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

Next-Generation Attack-Resilient Electricity Distribution Systems

Argonne NATIONAL LABORATORY

Mitigating vulnerabilities and securing energy distribution systems for reliable operation

Energy distribution management systems (DMS) and associated monitoring and control systems are critical for making decisions and exchanging information between energy components. However, existing cybersecurity technologies employed in distribution systems are still vulnerable to cyberattacks. As the deployment of distributed energy resources, microgrids, and advanced metering infrastructure expands, so does the attack surface for DMS infrastructures. This project develops and evaluates a holistic attack-resilient DMS control architecture to facilitate cyberattack prediction, detection, mitigation, and adaptation in the context of next-generation electricity distribution systems. The team identifies and analyzes vulnerabilities and interdependencies in DMS architectures to develop rapid response and restoration methodologies that support the seamless coordination among heterogeneous systems under known and unknown cyber incidents.

KEY TAKEAWAYS

- Conducts comprehensive review of distribution management system architecture and applications and perform cybersecurity vulnerability and impact analysis using attack tree models and a dedicated simulation platform
- Develops attack-resilient awareness, detection, and mitigation strategies at the device, application, and system levels
- Ensures uninterruptable operation, secure information sharing, and coordination among energy distribution management systems and components

OUTCOME

This project greatly improves the cyber-resilience of next-generation distribution systems and significantly increases deterrence against adversaries. It simplifies and enhances the cybersecurity and interoperability of DMS systems and functions for applicability across multiple existing and future architectures.

PARTICIPANTS	ROLE
Argonne NATIONAL LABORATORY	Performs DMS architectural cybersecurity analysis and impact analysis; develops attack-resilient awareness, control, and mitigation strategies

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Ravindra Singh
Principal Investigator
Argonne National Laboratory
630-252-4337
ravindra.singh@anl.gov

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 2017 – December 2021

Total Award Value: $1,592,448
DOE Share: $1,592,448
Cost Share: $0

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: May 2021