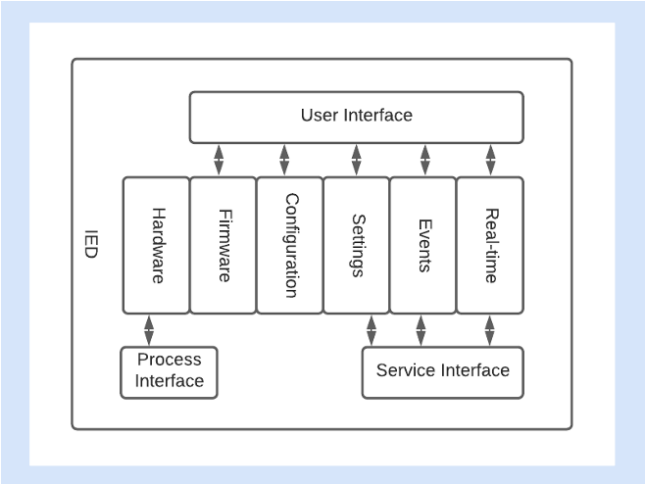
Secure IED Management Strategies



Intelligent Electronic Devices (IEDs)

- Develop a roadmap to close the Operations Technology (OT) visibility gap
- Manage compliance risk with minimal resources
- Drive Intelligent Electronic Devices (IED) procurement requirements towards more manageable systems
- Identify opportunities to enhance security controls using information from IED management systems

Background, Objectives, and New Learnings

IEDs play a critical role in the operation of power delivery systems. These systems are directly connected to the power delivery infrastructure and provide high-speed protection and control functionality. These are critical systems and are a high priority for utility personnel. However, they present a unique set of challenges that stem from their technical design and approach to device management.

In most cases, these devices are purpose-built for specific grid applications using an embedded hardware/software architecture. Various IED vendors have taken a range of different approaches toward providing common capabilities like configuration revisions and event reporting. This practice requires utilities to manage multiple different vendor-specific software tools to interface with different devices. In addition to the variability among devices from different equipment vendors, the long technology refresh cycle for this type of equipment challenges utilities to manage decades-old legacy systems alongside modern control devices.

With all the variation in protocols and interfaces among devices from different vendors developed at different times, utilities must approach IED management with device-specific solutions. This results in significant complexity for the IED management systems. As the IED management activity is increasingly automated to eliminate human error and maximize efficiency, different management systems will need to be integrated to avoid conflicts and ensure the system is configured properly.

This project will provide participants with a framework to assess management challenges associated with individual IEDs and recommend a comprehensive, integrated management strategy that is optimized for the unique fleet of IEDs installed in their power delivery infrastructure.

Integrated management capabilities include:

- Password management
- Firmware/Patch deployment
- Configuration/Settings management
- Asset tracking
- Protocol monitoring

Project Approach and Summary

Different aspects of IED management may span multiple utility organizations. To ensure all relevant processes are documented, a cross-organizational utility team should work with EPRI to document and categorize IEDs and associated management systems (vendor-provided and 3rd party).

Once the set of existing IEDs and management tools have been documented, EPRI will assess management capabilities and limitations of specific IED variations which may include

differentiation by device make, model, and firmware. Leveraging vendor documentation, lab testing, and collaboration with other members, a device-specific management strategy will be identified. The strategy will use the Secure IED Management Model developed by EPRI in previous research as a framework to capture all aspects of management and any dependencies that should be coordinated. For example, a dependency could define a relationship between automated password management and automated fault data retrieval.

Once these management strategies have been enumerated and coordinated on a single-device level, they will be rolled up to the system level to provide different options for how to optimize existing management systems in the near term and will include a plan to increase the maturity level of these systems in the future.

Benefits

- Help close the OT visibility gap
- Lower compliance risk
- Drive procurement requirements toward open standards
- Identify opportunities to enhance security controls that are customized for your environment

Deliverables

Each participating utility will receive:

- IED and Management Systems documented in a system level matrix with device-specific challenges and associated tools
- Preliminary assessment of existing management capabilities and gaps delivered in presentation format
- Final report that includes recommendations and options to comprehensively address the challenges of IED management that maximizes return on resources

Price of Project

The cost of this supplemental project is $75,000. This supplemental project qualifies for Tailored Collaboration (TC) and Self-Directed Funding (SDF).

Project Status and Schedule

The project schedule is based on the availability of both the utility employees who will be attending this course and the EPRI cyber security engineers. A schedule will be proposed and mutually agreed upon by the utility and EPRI in the project statement of work (SoW).

Who Should Join

Utilities who have plans to expand OT visibility and enhance IED management capabilities should join this project.

Technical Contact

John Stewart at 865.279.1447 (jstewart@epri.com).

Technical Advisor Contact Information

Central: Chuck Wentzel at 618.320.0011 (cwentzel@epri.com)

Northeast: Tim Anderson at 704.595.2054 (tanderson@epri.com)

Southeast: Barry Batson at 704.595.2879 (bbatson@epri.com)

West: Brian Dupin at 650.906.2936 (bdupin@epri.com)

Contact Information

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

Product ID: 3002022701 Project ID: 1-116610 April 2022

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

© 2022 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER...SHAPING THE FUTURE OF ENERGY are registered service marks of the Electric Power Research Institute, Inc.