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

Cyber-Secure Power Router

SEEDS
CYBERSECURITY CENTER FOR SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS

Developing a reference design for a preproduction prototype that is secure against attacks at the physical and communication layers

The project team is developing new adaptive technologies that allows for the secure distribution and control of attack resilient grid connected by introducing security during the hardware development process. The team is developing a reference design for a preproduction prototype that is secure against attacks at the physical layer and the communication layer. The project integrates multiple layers of security into the architecture employing numerous mitigation strategies such as encrypted communication and hardware storage of encryption algorithms. The attack detection, location, and mitigation algorithms designed through this effort address challenges specific to cyber-physical devices.

KEY TAKEAWAYS

- Integrates layers of security as the controller board is developed to ensure cyber-hardening by design
- Uses a trusted platform module to enhance device security by generating encryption and storing encryption algorithms
- Develops an interface that allows for secure communication with, and control of, cyber-physical devices

OUTCOME

The resulting cyber-physical device has a communication layer, control layer, and hardware layer. The communication layer consists of a Trusted Platform Module that ensures all communication is encrypted and is secure from various network communication attacks. The control layer ensures that invalid inputs cannot compromise the system. The hardware layer ensures the hardware is available using shoot-through protection.

PARTICIPANTS	ROLE
SEEDS CYBERSECURITY CENTER FOR SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS	This project is part of the Secure Evolvable Energy Delivery Systems (SEEDS) academic consortium. SEEDS researches and develops innovative cybersecurity technologies, tools, and methodologies to advance the energy sector's ability to survive cyber incidents while sustaining critical functions.
UNIVERSITY OF ARKANSAS	Designs, builds, and develops a cyber-secure physical system

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Dr. Alan Mantooth
Distinguished Professor
University of Arkansas
479-575-4838
mantooth@uark.edu

Dr. Chris Farnell
National Center for Reliable Electric Power Transmission
University of Arkansas
479-575-4487
cfarnell@uark.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 SEEDS academic consortium, led by the University of Arkansas.

SEEDS Period of Performance: October 2015 – March 2022

SEEDS Total Award Value: $15,309,114
DOE Share: $12,226,504
Cost Share: $3,082,610

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