Supplemental Project Notice

INTEGRATED CYBER-PHYSICAL SECURITY FOR DISTRIBUTION AUTOMATION

Control with cyber-physical security system modifications

PROJECT HIGHLIGHTS

- Improve the physical and cyber security of automated devices
- Minimize risks associated with remotely deployed devices
- Develop methods to track entry into line deployed automated equipment enclosures
- Gain experience with emerging technologies to guide system-wide technology deployments

Background, Objectives, and New Learnings

Distribution automation (DA) equipment is typically a key component of a utility's grid modernization plan. These devices give utilities the ability to monitor and control the distribution system in a much more active and granular way.

While these devices offer advantages in reliability, flexibility, and controllability, they can also introduce risk. Since reclosers, sensors, and controls are distributed broadly across the distribution system, they are often located where they are visible and potentially accessible by the public. Each one of these remote devices could provide an opportunity for a bad actor to gain access to utility systems, disrupt operations, or vandalize utility equipment. It is important that utilities understand these risks and build appropriate systems to mitigate the risks.

Examples of unique cyber and physical security risk challenges presented by DA equipment include:

- Physical proximity and accessibility to the public
- Ground-level control enclosures
- Remote locations that could be long distances from utility personnel
- Communications to each deployed field device may provide attack vectors into a utility network
- Potential targets for theft and vandalism (batteries, hardware, controllers)

These characteristics combine into a system that has a unique mix of cyber and physical security risks.

Based on feedback from member utilities, EPRI identified a need to develop an integrated approach to cyber-physical security for field deployed controls used for distribution automation. Utilities must protect these important assets from malicious actors along with protecting against a potential cyber attacker who may attempt to use the control as location to gain access to the utility's network for malicious purposes.

The project builds on the results of laboratory testing and seeks to apply and refine the approach in the field.

Benefits

Project participants benefit from this research by refining approaches and technologies to improve the security of their automation assets and minimize risks of deploying network connections in remote

locations. Public benefits include increased reliability from a more secure automated distribution grid.

Project Approach and Summary

EPRI has developed prototypes of a cyber-physical security system for distribution automation controls and is currently testing the system in a laboratory environment. The prototype system consists of a door sensor, a security gateway, small camera with a single board computer, and an optional badge reader installed into a recloser control. The recloser control and sensors are securely connected through the security gateway via a cellular modem to mimic a utility's network connection. These components work together to build the security monitoring system:

- The door sensor monitors the state of the enclosure door and closes a contact when the door is opened.
- When the door is opened, the camera activates and acquires images of individuals at the enclosure. Images are uploaded to a remote server and are analyzed against a database of known personnel using a facial recognition system.
- The data from the sensors, camera, badge reader, and facial recognition analysis are communicated to the Security Operations Center where threats can be assessed and potential attacks isolated using advanced security orchestration and automation tools.

This project plans to demonstrate the prototype system with project participants, evaluate the capabilities in a real-world environment, and develop recommendations how the prototype system could be further refined for utility applications. The project consists of the following tasks:

- **Hardware deployment:** EPRI plans to supply equipment needed to deploy the system and provide support for field installation by utility crews.
- **Monitoring***:* EPRI plans to work with the member utility to monitor the status of the sensors and provide access to a security dashboard and email alerts where events can be monitored. The locations will be monitored for up to 24 months, and any potential intrusions will be investigated by utility personnel. Utility personnel may be asked to randomly check the status of the controls to test the system during the project.
- **Reporting:** EPRI plans to prepare a report for each participating utility documenting the demonstration and findings of interest, including options for how to expand this security monitoring to their entire fleet of field deployed controls, and how threat detection and automation platforms can be deployed on their premises. Additionally, EPRI plans to prepare a collaborative report documenting the non-proprietary findings across all demonstrations.

Deliverables

- Equipment and associated documentation required for the demonstration.
- Periodic webcasts with participants.
- Report documenting findings from field demonstrations.

The non-proprietary results of this work will be incorporated into EPRI's Distribution Systems and Cyber Security R&D program and made available to the public for purchase or otherwise.

Price of Project

The price of the project depends on the number of demonstration sites a utility plans to install.

- 5 sites: $90,000
- 10 sites: $130,000
- 20 sites: $190,000

Contact EPRI if interested in demonstrating at additional sites.

Project Status and Schedule

EPRI plans to commence installation within four months of funding the project pending utility readiness. The project's monitoring period is two years. This project can be funded over a three-year period.

Who Should Join

Distribution utilities who actively deploy communicating line devices that could demonstrate technologies to strengthen both their physical and cyber security.

Contact Information

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

Technical Contact

Luke Varner at 865.218.8179 (lvarner@epri.com)

To join, contact your Information, Communication, and Cyber Security Technical Advisor

West: Brian Dupin bdupin@epri.com
Central: Chuck Wentzel cwentzel@epri.com
Northeast: Annie Haas ahaas@epri.com
Southeast: Barry Batson bbatson@epri.com

Product ID: 3002025419 **Project ID:** 1-117162 **March 2024**

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