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

Deep Cyber-Physical Situational Awareness for Energy Systems: A Secure Foundation for Next-Generation Energy Management

Texas A&M Engineering Experiment Station

Next generation secure energy management system from devices to control centers

This project develops a next generation secure energy management system that co-manages and analyzes energy delivery and cyber communication network architectures. It provides a unified cyber-aware and physics-aware secure data flow pipeline that extends from end-devices out into the field and up through the applications in a control center's energy management system to provide security and resilience. The team is developing deep cyber-physical situational awareness via monitoring and characterization of components and events across the system in both physical and cyber infrastructures. The system is able to design and establish customized cybersecurity measures based on identified cyber-physical threats, delivering clear and accessible cybersecurity analytics to utility owners and operators.

KEY TAKEAWAYS

- Designs a secure, next-generation cyber-physical energy management system that detects malicious and abnormal events through the fusion of cyber and physical data
- Builds an end-to-end secure architecture for managing the energy system, communications, security, and cyber-physical grid modeling and analytics
- Creates power system applications that are inherently cyber aware

OUTCOME

This project uses deep visibility to design a next generation secure energy management system that enables stakeholders across energy industrial control domains to better prepare, mitigate, repair, and recover from cyber threats. A key focus is the visibility of cyber-physical threats, the understanding of those threats, and clarification capacity of cyber security analytics, as well as energy impact prioritization to design and establish countermeasures.

PARTICIPANTS	ROLE
TEES | Texas A&M Engineering Experiment Station	Project lead; provides expertise in cyber-physical power systems modeling and analysis; provides lab and research personnel, facilities, equipment, supplies, and services
RUTGERS	Develops and applies cyber-physical modeling; provides expertise in the embedded system security side and cyber-physical resilience
UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN	Provides expertise on security solution practicality; facilitates industry interactions, including demonstrations
Sandia National Laboratories	Develops and tests a mathematical framework for characterizing grid components/devices for input into overall energy management system design; develops the online response mechanism
Pacific Northwest NATIONAL LABORATORY	Uses cyber-physical protection system modeling and evaluation for cyber risks experience to leverage operator insights and expertise on hardware-in-the-loop testbeds

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Katherine Davis
Principal Investigator
Texas A&M Engineering Experiment Station
979-458-5093
katedavis@tamu.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

Period of Performance: October 2018 – December 2021

Total Award Value: $2,745,830
DOE Share: $2,049,883
Cost Share: $695,947

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