SAND2020-11400PE

Exceptional service in the national interest

Intrusion Detection & Response for Distributed Energy Resources & Building Automation Systems

PRESENTED BY

C. Birk Jones, Ph.D.

SENIOR MEMBER OF STAFF

RENEWABLE, DISTRIBUTED SYSTEMS INTEGRATION

October 20, 2020

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

AGENDA

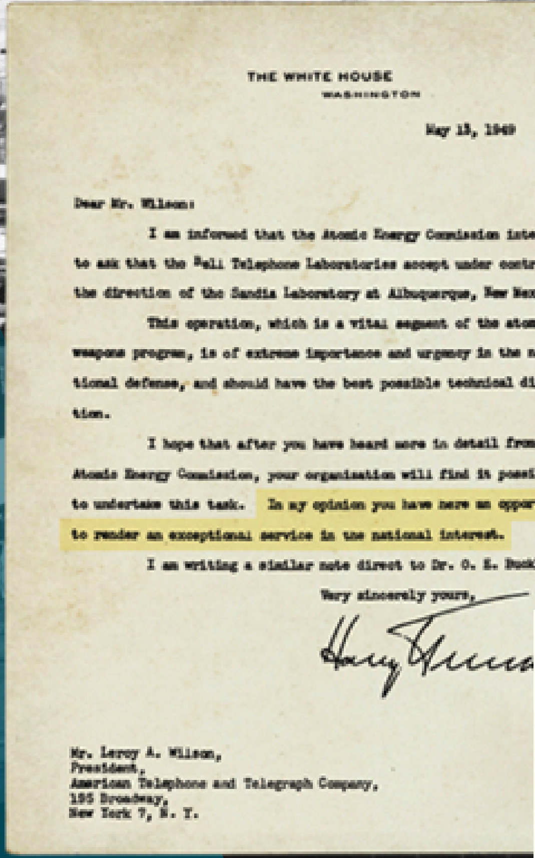
- **Sandia National Laboratories**
- **My Background**
- **Electric Grid**
- **Distributed Energy Resources (DER)**
  - *Integration & Control*
  - *Cybersecurity*
- **Building Automation Systems**
  - *Automation & Control*
  - *Intrusion Detection & Response*
  - *Automation Interactions with the Grid*

Sandia National Laboratories

SANDIA'S HISTORY IS TRACED TO THE MANHATTAN PROJECT

…In my opinion you have here an opportunity to render an exceptional service in the national interest.

- July 1945
  Los Alamos creates Z Division
- Nonnuclear component engineering
- November 1, 1949
  Sandia Laboratory established
- AT&T: 1949–1993
- Martin Marietta: 1993–1995
- Lockheed Martin: 1995–2017
- Honeywell: 2017–present



THE WHITE HOUSE
WASHINGTON

May 13, 1949

Dear Mr. Wilson:

I am informed that the Atomic Energy Commission intends to ask that the Bell Telephone Laboratories accept under contract the direction of the Sandia Laboratory at Albuquerque, New Mexico.

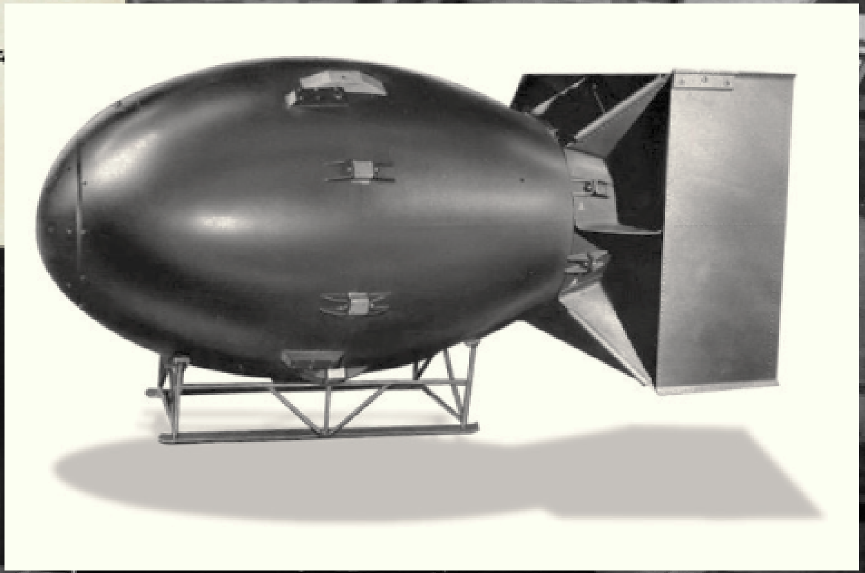
This operation, which is a vital segment of the atomic weapons program, is of extreme importance and urgency in the national defense, and should have the best possible technical direction.

I hope that after you have heard more in detail from the Atomic Energy Commission, your organization will find it possible to undertake this task. In my opinion you have here an opportunity to render an exceptional service in the national interest.

I am writing a similar note direct to Dr. O. E. Buckley.

Very sincerely yours,

Mr. Leroy A. Wilson,
President,
American Telephone and Telegraph Company,
195 Broadway,
New York 7, N. Y.



SANDIA HAS FACILITIES ACROSS THE NATION

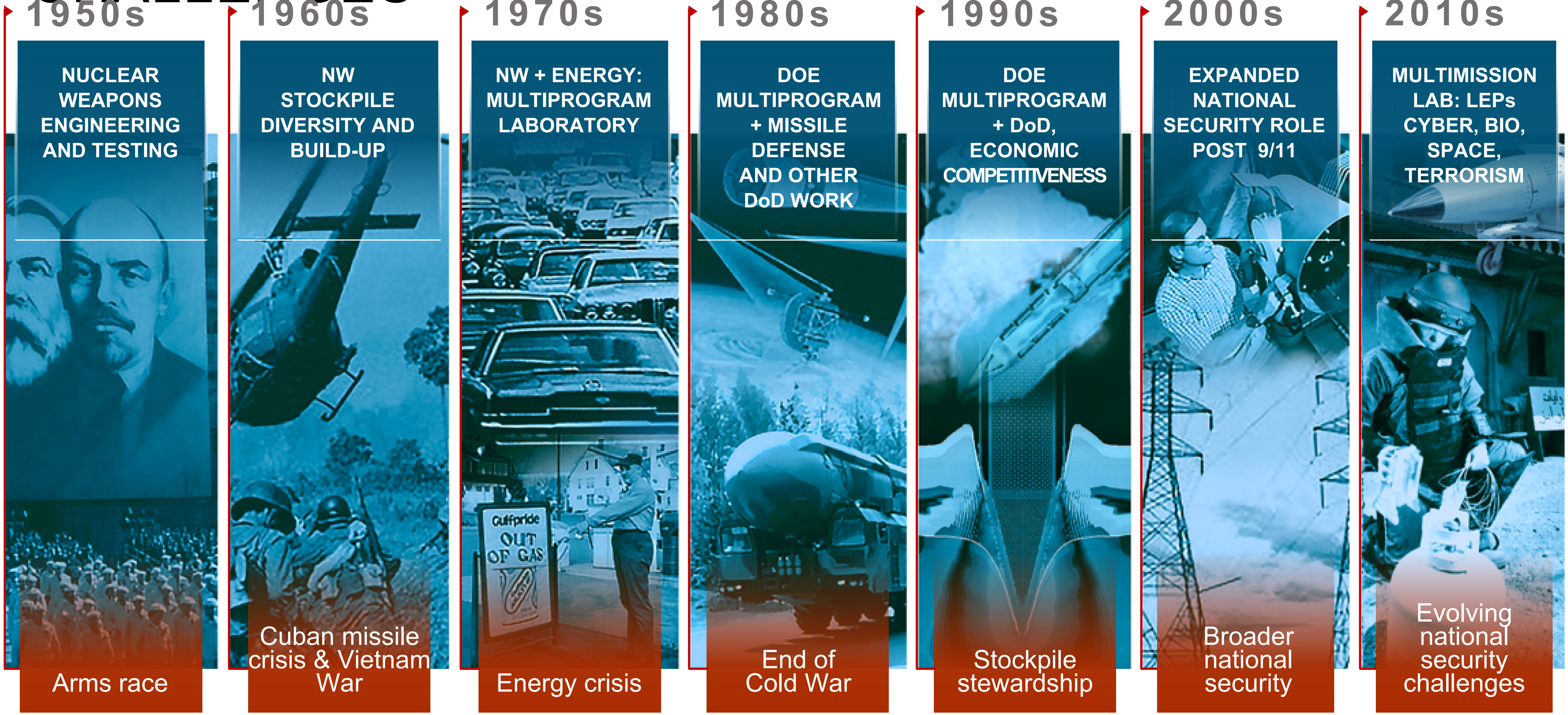
Main sites

- Albuquerque, New Mexico
- Livermore, California

Activity locations

- Kauai, Hawaii
- Waste Isolation Pilot Plant, Carlsbad, New Mexico
- Pantex Plant, Amarillo, Texas
- Tonopah, Nevada

SANDIA ADDRESSES NATIONAL SECURITY CHALLENGES



1950s

NUCLEAR WEAPONS ENGINEERING AND TESTING

Arms race

1960s

NW STOCKPILE DIVERSITY AND BUILD-UP

Cuban missile crisis & Vietnam War

1970s

NW + ENERGY: MULTIPROGRAM LABORATORY

Energy crisis

1980s

DOE MULTIPROGRAM + MISSILE DEFENSE AND OTHER DoD WORK

End of Cold War

1990s

DOE MULTIPROGRAM + DoD, ECONOMIC COMPETITIVENESS

Stockpile stewardship

2000s

EXPANDED NATIONAL SECURITY ROLE POST 9/11

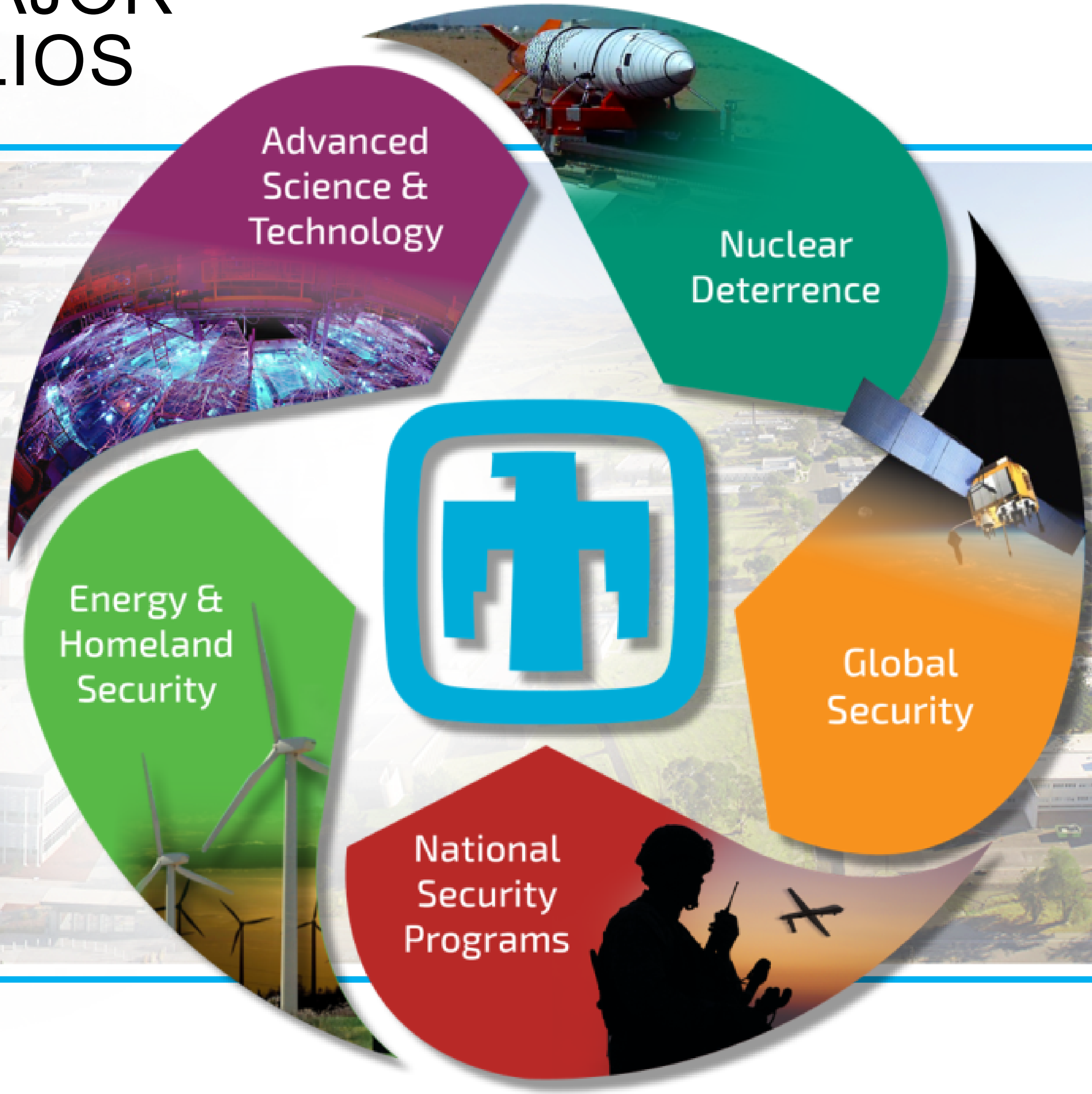
Broader national security

2010s

MULTIMISSION LAB: LEPs CYBER, BIO, SPACE, TERRORISM

Evolving national security challenges

SANDIA HAS FIVE MAJOR PROGRAM PORTFOLIOS


Advanced Science & Technology
Nuclear Deterrence
Global Security
National Security Programs
Energy & Homeland Security

My Background

My Background

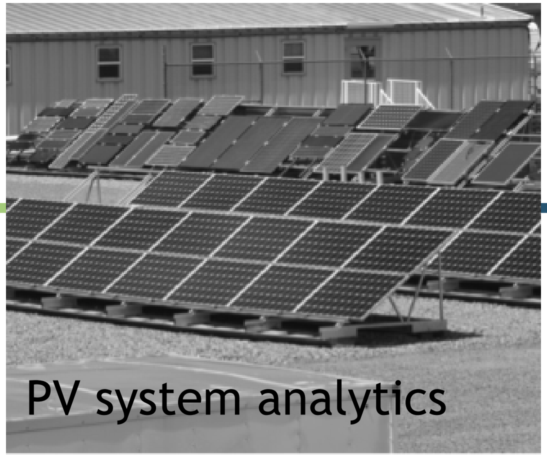
C. Birk Jones

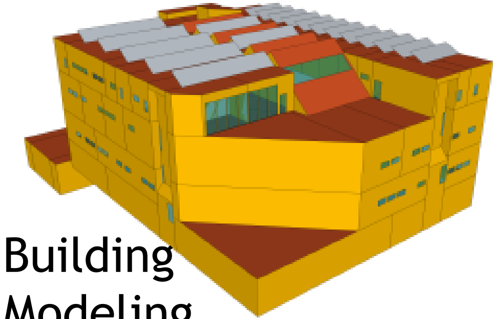
Education:

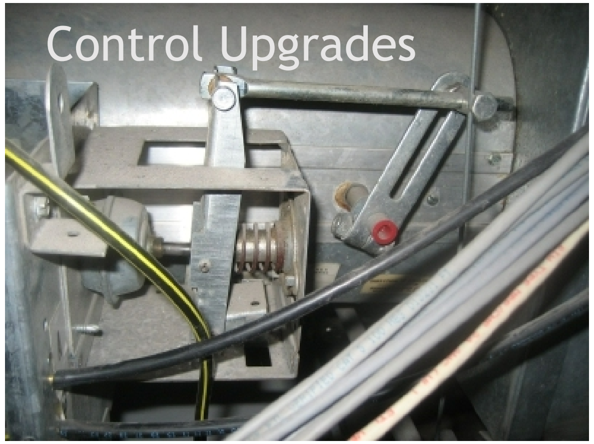
- B.S. Civil and Environmental Engineering
  University of California at Davis, Davis, CA, 2004
- M.S. Construction Engineering
  University of New Mexico, Albuquerque, NM, 2009
- Ph.D. Mechanical Engineering
  University of New Mexico, Albuquerque, NM, 2015

Work Experience:

- Civil & Environmental Engineer
- Structural Engineer & Construction Engineer
- Mechanical Engineer
- Senior Member of Technical Staff at Sandia
  - *Photovoltaic Reliability*
  - *Grid Integration*
  - *Cybersecurity*


PV system analytics


Building Modeling


Control Upgrades

Building HVAC Controls

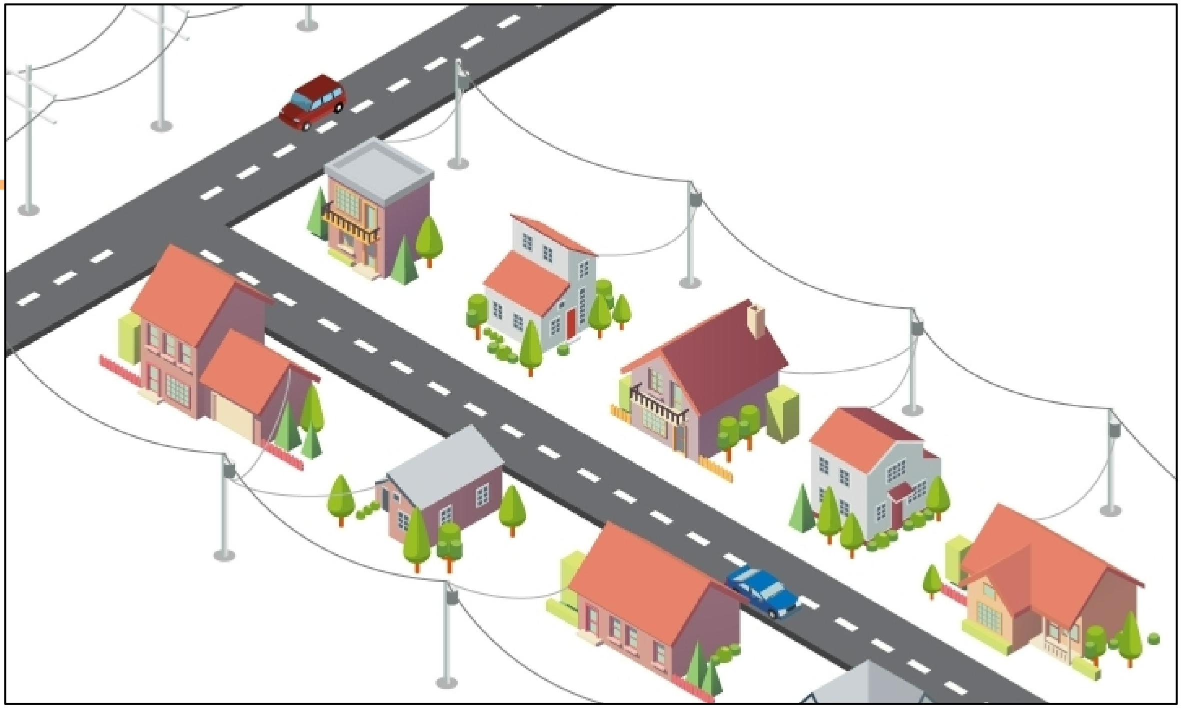
The Electric Grid

Electric Networks

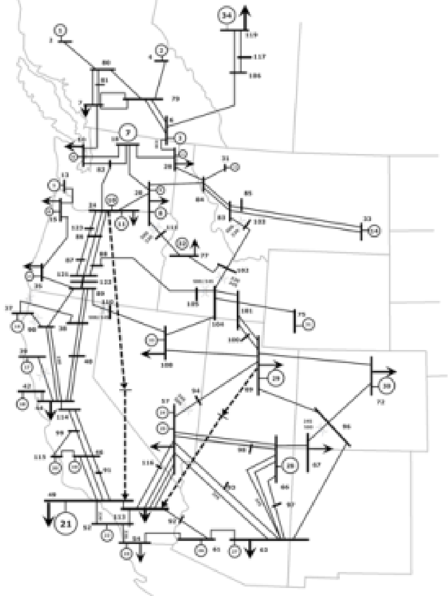
- Power generation, delivery, and consumption at residential, commercial, industrial, and mixed use loads

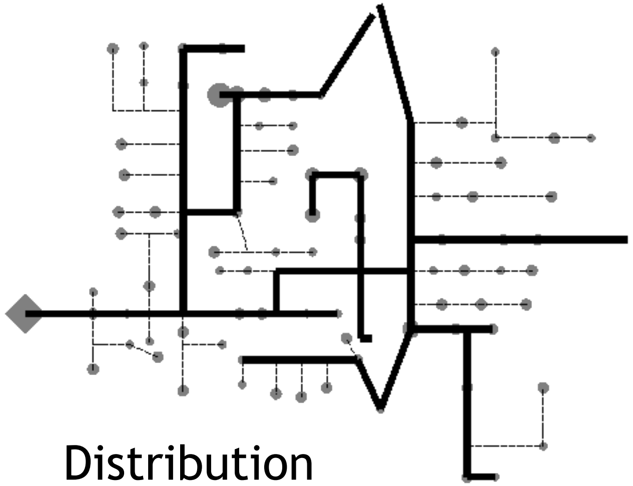
- Transmission
  - Long distance and high voltage
  - Network of generators and loads

- Distribution
  - Short distance and low low voltage
  - Network of loads (and now generators)



Transmission





Distribution

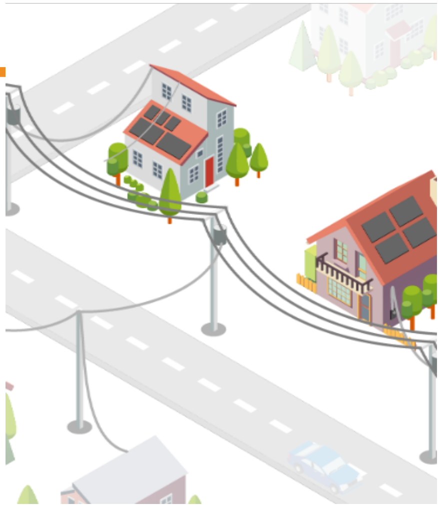
Distributed Energy Resources

Integration & Control of Photovoltaic Svstems

- High penetrations of PV systems require controls to mitigate grid disturbances

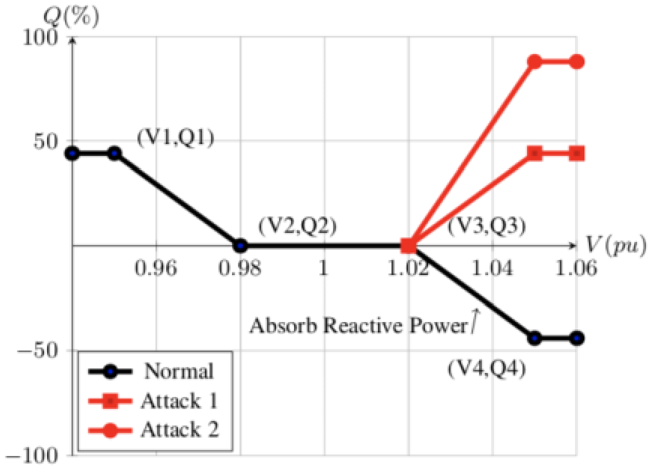
- PV inverters are capable of providing reactive power support

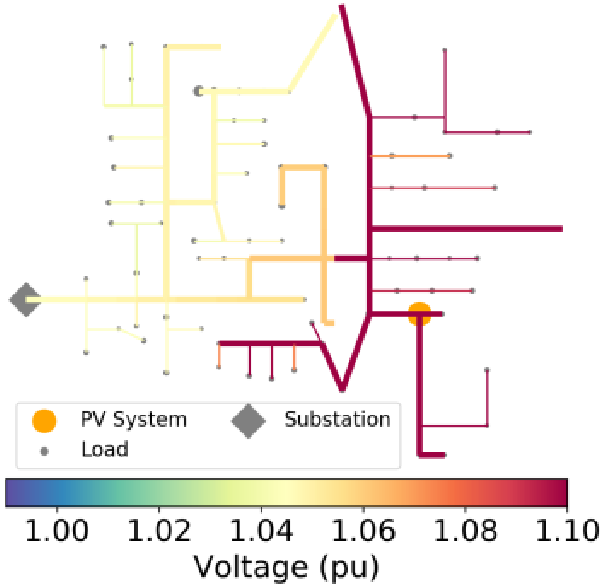
- Manipulation of the inverters may result in grid issues – including voltage violations



PV Integration

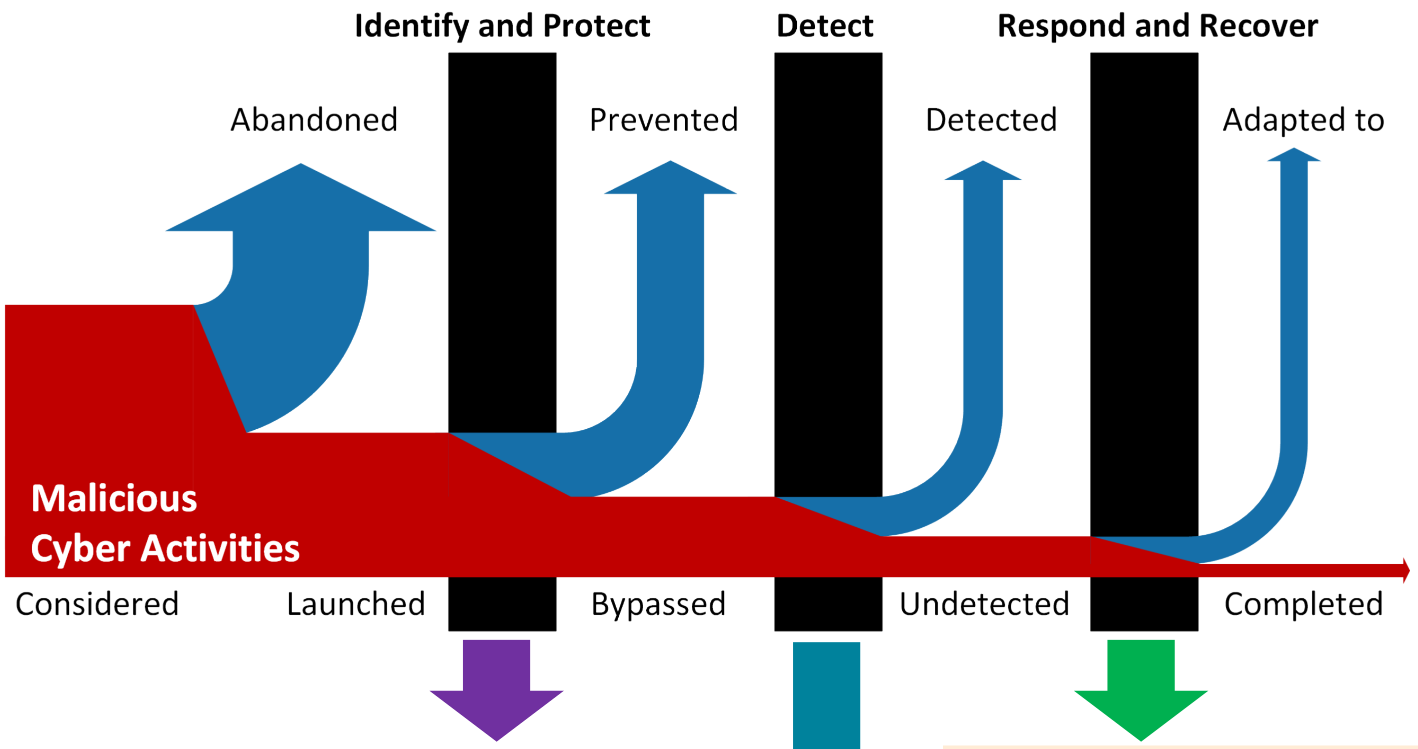
Inverters can provide grid services





Manipulation causes unnecessarily high voltages

Cybersecurity Concerns and Mitigation Measures



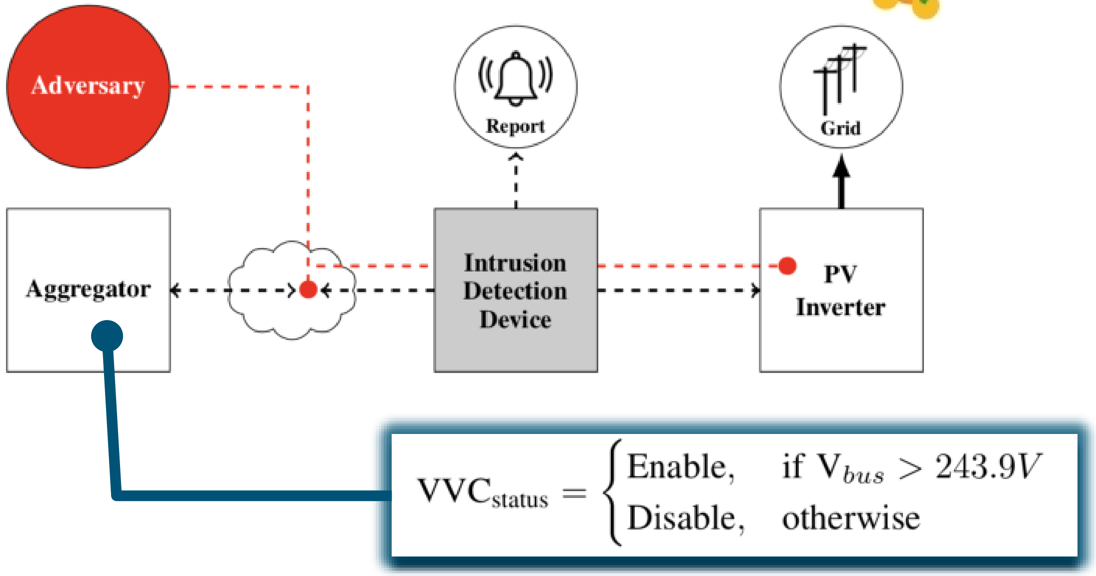
- Threat Models
- Risk Quantification
- Cyber Assessments
- Network Segmentation
- Dynamic Networking and Moving Target Defense
- Trusted and Protected Computing
- Cryptography
- Virtualized Testbed Environments
- Engineering Controls
- Physical Security
- Security for Cloud-Services
- Obfuscation and Deception
- Authentication

- Situational Awareness
- Intrusion Detection

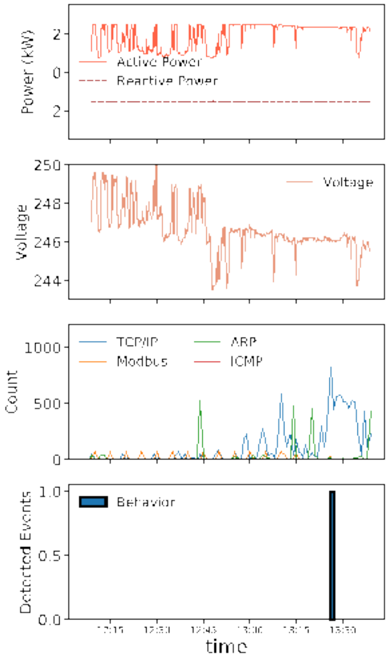
- Resilient Designs
- Dynamic Assessment
- Contingency Operating Modes
- Restoration
- Investigations and Attribution

Research Example:
PV Inverter Intrusion Detection

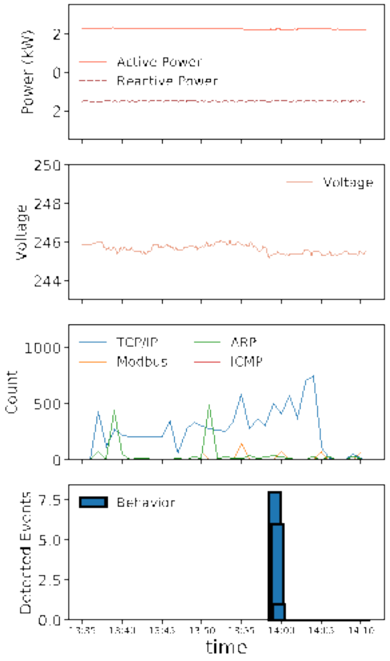
- **Intent:** Compare signature vs behavior based detection methods
- **Hypothesis:** Behavior-based approaches will detect a larger number of attack types
- **Method:**
  - Actual communications with a grid-tied inverter.
  - Intrusion detection on a Raspberry Pi
  - Adversary attempted to manipulate PV inverter operations



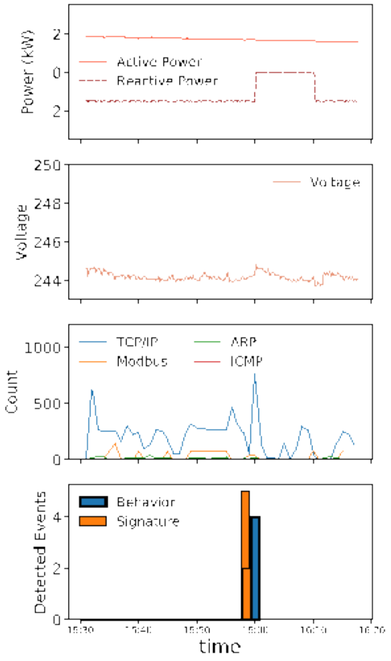
$$\text{VVC}_{\text{status}} = \begin{cases} \text{Enable}, & \text{if } \text{V}_{bus} > 243.9V \\ \text{Disable}, & \text{otherwise} \end{cases}$$



TCP Handshake Spoof



MitM Denial of Service



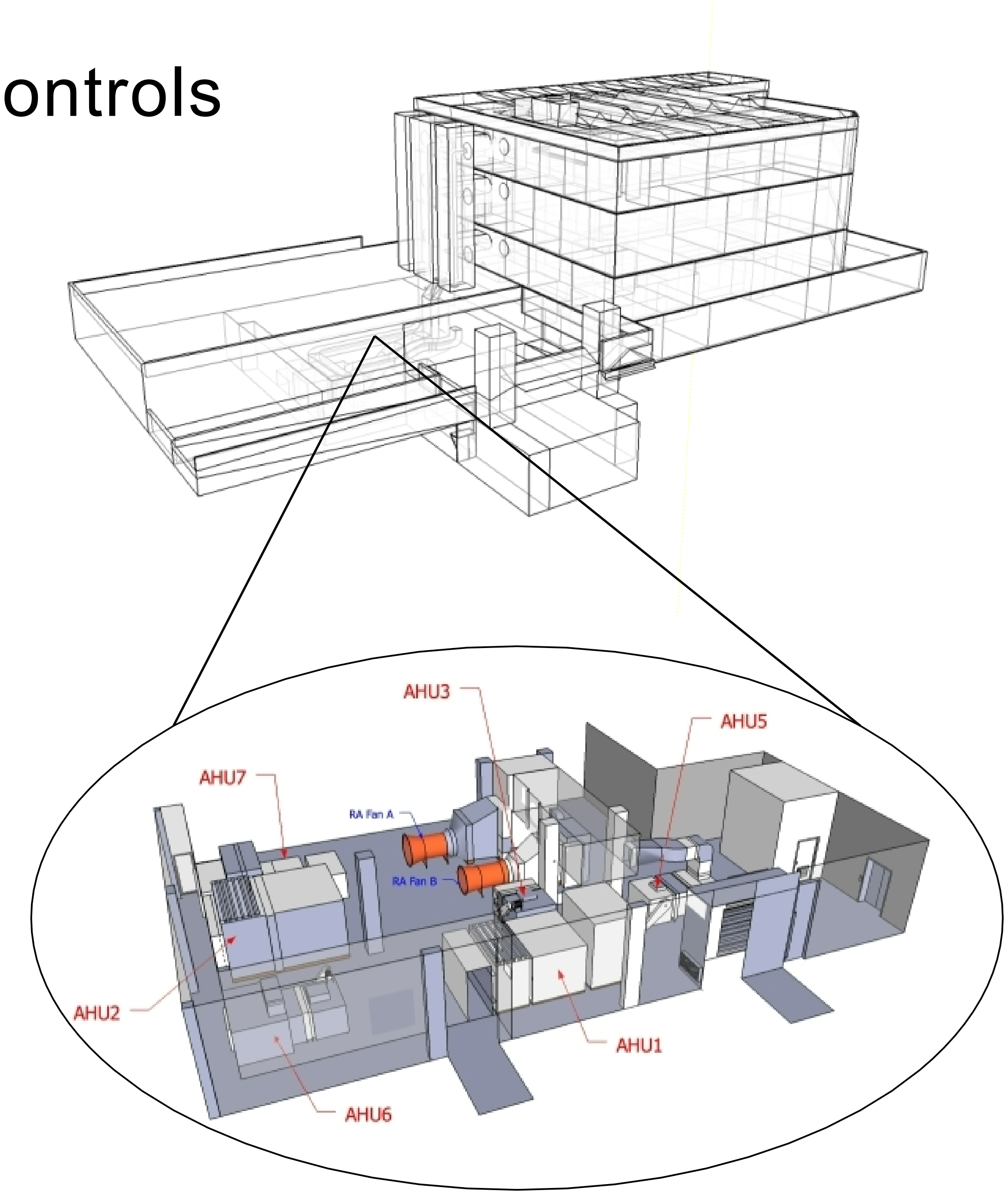
MitM Data Spoof

C. B. Jones, A. R. Chavez, R. Darbali-Zamora and S. Hossain-McKenzie, "Implementation of Intrusion Detection Methods for Distributed Photovoltaic Inverters at the Grid-Edge," *2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Washington, DC, USA, 2020, pp. 1-5, doi: 10.1109/ISGT45199.2020.9087756.

Building Automation Systems

Building Automation System Controls

- Building Automation Systems (BAS) typically control the heating, ventilating, and air conditioning (HVAC) systems
- Heating & Cooling systems are comprised of multiple sub-systems
  - Air handling units
  - Chilled & hot water
  - Terminal units
- Multiple cybersecurity concerns exist

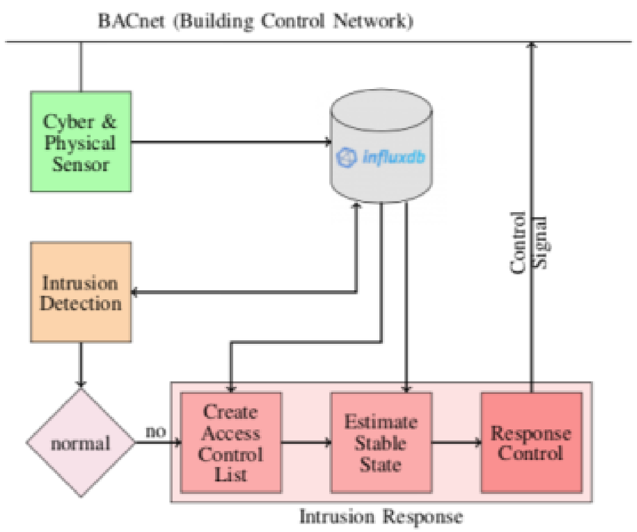


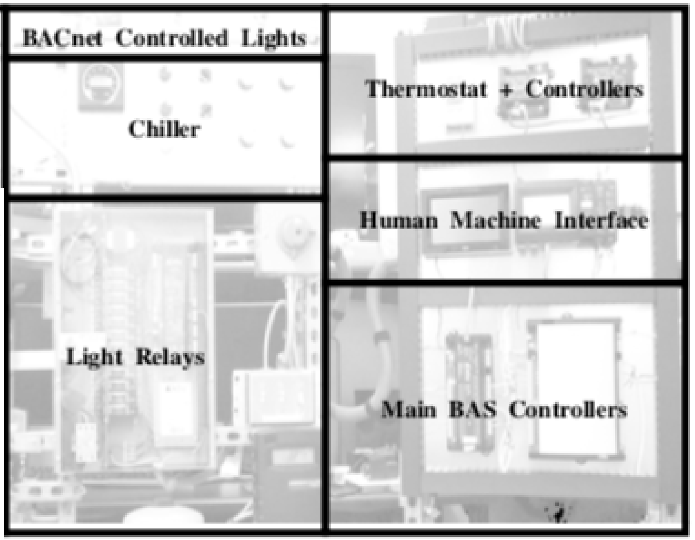
Research Example:

BAS Intrusion Detection & Response

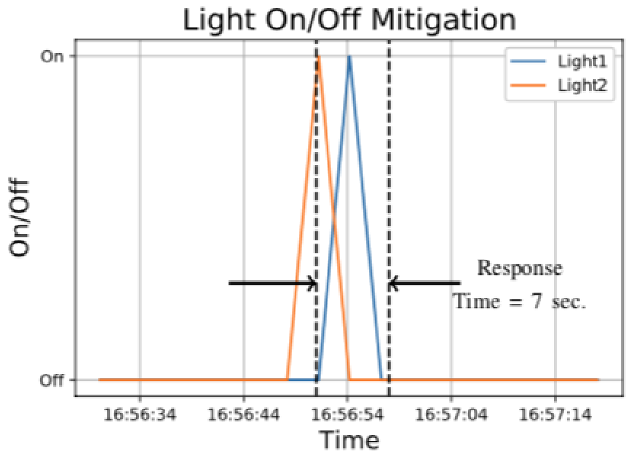
- **Intent:** Create and test a analytics platform that detects and corrects unwanted changes to the BAS.
- **Hypothesis:** An artificial neural network could detect and identify the data point being manipulated.
- **Method:**
  - BAS testbed
  - Created cyber & physical sensors
  - Used an Adaptive Resonance Theory neural network on a Raspberry Pi computer
  - Implemented two attacks on the lights and fan

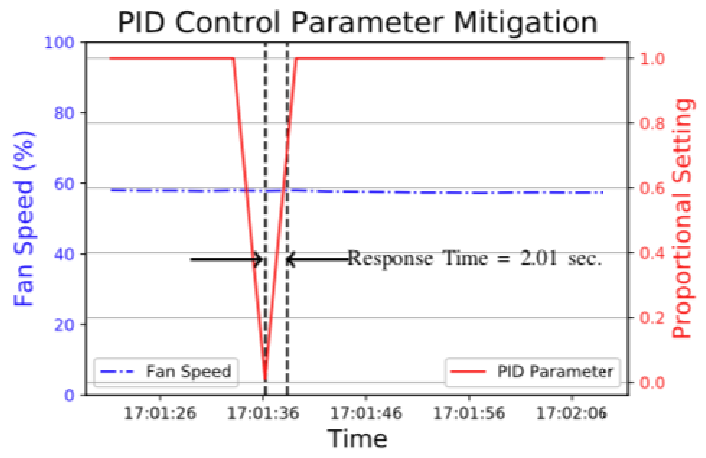
Analysis Platform





BAS Testbed





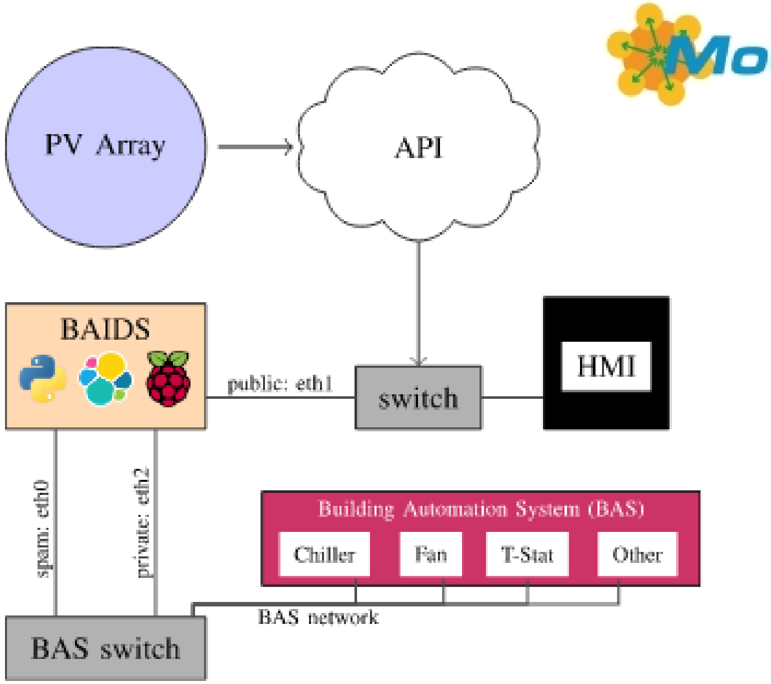
C. B. Jones, C. Carter and Z. Thomas, "Intrusion Detection & Response using an Unsupervised Artificial Neural Network on a Single Board Computer for Building Control Resilience," *2018 Resilience Week (RWS)*, Denver, CO, 2018, pp. 31-37, doi: 10.1109/RWEEK.2018.8473533.

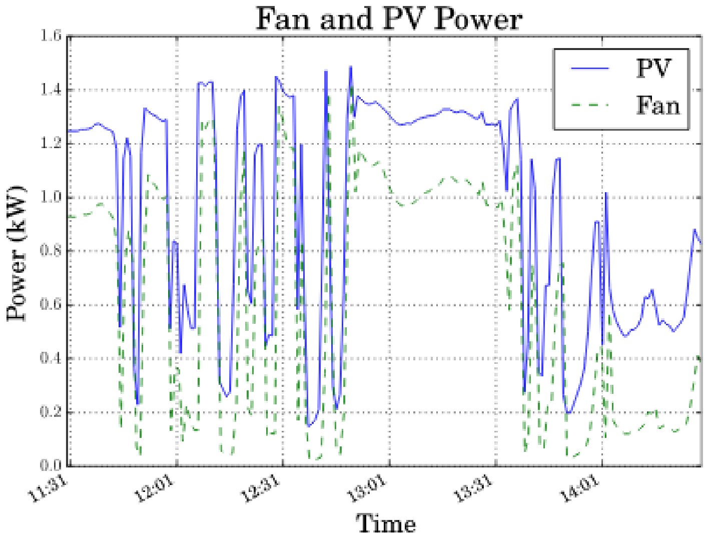
Research Example:
Building Automation Interactions w/ Grid

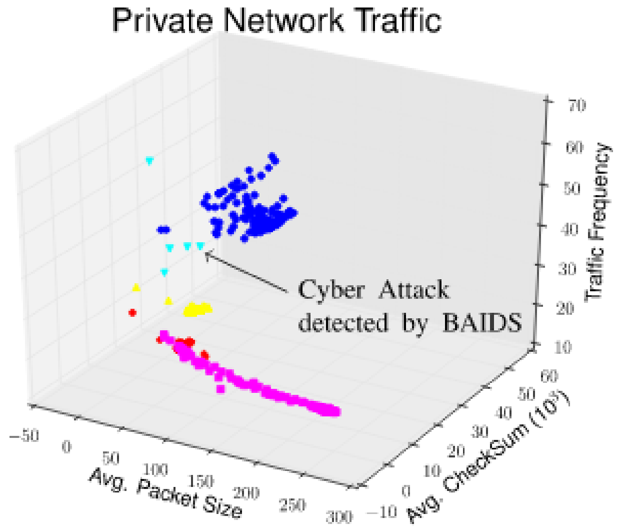
- **Intent:** Create and test an intrusion detection devices that monitors network traffic between a building and an outside source.

- **Hypothesis:** A bump-in-the-wire device can detect abnormal behavior.

- **Method:**
  - Connected PV array and Building Fan
  - Actual communications passed through Raspberry Pi before entering BAS network
  - Neural Network algorithm on Raspberry Pi analyzed traffic







C. B. Jones and C. Carter, "Trusted Interconnections Between a Centralized Controller and Commercial Building HVAC Systems for Reliable Demand Response," in *IEEE Access*, vol. 5, pp. 11063-11073, 2017, doi: 10.1109/ACCESS.2017.2714647.

Thank You

Questions?

C Birk Jones

Senior Member of Technical Staff
Renewable and Distributed Systems Integration
Sandia National Laboratories
cbjones@sandia.gov