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

Adaptive and Proactive Security Assessment on Energy Delivery Systems

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Customizable framework for automated energy delivery system security monitoring and countermeasure implementation

This project provides a customizable framework for modeling security requirements for complex energy delivery systems (EDS), and for monitoring, assessing, and implementing first-response countermeasures for adaptive EDS security. The researchers are developing an EDS Security Automated Tool (EDS-SAT) that maintains a repository of security requirements, known vulnerabilities and exposures that can be used to analyze each stakeholder's unique needs. The repository considers relationships between common components to offer a customized process-driven workflow that dynamically collects and analyzes security data within each unique EDS implementation. EDS domain experts and security officers may leverage the information to perform various types of security-related assessments based on continuous real-time information. They can also develop new security measures in the EDS domain based on the information obtained in the EDS-SAT.

KEY TAKEAWAYS

- Provides support for the efficient monitoring of energy delivery system data to effectively assess system-specific security risks
- Allows operators to evaluate the state of their infrastructure against security requirements
- Prevents, detects, and mitigates security risks across diverse implementations of existing and emerging technologies

OUTCOME

This project delivers a comprehensive, automated, and self-iterative security assessment tool that is applicable to unique EDS infrastructures with varying security considerations. The tool, which utilizes both collecting and processing modules, will enable EDS operators to assess current system states, collect evidence of security incidents, identify potential security techniques and ascertain improvements, and implement first-response countermeasure tools for enhanced, customized EDS security.

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.
ASU Arizona State University	Lead Institution; designs, develops, and verifies the EDS-SAT tool.
BERKELEY LAB	Collaborator; serves as subject domain experts in security incidents in EDS
Pacific Northwest NATIONAL LABORATORY	Collaborator; provides validation of EDS-SAT

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Gail-Joon Ahn
Professor
Arizona State University
480-965-9007
Gail-Joon.Ahn@asu.edu

Ziming Zhao
Assistant Research Professor
Arizona State University
Ziming.zhao@asu.edu

Anna Scaglione
Site Lead, Professor
Arizona State University
607-227-0401
Anna.scaglione@asu.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