U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Integration of Green Renewable Energy Sources Securely with Buildings and Electric Power (INGRESS)

Securing renewable resources in the built environment

Background

Energy delivery system cybersecurity is critical to energy distribution and delivery. As technology advances, it is increasingly important to design systems that are resilient and can survive sophisticated, evolving cyber-attacks. Distribution system and building owners and operators could benefit from improved cybersecurity situational awareness, within energy distribution systems, to assist them in identifying a cyber-attack on these control systems and in determining whether an identified cyber-attack could degrade grid stability and operations.

Objectives

The project team will research, design, and develop an open-source, inline, advanced cyber-attack detection and resiliency-enabling building and grid cybersecurity platform deployable for legacy and emerging behind-the-meter Distributed Energy Resources (DER). The platform will build and continuously improve upon models of equipment to automatically identify and prevent malicious control commands or DER operations in real time. The platform will also support secure and interoperable communication with electric utilities and building control and management systems.

Project Description

The Integration of Green Renewable Energy Sources Securely with Buildings and Electric Power (INGRESS) project will enhance building and grid resiliency to cyber-attacks and improve reliability by advancing state-of-the-art, model-based validation of control system traffic. INGRESS will prevent malicious control commands, which could affect grid operations, from being issued to various types of behind-the-meter equipment. It will detect a cyber-attack from the grid-edge. The team will develop algorithms to sense electric power grid health from the edge, and then draw correlations with corresponding observations from the building management systems. This project will achieve interoperability among DERs, building management systems, and utility operations by leveraging the Open Field Message Bus (OpenFMB) framework. It will enable both hardware and communication layer cybersecurity capabilities by leveraging the security features available through the OpenFMB framework and VOLTTRON information exchange bus. VOLTTRON is DOE's reference platform for transactional energy applications. INGRESS will also enable non-intrusive retrofitting of security into legacy environments by implementing the bump-in-the-wire (BITW) solution.

Benefits

- Cost-effective and non-intrusive BITW technology that transparently augments security into legacy and emerging DER systems.
- Interoperability with a variety of different vendor network, hardware, software, and control devices.
- Advanced cyber and physical attack detection and resiliency capability for the grid-edge.

Partners

- United Technologies Research Center (UTRC), lead
- University of Illinois at Urbana - Champaign
- Pacific Northwest National Laboratory (PNNL)

Period of Performance

October 2016 – September 2019

Project Cost

Total: $3,521,324

Federal: $2,614,008

Cost Share: $907,316

Content last updated: May 2017

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) Research and Development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of emergency disruptions due to cyberattacks.

For more information: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

Initial Leads

Carol Hawk
Program Manager

Devu Manikantan Shila
Principal Investigator
UTRC
860-610-7198
manikad@utrc.utc.com

Current Contact as of Aug. 2020

Akhlesh Kaushiva
Program Manager
DOE CESER
202-287-6062
akhlesh.kaushiva@hq.doe.gov

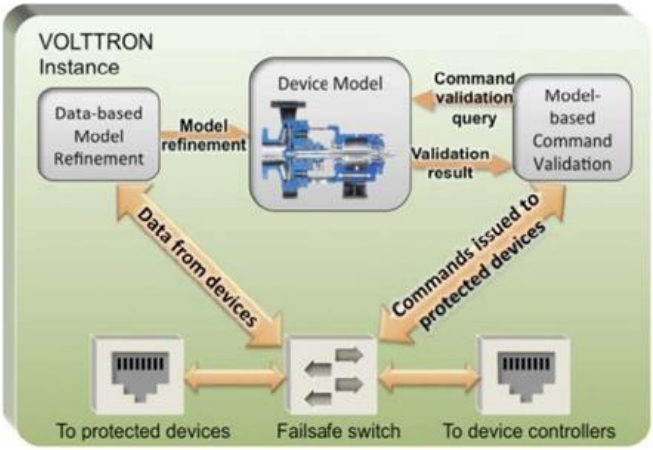

Figure 1: Inline VOLTTRON-based Security Platform

Technical Approach

The key innovation of INGRESS is the research and development of a VOLTTRON-based advanced cyber-attack detection and resiliency enabling platform that:

- Detects and prevents malicious control commands issued to various types of behind-the-meter equipment by developing machine learning models that characterize the normal behavior of the controlled devices and controllers along with metrics for the deviation from normal behavior;
- Identifies threats emerging from systems, such as smart meters and DERs, that can cause instability or outages in the grid by leveraging analytics on the data streams from power quality sensors, building management loads and generation, and operational data;
- Achieves resiliency by implementing VOLTTRON's architecture that mitigates risks from attacks on control system environments by switching the controllers from high-performance to a high safety state;
- Is interoperable with utility operations and building and energy management systems, and
- Prevents subversion of the security mechanisms from hardware and network layer attacks by leveraging the security features.

Project Phases

The INGRESS project will be conducted in two phases. Phase 1 focuses on the research and development of the INGRESS cybersecurity platform. Phase 2 concentrates on the demonstration of INGRESS technology.

Phase 1: INGRESS Research and Development

The research and development phase of INGRESS will include work on attack scenario and threat model definition; model-based validation subsystem; anomaly detection module; inline hardware platform selection and software support; VOLTRON; situational awareness development and integration; system integration and pre-deployment testing; and a commercialization plan.

Phase 2: Demonstration of INGRESS Technology

In Phase 2, INGRESS will be demonstrated within the hardware in the loop platform containing chiller plant and rooftop air conditioner models, ALC WebCTRL building management system, and a large commercial buildings environment.

Anticipated Results

Project results will include the following:

- Cost-effective and non-intrusive BITW (bump-in-the-wire) technology that transparently augments cybersecurity into legacy and emerging DER systems.
- Interoperability with a variety of different vendor network, hardware, software, and control devices.
- Advanced cyber-attack detection and resiliency capability for the grid-edge.