

SUCCESS STORY

XCEL ENERGY STAFF BENEFITS FROM REMOTE CYBER SECURITY OPERATIONAL TECHNOLOGY EQUIPMENT FAMILIARIZATION COURSE

Utility operational technology (OT) cyber security analysts must objectively be familiar with the systems they are tasked to protect, which can often be quite different than enterprise information technology (IT) environments. This includes not only the network communications protocols used in OT environments, but also general familiarity with various protection device functionality and their operations.

This training course provided Xcel Energy utility cyber security engineers, analysts, and managers with hands-on exercises and supporting discussions for a variety of components commonly used to monitor and protect both the power delivery networks and the network infrastructures that support grid operations.

By having basic knowledge of the types of equipment used in OT environments, which can range from protective relays to intrusion detection systems, cyber security resources will improve their proficiencies and productivity in the OT environments they are tasked to monitor and protect.

Learning about different equipment in a sandboxed laboratory environment allows utility cyber engineers an opportunity to solve unique challenges as a cohesive team and forces them to explore and experiment with various solutions without the risk of damaging production devices.

EPRI's OT cyber security engineers and subject matter experts developed this course with hands-on interaction as a primary goal. The modules created cover a wide breadth of topics that are applicable to transmission and/or distribution utilities of any size.

Leveraging EPRI's Cyber Security Research Lab in Knoxville, TN, Xcel's attendees had safe and interactive access with physical devices in a lab environment. This training was conducted virtually for Xcel Energy staff.



"I was privileged to be chosen to participate as one of eight Xcel Energy students in a six-day EPRI Operational Technology (OT) Equipment Familiarization Course. Although conducted remotely, we were immersed in a realistic, hands-on experience by connecting to equipment in the EPRI Cyber Security Research Lab (CSRL). The instructor facilitation was superb; they encouraged us to learn and explore in a safe, yet realistic environment, which was available between and after classes as well. My understanding of substation architecture, communication protocols and hardware and software in use at Xcel Energy was dramatically improved. The course also provided a splendid opportunity for me to engage and build relationships with my classmates and the exceptional industry professionals at EPRI; if I have specific technical questions, I know exactly who to call."

~ TAYLOR COX

*Sr. Consultant,
Business Continuity
Enterprise Security and
Emergency Management
Xcel Energy*



The courses are held for individual utility teams and can accommodate up to eight participants. The course size is limited to promote interaction from all participants and to ensure that every participant has an opportunity to actively engage with equipment during hands-on activities.

Xcel Energy participating staff received:

- Approximately 32 hours of interactive, hands-on, instructor-led training on a variety of topics to familiarize attendees with OT equipment and environments.
- Remote access to EPRI's Cyber Security Research Lab to interact

and explore a variety of OT equipment in a safe, sandboxed environment.

- Electronic copies of all training materials used during the course, along with audio/video recordings of the course lectures, discussions, and exercises.

PROJECT HIGHLIGHTS

- Familiarize OT cyber security employees with different types of equipment commonly used in substations.
- Learn about different types of communications protocols and network monitoring tools to identify potentially malicious traffic.
- Obtain hands-on access with real equipment in a sandboxed laboratory environment, such as relays and automation controllers.
- Develop confidence in cyber security processes and technologies.
- Enhance knowledge to monitor and protect equipment from cyber attacks.

EPRI CONTACT

WILLIAM WEBB,
Sr. Technical Leader,
865.218.8132,
wwebb@epri.com

For more information, contact:

EPRI Customer Assistance Center
800.313.3774 • askepri@epri.com



Product ID 3002028332

October 2023

EPRI

3420 Hillview Avenue, Palo Alto, California 94304-1338 USA • 650.855.2121 • www.epri.com

© 2023 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER...SHAPING THE FUTURE OF ENERGY are registered marks of the Electric Power Research Institute, Inc. in the U.S. and worldwide.