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

Real-Time Cyber Analysis to Improve Operational Response to a Cyber Attack

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

A security database and response simulation tool to streamline critical decision making in real-time

Energy delivery system (EDS) operators face many uncertainties when identifying and mitigating cyberattacks. While EDS operators have multiple guidelines for protecting their environments from a cyber incident, they are only helpful if the operator can access them effectively in real time to respond to a crisis. The research team is developing an operational response tool for EDS operators to simulate cyberattacks and analyze the consequences of their decisions. This simulation tool allows operators to prepare for future cyberattacks and make effective decisions when responding to live cyber incidents. The simulator considers existing industry standards and best practices, empirical evidence, and the operator's specific physical infrastructure to propose possible responses. All cases will be saved into the database for future use.

KEY TAKEAWAYS

- Compiles and makes available a database of response strategies from observed and hypothetical cyber-attack cases
- Delivers a tool for energy delivery system operators to prepare for cyberattacks through simulations and make optimal decisions in real-time during live attack scenarios
- Provides a range of possible response plans on a unified platform, while recording results of simulations and iterating responses through empirical evidence

OUTCOME

The tool developed in this research will continually improve its understanding and simulations of EDS operator environments, even as new components are introduced. The attack simulation will allow operators to better understand their behaviors and provide insights about effective strategies to improve performance to more efficiently and effectively respond to live attacks.

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.
Massachusetts Institute of Technology	Lead institution; tests the simulation tool at the MIT cogeneration facility
AUSTIN ENERGY®	Provides industrial control system testbed
Pacific Northwest NATIONAL LABORATORY	Provides industrial control system testbed

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Michael Siegel
Principal Research Scientist
Massachusetts Institute of Technology
617-253-2937
msiegel@mit.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