SCADA Lab Capstone Report

Author:
Jessica Jones
Joseph Arenas
Kiyoshi Hashida
Marc Ivan Mañalac
Mark Pascual
Waylon Bader

Faculty Advisor:
Mark Nelson

Date:
05/13/2022

+
A report submitted in partial fulfillment
of the requirements for

EE496

Department of Electrical Engineering
University of Hawaii at Manoa

Abstract

Supervisory Control and Data Acquisition (SCADA) systems play a crucial role in maintaining efficiency in sectors of critical infrastructure. However, many SCADA systems were created and designed using outdated technology, increasing their susceptibility to being compromised. As SCADA systems bridge the gap between cyberspace and the "real world", an increasing number of cyberattacks on SCADA systems have brought to light how vulnerable these systems are to internal and external threats, how devastating an attack can be, and how necessary it is to utilize improved security measures. This paper discusses the importance of anticipating vulnerabilities in the design and construction of SCADA systems, as well as the development of our test bed to assess the effectiveness of various security methods, such as Software Defined Networks and Zero-Trust architecture.

I. Introduction

The UH SCADA Lab is laying the foundation to outfit our SCADA system with Software Defined Networking (SDN) and Machine Learning to create a custom Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). SCADA is a control system that collects real time data for operators to interpret. It incorporates a Human-Machine Interface (HMI) offering control over local and remote systems. These systems are used in critical infrastructure, such as to help operate mass transit, healthcare, industrial, manufacturing, electrical, water, and wastewater treatment facilities and systems.

Most SCADA systems in place today were developed years, if not decades, ago [1]. As the Internet of Things (IoT) is becoming standard, businesses are connecting their SCADA

systems to the internet. However, considering how these systems use older technology and that cyberattacks have grown in frequency, complexity, and severity since these systems were implemented, the increased connectivity has given attackers more ability to harm critical infrastructure [2]. In fact, you may have heard of attacks against SCADA systems in the news.

On December 23, 2015, in the Ivano-Frankivsk region of Ukraine, the power grid was hacked and shut down, leaving a quarter million Ukrainians without power. After managing to hack into the Information Technology (IT) network through phishing emails, attackers analyzed the network for vulnerabilities. The group bypassed a firewall that connected their Operational Technology (OT) to their IT network. Once the attackers gained access, they began changing configurations of the SCADA system, which included rewriting code controlling uninterruptible power supplies (UPS) and blocking operators from closing breakers to restore power. The attack cut power for 1 to 6 hours, and is acknowledged as the first successful attack on a power grid [3]. Additional attacks on SCADA systems include the recent attacks against the Colonial Pipeline and Florida's water system.

Infrastructures mentioned above have impacted first world countries greatly. Society as a whole has become heavily dependent on the structure placed by these infrastructures. When a person walks into a house, they expect the water to run, electricity to work, and the toilet to flush. This can be seen in a bigger picture with traffic lights, airports, and everything related to transportation. These infrastructures have become so common that no one thinks twice about it until it's not there or not working the way it should. Electrical, water, and wastewater are key infrastructures that help society as a whole run smoothly. A power outage caused by a SCADA

attack on one of these infrastructures would definitely slow society down. Traffic lights would stop working properly and electricity that power electronics would no longer be there. This could extend to the water and wastewater facilities; water and toilets in a house will no longer work the way it should. This causes inconvenience and creates confusion for everyone affected. The infrastructures affected will lose money due to no customers using the facilities and workers working overtime to find and fix the problem. Furthermore, as Microsoft's Special Report on Ukraine highlights, attacks against SCADA systems may be used as retaliation for political and military actions [4]. As you can see, SCADA affects everyone's life in social, political, and economic aspects.

In this report, we will discuss our continued work on SCADA lab capstone, what we have accomplished this semester, and the future direction of the project. Section II will cover the project result and analysis portion which is split into subsections A and B. Section III discusses the future and subsequent work that will be conducted on this project in two subsections A and B which will cover more on zero trust architecture and machine learning. Section IV is our acknowledgements for the project, and section V concludes this report.

II. Project Result and Analysis

A. Final Design

The physical network layout of our SCADA network is depicted in Figure 1. The SCADA Lab in Holmes Hall will serve as our headquarters for accessing and configuring the network as well as implementation of our SDNs, machine learning, and zero trust. The Information Technology Center (ITC) will house our industrial utility power system equipment

such as our transmission line Protection and Automation System (SEL-311B), Protection, Automation, and Bay Control System (SEL-451), and our Real-Time Automation Controller (SEL-3505). The final design of our system took into account the applicability of our current devices and security features that we plan on installing in future iterations of the capstone project.

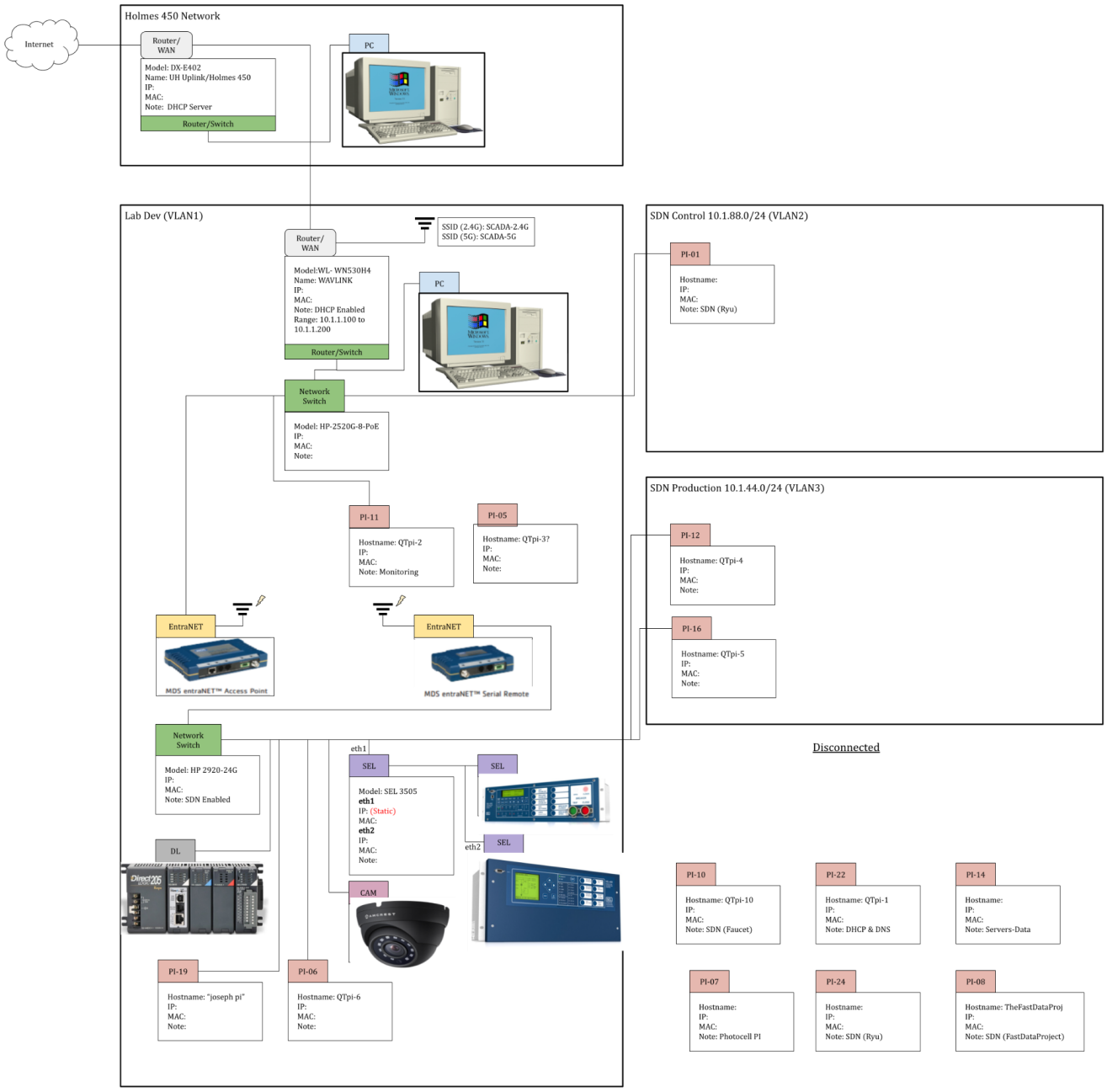

Figure 1: The SCADA Network Map

As previously mentioned, the application of this project was chosen to simulate a real life SCADA system such as electrical utility distributors by using a programmable logic controller (PLC).

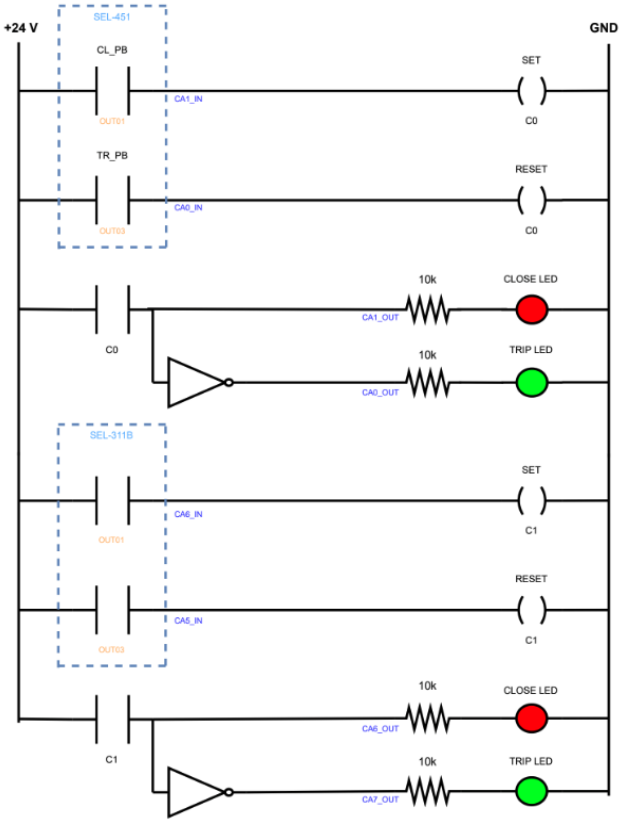

Figure 2: Ladder Logic Diagram

The PLC uses ladder logic, which can be seen as incoming voltage on the left side and returning voltage to the right. In between these two sections are where the basic inputs are put in. The term ladder logic is given by how it looks, a ladder with logic. The PLC outputs DC voltage which is mainly used to turn on relays which open or close contacts assigned to the relay. To simulate a distribution network on a utility grid, we must look at the basic understanding of what

that means. It can be seen as a simple switch that is either in the “on” state or in the “off” state. The ladder logic design shown in Figure 2 is a simple SR (set/reset) latch circuit so that there is a saved state in the breaker operation. The set and reset coils for the SEL-451 are labeled as C0 control the normally open contact labeled as C0. The SEL-311B uses the same setup, with the coils and contact labeled as C1. The contacts in the blue box are located on the SEL devices. These contacts are labeled OUT101 and OUT103, which are the contact screws on the back of the device. The SEL-451 has a physical push button for manual operation, while the SEL-311B must use a series of buttons to go through a menu to do a manual operation.

The PLC is a solid state device which requires this type of circuitry to replicate a mechanical AC circuit breaker used in a substation. To ensure that the states are being saved, red and green LEDs are used to represent closed and open respectively and are connected after an assigned contact. The two LEDs are in parallel with each other. The green LED is wired in series with an inverter to allow power to it when the contact is considered open. The main idea behind this design is to give us a status indication that a signal was sent to the appropriate device. Figure 3 shows the status indicator lights wired on a breadboard.

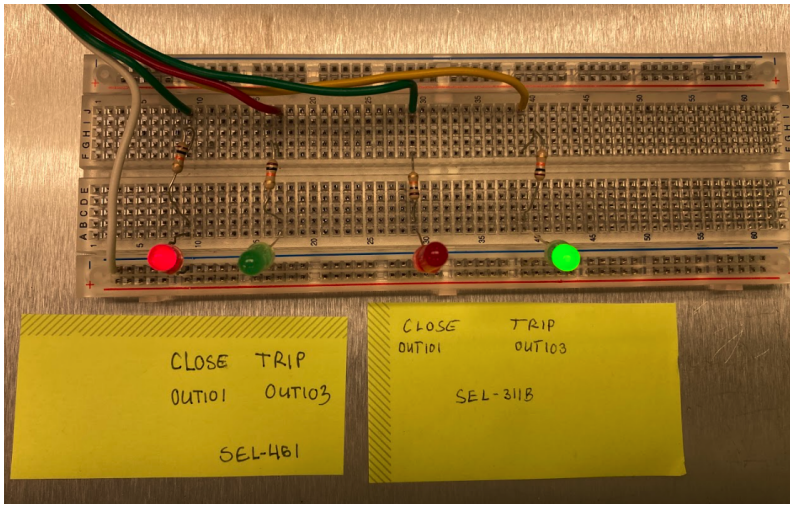

Figure 3: Circuit Breaker Status Indicators

The SEL-451 and SEL-311B can be accessed through a terminal interface such as PuTTY on a computer connected to the same network that the SEL equipment is on. Figure 1 shows both the SEL-451 and the SEL-311B are directly connected to the SEL-3505. The SEL-3505 allows us to connect to and control the SEL-451 with an Ethernet cable and the SEL-311B with a serial cable. The SEL-3505 is also connected to the SCADA lab router, where an internet connection can be made via Ethernet or Wi-Fi. For demonstration purposes, our team decided to gain access to the SEL devices by connecting a laptop to the Wi-Fi. We connected to the SEL-3505 with an SSH connection using PuTTY along with the parameters shown in Figure 4.

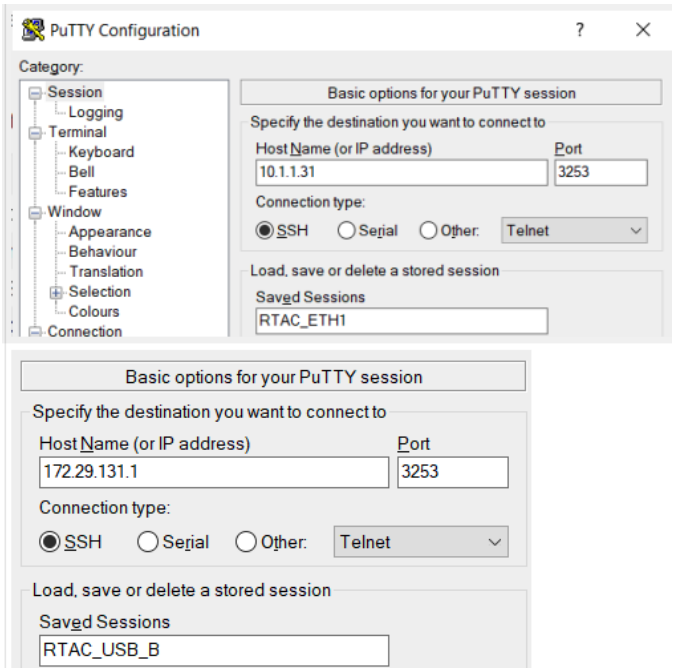

Figure 4: PuTTY Configuration

Once we are connected to the SEL-3505, a terminal shell screen pops up asking for login credentials. Once we gain access, we will need to go through two levels of security to connect to the SEL-3505. There are two levels of authentication to be able to do everything in the SEL devices. Level 1 requires the command “acc” and a password. Level 2 requires the command “2ac” and a password. Figure 5 shows the terminal commands. Once we reach this level, we can type in the command “who” to find the devices connected to the 3505. The SEL-311B is connected to the serial port 2 and is shown on Figure 6.

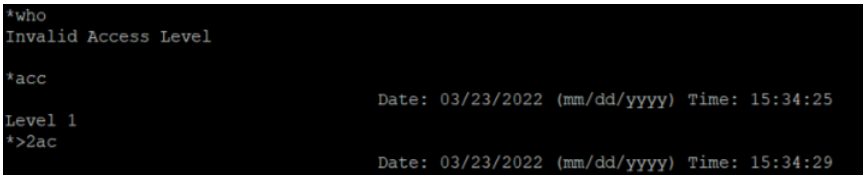

Figure 5: Level 1 and Level 2 Commands

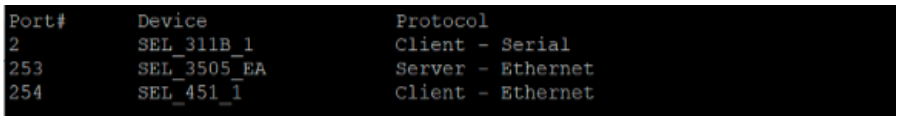

Figure 6: Who Command

To select the SEL-311B, the command “por 2” will need to be typed in the terminal. When the connection is established, a two level authentication process will need to be performed again. This step is the same as the connection to the SEL-3505. After the user reaches level 2, the circuit breakers connected to the SEL-311B can be operated from this terminal. If the user knows the SEL-311B contacts on the back that operate the breaker, they can type in the “pulse” command to either open or close it. The command consists of the word pulse followed by the contact number and the duration of the pulse. Figure 7 shows the pulse command used to trip the breaker.

Figure 7: Pulse Command to Trip Breaker

Our network is designed to be broken into two parts, connected together with a radio frequency (RF) link. For a point to point wireless solution, Hawaiian Electric gave SCADA Lab a Microwave Data Systems (MDS) entraNET 900. The MDS entraNET system consists of an Access Point and a Remote. Originally we were given a Serial Remote, but after testing determined our network design would benefit greatly from having an Ethernet connection, so we purchased a Dual Serial/Ethernet Remote off of ebay.com. The MDS entraNET devices

communicate over the 900 MHz industrial, scientific and medical (ISM) band, and have a max transmission range of 30 miles with good line of sight (LOS) and transmitting at full power. We purchased two Yagi-Uda antennas with 6 dBi of gain, which complements the MDS entraNETs max power output of 30 dBm, keeping our setup at or under the Federal Communications Commission's (FCC) Maximum Effective Isotropic Radiated Power (EIRP) of 36 db. We will be splitting the SCADA Lab into two separate spaces, a local Control Center, located in Holmes Hall, and a remote Substation, located at the ITC building (see Figure 8). These buildings are less than half a mile apart, and installation of antennas onto their respective roofs will allow for clean LOS. Once installed, the transmitted power can be adjusted to give max throughput while minimizing our footprint in the spectrum, in order to be good stewards of the RF environment.

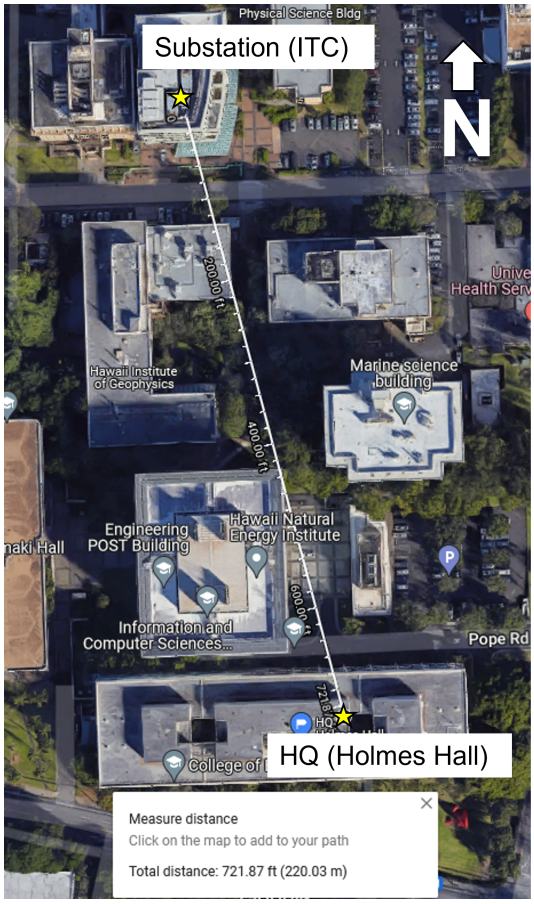

Figure 8: LOS from Holmes Hall to the ITC Building

B. Explanation of how previous and concurrent course work is related to the project.

Although many of our lab members came into the project with zero experience or understanding of SCADA, we were still able to produce a tremendous amount of progress in the building of our system using courses we have taken in the first two to three years in the college of engineering. Listed below are a few ways in which previous and concurrent course work related to the project empowered students in this lab.

In order to understand the function of our SCADA devices and its capabilities, our administrators must have a foundation of basic electrical engineering concepts such as the relationship between current, resistance, and voltage learned in Introduction to Circuits I, and II. The configuration of our PLC uses theory taught in Microelectronic Circuits and Logic Design. With these prior courses, the team was able to design a physical circuit to visually display breaks in the relay and configure cameras and sensors into our system.

Whilst some of our devices come with a user-friendly interface for configuration, most of them require knowledge of the Linux operating system and command line interfaces to interact with the components that were taught in the Operating Systems and Intro to Programming. For instance, in order to send real-time commands to our equipment, a user must be able to access the device through our network via SSH and pass two layers of security, then enter the appropriate command in the prompt. Our team must also be capable of understanding network protocols, and identifying ports, and addresses which were covered in classes such as Intro to Computer and Network Security, Cyber-Physical Systems and IoT.

C. A discussion of related work and how the project is different.

Overall, our project is similar to other projects combining SDN and Machine Learning to create a custom IDS / IPS [5]. Ours differs mainly in the use of SCADA as the basis of the network being protected, and trying to integrate our design into previously existing SCADA infrastructure. A SCADA network needs to have 100% uptime, in order to monitor and control the health of the system as a whole. The control signals along our network need maximum reliability to get to their respective machines, and maintaining security is of the utmost importance. We are also using Raspberry Pi's as our SDN controllers. When retrofitting existing SCADA systems with our project, using a Raspberry Pi helps to keep the cost down and provides limited interference with existing hardware. However, this limits us in which SDN controllers we can use, because not all controllers can run on a Raspberry Pi.

III. Future Work or subsequent Development

A. Software Defined Network

Software defined networks are a virtualized network which can dynamically adapt to our systems needs for collecting and controlling data flow. While there are a number of commercial SDNs available, we are experimenting with open source versions of SDNs that we can personalize to later introduce machine learning algorithms using python.

B. Zero Trust

The standard model of trust from computers is based on a human concept of trust. This model of trust is inherently broken. For example, if we see a coworker working at their desk

every day with their work identification badge on display, we would assume that they are a trustworthy employee. What we may not know is that the same coworker was let go weeks ago and is now trying to steal company information. This brings us to the new model of trust called zero trust introduced by the National Institute of Standards and Technology, or NIST. Zero trust safeguards computers from making human mistakes such as the one mentioned above. In coming semesters of this project, our SCADA systems will incorporate zero trust practices using processes such as two-factor authentication, history sessions, environmental variables, and more in accordance with the zero trust tenets [6] [7].

IV. Acknowledgement

We would like to take this opportunity to express our gratitude at the generosity of our sponsors and mentors. The funds provided by the National Security Innovation Network allowed us to purchase the necessary equipment to build and expand our lab. We would like to thank Schweitzer Engineering Laboratories and the Hawaiian Electric Company for donating equipment. We would also like to thank the College of Engineering and the University of Hawaii Information Security team for allowing us to use their lab space. Last but not least, we would like to thank our mentors from the United States Indo-Pacific Command and the National Security Agency. Once again, we are appreciative of everyone who contributed to our project.

V. Conclusion

SCADA equipment controls all aspects of our lives: power, water, and there is even SCADA in our cars and airplanes. It is vital we find a way to protect these SCADA systems

from bad actors. This semester, we have built control systems using the equipment given to us to turn an LED on and off remotely, simulating control over a full power grid. We have created a full production network, complete with three virtual local area networks (VLAN), simulating the substation, control center, and administration networks. We have installed our wireless solution which connects the substation network to the control center network. Furthermore, we have been working with multiple different SDN controllers, and are close to determining which one fits our needs the best. SCADA Lab is on the cusp of a fully operational SCADA system, so next semester we can physically separate the control center from the substation, and start combining Zero Trust, Machine Learning, and SDN to create a rules based functioning IPS for SCADA systems.

Appendix I: References

[1] Hunzinger, R. (2014, October 29). *Is it time for new SCADA software technology?* automation.com. https://www.automation.com/en-us/articles/2014-2/is-it-time-for-new-scada-software-technology

[2] Dunsavage, J. (2022, April 29). *Cyberattacks growing in frequency, severity, and complexity*. III | The Triple-I Blog. https://www.iii.org/insuranceindustryblog/cyberattacks-growingin-frequency-severity-and-complexity/

[3] Zetter, Kim (3 March 2016). "Inside the cunning, unprecedented hack of Ukraine's power grid". Wired. San Francisco, California, USA. ISSN 1059-1028.

https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[4] Digital Security Unit. (2022). *Special Report: Ukraine*. Microsoft. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

[5] Ahmed, Md. Rayhan; Islam, salekul; Shatabda, Swakkhar; Islam, A. K. M. Muzahidul; Robin, Md. Towhidul Islam (2021): *Intrusion Detection System in Software-Defined Networks Using Machine Learning and Deep Learning Techniques –A Comprehensive Survey.* TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.17153213.v1

[6] IBM Technology. *Zero Trust Explained in 4 Minutes.* [Online]. Available: https://www.youtube.com/watch?v=yn6CPQ9RioA

[7] S.Rose, O. Borchet, S. Mitchell. S, Connelly.*NIST Zero Trust Architecture*. National Institute of Standards and Technology. p.6. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Appendix II: Acronyms

EIRP	Effective Isotropic Radiated Power
FCC	Federal Communications Commission
HMI	Human-Machine Interface
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISM	Industrial, Scientific and Medical
IT	Information Technology
ITC	Information Technology Center
LOS	Line of Sight
MAC	Media Access Control
MDS	Microwave Data Systems
NIST	National Institute of Standards and Technology
OT	Operational Technology
PLC	Programmable Logic Controller
RF	Radio Frequency
SCADA	Supervisory Control and Data Acquisition
SDN	Software Defined Network
SEL	Schweitzer Engineering Laboratories
UPS	Uninterrupted Power Supply