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

Security Gaps due to Coupling of Energy Delivery Sub-Systems

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Strengthening system communication and security for an increasingly interdependent energy architecture

This research addresses vulnerabilities created by three critical system interdependencies across the energy sector: natural gas used in electricity generation, new resources and privately owned components that interact with the power grid, and third-party energy data management. Natural gas fuels electricity generation. If a critical vulnerability is exploited in either system, the interconnections between them may result in an inter-domain attack. Similarly, many recently introduced resources, such as electric vehicle charging stations and solar power control networks, maintain high-voltage connections with the local power grid and are often managed and monitored by third parties. An attack against any of these resource components may disrupt power quality or distribution across the greater region. Finally, the collection of some energy delivery system (EDS) data is externally managed by third-party companies. Interrupting communications between these entities and the EDS infrastructure will create operator blindness to the EDS system state. The research team will assess and mitigate the risks to EDS created by coupled infrastructures by developing and validating open source tools for inter-domain communication that identify disruptions, instabilities, and vulnerabilities, triggering remedial actions across these inter-connected systems.

KEY TAKEAWAYS

- Identifies potential vulnerabilities within interconnected sub-systems to minimize cybersecurity risks introduced at the interface
- Improves communication and information sharing protocols for complex energy delivery systems and devices
- Develops and validates a tool for collaborative system modeling and security planning

OUTCOME

The open-source software developed by this project enables interconnected entities to co-simulate their networks for collaborative security and cyberattack response planning. This will provide the tools necessary to minimize cybersecurity risks between coupled entities as EDS infrastructure becomes increasingly complex and interdependent.

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.
ASU Arizona State University	Leads research, development, and testing

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Anna Scaglione
Site Lead, Professor of Electrical and Computer Engineering
Arizona State University
607-227-0401
anna.scaglione@asu.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