Collaborative Defense of Transmission and Distribution Protection and Control Devices against Cyber Attacks (CODEF)

Real-time cybersecurity with power grid devices working together to validate commands and operations

Background

A cyber attack against a utility's sensor network could pose a risk of energy delivery disruption. For example, an attacker could attempt to maliciously control the operation of switching devices to weaken the state of a power system. Access to the utility network may also allow the attacker to manipulate protective devices and forcibly remove equipment from service, as well as inject fake signals into intelligent electronic devices (IEDs) to cause unintended operation.

One means of enhancing utility network cybersecurity is to enable protection and control devices, both between and within substations, to reach collaborative consensus to verify that a received input makes sense in the current operational state of the power grid.

Barriers

- Devices must utilize a common communications protocol to collaboratively verify commands.
- Slow collaborative validation may impede protection and control function.
- A compromised IED cannot differentiate between normal and malicious changes in its configuration settings or between spoofed electric power measurement signals and real measurements.

Project Description

The CODEF project is developing a distributed security domain layer that enables transmission and distribution grid protection and control devices to collaboratively defend against cyber attacks. Leveraging distributed security extensions of the IEC 61850 communications protocol will allow protection and control relays to collaboratively validate that inputs, configuration changes, or power system data make sense for reliable grid operation.

Capabilities of the collaborative defense system include detecting malicious commands—even those that comply with expected syntax, protocol, and device function—that if acted on could jeopardize power grid operations; detecting insider attacks, spoofed power system data, or configuration set points by anticipating their effect on power grid operations; and blocking incorrect functions and reporting on compromised devices. A fast, inter-device cross-checking framework completes collaborative validation as fast as the protection device's response time so as to not impede the protection and control function.

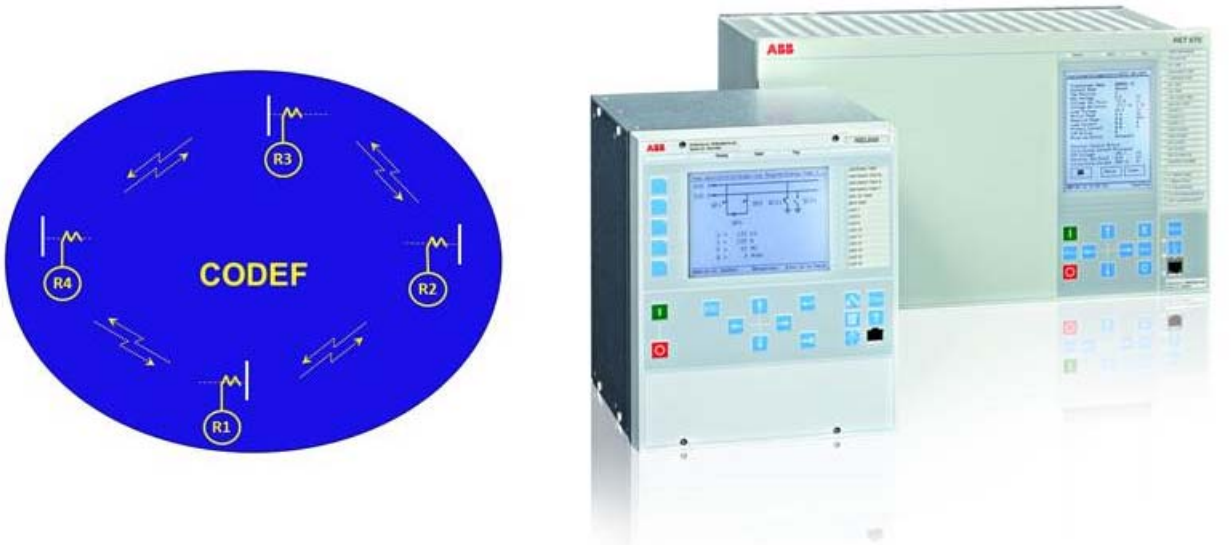
The technology will be incorporated into the firmware of enhanced relays in a utility setting, with the effort taking a vendor-neutral approach towards adoption.

Benefits

- Barrier to cyber activity that could jeopardize grid operations
- Real-time cybersecurity that is aware of power grid operations
- Power grid devices that work together to validate commands

Partners

- **ABB**
- Bonneville Power Administration
- University of Illinois at Urbana-Champaign (UIUC)



CODEF project depiction of collaborative device-checking, alongside targeted ABB products that will implement the system

Technical Objectives

This project consists of research, demonstration, and commercialization to advance the state of the art for cyber defense methods in transmission and distribution protection and control devices. The effort encompasses four phases, as discussed below.

Phase 1: Research and Design

- Identify threat models and cybersecurity gaps
- Design collaborative defense algorithms and methods that address the identified models and gaps

Phase 2: Development and Validation

- Develop and implement algorithms to meet design objectives
- Validate components of the defense in a laboratory setting

Phase 3: Demonstration

- Demonstrate firmware enhancements to IEDs in an instrumented utility test environment with respect to efficacy, performance, and ease of deployment

Phase 4: Knowledge Transfer

- Incorporate solution into commercial product lines
- Promulgate recommendations to IEC and other standards organizations
- Publish findings in conferences and journals

End Results

Project results will include the following:

- Inter-device-level solution for smart detection of spurious power system data using power system domain knowledge
- Inter-device-level cross-checking for secure configuration using power system protection domain knowledge
- Device-level checking for secure configuration using semantic analysis of substation configuration language
- Device-level solution for detection of erroneous or malicious direct control commands to protection and control devices
- Recommendations for security extensions of IEC 61850 and other standards

Content last updated: June 2015

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

Reynaldo Nuqui
Principal Scientist
ABB
919-807-5039
reynaldo.nuqui@us.abb.com

Current Contact as of Aug. 2020

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