A hardware-in-the-loop (HIL) testbed for cyber-physical energy systems in smart commercial buildings

Article *in* Science and Technology for the Built Environment · April 2024

DOI: 10.1080/23744731.2024.2336839

CITATIONS
6

READS
261

7 authors, including:

Guowen Li
Texas A&M University
11 PUBLICATIONS **177** CITATIONS
SEE PROFILE

Zhiyao Yang
Texas A&M University
50 PUBLICATIONS **518** CITATIONS
SEE PROFILE

Yangyang Fu
Texas A&M University
71 PUBLICATIONS **1,513** CITATIONS
SEE PROFILE

Zheng O'Neill
Texas A&M University
215 PUBLICATIONS **5,679** CITATIONS
SEE PROFILE

Manuscript accepted by Science and Technology for the Built Environment
DOI: https://doi.org/10.1080/23744731.2024.2336839

A Hardware-in-the-loop (HIL) testbed for cyber-physical energy systems in smart commercial buildings

GUOWEN LI[1], ZHIYAO YANG[1], YANGYANG FU[1], ZHENG D. O'NEILL[1,*], LINGYU REN[2], OJAS PRADHAN[3], JIN WEN[3]

[1]*Texas A&M University, College Station TX, USA*
[2]*Raytheon Technologies Research Center, East Hartford, CT, USA*
[3]*Drexel University, Philadelphia PA, USA*

**Corresponding Author Email: ZONeill@tamu.edu*

In recent years, there has been a growing trend towards the development of smart buildings that rely on cyber-physical systems (CPS) to optimize occupant comfort, safety, and energy efficiency. To ensure the reliable and efficient operation of CPS with designed control strategies, it is important to evaluate their performance under various scenarios before deploying them in the real world. This is where a Hardware-in-the-loop (HIL) testbed designed for studying sensor and control-related studies in smart buildings can be highly valuable. With the growing threat of cyber-attacks and physical faults targeting smart buildings, it is essential to ensure the security of building operations. A HIL testbed can emulate cyber-attack and physical fault scenarios, allowing researchers to develop and test threat detection and mitigation algorithms. This enables researchers to identify potential issues and optimize the algorithms in a safe and controlled environment before they are deployed in real-world settings, reducing the risk of failures that can negatively impact occupant comfort, safety, and energy efficiency. Therefore, this paper developed a HIL testbed designed for cyber-physical energy systems (e.g., buildings automation system (BAS)) in smart commercial buildings. The HIL testbed is comprised of a real-time building and Heating, Ventilation, and Air-Conditioning (HVAC) emulator using Modelica-based dynamic models, a set of BAS controllers, and a BAS computer server. The data generation capability of the HIL testbed is demonstrated by tracking normal and faulty operating data in the BAS, as well as monitoring detailed network traffic in the local BAS network. This study further demonstrates the HIL testbed's capability by conducting case studies on real-time physical fault and cyber-attack experiments using a Department of Energy (DOE) prototype commercial building. It is anticipated that the fully functional HIL testbed will be utilized for a variety of sensor and control-related studies, including but not limited to testing, developing, validating of different HVAC control strategies, fault detection & diagnosis, energy monitoring and analysis, cyber security study, etc.

Introduction

Background and motivation

The building sector consumed about 76% of electricity and was responsible for 40% of all U. S. primary energy use and associated greenhouse gas emissions (DOE 2015). As the brain of Cyber-Physical Systems (CPS) for the smart building, Building Automation System (BAS) can potentially provide significant energy savings through the optimization of building services with improved sensing devices and advanced load management algorithms. With the increasing usage of remote & mobile access, integrated wearable technologies, data exchange, and cloud analytics in modern smart buildings, the building industry moves towards open communication technologies. Providing access to the BAS through the building's intranet or even remotely through the Internet, has become a common practice. However, BAS was historically developed as a closed environment and designed with limited cyber-security considerations (Li, Ren, et al. 2023). Thus, smart buildings are vulnerable to cyber-attacks with increased accessibility.

Low-cost remote management, outsourced cloud analytics, sensors and controls, connected devices, and associated communication networks together play vital roles in smart buildings, which have several inherent vulnerabilities to cyber-attacks. Firstly, the most popular communication protocol for the BAS in commercial buildings, Building Automation and Control networks (BACnet) protocol was not designed with security as a primary requirement, as the original intention and implementation of BAS were isolated from the external connection. With the advancement of networking technology, BAS networks now are connecting to internal enterprise networks for remote management and cloud-based data analytics. As such, the attack surface against BAS networks in buildings has increased (Peacock 2019). In 2013, researchers discovered security vulnerabilities in Tridium Niagara, a widely used commercial BAS, and successfully hacked the Tridium system in Google's Sydney headquarter (Honorof 2013). A massive credential data theft at Target in 2014 began with attackers compromising the HVAC systems (Vijayan 2014). Secondly, as more devices and software systems interconnected and interacted, vulnerabilities in one component can be used to access the data, attack, and/or compromise other components. If buildings and the grid are more tightly integrated and connected as in Grid-interactive Efficient Buildings (GEBs), vulnerabilities in building software and devices could be used to attack the larger grid. Even if the grid is not directly compromised, the grid that is more heavily reliant on building-based services to maintain stability is indirectly made more vulnerable by greater building-level automation and connectivity (Roth and Reyna 2019).

Cyber-attacks impact physical systems such as BASs by tampering with the cyber system directly and influencing the physical system indirectly. To investigate such impacts, simulation-based studies have been widely adopted to evaluate the behavior of systems with complexity ranging from the traditional programmable logic controller (PLC) (Werth and Morris 2021) to smart heating, ventilation, and air-conditioning (HVAC) controllers under transactive energy systems (Zhang et al. 2019). More specifically for the BACnet protocol, many researchers have identified and classified vulnerabilities including snooping, application service attack, network layer attack, network layer Denial of Service (DoS) attack and application layer DoS attack (Holmberg and Evans 2003; Kaur et al. 2015). Peacock identified a comprehensive list of known attacks that can be launched on a network-based control system, including DoS, flooding,

smurfing, spoofing, writing attack, etc. (Peacock 2019). Fu et al. (Fu, O'Neill, and Adetola 2021) summarized two types of attacks that have significant influences on controlled physical systems, including data intrusion attack and DoS attack. Data intrusion attack refers to the manipulation of communicated data through remote attacks that can utilize the WriteProperty to corrupt the value of the payloads. Huang et al. (Huang et al. 2009) provided basic models for data-intrusion attacks, such as max/min attack, scaling attack, additive attack, etc. Sridhar and Manimaran (Sridhar and Govindarasu 2014) extended the basic attacks to include ramp, pulse, and random attacks. Wardell et al. (Wardell et al. 2016) numerically evaluated the data integrity attacks on an HVAC system by changing system control setpoints, generating false sensor inputs, and overwriting control signals, etc. Paridari et al. (Paridari et al. 2017) proposed a cyber-physical-security framework that integrates an analytical strategy for attack detection and an estimation-based resilient performance controller. This framework is then demonstrated with simulated data integrity cyber-attacks launched on key measurements. DoS attacks on the network refer to the blocked transmissions between controllers and the plant due to the unavailability of communication devices, communication paths, or local plant devices. The consequences of a DoS attack on the communication network systems have been unanimously considered as signal delaying or signal blocking during the transmission by most of the research. Xin et al. (Lou et al. 2019), Sridhar and Manimaran (Sridhar and Manimaran 2010) assessed the impact of a DoS attack that blocks network signal on the power grid real-time control. Fu et.al. in (Fu et al. 2021; Fu, O'Neill, and Adetola 2021) provided a Modelica-based modeling tool for the evaluation of cyber-attacks on the building energy and control systems. They considered both data intrusion attacks and DoS attacks. For the DoS attack, one of their assumptions in the paper is that the effects of the attacks on the cyber system have been well-mapped to their physical counterparts. For example, they implicitly assumed that DoS attacks will cause signal delaying or signal blocking, but they didn't mention what the delay patterns would be for different DoS attacks.

Besides cyber-attacks, physical faults also have a significant impact on smart buildings. Physical faults are defects or malfunctions in building components or systems that can result in suboptimal performance, safety hazards, or energy inefficiencies. Physical faults can be caused by a wide range of factors, including aging equipment, poor maintenance, design flaws, or environmental factors. For example, a malfunctioning sensor or actuator in the building's HVAC system can lead to suboptimal temperature or humidity control, leading to occupant discomfort and potentially affecting their health. a fault in the building envelope, such as air leaks or inadequate insulation, can result in increased heating or cooling loads and wasted energy. Faulty control systems or sensors can also result in excessive energy consumption, leading to higher energy bills and increased greenhouse gas emissions. Researchers have conducted several studies to investigate the impacts of physical faults on smart buildings. Zhao et al. (2019) provided a systematic review on fault detection and diagnosis in HVAC systems using machine learning techniques. The authors argue that machine learning-based methods have the potential to significantly improve the accuracy and efficiency of fault detection and diagnosis in building energy systems, leading to improved performance and energy efficiency. However, there are also challenges to the implementation of these methods, such as the need for high-quality data and the complexity of machine learning algorithms (Zhao et al. 2019). Similarly, Gunes et al. (2020) presented a study on improving energy efficiency and thermal comfort of smart buildings with

HVAC systems in the presence of sensor faults. The authors proposed a read-back and nearest neighbor monitoring approach considering temporal and spatial correlations between data of sensors to mitigate the faults of interest. The authors adopted a model-based design methodology for the multi-room building as a CPS application and tested their proposed approach in the simulation experiment (Gunes, Peter, and Givargis 2015). In another study, Lu et al. (2021) conducted a holistic fault impact analysis of the high-performance sequences of operation for HVAC systems using a Modelica-based case study in a medium-office building. The authors injected a total of 359 fault scenarios in three different seasonal operating conditions into the simulation model. The evaluated KPIs (key performance indicators) include control loop quality, thermal comfort, operational cost, source energy, site energy, and power system metrics (Lu et al. 2021).

The aforementioned state-of-the-art research mainly focuses on numerical evaluations of the impact of given cyber-attacks and physical faults on smart buildings. There are barely any experimental data to provide comprehensive support for such studies. To launch cyber-attacks and physical faults on real buildings, even for experimental purposes, is not acceptable for most building operators and researchers. First, conducting experiments on a real building is a resource-consuming process due to scalability and deployment concerns. The setup of such an experiment on one building requires significant efforts and expertise and may not be reusable for other buildings. Second, many experiments for cyber-attacks are required if a high-quality data set is required. However, the building operators barely allow the building to operate under the attacked or faulty mode for a long time. Third, the potential risks for such experiments that may lead to adverse or even severe effects on the system such as occupant discomfort, energy wastage, and equipment downtime. In order to investigate the BAS behavior under cyber-attacks and physical faults as well as to develop cyber-resiliency countermeasures to safeguard the smart buildings, a testbed capable of emulating real-time cyber-physical events in real controllers and interacting with a virtual building model is highly desired.

Such a testbed should not only support cyber-physical security but also control-oriented studies on smart buildings. One emulation solution is using a Hardware-in-the-loop (HIL) system to simulate a building by connecting the controller to a virtual building system model in lieu of the actual system. Hardware-in-the-loop simulation (HIL) is defined as the operation of real physical components in connection with real-time simulated components (Isermann, Schaffnit, and Sinsel 1999). In the building energy sector, controllers, actuators, and/or HVAC equipment that may not be modeled to ensure acceptable accuracy are often replaced with real hardware in HIL simulations. HIL is a technique is usually used in the development and testing of complex real-time embedded systems. The complexity of the plant under control is included in testing and development by adding a mathematical representation of all related dynamic systems. These mathematical representations are referred to as the behavior models in the rest of this paper. The embedded system to be tested interacts with this behavior model through the electrical emulation of sensors and actuators. Therefore, hardware controllers and control strategies (e.g., load control algorithms) can be tested and optimized in conjunction with a real-time emulator that is connected to the real controller. Models running on the real-time emulator represent the building energy equipment and system. This enables a closed control loop in a partially virtual system with real controllers.

For the HIL applications in buildings, as shown in Figure 1, a flexible HIL testbed can be utilized for a variety of sensor and control-related studies, including but not limited to testing, development, comparison, and benchmarking of different HVAC control strategies (e.g., traditional rule-based control (RBC), model predictive control (MPC), deep reinforcement learning (DRL)), fault detection & diagnosis, cyber security study, and energy monitoring and analysis. The testing can be for single smart building studies and smart and connected communities for energy efficiency, demand flexibility, and decarbonization.

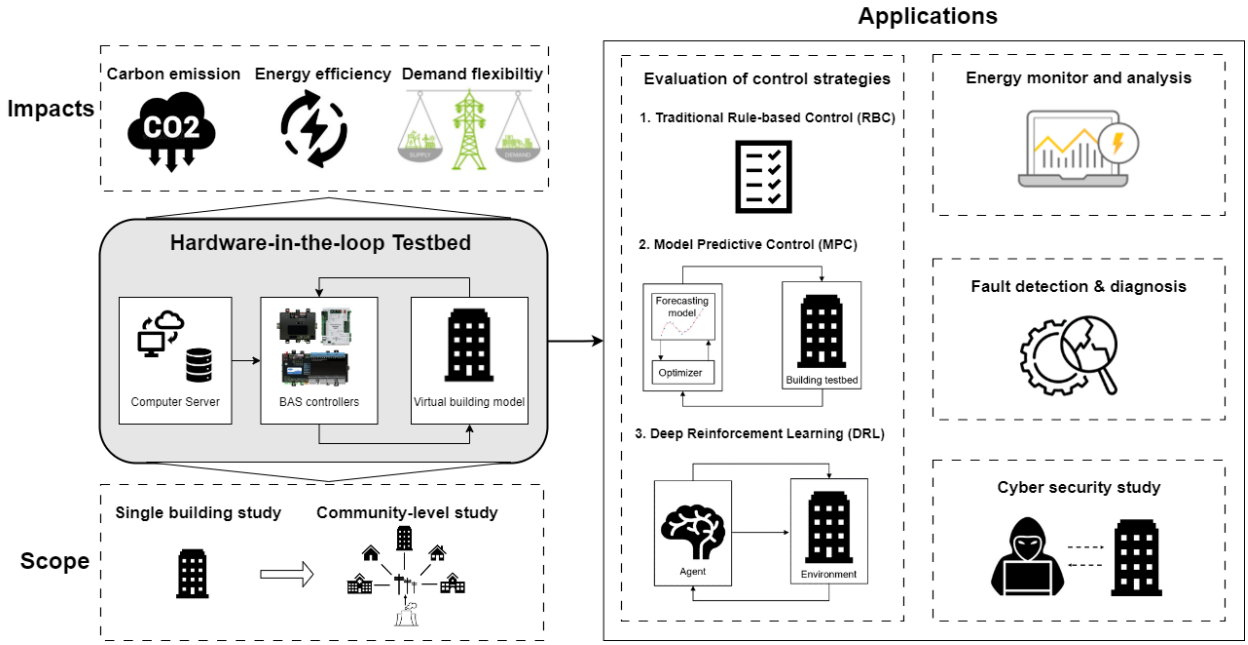

Fig. 1. Potential applications of the developed HIL testbed.

In contrast to the HIL approach, other conventional development strategies, where most control loops are only tested for the first time on the fully assembled system, are time-consuming and cost-intensive because a real test in buildings/subsystems, even in a laboratory, involves many variables in a complex multi-physics environment (O'Neill and Henry 2016). Calfa et al. provided a means of comparison between pure simulation and the three experimental techniques (i.e., HIL, fix boundary and field study) using ranking numbers in terms of Setup Cost, Setup Complexity, Testing Time, Disturbance Range, and Representative Results. Pure simulation shows its advantages in lowest setup cost, lowest testing time, and best disturbance range, but it has the worst representative results. Field study (or field demonstration) has the medium setup cost and medium disturbance range, but it has best representative results. Although HIL requires highest setup complexity, it comes with the benefits of medium representative results, medium testing time, highest disturbance range (Calfa et al. 2023).

Table 1 presents the pros and cons of HIL, pure simulation, and field demonstration. A field demonstration is the most realistic testing environment capturing all real-world conditions, but it is cost-intensive with limited repeatability for example the weather conditions are hard to repeat in real buildings in different locations. A pure simulation is time-efficient and cost effective, but

it may not accurately capture the realistic physical dynamics. A HIL testing is relatively more realistic and repeatable on testing the key hardware components, but it also relies on the accuracy and the reliability of the emulated components. It's worth mentioning that Modelica, a dynamic equation-based modeling language, could be used for an explicit representation of the controllers and control logic present in real buildings and used for control evaluation such as the BOPTest framework (Blum et al. 2021). However, to the best knowledge of authors, the current version of the BOPTest lacks the capability to comprehensively model both local controllers and network behavior for building automation systems. It is important to note that capturing local controller behavior extends beyond the modeling of a simple PI controller; rather, its performance is constrained by the local hardware and software.

Table 1. Comparison of HIL, pure simulation, and field demonstration.

Approach	Pros	Cons	Suitable tasks
HIL	• Realistic and repeatable testing on the key hardware components. • Flexible testing boundary provided by simulation. • Faster and less expensive than full experimental testing.	• Limited by the accuracy & reliability of the simulation. • Require interface devices and software between equipment hardware and simulation.	Prototyping & control development for critical component
Pure simulation	• Time-efficient and cost-effective • Easy to conduct for various operation scenarios. • No hardware installation and operation required	• May not accurately capture realistic physical dynamics. • Depends heavily on quality of available data, model inputs, and assumptions.	Design and control parameter optimization
Field demonstration	• Most realistic testing environment • Capture all real-world conditions	• Time-consuming • Cost-intensive • Limited repeatability	Verification and validation of product design and control

In summary, HIL testing shows the following advantages over field demonstration, including the ability to (1) test hardware under conditions beyond normal operations such as sensor faults, actuator failures, extended operation ranges without causing destructive consequences, and (2) easily replicate experiments with the same boundary conditions. Compared with pure simulation, HIL testing can significantly enhance result fidelity by incorporating hardware that is difficult to model. Furthermore, HIL allows the testing and evaluation of physical controllers with proprietary algorithms without necessitating knowledge of the algorithms' specifics, as only their interfaces with connected simulators are required (Isermann, Schaffnit, and Sinsel 1999; Fathy et al. 2006; Huang et al. 2018).

Research gaps and contributions

This paper identified the following research gaps:

- The HIL approach has been widely applied in the automotive and power industry, however, not much has been done in the building energy and automation sector (Xu, Haves, and Deringer 2004; Bushby et al. 2010; Otten, Li, and Alleyne 2010; Huang et al. 2018; Calfa et al. 2023). To the best knowledge of authors, no publicly available HIL experiments related to cyber-attacks and physical faults using a complete set of real BAS controllers have been conducted on smart commercial buildings. Research using the HIL approach for sensor and control-oriented studies, especially for cyber-physical security in smart buildings, is still needed.
- In order to advance state-of-the-art in cyber-physical security of smart buildings, there is a need for more experimental datasets that should capture both the network-level and physical-level dynamic behavior of the building energy system with considerations of actual local controllers and network performance.

To fill in the aforementioned research gaps, this paper has the following contributions:

- This study presents a flexible HIL testbed supporting the cyber-physical security research of BASs in smart buildings through two case studies of cyber-attack and physical fault experiments. In the proposed HIL testbed, a high-fidelity Modelica building energy system model is built as the behavior mode and interacts with real BAS controllers. The local controllers are managed by a BAS server and communicate with each other through the BACnet/IP protocol. Both network traffic data and physical system operating data are monitored and recorded. While simulations play a crucial role in the early stages of development, incorporating real controllers and communication protocols like BACnet in HIL testing enhances the validation process and ensures that the tested systems meet the requirements of practical applications.
- With this HIL testbed, experiments can be cost-effectively conducted to investigate in more details on the sensors, building network, and control-oriented studies, for example, investigating how cyber-attacks and physical faults can have different direct effects on the building network and real controllers, and indirect effects on the simulated HVAC system. The flexibility can help mitigate most of the concerns related to on-field cyber-attack and physical fault experiments on a real BAS while keeping sufficient fidelity to make the data trustful.
- The developed HIL testbed offers many advantages including but not limited to (1) conducting different types of cyber-attacks and physical faults experiments on real controllers without jeopardizing real building energy equipment; (2) launching cyber-attacks and physical faults at any time in this testbed without causing any real-world adversarial impacts such as occupancy discomfort, excessive energy consumption, etc.; (3) generating experimental datasets with detailed network traffic and system operating data under the same disturbance conditions. The experimental datasets will be used to develop and validate attack/fault detection algorithms in our future work.

The rest of this paper is organized as follows. Section 2 introduces the proposed HIL testbed and simulation framework, including the hardware, software, and data communication schemes. Section 3 provides a detailed HIL setup for a high-fidelity building energy system model based on a DOE (Department of Energy) prototype commercial building (Goel et al. 2014). Section 4 describes the detailed implementation of cyber-attacks and physical faults on the building cyber-physical system with emulated data presented, followed by Section 5, where conclusions and future work are discussed.

HIL testbed setup

Architecture and configuration

The HIL testbed, as shown in Figure 2, is developed for sensor and control-oriented studies on smart buildings. The testbed consists of three major components: a real-time dSPACE HIL machine, a set of Automated Logic Company (ALC) BAS controllers, and a computer server for the BAS system. The detailed hardware and software used in this testbed are summarized in Table 2 and Table 3. The real-time HIL machine emulates a virtual building and HVAC system that are both modeled in Modelica (Fritzson 2014). The ALC controllers provide rule-based control logic for different HVAC equipment, and their control commands are sent to the virtual building through the real-time HIL machine. The computer server hosts the software environment for all the hardware and customized services such as a master program that controls the experiments. The computer server also acts as a remote access point to the BAS system providing monitoring and trending of operation data as well as supervisory control (Li, O'Neill, et al. 2023; Li, Yang, et al. 2022).

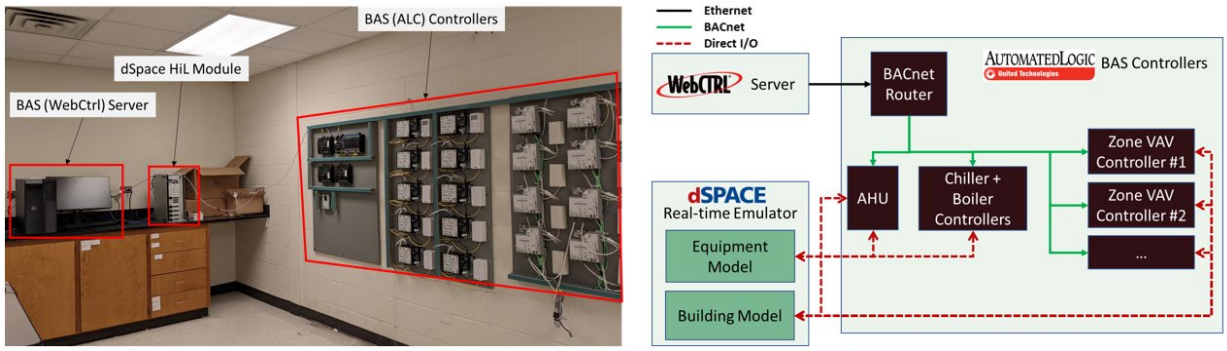

Fig. 2. The system architecture of the developed HIL testbed.

The HIL machine is a set of dSPACE tools, which provides real-time emulation of a building energy system modeled in Modelica. The building model takes the control commands from ALC controllers as inputs and generates typical measurements for the building energy system as outputs that are sent back to the ALC controllers. The real-time emulation depends on a set of hardware and software. For the hardware, besides the SCALEXIO™, additional A/D, D/A boards and wires are used to establish the communications between the SCALEXIO™ and the ALC controllers. For example, the simulation models are compiled and deployed to the dSPACE module with designated channels receiving signals such as a damper position from the BAS controllers via the A/D boards and used as the input to the simulation models. The simulated results, such as the zone

temperature, are then transmitted back to the BAS controllers via the D/A boards. With the dSPACE HIL module, the operation of the building and its HVAC system can be directly emulated without the need for actual zones and equipment.

The set of BAS controllers includes typical controllers for HVAC equipment such as Air Handler Units (AHUs), chillers, and VAV terminal boxes containing the default control logic of the equipment, and in real buildings, they are normally installed close to the equipment under control. A local ARCnet network is established through a router. This enables all controllers to communicate with a centralized BAS through a BACnet protocol. All local controllers used in this testbed are natively BACnet compatible. In addition, a web-based BEMS known as WebCTRL™ is adopted for the testbed. Modern BAS allows users to fully access their buildings' schedules, setpoints, trends, alarms, and other control functions from virtually any computer, anywhere in the world. As a native BACnet system, this BEMS interfaces with LonWorks, Modbus and many other protocols to provide an integrated solution to building control needs. The ALC controllers communicate with the WebCTRL™ Server through a communication network using the BACnet protocol. During normal operation, these controllers take in signals from local sensors and output control signals accordingly. They also respond to the supervisory control dispatched directly by the WebCTRL™ server, and the control outputs of the local controllers are also accessible in the WebCTRL™ server. Both the measurement inputs and the control outputs of a local controller can be connected directly to outside sources with voltage input/output (I/O). The default control logic in these controllers can be updated in the WebCTRL™ server using the EIKON-Logic™ and downloaded to the local control board.

The computer server is a workstation that hosts the software environment for the testbed, including a WebCTRL™ server that supports building automation services, an open-source database that supports data storing and querying, a set of the HIL machine software tools such as dSPACE ControlDesk™ that controls the HIL experiment, and an adversary program that performs cyber-attacks on the building control system utilizing the vulnerabilities of BACnet protocol.

Table 2. Summary of major hardware in the HIL testbed.

Item	Manufacturer	Configuration
DS6221	dSPACE. Inc	Multi-channel A/D board with 16-A/D input channels, 16 independent A/D converters, 8 external trigger channels
DS6241	dSPACE. Inc	Multi-channel D/A board with 20 D/A channels with independent converters and dedicated ground sense line per channel
DS6101	dSPACE. Inc	10 ADC, 12 digital inputs, 10 variable inputs (analog/digital), 8 DAC (DC), 4 DAC (DC) additional with current sink functionality, 3 DAC (AC), 14 digital outputs, 6 resistance simulation, 1 pair of direct coupled I/O channels
Computer server	Dell	Dell Precision T7920, Intel Xeon Gold 6230
ACE 6001MC	dSPACE. Inc	Advanced control kit SCALEXIO 6001 consisting of DS6001 SCALEXIO processor board with Intel Core i7-6820EQ quad-core processor.

BAS controllers	ALC	VAV box controller, ZN341A (3 binary outputs, 4 universal inputs and 1 analog output)
	ALC	AHU controller, OFBBC (supports up to 9 expanders, 180 I/O channels total)
	ALC	Chiller/boiler plant controller, OF1628-NR (supports up to 9 expanders, 224 I/O channels total)

Table 3. Summary of major software in the HIL testbed.

Item	Manufacturer	Configuration
ConfigurationDesk™	dSPACE. Inc	Software kits to configure behavior model
ControlDesk™	dSPACE. Inc	Software kit to control and visualize real-time experiment
Dymola/Modelica	Dassault	Software tool to model dynamic building energy system
WebCTRL™	ALC	Building automation system server
EIKON-Logic™	ALC	Software to configure controller logic for ALC equipment controllers
Python	n/a	Open-source programming environment to provide customized WebCTRL API and supervisory control
Wireshark	n/a	Open-source network packet analyzer

Workflow and dataflow

Figure 3 and Figure 4 present the detailed workflow and dataflow for the HIL setup and testing. The first step is to create a mapping sheet of I/O points for the ALC controllers. For example, for each VAV terminal box in the Modelica model, the damper positions and the reheat coil valves receive 0-10 V voltage analog signals from the ALC VAV controller. The range of 0 to 10 is then mapped into [0,1] for Modelica models, where 0 and 1 mean 0 and 100% openness of the controlled actuators respectively. The major outputs represent the measurements required by the ALC controllers, such as zone air temperature, discharge air temperature, supply air flow rate, outdoor air dry-bulb temperature, and outdoor relative humidity. These digital signals are then converted to analog voltage signals and sent to ALC controllers. Note different ranges are used for these converted analog signals due to the design of the ALC controller. Only the mapped voltage signals are sent to the ALC controllers and are thus required by this HIL test. Detailed mapping between the digital signals and the analog signals are shown in Table 4. The second step follows the mapping sheet by exposing the I/O of the Modelica model to be connected with emulator machine. Then, steps 3 and 4 aim to deploy the compiled model in the dSPACE real-time emulator machine. This model is loaded as a behavior model in the HIL machine. The behavior model should be configured in dSPACE Configuration Desk to connect its inputs to the dSPACE A/D channels and its outputs to the dSPACE D/A channels. Step 5 setups the HIL testing settings such as the start time and end time, the saved variables, data timestep, etc. The final step is to run the experiments and extract the real-time data generated from the HIL testbed.

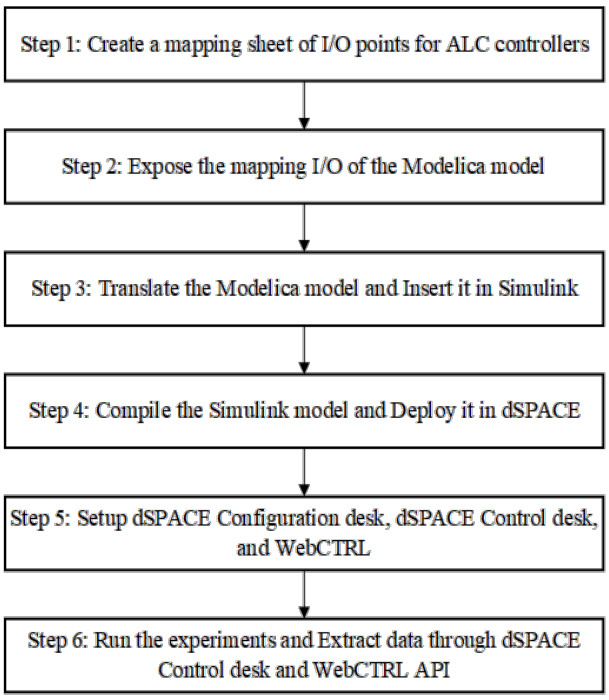

Fig. 3. Workflow of setting up the HIL testbed.

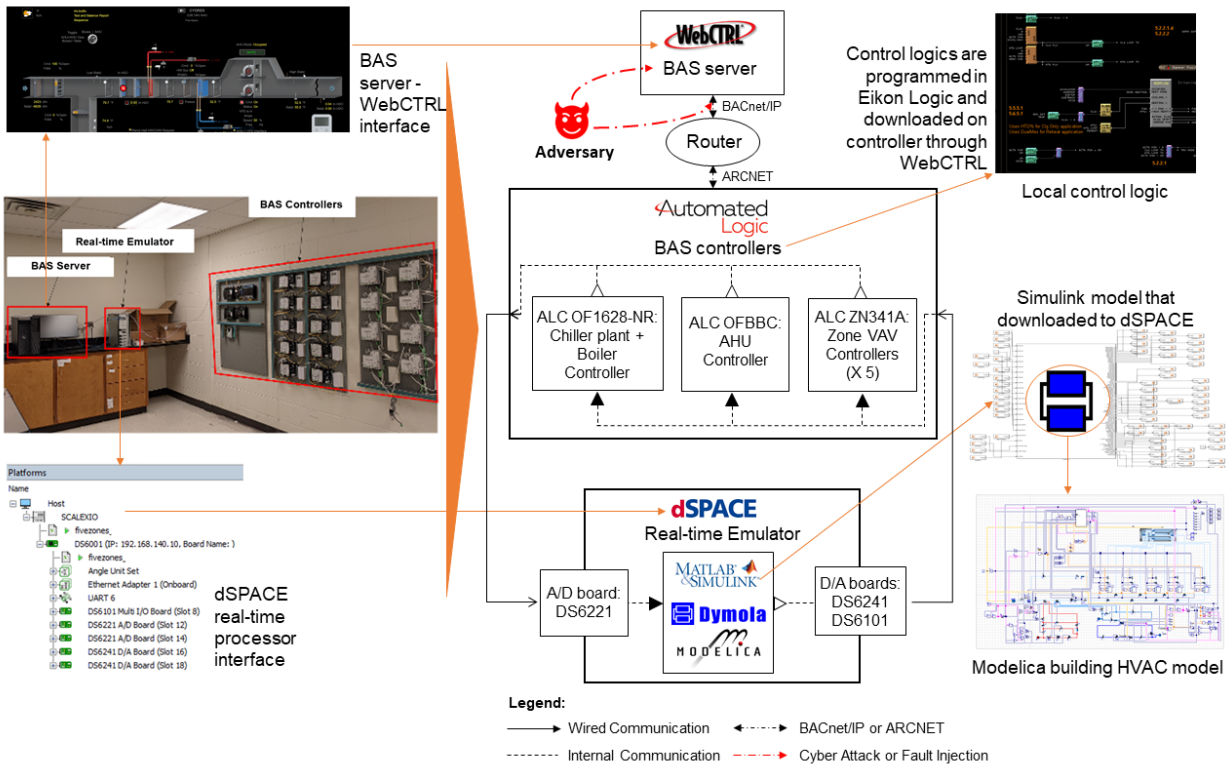

Fig. 4. Dataflow of testing in the HIL testbed.

Table 4. Mapping sheet of digital signals and analog signals in the HIL testbed.

Controllers	Variable names	I/O type	Voltage signals (Analog signals from controllers)	Mapped signals (Digital signals to Modelica model)
VAV terminal box controllers (Core, East, North, South, and West zones)	Zone air temperature	AI	0-5 V	-3.89 – 51.67 ℃
	Supply air temperature	AI	0-5 V	7.22 - 35 ℃
	Supply air flow rate	AI	0-5 V	0 - 4.72 m^3/s
	Air damper position	AO	0-10 V	0-100 %
	Reheat coil valve	AO	0-10 V	0-100 %
AHU controller	Supply air temperature	AI	0-10 V	-3.89 – 51.67 ℃
	Outdoor air flowrate	AI	0-10 V	0 – 10.38 m^3/s
	Mixed air temperature	AI	0-10 V	-28.89 – 48.89 ℃
	Duct static pressure	AI	0-10 V	0 - 1379 Pa
	Supply fan status	BI	0/10 V	On/Off
	Return fan status	BI	0/10 V	On/Off
	Return air flow sensor	AI	0-10 V	0 – 10.38 m^3/s
	Return air temperature	AI	0-10 V	-3.89 – 51.67 ℃
	Supply air flow sensor	AI	0-10 V	0 – 10.38 m^3/s
	Cooling coil entering temperature	AI	0-10 V	-3.89 – 51.67 ℃
	Cooling coil leaving temperature	AI	0-10 V	-3.89 – 51.67 ℃
	Heating coil entering temperature	AI	0-10 V	-28.89 – 48.89 ℃
	Heating coil leaving temperature	AI	0-10 V	-3.89 – 51.67 ℃
	OA temperature	AI	0-10 V	-28.89 – 48.89 ℃
	OA relative humidity	AI	0-10 V	0-100 %
	Supply Fan Start/Stop	BO	0/10 V	On/Off
	Supply Fan Speed Ratio	AO	0-10 V	0 - 100 %
	Return air damper position	AO	0-10 V	0 - 100 %
	Economizer OA damper position	AO	0-10 V	0 - 100 %
	Exhaust air damper position	AO	0-10 V	0 - 100 %
	Cooling valve opening degree	AO	0-10 V	0 - 100 %
	Chilled water supply temperature	AI	0-10 V	3.89 - 20 ℃

	Chilled water return temperature	AI	0-10 V	3.89 - 20 ℃
	Chilled water flow rate	AI	0-10 V	0 – 0.005 m^3/s
	Condenser water supply temperature	AI	0-10 V	15 - 45 ℃
	Condenser water return temperature	AI	0-10 V	15 - 45 ℃
	Differential pressure of chilled water	AI	0-10 V	0 – 36000 Pa
	Chilled water isolation status	BI	0/10 V	On/Off
Chiller plant controller	Condenser water isolation valve	BI	0/10 V	On/Off
	Chilled water pump status	BI	0/10 V	On/Off
	Cooling Tower Status	BI	0/10 V	On/Off
	Condenser water pump status	BI	0/10 V	On/Off
	Chiller On/Off	BO	0/10 V	On/Off
	CH-1 CHW Valve	AO	0-10 V	0 - 100 %
	CHWP1 Enable	BO	0/10 V	On/Off
	CHWP1 VFD Output	AO	0-10 V	0 - 100 %
	ECO CHW BYP VLV	BO	0/10 V	On/Off
	CWP1 Enable	BO	0/10 V	On/Off
	CWP-1 Speed	AO	0-10 V	0 - 100 %
	CT-1 Fan Enable	BO	0/10 V	On/Off
	CT-1 VFD Speed	AO	0-10 V	0 - 100 %

Note: AI = Analog Input, AO = Analog Output, BI = Binary Input, BO = Binary Output.

Building system model and BAS control logic

Building energy system model

The schematic of the simulated HVAC system for a medium-sized office building is illustrated in Figure 5. Heating and cooling are delivered by a single-duct VAV system. One AHU connected with five VAV terminal boxes serves five zones (four perimeter zones and one interior zone) on one floor. The chilled water is supplied by a central chiller plant that consists of a chiller, a waterside economizer, a cooling tower, a chilled water pump, and a cooling water pump. A boiler, fed by natural gas, supplies the hot water to the AHU heating coils. The VAV boxes are used to control the temperature of a corresponding zone with a centralized chiller and a boiler providing cooling/heating energy to zones. The supply air is conditioned by the heating/cooling equipment (e.g., coils) within the AHU. The VAV box adjusts this supply air, both in volume and temperature, to serve the desired zone to maintain the design zone air temperature setpoint and meet the required ventilation rate. The VAV box studied in this study accomplishes this by using both an airflow damper and a reheat coil valve. The damper closes or opens the airflow pathway to modulate the

volumetric flow rate of the supply air into the zone. The reheat coil is a heating coil inside the VAV box, and its waterside valve can be regulated to reheat the supply air if needed. Table 5 shows the detailed equipment sizing information of the studied single-duct VAV terminal reheat system.

Figure 6 shows the Modelica model for the studied HVAC system. Modelica, an equation-based modeling language, has been utilized to model and simulate building energy and control systems (Li et al. 2021; Li, Fu, et al. 2022; Chen et al. 2019). The virtual building model is modeled based on the open-source Modelica Buildings Library (MBL) (Wetter et al. 2014) developed by Lawrence Berkeley National Laboratory. This Modelica model is based on and validated against a medium-size office DOE prototype model (Goel et al. 2014) developed by Pacific Northwest National Laboratory in EnergyPlus (Crawley et al. 2001). The system model consists of an HVAC system, a building envelope model, and a model for air flow through building leakage and through open doors based on wind pressure and flow imbalance of the HVAC system. The HVAC system is sized for Chicago, IL, USA in climate zone 5A. The air-side control sequences follow ASHRAE Guideline 36 (ASHRAE 2018) and the water-side control sequences follow ASHRAE project RP-1711 (Taylor 2020). More details of this HVAC system can be found in (Fu, O'Neill, and Adetola 2021; Fu et al. 2021).

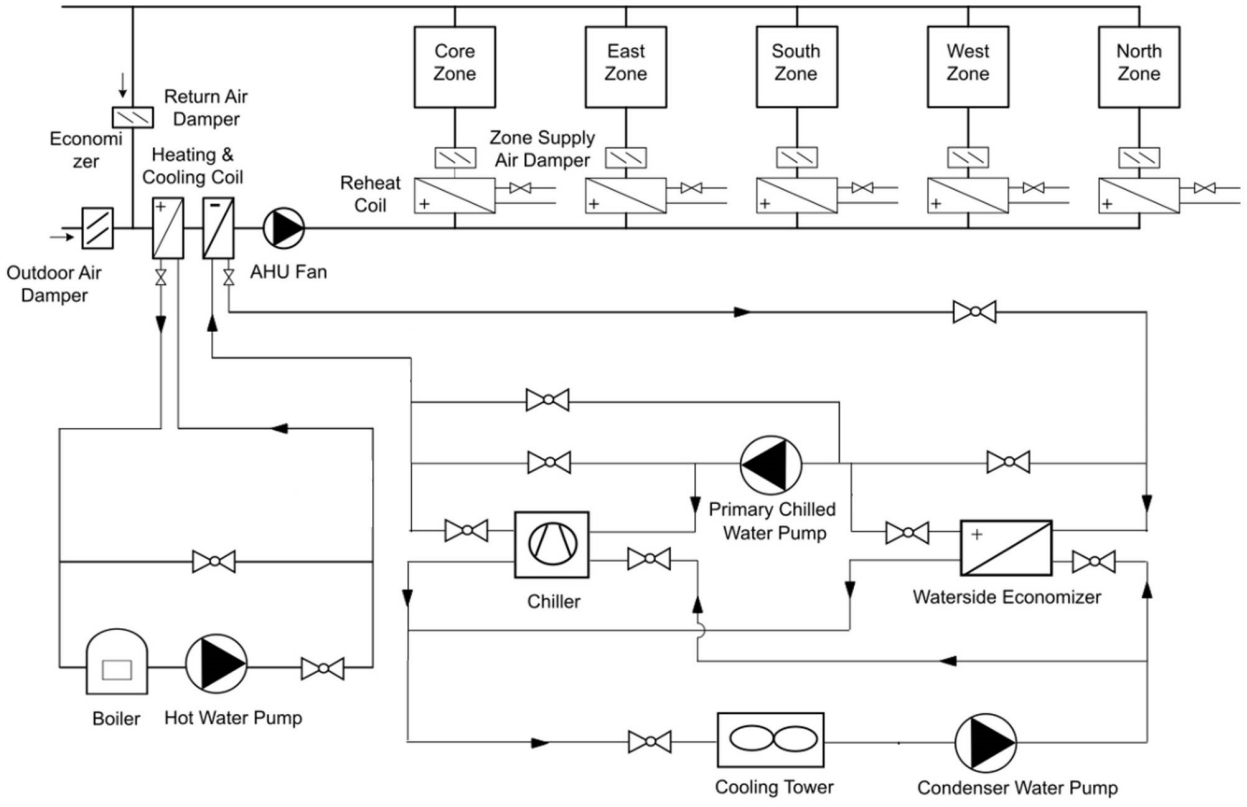

Fig. 5. Schematic diagram of the simulated HVAC system in the real-time HIL emulator.

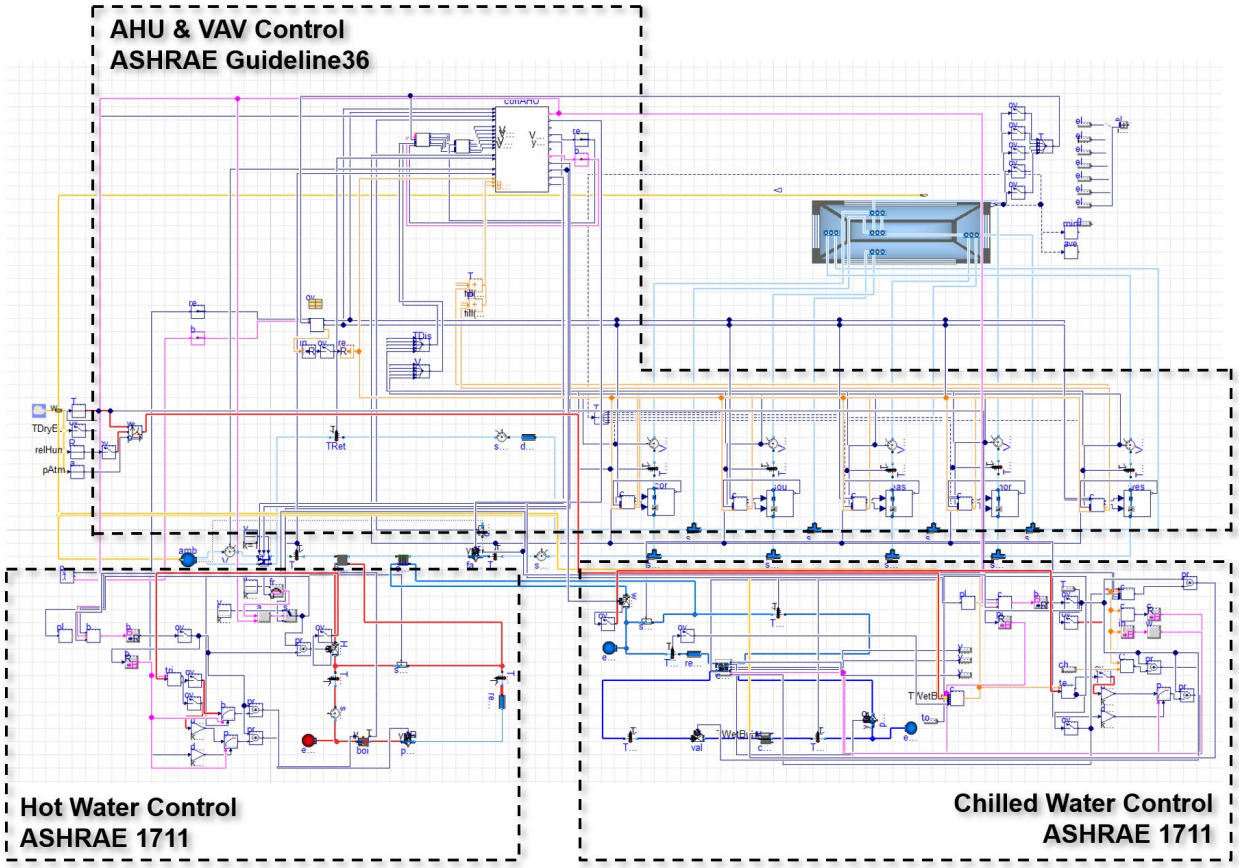

Fig. 6. Modelica implementation of the studied HVAC system for a commercial building (Fu et al. 2021).

Table 5. Equipment sizing parameters of the studied HVAC system.

Equipment	Quantity	Component/location/name	Nominal information	Value	Unit
VAV terminal boxes	5	Core zone	Air flow rate	4.5	m^3/s
		East zone	Air flow rate	0.90	m^3/s
		North zone	Air flow rate	0.95	m^3/s
		South zone	Air flow rate	0.95	m^3/s
		West zone	Air flow rate	0.70	m^3/s
AHU	1	Cooling coil	Cooling capacity	100.7	kW
		Heating Coil	Heating capacity	55.4	kW
		Fan	Air flow rate	4.8	m^3/s
			Head pressure	1381	Pa
			Power consumption	13.5	kW

Chiller	1	Design parameters	Nominal capacity	101	kW
			Design COP	5.9	-
		Evaporator	Design outlet temperature	5.6	℃
			Design inlet temperature	11.6	℃
			Flowrate	0.0040	m^3/s
		Condenser	Design inlet temperature	29.4	℃
			Volume flow rate	0.0043	m^3/s
		Compressor	Speed type	Variable speed	-
			Power consumption	18.2	kW
Chilled water pump	1	Design parameters	Head pressure	255	kPa
			Power consumption	2.1	kW
			Volume flow rate	0.0040	m^3/s
			Speed type	Variable speed	-
Condenser water pump	1	Design parameters	Head pressure	215.7	kPa
			Power consumption	1.9	kW
			Volume flow rate	0.0043	m^3/s
			Speed type	Constant speed	-
Cooling tower	1	Design parameters	Nominal capacity	117	kW
			Design approach temperature	3.9	℃
			Power consumption	4.3	kW
		Fan	Fan speed type	Variable speed	-
Hot water pump	1	Design parameters	Head pressure	157	kPa
			Power consumption	0.4	kW
			Volume flow rate	0.0013	m^3/s
			Speed type	Variable speed	-

Boiler	1	Design parameters	Nominal capacity	55	kW
			Power consumption	4.3	kW
			Efficiency	0.9	-

BAS control logic: example of VAV control

A high-performance control sequence for a VAV box control in HVAC practice, called dual maximum logic, is shown in Figure 7. The term dual maximum refers to the airflow setpoints for heating and cooling. This "dual max" logic allows the minimum airflow setpoint to be lower than in a conventional sequence (i.e., single maximum logic) where the minimum airflow equals the heating airflow (ASHRAE 2018). Thus, the dual maximum logic could save more energy compared with the single maximum logic.

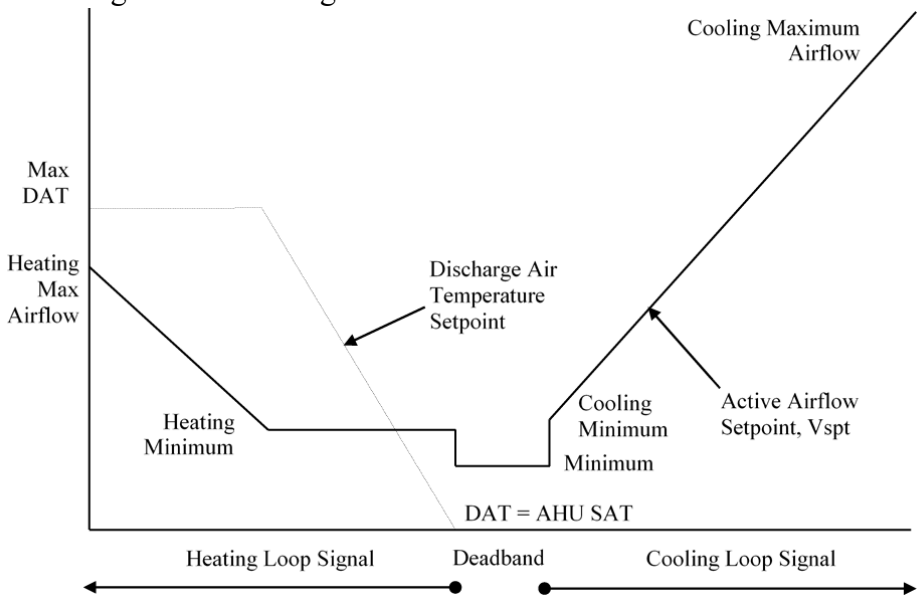

Fig. 7. Dual maximum logic of the VAV terminal unit with reheat (ASHRAE 2018).

It should be noted that HVAC controllers used in the building automation industry typically don't use PLCs and have limited onboard memory. Although some intelligent controllers (e.g., a fuzzy logic controller, a pattern recognition adaptive controller, etc.) have been developed over the past two decades, the most commonly used controller in HVAC applications remains the Proportional-Integral (PI) type (Seem 1998; Zhao, Fan, and Mijanovic 2013). Indeed, 95% of industrial controllers are of the Proportional-Integral-Derivative (PID) type even though most loops are actually PI controls (Åström and Hägglund 2006).

The HVAC controllers used in this study come fully programmable via software called EIKON-Logic^{TM} located in the BAS computer server. The software is a drag-and-drop format using micro-blocks, which carry out mathematical operations. Custom micro-blocks using Operator's Control Language (OCL) can also be used to realize complicated calculations. A sample control program for dual maximum control logic is shown in Figure 8. This PID block compares two quantities, in

our case the zone discharge air temperature (DAT) with the supply air temperature (SAT) setpoint, and tries to maintain the setpoint using PID controls. The proportional portion is simply the difference between the two values. The integral portion is the time-weighted error. The derivative portion is the rate of change in the difference. Due to the limitations of controllers, most HVAC control is currently done without the derivative component, making the control simply PI. The implementation of this block is fairly straightforward, but the tuning of the loop determines the effectiveness of the logic. Each of the proportional and integral values is given a weight by which they are multiplied to determine the significance of each in determining control output. Additionally, a bias can be set in the block to set the default output of the block. This is collectively referred to as tuning the loop.

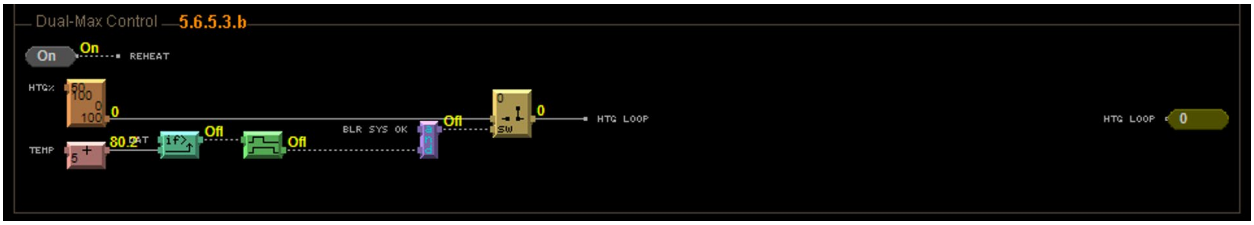

Fig. 8. Example of dual maximum control program in the BAS computer server.

During the cooling season, the outdoor air temperature is warm and the VAV box always stays in cooling mode. Therefore, only the discharge air damper position needs to be controlled following the dual maximum control logic. The control is accomplished by using a PID block, with the derivative component set to zero. Thus, the logic is effectively just a PI control. Zone temperature and setpoint are compared to determine an appropriate damper position, which is then sent back to the Dymola model through the emulator of dSPACE using the A/D board. The model is accordingly updated and continues to solve for zone temperature at each time step, writing this value (sensor information) to the controllers to complete the HIL loop via the D/A board. Both zone air temperature, discharge air damper position, and the reheat coil valve position are trended and recorded in the BAS server, as shown in Figure 9.

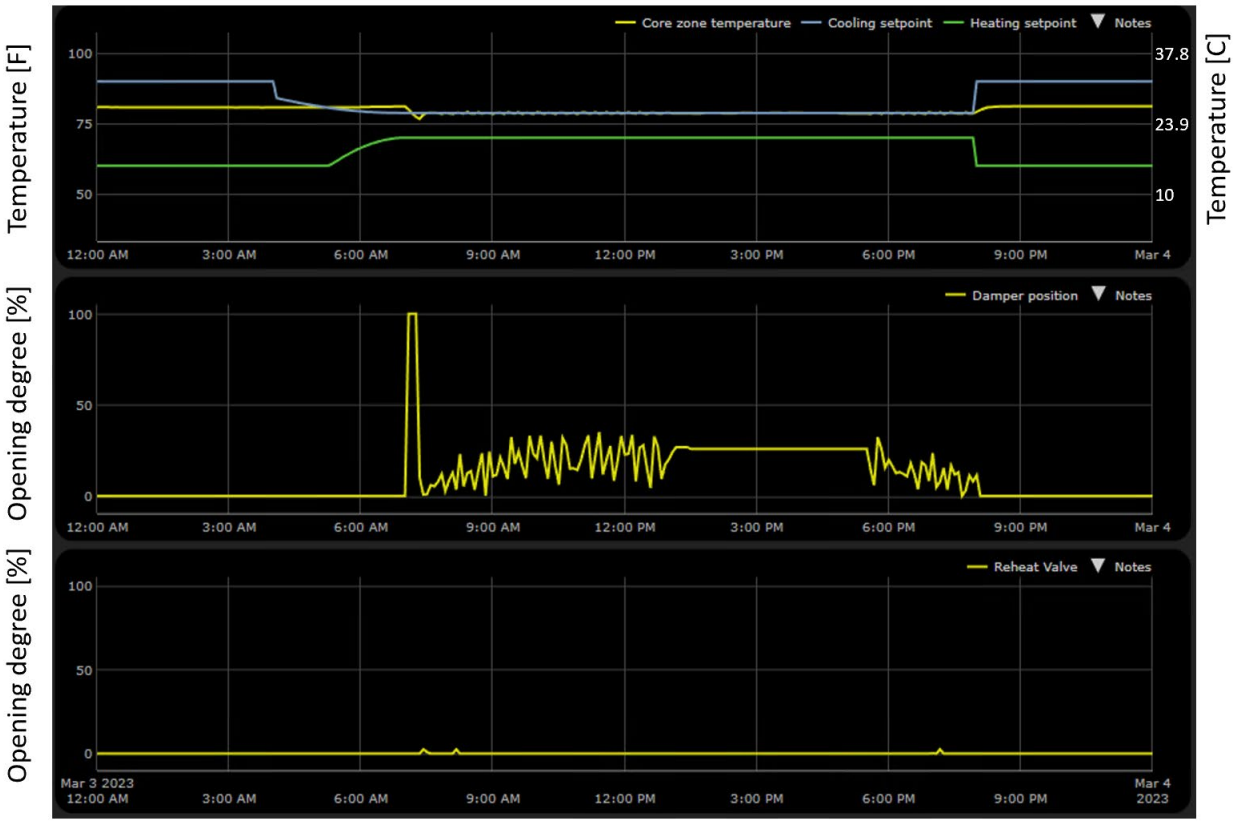

Fig. 9. Real-time measurements of the core zone under control of VAV box.

Case Studies: Physical Fault and Cyber-attack Experiments

Section 4 demonstrates the data generation capability of the HIL testbed by tracking the normal and faulty operating data in the BAS, as well as monitoring the detailed network traffic in the local BAS network. All the other operating parameters in the BAS are available for recording and trending, which captures the system response under normal and imposed faulty conditions.

Normal operation dataset

The BAS server (i.e., WebCTRL^{TM}) continuously oversees the status of all equipment controllers within the local network. Therefore, it provides the capability of recording and trending the operating data over the desired timespan. The data recording can be set with a sampling interval from seconds to hours. The tracked and recorded data can also be stored in files for review and post-operation analysis. Figure 10 shows a part of the measurement data extracted from the BAS server under normal operation. The cooling temperature setpoint is $24\,℃\,(\text{i.e.},75.2\,℉)$. The occupied schedule is from 7 a.m. to 8 p.m.

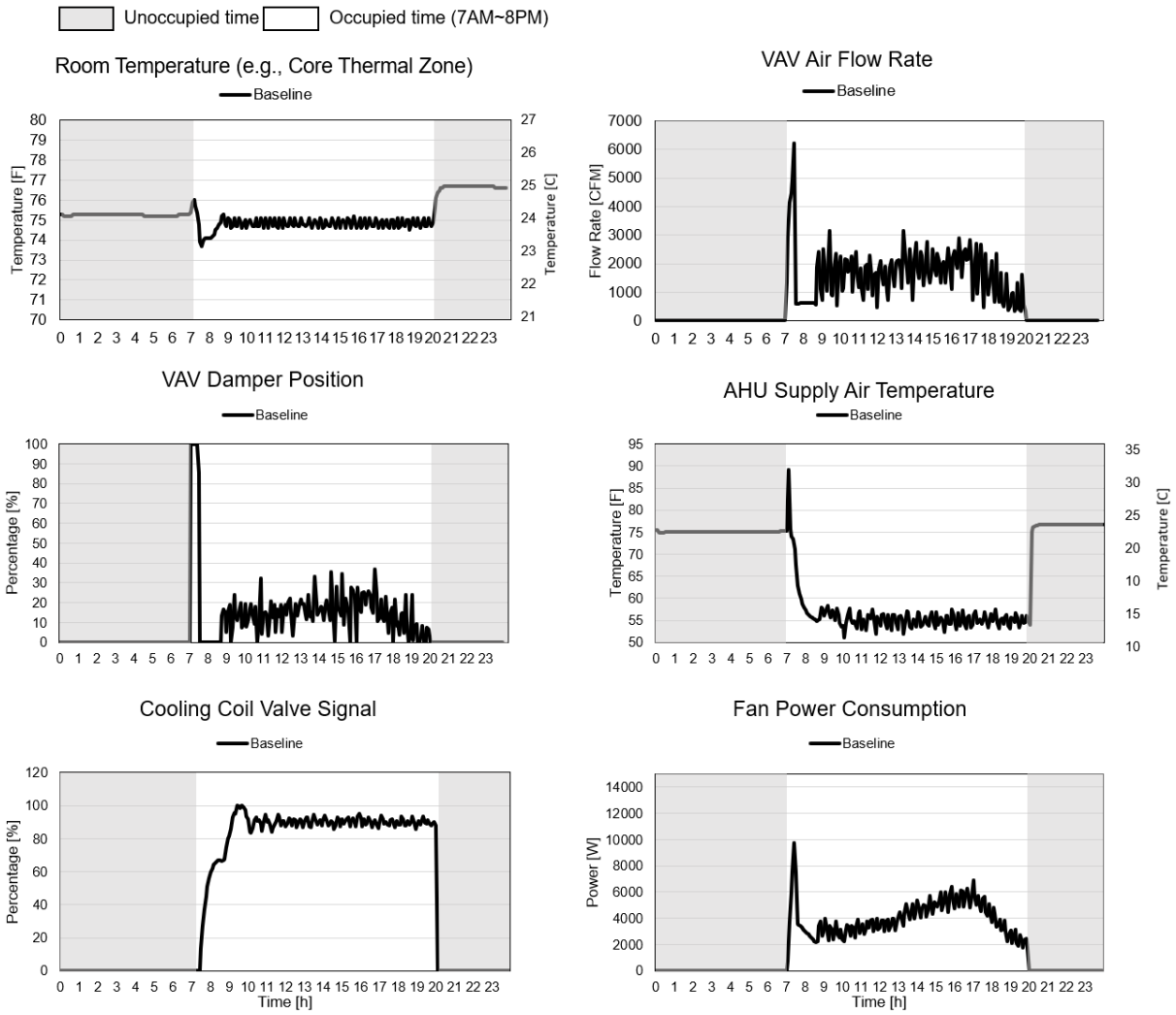

Fig. 10. Measurement data for the normal operation scenario.

Physical fault dataset

To mimic the physical fault, we changed the temperature setpoint of AHU supply air through the WebCTRLTM server to the maximum value, 35 ℃ (95°F), from 10:00 am to 11:00 am. This scenario was tested on August 1st using Typical Meteorological Year version3 (TMY3) weather datasets of Chicago. Figure 11 shows the experimental data of the physical fault scenario. The black lines indicate the normal operating data, which represents the baseline that was free of faults and attacks. For the cooling days, the zone temperature is controlled at 23.9 ℃ (75°F) during occupied periods by adjusting the zone supply air flow rate and AHU supply air temperature in response to zone heat gains and outdoor air conditions. The occupied schedule is 7:00 am – 8:00 pm. The red lines indicate the faulty data measured from the HIL testbed. It's noted that the physical fault impacts the building system during both the attack period and the post-attack period. The post-attack period is defined as the time that a system requires to recover to its baseline

operation after the attack (Fu et al. 2021). For example, during the attack period (10:00 am to 11:00 am), both AHU supply air temperature and zone temperature raised up to 26.7 ℃ (80 °F). Then AHU supply temperature and zone temperature returned to the baseline during the post-attack period (11:00 am to 2:00 pm).

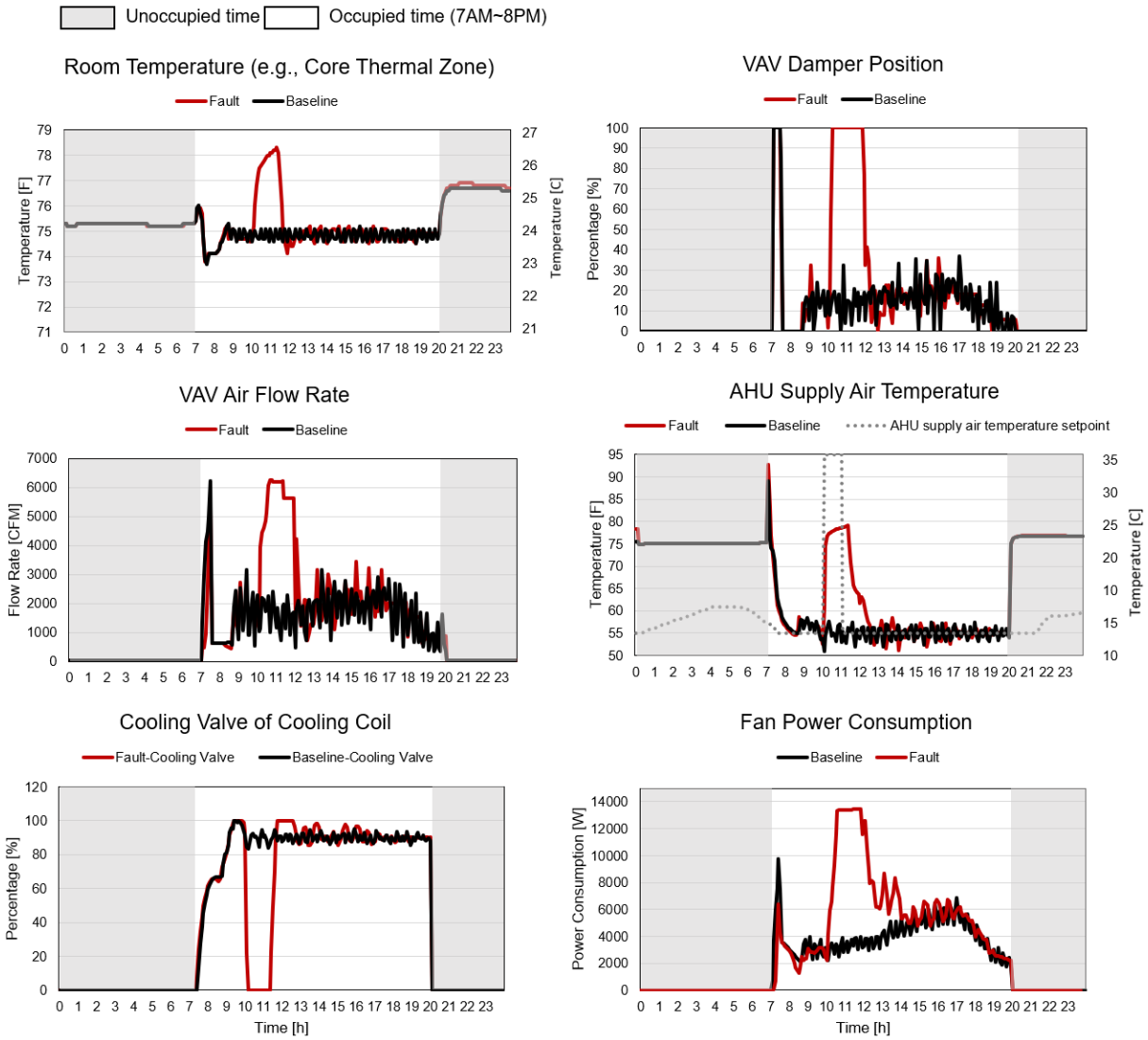

Fig. 11. Measurement data for the physical fault scenario.

Cyber-attack dataset

In most applications, the BACnet protocol does not require authentication for field devices, nor does it encrypt the payloads. An attacker device could register on the BACnet/IP router as a foreign device and join the local broadcast list. To interrupt the service of a critical field device, the attacker can keep sending reinitialization requests so that the target device is constantly in soft-rebooting and fails to answer any benign requests. Using the developed HIL testbed, we were able to apply this device DoS attack on the AHU controller. On the BAS server, we launched an attack

agent using a docker container. This attack agent consists of a lightweight BACnet simulator that communicates directly to the hardware controllers and a Python script that defines the attacking schedule of the BACnet simulator dedicated to breaking down the AHU controller. The device DoS attack was tested on August 1st from 10:00 am to 11:30 am using TMY3 weather datasets of Chicago. Figure 12 shows the experimental data of the cyber-attack scenario. The red lines indicate the faulty data measured from the HIL testbed. The black lines represent the baseline that was free of faults and attacks. During the experiment, it is observed that the reinitialization attack caused missing data points to certain variables of the AHU controller during the attack period. It's noted that the cyber-attack impacts the building system during the attack period (10:00 am to 11:30 am) as well as the post-attack period (11:30 am to 3:00 pm).

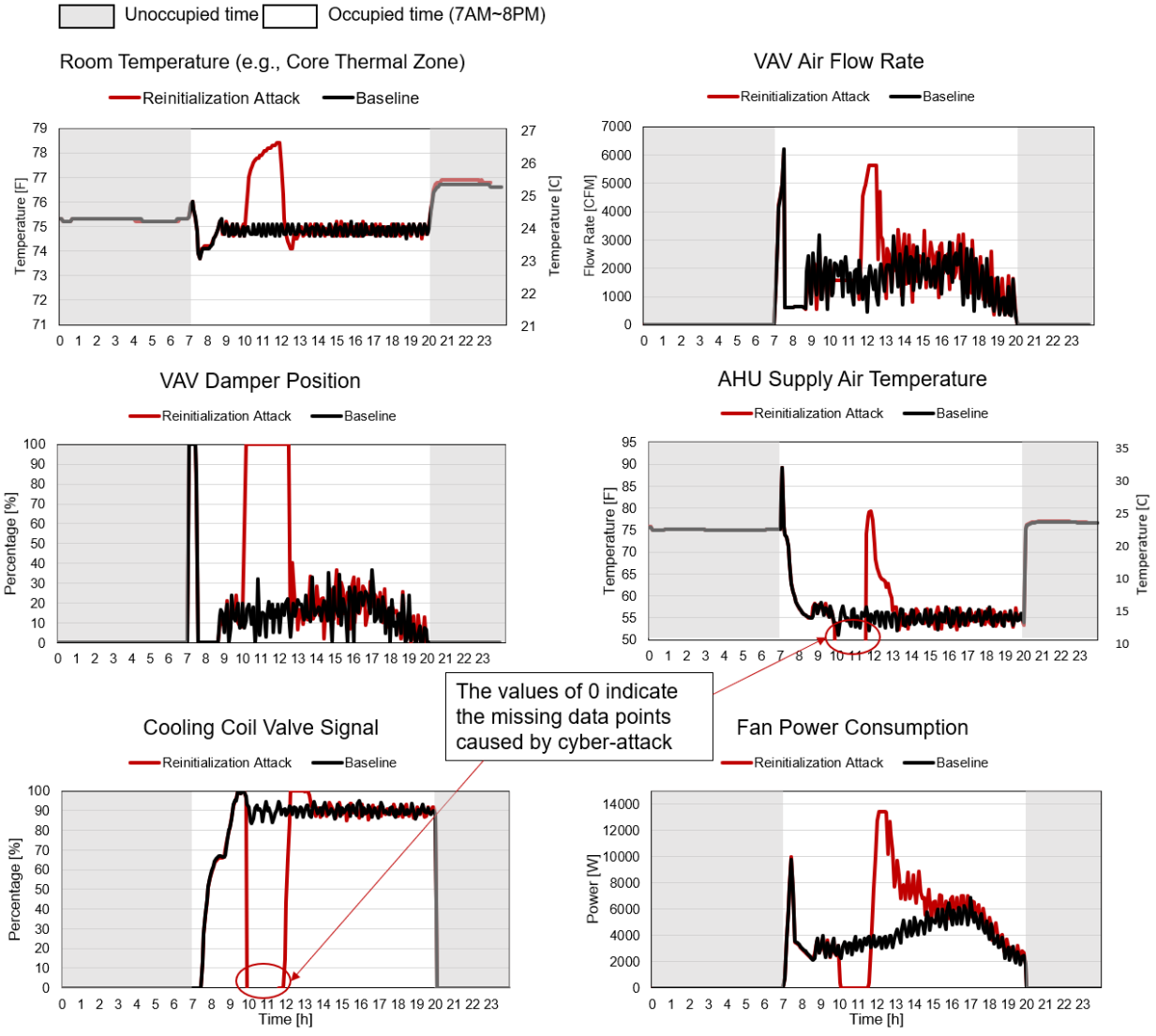

Fig. 12. Measurement data for the cyber-attack scenario.

Network traffic recording

Besides the BAS operating data recorded by the generic WebCTRL™ system, the network traffic in the BAS local network is also critical data used to detect cyber threats. Therefore, the HIL testbed is also equipped with network traffic monitoring capabilities to generate network data with sufficient details for threat analytics. Using the open-source Wireshark software on the BAS server computer enables network traffic monitoring on the ethernet port connecting the server and the BACnet router and the rest of the BAS local controllers. The following example shows the monitored network activities of about 3000s during idle and active operation of the supervisory BAS. Figure 13 shows the network traffic captured during a DoS attack in the HIL testbed. The attack began at around 1100s. The monitored transmission packet rate increased from less than 1000 packets/min up to over 12000 packets/min. In addition to the packet transmission rate illustrated above, Wireshark also keeps track of the addresses, length, protocol, and related information of each packet. Figure 14 shows a screenshot of the network traffic details. The Wireshark keeps track of the addresses, length, protocol, and related information of each packet. The repeating pattern between groups of packets transmit every 10 seconds. Packets are transmitted between the WebCTRL™ server (IP address 10.13.254.2) and the BACnet router (IP address 10.13.254.5) using the BACnet-APDU protocol. These detailed network traffic data generated by the HIL testbed are instrumental for developing algorithms to detect irregular network activities and identify cyber threats against the BAS in our future work.

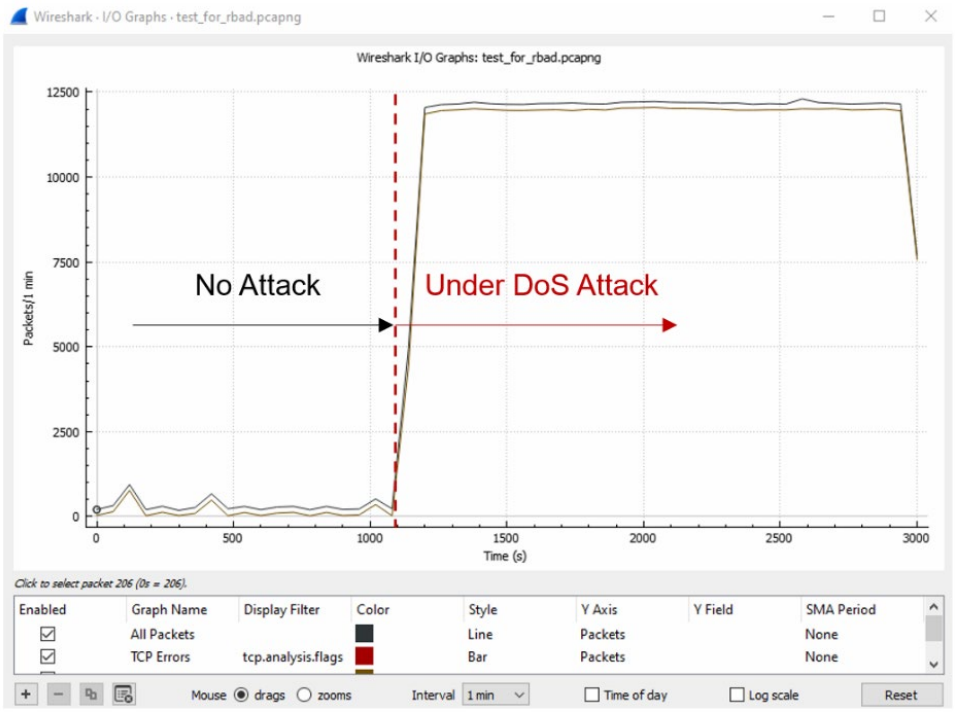

Fig. 13. Transmission packets rate captured from the HIL testbed.

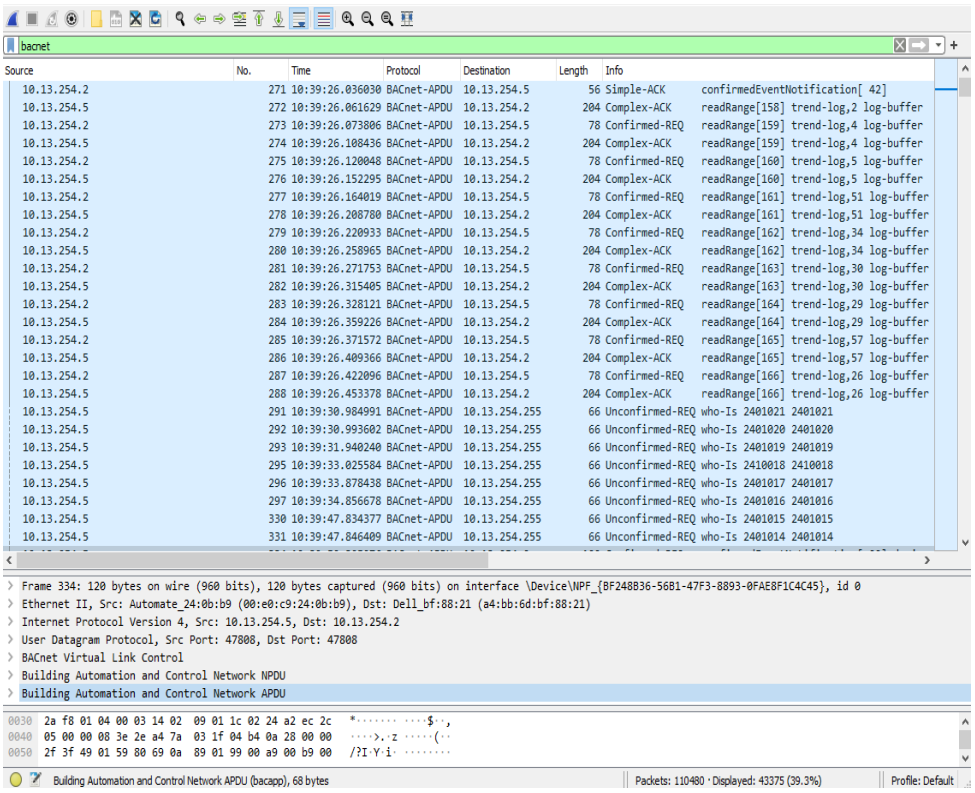

Fig. 14. Network traffic details recorded by the Wireshark.

Conclusions and future work

Conclusions

This paper presents a flexible HIL testbed for cyber-physical security studies on BASs in smart buildings. The HIL testbed consists of a real-time building and HVAC emulator, a set of BAS controllers, and a BAS server computer. The hardware setup and data transmission within the HIL testbed are described in detail. The data generation capability of the HIL testbed is demonstrated by tracking the normal and faulty operating data in the BAS, as well as monitoring the detailed network traffic in the local BAS network. Real-time physical fault and cyber-attack case studies are carried out using the HIL testbed set up for a DOE prototype commercial building. With the help of realistic operation signals from the BAS and building equipment dynamic from simulation, the HIL testbed demonstrates its capability to generate and capture transient responsive behavior of the network of controllers under physical fault and cyber-attack scenarios. The fully functional HIL testbed can now be used to facilitate the development of threat detection and mitigation algorithms.

Future work

The main scope of this paper is to design a flexible HIL testbed supporting sensor and control-related research in smart buildings, and present the data generation capability. The experimental datasets and network traffic data generated from this testbed are instrumental in developing threat detection and mitigation algorithms. Based on the verified capability of the HIL testbed, the future work includes:

- Generate more datasets from physical fault and cyber-attack experiments considering both cyber systems and physical systems under more complex operating conditions.
- Develop cyber-attack detection and physical fault detection algorithms. The HIL testbed will be used to demonstrate whether or not the threat detection and mitigation mechanisms are in action when the algorithms are deployed in the testbed and tested under various scenarios.
- Develop a joint classification framework based on both the network analyzer and fault detection and diagnostics module with the capability of differentiating cyber-attacks and physical faults.
- Develop cyber-resilient control strategies to support efficient and safe operations of buildings under faults and attacks. Adaptive model predictive control and measurement compensator could be used to provide adaptiveness to the building energy systems. Demonstrate the cyber-resilient control strategies through real-time HIL experiments.

Nomenclature

AHU = Air Handling Unit
AI = Analog Input
ALC = Automated Logic Company
ANN = Artificial Neural Network

AO = Analog Output
APDU = Application Protocol Data Unit
API = Application Programming Interface
ARCnet = Attached Resource Computer network
BAS = Building Automation System
BACnet = Building Automation and Control networks
BEMS = Building Energy Management System
BI = Binary Input
BO = Binary Output
COP = Coefficient of Performance
CPS = Cyber-Physical Systems
D/A = Digital/Analog
DAT = Discharge Air Temperature
DOE = Department of Energy
DoS = Denial of Service
DRL = Deep Reinforcement Learning
GEB = Grid-interactive Efficient Building
HIL = Hardware-In-the-Loop
HVAC = Heating, Ventilation, and Air Conditioning
I/O = Input / Output
KPI = Key Performance Indicator
MPC = Model Predictive Control
OCL = Operator's Control Language
PCA = Principle Component Analysis
PI = Proportional-Integral
PID = Proportional-Integral-Derivative
PLC = Programmable Logic Controller
PSO = Particle Swarm Optimization
RBC = Rule-based Control
SAT = Supply Air Temperature
TMY3 = Typical Meteorological Year, version 3
VAV = Variable Air Volume
VFD = Variable Frequency Drive

Funding

The research reported in this paper was partially supported by the Building Technologies Office at the U.S. Department of Energy through the Emerging Technologies program under award number DE-EE0009150.

References

ASHRAE, Guideline. 2018. "36: High performance sequences of operation for HVAC systems." *American Society of Heating, Refrigerating and Air-Conditioning Engineers, Atlanta*.

Åström, Karl J, and Tore Hägglund. 2006. "PID control." *IEEE Control Systems Magazine* 1066.

Blum, David, Javier Arroyo, Sen Huang, Ján Drgoňa, Filip Jorissen, Harald Taxt Walnum, Yan Chen, Kyle Benne, Draguna Vrabie, and Michael Wetter. 2021. "Building optimization testing framework

(BOPTEST) for simulation-based benchmarking of control strategies in buildings." *Journal of Building Performance Simulation* 14 (5):586-610.
Bushby, Steven T, Michael A Galler, Natascha Milesi Ferretti, and Cheol Park. 2010. "The virtual cybernetic building testbed–a building emulator." *ASHRAE Transactions* 116 (1):37-44.
Calfa, Caleb, Zhiyao Yang, Yicheng Li, Zhelun Chen, Zheng O'Neill, and Jin Wen. 2023. "Performance Assessment of a Real Water Source Heat Pump within a Hardware-in-the-Loop (HIL) Testing Environment." *Science and Technology for the Built Environment* (just-accepted):1-26.
Chen, Yongbao, Zhe Chen, Peng Xu, Weilin Li, Huajing Sha, Zhiwei Yang, Guowen Li, and Chonghe Hu. 2019. "Quantification of electricity flexibility in demand response: Office building case study." *Energy* 188:116054.
Crawley, Drury B, Linda K Lawrie, Frederick C Winkelmann, Walter F Buhl, Y Joe Huang, Curtis O Pedersen, Richard K Strand, Richard J Liesen, Daniel E Fisher, and Michael J Witte. 2001. "EnergyPlus: creating a new-generation building energy simulation program." *Energy and Buildings* 33 (4):319-331.
DOE, US. 2015. "Chapter 5: Increasing efficiency of building systems and technologies." *Quadrennial Technology Review: An Assessment of Energy Technologies and Research Opportunities*:143-181.
Fathy, Hosam K, Zoran S Filipi, Jonathan Hagena, and Jeffrey L Stein. 2006. Review of hardware-in-the-loop simulation and its prospects in the automotive area. Paper presented at the Modeling and simulation for military applications.
Fritzson, Peter. 2014. *Principles of object-oriented modeling and simulation with Modelica 3.3: a cyber-physical approach*: John Wiley & Sons.
Fu, Yangyang, Zheng O'Neill, Zhiyao Yang, Veronica Adetola, Jin Wen, Lingyu Ren, Tim Wagner, Qi Zhu, and Terresa Wu. 2021. "Modeling and evaluation of cyber-attacks on grid-interactive efficient buildings." *Applied Energy* 303:117639.
Fu, Yangyang, Zheng O'Neill, and Veronica Adetola. 2021. "A flexible and generic functional mock-up unit based threat injection framework for grid-interactive efficient buildings: A case study in Modelica." *Energy and Buildings* 250:111263.
Goel, Surpriya, Michael Rosenberg, Rahule Athalye, Yulong Xie, W Wang, Reid Hart, Jian Zhang, and Vrushali Mendon. 2014. "Enhancements to ASHRAE standard 90.1 prototype building models." In.: Pacific Northwest National Lab.(PNNL), Richland, WA (United States).
Gunes, Volkan, Steffen Peter, and Tony Givargis. 2015. Improving energy efficiency and thermal comfort of smart buildings with HVAC systems in the presence of sensor faults. Paper presented at the 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems.
Holmberg, David G, and D Evans. 2003. *BACnet wide area network security threat assessment*: US Department of Commerce, National Institute of Standards and Technology.
Honorof, Marshall. 2013. "Building Hack Almost Landed Google in Hot Water." In, https://www.nbcnews.com/id/wbna51805522.
Huang, Sen, Weimin Wang, Michael R Brambley, Siddharth Goyal, and Wangda Zuo. 2018. "An agent-based hardware-in-the-loop simulation framework for building controls." *Energy and Buildings* 181:26-37.
Huang, Yu-Lun, Alvaro A Cárdenas, Saurabh Amin, Zong-Syun Lin, Hsin-Yi Tsai, and Shankar Sastry. 2009. "Understanding the physical and economic consequences of attacks on control systems." *International Journal of Critical Infrastructure Protection* 2 (3):73-83.
Isermann, Rolf, Jochen Schaffnit, and Stefan Sinsel. 1999. "Hardware-in-the-loop simulation for the design and testing of engine-control systems." *Control Engineering Practice* 7 (5):643-653.
Kaur, Jaspreet, Jernej Tonejc, Steffen Wendzel, and Michael Meier. 2015. Securing BACnet's pitfalls. Paper presented at the IFIP International Information Security and Privacy Conference.

Li, Guowen, Yangyang Fu, Amanda Pertzborn, Zheng O'Neill, and Jin Wen. 2022. Demand flexibility evaluation for building energy systems with active thermal storage using model predictive control. Paper presented at the 2022 ASHRAE Annual Conference, Toronto, Canada.

Li, Guowen, Yangyang Fu, Amanda Pertzborn, Jin Wen, and Zheng O'neill. 2021. An Ice Storage Tank Modelica Model: Implementation and Validation. Paper presented at the Modelica Conferences.

Li, Guowen, Zheng O'Neill, Jin Wen, Ojas Pradhan, Lingyu Ren, Teresa Wu, Veronica Adetola, K Selcuk Candan, and Qi Zhu. 2023. CYDRES: CYber Defense and REsilient System for securing grid-interactive efficient buildings. Paper presented at the Proceedings of the 10th ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation.

Li, Guowen, Lingyu Ren, Yangyang Fu, Zhiyao Yang, Veronica Adetola, Jin Wen, Qi Zhu, Teresa Wu, K Selcuk Candanf, and Zheng O'Neill. 2023. "A critical review of cyber-physical security for building automation systems." *Annual Reviews in Control*. https://doi.org/https://doi.org/10.1016/j.arcontrol.2023.02.004.

Li, Guowen, Zhiyao Yang, Yangyang Fu, Lingyu Ren, Zheng O'Neill, and Chirag Parikh. 2022. "Development of a hardware-In-the-Loop (HIL) testbed for cyber-physical security in smart buildings." *arXiv preprint arXiv:2210.11234*.

Lou, Xin, Cuong Tran, Rui Tan, David KY Yau, and Zbigniew T Kalbarczyk. 2019. Assessing and mitigating impact of time delay attack: a case study for power grid frequency control. Paper presented at the Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems.

Lu, Xing, Yangyang Fu, Zheng O'Neill, and Jin Wen. 2021. "A holistic fault impact analysis of the high-performance sequences of operation for HVAC systems: Modelica-based case study in a medium-office building." *Energy and Buildings* 252:111448.

O'Neill, Zheng, and Aaron Henry. 2016. Development of a Hardware-in-the-loop Framework with Modelica for Energy Efficient Buildings. Paper presented at the Proceedings of the 3rd ACM International Conference on Systems for Energy-Efficient Built Environments.

Otten, Richard, Bin Li, and Andrew Alleyne. 2010. "Hardware-in-the-loop load emulation for air-conditioning and refrigeration systems."

Paridari, Kaveh, Niamh O'Mahony, Alie El-Din Mady, Rohan Chabukswar, Menouer Boubekeur, and Henrik Sandberg. 2017. "A framework for attack-resilient industrial control systems: Attack detection and controller reconfiguration." *Proceedings of the IEEE* 106 (1):113-128.

Peacock, Matthew. 2019. "Anomaly detection in bacnet/ip managed building automation systems."

Roth, Amir, and Janet Reyna. 2019. "Grid-interactive efficient buildings technical report series: Whole-building controls, sensors, modeling, and analytics." In.: USDOE Office of Energy Efficiency and Renewable Energy (EERE), Energy ….

Seem, John E. 1998. "A new pattern recognition adaptive controller with application to HVAC systems." *Automatica* 34 (8):969-982.

Sridhar, Siddharth, and Manimaran Govindarasu. 2014. "Model-based attack detection and mitigation for automatic generation control." *IEEE Transactions on Smart Grid* 5 (2):580-591.

Sridhar, Siddharth, and G Manimaran. 2010. Data integrity attacks and their impacts on SCADA control system. Paper presented at the IEEE PES general meeting.

Taylor, S. 2020. "Advanced Sequences of Operation for HVAC Systems-Phase II Central Plants and Hydronic Systems." *ASHRAE RP-1711 (in progress)*.

Vijayan, Jaikumar. 2014. "Target attack shows danger of remotely accessible HVAC systems." In, https://www.computerworld.com/article/2487452/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html.

Wardell, Dean C, Robert F Mills, Gilbert L Peterson, and Mark E Oxley. 2016. "A method for revealing and addressing security vulnerabilities in cyber-physical systems by modeling malicious agent interactions with formal verification." *Procedia computer science* 95:24-31.

Werth, Aaron W, and Thomas H Morris. 2021. Prototyping PLCs and IoT Devices in an HVAC Virtual Testbed to Study Impacts of Cyberattacks. Paper presented at the Proceedings of Fifth International Congress on Information and Communication Technology: ICICT 2020, London, Volume 1.

Wetter, Michael, Wangda Zuo, Thierry S Nouidui, and Xiufeng Pang. 2014. "Modelica buildings library." *Journal of Building Performance Simulation* 7 (4):253-270.

Xu, Peng, Philip Haves, and Joe Deringer. 2004. "A simulation-based testing and training environment for building controls."

Zhang, Yue, Scott Eisele, Abhishek Dubey, Aron Laszka, and Anurag K Srivastava. 2019. Cyber-physical simulation platform for security assessment of transactive energy systems. Paper presented at the 2019 7th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES).

Zhao, Futao, James Fan, and Stevo Mijanovic. 2013. PI auto-tuning and performance assessment in HVAC systems. Paper presented at the 2013 American control conference.

Zhao, Yang, Tingting Li, Xuejun Zhang, and Chaobo Zhang. 2019. "Artificial intelligence-based fault detection and diagnosis methods for building energy systems: Advantages, challenges and the future." *Renewable and Sustainable Energy Reviews* 109:85-101.