A Multi-level Fidelity Microgrid Testbed Model for Cybersecurity Experimentation

Aditya Ashok, Siddharth Sridhar, Tamara Becejac, Theora Rice, Scott Harpool, Matthias Engels, Mark Rice, Thomas Edgar

12th USENIX Workshop on Cyber Security Experimentation and Test (CSET '19)

August 12, 2019

PNNL is operated by Battelle for the U.S. Department of Energy

Introduction

- Cyber attacks on industrial control systems have been increasing in number and sophistication over the last decade.
- Testbeds are extremely essential in providing realistic environments for testing and validating new cybersecurity technologies.
- Self-contained test systems that have cross-domain critical infrastructure elements are ideal candidates for implementation and instantiation on a testbed.
- A campus microgrid provides cross-domain opportunities (electrical, buildings, cyber, water, etc.,) while also being self-contained with a single authority of control.
- This allows us to instantiate all the associated elements at a high-level of fidelity to allow realistic cybersecurity experimentation.

Proactive Adaptive Cybersecurity Framework for Control Systems (PACiFiC) Initiative

Problem

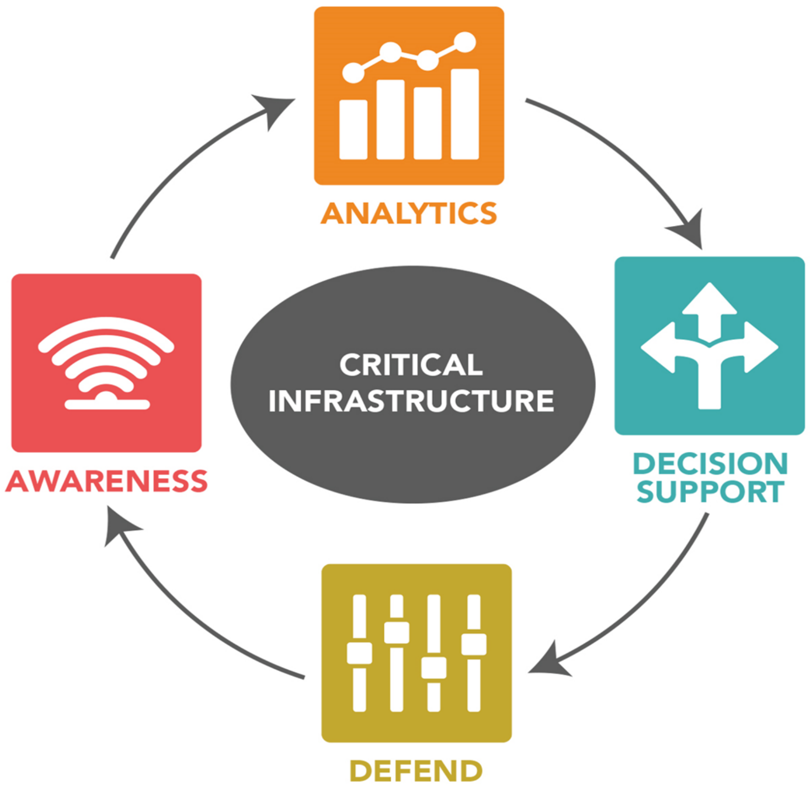
- **Operational technology** (OT) [control systems & their environment] **are in use** in our high consequence infrastructures.
- Current OT is **insecure, out of date, static, and targeted** by our adversaries.

Approach

- Define **secure design and development principles** that apply to **all OT** systems.
- Develop and test **adaptive cyber defenses** holistically.
- Include **human, cyber, communications, and process physics**.

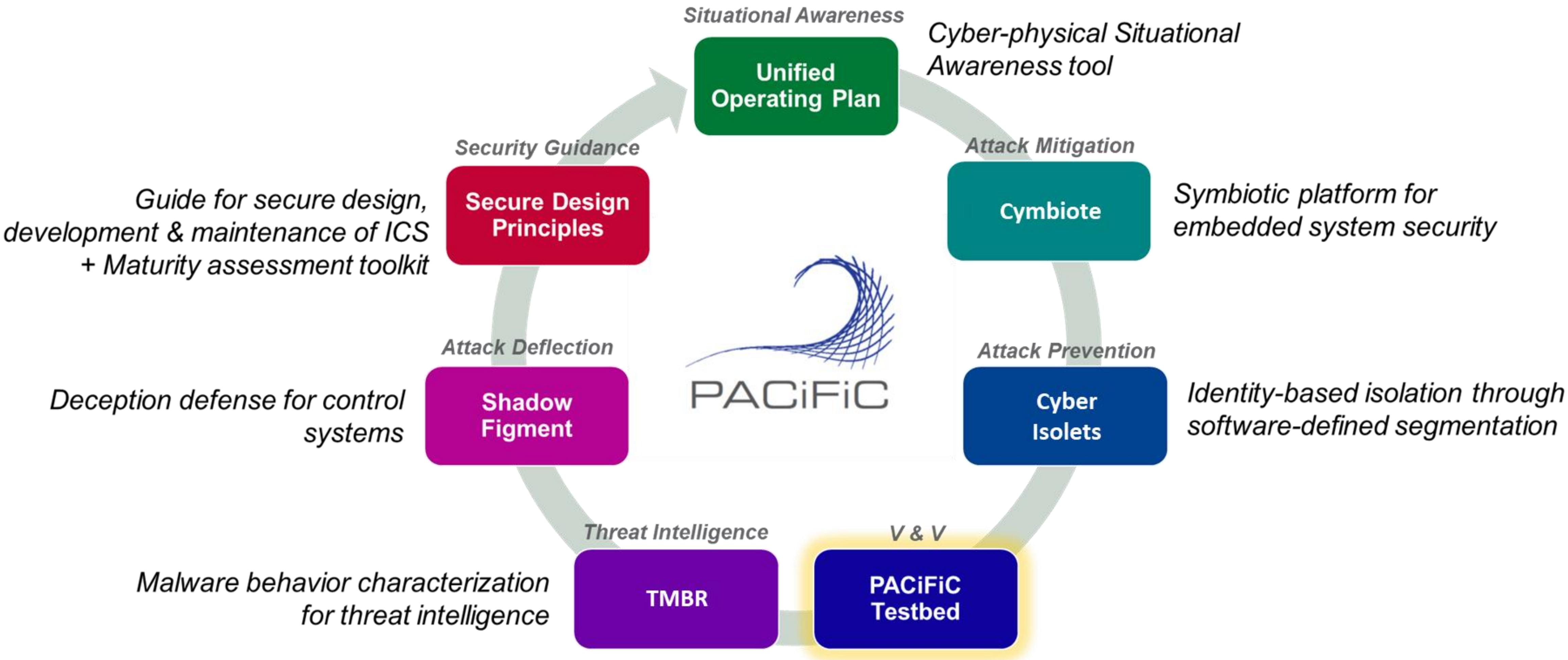
Impact

- Measurably **more secure, reliable, robust, and resilient** control systems while retaining the same level of performance.
- Enhanced capability in **measuring, testing, and demonstrating** OT cyber security.



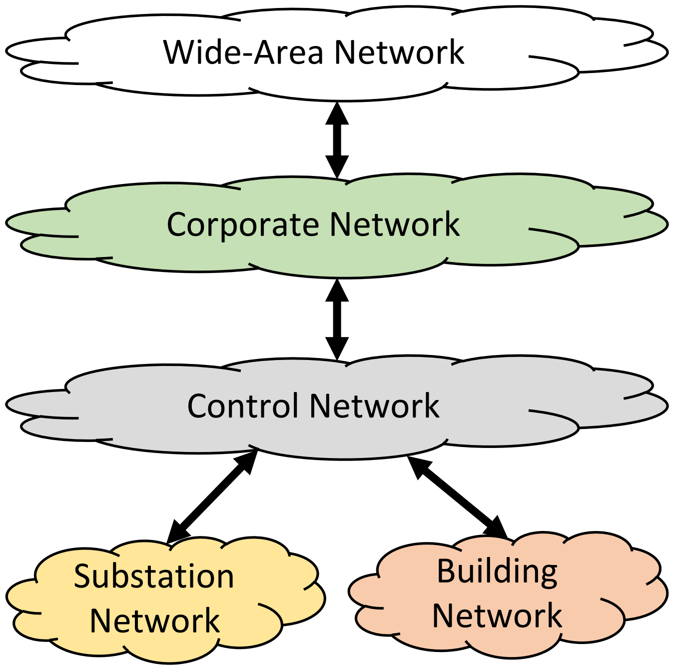
Pacific Northwest
NATIONAL LABORATORY

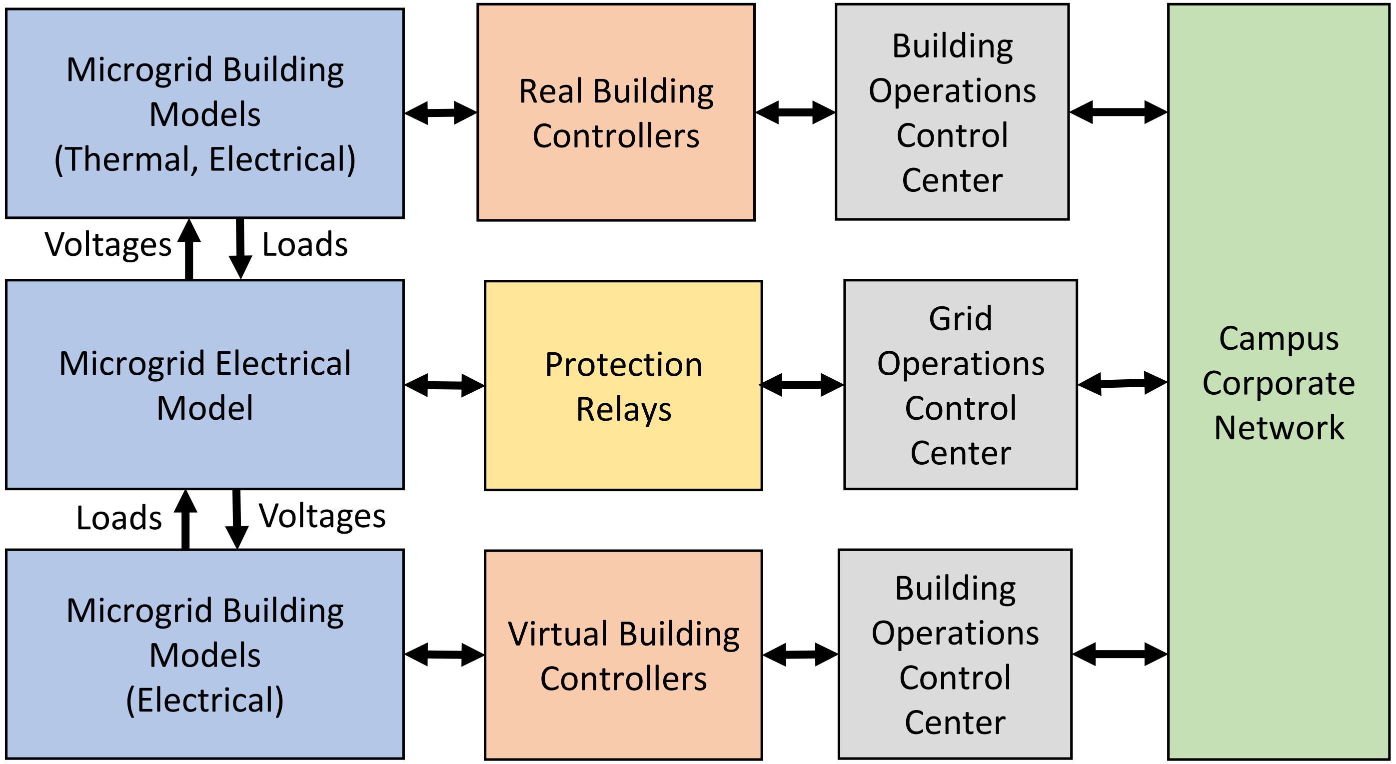
Select PACiFiC Initiative Projects



A Campus Microgrid Model for Cybersecurity Experimentation

Conceptual Cyber-Physical Model





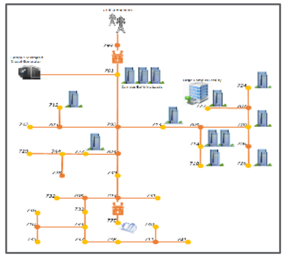
PACiFiC – Microgrid Testbed

Objective: Enable research, testing, and validation of proactive, cyber attack prevention, detection, and mitigation strategies developed for grid and building critical infrastructure domains as a part of the PACiFiC initiative.

Simulation Environment

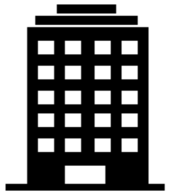
High-fidelity Commercial Building in Dymola

VOLTTRON & FNCS



Micro-grid model in OPAL-RT

FNCS



Low-fidelity residential Buildings in GridLAB-D

Domains

- Grid
- Buildings
- Process control

Simulators & Tools

- OPAL-RT
- Dymola
- GridLAB-D
- VOLTTRON
- FNCS

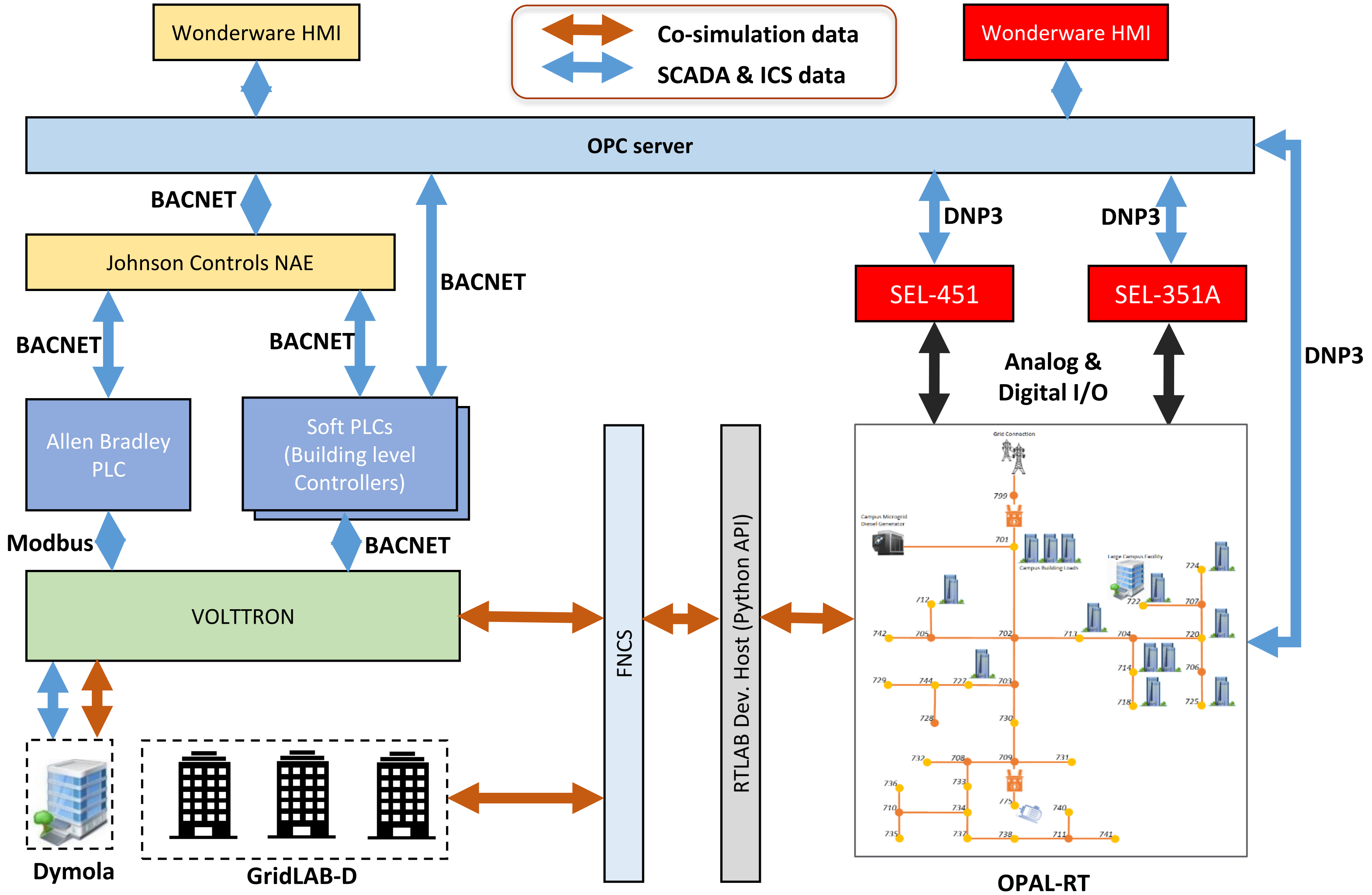
Hardware & Software

- SEL 351A & 451
- Kepware OPC server
- Allen Bradley Control Logix PLC
- Johnson Controls Network Automation Engine
- Wonderware Visualization

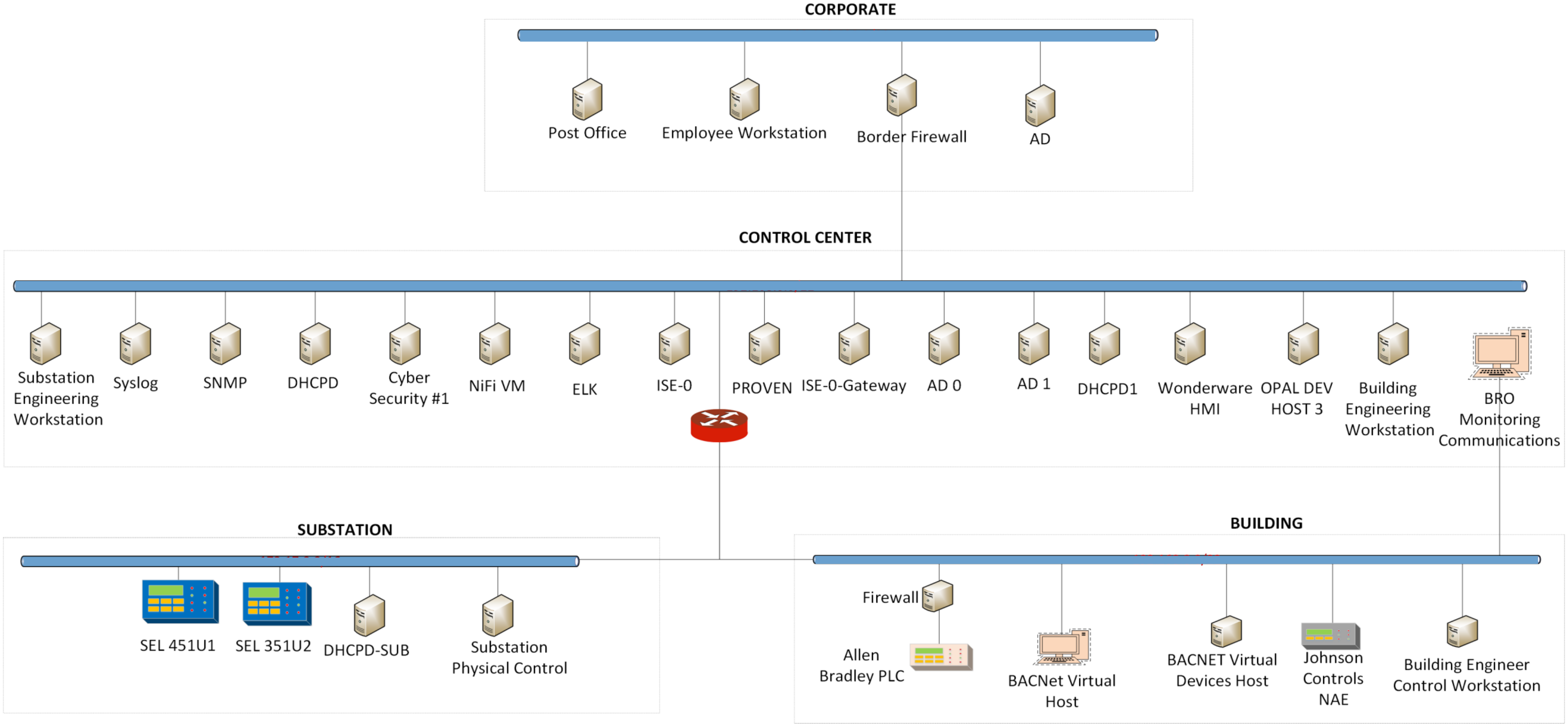
Protocols

- DNP3
- Modbus
- BACNET

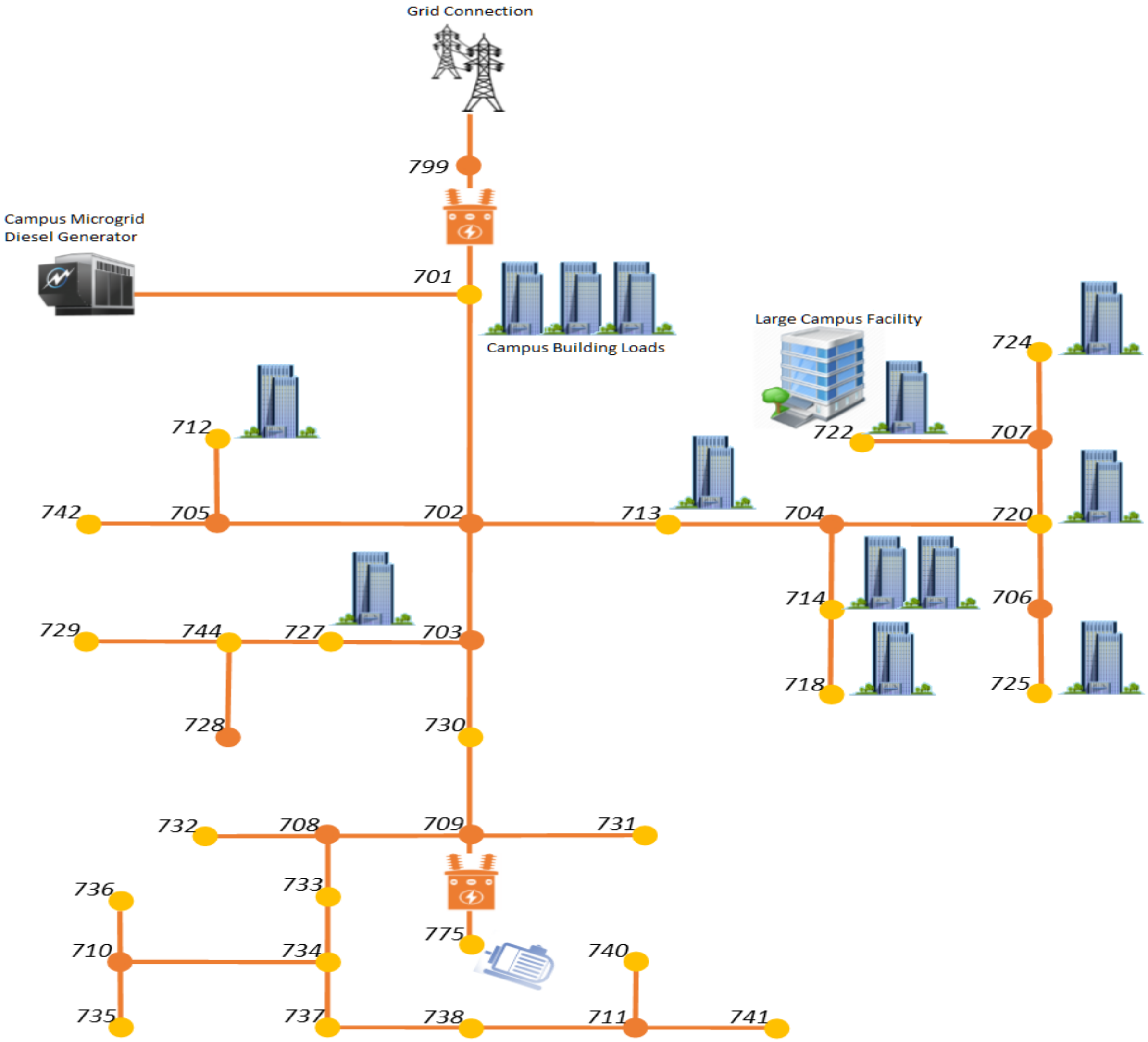
PACiFiC Testbed – Architecture (Physical)



PACiFiC Testbed – Architecture (Cyber)



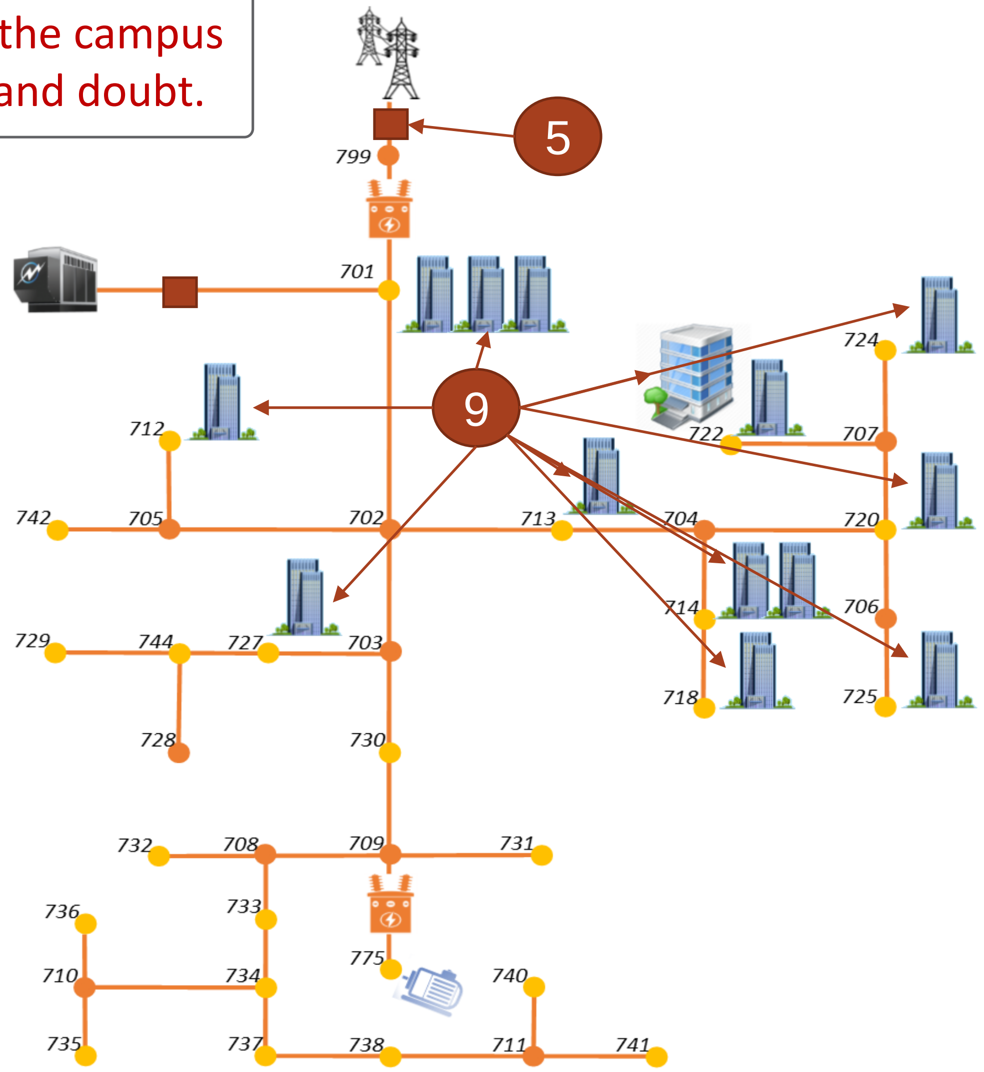
Microgrid Model (modified IEEE 37 node feeder)



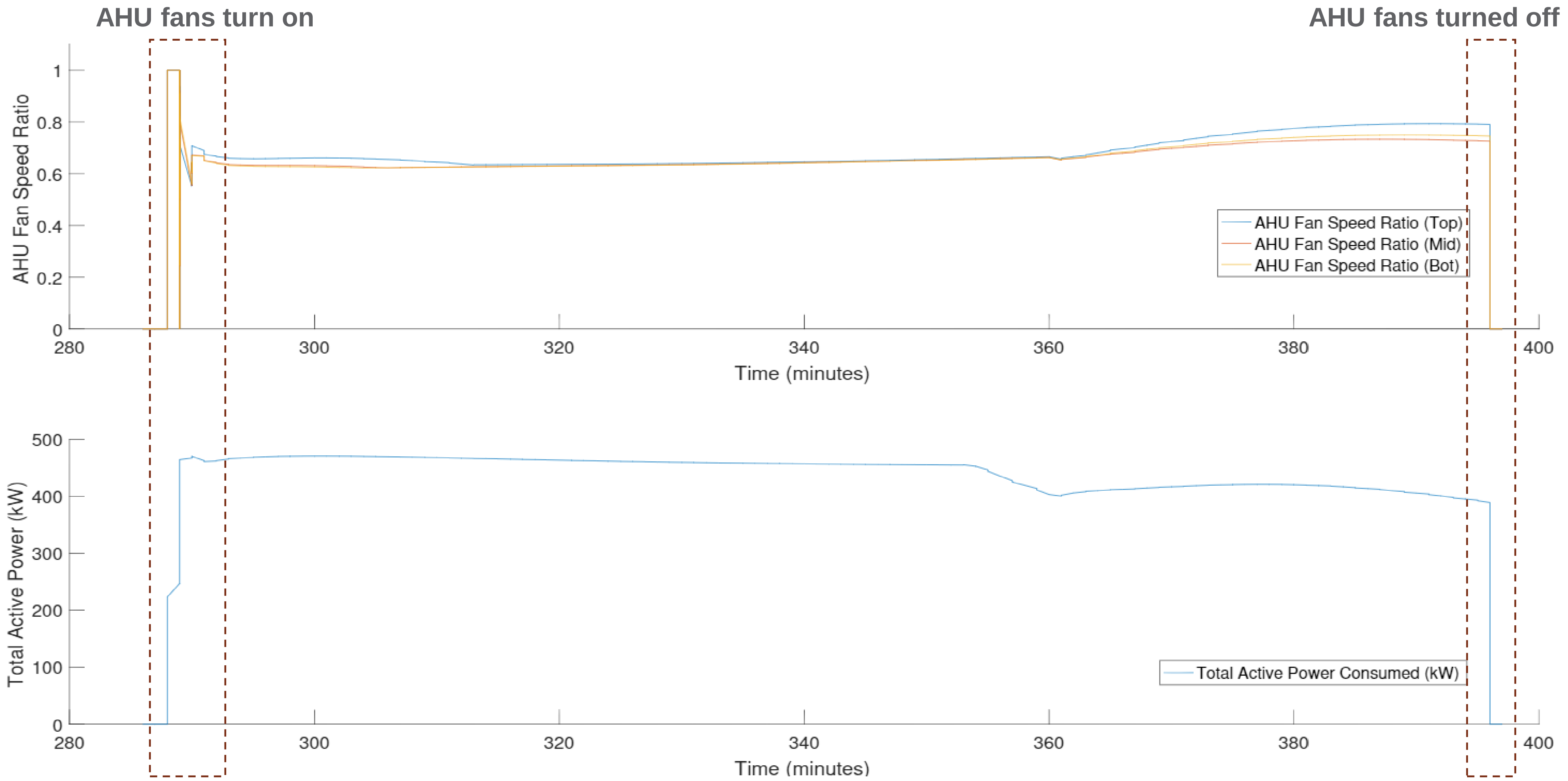
Demo Use Case – Cyber Attack Scenario

Attacker Objective: To disrupt operations at critical facilities of the campus by causing a blackout in the microgrid; cause fear, uncertainty, and doubt.

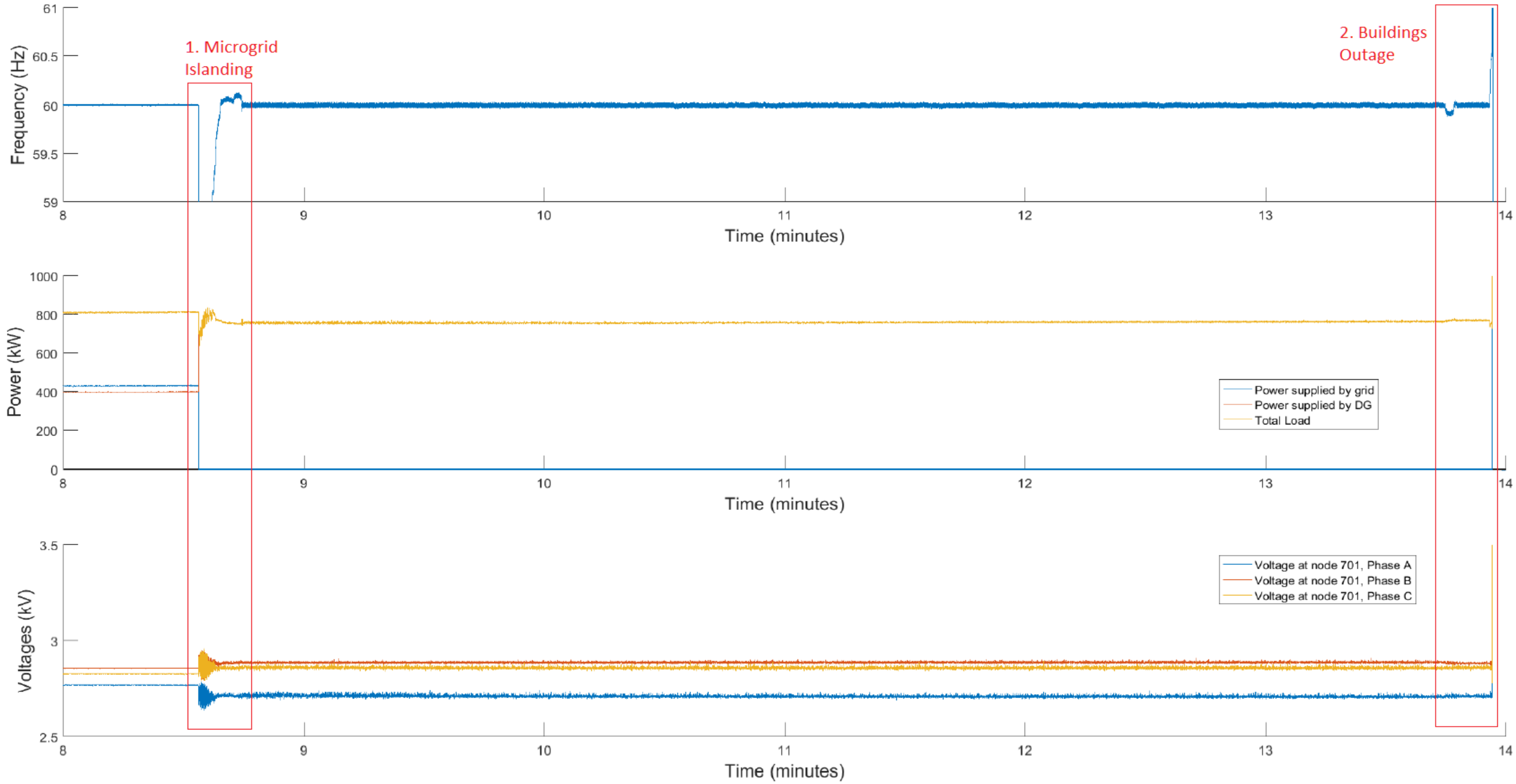
1. Phishing Attack to compromise corporate workstation
2. Credentials Theft to connect to OT network
3. Pivot to Grid OT via VPN from corporate network
4. Craft Payload to change protective relay settings
5. Execute Attack stage 1 – Microgrid Islanding
6. Pivot to Building OT via VPN from corporate network
7. Perform reconnaissance on Building network
8. Prepare for Attack stage 2 – Turn off all AHU fans
9. Execute Attack stage 2 to cause microgrid blackout



Demo Use Case – Results (Building Simulation)



Demo Use Case – Results (Microgrid Simulation)



Conclusion

- Developing a scalable, high-fidelity, and realistic testbed is extremely valuable to test and evaluate cybersecurity research.
- A microgrid model serves as an ideal candidate use case that can be instantiated with a high-fidelity preserving cross-domain interactions (electrical, building, cyber) while being self-contained.
- We presented our testbed's capability to instantiate a campus microgrid model for supporting cybersecurity testing and experimentation.
- We also presented an exemplar multistage cyber attack case study to demonstrate and showcase the testbed's value and capability.

Pacific Northwest
NATIONAL LABORATORY

Thank you

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*

Aditya Ashok
Engineer
ELECTRICITY INFRASTRUCTURE

Phone: (509) 372-4792
Mobile: (515) 509-7636
aditya.ashok@pnnl.gov

902 Battelle Boulevard
P.O. Box 999, MSIN J4-90
Richland, WA 99352
www.pnnl.gov