View in browser

PROGRAM SITE | VIDEOS | EVENTS | 2025 ARP | LINKS | @EPRINEWS


# July 2024 Newsletter

## Future EPRI Events

- **Coming Soon!**
  - **July 9, 2024:** EPRI P183D Distributed Energy Resources and Grid-edge Systems Task Force Webcast
  - **July 30, 2024:** EPRI P183 Cyber Security Program 2025 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

## P183D Distributed Energy Resources & Grid-edge Systems Task Force Webcast

Join us on Tuesday, July 9th, 2024 from 2:00 - 3:00pm EDT/11:00am - 12:00pm PDT for the P183D Distributed Energy Resources & Grid-edge Systems Task Force Webcast. The Distributed Energy Resource and Grid-edge systems Task Force supports the research activities for project set P183D and helps inform project directions and deliverables for utilities seeking to find practical and effective solutions for securing grid integration of DERs. This webcast features presentations on:

- **State of the DER Industry** – What is the latest on relevant cybersecurity standards and certifications for DERs, and how are public utility commissions (PUCs) beginning to approach cyber issues related to distribution-connected DERs?
- **Electric Vehicle Charging Infrastructure** – What are the consequences of large-scale cyber-attacks on EV chargers and what are the known cyber gaps that the industry needs to address?
- **Cloud-DER Integration** – What is the role of cloud for DER integration and can market offerings of Security-at-Service-Edge (SASE) services provide effective Zero Trust capabilities for internet-connected DERs?

**Tuesday**
**July 9, 2024**
2:00 - 3:00pm EDT / 11:00am - 12:00pm PDT

**Download Invitation (.ics)**

**Join WebEx**

---

**Tuesday**
**July 30th, 2024**
2:00 - 3:00pm EDT / 11:00am - 12:00pm PDT

**Register for Webcast**

## EPRI P183 Cyber Security Program 2025 ARP Rollout Webcast

Join us on Tuesday, July 30th, 2024, from 2:00 - 3:00pm EDT/11:00am - 12:00pm PDT for the P183 Cyber Security Program 2025 Advanced Research Portfolio (ARP) Rollout webcast. 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.**

## Meeting Materials Available

### Energy Storage Cyber Security Decision Framework Supplemental Project Webcast

Held on May 22nd, 2024, P183 Cyber Security and Energy Storage staff presented an overview of security risks, supply chain security concerns, and shared insights from the Energy Storage Cyber Security Decision Framework supplemental project. The recording and slides are available on the P183 Member Center.

**Download Materials**

## 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**

## 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.

### 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

### Welcome 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.

## 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

**SECtember.ai**

September 10-12, 2024 - Bellevue, WA

**InfoSec World**

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

**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