A Cybersecurity Testbed for Smart Buildings

Sivasathya Balamurugan, Steve Granda, Selam Haile, Anya Petersen, Jing Wang, and Jiazhen Ling

National Renewable Energy Laboratory

Presented at the 2023 ASHRAE Annual Conference
Tampa, Florida
June 24-28, 2023

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Conference Paper
NREL/CP-5R00-85639
March 2024

A Cybersecurity Testbed for Smart Buildings

Sivasathya Balamurugan, Steve Granda, Selam Haile, Anya Petersen, Jing Wang, and Jiazhen Ling

National Renewable Energy Laboratory

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Conference Paper
NREL/CP-5R00-85639
March 2024

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Building Technologies Office. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

Cover Photos by Dennis Schroeder: (clockwise, left to right) NREL 51934, NREL 45897, NREL 42160, NREL 45891, NREL 48097, NREL 46526.

NREL prints on paper that contains recycled content.

TA-23-C055

A Cybersecurity Testbed for Smart Buildings

Sivasathya Balamurugan **Steve Granda** **Selam Haile**

Anya Petersen **Jing Wang**
Full Member ASHRAE **Jiazhen Ling**
Full Member ASHRAE

ABSTRACT

Smart buildings are equipped with a plethora of cyber-physical systems, such as Internet of Things (IoT) devices and building automation systems. These devices, especially in commercial buildings, use legacy communications and hardware that were not designed with cybersecurity in mind. With increasing cyber threats in recent years, smart buildings have become an increasing target for attacks, but not enough published data are available from these incidents to study or replicate the scenarios to defend buildings. As part of the U.S. Department of Energy-funded project focusing on developing the Building Intelligence with Layered Defense Using Security-Constrained Optimization and Security Risk Detection (BUILD-SOS) platform, we developed a cybersecurity test bed for smart buildings. This test bed includes a building simulation tool, virtual devices, emulated operational technology networks, and remote hardware-in-the-loop. Using this test bed, we performed different cyberattacks on the smart building model and collected both physical building data, to understand the impacts on the building, and network data, to aid in separating mechanical faults from cyberattacks during the detection. This test bed is a significant tool in protecting smart buildings from cyberattacks because they can aid in both cybersecurity analysis and the evaluation of cyberattack detection tools by testing the tools in a secure environment without impacting the building operations.

INTRODUCTION

In recent years, building control systems have become increasingly interconnected with various smart components, distributed energy resources, and grid edge devices, allowing for more finely tuned control of building services ranging from heating, ventilating, and air-conditioning (HVAC) to lighting. As these devices are connected to larger control networks, their overall attack surface expands as well. Although traditional technical controls, such as network firewalls, are often deployed in building control networks, many building control devices residing on these networks are still resource-constrained, embedded systems that lack end point security and/or regular firmware updates. Further, gauging risks on these control networks through penetration testing can result in building hazards for occupants or costly bricking of devices, such as for legacy installations. As these systems are modernized, their

Sivasathya Balamurugan is a cybersecurity researcher, National Renewable Energy Laboratory (NREL), Golden, Colorado. **Steve Granda** is a cybersecurity researcher at NREL, Golden, Colorado. **Selam Haile** is a mechanical engineering researcher for buildings at NREL, Golden, Colorado. **Anya Petersen** is a senior software engineer for buildings at NREL, Golden, Colorado. **Jing Wang** is a mechanical engineering researcher for buildings at NREL, Golden, Colordao. **Jiazhen Ling** is a mechanical engineering researcher for buildings at NREL, Golden, Colorado.

overall architectures and control principles remain fundamentally the same, often retaining backward compatibility with legacy installations. In our test bed, we aim to capture these core tenants to allow researchers the capability to simulate the effects on the physics of real-world building models with hardware-in-the-loop (HIL) while performing cyberattacks and evaluation of cyberattack detection tools in a fully closed feedback loop without risks to real buildings or occupants.

BUILD-SOS TEST BED ARCHITECTURE

The test bed was architected to follow a typical building control network comprising a centralized device responsible for monitoring and scheduling operations. This topology, which commonly includes a device such as a building automation system (BAS) at its core, is critical. The design is based on monitoring and protecting a centralized point that is most valuable to attackers, pivoting across networks such as the BAS. The BAS is typically used to monitor sensors and control components, such as power systems, lighting, and HVAC, which often communicate over protocols such as Modbus, KNX, and BACnet. We selected the BACnet protocol to perform the cyber evaluations in this test bed. By virtually recreating the setup in the test bed as shown in Figure 1, we can leverage it to study the impacts of cyberattacks on smart buildings without impacting real buildings.

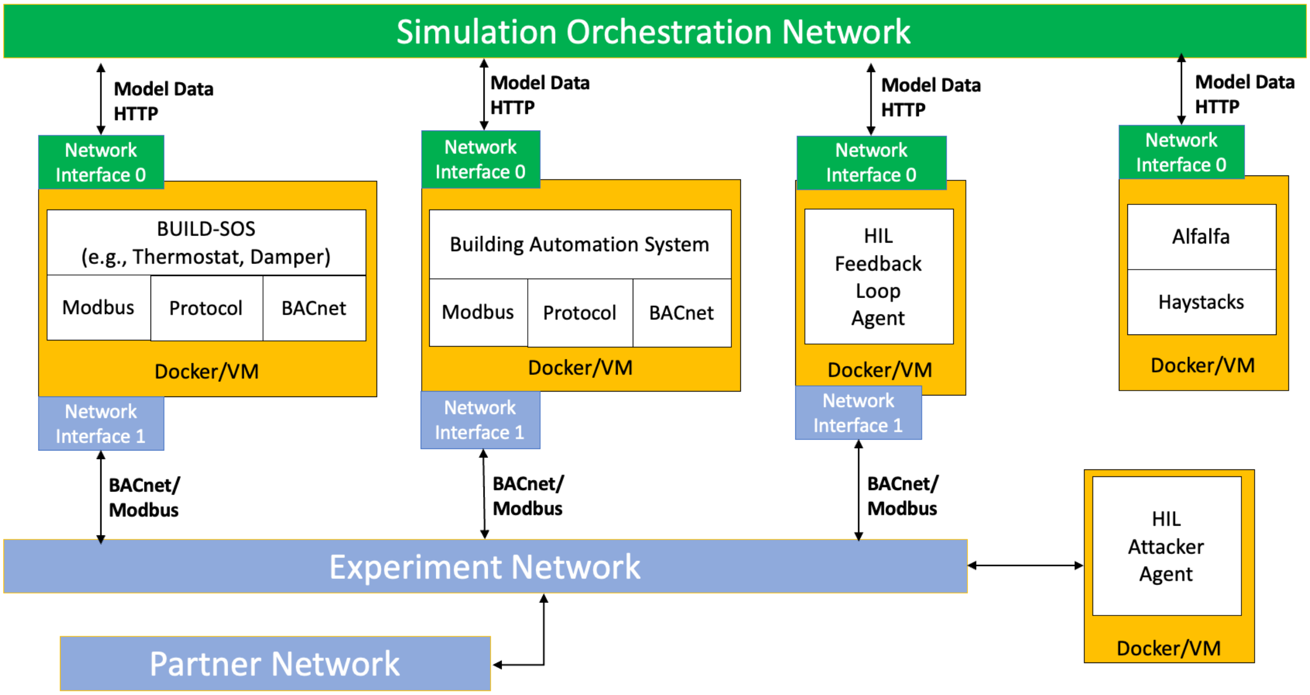


Figure 1 Architecture of the BUILD-SOS test bed

For realism during simulation, we used Alfalfa to provide the building status during both blue-sky operation and under an attack. As this model is running, it can receive input and provide output of the building state through a RESTful application programming interface (API). The building state can only be accessed using the API over a network, which we call the Simulation Orchestration Network.

Inside this network, docker containers and virtual machines represent devices acting as thermostats, air dampers, etc., that can poll the model for any changes and provide input for changes in state, such as temperature set points. We also used this orchestration network to integrate the state of the HIL with the simulation using a feedback loop agent, which continuously polls and updates the running building model with HIL sensor data.

With the virtualized devices and the HIL capability of communicating changes to the building model, we pivoted to the cyber aspects of communication on the experiment network. The experiment network was created to handle cyber activities such as the command-and-control traffic of the virtual devices, the HIL, and corresponding attacks. In the experiment network, the BAS was made to continuously monitor other devices, such as an air damper or thermostats, using the BACnet protocol to poll for changes. As changes are detected by the BAS, either through direct set point changes on the virtual devices or via a malicious actor carrying out attacks on the experiment network, the BAS pushes those updates to the model using the Simulation Orchestration Network. The state of the externally located HIL or virtual devices can be brought into both the model and the cyber network using the feedback loop agent connected over the partner's network segment, e.g., via a virtual private network (VPN) bridge.

The following section details the tools and models used to simulate the infrastructure and the networks of a commercial building.

Virtual Building

The study of building operation and device interaction, including control decisions and hacking scenarios, requires interactions with physics-based building energy models (BEMs) to read sensor values and control actuators as the simulation runs. This run time interaction allows external control integrations to impact the building operation and the collection of performance data across operational scenarios. Traditional applications of BEMs have been for offline analysis; models are configured and run non-interactively for intervals of one year or longer, and then the results are analyzed. Variations of physics-based BEM engines and extensive libraries of models have been built out over decades, including OpenStudio® (OpenStudio 2023), EnergyPlus® (EnergyPlus 2023), the Modelica Buildings library (Wetter et al. 2014), Spawn of EnergyPlus (Wetter et al. 2020), and BOPTEST (Blum et al. 2020). For the required run time interaction with BEMs, the BUILD-SOS platform leverages the open-source Alfalfa (Alfalfa 2023) web service for virtual buildings. Alfalfa manages the messy details of run time communication with building simulation and abstracts the choice of engine. Communication with BEMs is over a RESTful API that can run at a configurable timescale, with timescale one corresponding to real-world time. Alfalfa is a containerized web application stack built according to software engineering best practices, and the Alfalfa open-source ecosystem includes resources for deployment to a variety of on-premises or cloud computing platforms (Alfalfa Helm 2023) and for BACnet integration (Alfalfa BACnet Bridge 2023).

Building Modeling

Medium office building. This test case represents a one-floor new-construction building with five zones in Chicago, IL, USA, with total floor area of 1662.66 m^2. There are four perimeter zones and one core zone. The HVAC system is a single-duct, multizone, variable air volume (VAV) system with terminal reheat with one air handling unit (AHU). The AHU cooling coil is served by an air-cooled chiller, whereas the heating coil and the terminal box reheat coils are served by an air-to-water heat pump. The embedded controls for the AHU include supply fan static pressure reset and a dry-bulb economizer, whereas the terminal box controls use single-maximum airflow control.

Campus building. A Modelica-based high-fidelity model of a campus building was used to simulate the transient thermal performance of a research building located in a cooling-dominant climate and its associated HVAC systems (i.e., equipment and control) to facilitate various fault scenario studies. The model uses Spawn of EnergyPlus, jointly developed by the National Renewable Energy Laboratory and Lawrence Berkeley National Laboratory (LBNL), and LBNL's Modelica Buildings library, to co-simulate the thermal response from an EnergyPlus-based building model with HVAC equipment. The model includes three types of main components: a Spawn of EnergyPlus-based thermal zone model, a set of HVAC equipment including AHUs with VAV terminal boxes and fan coil units (FCUs) serving the thermal zones, and various types of control blocks for the HVAC system air side and water side. The EnergyPlus building model contains 18 thermal zones that are subject to various external and internal loads. The

HVAC equipment conditioned these thermal zones by either a combination of AHU and VAV reheat box or FCUs. Dedicated AHUs are also used to condition ambient fresh air to meet the indoor air quality requirement. Various control blocks were added to control the supply air temperature from the AHU and VAV reheat box, the fan speed, and the indoor air temperature set points. The model also simulates space carbon dioxide (CO2) concentrations by defining CO2 as a trace particle mixed with moist air, and the concentrations among various thermal zones are used as the basis for the fresh airflow rate control.

Virtual Devices

In the test bed, we modeled the operation of the BAS by emulating BACnet network communication and integrating typical command-and-control characteristics of devices in a building controlled by BAS. For this paper, we developed models of thermostat and dampers to represent some devices in the building model. The BAS device is responsible for controlling the building operation based on the building status received from Alfalfa. Using the state of the model, the BAS decides on the controls for various devices and communicates this to additional devices on the network using the BACnet protocol. The damper model is responsible for emulating an airflow damper device. The damper device is controlled over the network by polling the BAS for updates over the BACnet protocol. The operation of the damper, such as changing the damper position from “open” to “close,” will update its status in the building model, establishing a closed feedback loop. The thermostat model is used to control different HVAC units in the building.

The zone thermostat is responsible for providing feedback to the VAV damper model so that it will open or close based on the current temperature condition of the space it is serving. Depending on the opening of the VAV damper, the AHU fan will provide the necessary airflow. Modeling new virtual devices is completely possible because our codebase is easily extensible with many of the protocol and communication requirements handled by BAC0.

Hardware-in-the-Loop

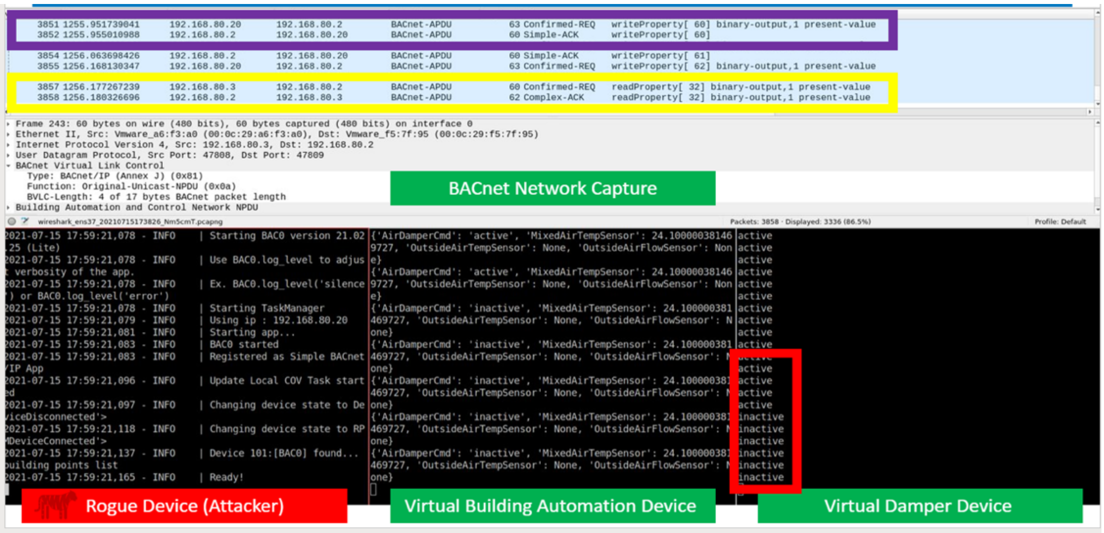
To extend the operation of our test bed and include external devices such as HIL or virtual devices from a partner, we used a VPN to tunnel data over a connected docker bridge. This tunnel allows devices on the experiment network, to communicate to an external partner network and exchange BACnet data. The addition of our feedback loop agent also allows us to readily integrate HIL devices to obtain physical device sensor status into a running Alfalfa model and provides a cyber component by relaying those value changes over BACnet.

Emulated Network

We chose the BACnet protocol as the default communication protocol to replicate the building automation and control. To emulate BACnet devices, Python scripts using BACpypes and the BAC0 library were deployed in docker containers communicating through the experiment network, which was emulated using an isolated docker network.

Attacker

The malicious actor was another virtual device used to attack building devices communicating over the experiment network. Simulated attackers in our topology were assumed to have pivoted to the building’s network and behaved as rogue devices. We implemented the rogue device in Python using the same BACnet communication libraries and codebase extended from our other virtual devices. The attacker device was configured to perform attacks on specific points by manipulating the BACnet communication through methods such as denial of service and register flooding, and it can perform reconnaissance by continuously polling registers on targets attached to the experiment network. Using the emulated network, the attacker was also capable of reaching outside the experiment network through the docker bridge and over a connected partner VPN. Figure 2 shows the Wireshark captures of the network data during the cyber-attack placed by the rogue device and the screenshot of the damper device shows the value being changed as part of the attack.



```
3851 1255.951739041   192.168.80.20   192.168.80.2    BACnet-APDU   63 Confirmed-REQ   writeProperty[ 60] binary-output,1 present-value
3852 1255.955010988   192.168.80.2    192.168.80.20   BACnet-APDU   60 Simple-ACK      writeProperty[ 60]
3854 1256.063698426   192.168.80.2    192.168.80.20   BACnet-APDU   60 Simple-ACK      writeProperty[ 61]
3855 1256.168130347   192.168.80.20   192.168.80.2    BACnet-APDU   63 Confirmed-REQ   writeProperty[ 62] binary-output,1 present-value
3857 1256.177267239   192.168.80.3    192.168.80.2    BACnet-APDU   60 Confirmed-REQ   readProperty[ 32] binary-output,1 present-value
3858 1256.180326696   192.168.80.2    192.168.80.3    BACnet-APDU   62 Complex-ACK     readProperty[ 32] binary-output,1 present-value
```

```
▸ Frame 243: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: Vmware_a6:f3:a0 (00:0c:29:a6:f3:a0), Dst: Vmware_f5:7f:95 (00:0c:29:f5:7f:95)
▸ Internet Protocol Version 4, Src: 192.168.80.3, Dst: 192.168.80.2
▸ User Datagram Protocol, Src Port: 47808, Dst Port: 47809
▾ BACnet Virtual Link Control
    Type: BACnet/IP (Annex J) (0x81)
    Function: Original-Unicast-NPDU (0x0a)
    BVLC-Length: 4 of 17 bytes BACnet packet length
▸ Building Automation and Control Network NPDU
```

BACnet Network Capture
wireshark_ens37_20210715173826_Nm5cmT.pcapng
Packets: 3858 · Displayed: 3336 (86.5%)
Profile: Default

```
2021-07-15 17:59:21,078 - INFO    | Starting BAC0 version 21.02
.25 (Lite)
2021-07-15 17:59:21,078 - INFO    | Use BAC0.log_level to adjus
t verbosity of the app.
2021-07-15 17:59:21,078 - INFO    | Ex. BAC0.log_level('silence
') or BAC0.log_level('error')
2021-07-15 17:59:21,078 - INFO    | Starting TaskManager
2021-07-15 17:59:21,079 - INFO    | Using ip : 192.168.80.20
2021-07-15 17:59:21,081 - INFO    | Starting app...
2021-07-15 17:59:21,083 - INFO    | BAC0 started
2021-07-15 17:59:21,083 - INFO    | Registered as Simple BACnet
/IP App
2021-07-15 17:59:21,096 - INFO    | Update Local COV Task start
ed
2021-07-15 17:59:21,097 - INFO    | Changing device state to De
viceDisconnected'>
2021-07-15 17:59:21,118 - INFO    | Changing device state to RP
MDeviceConnected'>
2021-07-15 17:59:21,137 - INFO    | Device 101:[BAC0] found...
building points list
2021-07-15 17:59:21,165 - INFO    | Ready!
```

```
{'AirDamperCmd': 'active', 'MixedAirTempSensor': 24.10000038146
9727, 'OutsideAirTempSensor': None, 'OutsideAirFlowSensor': Non
e}
{'AirDamperCmd': 'active', 'MixedAirTempSensor': 24.10000038146
9727, 'OutsideAirTempSensor': None, 'OutsideAirFlowSensor': Non
e}
{'AirDamperCmd': 'inactive', 'MixedAirTempSensor': 24.100000381
469727, 'OutsideAirTempSensor': None, 'OutsideAirFlowSensor': N
one}
{'AirDamperCmd': 'inactive', 'MixedAirTempSensor': 24.100000381
469727, 'OutsideAirTempSensor': None, 'OutsideAirFlowSensor': N
one}
{'AirDamperCmd': 'inactive', 'MixedAirTempSensor': 24.100000381
469727, 'OutsideAirTempSensor': None, 'OutsideAirFlowSensor': N
one}
{'AirDamperCmd': 'inactive', 'MixedAirTempSensor': 24.100000381
469727, 'OutsideAirTempSensor': None, 'OutsideAirFlowSensor': N
one}
{'AirDamperCmd': 'inactive', 'MixedAirTempSensor': 24.100000381
469727, 'OutsideAirTempSensor': None, 'OutsideAirFlowSensor': N
one}
```

```
active
active
active
active
active
active
active
active
active
active
active
active
active
active
active
inactive
inactive
inactive
inactive
inactive
inactive
```

Figure 2 Screenshot showing the attacker overwriting values in a damper device.

EXPERIMENTAL SCENARIOS & ANALYSIS

We defined a comprehensive list of scenarios to depict the impacts of the cyber-induced faults on different types of buildings in different seasons, as shown in Table 1. A complete data set has been published as well (Balamurugan et al. 2023).

Table 1. List of Scenarios

Scenario No.	Building Model	Season	Cyber-Induced Fault	Impact
S1	Medium office	Summer	None	Business-as-usual
S2	Medium office	Winter	None	Business-as-usual
S3	Medium office	Summer	Cooling coil stuck closed	Thermal discomfort
S4	Medium office	Winter	Simultaneous heating and cooling	Energy waste, increased operational cost
S5	Medium office	Winter	Outside air damper stuck open	Energy waste
C1	Campus	Summer	None	Business-as-usual
C2	Campus	Summer	Overridden thermostat set point	Occupant discomfort and energy waste

Cooling Coil Stuck Closed—S3

During normal operation, the cooling coil valves are controlled by the supply air temperature set point, whereas the VAV dampers are controlled by the space temperature set points. In this attack scenario, the operation of the cooling coil was disrupted by commanding it to be stuck closed. The attack lasted for 10 hours, from 8:00 a.m. until 6:00 p.m. When the coil was 100% closed, the supply air temperature increased from 53°F (285K) to 77°F (298K), which led to an increase in the zone temperature from 68°F (293K) to 74°F (296.5K), as shown in Figure 3. This increase would cause thermal discomfort or affect processes or equipment in spaces such as a data center.

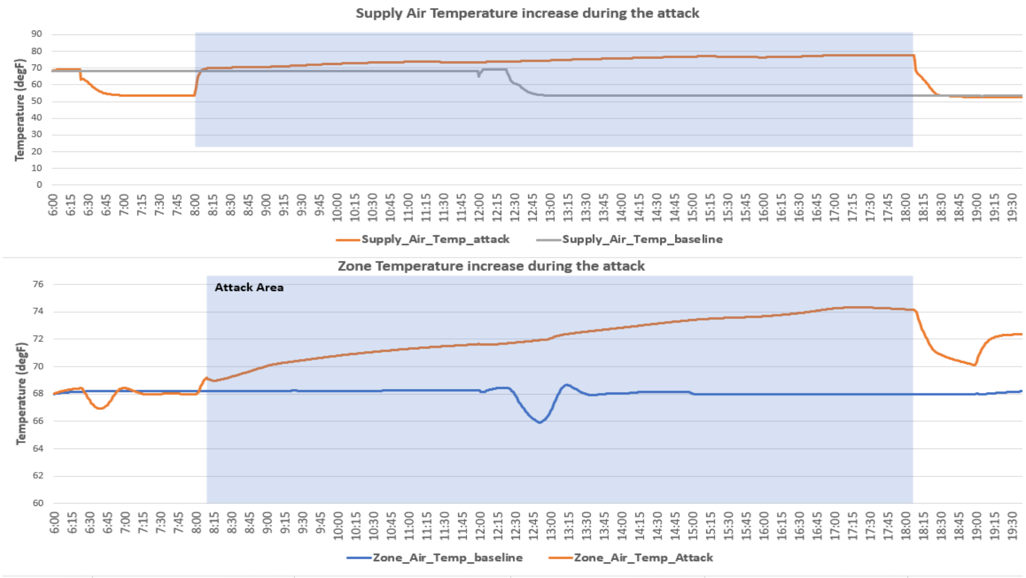


Figure 3 Cooling coil stuck closed attack for a multizone VAV system.

Simultaneous Heating and Cooling—S4

During normal operation, there would not be simultaneous heating and cooling by an AHU. This usually happens when there is a cooling coil leak. When this happens, the heating coil needs to open to offset the extra cooling. In this attack scenario, we simulated a cyberattack that changes the normal operation of the AHU and forces a 50% heating valve opening during winter irrespective of the space condition. As shown in Figure 4, the attack lasted for 8 hours, from 8:00 a.m. until 4:00 p.m. During the attack, the cooling valve had to open to compensate for the unnecessary heating because of the attack causing energy losses in both the cooling and heating systems. Figure 4 shows the impact of the attack on the chiller and heat pump energy consumptions.

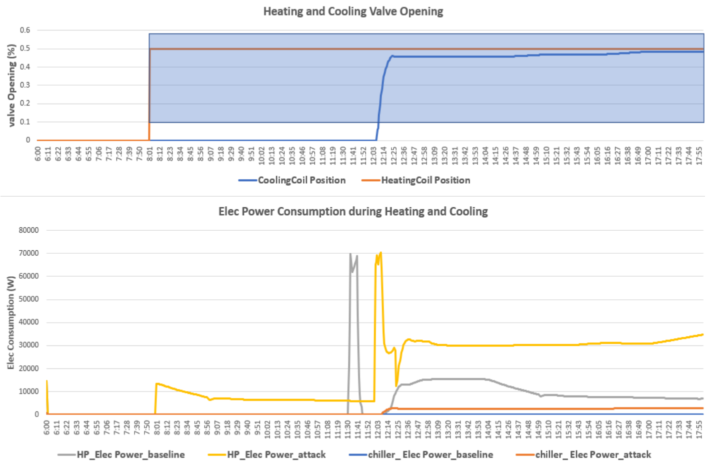


Figure 4 Simultaneous heating and cooling attack for multizone VAV system

Outside Air Damper Stuck Open—S5

During winter, the outside air damper needs to be open to its minimum damper position, which is usually determined by the ventilation requirements of the space it is serving. Bringing in more outdoor air than is needed for ventilation will make the operation more energy intensive because it requires more energy to heat the relatively colder outdoor air temperature. In this attack scenario, we simulated a condition where the attacker forced the outside air damper to be stuck open at 80%. As shown in Figure 5, during the attack, which lasted from 8 a.m. until 4 p.m., the mixed temperature dropped below its value before the attack started due to the mixing of a relatively small fraction of return air with a higher fraction of colder outdoor air caused by the attack. As a result, the heat pump was forced to operate more frequently and consume more energy than the baseline, as indicated in Figure 5.

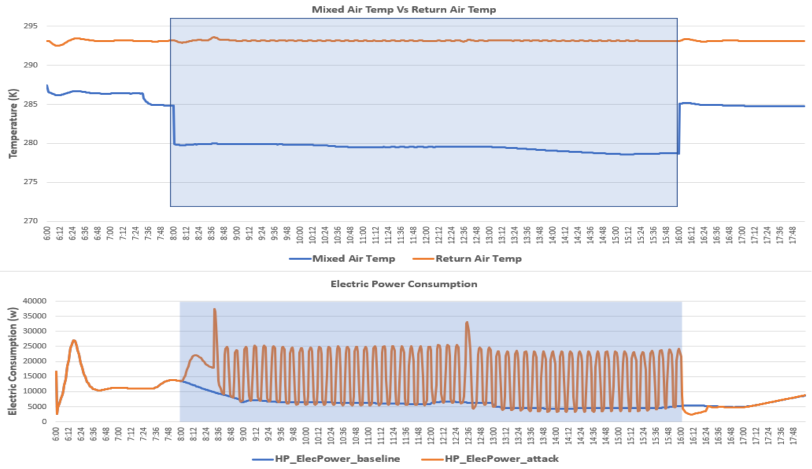


Figure 5 Outside air damper stuck open attack for multizone VAV system.

Overridden Thermostat Set Point—C2

In this HIL experiment, we performed a cyberattack on the thermostat in the room in a campus building. The zone was conditioned by a VAV with reheat coil. The central hot water plant was a source for heat for the reheat coil. The valve for the reheat coil was modulated by the zone space temperature and space temperature set point, 69.5°F (294K). This attack lasted for 5 hours, from 12:00 p.m. until 5:00 p.m. Before the attack, the controller was able to meet the zone temperature set point by checking the valve opening to control the flow of the hot water coming into the coil. During the attack, the zone temperature sensor value was overridden to read a value of 59°F (288K) irrespective of the space condition. This space temperature value was lower than the set point and forced the controller to believe that the space was colder than it was. As a result, the hot water valve was fully open so that more hot water would flow into the VAV, and the heater was continuously working. This resulted in the actual space temperature to be well above the temperature set point, 78.5°F (299K), as shown in Figure 6. This would implicate occupant discomfort due to the high room temperature, and it would implicate energy consumption because the amount of hot water use increased.

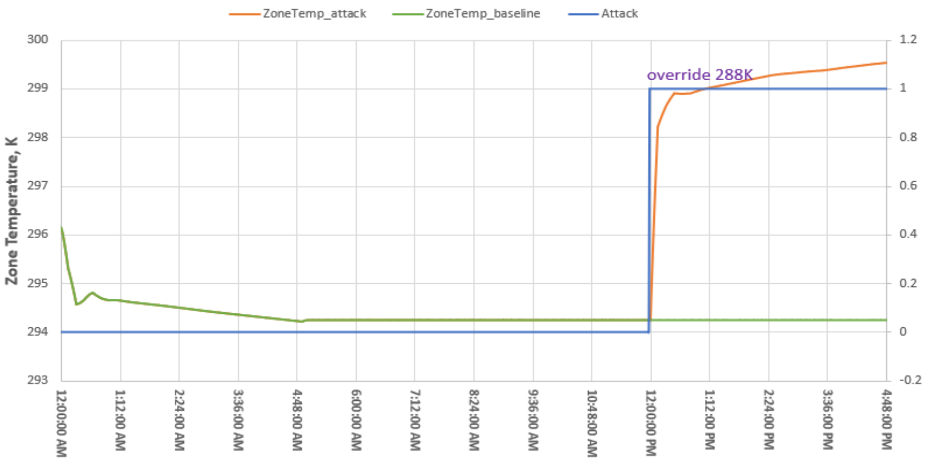


Figure 6 Thermostat set point overwritten by attacker with HIL.

CONCLUSION

This paper explained the BUILD-SOS test bed developed for building cybersecurity analysis. Buildings have both legacy devices and communication protocols that were not designed for secure cyber connections to operational technology networks, so they are susceptible to cyberattacks. To prevent potential cyberattacks on buildings, it is important to identify their vulnerabilities and take measures to improve them. In case of a cyberattack, it is crucial to detect and take corrective actions to reduce the impact on the building/business. Vulnerability analyses, attack detection, and mitigation systems that have the least impact on building occupants and the buildings are needed; thus, the BUILD-SOS test bed proposed in this paper can be used as this type of platform. This test bed replicates and simulates the building using Alfalfa with a defined building model to study the building impacts of cyberattacks with the least impacts on real buildings and occupants. In addition to the existing tools in the test bed, we will continue to expand the test bed to add additional communication protocols and devices to develop the capability to perform extensive studies in the future.

ACKNOWLEDGMENTS

This work was done as part of the BUILD-SOS project funded by the U.S. Department of Energy along with our partners at the University of Central Florida, the University of Massachusetts Lowell, and Siemens. Special thanks to Dane Christensen, Sugirdhalakshmi Ramaraj, Tobias Shapinsky, Kyle Benne and Charisa Powell (former) of NREL for their contributions.

This work was authored in part by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding was provided by Buildings Technology Office (BTO). The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

REFERENCES

Alfala. 2023. GitHub. NREL. https://github.com/NREL/alfalfa.
Alfalfa BACnet Bridge. 2023. GitHub. NREL. https://github.com/NREL/alfalfa-bacnet-bridge.

Alfalfa Helm. 2023. GitHub. NREL. https://github.com/NREL/alfalfa-helm.

ASHRAE. 2018. *ASHRAE Guideline 36*. Atlanta: ASHRAE.

Balamurugan, S., Granda, S., Haile, S., and Peterson, A. 2023. A dataset of cyber-induced mechanical faults on buildings with network and buildings data. *NREL Data Catalog. http://data.nrel.gov/submissions/210*.

Blum, D., Arroyo, J., Huang, S., Drgoňa, J., Jorissen, F., Taxt Walnum, H., Chen, Y., Benne, K., Vrabie, D., Wetter, M., and L. Helsen. 2021. Building optimization testing framework (BOPTEST) for simulation-based benchmarking of control strategies in buildings. *Journal of Building Performance Simulation* 14(5)586–610. https://doi.org/10.1080/19401493.2021.1986574.

BOPTEST. 2023. Test case name: Brief description. Test cases: Ready-made building emulators. https://ibpsa.github.io/project1-boptest/testcases/ibpsa/testcases_ibpsa_multizone_office_simple_air/.

EnergyPlus. 2023. https://energyplus.net/.

Lu, X. 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* & *Buildings* 252:11148.

OpenStudio. 2023. https://openstudio.net/.

U.S. Department of Energy (DOE) Office of Energy Efficiency and Renewable Energy (EERE). 2014. Spawn-of-EnergyPlus (Spawn). Buildings. https://www.energy.gov/eere/buildings/articles/spawn-energyplus-spawn.

Wetter, M., Benne, K., Gautier, A., Nouidui, T.S., Ramle, A., Roth, A., Tummescheit, H., Mentzer, S., and C. Winther. 2020. Lifting the garage door on Spawn, an open-source BEM controls engine. *2020 Building Performance Modeling Conference and SimBuild co-organized by ASHRAE and IBPSA-USA*. https://escholarship.org/uc/item/9c28b4qp.

Wetter, M., Zuo, W., Nouidui, T.S., and X. Pang. 2014. Modelica Buildings library. *Journal of Building Performance Simulation* 7(4):253–270. https://www.osti.gov/pages/biblio/1249559.