Multi-layered Resilient Microgrid Networks

A cyber-resilient control and protection architecture for deployment of microgrids in distribution networks

Background

The distribution grid must remain resilient as advanced grid architectures, such as microgrids, are introduced to improve reliability, in part through increased integration of distributed energy resources (DER), including renewable energy sources like solar photovoltaics. Microgrids are increasingly becoming an integral component of electric power grids as a framework to integrate DER; indeed, microgrids are being integrated into utility operations at all levels. In normal operation, the system will achieve optimal control through numerous distributed control actions of asset dispatch, load management, power transfer, and islanding.

This integration will require additional layers of communications, both horizontal and vertical, which must be accompanied by cybersecurity technologies that reduce potential cyber-attack surfaces and mitigate risks for wide-spread malfunctions of automation systems. The advanced cybersecurity technologies to be developed in this research project will become particularly important for fast control signals aimed at maintaining overall system stability, where encryption may be impractical but integrity and availability are the key concerns.

Examples of potential threats include: faking the microgrid disconnection from the grid, which can be a safety issue; compromising critical loads and generation in microgrids; changing the setting groups of protection relays in a microgrid causing the relays to trip erroneously; jamming communication channels between microgrid clusters; unwanted or premature islanding; and triggering out-of-phase reclosing in a microgrid to damage the rotating machines, among others.

Objectives

The project team will develop and demonstrate a cyber-resilient control and protection architecture for deployment of multiple microgrids in city/urban distribution networks. The design objective is to make the DER-rich distribution grid resilient to cyber-attacks, operator errors and sensor failures.

Project Description

The project team will leverage physics-based models in addition to cyber information to promote cyber-physical situational awareness. This builds on concepts successfully demonstrated under the "Collaborative Defense of Transmission and Distribution Protection and Control Devices against Cyber Attacks" (CODEF) project, in which the team leveraged Kirchhoff laws to distinguish physical measurements from spoofed values.

This multi-microgrid system will incorporate a multiple-layer power system control, communication and operation architecture overlaid with non-operational layers, such as weather forecasts. The system will optimize distributed generation and storage in multiple microgrids with integration into utility-level Distribution Management Systems (DMS)/DER Management System (DERMS), and will maintain safe and stable performance during communication failures, degradations due to severe natural events, or cyber-attacks.

Benefits

- Cybersecurity for advanced grid architectures, systems of microgrids, that improve grid reliability
- Reduce the risk that a cyber-attack might disrupt operation of self-configurable microgrid networks with multiple DER

Partners

- ABB, Inc. (lead)
- University of Illinois at Urbana-Champaign (UIUC)

Period of Performance

October 2016 – September 2019

Project Cost

Total: $3,098,965

Federal: $2,288,197

Cost Share: $810,768

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

Dmitry Ishchenko
Principal Investigator
ABB, Inc.
919-856-3915
dmitry.ishchenko@us.abb.com

Current Contact as of Aug. 2020

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

Technical Approach

The project will develop a cyber secure microgrid control platform that supports a heterogeneous ecosystem of microgrids with connections to utility and peer microgrids.

Microgrid participants in this ecosystem will exchange information at varying degrees of granularity and assumptions of trust

Individual microgrids are represented as loosely coupled systems with parametric uncertainties and potential state disturbances.

Threat Analysis and Modeling

Adversary View Security Evaluation Methodology – A threat model built using discrete-event simulation of attack graphs by an array of adversaries. The approach uses a game-theoretic decision model to drive adversary behavior and its impact on a system's operation. The attack model is coupled with a Stochastic Activity Network model that provides classical reliability and performability analysis.

Multi-Layered Control System Architecture and Cybersecurity Standards

Control System Architecture – Research and development of a methodology to enable coordinated control through aggregation and integration of multiple microgrids into utility DMS/DERMS system. This architecture adopts the DER integration architecture of the upcoming IEC TC 57 WG17 Standards and recommendations of IEC 62351 on cybersecurity for power systems data exchange.

Communication Architecture – The architecture will be built on top of IEC 61850 semantic object model extensions for DER with the associated specific communication protocol mappings considering both peer-to-peer and publisher-subscriber models. Extensions to abstract communications service interfaces of IEC 61850 can be proposed as needed.

Additionally, Software-defined Networking (SDN) will be evaluated as a mechanism to isolate a compromised microgrid network. SDN offers convenient method to manage modern networks by providing a global view and control over the entire system. The technical approach will focus on the following topics:

Classification/Prioritization of Network Flows in SDNs – Provide capabilities to the entire stack (protocol level, applications, controllers, routers and switches and even the underlying operating systems) so that simultaneous handling of flows with different priority/criticality levels can be achieved.

Isolation/Resiliency Guarantees in SDNs – Develop algorithms and mechanism that will (a) maintain system operation and (b) guarantee that the isolation requirements are still maintained, even during transitional states.

End Results

Project results will include the following:

- Cyber-resilient, standards-based platform for advanced distribution system architectures, systems of microgrids, that enhance reliable grid operation, in part through integration of distributed energy resources
- Distributed state estimation (DSE) developed to feed into many local microgrid control functions, and to detect cyber-attacks by forecasting the impact of a pending control action
- SDN developed to isolate a cyber-attack, and maintain microgrid ecosystem operation to ride-through the cyber-attack without loss of critical energy delivery functions.