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

Situational Awareness Framework for Cybersecurity Event Prediction and Quantifications

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Comprehensive energy delivery system assessment, visualization, and simulation for cutting edge preparedness against cyberattacks

Energy asset owners and operators do not have the capability to fully understand the risks associated with the cyber threats of today and tomorrow—risks that will continue to grow as information technology and operational technology networks increasingly merge. Without a better understanding of these risks, costs, and potential consequences, appropriate allocation of capital is a big challenge. This project investigates a risk modeling and data analytics platform that identifies risk tolerance and strategy for assessing, responding to, and monitoring cyber security risks on a simulation platform, which will help energy executives direct capital to the areas of greatest concern.

KEY TAKEAWAYS

- Leverages the situational awareness framework for risk ranking methodology to identify system risk tolerance levels and critical preparedness measures
- Simulates energy infrastructure to optimize security and mitigation strategies before live implementation
- Identifies organization-wide security concerns including engineering, controls, and disruption scenarios

OUTCOME

The data collection and analysis methods developed through this research enables energy system operators to make sense of more complex data across multiple organizations. This project identifies and classifies risks to energy systems for more effective preparedness and efficient response capabilities.

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	Leads research, development, and testing

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Abel Sanchez
Executive Director,
MIT Geospatial Data Center
Massachusetts Institute of Technology
617-452-3211
doval@mit.edu

John Williams
Professor
Massachusetts Institute of Technology
617-253-7201
jwr@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