View in browser

EPRI

PROGRAM SITE VIDEOS EVENTS 2025 ARP LINKS @EPRINEWS

August 2024 Newsletter

Future EPRI Events

- **Coming Soon!**
    - **September 16-19, 2024**: EPRI Fall 2024 ED&CS Advisory
- **Save the Date!**
    - **October 29-30, 2024** - EPRI P183C Joint Digital Substations Workshop
    - **December 9-12, 2024**: EPRI Cross-Sector Cyber Security Technology Transfer Event

EPRI Cyber Security News

Hotel Reservation

Mark Your Calendar

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

September 16-19, 2024

Location: Los Angeles, California

Who Should Attend: P183 Funders

EPRI Room Block Rate: $279/night

Available until August 16th, 2024 or until sold out, it's recommended to reserve your room ASAP!

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)

Download Webcast Materials

Strengthening Cybersecurity 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.

Download P183B Workshop Materials

Member Center Insights: How to Setup TIP Subscriptions and Your Personal Dashboard

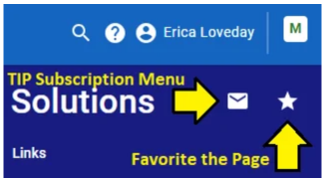
The EPRI Member Center is your one stop for all things program-related. For P183 Cyber Security for Energy Delivery & Customer Solutions, the Member Center keeps you in the know on all program activities, events, research, and projects. To begin, all members will need an EPRI ID to get the most out of the Member Center and be able to see all members-only content. Visit **https://enroll.epri.com/** to set up an EPRI ID, then login and head to the P183 Program page at **https://www.epri.com/research/programs/072143**.

To get the most out of your membership, set up TIP Subscriptions, Favorite the Program Page, and learn about your personal Dashboard.

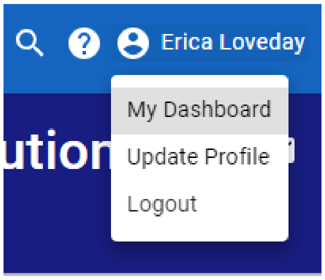
TIP Subscriptions & Favorites

TIP Subscriptions allow you to subscribe to announcement emails for programs. You can choose TIP Subscriptions and Favorite program pages from the icons on the top right of the program page (above), or by heading to the Program Index TIP Subscription Settings page at **https://www.epri.com/research/index**.

TIP email digests are available daily, weekly, or bi-weekly, and you can choose to receive all updates (new events, products, research, training, etc.) or only for when new products are added to the Member Center.



Personal Dashboard
Your personal dashboard brings together news from all Program Pages you've favorited and can help keep track of any events and training classes you've registered for and any Member Center pages you've bookmarked. Also listed are links to the latest EPRI Journal articles. You can find your Dashboard by hovering over your name while logged in, or by going to https://www.epri.com/dashboard.



Meeting Materials Available

P183D Distributed Energy Resources (DER) and Grid-Edge Systems Task Force Webcast

Held on July 9th, 2024, the DER and Grid-Edge Systems Task Force presented a webcast on the current state of DERs, issues in Cloud-DER integration, and possible cyber gaps of EV chargers.

Download P183D Materials

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

A Question to Our Advisors

How did the recent CrowdStrike incident affect your operational performance? Were your pre-defined disaster response plans sufficient to handle this incident?

Any thoughts or answers can be added to the ICCS Forum **here**.

EPRI Events - Save the Date!

October 29-30th, 2024

EPRI P183C Transmission & Distribution Joint Digital Substations Workshop

Location: EPRI Charlotte, NC Office
More information will be coming soon.

December 9-12th, 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