View in browser

PROGRAM SITE | VIDEOS | EVENTS | 2024 ARP | LINKS | @EPRINEWS

June 2024 Newsletter

Future EPRI Events

- **Coming Soon!**
  - **June 12-13, 2024:** EPRI P183B Birds of a Feather Cyber Security Workshop
  - **July 30, 2024:** EPRI P183 Cyber Security Program ARP Rollout Webcast
- **Save the Date!**
  - **September 16-19, 2024**: EPRI Fall 2024 ED&CS Advisory
  - **December 9-12, 2024**: EPRI Cross-Sector Cyber Security Technology Transfer Event

EPRI Cyber Security News

Almost Here! EPRI P183B Birds of a Feather Cyber Security Workshop

June 12-13, 2024

Location: FirstEnergy, Akron, Ohio
Who Should Attend: Cyber Security and IT Professionals at the **funding member utilities for P183B**

The Birds of a Feather Threat Management workshop brings together defenders of utility networks to foster a collaborative and proactive environment where

professionals can share their experiences, knowledge, and best practices in addressing the ever-evolving landscape of cyber threats. This year's workshop has a strong theme of cyber-physical IT/OT convergence and will include a virtual tour of FirstEnergy's SOC, practices to detect and protect against National Threats, Insider Threats and learning key practices from your peer utilities among other topics.

By learning from experts inside and outside of the utility industry, the workshop aims to facilitate the exchange of valuable insights and innovative solutions that can effectively mitigate the risks posed by sophisticated cyber-attacks on critical infrastructure. This collective learning experience strengthens the capacity of the industry to withstand and recover from potential cyber incidents.

June 12, 2024
8:00am - 5:00pm EDT
June 13, 2024
8:00am - 12:00pm EDT

FirstEnergy CAET (Center for Advanced Energy Technology) Facility
871 Mull Avenue, Akron, Ohio, 44313

Note: This is an in-person event, for P183B funding member utilities.

Register Now

Tuesday, July 30th, 2024
11:00am-12:00pm PT / 2:00-3:00pm ET

Join WebEx

EPRI P183 Cyber Security Program ARP Rollout Webcast

Join us on Tuesday, July 20th, 2024, from 11:00am-12:00pm PT/2:00-3:00pm ET for the P183 Cyber Security Program Advanced Research Portfolio (ARP) Rollout webcast. The 2025 ARP information is available to download in PDF format from the program Member Center site under **Projects - Project Overview & Updates.**

A webcast invitation will be sent at a further date.

EPRI Fall 2024 Energy Delivery & Customer Solutions Advisory & Sector Council Meeting

September 16-19, 2024

Location: Los Angeles, California
Who Should Attend: P183 Funders

It is recommended to make your room block reservation ASAP! The room block is available until August 16th, 2024, or while rooms last.

During this time, the Emmys will also be held at a location next to the hotel.

Note: This is an in-person event.
Energy Delivery & Customer Solutions (ED&CS) is the sector previously known as Power Delivery & Utilization (PDU).

JW Marriott Los Angeles L.A. LIVE
900 W Olympic Boulevard
Los Angeles, CA, 90015

EPRI Room Block Rate: $279/night
Available until August 16th, 2024

Hotel Reservation

Mark Your Calendar

Are you interested in joining the P183E Task Force?

Contact
Christine Hertzog, Principal Technical Leader or Nivedya Ashokan, Engineer III

Who Should Join: Electric utilities interested in data management, the usage of AI and machine learning with data, and the role of data in OT operations.

P183E Task Force Meeting Summary and Call for Members

Project Set 183E Cyber Security Data/Knowledge Applications

--Nivedya Ashokan, P183 Cyber Security - Engineer III

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

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.

Learn More About the ICCS Forum

The ICCS Forum is a new utility-only discussion forum where our members can ask questions for one another and EPRI, share experiences, and find answers.

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

Discussion areas are by P183 and P161 PSET but all areas are available to advisors. The forum requires an EPRI ID (advisors can create an ID at **http://enroll.epri.com**).

New Article from the P183 Knoxville Lab

Quantum Cyber Security: Fortifying Digital Defense Against Quantum Threats

--Larry Burnette, P183 Cyber Security - Technical Leader

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.

Meeting Materials

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.

Download Materials

EPRI Events - Save the Date!

Dec 9-12, 2024

EPRI Cross-Sector Cyber Security Technology Transfer Event

Location: EPRI office
More information will be coming soon.

Industry Events

Black Hat USA

August 3-8, 2024 -
Las Vegas, NV

InfoSec World

September 23-25, 2024 - Lake Buena Vista, FL

National Cyber Summit

September 24-26, 2024 - Huntsville, AL

Program Site

[Overview]
[Projects]
[Supplemental Projects]
[2024 ARP]

Advisor Engagement

[Events]
[Training Courses]
[Announcements]
[Links]
[ICCS Forum]

Other Information

[CS Roadmap for 2030]
[2024 ICCS At A Glance]
[P183 at a Glance]
[P183 Videos]

EPRI, 3420 Hillview Avenue, Palo Alto, CA 94304 USA
www.epri.com | 650-855-2121