Securing Grid-Interactive Efficient Buildings (GEB) through Cyber Defense and Resilient System (CYDRES)

Introduction

- Building Automation Systems (BAS) widely used in commercial buildings are the brain for the Grid-interactive Efficient Buildings (GEBS).
- Current BASs are designed and operated with limited consideration of cyber security and thus are vulnerable to cyber-attacks that can potentially result in severe consequences from occupant discomfort to disruption of grid operation.
- The project team is developing a real-time advanced building resilient platform, called Cyber Defense and Resilient System (CYDRES), deployable for existing and emerging BAS to empower GEB with cyber-attack-immune capabilities through multi-layer prevention, detection, and adaptation.
- Project Timeline: 05/01/2020 - 04/30/2023 (planned end date)

Technology Overview

- CYDRES aims to provide a real-time advanced building resilient platform through multi-layer prevention and adaptation mechanisms to monitor, detect, and respond to cyber-attacks and physical system faults.
- Module 1 - Network Analyzer: Advanced methods that automatically provide cyber-attack detection and defense through multi-layer control protocol validation.
- Module 3 & 4 - Mode Selector & Cyber Resilient Control: Targeted control response by reconfiguring the building automatically to a cyber-resilient mode through an intelligent mode selector based on the localized threat, building flexibility, and predicted impact.
- Module 5 - Visualization Platform: Cyber situational awareness informing the building operator of verified cyber-attacks.

Methodology

- Develop hardware-in-the-loop (HIL) testbed consisting of a real-time building emulator, real building HVAC controllers, and a BAS server.
- Implement 5 modules of the prototype CYDRES in the BAS server in the HIL testbed.
- Test, improve, and demonstrate the effectiveness of CYDRES prototype against various emulated cyber attacks and physical faults in the HIL environment.

Results

Module 1 - Network Analyzer: The proposed network analyzer (i.e., a conditional random field-based command validator and a LangSec-parser based input validator) can real-time detect cyber-attacks.
- The detection accuracy >99% and a false alarm rate < 13%. The emulated cyber-attacks were flagged within 30 seconds.

Module 2 - AFDDP: The proposed principal component analysis (PCA)-based fault detection strategy can detect real-time physical faults.
- The overall detection accuracy is over 85% and the false alarm rate is below 4%.
- Based on Module 1 and Module 2, our proposed approaches can differentiate between physical faults and cyber-attacks.

Module 3 & 4 - Mode Selector & Cyber Resilient Control: Cyber resilient control strategies are tested in the HIL testbed.
- Reconfiguration of optimization objective and constraints to shift control priority and to inject corrective measures.
- Compensator is able to reconstruct missing or corrupted measurements.

Module 5 - Visualization Platform: The cyber situational awareness platform is developed with an open-source, web-based, visualization dashboard.
- It provides real-time information of cyber detect and response process and near-term security hardening measurements deployment to prevent future incidents.

Impacts

Market:
- Global smart building market size to reach USD 109 Billion by 2026
- The market size of the intended end user of CYDRES is all BAS-controlled commercial buildings with primary energy saving of 0.86 Quad across the U.S. in 2030

Stakeholder engagement:
- ASHRAE BACnet 135 committee, NIST, Johnson Controls, Automated Logic, Cimetrics.

Publications

- 5 published journals, 10 conference papers, 12 oral presentations