Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by **Battelle** *Since 1965*

SHADOW FIGMENT

Model Driven Deception for Cyber-Physical System Defense

THOMAS W. EDGAR

Pacific Northwest National Laboratory

U.S. DEPARTMENT OF ENERGY

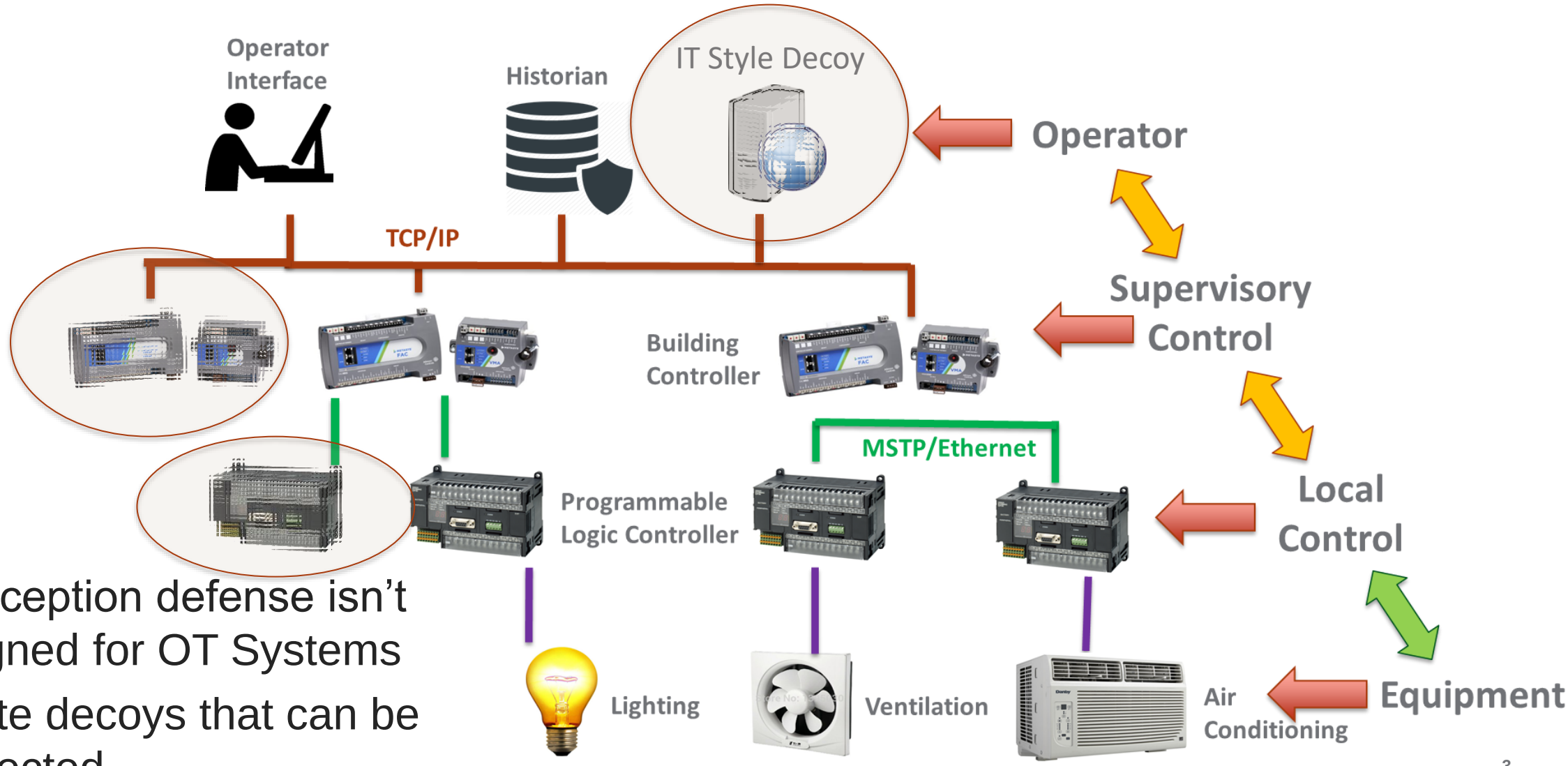
Business Problem

- Critical infrastructure systems have unique cybersecurity challenges
- Owners prioritize **system uptimes** & system availability
- Security solutions must not impact availability

99.999% UPTIME

- Protecting every asset is cost prohibitive
- Common IT solutions aren't supported
  - No continuous patching
  - Lack of crypto

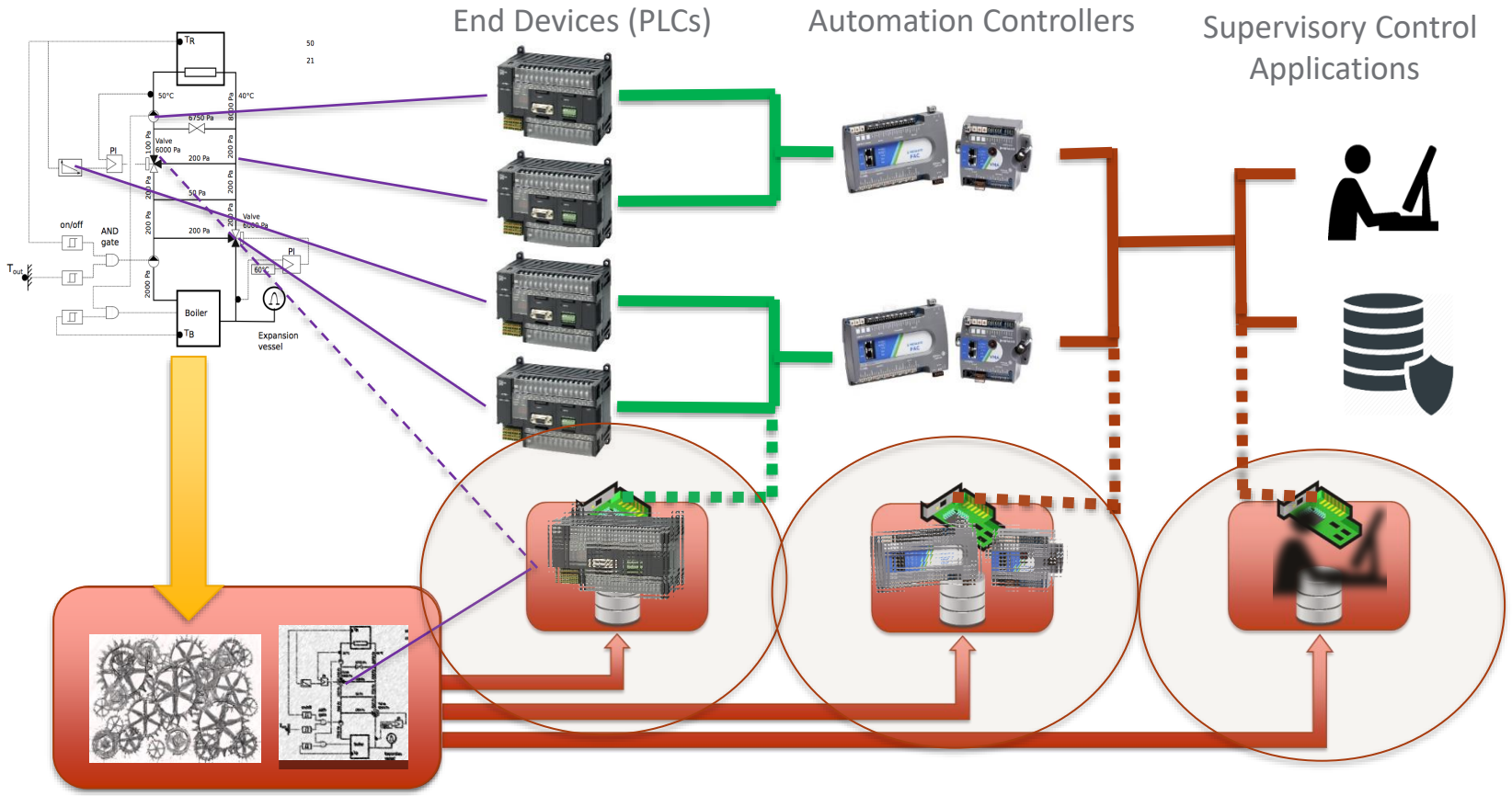
Technical Challenge



- IT deception defense isn't designed for OT Systems
- Create decoys that can be connected

Solution Architecture

- Proof of concept platform providing:
  - ML based process modeling
  - Decoy execution environment
  - Dynamic definition of deception



Development History & Results

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Principal Investigator
Thomas Edgar, Cyber Security Researcher
- Security applications for critical infrastructure
- Successfully licensed previous R&D100 winning technology

Development History
- 2017 Began internal research
- 2019 Began DOE TCF project
- 2019 IEEE HST publication

Funding History
- $200k Internal
- $150k DOE TCF
- $150k (*in-kind*) Attivo Networks

Technology Readiness Level
- TRL ~6

Research
- William Hofer, Cyber Security
- Juan Brandi-Lozano, Data Science
- Garret Seppala, Software Engineer
- Katy Nowak, Data Science
- Draguna Vrabie, Control Engineer

IP Protection
- US Application No. 16/389,758 and CA CA3041865A1 (priority date: 4/2018)

Market Validation
- DOE Technology Commercialization Fund award
- Attivo Networks collaboration

Technical Requirements & Benefits

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Requirements

- Execution platform (could be appliance)
- Network span/tap
- Deception deployment/configuration; ongoing
- Alert monitoring (SIEM integration)

Benefits

- Orient attacker resources away from real CPS
- Bias attacker's beliefs on real CPS operation
- Enhance detection of adversarial behavior with reduced false positive rate
- Understand threat objectives

Technical Roadmap

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Data

- Develop any unique data collection mechanisms
- Develop data parsers for control system protocols

Profiles

- Define high fidelity profiles of sector equipment
- Develop unique decoy services for sector equipment

Models

- Validate generative modeling with sector data
- Define common collections/ configurations of deceptions for sector

Platform

- Create execution platform
- Develop user interface
- Create interfaces with incidence management tools

Pilot

- Pilot within Ethernet based control system

Thank You

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Shadow Figment PoCs:

Principal Investigator
Thomas W. Edgar
thomas.edgar@pnnl.gov

Commercialization Manager
Kannan Krishnaswami
kannan.krishnaswami.@pnnl.gov

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

SHADOW FIGMENT
DEMO

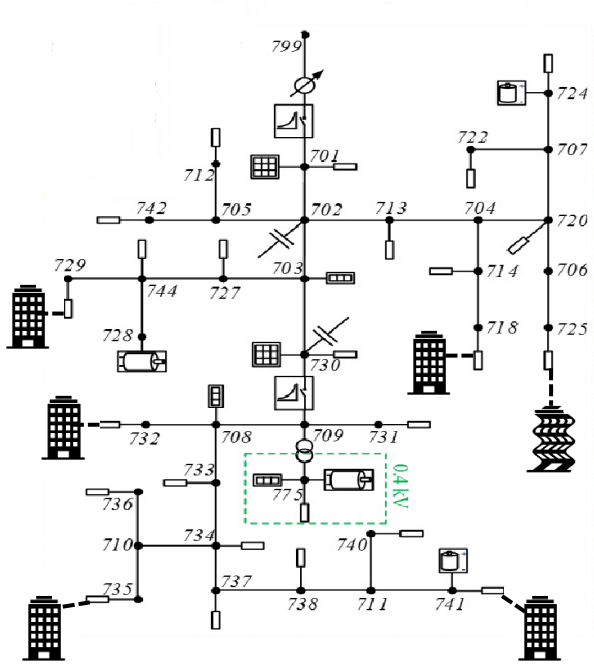
THOMAS W. EDGAR

Pacific Northwest National Laboratory

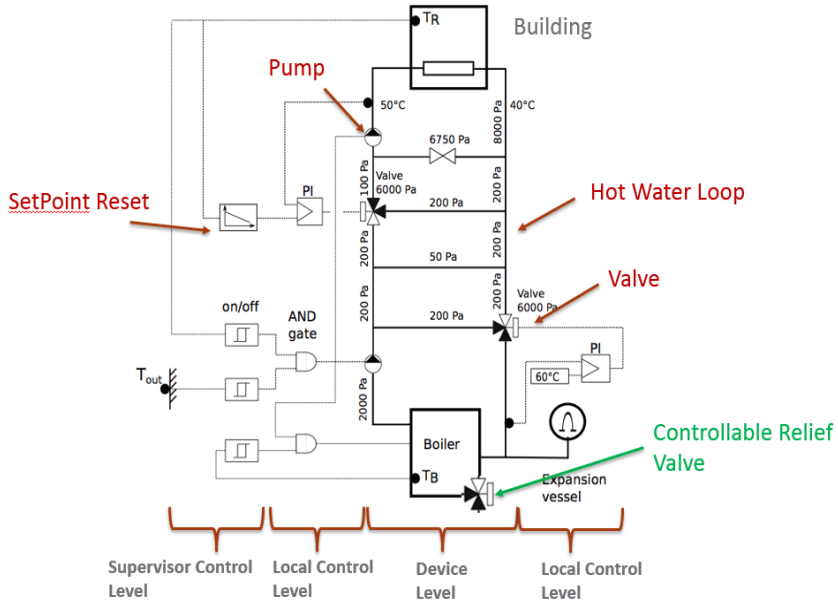
U.S. DEPARTMENT OF ENERGY

Demonstration Objectives

- Show decoy deployment
  - Two types of deception
- Highlight effect on threat awareness
- Demonstrate value to defender



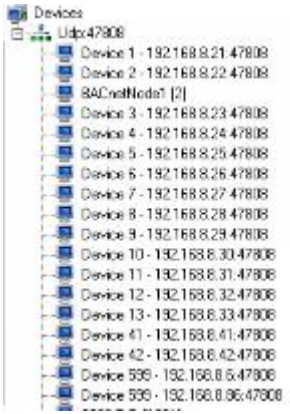
System copy deception



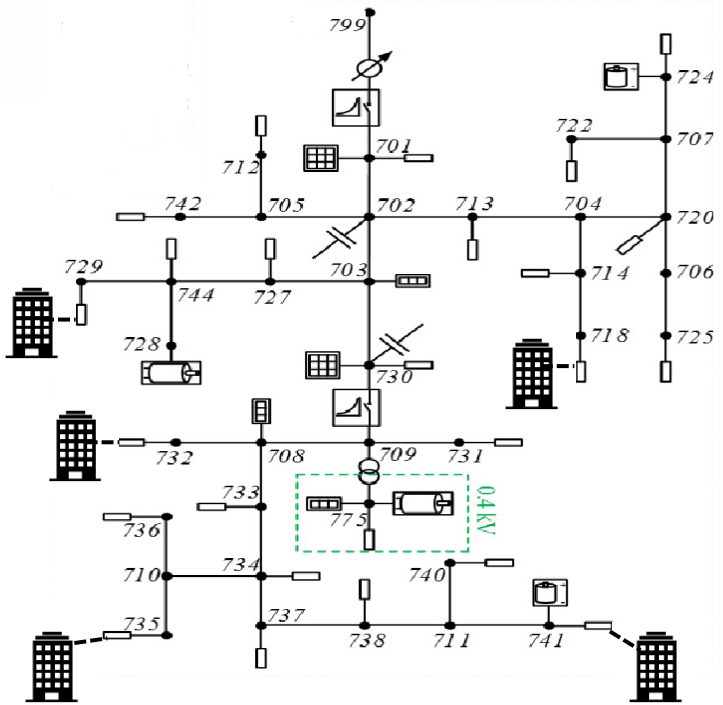
Integrated decoy deception

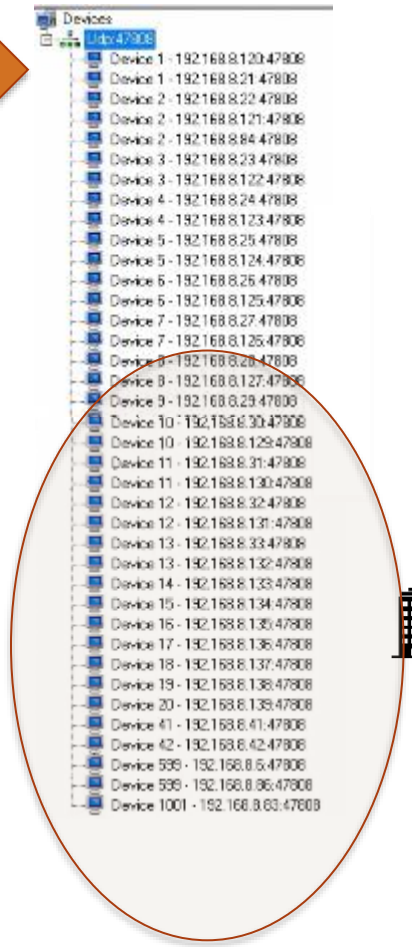
Creating Decoys

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

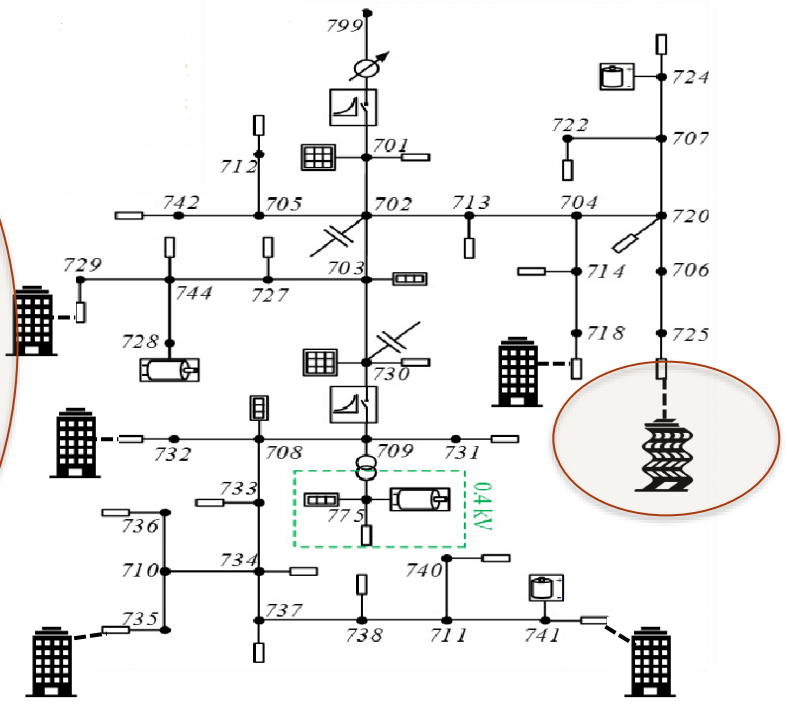


Actual Devices

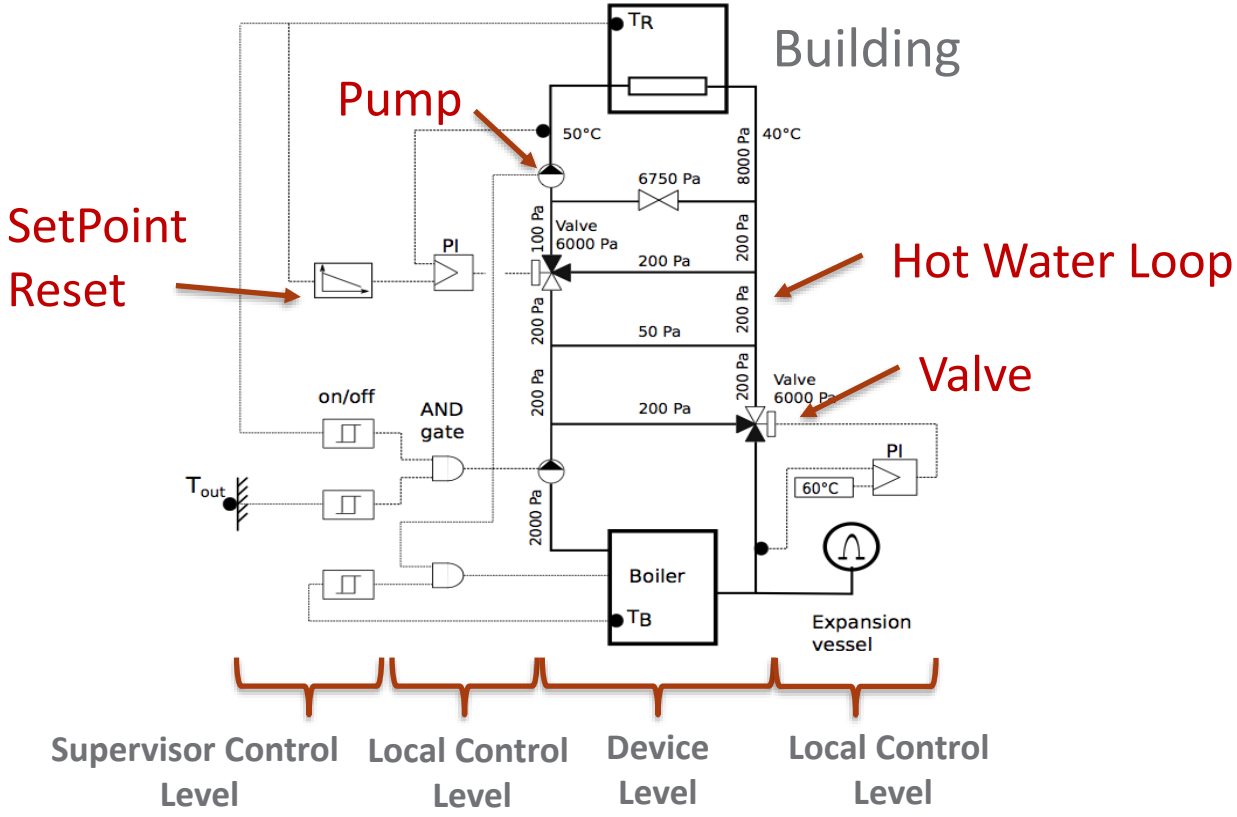


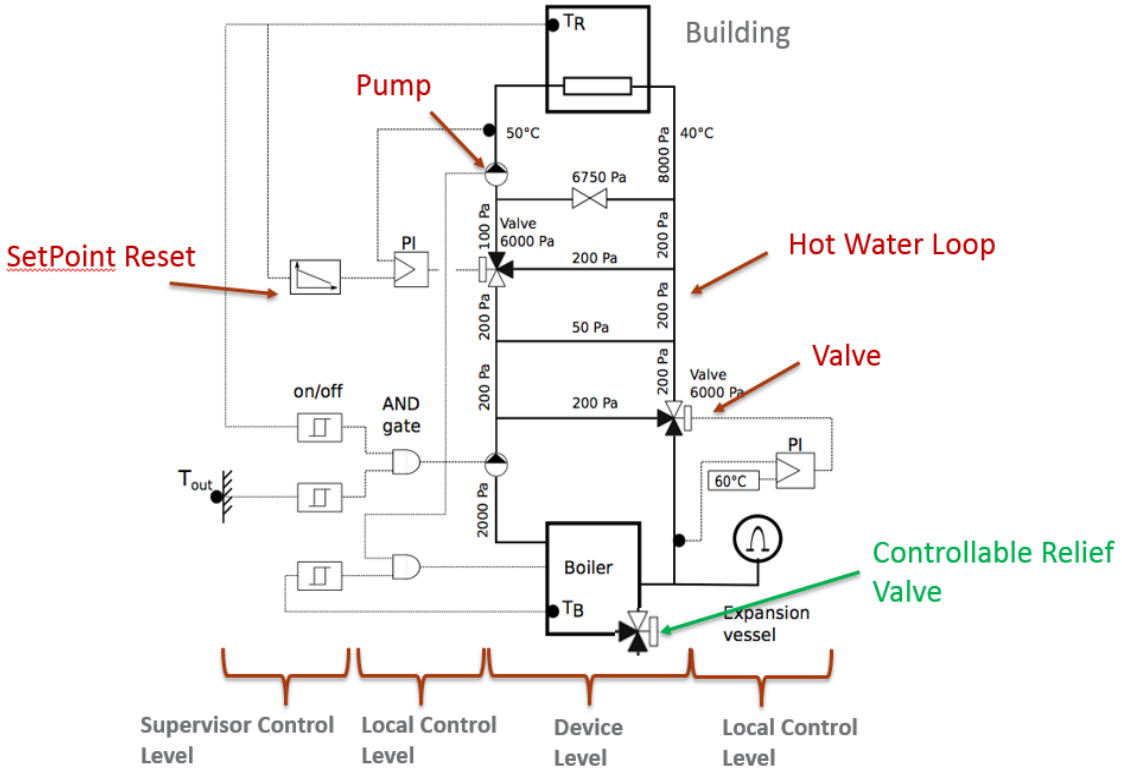


After Decoys Created



Boiler Model Decoy

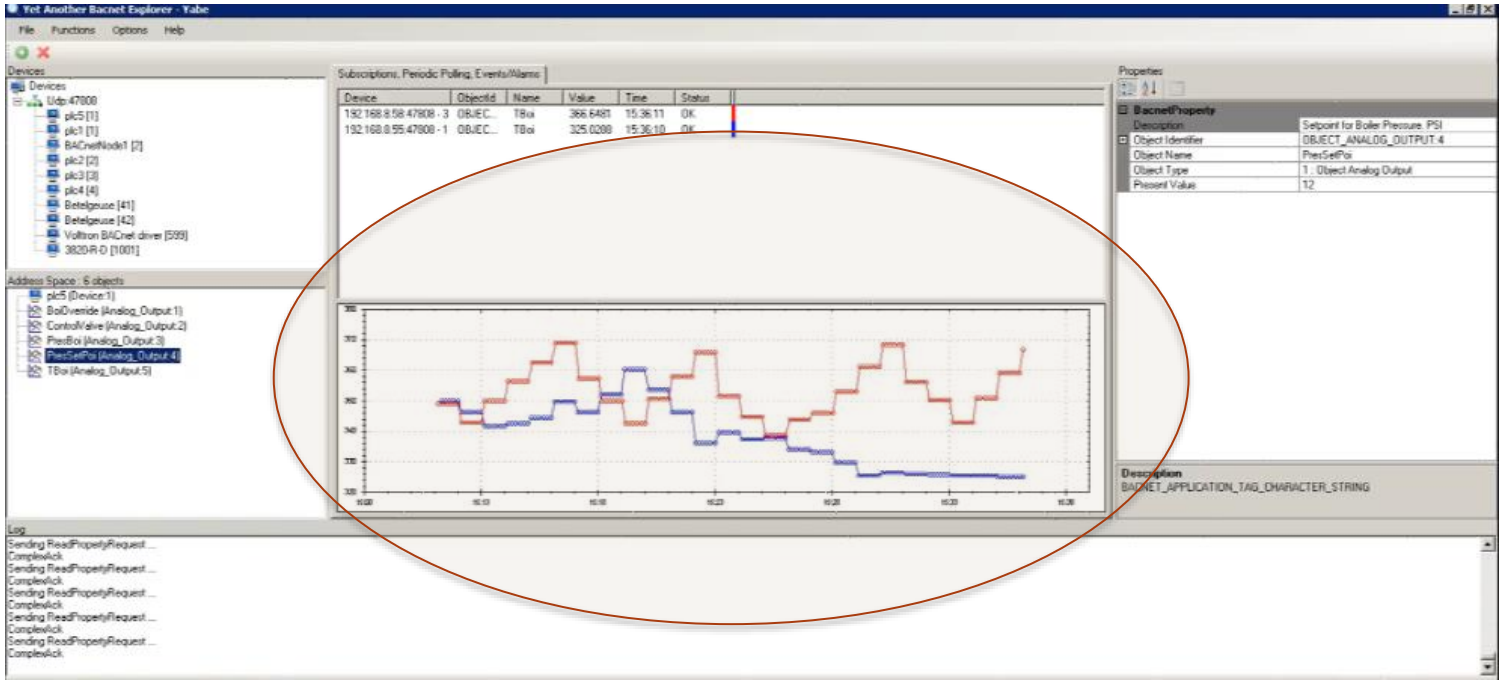




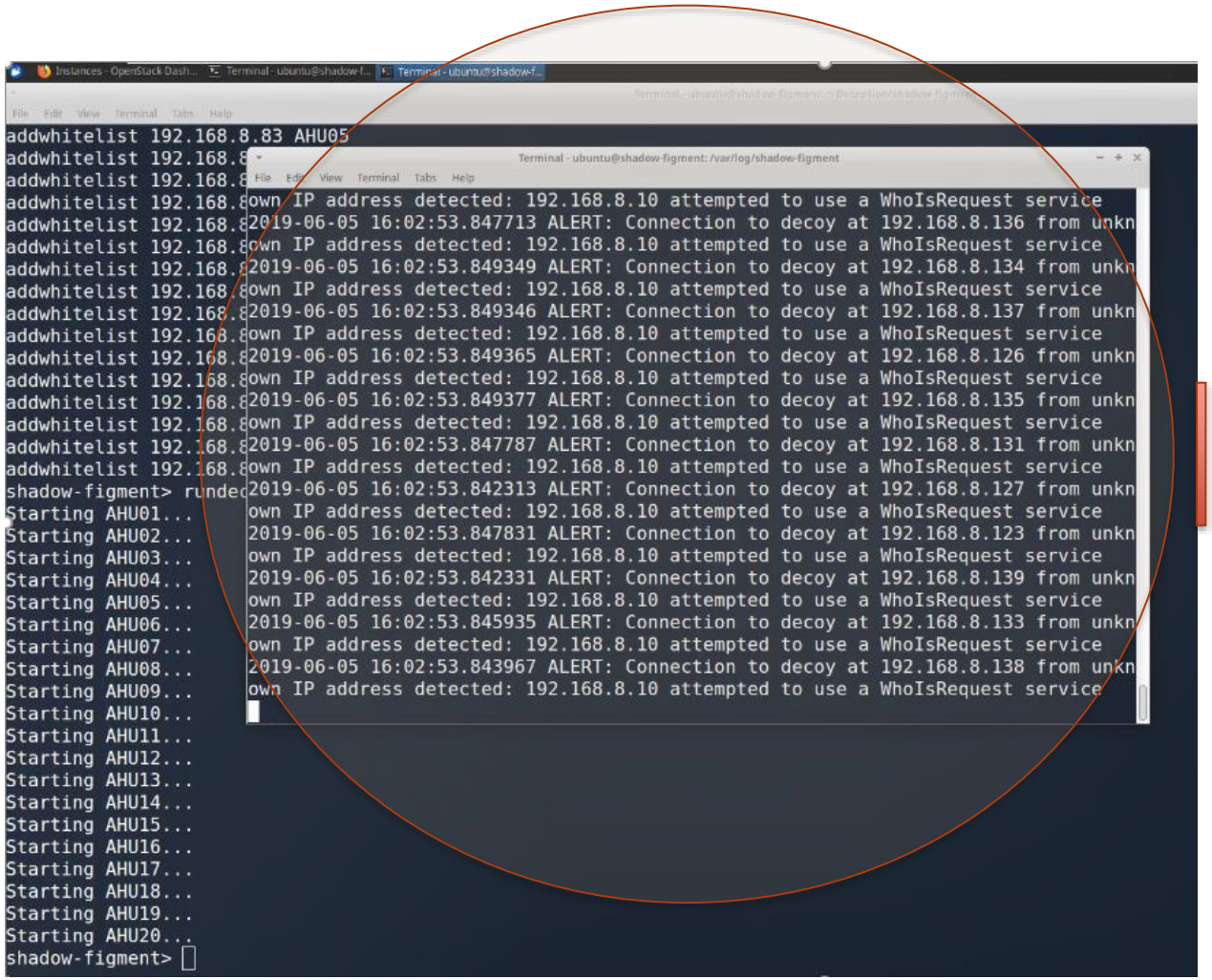
http://simulationresearch.lbl.gov/modelica/

Decoy PLC 5 with Control Valve and ability to override the status of the boiler

Deceiving the Attacker



Alerting the Defender



SIEM/SOAR Platform