View in browser

PROGRAM SITE VIDEOS EVENTS 2025 ARP LINKS @EPRINEWS

September 2024 Newsletter

Future EPRI Events

- **Coming Soon!**
  - **September 16-19, 2024**: EPRI Fall 2024 ED&CS Advisory
  - **October 1, 2024**: EPRI P183 Cyber Security Supplemental Project Webcast
  - **October 3, 2024:** EPRI P183C Transmission & Distribution Task Force Webcast
  - **October 29-30, 2024 -** EPRI P183C Joint Digital Substations Workshop
- **Save the Date!**
  - **December 11-12, 2024**: EPRI P183 & P209 Joint Technology Transfer Event

EPRI Cyber Security News

Event Registration

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

September 16-19, 2024

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

Save the Date: Upcoming Webcasts

Invitations Coming Soon

EPRI P183 Supplemental Projects Launch Webcast

October 1st, 2024
3:00pm - 4:00pm ET / 12:00pm - 1:00pm PT

P183C Transmission & Distribution Webcast

October 3rd, 2024
2:00pm - 3:00pm ET / 11:00am - 12:00pm PT

EPRI P183C Joint Digital Substations & Task Force Workshop

October 29-30, 2024

Location: EPRI Charlotte, NC Office
Who Should Attend: P183C Funders

Utilities are continuously exploring new P&C designs and digital substation technologies that promise to improve safety and reliability, reduce costs, enhance security, enable condition-based maintenance, and strengthen grid resiliency. Some examples of new digital substation technologies include:

- IEC 61850 standard
- Innovative security controls
- Process bus
- Fiber option communication and advanced network protocols
- Precision time protocol and secure time sources
- Virtualization advancements in protection and control

While the shift to digital substation technologies may provide significant advantages, this change cannot be realized without corresponding adjustments to substation infrastructure such as communications networks, cybersecurity controls and time synchronization. Existing methods and practices in engineering, settings and configuration management, operation and maintenance will also need to be updated in order to meet the new technology requirements.

Tuesday, October 29th
Joint Task Force Meeting
8:00am - 5:00pm

Wednesday, October 30th
Hands-on Tech Transfer Workshop at EPRI Lab
8:00am - 5:00pm

Event Registration

New Deliverable

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.

Download Deliverable

New Deliverable

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.

Download Deliverable

Meeting Materials Available

P183E Data/Knowledge Applications Task Force Webcast

Held on August 21st, 2024, the ***P183E Data/Knowledge Applications Task Force*** quarterly webcast introduced the new Task Force Chair, Henry Karikari from Centerpoint Energy. Attendees also previewed the new report *Machine Learning and Applications for Cyber Security Operations Version 1* (Product ID: 3002030133)

Download P183E Webcast Materials

Meeting Materials Available

P183B Incident & Threat Management Task Force Webcast

Held on August 22nd, 2024, the ***P183B Incident & Threat Management Task Force Webcast*** provided updates on the current Cybersecurity Research Lab progress and deliverables, plans for 2025 work, upcoming technologies, and an open discussion on the upcoming CIP-015 / INSM.

Download P183B Webcast Materials

CrowdStrike Security Incident: A P183E Perspective

Written by Christine Hertzog, Principal Technical Leader and P183 Task Force Lead

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.

ICCS Forum - Ask Us a Question

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**).

P183 Specific Forums:
Cyber Security Emerging Issues
Cyber Security Incident & Threat Management
Cyber Security for T&D
Cyber Security for DER and Grid-Edge Systems
Cyber Security for Data Applications

Join the Conversation

EPRI Events - Save the Date!

December 11-12th, 2024

EPRI P183 & P209 Joint Technology Transfer Event

Location: EPRI Charlotte office
More information will be coming soon.

Industry Events

InfoSec World

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

ISC2 Security Congress 2024

October 14-16, 2024 - Las Vegas, NV + Virtual

SECtember.ai

October 22-24, 2024 - Virtual Event (Free)

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