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

Proactive Response Strategy for Energy Delivery Systems

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Developing intrusion resilience and adaptive response and recovery capabilities for energy delivery system operators

Intrusion resilience capabilities in energy delivery systems (EDS) aim to preserve service during unauthorized intrusions. Fast-spreading intrusions are a critical threat to EDS that lead to degradation of system integrity and service availability. Researchers will design intrusion alert capabilities within system-level sensors that can inform proactive response strategies. The team will implement theoretically proven algorithms that monitor EDS for anomalous behavior, service degradation, and evidence of commonly known attacks. Proactive response algorithms allow an EDS to detect attacks, contain an intrusion, and maintain system operations until recovery is possible. This system reduces the manual load of monitoring alerts by human operators and provides semi-automated response suggestions.

KEY TAKEAWAYS

- Develops an intrusion-resilience framework for energy delivery systems that adaptively reacts and protects against malicious attacks in progress
- Combines offline knowledge about network topology with online alerts and measurements from system-level and physical sensors to enhance energy delivery system security
- Operationalizes a security-focused data collection and analysis framework

OUTCOME

The Proactive Response Strategy for EDS project develops a theoretically proven, semi-automated framework for detecting and responding to malicious cyber events. The goal of the intrusion-resilient system design is to adaptively react against malicious attacks in real time, given offline knowledge about the network's topology and online alerts and measurements from system-level and physical sensors.

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 ILLINOIS URBANA-CHAMPAIGN	Leads research, development, and testing
OSIsoft.	Engages stakeholders

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

William H. Sanders
Professor
Carnegie Mellon University
sanders@cmu.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