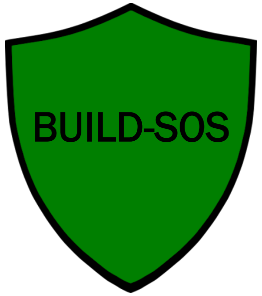
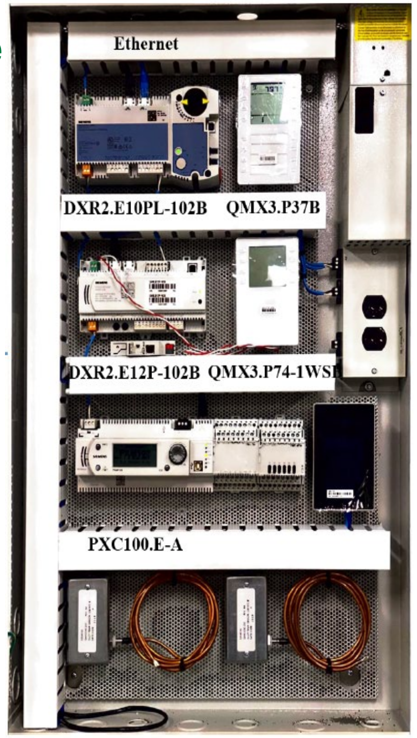
*B*uilding *I*ntelligence with *L*ayered *D*efense using *S*ecurity-Constrained *O*ptimization and *S*ecurity Risk Detection (*BUILD-SOS*)

Layered Defense to the Rescue



Probabilistic Sensing & Controls



University of Central Florida
Qun Zhou Sun, Director, Smart Infrastructure Data Analytics Laboratory
Email: QZ.Sun@ucf.edu
Tel: 407-823-3284

Project Summary

Timeline:

Start date: 04/01/2020

Planned end date: 07/30/2023

Key Milestones

1. Fault and attack detection algorithm. 05/30/2021
2. Establish emulated environment. 7/30/2021
3. Security-constrained stochastic optimization for controls. 7/30/2022
4. HIL testbed and real building demonstration. 7/30/2023

Budget:

Total Project $ to Date:

- DOE: $784,071
- Cost Share: $278,302

Total Project $:

- DOE: $3,000,000
- Cost Share: $750,000

Key Partners:

UCF	Siemens
NREL	U Mass Lowell

Project Outcome:

BUILD-SOS provides a holistic solution to secure building operations and can be broadly applied to commercial buildings and campuses that are prone to cyber threats.

Related to MYPP:

- **Improve cost & performance of fault-tolerant integrated control systems**
- **Predictive & prioritizing maintenance algorithms & adaptive controls that optimize building operations**

Team

- Develop data analytics and robust optimization algorithms; Provide campus building for demonstration; Overall project management.
- Energy modeling; system and communication integration; testbed development and monitoring.
- Provide software and hardware platform for research; assist to collect UCF campus BAS data; help with market transformation.
- Security vulnerability assessment; attack modeling and implementation; cybersecurity testbed development.

Challenge

- Cyber threats are real, and buildings can be targeted.

- Smart buildings are large IoT networks, which may have vulnerabilities through which malicious actors can access critical systems.
- Opportunities exist to improve security through design of next-generation building automation systems. Legacy systems may be harder to protect.

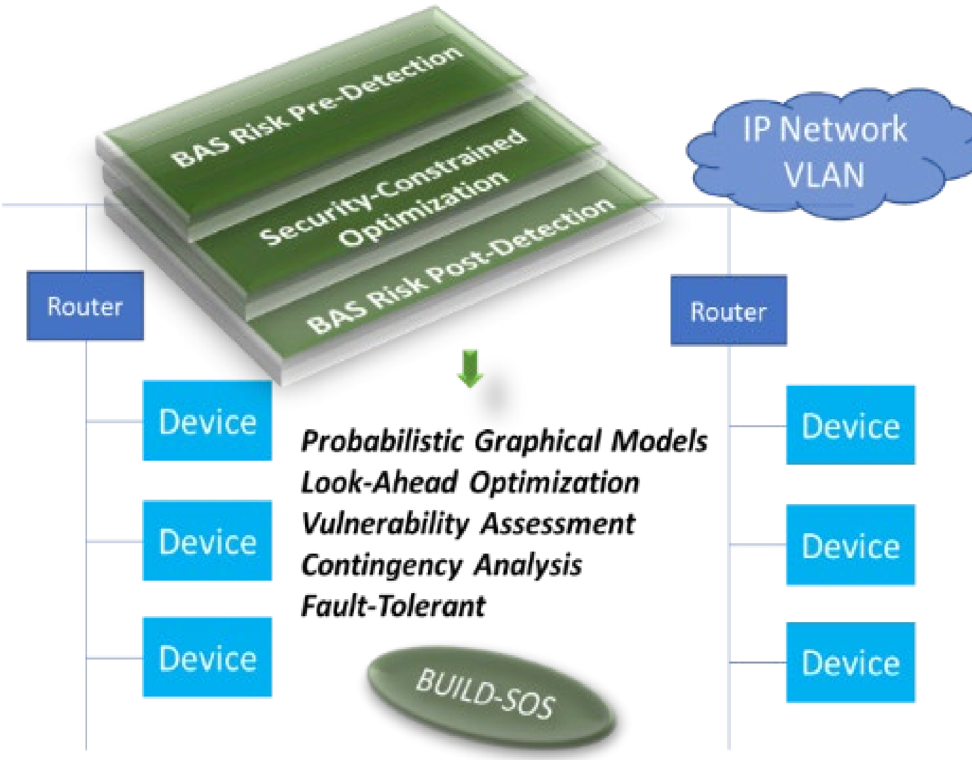
Existing Approaches

- Most building cyber security solutions are from IT perspectives and lack OT insights.
- Most existing Fault Detection and Diagnosis (FDD) tools consider single mechanical faults, and do not take into account cyber-induced faults, which could be more sophisticated, coordinated, and simultaneous.
- The state-of-the-art building controls are mostly aimed at improving efficiency while robustness against faults and cyber threats are generally not a priority.
- Most existing methods are deterministic while practically smart buildings are uncertain, with uncertainties come from building modeling, data sources, and even the unobservability of adversarial events.

Our Approach – Overview of Layered Defense

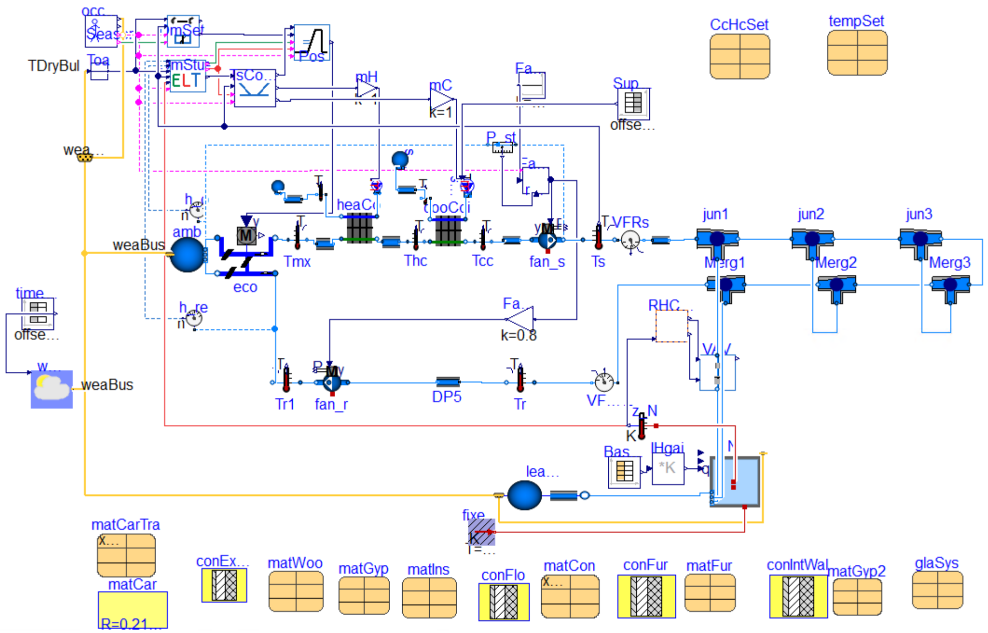
Distinctive Characteristics

- The BUILD-SOS platform is based on advanced data analytics and stochastic optimization.
- Hackers need to deeply understand both probabilistic detection algorithms and stochastic controls in order to execute any effective attacks.
- The layered approach provides a holistic cyber security solution bridging IT and OT.

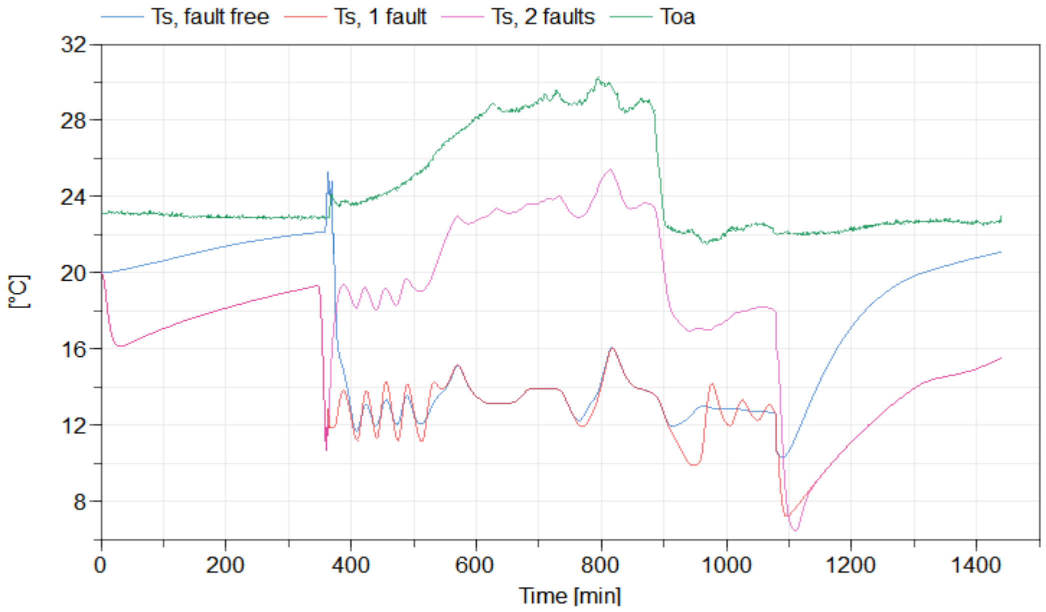


Approach – Cyber-Induced Fault Data Generation

- **Data from real-world BAS attacks are not available**
- **Traditional FDD algorithms are not intended to provide attack detection.**



- Building model in Modelica and calibrated using ASHRAE 1312 project data

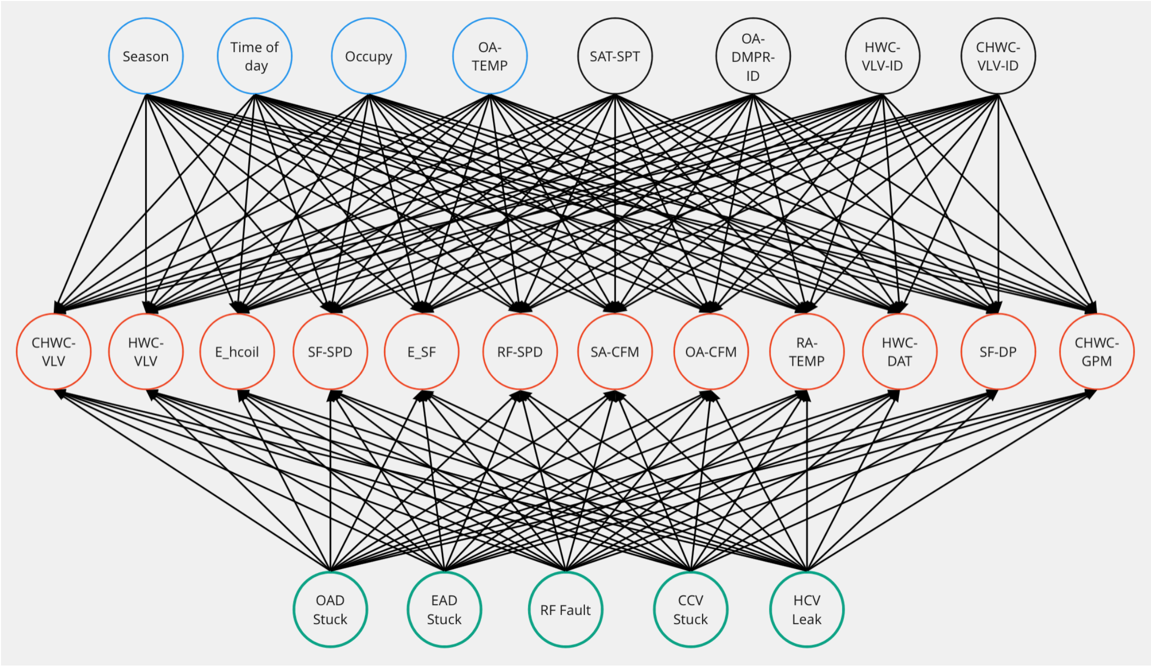


- Single fault and simultaneous fault data generation
- *Coordinated attacks will have more severe impact!!*

Reference :
Wen, J., and S. Li. "RP-1312–Tools for evaluating fault detection and diagnostic methods for air-handling units." *ASHRAE, Tech. Rep, Tech. Rep* (2012).

Approach – Fault and Attack Detection Algorithms

- Causal-based Bayesian Networks



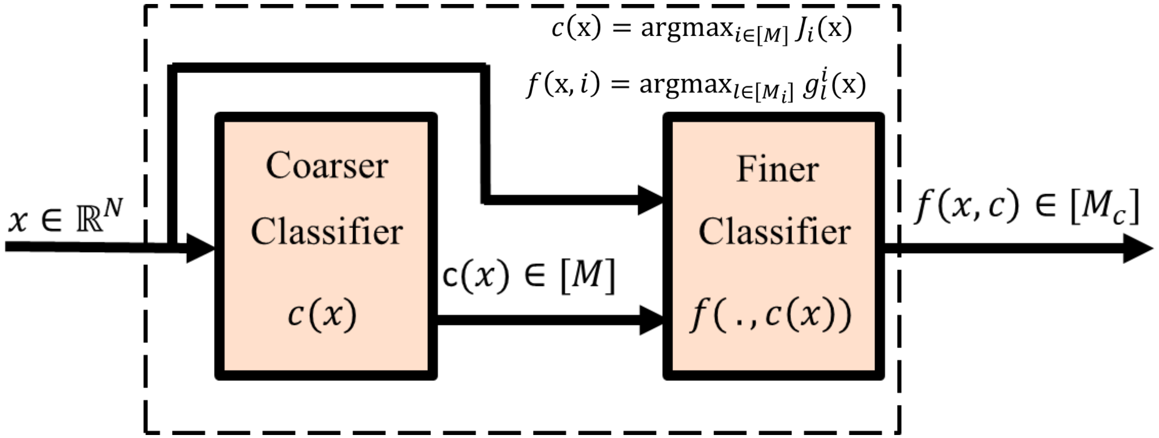
- A dense fully-connected network
- Network parameter learning using maximum likelihood
- Inference using variable elimination
- Root nodes are sources of uncertainties: environment inputs, human inputs, and component states.

- Domain Adaptation using Kernel Mean Matching

$$\underset{\beta}{\text{minimize}} \; \| \mathbb{E}_{\mathbf{x}\sim P_t}[\Phi(\mathbf{x})] - \mathbb{E}_{\mathbf{x}\sim P_s}[\beta(x)\Phi(\mathbf{x})] \|_F^2$$

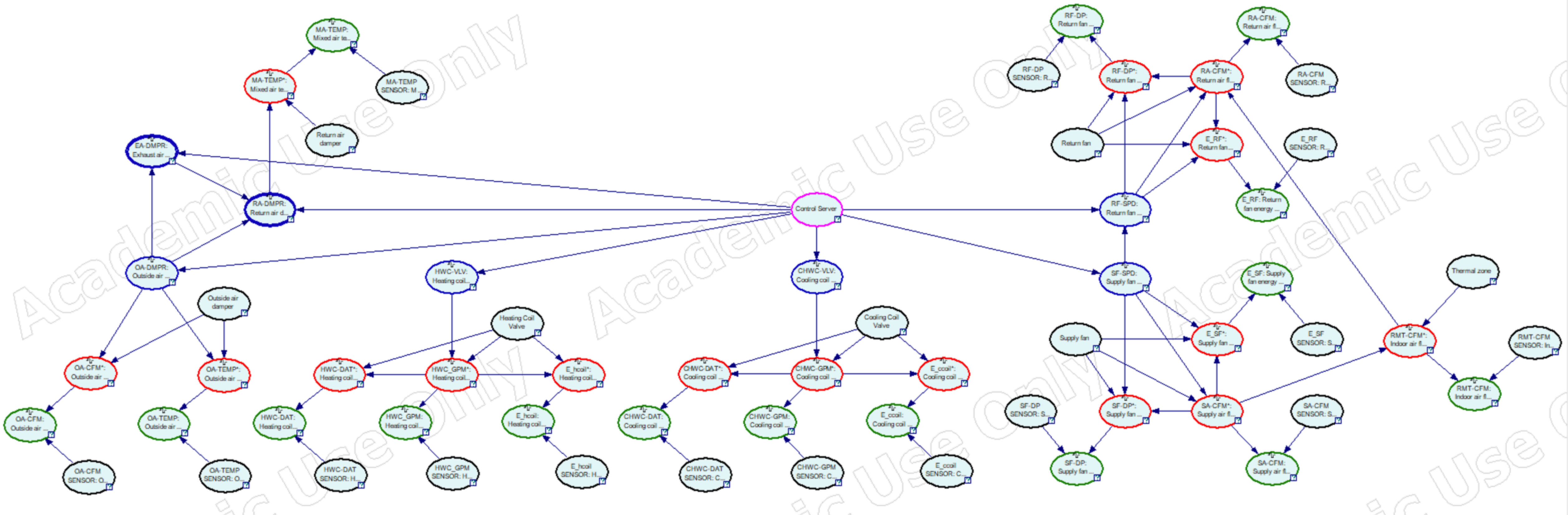
Subject to $\beta(x) \geq 0$ and $\mathbb{E}_{P_s}[\beta(\mathbf{x})] = 1$

- Hierarchical Classifiers



Approach – Fault and Attack Detection Algorithms

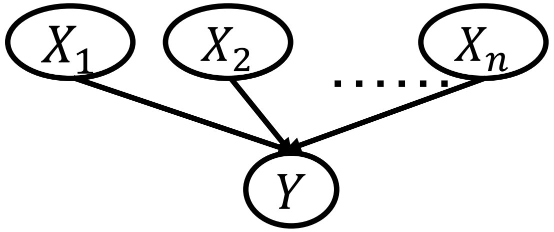
- Physics-Embedded Bayesian Networks to Detect Cyber-Induced Faults



- Sparse network
- Physics-Embedded
- Conditional Linear Gaussian Model
- Control server is included as an attack object

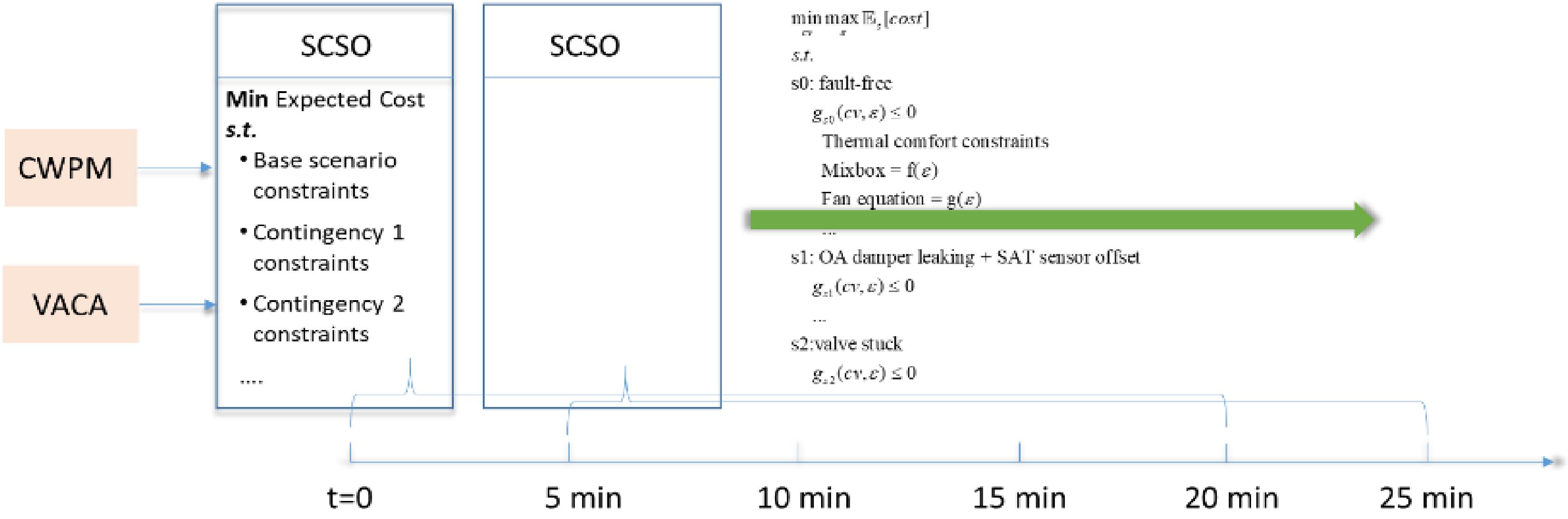
Linear Gaussian Model

$$P(Y|\boldsymbol{x}) = \mathcal{N}(Y; \beta_0 + \boldsymbol{\beta}^T \boldsymbol{x}, \sigma_W^2)$$



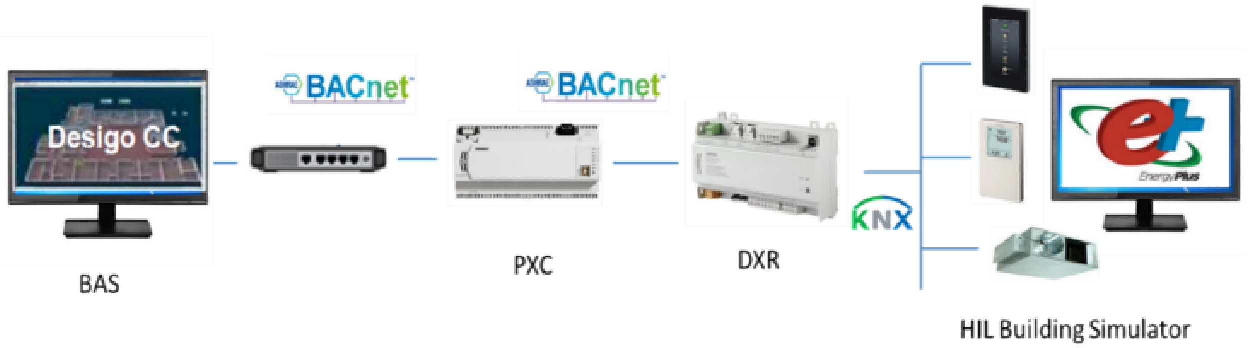
Approach – Fault-Tolerant Stochastic Controls

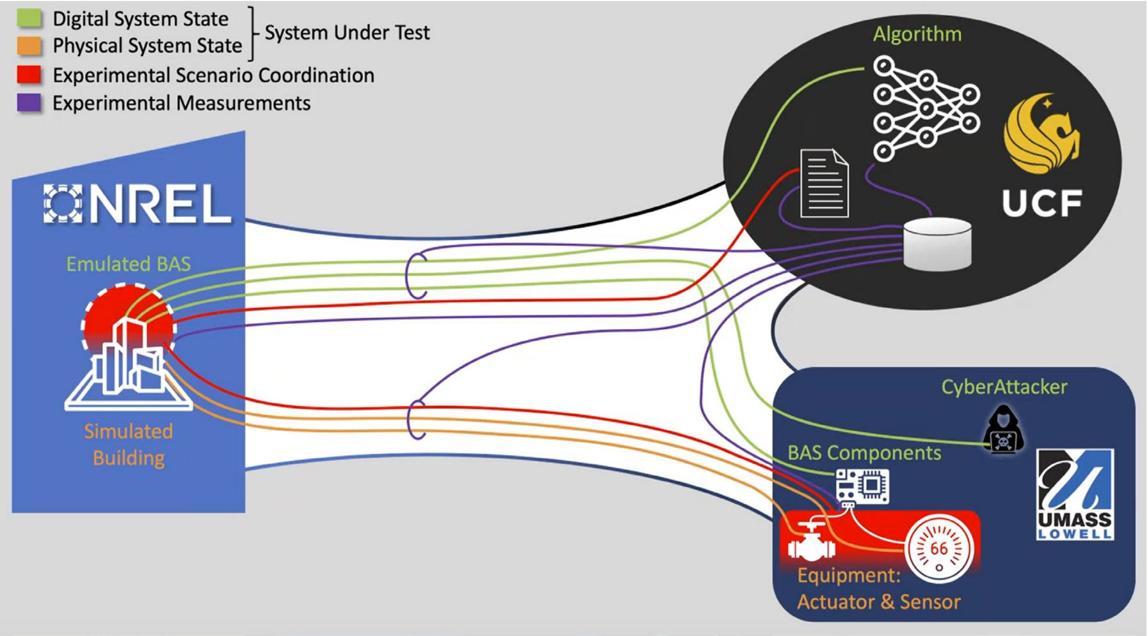
- Probabilistic modeling of each building component given unknowns
- Vulnerability Assessment: Investigate different attack scenarios and assess the vulnerability of each component
- Contingency Analysis: Rank the most vulnerable scenarios and integrate into fault-tolerant controls
- Fault-Tolerant Controls: Security-Constrained Stochastic Optimization (SCSO)

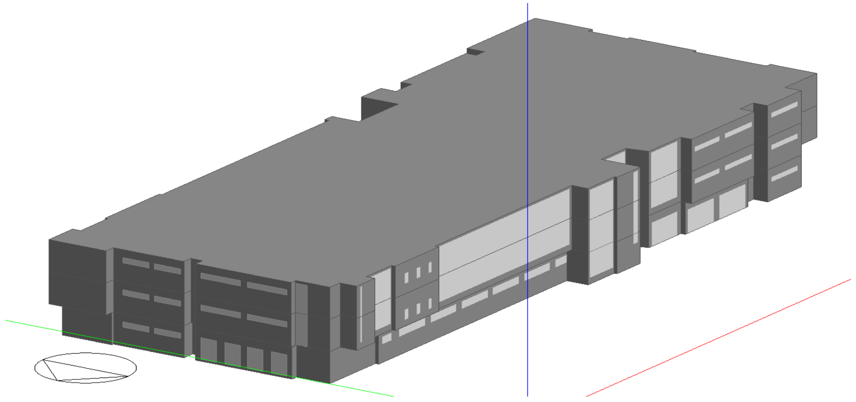


Approach – Testbed and Building Demonstration

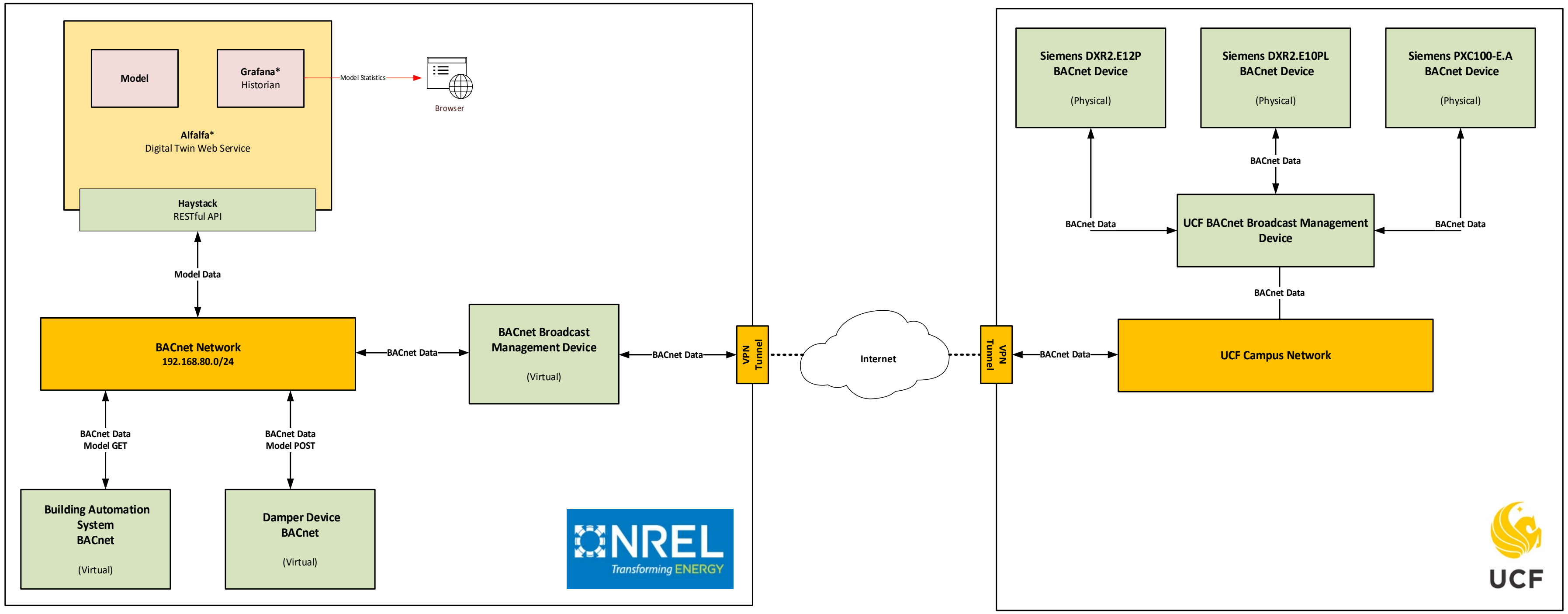
- **Building Cyber-Security Testbed (BCST)**

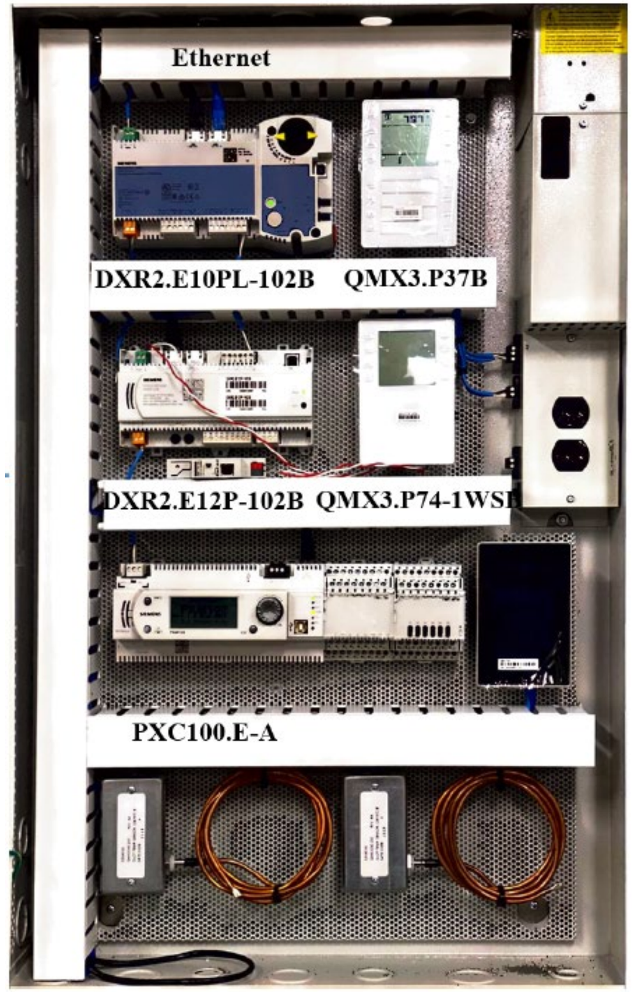






Approach – Building Cyber Security Testbed





Emulated environment and Hardware in the Loop

Impact

- **The resulted BUILD-SOS is expected to provide a holistic solution to secure building operations and can be broadly applied to commercial buildings and campuses that are prone to cyber threats.**
- **Demonstrates feasibility of fundamental methods and algorithms for a layered defense system serving smart buildings with advanced sensing technology. Demonstrates >20% accuracy improvement for fault detection including cyber-induced faults and coordinated attacks.**
- **Emulation and field experiments demonstrate the real threats from cyber attacks in buildings and the robustness of proposed layered defense system**
- **Contributes directly to BTO's MYPP/Logic Model:**
  – Improve cost & performance of fault-tolerant integrated control systems
  – Data collection methods & analytics for enhanced building control systems
  – Predictive & prioritizing maintenance algorithms & adaptive controls that optimize building operations

Progress – Detection Results from Bayesian Networks

- Five faults are examined, including one cyber attack on fan speed command.
- Detection probabilities are given for each object.
- Accuracy improvement over the state of the art FDD > 20%
- Passed Go/No-Go on fault and attack detection in the first budget period.

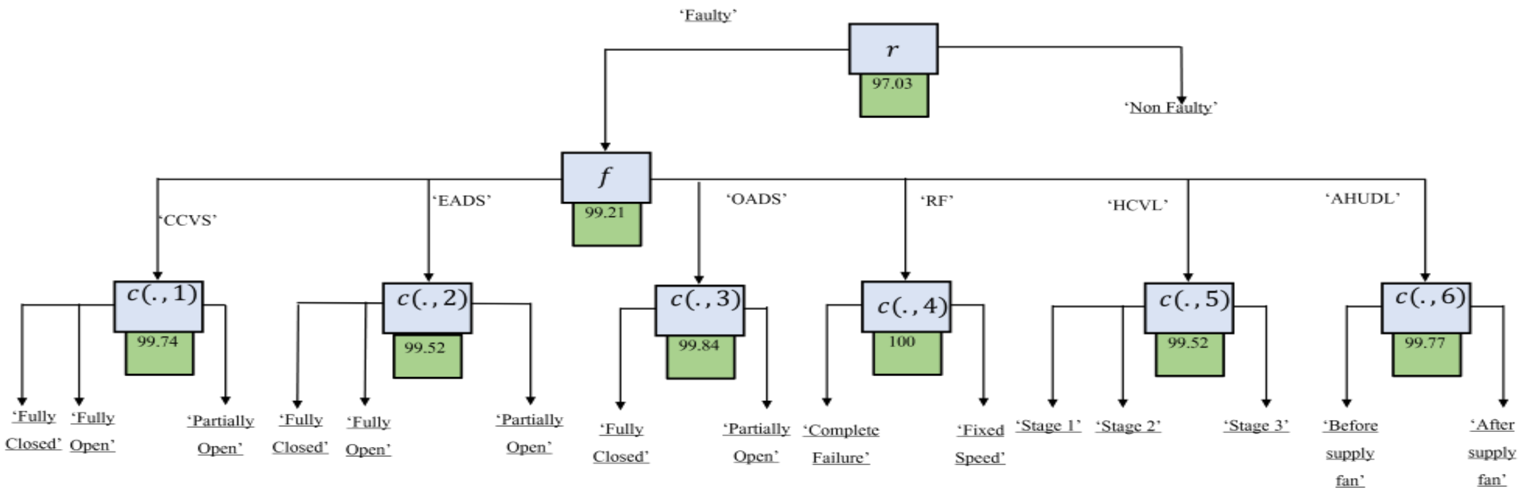
Fault description	Date	Rule-based Benchmark		Improved Rule-based System		Bayesian Network	
		Detection	Diagnosis	Detection	Diagnosis	Detection	Diagnosis
EA Damper Stuck (Fully Open)	8/20/2007	8%	0%	12.32%	6.45%	55%	55%
EA Damper Stuck (Fully Close)	8/21/2007	0%	0%	9.87%	4.03%	43%	43%
Return Fan at fixed speed (30%spd)	8/22/2007	100%	35%	100%	99.65%	100%	100%
Return Fan complete failure	8/23/2007	100%	99%	100%	99.96%	100%	100%
OA Damper Stuck (Fully Closed)	8/26/2007	99%	88%	99.17%	88.64%	82%	81%
Cooling Coil Valve Stuck (Fully Closed)	8/27/2007	100%	67%	100%	100%	98%	98%
Heating Coil Valve Leaking (Stage 1 - 0.4GPM)	8/28/2007	0%	0%	3.64%	2.17%	80%	76%
Heating Coil Valve Leaking (Stage 2 – 1.0GPM)	8/29/2007	51%	28%	51.03%	30.97%	87%	87%
Heating Coil Valve Leaking (Stage 3 – 2.0GPM)	8/30/2007	96%	28%	96.42%	32.5%	88%	88%
Cooling Coil Valve Stuck (Fully Open)	8/31/2007			87.12%	79.25%	98%	89%
Cooling Coil Valve Stuck (Partially Open - 15%)	9/1/2007	99%	61%	90.35%	78.56%	96%	96%
Cooling Coil Valve Stuck (Partially Open - 65%)	9/2/2007			71.1%	45.12%	100%	78%
Cooling Coil Valve Reverse Action	9/3/2007			88%	65.1%	99%	77%
OA Damper Leak (45% Open)	9/5/2007	0%	0%	8.92%	2.46%	83%	63%
OA Damper Leak (55% Open)	9/6/2007	11%	0%	9.86%	6.15%	89%	89%
AHU Duct Leaking (after SF)	9/7/2007	9%	0%	5.45%	3.78%		
AHU Duct Leaking (before SF)	9/8/2007	90%	84%	90.34%	80.42%		

Causal-based Bayesian networks

Object label	Return fan speed fixed 20%	Return fan speed fixed 30%	Return fan speed fixed 80%	Cyber attack RF 80% speed	Return fan complete failure
CTRL_SERVER	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Attack RF 80SPD: 1.0	Fault free: 1.0
HCV	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0
HWC_GPM_SENSOR	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0
HWC_DAT_SENSOR	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0
E_HCOIL_SENSOR	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0
CCV	Fault free: 1.0	Fault free: 0.930435, CCV fully open: 0.069565	Fault free: 0.930435, CCV fully open: 0.069565	Fault free: 1.0	Fault free: 0.981159, CCV fully open: 0.018841
CHWC_GPM_SENSOR	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0
CHWC_DAT_SENSOR	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0
E_CCOIL_SENSOR	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0
SF	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 0.998551
SA_CFM_SENSOR	Fault free: 0.995652	Fault free: 1.0	Fault free: 0.989855	Fault free: 1.0	Fault free: 0.985507
SF_DP_SENSOR	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 0.97971
E_SF_SENSOR	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0
RF	RF 20SPD: 0.931884, RF comp fail: 0.049275	RF 30SPD: 1.0	RF 80SPD: 1.0	RF 80SPD: 1.0	RF comp fail: 0.994203, RF 20SPD: 0.005797
RA_CFM_SENSOR	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 0.982609	Fault free: 1.0
RF_DP_SENSOR	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0
E_RF_SENSOR	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0
ZONE	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0	Fault free: 1.0
RMT_CFM_SENSOR	Fault free: 0.995652	Fault free: 1.0	Fault free: 0.989855	Fault free: 1.0	Fault free: 0.982609

Physics-Embedded Bayesian networks

Progress – Robustness of Hierarchical Classifiers

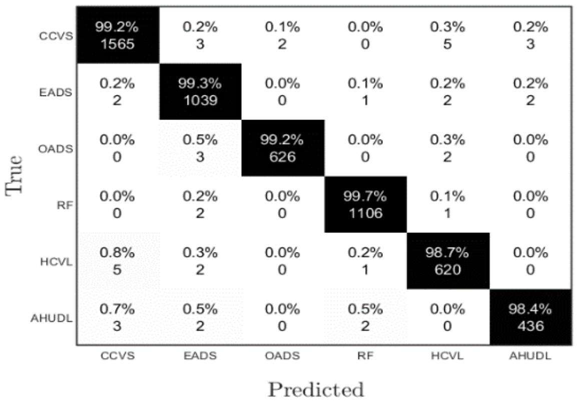


Example:
Declare faulty as non-faulty

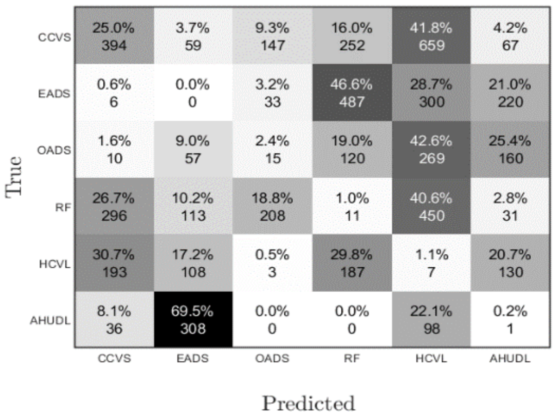
Attack FDD algorithms??

– We find that **Hierarchical FDD is more robust** than a single layer classifier

Before the Attack



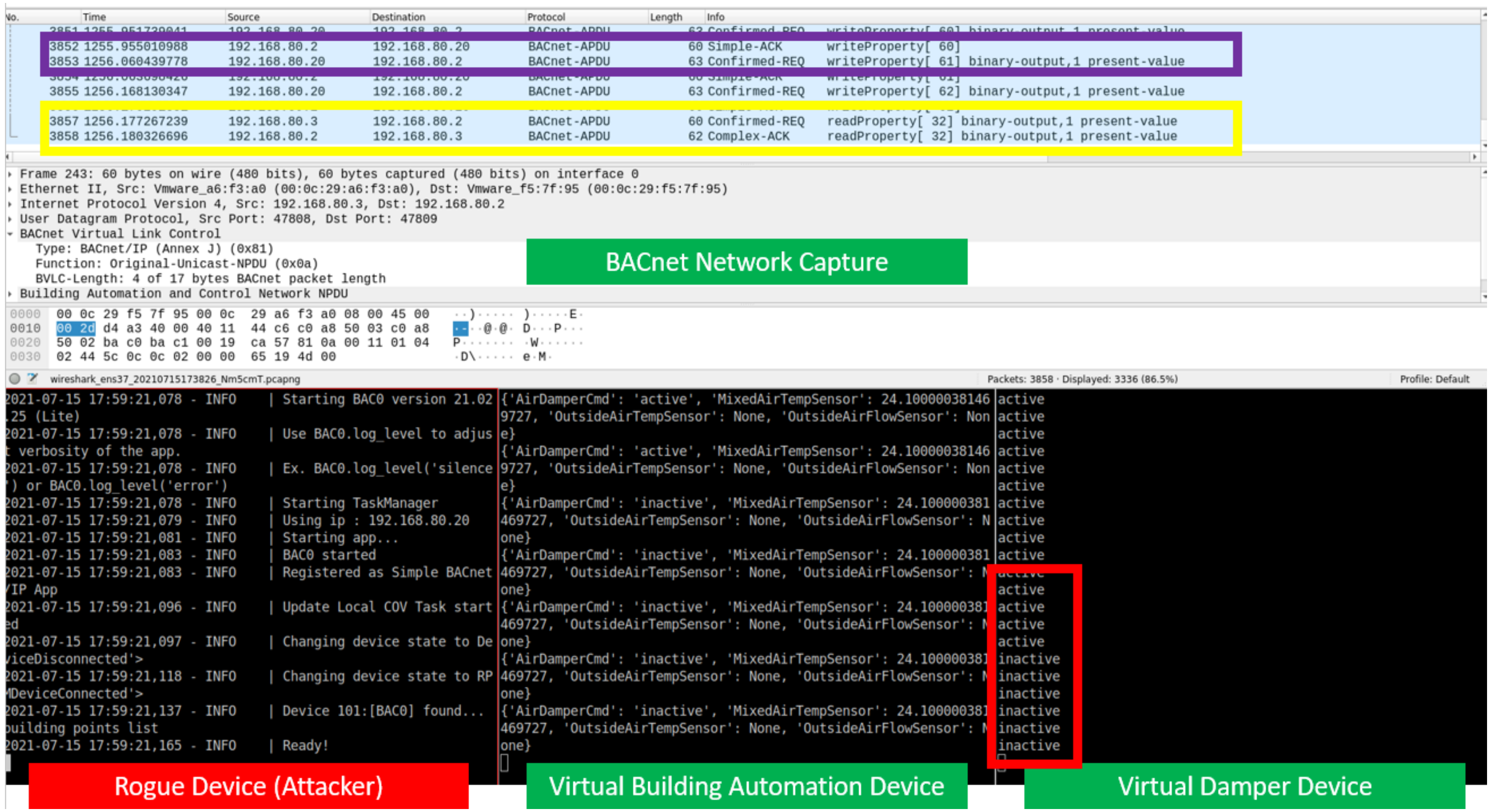
After the Attack



Attack	Success Ratio	Perceptibility
HFDD	88.40%	44.05%
Single-layer	94.92%	21.24%

*Attacking HFDD is **harder** than a traditional single-layer FDD*

Progress – Emulation and BCST



Denial of Service Attack

Man-in-the-Middle Attack

Link for demonstration video: https://app.box.com/s/8y7hbdpx9kxvssozberwaqlcvfqkz34v

Stakeholder Engagement

- **Forming the Industry Advisory Board**
  - Confirmed participation of facilities departments from UCF, UMass Lowell, and Siemens.
  - IAB will meet quarterly through the end of the project.
  - Current IAB members are broadening the participation and reaching out to their vendors including Johnson Controls and Automated Logic.
- **Publications**
  - Disseminated our research results in both energy conferences and security conferences
  - 6 journal papers submitted, 3 accepted
  - 7 conference papers published.

Remaining Project Work

- **Second Year:**
  - Conduct vulnerability assessment and develop attack scenarios
  - Integrate the risk assessment into stochastic robust fault-tolerant controls

- **Third year:**
  - Compare the controlled results with actual building responses and correct the attack detection results accordingly.
  - Fully integrate HIL testing across sites and demonstrate in UCF R1 building

Thank You

University of Central Florida
Qun Zhou Sun
Director of Smart Infrastructure Data Analytics Lab
QZ.Sun@ucf.edu
407-823-3284

REFERENCE SLIDES

Project Budget

Project Budget: BP1 = $1,279,302, BP2 = $1,221,781, BP3 = $1,248,911
Variances: None.
Cost to Date: $1,062,373
Additional Funding: None.

Budget History					
04/01/2020– FY 2020 (past)		FY 2021 (current)		FY 2022 – 07/30/2023 (planned)	
DOE	Cost-share	DOE	Cost-share	DOE	Cost-share
$784,071	$278,302	$1,157,021	$281,340	$1,058,908	$190,002

Project Plan and Schedule

Project Schedule	
Project Start: 04/30/2020	Completed Work
Projected End: 07/30/2023	Active Task (in progress work)
	◆ Milestone/Deliverable (Originally Planned) use for
	◆ Milestone/Deliverable (Actual) use when met on time

Task	FY2021 Q1 (Oct-Dec)	FY2021 Q2 (Jan-Mar)	FY2021 Q3 (Apr-Jun)	FY2021 Q4 (Jul-Sep)	FY2022 Q1 (Oct-Dec)	FY2022 Q2 (Jan-Mar)	FY2022 Q3 (Apr-Jun)	FY2022 Q4 (Jul-Sep)	FY2023 Q1 (Oct-Dec)	FY2023 Q2 (Jan-Mar)	FY2023 Q3 (Apr-Jun)
Past Work											
Milestone 1: Cyber-induced fault data generation	◆										
Milestone 2: Bayesian networks and hierarchial fault and attack detection			◆								
Milestone 3: Emulation Environment Implemented			◆								
Current/Future Work											
Milestone 4: Building vulnerabilities identified					◆						
Milestone 5: Attack scenarios developed given realistic attack costs						◆					
Milestone 6: Fault-tolerant security-constrained stochastic optimization									◆		
Milestone 7: Launch cyber-physical attacks in HIL BCST									◆		
Milestone 8: UCF campus building demonstration										◆	
Milestone 9: Results Dissemination							◆				◆