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

Federated Simulation for Development of Improved Incident Detection and Management

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

An accessible simulation platform for cutting-edge security control research, testing, and validation

The use of smart devices in energy delivery systems (EDS) creates a need for real-time coordination among interdependent systems. To secure these highly complex and distributed smart grid infrastructures, EDS operators and security researchers require detailed simulations of grid components to assess the impact of new security measures on system behavior. The research team is developing federated simulations of power systems and their underlying cyber infrastructure, coupled with real-time information-sharing and coordination mechanisms. In addition, they are producing publicly available synthetic case models and case studies for use within these simulation environments. Energy sector operators and researchers will be able to utilize the environments to develop effective analytics and visualizations that can be used to detect security incidents, intervene, and expeditiously recover.

KEY TAKEAWAYS

- Builds detailed simulations and information-sharing mechanisms for operators of interconnected energy delivery system components
- Develops effective analytics and visualizations for cyber event detection, intervention, and recovery
- Publishes case models for coordinated power grid security experimentation

OUTCOME

This project expands security and research potential across the increasingly complex energy sector. It delivers an interactive, expandable, and coupled simulation platform. EDS operators and security researchers can study algorithms for real-time incident detection and analysis, test and verify new theories, and conduct and share other cybersecurity research for EDS.

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.
ILLINOIS	Leads research, development, and testing
SEL SCHWEITZER ENGINEERING LABORATORIES	Engages industry stakeholders
Ameren ILLINOIS	Provides utility testbed

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Thomas Overbye
Professor Emeritus
Texas A&M
979-458-5001
overbye@tamu.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