



# **A Cybersecurity Testbed for Smart Buildings**

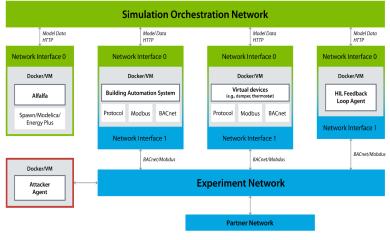
Sivasathya Balamurugan, Steve Granda, Selam Haile, Anya Peterson, Jing Wang, Jiazhen Ling National Renewable Energy Laboratory Acknowledgment: University of Central Florida, University of Massachusetts Lowell and Siemens

## OBJECTIVES

- Smart 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.
- 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.
- So, we have created a testbed for smart buildings that can help understand the impacts of cyber-attacks on buildings by generating both physical and cyber data for analysis and evaluate cyberattack detection tools in a secure environment.

### APPROACH

- This test bed includes a virtual building, virtual devices, emulated operational technology networks, and remote hardware-in-the-loop.
- Buildings research tools doesn't generally emulate networks but it's essential for cybersecurity research, thus a unique feature of the testbed.
- The malicious actor is another virtual device used to attack building devices communicating over the experiment network.
- The attacker device is configured to perform attacks on specific points by manipulating the communication through methods such as denial of service and register flooding



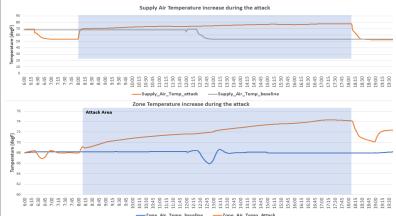
Architecture of cybersecurity testbed

### **EXPERIMENTAL SCENARIOS**

Building Model	Season	Cyber-Induced Fault	Impact
Medium office	Summer	Cooling coil stuck closed	Thermal discomfort
Medium office	Winter	Simultaneous heating and cooling	Energy waste, increased operational cost
Medium office	Winter	Outside air damper stuck open	Energy waste
Campus	Summer	Overridden thermostat set point	Occupant discomfort and energy waste

# RESULTS

- 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.
- During an attack, the operation of the cooling coil was disrupted by commanding it to be stuck closed.
- This increase would cause thermal discomfort or affect processes or equipment in spaces such as a data center.





	Time 851 1255 051730841	Source	Destination 102 158 88 2	Protocol RACost - ADDII	Length Info 62 Confirmed, PEO	writeBronerty[ 68] binary-output		
	557.5 MISTACK 0000000	102.001.00.2	192-103 (80.20)	BACnet-APDU	68 Stmole-ACK	writeProperty 60	1 Brecont Value	
	853 1256.060439778	192.168.88.20	192.168.88.2	BACnet - APDU	63 Confirmed-RED	writeProperty[ 61] binary-output	1 present-value	
		102.100.00.2	102-100-00-20	DROTIC CHAP DO	OU OLIPIC NON	An actor reporting to a		
3	855 1256.168138347	192.168.88.20	192.168.80.2	BACnet-APDU	63 Confirmed-REQ	writeProperty[ 62] binary-output	,1 present-value	
	857 1256.177267239 858 1256.180326696	192.168.88.3 192.168.88.2	192.158.80.2 192.158.80.3	BACnet-APDU BACnet-APDU	68 Confirmed-REQ 62 Complex-ACK	readProperty[ 32] binary-output, readProperty[ 32] binary-output,		
Ether Inter Jser BACne Typ Fun BVL	243: 60 bytes on wirnet II, Src: Vmware, armet Protocol Version Datagram Protocol, Sr: t Virtual Link Contro. e: BACnet/IP (Annex J Iction: Original-Unica .C-Length: 4 of 17 byt ing Automation and Co	S:f3:a0 (00:8c:29:a 4, Src: 192.168.80. 2 Port: 47808, Dst 1 ( 0x81) st-NPDU (0x8a) 25 BACnet packet 1e	6:f3:a0), Dst: Vmwa 3, Dst: 192.168.80 Port: 47869	re_f5:7f:95 (00:0c:2 2	erfsr7fres) inet Network C	apture		
86 18 28	00 0c 29 f5 7f 95 00 00 20 d4 a3 48 00 40 50 02 ba c0 ba c1 00 02 44 5c 0c 0c 02 00	0c 29 a6 f3 a0 0 11 44 c6 c0 a8 5 19 ca 57 81 0a 0	9 03 c0 a8 🧧 🤴 9 11 01 04 P ····	0. D. P W				
7 n	ireshark_ens37_20210715173826	Nm5cmT.pcapng				Packets: 3858 - 1	lisplayed: 3336 (86.5%)	Profile: I
	-15 17:59:21,078 - I	IFO   Starting	BAC0 version 21.02			Sensor': 24.10000038146 active		
					mpSensor': None, 'Out	sideAirFlowSensor': Non active		
	-15 17:59:21,078 - I	IFO   Use BACO.	log_level to adjus			active		
	sity of the app.					Sensor': 24.10000038146 active		
	-15 17:59:21,078 - I		log_level('silence	9727, 'OutsideAirTe	mpSensor': None, 'Out	sideAirFlowSensor': Non active		
	ACO.log_level('error			e}		active		
	-15 17:59:21,078 - II		TaskManager			mpSensor': 24.100000381 active		
	-15 17:59:21,079 - I		: 192.168.80.20		TempSensor': None, 'O	utsideAirFlowSensor': N active		
	-15 17:59:21,081 - I			one}		active		
	-15 17:59:21,083 - I					mpSensor': 24.100000381 active		
	-15 17:59:21,083 - I	IFO   Registere	d as Simple BACnet		TempSensor': None, 'Q	utsideAirFlowSensor': N accive		
P App				one}		active		
21-07	-15 17:59:21,096 - I	IFO   Update Lo	cal COV Task start			mpSensor': 24.100000381 active		
					TempSensor': None, 'Q	utsideAirFlowSensor': Nactive		
	-15 17:59:21,097 - I	IFO   Changing	device state to De			active		
21-07	connected'>					<pre>mpSensor': 24.100000381 inactive</pre>		
			invice state to DD	469727, 'OutsideAir	TempSensor': None, 'O	utsideAirFlowSensor': N inactive		
ceDis	-15 17:59:21,118 - II	IFO   Changing						
ceDis 21-07		IFO   Changing	Jevice state to N	one}		inactive		
ceDis 21-07 evice	-15 17:59:21,118 - II				nactive'. 'MixedAirTe	mpSensor': 24.100000381 inactive		
ceDis 21-07 evice 21-07	'-15 17:59:21,118 - I Connected'>		1:[BAC0] found	{'AirDamperCmd': 'i				
ceDis 21-07 evice 21-07 ildin	'-15 17:59:21,118 - I Connected'> '-15 17:59:21,137 - I ng points list	IFO   Device 10		{'AirDamperCmd': 'i 469727, 'OutsideAir		mpSensor': 24.100000381 inactive utsideAirFlowSensor': N inactive		
ceDis 21-07 evice 21-07 ildin	'-15 17:59:21,118 - I Connected'> '-15 17:59:21,137 - I	IFO   Device 10		{'AirDamperCmd': 'i		mpSensor': 24.100000381 inactive		
ceDis 21-07 evice 21-07 ildin	-15 17:59:21,118 - I connected'> '-15 17:59:21,137 - I g points list '-15 17:59:21,165 - I	IFO   Device 10	1:[BAC0] found	{'AirDamperCmd': 'i 469727, 'OutsideAir one}		mpSensor': 24.100000381 inactive utsideAirFlowSensor': N inactive inactive	Virtual Damper De	utee

#### CONCLUSION

• The test bed replicates and simulates the building using Alfalfa with a defined building model to study the impacts of cyberattacks with the least impacts on real buildings and occupants

Wireshark network capture of cyberattack under progress

- To prevent potential cyberattacks on buildings, it is important to identify their vulnerabilities and take measures to improve them.
- Vulnerability analyses, attack detection, and mitigation systems that have the least impact on occupants and the buildings are needed, which can be enabled or evaluated using the testbed