EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Power Delivery Cyber Security Tailored Assessment for Utility Transmission and Distribution Operations

Key Research Question

Utilities must objectively understand their cyber security posture and capabilities within their operation technology (OT) environments to develop the most effective cyber security plans that help ensure continued grid reliability and resiliency.

Some utilities conduct their own internal assessments based on existing models like the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) or the Department of Energy's (DOE) Cybersecurity Capability Maturity Model (C2M2) to provide that information. However, these utilities may benefit from an objective outside perspective on specific emerging topics or their internal assessment processes.

This tailored cyber security assessment methodology for power delivery systems will look closely at specific areas of your cyber security program instead of the entire program. This project can take the results from previous examinations, such as a NIST CSF or Department of Energy Cybersecurity Capability Maturity Model (C2M2) assessment and focus on select areas of concern or look at aspects of the program that have not been examined.

EPRI's assessment approach produces recommendations for improvements that may include goals, plans, and timelines.

Objective

The objective of this supplemental project is to deliver unbiased assessments that leverage EPRI expertise to examine select OT cyber security topics at utilities.

- Gain actionable information and insights to understand and improve specific aspects of OT cyber security
- Enact cyber security objectives and project plans based on utility-specific recommendations
- Access for one year to EPRI's metrics portal to benchmark important utility cyber security readiness parameters and inform risk reduction priorities

These assessments may:

- Aid utilities in prioritization of actions and development of project plans and timelines aligned to results recommendations.
- Assist in supporting justifications to all relevant stakeholders for OT cyber security investments in technologies, practices, and workforce.
- Identify trends and best practices through data analyses and observations.

Approach

Each tailored Assessment starts with identification of the module(s) listed below that will be applied to the project scope. Additional assessment modules may be added based upon participant requirements. The assessment methodology may request specific data furnished by utilities and may include surveys and other tools to collect that data.

These assessment modules cover the following programmatic and performance areas:

- Internal assessment and audit process
- Engineering design process
- Patch management and testing
- Transient cyber asset program
- Wireless access
- Remote access
- Tamper indication program
- Cyber security training
- GPS and precision timing

Research Value

Each assessment documents observations and analyses of gathered data and contains recommendations to improve cyber security aspects and help utilities prioritize actions to mitigate risks. As each participant completes improvement goals identified in the assessment report, OT cyber risks may be mitigated. This project includes one year of complementary access to EPRI's Cyber Security Benchmarker for comparative, anonymized analysis of common utility parameters.

Cyber security assessments serve the public good by offering new insights and recommendations that enhance utility cyber security programs and practices and help ensure grid reliability.

Deliverables

Each participating utility will receive:

- Confidential assessment report that documents observations, strengths, weaknesses, and prioritized opportunities for improvement based on EPRI expertise and relevant research.
- Action plan recommendations to inform project plans.
- Access for one year to the EPRI Cyber Security Benchmarker to submit data and produce benchmark reports based on anonymized data.

Price of Project

Contact EPRI for pricing. EPRI recommends a minimum of 2 modules for any utility project scope. There is no maximum number of modules that can be selected for a tailored cyber security assessment project. This supplemental project qualifies for Tailored Collaboration (TC) and Self-Directed Funding (SDF).

Project Schedule

The project schedule is based on the assessment scope and availability of the participant's resources and facilities. A typical assessment may comprise one to two months from start to finish based on the scope. A schedule will be proposed and mutually agreed upon by each project participant and EPRI.

Who Should Join?

Utilities seeking to leverage EPRI's expertise for objective evaluations of specific aspects of their OT cyber security programs should join this project. Utilities interested in benchmarking their anonymized results against other anonymized results to compare common performance parameters should join this project.

Contact Information

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

Technical Contact

Lee Watkins at 704.595.2768 (lewatkins@epri.com)

To join, contact any of the following Technical Advisors:

Northeast: Tim Anderson at 650.855.2000 (tanderson@epri.com)
Southeast: Barry Batson at 704.905.2787 (bbatson@epri.com)
Central: Chuck Wentzel, 650.855.8527 (cwentzel@epri.com)
West: Brian Dupin at 650.906.2936 (bdupin@epri.com)
International: Thomas TerBush at 202.293.6344 (tterbush@epri.com)

Product ID: 3002022419 Project ID: 1-115305-01-01 June 2021

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com