Pacific Northwest
NATIONAL LABORATORY

PNNL- 35048

Cyber Physical Subsystems under Adverse Conditions

September 2023

Theora Rice
Matt Kirkland
Cimone Wright-Hamor
Gustavo Gloria
Jennifer Appiah-Kubi

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from
the Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

PNNL- 35048

Cyber Physical Subsystems under Adverse Conditions

September 2023

Theora Rice
Matt Kirkland
Cimone Wright-Hamor
Gustavo Gloria
Jennifer Appiah-Kubi

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Abstract

The United States power grid is built upon complex cyber-physical systems (CPS), including many distributed energy resources (DERs) and microgrid structures. Due to cross-disciplinary domains that govern the interplay between cyber and physical technologies that sustain DERs, it is difficult to confidently predict how these systems will react under adverse conditions such as faults and cyberattacks. This project utilized power hardware-in-the-loop (PHiL) to gain system behavior knowledge and robust understanding through experimentation and observational science. It also produced a large volume of datasets to feed into other efforts to advance high-fidelity model simulations and to support the design of novel control approaches.

Summary

The Resilience through Data-driven, intelligently Designed Control (RD2C) initiative is beginning the exploration of resilience in CPS by evaluating microgrids with power electronics, as well as the effect of Distributed Energy Resources (DERs.) A key component of these explorations is to conduct research in high-fidelity systems that are representative of real-world behavior. Not only in steady state behavior, but also representative of systems during and after adverse conditions.

In order to understand how real-world subsystems behave in these adverse events, the Cyber Physical Subsystems under Adverse Conditions project was created. The approach the project takes is to conduct experiments within physical hardware subsystems to capture and characterize underlying features in adverse conditions. To do this, the team developed an evolving experimental methodology to ensure a repeatable, scientific approach to collecting data from the subsystem under study. Additionally, through these experiments the team generated a large number of datasets that can be used to better inform high-fidelity modeling efforts, as well as efforts to create new resilient control algorithms.

The subsystem under study in this project was a building control system. Commercial buildings are becoming more flexible and their models more complex, making the introduction of building control systems (BCS), and addition of the complex behavior loads [such as Variable Frequency Drives (VFDs)] more impactful upon microgrid dynamics. Thus, having an accurate model representation is mandatory for any microgrid system studies. Since heating, ventilation, and air conditioning (HVAC) systems alone consume around 44% of the total energy required in commercial buildings (Brian K. Paul 2019), their characterization and control are a high priority.

This report outlines how the experimental methodology was applied and evolved throughout the building control system trials. It also highlights specific interesting results, which predominantly involve the documentation of additional power draw in a system commanded to service two opposing extreme temperatures, and unpredictable transient power draw in devices after sudden voltage manipulation. The team concludes with a discussion of future trials that could be conducted in alternate subsystems, as well as additional threat scenarios worth future experimentation.

Acknowledgments

This research was supported by the **National Security Mission Seed**, under the Laboratory Directed Research and Development (LDRD) Program at Pacific Northwest National Laboratory (PNNL). PNNL is a multi-program national laboratory operated for the U.S. Department of Energy (DOE) by Battelle Memorial Institute under Contract No. DE-AC05-76RL01830.

Acronyms and Abbreviations

AHU	Air handling unit
BCS	Building control system
CCT	Controller configuration tool
CPS	Cyber Physical System
DER	Distributed energy resource
DG	Distributed generation
FEC	Field equipment controller
PHiL	Power Hardware-in-the-loop
HVAC	Heating, ventilation, and air conditioning
ICS	Industrial control system
IOM	Input/Output module
IOT	Internet of Things
NERC	North American Electric Reliability Corporation
PNNL	Pacific Northwest National Laboratory
RD2C	Resilience through Data-driven intelligently Designed Control
SA	Sensor actuator
SEB	Systems Engineering Building
SME	Subject Matter Expert
VAV	Variable air volume
VFD	Variable frequency drive

Contents

Figures

Tables

1.0 Introduction

The Resilience through Data-driven, intelligently Designed Control (RD2C) initiative “seeks to develop resilient and intelligent sensing and adaptive control algorithms through observational understanding and characterization of [cyber physical systems (CPS)] under adverse conditions.” (Pacific Northwest National Laboratory 2020) This initiative has been segmented into two thrusts: **Cyber-Physical Systems Observational Science** and **Designing Resilience for Sensing and Control**. The first of these thrusts is tasked with the study of CPS behavior, and developing a high-fidelity testing environment based upon the results of those studies. Thrust two has been tasked with exploring novel adaptive control algorithms for CPS resilience, and utilizing the thrust one testbed to refine their findings.

Under thrust one, the “**Cyber-Physical Subsystem Studies under Adverse Conditions**” project was tasked to gain better understanding of the system level behavior of critical infrastructure under adverse conditions. To do this, the team researched, developed and executed testing methodology for conducting power-hardware-in-the-loop (PHiL) experiments to gather high-fidelity data that can be used to characterize the behavior of CPS subsystems. The results of this project will feed into the foundations of high-fidelity modeling, and informing studies into CPS resilience.

1.1 Objectives

The goal of this project is to gain better understanding of system level behavior of DERs and microgrid subsystems under adverse conditions. To do this, the team set the primary objective to explore experimental methodology to capture and characterize underlying features (i.e., resilience and security properties) as well as emergent and ensemble behaviors of how cyber-physical systems behave in abnormal or failure conditions.

A secondary aim of this project has been to generate datasets from these PHiL experiments. Well documented datasets taken from a real-world system experiencing adverse conditions can be used to inform models and the design of adaptive control approaches. Cyber-physical modeling and simulation can increase fidelity by having realistic incident information inform how component subsystems of a larger-scale model react in a given situation. By having data from these subsystems to study, adaptive control approaches can be developed from a data-driven perspective, with knowledge of real-world system behavior giving a benchmark to improve upon.

2.0 Methodology

To study how critical infrastructure subsystems react in adverse conditions, the project team utilized scientific methodology to define hypothesis driven experiments that would be executed in a subsystem trial. This was chosen because it defines a method of experimentation revolving around well-documented, repeatable tests. These experiments were based around the study of system behavior when faced with energy disturbances and cyberattacks. A description of the development process is provided within this section, with an example trial provided in Section 3.

2.1 Research Questions and Hypothesis

To develop hypotheses, the team would first deliberate on research questions about subsystem behavior. For instance, how would a given subsystem behave if a main control component was under a denial of service cyberattack, and was unable to keep up with regular communications? When these research questions were settled on, the team would reach out to advising subsystem subject matter experts (SME) at the lab to narrow down what research questions would likely produce the most interesting results.

Once these research questions were chosen, the team used them to develop an experimental scenario that could be run to answer the question. Then, a hypothesis was created to posit the expected behavior of the subsystem within that experiment. The team was then able to use this experimental scenario to build the testing environment, and the hypothesis to identify the variables that needed to be measured to answer the question.

2.2 Experimental Environment

To build the testing environment, the team sought to model component and subsystem infrastructure with physical hardware, while examining larger-scale system-wide effects with simulation. This was done by heavily leveraging the PNNL powerNET testbed for its simulation capabilities with the OpalRT, and by seeking federation with other CPS hardware at the lab and external to the lab. The OpalRT technology is being used for the high-fidelity co-simulation testbed work in thrust one of the RD2C initiative, and thus allowed the team to leverage that work by inserting the subsystem under test as a load within the larger model. By doing this, the team was able to see the effect on the wider grid of the subsystem-directed experiments.

The PHiL subsystems were chosen and augmented to be representative of their real-world counterparts. The project initially began with the desire to answer research questions in the systems listed in Table 1. However, due to limitations that will be discussed in section 4, only the Building Control System was accessible for experimentation.

Table 1 - List of Desired Testing Subsystems

Desired Subsystems
Building Control System
Battery Inverter System
Home Automation System
Photovoltaic Inverter System

Electric Vehicle charging System

Wind Turbine System

Once the subsystem environment to test was found, the team readied the testing infrastructure needed to run the experiments. This would include infrastructure needed to allow experimenters to integrate the subsystem with the OpalRT models and other controls for governing energy behavior in the system, as well as devices that could be used to inject cyberattacks.

2.3 Measurement Infrastructure

Once the needed components were gathered for the experimental action to be accomplishable, the team needed to evaluate what data would need to be measured to answer the research question. Partially, this became driven by the hypothesis, which would state the expected outcome of the experiment. From here, the researchers would determine what independent variables would be manipulated by the experiment scenario, and what dependent variables would measure the outcome.

Given the nature of CPS, two types of dependent variables became immediately obvious: physical measurements of the system, and network measurements of system communication. Physical system measurements such as voltage and current allow researchers to see the effect of a given experiment on how much power the subsystem is utilizing. Network measurements allow researchers to see how the virtual aspects of the system are being impacted. Additionally, out-of-band sensors were also added as a category to catch inadvertent data that could indicate a change in system behavior.

2.4 Procedure

With the research questions, experimental environment, and measurement infrastructure in place, the final step was to define the specific test case procedures. To a certain extent, all experimental test cases within the same subsystem shared some procedures, which defined the specific steps needed to ensure appropriate capture or experiment data. These steps would document what time the experiment began, who was present, what actions were needed to begin recording data, and what actions were needed to end the data recording and save it to a secure location.

Procedures specific to the individual experiments were created to ensure the repeatability of the experimental action. By outlining specific commands and actions to take, and in what order, the team ensured that the experiment could be repeated with little variation. This means that the data could, ostensibly, be verified by another team utilizing the same experimental setup and actions. It also means that the experimental actions are documented, so that future researchers looking at the datasets can compare the activities with the datasets, and establish a shared timeline.

2.5 Analysis

Once the experiments were complete, analysis was done upon the resultant datasets. In the case of physical dependent variables such as voltage, the raw data collected was evaluated for unusual events. When detected, they were compared to the experimental action timeline, and correlated when appropriate. For virtual variables, analysis was done via scripting and software to determine any unusual artifacts. These were then written up, and documented along with their datasets.

3.0 Trial 1 and 2 – Building Control Systems

The introduction of building control systems (BCS) and complex behavior loads [such as Variable Frequency Drives (VFDs)] have increased the flexibility and complexity of the commercial building space. A direct result is the increase in accompanying model complexity, thus having an accurate model representation is mandatory for any microgrid system studies. Since heating, ventilation, and air conditioning (HVAC) systems alone consume around 44% of the total energy required in commercial buildings (Brian K. Paul 2019), their characterization and control are a high priority. Through well designed control systems, buildings can help in achieving the smart-resilient microgrid. Thus, their behavior under adverse conditions needs to be studied and properly modeled to be able to design the right control system (both on the local as well as system level).

This section is only an overview of Trial 1 and 2. More detailed information as to experimental design and environment structure is in trial testing documentation. This is available upon request.

3.1 Research Questions and Hypothesis

First, the team evaluated the research questions involving BCS in adverse conditions. The first trial focused on cybersecurity questions, to accommodate for initial limitations in power control. The second, focused on adverse power behavior.

3.1.1 Trial 1

The first trial comprises the most varied of the trial tests and broadly covered scenarios that could be caused by cyber adversaries. The research questions covered were:

1. Can aggressive network communications introduced by a third-party device influence the behavior of the system?

2. Can repetitively power cycling a device that consumes a large amount of power on start-up cause the system behavior to vary?

3. Is there any difference in system behavior if set points are managed remotely vs. locally?

4. Is system behavior deterministic upon startup?

5. If two dipartite temperature zones are set (i.e., one high temperature zone, one low temperature zone) in the geographically close spaces, will the system consume more energy?

These evolved into the hypothesis in Table 2.

Table 2 - Trial 1 Hypotheses

Hypothesis
Unusual network traffic on Ethernet-connected BAS devices will cause degradation of services, and/or cause other unwanted behavior in the probed device.
Keeping the system device in a continuous start-up process will cause built in system protection to activate and/or breakers to trip.
Remotely accessing and operating the system will have a different effect on the timing and communications of a system than local operation.
When the 3820 Annex is powered back on from an outage state, its startup behavior will be measurable, repeatable, and have an identifiable pattern.
Power draw due to different goal temperature set points will trip a breaker.

3.1.2 Trial 2

The second trial comprises tests that put the system in adverse power events. The research questions posed included:

1. In normal conditions, does the annex behave predictably?
2. Will varying the voltage change system behavior?
3. Will varying the frequency change system behavior?
4. Will causing a fault in the grid system change system behavior?

These evolved to the hypothesis in Table 3.

Table 3 - Trial 2 Hypothesis

Hypothesis
The 3820 Annex system will have a stable, repeatable pattern with minimal changes in any dependent variables.
When the voltage that supplies 3820 Annex is set off-nominal, the entire system and/or some components might exhibit unexpected behavior (e.g., reduced efficiency).
When the frequency range of the 3820 Annex is set off-nominal, the entire system and/or some of its components might exhibit unexpected behavior (e.g., reduced efficiency).
A sum of off nominal conditions, in this case a fault within the grid simulation, will cause the system components to exhibit unusual behavior.

3.2 Experimental Environment

To conduct experiments to answer the proposed research questions, the team required access to a building control system, as well as the capability to inject adverse cyber and power conditions.

3.2.1 The Systems Engineering Building Annex - Building Controls and Diagnostics Laboratory (SEB Annex)

To study BCS, the team utilized the SEB Annex, a PNNL resource for studying BCS devices and controls for proceeding experiments. It simulates an actual commercial building and loading regardless of the current weather or ambient conditions[1]. The building is subdivided into 4 rooms, of which can be individually temperature controlled. It should be noted that only 3 rooms are usable for experimentation, as one is utilized as a mechanical room. A diagram of the building is shown in Figure 3-1.

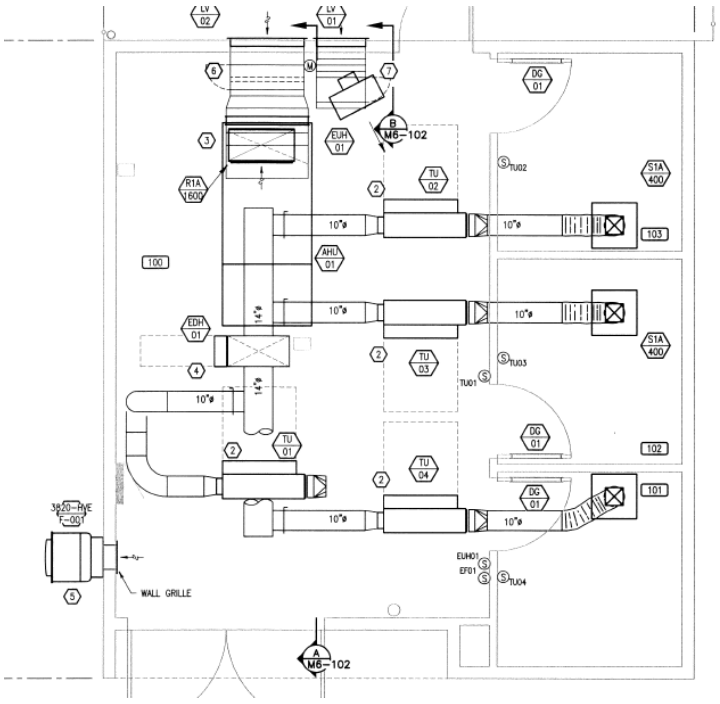

Figure 3-1 - SEB Annex Ductwork Diagram

The Annex HVAC system is comprised of the following components:

- The chilled water plant and its pump
- AHU system (including two VFDs)
- 4-zone VAV with 5kW reheater coils
- Temperature sensors (located in each room)

[1] System cannot simulate higher outside temperatures than the actual.

- Two air flow stations
- 208VAC Energy meters (one for the chiller and one for the rest of the system)
- The Johnson Controls NAE45 (Johnson Controls n.d.) – Serves as the main controller and connects the above items over RS485 (BACnet comms utilized)

3.2.2 The Experiment Infrastructure

The Annex system is designed as a representation of a commercial BCS. However, it was not designed to allow for controlling power to the building, and there were not workstations set up to provide the capability to inject adverse cyber events. Thus, modifications were made to the Annex to support the injection and control of the independent variables related to these fields in the experiments.

For Trial 1, the team introduced an adversary laptop to inject the cyber events outlined within the experimental scenarios. This was an HP laptop running Windows 10, with the capability to run basic cyber tools and commands. During testing, it was networked to have a direct connection to then Johnson NAE, which was the only ethernet-capable device within the Annex infrastructure.

To control power to the annex, this project procured and installed a Regatron TC.ACS System. This is a programmable, fully digital, 4 quadrant 3-phase 50kVA AC power amplifier. Each unit represents a three-in one configuration. The Regatron is utilized to provide variable power to the Annex. It also provides the following functionality:

1. 3-phase grid simulation
2. Built in 3-phase amplifier
3. Programmable RCL-load mode

Using these components, the team could execute the experimental test cases.

3.3 Measurement Infrastructure

To determine what data needed to be recorded to answer the research questions, the team evaluated the system and the hypothesis. Ultimately, for all tests in both Trial 1 and Trial 2 the following dependent variables were recorded:

- Voltage
- Current
- Network Communications
- Device “On” or “Off” behavior
- Audio

These were chosen because they encompass the data that defines the physical and virtual behavior of the system. To measure these dependent variables, the team introduced the following equipment into the experimental infrastructure:

- **Yokogawa DL950** (Yokogawa n.d.)**:** An analog data recorder that functions as a multi-channel oscilloscope and portable data acquisition recorder. It captures and records

both high-speed transients and long-run trends, making it ideal for recording electrical conditions during testing in the Annex.

The Yokogawa probes are connected and measuring the following items:

- VAV #1
- Chiller VFD (F Drive)
- System Voltage
- ABB VFD

- **SerialTAP** (PNNL 2022): A tool developed by PNNL that offers passive, fail-safe collection of serial bus communication (RS-232/485) to generate traditional style network captures. A single SerialTAP was installed on each of the RS-485 communication lines found in the Annex (see Figure 3-2). This traffic was then forwarded to a testing laptop used for data collection. For physical location within the annex, please refer to Figure 3-3.

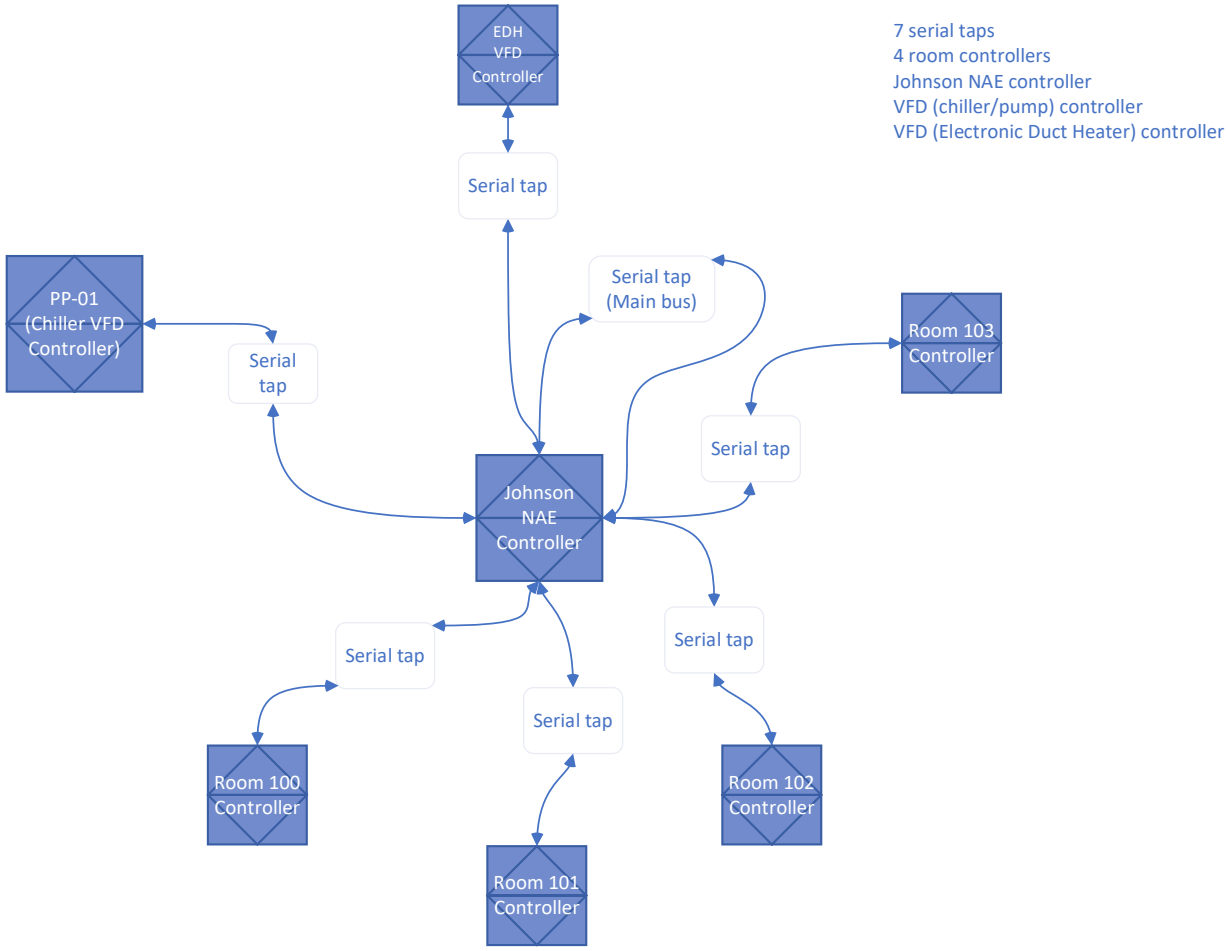

Figure 3-2: SerialTAP Installation locations

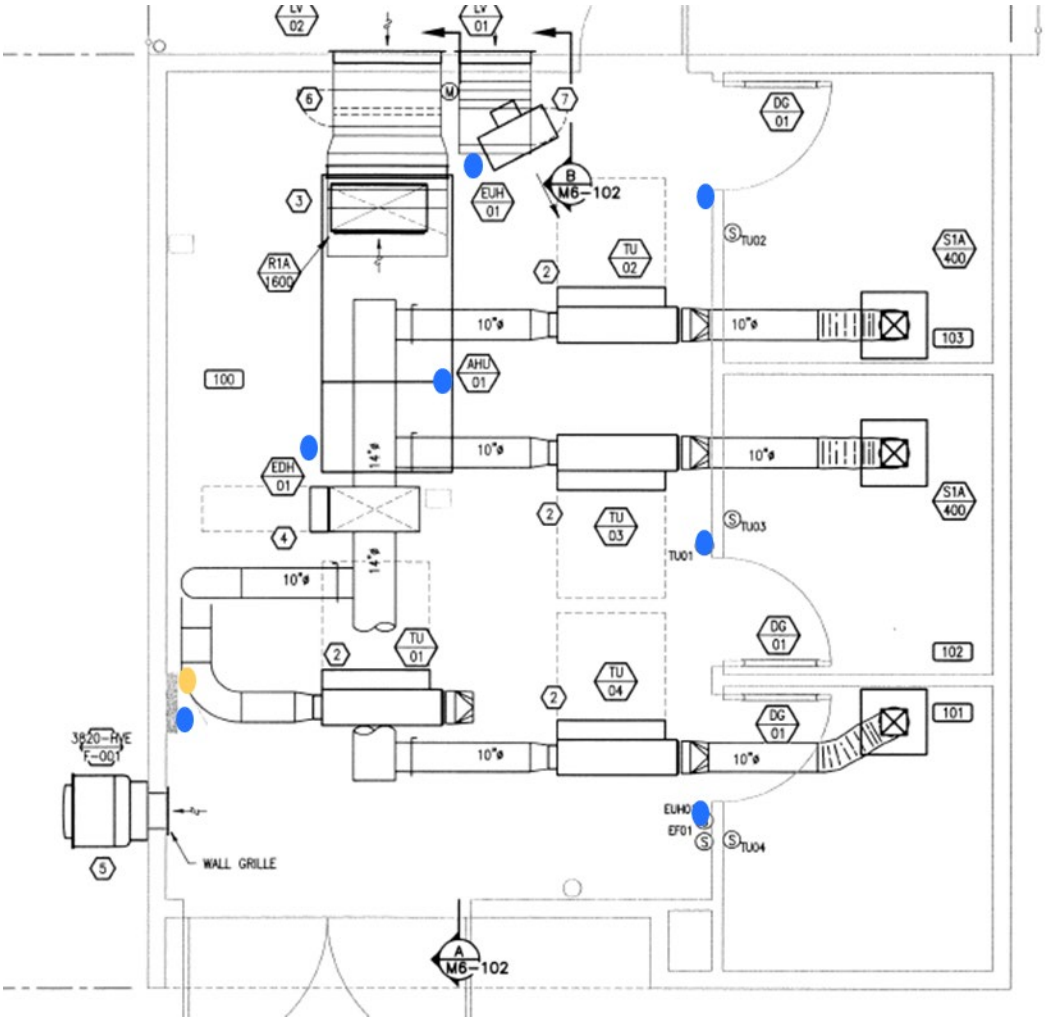

Figure 3-3: Physical layout inside the Annex (*Blue dots = SerialTAPs)

- **Yeti Blue Microphone:** At the suggestion of the SEB Annex cognizant space manager and a building controls subject matter expert, a microphone was installed in the center of the Annex. The building control equipment makes noise when working and depending on the system schedule will clatter at regular intervals. The team determined that an audio recording of the experiments would be valuable to collect, both to analyze for any environment noises, and to maintain a record of the experiment itself.

- **Testing Laptops:** Two laptops were utilized for testing. The first was an HP machine with Ubuntu installed, which collected all SerialTAP data streamed to it. The second laptop was a Dell Windows 7 machine that was used primarily for gathering microphone recordings.

- **APC Pro 1500 S UPS:** A uninterrupted power supply was installed in the Annex to provide consistent, clean power to the testing equipment in the Annex. This is essential, given that the team did not want testing infrastructure affected by any testing activities involving adverse power conditions.

For a complete diagram of the measurement infrastructure network, see Figure 3-4.

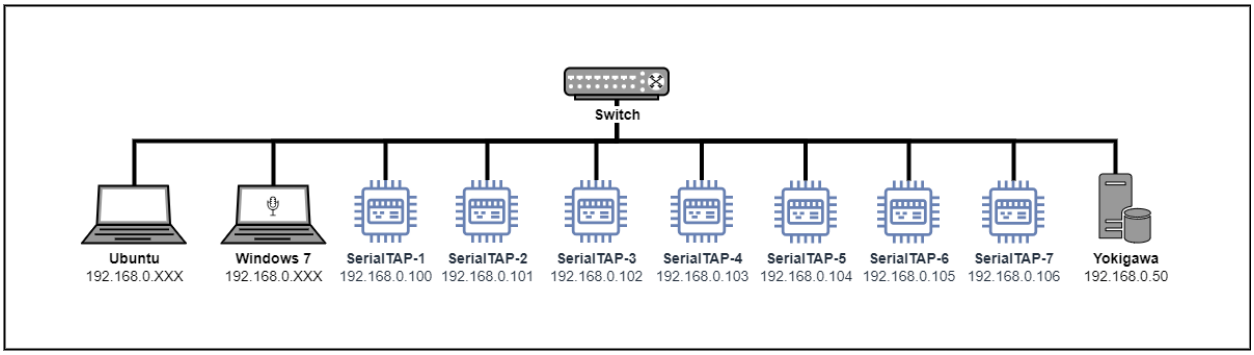

Figure 3-4: Testing Infrastructure Network Diagram

3.4 Procedure

As stated in the methodology, a procedure was developed to execute experiments to answer the given hypothesis. Sometimes, multiple test cases were needed per experiment to evaluate different variations of independent variable control. For such cases, procedures were developed for each individual case, though some directions were overarching. The complete list of test cases for Trial 1 and Trial 2 are available upon request.

For an example research procedure document, please refer to Appendix A.

3.5 Analysis

In all experimental test cases, the equipment in the SEB Annex behaved close to normal. However, one test case from Trial 1, and three test cases from Trial 2 produced some interesting results. For a summary of experimental results from Trial 1 and 2, please refer to Appendix B.

3.5.1 Trial 1, Test Case 5A

In Trial 1, Test Case 5A involved setting two rooms located directly beside each other to two opposing extreme temperatures. The first room was set to 65 degrees Fahrenheit, and the second to 85 degrees Fahrenheit. The results illustrated in Figure 4-1 show that system power increases as it struggles to reach an unattainable temperature.

Figure 4-5 - Trial 1, Test Case 5A VAV3 kWH System

3.5.2 Trial 2, Test Case 2 and 4

Some of the most impactful of the tests were Test Case 2 and 4 in Trial 2, during which the system voltage was abruptly changed, either because of an abrupt increase in voltage (Test Case 2), or because the supply system was turned on after a shutdown (Test Case 4.) These hypotheses are in rows 2 and 4 of Table 3. In these instances, the equipment had high-peaking current transients. For an example of this, see Figure 4-1, which shows the transients exhibited by the AHU variable frequency drive upon system restart due to grid fault.

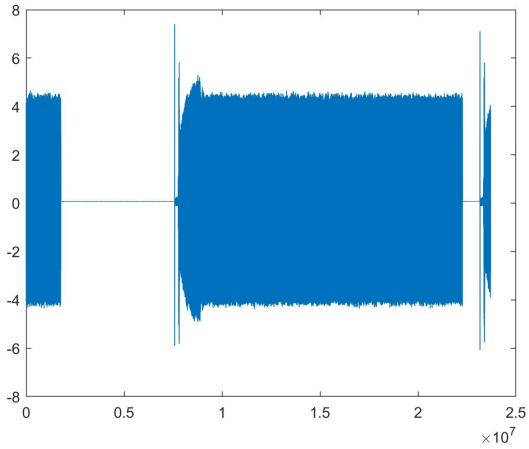

Figure 4-6 - Output current (scaled to voltage) of AHU's VFD during Test Case 4

Of these, the chiller controller was most concerning, with its transients peaking to about twice the normal peak value. In some instances, there were occurrences whose explanation have not been found yet.

3.5.3 Trial 2, Test Case 3

Frequency variations had no exceptional influence on the current waveforms of the equipment. However, they did produce an unexpected result within the testing infrastructure UPS. In Figure 4-3, one can see multiple outlier points of data within the microphone recording. One was determined to be a microphone bump that happened at the end of testing, while shutting down

data. However, the other extremes represent loud sounds that occurred when the UPS tripped due to frequency variation.

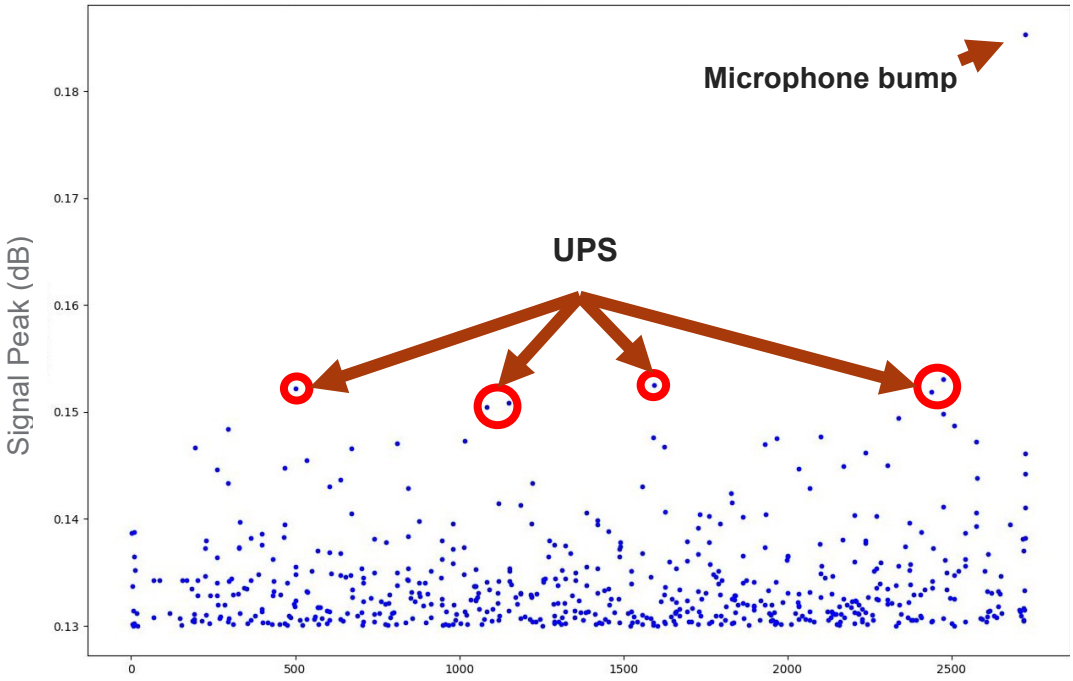

Figure 4-7 - Trial 2, Test Case 3 Microphone Data

Despite running within risk-rated frequency guidelines, the UPS would trigger at the lowest end of the frequency variation tests that the team ran. This caused a shift in testing procedure, as the team would need to conduct the tests in shorter bursts that the UPS could power the infrastructure before. This led to some interesting attack vectors that had not been previously considered, which will be discussed in the conclusion of this report.

4.0 Limitations

Through its lifetime, the project was subject to several limitations that prevented its full execution in all desired subsystem fields. Despite this, the team refined their methodology and skillset in conducting experiments, and created many high-fidelity datasets. The completed experimental documentation and datasets are available upon request.

The Cyber-Physical Subsystems under Adverse conditions project was subject to some limitations regarding access to the physical subsystems needed to conduct our testing. First, was the inherent risk in needing external collaboration needed to conduct tests in photovoltaic inverter systems, electric vehicle charging systems, and wind turbine systems. These are not currently systems that PNNL has invested in, and the project team was unable to locate an external partner with these resources that had similar enough tasking to collaborate with on these experiments.

Of the PNNL-based trials, trials 1 and 2 were conducted and completed. Trial 3 (Home automation internet of things) was unable to be completed due to availability of the chiller within the SEB Annex, and the Regatron.ACS. Trial 4, which involved the Battery Energy Storage System (BESS) was designed, but unable to be accomplished due to the same infrastructure problems involving the Regatron.ACS, and the functioning of the BESS.

Earlier in 2023, the chiller within the SEB Annex experienced a failure unrelated to project testing. This greatly affected our capability to test with the system, as during the summer months the chiller would be the primary acting BCS control. Unfortunately, a replacement for this pump was unable to be procured by the end of this project, and delayed testing within the BCS until temperatures lowered enough to be safe for testing equipment, and to utilize the heating elements.

Concerning the access to the Regatron.ACS and its connection to the BESS, there were infrastructure installation problems due to the COVID-19 epidemic and the resultant worker shortage. The installation was done in stages, which allowed for the initial connection to be made to the SEB Annex. However, after this instantiating the connection to the on-campus BESS system proved a long and arduous process, that ultimately was completed but not fully inspected and approved before the end of this project. Because of the lack of inspection, the in-process trial 3 had to be halted due to lack of equipment availability, as the Regatron.ACS was taken offline to inspect the new connection. Additionally, the project team learned that the BESS control board had failed, and that a new board was on order but unavailable.

5.0 Methodology Iteration

Through the execution of trials 1 and 2, the skillset of the execution team grew, and the experimental methodology evolved. First, and most importantly, the emphasis within the methodology outlined in Section 2 changed between these trials. During Trial 1, emphasis had been put upon experimentation, with analysis slated to happen after all experiments were complete. The result was that errors in the data indicative of measurement sensor fault were only caught after hours of testing had been completed.

This led to a greater emphasis being placed upon evaluating experimental and testing infrastructure prior to experimentation. Validation of the testing infrastructure, with documentation and SME guidance, became a key component of experimental procedure. Additionally, conducting experiment execution and analysis in parallel, using a larger team, allowed us to verify the integrity of the data before moving on to the next test case.

Additionally, as the team became more familiar with the BCS system and the testing infrastructure, scripts were able to be created to execute the tests in a more automated manner. For future experiments, the project team would suggest that adequate time be set aside at the beginning of the experimental methodology for planning, as well as proof-of-concept testing for automation scripting purposes. This would have saved time and effort during the experimental phase, and allowed for more iterations to be completed within the tight timelines.

6.0 Conclusion

Despite setbacks, the Cyber Physical Subsystems under Adverse Conditions project did manage to accomplish its objectives. Though not able to accomplish testing in the variety of subsystems proposed, the team utilized a consistent methodology in trial design, and evolved the methodology to include more refined and rigorous steps throughout execution.

Additionally, many datasets including power readings, network captures, and microphone data have been documented and annotated with experimental descriptions for future use. The results highlighted by these datasets can be used to inform the development of the high-fidelity co-simulation testbed still in use by the RD2C initiative, and to provide example data for control algorithm development.

6.1 Future Work

Concerning future work, Trial 3 and Trial 4 research questions have been developed, and are documented in Appendix C and Appendix D. These could be executed with proper infrastructure support, to provide more datasets to support model and algorithm development.

In light of Trial 1 and 2 results, some follow on experiments have been documented to further explore potentially dangerous attack mechanisms:

1. Sustained abrupt voltage ramp-up: When voltage was changed abruptly, transients lasting about a cycle were observed in the VAV and chiller waveforms. The transients were peaking to about twice the normal peak value. If the system voltage is ramped up in a fast sustained manner (i.e., a ramp-up every cycle or two), it is possible that the current waveform obtained may have an RMS value high enough to trigger protection equipment to disconnect the system.
2. Sustained pulsing of system voltage: When power supply is restored, the AHU draws a higher starting current. It would be interesting to observe how the AHU performs when system voltage is pulsed very fast.
3. UPS usage in data centers: The results from the trial test show that the UPS will trigger in the event of especially low frequencies. It would be an interesting test scenario to take multiple UPS devices, representative of several vendors, and subjecting them to more grid-based experiments. This would explore whether a scenario in which an attacker may be able to trigger a UPS to turn on and drain by manipulating certain aspects of the physical system.

Another accomplishment of this project has been the investment into experimental infrastructure that has now federated the powerNET cyber physical testbed with the SEB Annex BCS, and with the BESS. Within the Trial 2 experiments, the team successfully operated the Regatron power amplifier with the Opal simulator in a closed loop system, that allowed the team to execute multiple grid fault experiments. This will allow future researchers to conduct large scale simulation tests involving BCS and BESS resources as a PHiL load.

7.0 References

Brian K. Paul, Steven Kawula, Chuankai Song. 2019. "A manufacturing process design for producing a membrane-based energy recovery ventilator with high aspect ratio support ribs." *Journal of Manufacturing Systems* 52 (Part B): 242-252.

Johnson Controls. n.d. "NCE25, NAE35, and NAE45 Catalog Page." *Technical specifications - NCE25, NAE35, and NAE45 models.* Accessed September 28, 2023. https://docs.johnsoncontrols.com/bas/r/Metasys/en-US/NCE25-NAE35-and-NAE45-Catalog-Page/9.0.8/Technical-specifications-NCE25-NAE35-and-NAE45-models.

Pacific Northwest National Laboratory. 2020. *Resilience Through Data-Driven, Intelligently Designed Control (RD2C) Initiative .* Accessed 2023. https://www.pnnl.gov/projects/rd2c-initiative.

PNNL. 2022. "SerialTAP Cybersecurity Tool." January. Accessed September 27, 2023. https://www.pnnl.gov/sites/default/files/media/file/DDST_0158_FLYER_SerialTap_WEB_V2.pdf.

Regatron. n.d. *tc-acs-series.* Accessed September 27, 2023. https://www.regatron.com/product/overview/programmable-bidirectional-ac-power-sources/tc-acs-series/.

Yokogawa. n.d. *DL950 ScopeCorder Data Acquisition Recorder.* Yokogawa. Accessed September 27, 2023. https://tmi.yokogawa.com/us/solutions/products/data-acquisition-equipment/high-speed-data-acquisition/dl950/.

Appendix A – Trial 2, Test Case 1 Testing Procedure

A.1 Research Question 1 (Baseline)

The traditional power system grid with large, centralized power generation, transmission, and distribution networks is highly complex, making delivering quality power to end-users difficult. Furthermore, delivering quality "clean" power is even more complicated to achieve with the integration of inverter-based generation on the distribution level and the interconnection of dynamic, non-linear loads. These new components can introduce additional power quality issues (nonlinearities, oscillations, modulations, etc.) To understand the impact of such distortions, a BCS behavior under standard 'clean' power needs to be recorded and used for future benchmarking.

This test case will establish electrical baseline measurements for the normal operation of the 3820A annex. Power draw, load currents, and voltages will be measured and recorded and will serve as a basis for all other tests.

Table 4. Research Question 1

Hypothesis	
The 3820 Annex system will have a stable, repeatable pattern with minimal changes in any of the dependent variables.	
Independent (Manipulated) Variables	**Dependent (Measured) Variables**
• Supply System Voltage • Supply System Frequency	• Voltage change • Current Draw • Power Draw • Frequency Change • Communications • System Behavior • Device "On" or "Off" behavior • Device Logs • Temperatures

Table 5. Research Question 1 Test Cases

Test	Description
Case 1	Set the "ideal" supply system conditions (i.e., f=60Hz and V=1p.u.) and record BCS behavior.

A.1.1 Risks and Mitigations

There are no identified risks. The supply system which is comprised of REGRATRON amplifier has been already tested and proved that it can provide stable supply for 3820 Annex system (including all the loads).

Test 1 Execution Steps

1. Ensure Regatron (located in SEB112) is on, and powering the SEB Annex at 60hz frequency, and 277 Volts.
2. Check that the SerialTAP Laptop (located in SEB Annex) is on, and the appropriate command for collecting SerialTAP data is entered into the terminal.
    a. Open terminal
    b. Type "**`sudo su`**", followed by "**`password`**" at the password prompt
    c. Type "**`cd /root`**"
    d. SerialTAP command (must be sudo in /root): **"`nohup tshark -b duration:300 -b files:720 -I udpdump -o extcap.udpdump.payload:mstp -o extcap.udpdump.port:3333 -w serialtap-seb.pcapng`"**
3. Check that the microphone laptop (located in SEB Annex) is on, and the appropriate program for recording from the microphone is open
4. Ensure microphone (located in SEB Annex) is positioned to gather sound from the room
5. Check that Yokogawa is on, that it's reading the correct channels, and that it is set to sample at 200u
6. Ensure SEB annex doors are closed before beginning of test
7. Begin Capture by executing SerialTAP command, beginning microphone capture, and beginning Yokogawa capture
    a. START TIME (Example entry, recorded from single phone or watch external to the system): 4/21/2022 5:51PM PDT)
        i. Run 1: 4/25/2022 12:13PM PDT
        ii. Run 2: 4/25/2022 12:34PM PDT
        iii. Run 3: 4/25/2022 12:42PM PDT
        iv. Run 4: 4/25/2022 12:53PM PDT
        v. Run 5: 4/25/2022 01:07PM PDT
8. Once five minutes has passed, end SerialTAP collection, microphone data collection, and Yokogawa data collection
    a. END TIME
        i. Run 1: 4/25/2022 12:19PM PDT
        ii. Run 2: 4/25/2022 12:39PM PDT
        iii. Run 3: 4/25/2022 12:47PM PDT
        iv. Run 4: 4/25/2022 12:58PM PDT
        v. Run 5: 4/25/2022 01:12PM PDT
9. Gather and export to single external hard drive:
    a. Microphone Data
    b. SerialTAP Data
    c. Yokogawa Data
10. Confirm all data has been saved with correct filenames onto external drive.
    a. Please follow naming conventions in file-name-convention.txt within the project share.
11. Repeat steps 1-10 four additional times.

Appendix B – Experiment Results

Table 6: List of experiment results

Trial	System	Test Case ID	Hypothesis	Results?
1	BCS	1	Unusual network traffic on Ethernet-connected BAS devices will cause degradation of services, and/or cause other unwanted behavior in the probed device.	False
1	BCS	2	Keeping the system device in a continuous start-up process will cause built in system protection to activate and/or breakers to trip.	False
1	BCS	3	Remotely accessing and operating the system will have a different effect on the timing and communications of a system than local operation.	False
1	BCS	4	When the 3820 Annex is powered back on from an outage state, its startup behavior will be measurable, repeatable, and have an identifiable pattern.	False
1	BCS	5	Power draw due to different goal temperature set points will trip a breaker.	False[1]
2	BCS	1	The 3820 Annex system will have a stable, repeatable pattern with minimal changes in any dependent variables.	True
2	BCS	2	When the voltage that supplies 3820 Annex is set off-nominal, the entire system and/or some components might exhibit unexpected behavior (e.g., reduced efficiency).	True
2	BCS	3	When the frequency range of the 3820 Annex is set off-nominal, the entire system and/or some of its components might exhibit unexpected behavior (e.g., reduced efficiency).	False[2]
2	BCS	4	A sum of off nominal conditions, in this case a fault within the grid simulation, will cause the system components to exhibit unusual behavior.	True

[1] Results do show that there is impact upon the system, but not enough to physically trip a breaker
[2] The testing infrastructure UPS did exhibit unexpected behavior, but it was not within the scope of this test

Appendix C – IoT Research Questions

The increased adoption Internet of Things (IoT) in building control system presents a fundamental shift in the maintaining and operating equipment. While IoT provides traditional building controls with more insight into performance, there are risks associated with this adoption. These new components can introduce new attack vectors that may jeopardize the power stability and system efficient. The building behavior during an attack needs to be recorded and characterized to understand the impacts of such threats. Below in Table 7 is a summary of the IoT attack types considered.

Table 7 IoT -Attack

Research Question #	Attack Type
1	Scanning/BOTNET
2	Continuous Reboot Annex
3	Remote Attack
4	Device Reboot Order
5	Man-in-the-Middle
6	System Error Handling

Research Question 1 (Scanning/BOTNET): Will unusual network traffic on wireless-connected temperature and motion sensor devices cause degradation of services, and/or cause other unwanted behavior in the probed device?

The first research question for Trial 1, seeks to study the impact of scanning on power draw.

The first step in a cyberattack campaign is reconnaissance. A standard method to inspect the system and begin determining vulnerabilities is to run a series of scans that become progressively more targeted. These scans attempt to identify the devices' operating system under scan, as well as open ports and protocols. The results of these scans allow for a greater understanding of how the system communicates, active services, and exploitable vulnerabilities.

However, if multiple devices all scan and probe the NAE controller at the same time, will this be enough to cause a denial of service attack? The goal within this experiment will be to cause the IoT devise, as well as additional spoofing IoT devices, to scan the Johnson controller simultaneously to deprioritize its communications with the HVAC system. This will represent a very small-scale BOTNET type attack.

Research Question 2 (Device Reboot Order): Is the startup behavior will be measurable, repeatable, and have an identifiable pattern after recovering from an outage?

When a BCS has power restored after an outage, services and devices return at different times. Each control device part of "the system" will reboot to an operational state. This process is hypothesized to be identical each time a device reboots. By extension, the startup process for the entire system should also be similarly identical. However, the team was informed by the Annex subject matter expert (SME) that this has never been tested. He further said that if there is variance in which devices start first, it could affect the initial startup power draw and how long this spike in demand lasts.

The system's behavior after startup can be defined by a set of time-dependent measurable physical variables, including but not limited to device-specific power consumption, order-of-

operation, and communications flags. The temporal patterns of all measured variables form the system behavior. The research question will focus on this behavior and its similarity between test runs.

Research Question 3 (Man-in-the-Middle Attack): Will the HVAC change state and pull more power from the grid than expected when a 3-party sensor is spoofed?

3rd -party IoT devices are being integrated into BCS to create smart buildings. The data from these devices assists in making buildings more eco-friendly by decreasing cost and increasing occupant comfort. However, these devices are known to have vulnerabilities and minimal security features. Integrating these 3rd -party devices could expose the BCS to the internet.

Through shared network access between the IoT devices and a BCS, the BCS may be subject to traditional cyber-attack surfaces. Many IoT devices are known to have weak authentication, no encryption, missing firmware updates, and limited device management. These common vulnerabilities may provide enough control to impact the power draw of a BCS on the grid.

Research Question 4 (Man-in-the-Middle Attack part 2): Can a device spoofing a 3-party sensor subvert the Johnson NAE Controller in such a way that it can directly communicate with and effect other devices within the serial bus system?

In a follow up to Research Question 3, if the spoofing attempt is successful, the team would like to run an experiment by attempting to route BACnet packages through the controller. The test would involve the attacker laptop attempting to send a BACnet control package to the AHU controller.

Research Question 5 (System Error Handling): Will the controller continuously tell the gateway to resend the packet and eventually congest the network when a 3-party sensor sends a malformed packet to the controller?

There must be a gateway for IoT devices to talk to traditional BCS. The gateway converts the IoT device data to BACnet and sends the information to the controller. However, the BACnet protocol is flexible, which allows vendors to implement their variations of BACnet. Traditional BACnet systems are highly reliable, and only a master device can initiate a request, simplifying detecting failure.

Through the gateway, one could improperly implement converting data to BACnet and cause a malformed packet to be sent to the controller. 3rd -party devices and gateways are not controlled by the master node or the BCS vendor. This may lead to improper error handling, which may jeopardize the efficiency of the system.

Appendix D – BESS Research Questions

Research Question 1: Will the BESS discharge when system frequency is low?

In an electrical system, system frequency falls when load increases, and rises when load decreases. Considering that the BESS may be providing frequency support, it may be that the BESS discharge when system frequency is low (to provide generation to the increasing load), and charge when system frequency is high (to increase the decreasing load). If the BESS in this example is enabled to provide this ancillary service, it is expected that changing the system frequency will create this synthetic charge and discharge. It would be interesting to see how a cyber-physical attack aiming to change system frequency will cause this behavior in an unwanted manner.

Research Question 2: Can configuration changes be sent to the MsBMS during battery charge and discharge? If so, what configuration changes represent the greatest risk?

The master battery management system (MsBMS) of the BESS connects to the rack management system controller (RMSC) of the racks, and has an HTTP-based connection to the human-machine interface (HMI) of the MsBMS. For the safe and secure operation of the rack, it is emphasized that configurations (available through the MsBMS) are not changed while the battery is discharging or charging, or connected to the network. The accessibility of such control via the MsBMS and the provision of a web-connected HMI to the MsBMS present a good cyberattack opportunity. It is possible that an attacker will connect to the HMI over the internet, decipher the login credentials, and send grave control commands to the RMSC. This is interesting to explore.

Research Question 3: Can aggressive network communications introduced by a third-party device influence the behavior of the system?

The BESS uses two types of communication. They are:

- Modbus TCP – Using Sun Spec modeled Modbus register mapping.
- CAN – If this is chosen then they will have to integrate all functionality currently implemented in the MsBMS.

Using TCP protocols, a repeat of research question 1 from trial 1 could be interesting.

Research Question 4: Can sensitive areas of memory within the BESS be identified by a third-party device on the network? Can we scan for and identify non-empty registers and coils?

Research Question 5: Can we force values of our choosing by writing enough times to a given piece of memory more frequently than the BESS cycles through its MODBUS server checks?

The BESS utilizes the MODBUS/TCP protocol for communication. The MODBUS protocol is an unencrypted, unauthenticated network protocol that, if implemented incorrectly can allow sensitive areas of memory to be written by any MODBUS client. Crafting specialty packets in Python or a MODBUS fuzzer can be utilized to test for areas of memory that hold important data (i.e., operating voltage values). If these areas of memory are identified and can be written to, it would be a simple matter to perform a host of injection attacks that can overshadow real values with fabricated, injected values.

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354

1-888-375-PNNL (7665)

www.pnnl.gov