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

Supporting Security with Advanced Multimodal Grid Data Analytics

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Improving cyber-physical sensor data integrity and analysis for attack preparedness

Energy delivery systems (EDS) rely on a network of physical sensors to automate processes and identify potential cyber intrusions. However, these sensors are susceptible to noise interference and often communicate via unsecured protocols, undermining data quality and integrity, as well as system security. This project introduces a Grid Security System (GSS) to bridge the gap between the cyber and physical worlds. The research team leverages high-resolution measurements from micro-synchrophasors — synchronized, fast-sampling devices, developed to do real-time measurements in the distribution grid — to analyze sensor data for anomalies indicative of both cyber and physical signatures of attacks. These advanced sensing modalities will provide high-quality, reliable data to enhance EDS security and strengthen intrusion detection analytics.

KEY TAKEAWAYS

- Bolsters energy delivery system security and guarantees sensor data quality to improve forensic analysis
- Incorporates advanced micro-synchrophasor technology for real-time cyber-physical intrusion detection
- Enhances anomaly detection and timely attack response time in distribution systems

OUTCOME

The implementation of micro-synchrophasors components delivers an affordable solution for enhancing EDS sensor data integrity and security, overcoming financial barriers that have limited similar advances. By assessing the quality of data used to conduct forensic analyses, the GSS minimizes false positive detections of data anomalies, allowing EDS operators to increase their preparedness against known attacks and decrease response time.

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.
Arizona State University	Lead Institution; develops algorithms which analyze data from micro-synchrophasors to detect anomalies.
PSL POWER STANDARDS LAB	Micro-synchrophasor manufacturer; develops use cases
WATER | ENERGY | LIFE CITY OF RIVERSIDE PUBLIC UTILITIES	Provides access to micro-synchrophasor data
EPRI ELECTRIC POWER RESEARCH INSTITUTE	Engages stakeholders
EnerNex A CESI Company	Assists in attack scenario development
OSIsoft.	Engages stakeholders

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