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

Cyber Resilient Flexible Alternating Current Transmission Systems

Continuous comparative analysis of system voltages, currents, and power flows for physics-based cybersecurity

This project researches, develops, and demonstrates defense-in-depth cybersecurity solutions for flexible alternating current transmission system (FACTS) devices to mitigate and eliminate outsider and insider threats in transmission power grids. The methods and systems developed leverage the unique and dynamic responses of FACTS devices and systems to identify and alert operators to any malicious commands acting on the device. The team detects threats to FACTS devices and their interfaces with supervisory control and data acquisition (SCADA) and wide area monitoring, protection, and control (WAMPAC) systems by correlating signatures of FACTS voltages and currents from different measurement points. These solutions establish command and measurement benchmarks, assess the system's state based on physical models, and analyze large signal transients with compensation equipment to identify inconsistent and malicious inputs. To validate these systems, ABB will deploy them in FACTS controllers, SCADA and energy management system (EMS) application servers, and WAMPAC servers in a substation environment.

KEY TAKEAWAYS

- Develops physics-based technology to deliver real-time detection and accommodation for cyberattacks against flexible alternating current transmission system controllers and devices
- Aggregates data from various sources to create a hybrid intrusion detection and moving target defense system
- Creates a firmware update to secure devices from control by adversaries with malicious intent

OUTCOME

This project provides domain-based cybersecurity defense mechanisms for FACTS devices, FACTS systems, and their interfaces with WAMPAC systems and SCADA, securing them from adversarial control. It advances the cybersecurity of FACTS devices with new firmware by feeding changes in data to defense mechanisms for threat analysis. The final cybersecurity solutions will be incorporated into future Hitachi ABB products.

PARTICIPANTS	ROLE
ABB	Deploys and tests the cybersecurity functions in a FACTS controller, develops the functions needed to secure a FACTS station, and integrates the cybersecurity functions developed by its partners in SCADA/EMS and WAMPAC into application servers in network management and substation automation
ILLINOIS	Develops security solutions against cyberattacks originating from WAMPAC and other higher-level controllers aimed at controlling FACTS and their stations
IOWA STATE UNIVERSITY	Secures the SCADA system against cyberattacks aimed at compromising operations of FACTS devices; develops a hybrid technique that employs moving target defense and anomaly detection to complement information technology security solutions

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Reynaldo Nuqui
Principal Investigator
ABB
919-807-5039
reynaldo.nuqui@us.abb.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: $3,235,021
DOE Share: $2,490,780
Cost Share: $744,241

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