U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

SDN4EDS: Software-Defined Networking for Energy Delivery Systems

Pacific Northwest NATIONAL LABORATORY

Guidance for software-defined networking technology for the energy sector

Energy delivery system (EDS) networks contain unique engineering challenges in the areas of performance, cybersecurity, situational awareness, efficiency, complexity, and ease of use. Traditional networking technology was designed to meet business networking requirements and generally does not meet EDS requirements for autonomous operation and high levels of resilience. Software-Defined Networking (SDN) is a new paradigm in networking technology that provides the resilience, flexibility, security, and adaptability required to meet EDS network needs. This project increases the adoption of SDN technologies by providing a comprehensive blueprint and a proven secure reference architecture for how SDN technology can be deployed in the energy sector to improve network resiliency beyond traditional Ethernet networks. This research has shown how traditional network security products, such as intrusion detection systems, can be integrated into an SDN environment. The team has also enhanced a software tool that can help utilities define, distribute, and enforce the behavior for common EDS protocols.

KEY TAKEAWAYS

- Builds trust and interoperability across software-defined networking products to increase cybersecurity for all levels of energy delivery system networks
- Creates a software tool for utilities to centrally define, distribute, and enforce traffic and protocol behavior for common energy delivery system protocols
- Provides a blueprint reference architecture for implementing software-defined networking in real world conditions

OUTCOME

This project will lead to higher adoption of SDN technologies in EDS environments to improve network resiliency and cybersecurity. The research has demonstrated that SDN improves security for local area networks by decreasing the attack surface and improving situational awareness. It has shown interoperability of software and hardware of various vendor products. Project results are captured and published in a Blueprint Reference Architecture document that allows industry to easily implement their own SDN test environment based on the testbed developed for this project, enabling them to further investigate SDN technology with their own equipment and configurations.

PARTICIPANTS	ROLE
Pacific Northwest National Laboratory	Coordinates all project activities; establishes and maintains the SDN laboratory environment; develops blueprint document
SEL Schweitzer Engineering Laboratories	Provides hardware and software environments used for the project; contributes to the development of the blueprint document.
Juniper Networks	Contributes to the development of the wide-area networking component of the blueprint document
Southern California Edison – Energy for What's Ahead	Provides content to the blueprint document
California ISO – Shaping a Renewed Future	Provides content to the blueprint document
dispersive technologies	Provides content to the blueprint document
Sandia National Laboratories	Provides red team analysis of the SDN environment and contributes to the development of the blueprint document
– *U.S. Indo-Pacific Command*	Provides content to the blueprint document
Spectrum Solutions	Develops and provides a situation awareness tool for viewing SDN metrics
NREL – National Renewable Energy Laboratory	Provides an end-point site for a wide-area network connection to simulate a distributed energy resource

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Scott Mix
Principal Investigator
Pacific Northwest National Laboratory
509-371-6853
scott.mix@pnnl.gov

Current Contact as of February 2020:

Akhlesh Kaushiva
Senior Technical Systems and Cybersecurity Advisor
Department of Energy (DOE)
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
202-287-6062
Akhlesh.Kaushiva@hq.doe.gov

Period of Performance: September 2017 – June 2021

Total Award Value: $2,500,000
DOE Share: $2,500,000
Cost Share: $0

CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS (CEDS)

CEDS projects are funded through DOE CESER, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyberattacks.

Website: https://www.energy.gov/ceser

Date Written: June 2021