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

Network Function Insertion for Reliable and Secure Control Messaging Over Commodity Transport

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Deploying infrastructure-agnostic secure communication solutions for energy delivery systems

Encrypting communication between energy delivery systems (EDS) devices and networks is made difficult by both physical and financial barriers. The research team overcomes these obstacles by designing and implementing a network function that can be deployed into existing EDS networks without infrastructure disruption. The function provides both reliable and secure EDS communications over untrusted networks irrespective of the capabilities of the existing endpoint equipment. As a result, the implementation of secure, reliable transport is no longer dependent upon the actual industrial hardware. This solution provides agility in responding to new threats without downtime of production equipment or waiting for vendor upgrades. It also allows continual monitoring of network data to ensure the injection of new security protocols when needed, without impacting production sensor or control equipment. This establishes secure and reliable communication between EDS devices, regardless of pre-existing infrastructure.

KEY TAKEAWAYS

- Creates a function-based solution to securing both new and legacy infrastructures across energy delivery system networks
- Guarantees energy delivery system security regardless of hardware and communication protocols
- Monitors network security and rapidly implements required function updates

OUTCOME

This project overcomes fundamental and systemic barriers to EDS network security, including infrequent or delinquent software updates and the inability to secure legacy system components. EDS operators are able to deploy the network function on any existing infrastructure to implement secure communication between previously unsecured devices and inject rapid security updates, even when component hardware is no longer supported by the vendor.

PARTICIPANTS	ROLE
CREDC CYBER RESILIENT ENERGY DELIVERY CONSORTIUM	The CREDC performs multidisciplinary research and development that focuses on the cybersecurity of energy delivery systems. The central project goal is to create an ecosystem where research results lead directly to the development of applications and methodologies, which are then validated in realistic contexts.
UNIVERSITY of HOUSTON	Leads research, development, and testing
SEL SCHWEITZER ENGINEERING LABORATORIES	Engages stakeholders

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Deniz Gurkan
Associate Professor
University of Houston
713-743-4037
dgurkan@central.uh.edu

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

This is a subproject sponsored by the CREDC academic consortium, led by the University of Illinois.

CREDC Period of Performance: October 2015 – May 2022

CREDC Total Award Value: $28,099,258
DOE Share: $22,476,290
Cost Share: $5,622,968

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