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

Towards Attack Resilient Data Analytics for Power Grid Operations

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

An analytics-based approach to surviving cyberattacks while sustaining critical network functions

Energy delivery systems (EDS) remain resilient against cyberattacks by initiating real-time contingencies such as microgrid islanding, relay tripping, and load shedding to minimize impacts and maintain service delivery. However, these controls are data-dependent and may be exploited by an adversary through data integrity attacks that produce malicious control decisions. Currently, the resiliency of power system analytics against data integrity attacks is not considered standard practice for grid operations. In this project, the research team fills this gap by developing resilient data analytics to detect and mitigate the impact of compromised data on EDS contingency operations such as microgrid islanding and load shedding. This project develops techniques for improved, reliable, and scalable resiliency.

KEY TAKEAWAYS

- Develops a technique to predict stable islanding and reconnection timings in a way that is resilient to data integrity attacks
- Utilizes resilient analytics to advise reliable load shedding and relay operating schemes
- Mitigates the risk of enacting security contingencies based on maliciously injected data

OUTCOME

This project expands EDS resiliency toolkits through data-driven decision-making methodologies that use existing system components, as opposed to requiring costly hardware updates. These EDS components will use highly secure analytics to execute protective action against cyberattacks.

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 the research initiative to develop data analysis algorithms
PACIFIC POWER	Engages utility stakeholders
SEL SCHWEITZER ENGINEERING LABORATORIES	Provides a Schweitzer Engineering Laboratories real-time automation controller for research algorithm testing
Portland General Electric	Tests and benchmarks research algorithms on a distribution network model

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

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