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

Real-Time Situational Awareness of Risk to EDS to Cyber Attack

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Building a methodology for protecting electric grid components from cyber-induced cascading failures

Energy Delivery System (EDS) vendors and operators must implement and validate preparedness measures to protect electric grid infrastructure against cyberattacks and cyber-physical cascading failures. However, current assessment techniques for understanding system resilience require separate analysis of physical and cyber components, leading to gaps in situational awareness. This project develops a methodology to assess the risk of cyberattack-induced cascading failures, taking into consideration the complex cyber-physical interdependencies of energy delivery infrastructure. In the long-term, this project provides real-time situational awareness of threats by developing and implementing a standardized metric for how far or close a given grid system is to a cyber-induced cascading failure, and how to mitigate this emergency scenario. This methodology will be validated using realistic cyber-physical models in simulation and emulation testbeds.

KEY TAKEAWAYS

- Develops accurate models, algorithms, and metrics to comprehensively analyze energy delivery system resiliency to cascading failures
- Implements a technological solution to conduct system analyses, assess impacts of potential vulnerabilities, issue alerts, and suggest redemptive action in real-time
- Creates a more accurate understanding of potential risks to electric grid cyber-physical components

OUTCOME

This project advances EDS resiliency and situational awareness assessment by leveraging prior work on EDS cascading failure modeling to address complex cyber-physical interdependencies across electric grids. It develops a tool that can make real-time assessments of the potential impact of cyber vulnerabilities and facilitates logical remedial actions.

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.
Oregon State University	Leads research, development, and testing
accenture	Engages stakeholders

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Rakesh Bobba
OSU Site Lead
Assistant Professor
Oregon State University
541-737-3333
Rakesh.Bobba@oregonstate.edu

Eduardo Cotilla-Sanchez
Assistant Professor
Oregon State University
541-737-8926
ecs@oregonstate.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