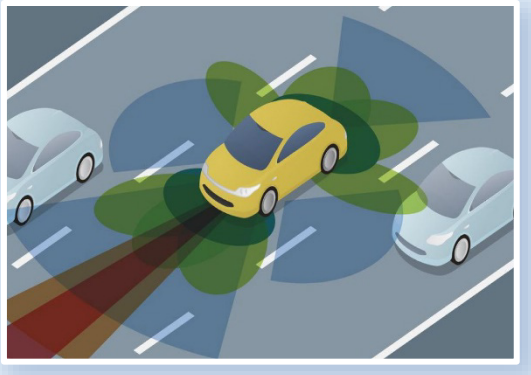
Supplemental Project Notice

OT CYBER RISK ASSESSMENTS FOR TRANSMISSION AND DISTRIBUTION OPERATIONS



PROJECT HIGHLIGHTS

- Identify the highest priority cyber risks to your OT operations to plan appropriate mitigations
- Build the baseline plan to address cyber-physical threats to critical infrastructure
- Maintain an objective risk management process to inform and strengthen your cyber security program
- Develop and justify action plans based on EPRI recommendations

Background, Objectives, and New Learnings

Drivers understand when they get in a car that there are blind spots in their vision. Mitigations include rear and side view mirrors and sensor arrays to detect objects around a vehicle. Utilities have similar problems in fully gauging their cyber security posture and capabilities within their operation technology (OT) environments. Identifying threats, strengths, and weaknesses to programs may be challenged by the diversity of SCADA vendor options, embedded security offerings, and sites with different legacy technologies and configurations. The threat landscape rapidly changes too, and emerging threats may be out of range in your risk assessments.

EPRI's Cyber Security team offers OT Cyber Security Risk Assessments that deliver an objective look at your cyber security program. EPRI experts examine a program's consideration of threats and cyber security mitigations and quantify the likelihood and impacts of existing and emerging threats in reputational, environmental, financial, safety and operational categories. These threats can be adversarial—a malicious actor, or non-adversarial—severe weather or infrastructure failure.

When a utility understands all the risks facing their program, then controls can be prioritized and implemented to effectively manage risk, appropriately protect the utility's infrastructure, and avoid the potential threat impacts.

Benefits

The OT Cyber Risk Assessment for Utility Transmission and Distribution provides an independent and comprehensive evaluation of risks that must be mitigated by your cyber security program. By identifying and evaluating the risks to the program, a utility can prioritize program improvements based on the impact or likelihood of a threat event. Utilities can use their risk assessment results to:

- Build the baseline plan to resolve the highest priority risks to your OT operations and enact appropriate mitigations
- Establish and maintain an objective and ongoing risk management process that strengthens your cyber security program

- Gain an accurate snapshot in time of risks for comparative assessments in future years
- Use recommendations to create action plans
- Eliminate blind spots in utility-run risk assessments
- Educate utility stakeholders on the potential adverse impacts of inaction to prioritized threats

Project Approach and Summary

EPRI's cyber risk assessment process starts with a discussion of utility needs to define the assessment scope—what portions of your program and organization do we look at. The risk assessment approach includes a review of your cyber security program, technologies, processes, and workforce capabilities along with cyber and physical risks.

Our researchers review relevant documents and conduct interviews with utility resources to develop an objective view of utility performance mapped to six risk impact categories.

Results are documented in a table that delivers quantifiable scores and recommendations for actions to mitigate risks on a prioritized basis. The report will also identify EPRI research results that can help inform and accelerate utility action plans for risk mitigations.

Deliverables

- Risk assessment report based on analysis of gathered information. The assessment report includes identification of risks and current mitigations.
- Action plan that details the major milestones to recommended cyber security improvements.

Price of Project

Contact EPRI for pricing. This supplemental project qualifies for Self-Directed Funding (SDF) and co-funding.

Project Status and Schedule

The project schedule is based on the scope and schedule availability of the participant's staff and facilities. A typical assessment could take up to two months. A schedule will be developed and mutually agreed upon by the project participant and EPRI. This project can be deployed on an annual or biennial basis.

Who Should Join

Utilities of any size and in any location may benefit from independent and comprehensive evaluations of risks to their cyber security programs.

Contact Information

For more information, contact the EPRI Customer Assistance Center at 800.313.3774 (askepri@epri.com).

Technical Contact

Esther Amullen at 650.855.1027, eamullen@epri.com

To Join, Contact Your Information, Communication, and Cyber Security Technical Advisor

West: Brian Dupin at bdupin@epri.com

Northeast: Barry Batson at bbatson@epri.com

Southeast: Chuck Wentzel at cwentzel@epri.com

Product ID: 3002023216 **Project ID:** 01-115856 **April 2025**

EPRI

3420 Hillview Avenue, Palo Alto, California 94304-1338 USA • 800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com