

SEEDS: Cybersecurity Center for Secure Evolvable Energy Delivery Systems



Research and development of solutions for cyber vulnerabilities across energy delivery systems

The Secure Evolvable Energy Delivery Systems (SEEDS) Center is an academic consortium led by the University of Arkansas that supports research and develops innovative cybersecurity technologies, tools, and methodologies that advance the energy sector's ability to survive cyberattacks and incidents while sustaining critical functions. SEEDS verifies and validates the efficacy of the developed solutions and methodologies for transition to practice and across the energy delivery system by protecting hardware assets, making systems less susceptible to cyber threats, and providing reliable delivery of electricity, oil, and natural gas. The Center has a membership-based Industrial Advisory Board that makes recommendations regarding industry needs. SEEDS is co-funded with DOE by the Department of Homeland Security Science and Technology Directorate.

KEY TAKEAWAYS

- Establishes and supports an academic consortium of energy delivery system cybersecurity researchers
- Produces solutions to increase the survivability of critical electricity and oil and natural gas systems during cyber incidents
- Engages an Industrial Advisory Board to coordinate research and development efforts with industry needs

OUTCOME

By March 2022, SEEDS will be a self-sustaining, membership-based center to enable the continued development of cyber technology and to transition technologies to the energy sector. The research and development activities sponsored by the Center propagates a highly qualified student workforce that is industry-ready to support energy delivery cybersecurity.

PARTICIPANTS

ROLE



Lead research institution; implements consortium funding and administration; performs research and development (R&D) on cyber risk assessment, attack detection, secure communications, and device hardening



University research institution; performs R&D on cyber risk assessment, incident response, and visualization



University research institution; performs R&D on cybersecurity in power grid communications, renewable generation, demand response, and oil and natural gas systems



University research institution; performs R&D on secure substation-related communications, key management, and attack detection



University research institution; performs R&D on topology and false data injection attacks



Electric Cooperatives
of Arkansas

Utility partner for research, demonstration, and validation

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

H. Allen Mantooth
Principal Investigator
University of Arkansas
202-287-6062
mantooth@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

Period of Performance: October 2015 – March 2022

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: September 2021