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

Security Enhancements for Distributed Energy Resource Systems in Standardized Institute of Electrical and Electronic Engineers 1547 Environments

Bolstering cybersecurity while applying energy resource interoperability standards

This project is researching, developing, and validating methods for secure distributed energy resource (DER) facility interconnection and operation based on the Institute of Electrical and Electronic Engineers (IEEE) standard 1547. This standard introduces requirements for coordinated control and interoperability of several geographically co-located DER units. Facilitating the integration of DER components into the power grid enables easier aggregation, control, sale, and distribution of alternative and distributed energy, such as wind and solar, but also increases DER vulnerability to cyberattacks. The team will identify harmonized cybersecurity requirements across multiple standards and frameworks, analyze measurement redundancies across interfaces, develop secure architectures and distributed stability controls, and provide guidance to secure adoption of the IEEE 1547 revision with best-practice recommendations and a reference implementation.

KEY TAKEAWAYS

- Develops an architecture to secure points of physical and logical connections to distributed energy resources including interoperable management systems for verifiable consensus decisions among components
- Develops approaches to provide aggregated distributed energy resource plant response to maintain voltage and frequency stability in cyber-adversarial environments
- Improves secure communication profiles for IEEE 1547 environments

OUTCOME

The project team will demonstrate and recommend cybersecure, infrastructure-agnostic methods and best-practices to advance DER interoperability in compliance with the revised IEEE 1547 standards. Revisions of the standards will be codified and provided as open-source reference use cases to facilitate implementation for current or planned DER installations.

PARTICIPANTS	ROLE
ABB	Conducts project management; main contributor of project resources; develops secure mechanism for implementing the aggregated DER plant model and security extensions for IEEE 1547 protocols
UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN	Leads research in threat modeling, cyber-physical approaches to attack detection and mitigation, stability control in adversarial environments, and reachability analysis
DUKE ENERGY®	Provides guidance on the usability and practicality of the system; serves as the utility partner in the demonstration phase of the project
OAK RIDGE National Laboratory	Conducts independent red team testing

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Dmitry Ishchenko
Principal Investigator
Hitachi ABB Power Grids
919-856-3915
dmitry.ishchenko@hitachi-powergrids.com

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 – September 2021

Total Award Value: $3,358,734
DOE Share: $2,506,987
Cost Share: $851,757

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