I joined EPRI with perfect timing to be able to participate in the workshop. Having experiences in the Power Delivery cybersecurity space through my various roles at outside organizations, I was excited to be able to speak to the Members that participated and glean additional understanding of the current state and challenges they faced in Threat Management and Incident Response. I was surprised with the maturity of processes within various Member organizations dedicated to Threat Management and Incident Response. The use of various technologies including large datasets and Machine Learning to satisfy specific use cases over disparate datasets. The overall discussions and collaboration were great!

Question: What are your predictions for cybersecurity in 2025?

Threats continue to evolve with threat actors having potential political motivations and/or looking to monetize their targets. Threat actors continue to adopt Artificial Intelligence (AI) for rapid prototyping and exploitation of gaps in cybersecurity controls and general weaknesses in design and implementation of systems. Threat actors have shown they are gaining system expertise to "fly under the radar" using installed tools (Living off the Land) once a foothold is gained. Threat Detection and Incident Response will need to mature to handle the large volumes and disparate sets of data to find potential anomalous activity quicker and with higher levels of fidelity.

Question: Tell us about an accomplishment in your life that is not work-related that means a lot to you, like a hobby or something you've done or do now.

Great question, anyone that knows me will hear about my hobby! From an early age, I was always interested in automotive and technology. Having previously been an ASE certified automotive technician I gained quite a bit of experience solving automotive problems and implementing solutions. With that, other than ICS/OT cybersecurity, my break away from work passions are acquiring, building/fixing General Motors muscle cars from the late-60s. I have developed a good collection of vehicles that meet my passions and keep me busy. Interacting

with others with similar passions at automotive type events – car shows and swap meets, is a hot go-to for my weekend activity.

Meeting Materials and CrowdStrike Insights (August Update)

The August 2024 EPRI newsletter highlights upcoming events such as the Fall 2024 ED&CS Advisory (September 16-19) and the Joint Digital Substations Workshop (October 29-30). It reviews materials from the 2025 Cyber Security Program Rollout webcast and discusses cybersecurity lessons from the CrowdStrike incident. The newsletter also promotes resources like the ICCS Forum and the EPRI Member Center for program-related updates and research. Key insights include cybersecurity for DER systems and incident management.

Meeting Materials

EPRI P183 Cyber Security Program 2025 Program Rollout

The 2025 Program Rollout Webcast was held on July 20th, 2024. During the webcast members learned about the new program offerings and expectations and objectives to be achieved in 2025 as well as a brief overview of each of the different Program sets:

- Strategic Intelligence and Emerging Issues (183A)
- Incident and Threat Management (183B)
- Cyber Security for Transmission and Distribution (183C)
- Cyber Security for DER and Grid Edge Systems (183D)
- Cyber Security Data Applications (183E)

Strengthening Cyber Security Confidence: Lessons from the CrowdStrike Update Incident

Written by Chuck Moran, Principal Technical Leader – P183B

While it is early to get full visibility into the specific operational and financial impacts in the Electric Sector from the CrowdStrike errant content update, an immediate impact comes to mind - customer confidence in cybersecurity solutions for threat prevention and monitoring through solutions such as Endpoint Detection & Response (EDR) in the OT/ICS space. Cybersecurity in the OT/ICS is highly held to the "do no harm" mindset. Based on early reports, organizational financial harm over all sectors is expected to soar over $5 Billion USD.

Understanding that, cybersecurity solutions face challenges of delivering dynamic solutions that match the current threat actor's speed and agility. Specifically in this case for CrowdStrike, their Rapid Response Content for Microsoft Windows is designed to address a quickly changing threat landscape. While modernization and digitalization have occurred in the Electric Sector, many of the critical basic control/safety components (e.g. Purdue Level 1) deployed today are

still purpose-built embedded systems that would have fallen outside the scope of a direct impact.

How this outage was addressed and in looking towards the future, we must still consider availability as key in critical systems and components within the Electric Sector. To minimize potential impacts to critical systems and components, processes both vendor-side and customer-side should be reviewed and matured based on lessons learned. On the vendor-side, additional robust testing, and validation via Quality Assurance (QA) within their software development lifecycle must be implemented to limit unexpected customer impacts.

However, it is likely difficult within a vendor QA to account for every customer configuration (e.g. other installed software, services, components, etc.) for multiuse operating systems (e.g. host-based systems like Microsoft Windows). With that, consideration must be given to every potential change (even things that might just be considered routine "content") - through a defined Change Management process including internal testing/rollout requirements based on the potential impacts and risks to organization, processes, and people. Looking back to 2010, a similar issue occurred with just "content" updates from McAfee within Windows XP resulting in similar, albeit smaller, scale outage. So, while the frequency may be low, depending on the systems - the impacts could be high for an organization as demonstrated on July 19, 2024. Consideration must still be given to High-Impact Low-Frequency (HILF) events.

To support these customer-side processes, CrowdStrike announced it is introducing additional customer controls over the delivery of all updates including the Rapid Response Content. As organizations had to execute their pre-defined Response and Business Continuity plans, opportunities were likely identified for improvements. Based on the organization's lessons learned, these plans should be updated accordingly, and technical controls updated (e.g. leveraging controls for staged rollouts based on potential risks and impacts).

Meeting Materials Available

Birds of a Feather Workshop

Held on June 12-13th, 2024, P183 Cyber Security presented the Birds of a Feather Cyber Security workshop, hosted by FirstEnergy at their Center for Advanced Energy Technology facility in Akron, OH.

P183B Incident & Threat Management Task Force funders heard presentations about Cyber Security for AI, Retentive Network AI Models, Grid Monitoring and Sensor Placement, Threat Detection, and Insider Threats.

Figure 2-2. Birds of a Feather Workshop held at FirstEnergy

Deliverables and Updates (September Update)

The September 2024 EPRI newsletter highlights upcoming events such as the Fall 2024 ED&CS Advisory (September 16-19) and webcasts on supplemental projects and digital substation technologies. New deliverables include reports on machine learning applications for OT cybersecurity and the rise of AI-assisted ransomware threats. The newsletter also discusses lessons from a recent CrowdStrike security incident and provides insights from recent task force webcasts. It encourages participation in the ICCS Forum for discussions among EPRI members on emerging cybersecurity issues.

Machine Learning and Applications for OT Cyber Security Operations Version 1

This deliverable delves into the fundamentals of ML, including data preprocessing techniques, effective feature engineering methods, common ML algorithms, and criteria for model selection and evaluation metrics. Practical applications of ML in OT security are then examined, such as anomaly detection, predictive insider threat detection, and AI-powered threat intelligence. The report also addresses emerging threats and vulnerabilities associated with AI, the regulatory landscape, and best practices for securing AI in OT environments. It concludes with discussions on comprehensive risk assessment, robust AI governance, and the importance of human-AI collaboration to ensure the resilience and security of OT systems.

Ransomware as a Service (RaaS): The Rise of AI-assisted Threats and AI-assisted Mitigation

The integration of AI into Ransomware as a Service (RaaS) has significantly enhanced the capabilities and impact of ransomware attacks. Automation and AI-driven phishing attacks have increased the likelihood of success. Sophisticated malware development and the use of AI-generated deepfakes add layers of complexity and stealth to ransomware campaigns, making them harder to detect and defend against. To effectively combat these advanced threats, organizations must adopt comprehensive security measures, including advanced threat detection tools, robust data protection strategies, and continuous employee education on the

latest tactics used by cybercriminals. By staying informed about these emerging trends, organizations can better prepare for and mitigate the risks associated with AI-enhanced RaaS attacks.

CrowdStrike Security Incident: A P183E Perspective

Written by Christine Hertzog, Principal Technical Leader

Cyber resiliency is a key topic for 183E in terms of understanding the systems and the data necessary to stand up utility cyber security operations. Utilities may want to take a closer look at their recovery plans and make sure that they have spares that cover the triad of people, process, and technology. From a people perspective, that means having an N+1 approach to authorized access to recovery data stores for critical systems. From a process perspective, that means having physically accessible recovery data storage in case cloud-based data storage is unavailable. From a technology perspective, spare hardware to run critical systems for cyber security operations. Recovery time objectives (RTOs) and recovery point objectives (RPOs) must be defined for cyber security systems and functions in addition to those established for grid operations, documented in recovery plans, and drilled through table top exercises.

Updates and Tech Transfer Workshop (October Update)

This edition focuses on upcoming events, including the P183C Joint Digital Substations Workshop (October 29-30) and the P183 Cyber Security Supplemental Project Webcast (October 1). It highlights recent deliverables and contains insights from the P183E Data Applications Task Force and P183B Incident Management Task Force webcasts are also provided. Members are encouraged to engage in the ICCS Forum and prepare for the December Joint Technology Transfer Event.

About EPRI

Founded in 1972, EPRI is the world's preeminent independent, non-profit energy research and development organization, with offices around the world. EPRI's trusted experts collaborate with more than 450 companies in 45 countries, driving innovation to ensure the public has clean, safe, reliable, affordable, and equitable access to electricity across the globe. Together…shaping the future of energy.

Program:

Cyber Security for Energy Delivery and Customer Solutions (183)

3002030015

EPRI
3420 Hillview Avenue, Palo Alto, California 94304-1338 USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com