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

Texas A&M University
Zheng O'Neill, PhD, PE
Tel: 979-458-4931; Email: ZONeill@tamu.edu

Project Summary

Timeline:

Start date: 05/01/2020

Planned end date: 04/30/2023

Key Milestones

1. Network analyzer can detect > 75% of attacks that violate the protocol state transition rules; 04/30/2021
2. The anomaly, including cyber-attacks, detection accuracy of > 85%, with a false alarm rate of <15%; 04/30/2022
3. CYDRES is demonstrated in a HIL and a real building with cyber-attack detection accuracy > 85%, false alarm rate < 15%; control mitigation response within 5 minutes; 04/30/2023

Budget:

Total Project $ to Date:

- DOE: : $788,971
- Cost Share: $224,739

Total Project $:

- DOE: $2,848,785
- Cost Share: $712,809

Key Partners:

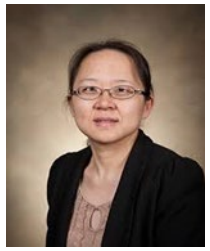
Raytheon Technologies Research Center	Carrier/ALC
Drexel University	Johnson Controls
Arizona State University	Cimetrics
Northwestern University	Slipstream
Pacific Northwest National Laboratory	ASHRAE BACnet committee

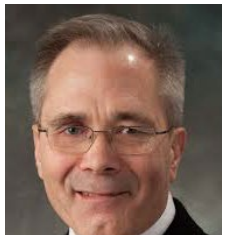
Project Outcome:

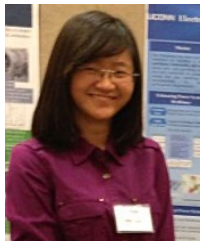
1) A prototype of the called **CY**ber **D**efense and **RE**silient **S**ystem (CYDERS) will be developed and tested in an HIL environment and a real building.
2) A demonstration of **a cyber-attack-immune GEB** through multi-layer prevention, detection, and adaptation that can achieve at least 15% HVAC energy savings while maintaining occupant thermal comfort.
3) A comprehensive commercialization plan for technology transfer through working closely with industry partners.

CYDRES Team

- **Project Team**
  - Texas A&M University: Drs. Z. O'Neill, Y. Fu, Z. Yang; Graduate Students
  - Raytheon Technologies Research Center: Drs. T. Wagner, L. Ren, F. Koufogiannis
  - Drexel University: Dr. J. Wen; Graduate Student
  - Arizona State University: Drs. T. Wu and S. Candan; Graduate Students
  - PNNL: Dr. V. Adetola
  - Northwestern University: Dr. Q. Zhu; Graduate Students


O'Neill


Wagner


Ren

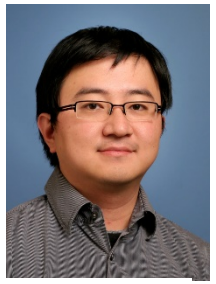

Koufogiannis


Wen

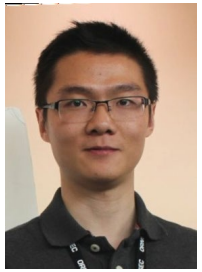

Wu


Candan


Adetola


Zhu


Fu


Yang

Industry Advisory Group

- ASHRAE BACnet committee
- Johnson Controls Inc (JCI)
- Carrier/ALC
- Cimetrics
- Slipstream


Bushby


Butler


Lomonaco

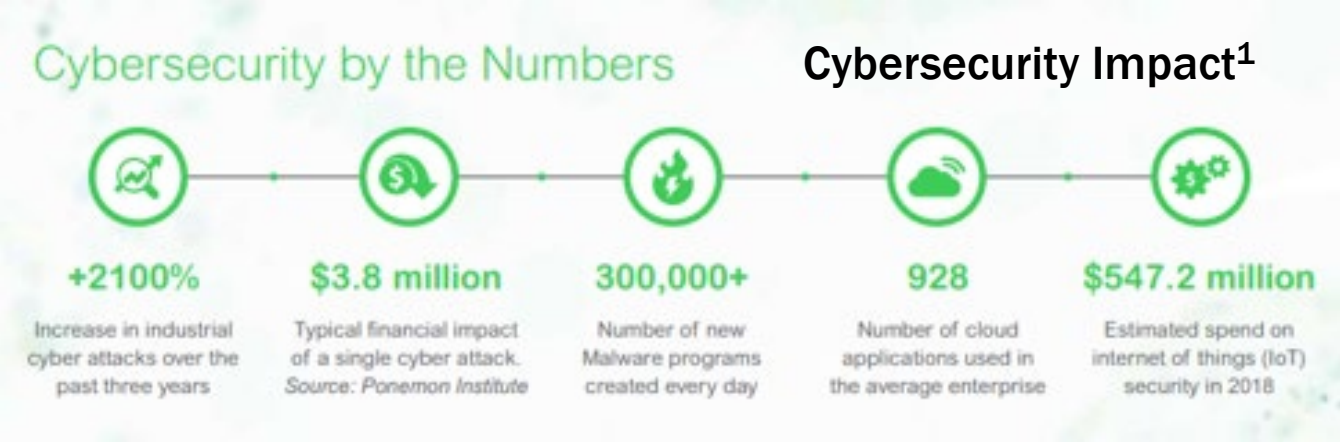

Parikh


Zhou


Benes

CYDRES Challenge

- Many building systems, especially the emerging GEBs are vulnerable to cyber-attacks.
- Cyber-threats that may have adverse or even severe consequences, e.g., occupant discomfort, energy wastage, equipment downtime, and disruption of grid operation.
- Differentiating cyber-attacks from equipment or operational faults allows ensures appropriate automated mitigation and provide actionable recommendations to the facility manager.
- Existing physical behavior-based anomaly detection methods fail to provide such distinction.



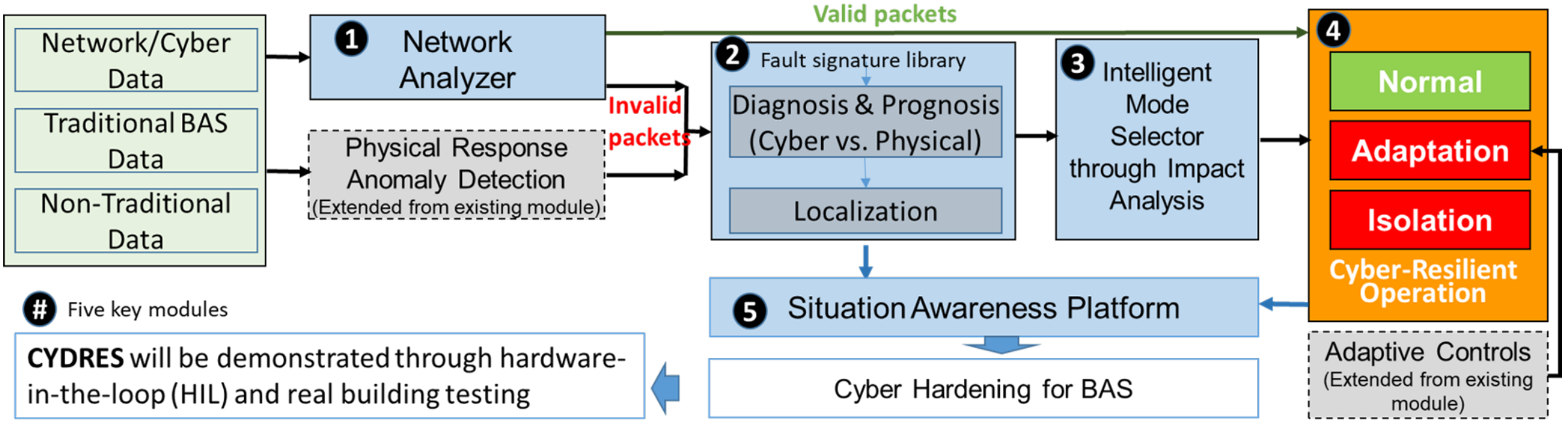
Overall median and mean perceptions of significance of building automation and control system vulnerabilities[2]

BACS Vulnerabilities	Median	Mean	SD
Cyberattack on the Management level device	7	5.82	1.73
Tampering with the Automation network	6	5.40	1.85
Insertion of an unauthorized Management level device	6	5.33	1.88
Overriding a Controller outputs or inputs	6	5.29	1.80
Manipulation of Security sensor (Detector)	6	5.28	1.82
Manual override of Controllers output switches	6	5.19	1.84
Manipulation of a Sensor or Actuator	5	5.09	1.71
Monitoring the ICT network	6	5.06	1.85
Loss of mains power	6	5.06	2.03
Extraction of a Controller's latent memory	6	5.05	1.84
Damaging a Controller	6	5.02	1.83
Automation network traffic monitoring	6	5.01	1.77
Damage a Management level device	6	4.99	1.79
Automation network traffic data injection	5.5	4.98	1.89
Physical disconnection of a Sensor or Actuator	5	4.81	1.88
Damaging a Sensor or Actuator	5	4.81	1.76

1. https://blog.se.com/building-management/2019/05/30/understanding-cybersecurity-in-smart-buildings/
2. D. Brooks, et al. Building Automation & Control Systems: An Investigation into Vulnerabilities, Current Practice & Security Management Best Practice, technical report.

CYDRES Approach – Overview

Key elements of the proposed cyber defense and resilient system (CYDRES)*

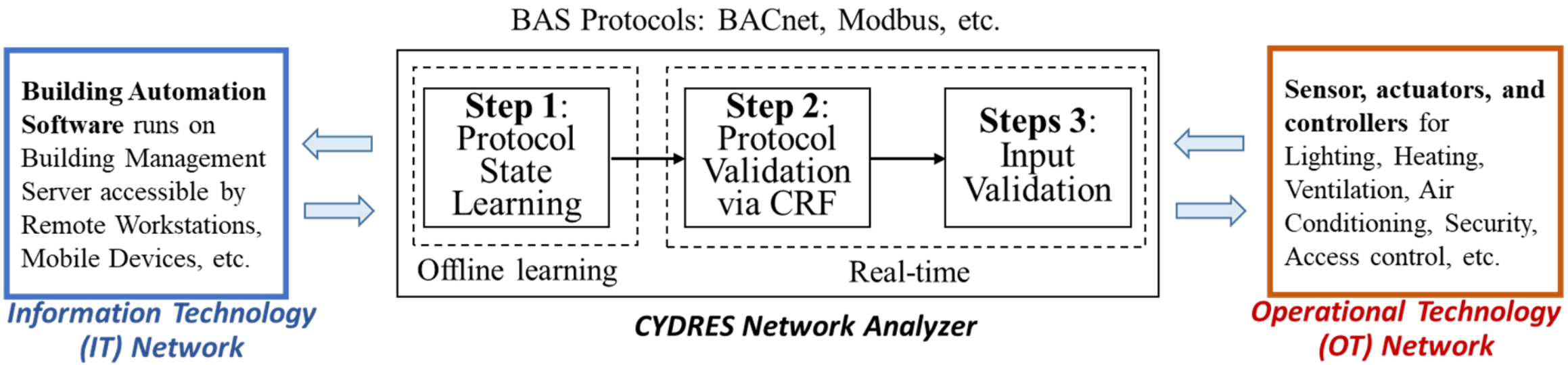


CYDRES **aims to provide a** ***real-time advanced building resilient platform through multi-layer prevention and adaptation mechanisms*** to monitor, detect, and respond to cyber-attacks and physical system faults.

**Budget Period 1 effort focuses on Modules 1, 2 and 3*

CYDRES Approach – Network Analyzer

Module 1 – Network Analyzer: Advanced methods that automatically provide cyber-attack detection and defense through multi-layer control protocol validation



Risks: Proposed network analyzer could add extra latencies in the control system environment.

Mitigation: Learn protocol states and detection algorithms offline using existing data and data collected from the HIL testbed. Deploy pre-trained models on BAS server for real time prediction.

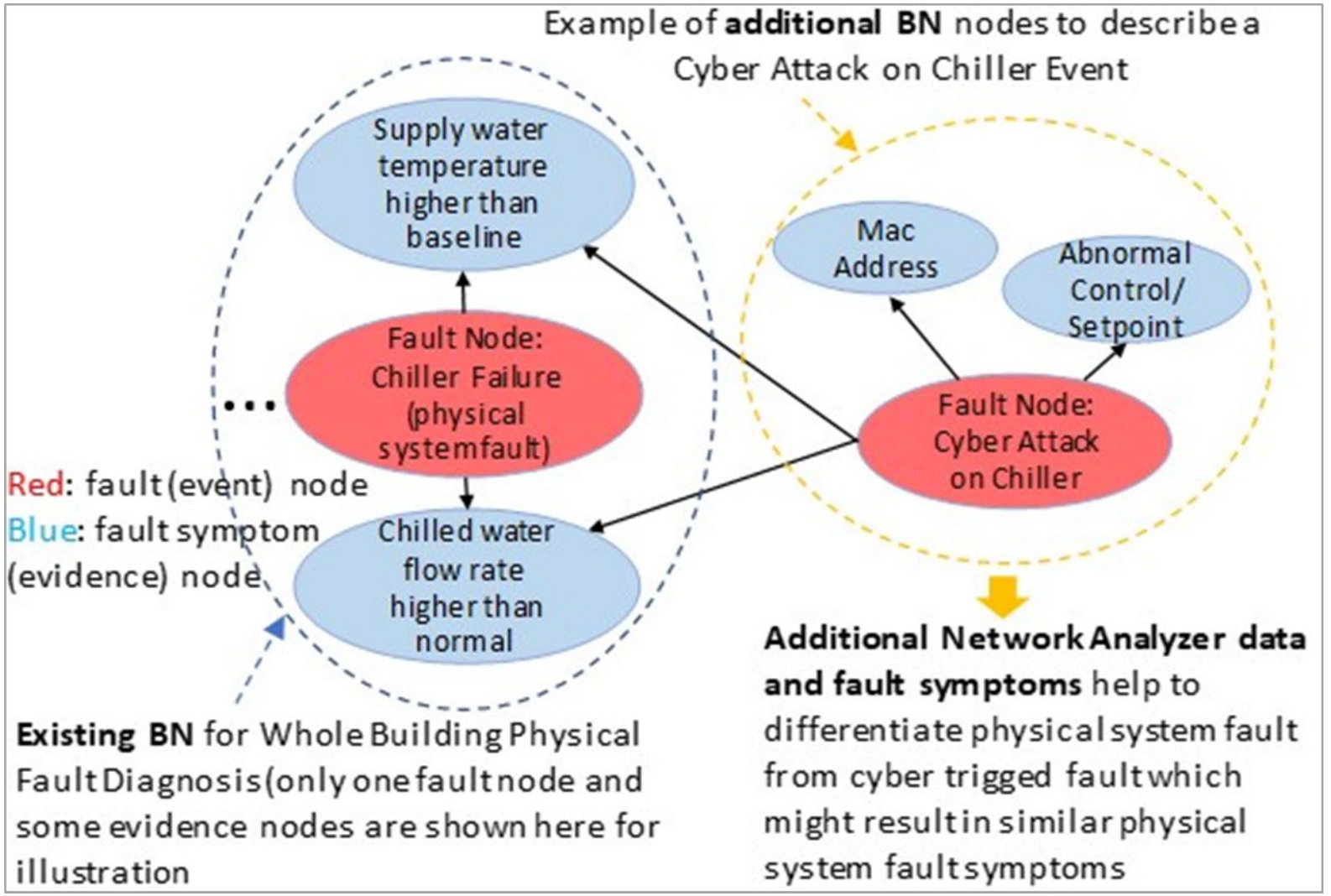
CRF: Conditional Random Field

CYDRES Approach – AFDDP

- Module 2 – AFDDP: Integrated cyber- and physical-system fault diagnosis, prognosis, and localization using multi-stream data-sources, ensemble machine learning, and dynamic adaptive techniques for accurate situation awareness and physical-system health assessment.

Risk: Curse of dimensionality due to large data sources.

Mitigation: Several feature reduction methods such as RMT to mitigate these risks.



The proposed dynamic BN for cyber and physical faults diagnosis

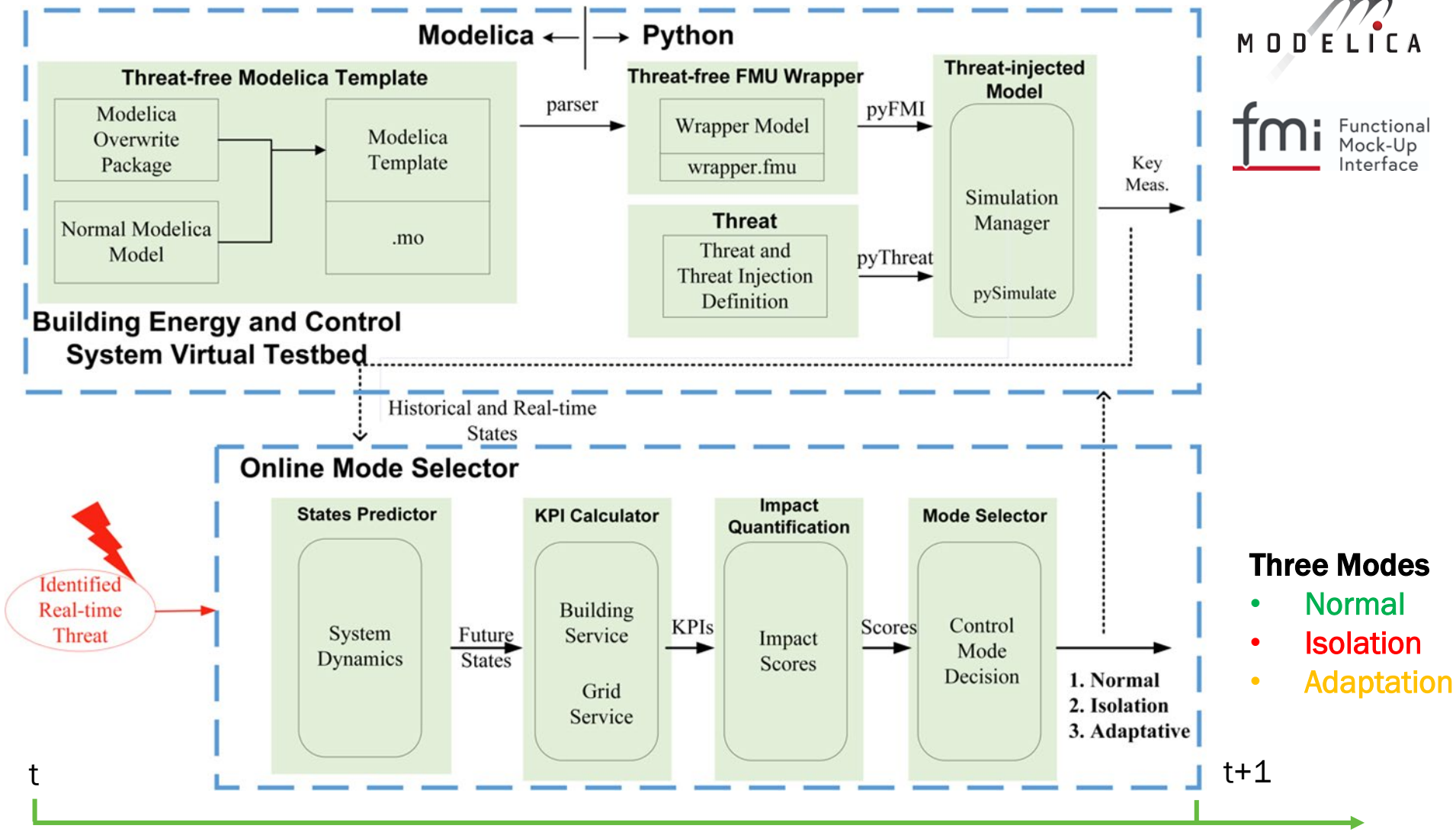
AFDD: Automated Fault Detection, Diagnosis and Prognosis
BN: Bayesian Network

CYDRES Approach – Mode Selector through Impact Analysis

Modules 3: Intelligent mode selector through impact analysis

Risk: The training of the state predictors may add overhead time for online decision making.

Mitigation: Learn system states from BAS data offline and deploy the learned model for online prediction.



Three Modes
- Normal
- Isolation
- Adaptation

CYDRES Impact – Values Proposition & Market Opportunity

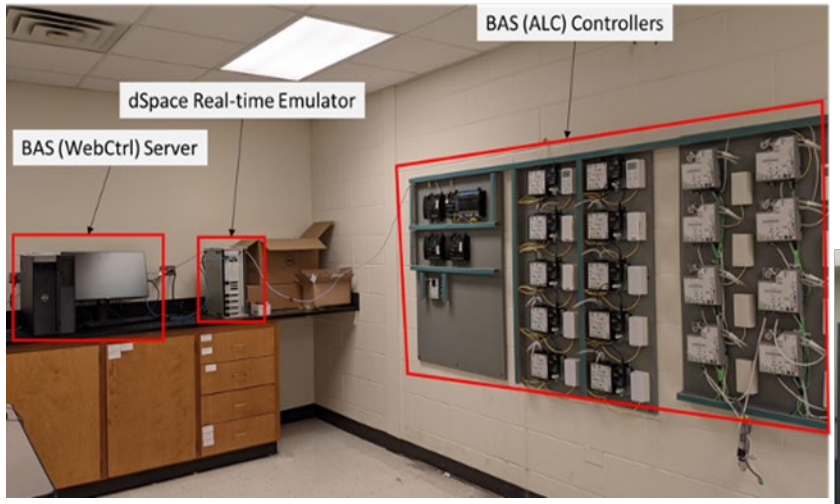
- The global Smart Building Market size is projected to reach USD 109.48 Billion by 2026, exhibiting a Compound Annual Growth Rate (CAGR) of 12.6% during the forecast period.
- The target market is the building automation system, which is expected to reach $91.11 billion by 2022.
- U.S. cybersecurity breaches involving building control system increased by 75% from 2011 to 2014. (Memoori report).
- With a rapid growth of smart building and GEBs, it is anticipated that the proposed CYDRES will enable cyber-attack-immune buildings through control capabilities to detect and adapt to cyber-related threats.

The market size of the intended end user of this technology is all commercial buildings with BAS in the U.S., and the primary energy savings anticipated across the U.S. 2030 building stock is approximately 0.86 Quads (860 TBtus), as estimated using the DOE *Scout* tool.

CYDRES Impact – Competitive Advantage

1) Enable **cyber-attack-immune** GEBs to automatically prepare, adapt, and isolate the building energy and control systems to protect the building systems, to mitigate the impact of the cyber threats, and to maintain continuity of the building operation and occupants' comfort.
2) Achieve at least 15% HVAC energy savings while maintaining occupants' comfort.
3) Preserves building demand flexibility and minimizes electrical grid's impact (e.g., grid instability due to large scale coordinated building attack during on-peak operation).

CYDRES will be validated through a multi-stage integration and testing process via hardware-in-the-loop (HIL) and real building testing. The project will streamline the cutting-edge network analyzer and control algorithms for cybersecurity into commercial BAS products and expedite the transfer of the latest technologies to benefit building owners, building automation companies, and utility companies.



TAMU HIL testbed

CYDRES Progress – Network Analyzer

Through preliminary testing, the CRF based command validation can detect > 75% of attacks that violate the protocol state transition rules (Passed BP1 Go/No-Go Decision Point)

CRF-Command Validator vs. other Cyber Detectors

- Higher detection rate on attacks that violates the protocol state transition rules (>95% at this time).
- No dependencies on prior knowledge of the protocol or BAS implementation.

Attack	Base case	Attack case	Detection Accuracy	Location	Detection Delay (Ave.)
Network DOS Attack	Benign Server Sending ReadProperty requests to 3 devices in 5Hz	150 Zoombies Attacking Device 1	44 / 46 = 95.65%	Device 1 (44) Device 2 (23) Device 3 (15)	2.656s
		300 Zoombies Attacking Device 1	45 / 45 = 100%	Device 1 (45) Device 2 (6) Device 3 (3)	0.847s
		600 Zoombies Attacking Device 1	43 / 45 = 95.55%	Device 1 (43) Device 2 (25) Device 3 (25)	1.326s
Device DOS Attack	Benign Server Sending ReadProperty requests to Device in 5Hz	Reinitilization request to Device 1 per 20s	21 / 21 = 100%	Device 1	0.883s
Device Backdoor Attack	Benign Server Sending WriteProperty requests to Device in 5Hz	WriteProperty request with out-of-bound payload (40%)	255 / 255 = 100 %	Device 1	0.082s
Overall	-	-	>95%	-	<2.6s

CRF: Conditional Random Field

DOS: Denial of Service

CYDRES Progress – AFDD

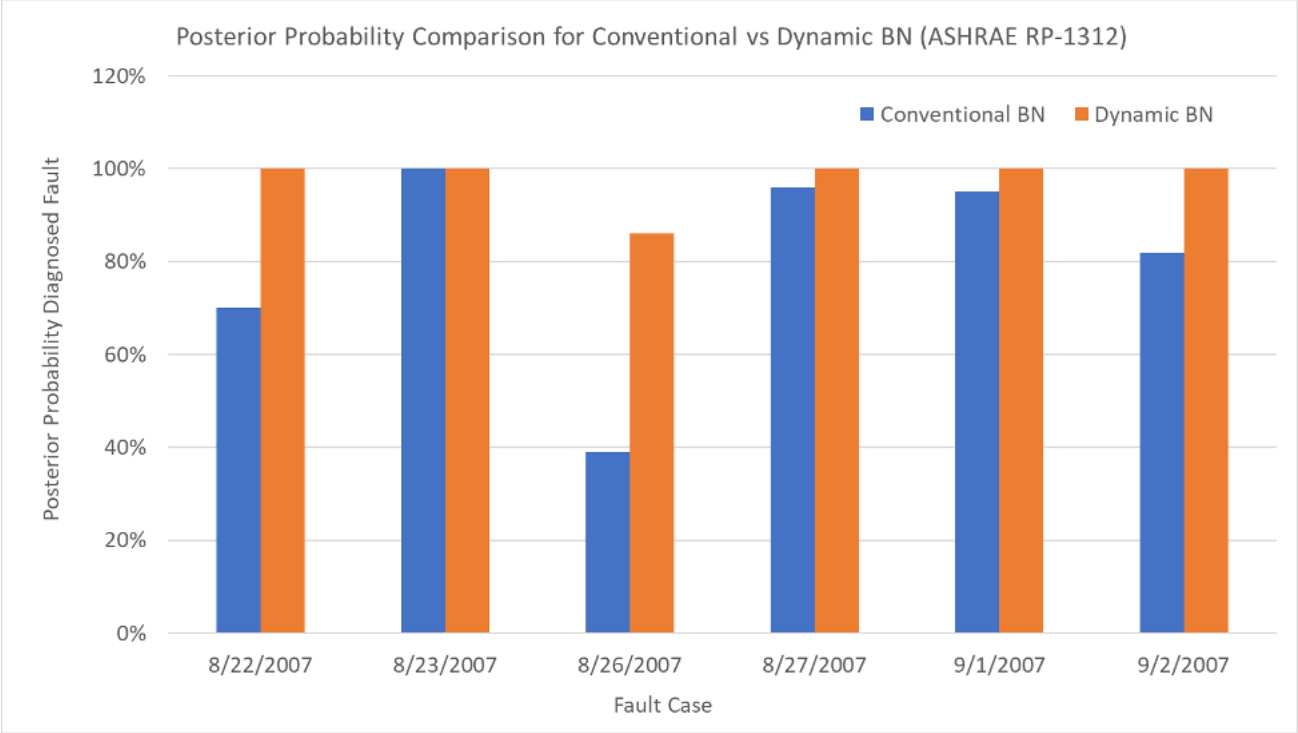
Dynamic Bayesian Network (DBN) shows more sensitivity than conventional BN and is robust to different control strategies

- DBN Based On Typical Control Sequences
  - Tested 14 whole building fault cases (from DE-FOA-0001167) and 11 component-level fault cases (from ASHRAE RP-1312).
  - Sensitivity analysis on temporal conditional probabilities showed that the DBN is a robust method for fault diagnosis.

- DBN Based On ASHRAE Guideline-36: High Performance Sequences of Operation for HVAC Systems.
  - Tested 18 fault cases for the cooling/shoulder season.
  - Causal relations based on difference between fault-injected model and baseline model experimental data simulated in Modelica.

Fault diagnosis result summary using DBN

Dataset	Control Sequence	Total fault cases	Diagnosed	Misdiagnosed
DE-FOA-0001167	Traditional	14	12	2
ASHRAE RP-1312	Traditional	11	11	0
Modelica	ASHRAE G-36	18	14	4



CYDRES Progress – Intelligent Mode Selection

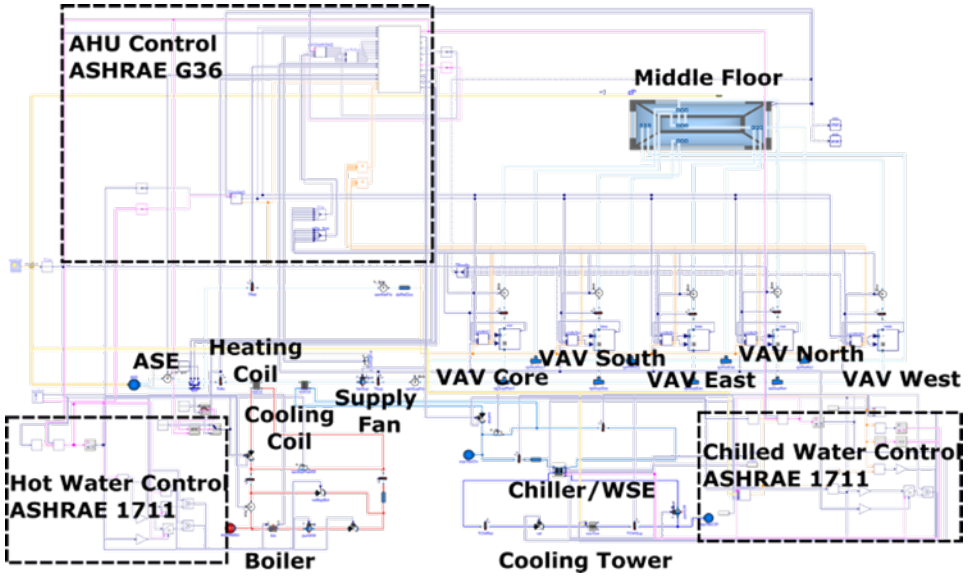
Mode selection strategy provides real-time cyber-resilient decisions

Numerical Testcase

- **Case Description**
  - At 12pm on a summer day, Module 2 identifies an attack that remotely shut off the chiller.
  - Online mode selector look ahead 2 hours for impact quantification.
- **Case Results**
  - Mode Selection: Adaptive Control

Metric	Attack	Baseline
KPI Costs	2.38	2.17
Impact Score	9.7%	
Computation Time (s)	0.68	

System Model in Modelica



Category	Consequence	KPI	Calculators
Quality of Building Service	Compromised energy efficiency	Energy Usage (kWh)	$\sum_{e\in E}\sum_{t=t_0}^{t_N} P_e(t)$
	Compromised power demand	Peak Power Demand (kW)	$\max_{t_0\le t\le t_N}\sum_{e\in E} P_e(t)$
	Increased thermal discomfort	Total Discomfort Hours (Kh)	$dt_T^z = \frac{1}{3600}\int_{t_0}^{t_N} c(T^z(t))dt$
Quality of Grid Service	Compromised demand flexibility	Demand Flexibility	$\overline{DFI}(t,\Delta t) = \frac{\int_t^{t+\Delta t}\bar{P}dt - \int_t^{t+\Delta t} P_{ref}dt}{\Delta t}$ $\underline{DFI}(t,\Delta t) = \frac{\int_t^{t+\Delta t} P_{ref}dt - \int_t^{t+\Delta t}\underline{P}dt}{\Delta t}$

CYDRES Stakeholder Engagement – Market Study & IAB

- **Market Barriers**
  - Cost, accuracy, the easy-of-use, and scalability.
  - Lack of awareness and education on cyber-security in buildings.
- **Mitigation Strategy**
  - Reducing engineering costs through computationally efficient learning-based approaches and increasing AFDDP accuracy through more data-driven statistical process control methods and machine learning strategies are the key objectives of this project.
  - Teaming up with ALC, a major BAS manufacturer and distributor, and ASHRAE BACnet committee can help quickly reach a large percentage of end users through their existing sales network.

Name	Position and Affiliation
Steven Bushby	Leader, Mechanical Systems and Controls Group Engineering Laboratory National Institute of Standards and Technology ASHRAE BACnet SSPC 135 Chair (2000-2004)
Jim Butler	CTO, Cimetrics Inc. ASHRAE BACnet IP workgroup (BACnet/SC) Chair
Carol Lomonaco	Johnson Controls, Inc., Sr. Product Manager – Metasys ASHRAE TC 2.10 Resilience and Security Chair
Joe Zhou	Principal Engineer, Slipstream Lead Author for Smart Grid Application Guide: Integrating Facilities with the Electric Grid
Chirag Parikh	Applications Engineer, Carrier Automated Logic Corporation
Nathaniel Benes	Manager, Automation Technology, UNL ASHRAE Voting Member, BACnet SSPC 135 U.S. Technical Expert, ISO/TC 205

CYDRES Stakeholder Engagement – Activities

This 3-year project just passed the BP1 Go/No GO gate review. Stakeholder engagement activities:

- Strategically pursued industrial partnership with building automation company and building network communication protocol standard committees.
  - ALC, JCI, ASHRAE BACnet committee/Cimetrics.
  - ASHRAE Technical Committee (TC) 7.5 Smart Building Systems.
- Engage with ASHRAE SSPC 135 to add secured communication to BACnet.
- JCI/ALC are working closely with the team as technical advisors.
- In the late phase of the project, JCI/ALC will help evaluate the cost effectiveness of deploying the proposed CYDRES, the additional benefit it will provide, and its impact on the existing pricing model.
- If additional follow-on support is obtained, JCI/ALC will take the lead in demonstrating the proposed approach in a wider set of buildings by integrating with the business model.

CYDRES Remaining Project Work

1. **Network Analyzer (BP2)**
   - Further development of the CCV
     - Develop software modules to enable real-time CCV detection
     - Develop interface to Module 2 -AFDDP
   - Further evaluation and testing
     - Test the detection performance of CCV on HIL with physical impact analysis
     - Test the integration performance of CCV in passing data to Module 2
2. **AFDDP (BP2 &BP3)**
   - AFDDP for integrated Network and BAS data, using new baseline strategy, RMT feature, and DBN
   - Fault diagnosis and prognosis using acoustic sensors
   - Testing of AFDDP strategies using data collected from the HIL testbed and a real building
3. **Cyber Resilient Control Framework (BP2 & BP3)**
   - Cyber resilient control framework though adaptive MPC
   - Testing using HIL testbed and a real building
4. **Situation Awareness Framework (interface) (BP2 & BP3)**
5. **CYDRES Demonstration and Testing (BP3)**

CCV: CRF-Command Validator
CRF: Conditional Random Field
AFDD: Automated Fault Detection, Diagnosis and Prognosis
HIL: Hardware-In-the-Loop
RMT: Robust Multivariate Temporal
DBN: Dynamic Bayesian Network
MPC: Model Predictive Control

Thank You

Texas A&M University
Zheng O'Neill, PhD, PE
Tel: 979-458-4931; Email: ZONeill@tamu.edu

REFERENCE SLIDES

Project Budget

Project Budget: BP1: DOE $952, 859, CS $242, 066; BP2: DOE $1,069,394, CS $266,565; BP3: DOE $826,532, CS: $205,178.
Variances: 18% BP1 budget was carried over to BP2
Cost to Date: DOE: $788,971, CS: $224,739
Additional Funding: None

Budget History					
05/01/2020– FY 2020 (past)		FY 2021 (current)		FY 2022 – 04/30/2023 (planned)	
DOE	Cost-share	DOE	Cost-share	DOE	Cost-share
$952,859	$241,066	$1,069,394	$266,565	$826,532	$205,178

Project Plan and Schedule