U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Enhanced Security for the Power System Edge

Strengthen cybersecurity of grid-edge devices as they interact with each other and the cloud to enhance power system cyber-resilience

Background

Increasing deployment of intelligent field devices is changing the utility landscape. The power system is more resilient and capable as a result, and accompanying cybersecurity technologies that can detect, prevent, and mitigate cyber incidents are becoming increasingly important. For instance, as the installation of autonomous Distributed Energy Resources (DER) devices grows, intelligent distribution systems can increasingly provide for, and benefit from, real-time situational awareness of cyber-activity. Cybersecurity technologies are needed to ensure continuous cybersecurity of utility field devices whether connected to the back-end cloud, or running autonomously, to reduce the cyber-attack surface and lower the risk that a cyber-incident might interfere with energy delivery.

The energy sector community values greater interoperability and real-time power system situational awareness for equipment on the grid-edge, including distribution feeders. As shown in Fig. 1, grid-edge devices communicate with each other directly and by means of the cloud. This research will develop security enhancements that emphasize interoperability and provide for real-time situational awareness, first in the form of a secure gateway for brownfield, or legacy power system devices, then as an internal Field Programmable Gate Array (FPGA) upgrade designed as part of greenfield, or present day, devices.

Objectives

The project team is developing the Utility Distribution Edge Security architecture model to enhance the security of the edge of the utility network, shrink the cyber-attack surface and thereby reduce risk. The security architecture model offers three advantages to current architecture:

- Improvement in system security and integrity
- Improvement in the system speed and efficiency
- Applicability to existing brownfield and greenfield deployments

Project Description

The project team will first research, develop and implement an enhanced cybersecurity gateway and a security management channel for use with existing devices, communications, and networks to improve the security posture of deployed power grid endpoints. Then, the team will develop technology that can embed security into a FPGA on the endpoint itself to provide enhanced security with boosted performance.

Benefits

- Cybersecurity for grid-edge devices that use the cloud for advanced analytics, creating more cyber-resilient power grid architectures and enabling the creation of new market opportunities

Partners

- Intel Federal, LLC (lead)
- Schneider Electric
- LiveData Utilities

Period of Performance

October 2016 – December 2019

Project Cost

Total: $4,441,532

Federal: $3,253,513

Cost Share: $1,188,019

Content last updated: May 2017

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) Research and Development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of emergency disruptions due to cyberattacks.

For more information: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

Initial Leads

Carol Hawk
Program Manager

Sven Schrecker
Principal Investigator
Intel Federal LLC
858-213-4225
sven.schrecker@intel.com

Current Contact as of Aug. 2020

Akhlesh Kaushiva
Program Manager
DOE CESER
202-287-6062
akhlesh.kaushiva@hq.doe.gov

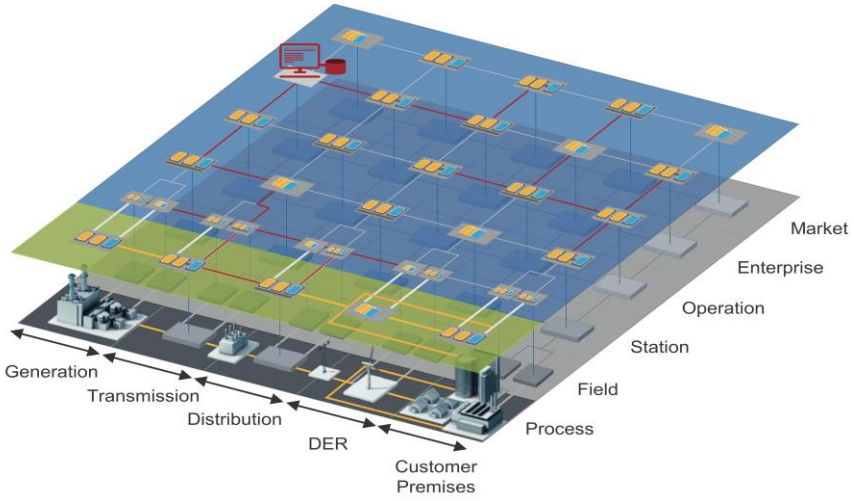

Figure 1. Protected Communication Layer Mapped onto Grid-Edge Devices and the Cloud

Technical Approach

This research will first develop a cybersecurity gateway that is physically separate from the protected device; that is, security enhancements are not actually deployed on the device itself. The gateway will act as a security proxy, to help protect legacy devices that may not have the internal resources needed to support security enhancements. The gateway creates a security layer on top of the existing operational communications, so that the protected device interacts with other network devices through the security gateway. This reduces the cyber-attack surface, so that physical access to the device, or the connection between the device and the gateway, is required to perpetrate a cyber-attack. Following successful development of the gateway, the same cybersecurity controls as found in the gateway will be implemented in an FPGA coprocessor on the power system edge device to create a trusted execution environment that isolates operational applications from the security implementation.

Separate Security and Operational Data Streams

Within the enhanced gateway security infrastructure, power system applications are logically separated and secured to support specific energy delivery functions, so that security traffic travels across a separate channel between each edge device and the back-end management instance.

Traffic is secured by policy-based trust boundaries, with each operational system accessible only to an authorized group of users and devices. Administrators can also create new secure segments as needed based on scalable Layer 2 and Layer 3 Virtual Private Networking (VPN) domains, referred to as trusted transaction spaces.

These software-defined network segments will operate securely and independently from each other, minimizing the fault domain. Within each virtual network, the gateway security infrastructure supports mutual authentication, traffic authorization, on-demand security control activation, prioritization of traffic flows, and flexible allocation of bandwidth to enable more secure, consistent performance.

End Results

Project results will include the following:

- Demonstrate security improvement leveraging interoperable security deployment at the edge of the energy infrastructure that applies to both green-field and brown-field environments.
- Reduce cyber-attack surface in a way that does not impede the normal functioning of the critical energy delivery functions.
- Provide cybersecurity gateway that is manageable from the cloud with uptime acceptable to the Industry Advisory Group.
- Continuous situational awareness that offers the asset owner with the moment-by-moment cybersecurity state of the energy delivery control systems and components, with performance acceptable to the Industry Advisory Group.