ISAAC: The Idaho Cyber-Physical System Smart Grid Cybersecurity Testbed

A Thesis

Presented in Partial Fulfillment of the Requirements for the

Degree of Master of Science

with a

Major in Computer Science

in the

College of Graduate Studies

University of Idaho

by

Ibukun Adesile Oyewumi

Major Professor: Yacine Chakhchoukh, Ph.D.

Committee Members: Daniel Conte de Leon, Ph.D.; Brian Johnson, Ph.D.

Department Administrator: Terrence Soule, Ph.D.

December 2019

Authorization to Submit Thesis

This thesis of Ibukun Adesile Oyewumi, submitted for the degree of Master of Science with a Major in Computer Science and titled “ISAAC: The Idaho Cyber-Physical System Smart Grid Cybersecurity Testbed,” has been reviewed in final form. Permission, as indicated by the signatures and dates below is now granted to submit final copies for the College of Graduate Studies for approval.

Advisor: ______________________ ______________

Yacine Chakhchoukh, Ph.D. Date

Committee Members: ______________________ ______________

Daniel Conte de Leon, Ph.D. Date

______________________ ______________

Brian Johnson, Ph.D. Date

Department Chair: ______________________ ______________

Terrence Soule, Ph.D. Date

Abstract

The landscape of cyber and other threats to Cyber Physical Systems (CPS), such as the Power Grid, is growing rapidly. Smart and distributed devices capable of extensive inter- and intra- networking are playing a more significant role in CPS thereby increasing the risks associated with such systems. Realistic and reconfigurable testbeds with correctly implemented security policies capable of mitigating threats are needed to develop, test, improve, and deploy practical cybersecurity solutions for CPS. This thesis primarily discusses the design and implementation of ISAAC, the Idaho CPS Smart Grid Cybersecurity Testbed, a cross-domain, distributed, and reconfigurable testbed, which emulates a realistic power utility and provides researchers with the tools needed to develop and test integrated cybersecurity solutions. Furthermore, the thesis showcases the post-implementation capabilities of the testbed through a two-pronged validation: i) mapping with an ICS reference architecture model; and ii) an emulated cyber-attack experimental scenario.

Acknowledgements

First and foremost, I would like to convey my heartfelt appreciation to to Dr. Daniel Conte de Leon. He introduced me to research, provided step-by-step guidance, funding sourcing and instilled a source of inspiration to push harder. I am also grateful for the broad exposure outside academic activities that he provided me in terms of teaching opportunities, collegiate and US Department of Energy (DoE) cyber-defense competitions.

I would like to thank Dr. Brian Johnson for his encouragement, mentoring and funding for my graduate studies. Dr. Johnson was instrumental in introducing me to CPS, and discussing new ideas. His inputs were critical in defining the direction of my program and his impact on this thesis remains invaluable. In addition, my appreciation goes to Dr. Yacine Chakhchoukh. He made immeasurable contribution to my publications, thesis and funding for my graduate program. He was also instrumental in the guidance of my research work.

I found the guidance and tutoring of Dr. Jim Alves-Foss, Dr. Michael Haney and Dr. Frederick Sheldon extremely useful. They were welcoming and open to discuss new ideas related to Cybersecurity and professional career development. I am really thankful to Dr. Haney for sharing his experience in academia and industry with me in order to make a decision on my next course of actions.

I would like to thank Arvilla Daffin, Victor House, John McFarland, Ray Anderson, John Jacksha, Arleen Furedy and Susan Branting for their moral, administrative and technological support in attending Cyberdefense competitions, conferences, academic events and technical research in the past two years. I would also like to thank all of the agencies that financially supported my research: Department of Computer Science at University of Idaho, the State of Idaho: through Idaho Global Entrepreneurial Mission (IGEM) Grant for Security Management of Cyber-Physical Control Systems, 2016 (Grant Number IGEM17-001), the Center for Secure and Dependable Systems at University of Idaho, the U.S. National Science Foundation (NSF) CyberCorps R award 1565572, the M. J. Murdock Foundation, Idaho National Laboratory and Schweitzer Engineering Laboratories. I appreciate the moral support of friends, family, faculty, colleagues and everyone who have made enormous sacrifices for me. Thank you all.

Dedication

Oluwaremilekun Abigael Oyewumi

In the vastness of space and immensity of time, I would much prefer it if you were alive and well.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

Industrial Control Systems (ICS) are real-time operational infrastructure that operate and automate critical processes. Supervisory Control and Data Acquisition (SCADA) systems are an important part of ICS. SCADA systems are designed to provide real-time data from industrial processes, locally or from remote locations [1]. Advances in automation technology and other digitalized movements have resulted in a transition of ICS into Cyber Physical Systems (CPS) [2].

Cyber-physical systems (CPS) are complex inter-networked systems that consist of cyber components for accessibility, computation and communication, closely interfacing with physical system components typically called field devices such as sensors and actuators. In recent years, there has been an exponential increase in the use and capabilities of CPS and these systems continually play an increasingly important role in critical infrastructure. Examples of cyber-physical systems are power grids, autonomous systems, robotics systems, health monitoring systems, etc.

CPS is also a widely used generic term for a variety of several control systems, such as SCADA systems and modern smart grids. These systems consist of computing, electrical and mechanical components with other automated or manual processes managed by human personnel. CPSs control physical processes by integrating their sensing, actuation, transmission and computational capabilities to create automated or semi-automated control of physical equipment in many industries such as: electric utilities, manufacturing, sewage plants, distribution systems, aviation, autonomous systems and many more.

Traditional CPSs contain three parts: sensors, computation applications, and actuators. These perform three basic functions: i) sensing characteristics of the physical world such as temperature, electrical measurement values etc.; ii) processing measurement data appropriately based on the data source; and iii) generating response actions through actuation. The traditional architecture of this operation is depicted in Figure 1.1

Traditional CPSs were air-gapped and designed on ”security by obscurity” with an assumption that an attacker would lack sufficient knowledge about the operational characteristics of the system. Avail-

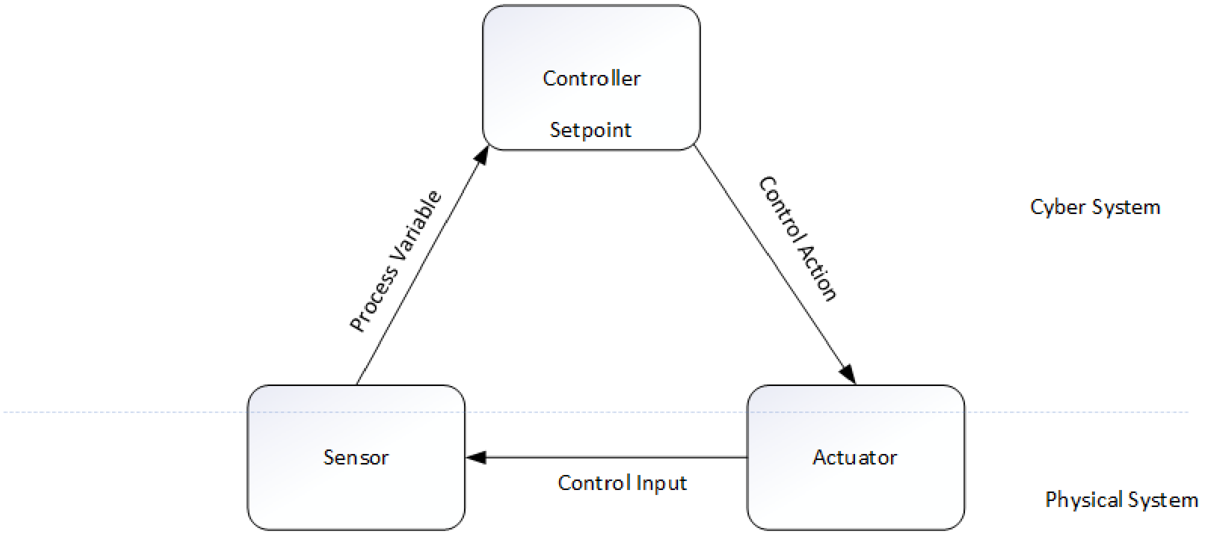


Figure 1.1: Block Diagram of a CPS Operational System.

ability and safety dominated security concerns for traditional CPS but with the introduction of newer technologies, confidentiality and integrity have become more critical security requirements.

With the transition of ICS to CPS, successful execution of cyber attacks against CPS have a potential for disastrous consequences. A disruption in data transmission and processing activities of a CPS can devastate system operations, resulting in loss of life, finances, and access to critical resources [3].

In recent decades, CPS have started using non-proprietary, non-vendor specific distributed devices. The electric utility sector is increasingly adopting information technology to support their electricity grids, creating smart grids. CPS have also started using newer feature mechanisms with non-proprietary, non-vendor specific, and distributed devices such as: 1) digital fault recorders; 2) synchrophasor based devices like Phasor Measurement Units (PMU) and Phasor Data Concentrators (PDC); 3) Advanced Metering Infrastructure (AMI); 4) more capable Intelligent Electronic Devices (IEDs); and 5) wired and wireless communications for data processing. Such distributed devices are all inter-connected in a CPS, to form smarter power grids.

Smart grids are large CPSs that include smarter, inter-connected devices with advanced automation capabilities. They are considered a vital part of the national critical infrastructure sectors by the Department of Homeland Security of the United States of America [4]. The newer feature mechanisms in

CPS have brought many advantages and risks [3]. They have has also increased the correlative threats and vulnerabilities of the smart grid [5]. As such, CPS have become attractive targets for multiple threat actors, e.g: state-sponsored attackers, hacktivist groups, etc. Attacks on CPS are increasing with time and the growing threat landscape of smart grids remains a subject of interest for security researchers due to the catastrophic impact of a security breach [6].

1.1 Problem

Cyber Physical Systems (CPS), such as smart grids, are essential pieces in critical infrastructure worldwide. With advances in technology, most CPS are in a networked environment and the security of the physical systems or machines depends on the security of the cyber or computational systems of the CPS. However, cybersecurity was not typically a main design consideration in legacy power grid equipment since the main concern was the availability of the physical operational systems. As CPS owners continue to install remote network control devices and incorporate an exponentially increasing number of insecure Internet-of-Things (IoT) or Industrial-Internet-of-Things (IIoT) devices in industrial processes, new vulnerabilities are introduced to the operations of CPS.

The number of cyber-attacks being faced by CPS is increasing due to the advances in automation, interoperability, security across multiple domains and availability requirements. Cyber Physical Systems (CPS) are adopting a variety of distributed devices, which possess extensive inter- and intra- networking capabilities. As such, CPS are experiencing an increased threat of cyber-attacks against them. Successful execution of cyber-attacks on CPS has a potential to cause widespread loss of resources and utilities.

The 2018 Symantec Internet Security Report shows a 29% increase in CPS related vulnerabilities, with 165 recorded vulnerabilities affecting CPS technology in 2016, and 212 vulnerabilities in 2017 [7]. The Cisco 2018 Annual Cybersecurity Report also shows that threat actors who want to target CPS to cripple critical infrastructure are actively engaged in creating backdoor pivot points to facilitate future attacks [8]. The report indicates that 31% of security professionals have already seen cyber-attacks in information technology, and 38% expect cyber-attacks to extend into operational technology. This demonstrates that cyber-attacks against CPS are increasing rapidly.

Threat actors target critical components of the smart grid through their exposure to external networks, such as corporate networks and the Internet. Recently, a number of cyber-attacks such as malware campaigns have been aimed at collecting information on CPS across North America and Europe. Such adversarial activities have raised concerns among cybersecurity researchers. As a result, CPS protection models such as the HESTIA (High-level and Extensible System for Training and Infrastructure risk Assessment) system [9], [10], have been suggested as a feasible solution to strengthen CPS security .

To create a secure and resilient CPS, security research in the field of CPS must be tested and validated in a real-world environment. It is difficult to test CPS research on a real environment because the potential of unintended and unknown negative effects that the testing could create is too high. To test and validate such research, development of a realistic and experimental infrastructure, such as a testbed is needed. Testing resiliency, i.e., the ability to sustain attacks, of a CPS versus cyber-attacks is also challenging to perform on a live environment. A comprehensive testbed will also provide a realistic environment to study complex cyber-physical systems, that cannot be accurately evaluated using only simulation tools. In power systems, for example, both the complexity and real time interactions with communication and control hardware cannot be reflected by offline simulations. Developing a testbed can also positively impact CPS education.

1.2 Proposed Solution

Many research programs at academic institutions and government agencies are focused on the design and implementation of CPS testbeds. These programs are developing several strategies to mitigate attacks against a CPS. To analyze and assess the security of smart grids, realistic environments with proven experimental programs become necessary for cybersecurity research. Such realistic environments should ideally also be capable of simulating attack-defend scenarios. Such a comprehensive environment will help in securing CPS through development of novel security systems.

In this thesis, we introduce the design and implementation of ISAAC, the Idaho CPS Smart Grid

Cybersecurity Testbed. ISAAC is a crossdomain, distributed, and reconfigurable testbed, which emulates a realistic power utility and provides researchers with the tools needed to develop and test integrated cybersecurity solutions. The testbed capabilities include: 1) Fully emulated power utility modeling capable of integrating multiple substations with SCADA control networks; 2) Emulated wide-area power transmission and distribution systems, 3) Fully emulated SCADA and ICS control centers, 4) Advanced visualization and cyber-analytics, including machine learning. ISAAC enables the development, testing, evaluation, and validation of holistic cyber-physical security approaches for cyber physical systems and modern power grid CPS systems.

1.3 Contributions

The problems outlined in the previous section were tackled using three distinct approaches: I) design and implementation of an adaptive and reconfigurable cyber-physical systems testbed with hardware-in-the-loop controllers. The testbed was designed for real time experimental research aimed at investigating and observing the impact of possible cyber-attacks and evaluating the performance of new cybersecurity solutions on the smart grid using real automation controllers, IEDs, SCADA software, and cyber-physical networks; II) validation of the capabilities of the testbed using an experiment case study and an ICS architecture reference model; and III) design, architecture and implementation of enhancements to ensure usability and security of the testbed.

Contribution I is the design and implementation of ISAAC, the Idaho CPS SCADA Cybersecurity testbed at the University of Idaho. ISAAC, is an adaptive and reconfigurable cyber-physical systems testbed. ISAAC can also be used to test resiliency of CPS in an "under cyber-attack" type of scenarios. It consists of power utility and cyber system resources that enable researchers to perform simulations of smart grids and other CPS. Contribution I is outlined in Chapter 2. Chapter 3 further discusses the implementation of the testbed, including it's current and potential utilization and security considerations to ensure the Confidentiality, Integrity and Availability of the testbed.

Contribution II discusses an experimental validation of ISAAC using a microgrid simulation and simulated attack scenario against physical microgrid controllers, using real attack simulation tools and an industry-standard Supervisory Control and Data Acquisition (SCADA) software. This contribution also outlines the mapping of the ISAAC's layout with a standard benchmark for CPS architectures using logically segmented zones to secure the enterprise and the CPS network zones to form an integrated enterprise architecture using the Purdue Model for Control Hierarchy Logical Framework (Purdue reference model) [11]. Contribution II is outlined in Chapter 4.

Contribution III outlines how we ensure the Confidentiality, Integrity and Availability (CIA) triad of the testbed and it's environment using: i) experiment isolation methods; and ii) intrusion detection. We also provided recommended security strategies to further enhance the design and security of the testbed. Contribution III is outlined in Chapter 5

1.4 Author's Related Refereed Publications

Two of the contributions presented in this thesis have already been published through conference article publications. The publications were achieved in the process of conducting graduate research toward obtaining a Master of Science degree in Computer Science. This thesis includes additional details that were not included in the publications due to length restrictions and additional work developed. There may be paragraphs or sections that are verbatim of the published articles. The conference articles were copyrighted by the Institute of Electrical and Electronics Engineers (IEEE) with copyright and credit notice outlined in Appendix A.

In this section, I highlight two bibliographic entries applicable to the IEEE copyright. Entry 1 highlights the design and implementation of the cybersecurity CPS smartgrid testbed (see Chapter 2). Entry 2 outlines the attack validation experimental case study of the testbed (see Chapter 3 and Chapter 4). A few sections in Chapter 5 were also copyrighted by IEEE, however, additional details are provided on experiment isolation and intrusion detection approaches for the testbed and its environment.

1. Oyewumi, Ibukun A., Jillepalli, Ananth A., Richardson, Philip, Ashrafuzzaman, Mohammad, Chakhchoukh, Yacine, Johnson, Brian K., Haney, Michael A., Sheldon, Frederick T. and Conte

de Leon, Daniel, ”ISAAC: The Idaho CPS Smart Grid Cybersecurity Testbed,” 2019 IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 2019, pp. 1-6. doi: 10.1109/TPEC.2019.8662189.

2. Oyewumi, Ibukun A., Challa, Hari, Jillepalli, Ananth A., Richardson, Philip, Chakhchoukh, Yacine, Johnson, Brian K., Conte de Leon, Daniel, Sheldon, Frederick T. and Haney, Michael A., ”Attack Scenario-based Validation of the Idaho CPS Smart Grid Cybersecurity Testbed (ISAAC),” 2019 IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 2019, pp. 1-6. doi: 10.1109/TPEC.2019.8662168.

1.5 Thesis Overview

The remainder of this thesis is structured as follows: Chapter 2 outlines the design overview of the ISAAC testbed with a detailed description of ISAAC’s architecture and its components. Chapter 3 further discusses ISAAC’s implementation through a review of current and potential uses. Chapter 4 puts forth an experimental and formal reference model validation of the ISAAC testbed using an attack scenario and a standard benchmark for CPS architectures. Chapter 5 discusses design and architecture enhancements to ensure the Confidentiality, Integrity and Availability (CIA) triad of the testbed and its environment. Chapter 6 discusses about similar, related projects and also lays out the difference between the related work items and ISAAC. Chapter 7 proposes possible future work for the ISAAC testbed. Finally, Chapter 8 summarizes the content of the thesis, direction of the research and provides a brief conclusion. A complete list of bibliography follows.

Chapter 2: The Idaho CPS Smart Grid Cybersecurity Testbed Design

The Idaho CPS Smart Grid Cybersecurity Testbed (ISAAC) facilitates an experimental research environment to assess the security level of a CPS organization or any part of it. ISAAC is divided into three modules: 1) the Securing Cyberphysical systems ANalytics, Visualization, IoT, and machine Learning Laboratory of Enquiry (SCANVILLE); 2) the Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL) [12]; and 3) the Power lab Testbed (PoT). Figure 2.1 shows a high-level block diagram of the ISAAC testbed.

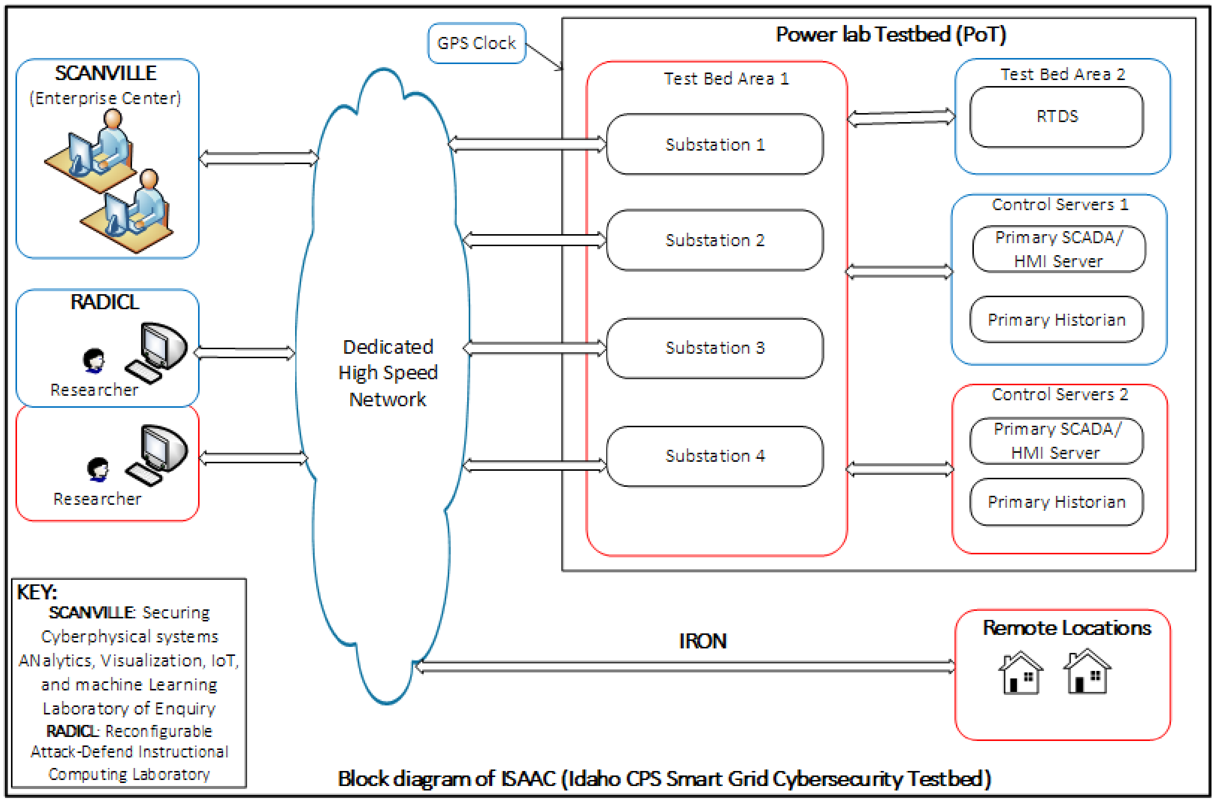

GPS Clock
Power lab Testbed (PoT)
SCANVILLE
(Enterprise Center)
Test Bed Area 1
Substation 1
Substation 2
Substation 3
Substation 4
Test Bed Area 2
RTDS
Control Servers 1
Primary SCADA/ HMI Server
Primary Historian
Control Servers 2
Primary SCADA/ HMI Server
Primary Historian
RADICL
Researcher
Researcher
Dedicated High Speed Network
KEY:
SCANVILLE: Securing Cyberphysical systems ANalytics, Visualization, IoT, and machine Learning Laboratory of Enquiry
RADICL: Reconfigurable Attack-Defend Instructional Computing Laboratory
IRON
Remote Locations
Block diagram of ISAAC (Idaho CPS Smart Grid Cybersecurity Testbed)

Figure 2.1: High-level Block Diagram of the Idaho CPS Smart Grid Cybersecurity Testbed (ISAAC).

SCANVILLE is the enterprise center equivalent of a CPS organization and it consists of infrastructure that aid in the process of: 1) monitoring, evaluating, assessing, and testing SCADA network architecture;

and 2) development of resilient models and defense mechanisms for securing SCADA networks. RADICL enables carrying out real-time experimental cyber-attacks from a virtually air-gapped or air-locked computing laboratory. The PoT consists of physical industrial control devices such as automation controllers and protection relays. The PoT can also simulate realistic electromagnetic transient time domain behavior using a Real Time Digital Simulator (RTDS) [13]. Using RTDS simulations, PoT is able to provide hardware-in-the-loop simulations for demonstrating the practical impacts of cybersecurity on industrial control processes.

SCANVILLE, RADICL, and PoT are fully implemented, and are interconnected through programmable high-performance Ethernet switches and a dedicated on-campus fiber network with switch-to-switch Media Access Control Security (MACSec) encryption. The ISAAC setup provides a realistic enterprise-level SCADA network with several experimental computing nodes. ISAAC can also be used in simulating CPS organizational models, such as the METICS-Acme model [9]. It can also be used to simulate the real time behavior of power systems such as the IEEE 14 bus system [14].

Connectivity between ISAAC and other research laboratories and branch-campuses across Idaho is planned through the Idaho Regional Optical Network (IRON). IRON is a high-density fiber-optic network backbone.

2.1 The Idaho CPS Smart Grid Cybersecurity Testbed (ISAAC) Architecture

Figure 2.2 shows a detailed architecture that depicts the current implementation of ISAAC, which replicates up to four electrical power substations controlled by an enterprise center. ISAAC provides capabilities to: 1) conduct cyber-security analytics; and 2) visualization features to centrally monitor and control activities on the test bed. The categorization of ISAAC's components are as follows:

1. Physical Components

    - PoT's Simulation

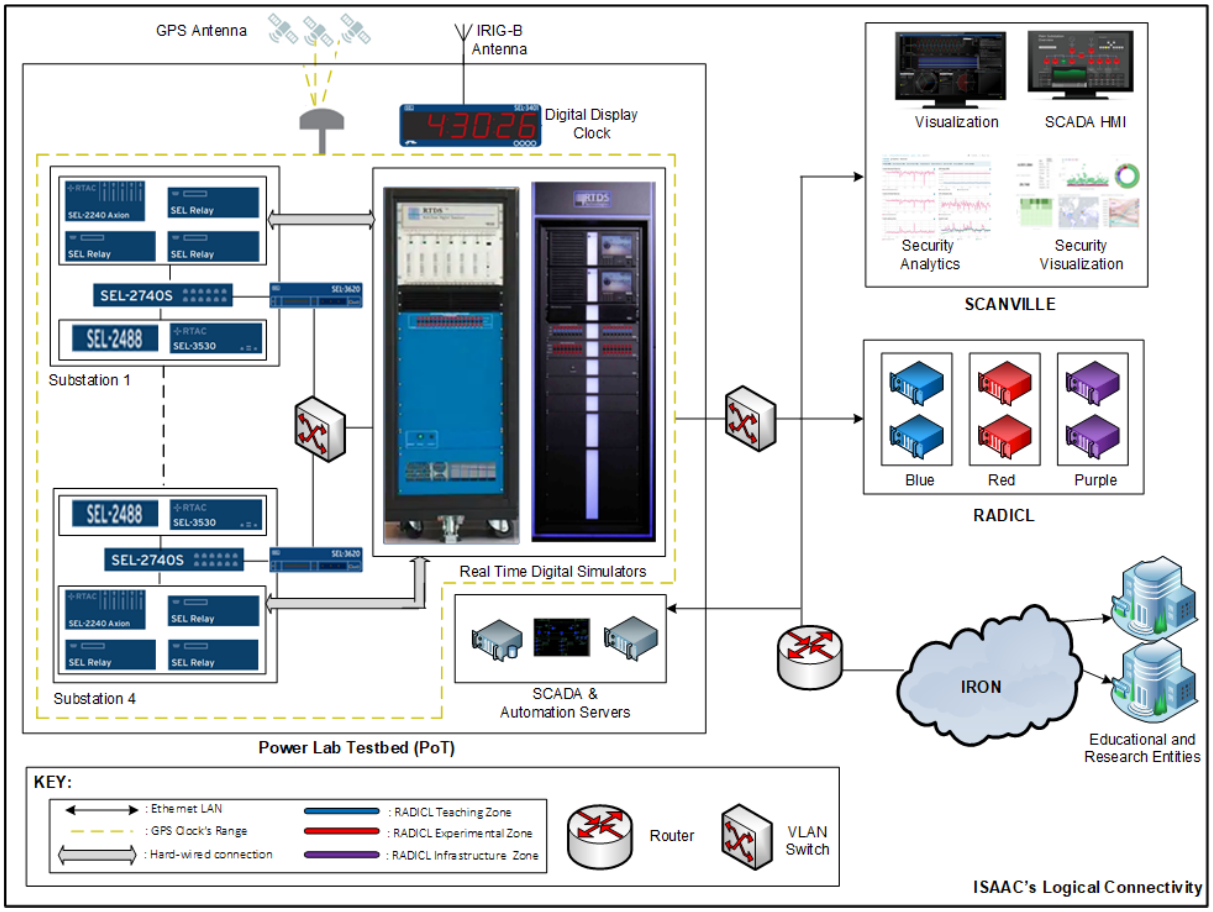


Figure 2.2: ISAAC's Logical Connectivity Diagram.

- PoT's Substations
- SCADA Control

2. Cyber Components

To increase readability of each of the components' explanations, let us segregate each of the components into individual sections.

2.1.1 Power Lab Testbed's Simulation Component

ISAAC's PoT module utilizes a RTDS to simulate a power grid utility. RTDS is a power system simulator that creates a real-time simulation environment and facilitates testing of physical equipment, such as control and protection devices and sensors, to create models for power system flow cases. A graphical user interface, RSCAD, is used to build power system models for the simulator. The RTDS is interfaced with real, physical power devices, such as relays and Phasor Measurement Units (PMUs), through analog and digital input interface cards, to evaluate the behavior and impact of these devices under different scenarios.

At the substation level, IEDs communicate with the RTDS using analog or digital inputs. The Real Time Automation Controllers (RTAC) process SCADA measurements by connecting with intelligent electronic devices (IEDs) using DNP3, IEC 61850 GOOSE protocols, and analog inputs. Communication between the RTACs and the SCADA servers occurs via the DNP3 (Distributed Network protocol). The RTDS devices communicate with the SCADA control servers using the IEC 61850 and DNP3 protocols. A single RTAC module in the SEL-2240 Axion node serves the DNP3 protocol to enable situational awareness and wide-area system measurement in SCANVILLE.

The pattern of Light Emitting Diodes (LEDs) on the commercial protection and control hardware allows a viewer to visualize electrical activity and status of the equipment. The devices are deployed in a segmented network enclave, that is established using a programmable Virtual Local Area Network (VLAN) switch. They communicate with the substation control devices using hardwired connections (analog and digital inputs), and Ethernet communication is used for managing the hardware and other control communication.

2.1.2 Power Lab Testbed's Substations Component

ISAAC's PoT module replicates up to four power substations consisting of physical industrial control devices, such as IEDs, measurement units, and data concentrators. These devices are interfaced to the RTDS hardware to provide a complete control hardware loop, which aids in studying the impact of control events on the physical layer. The substation models are designed to be scalable for facilitating an increase of the RTDS electric power generation model's size and scope. The RTDS can model additional SCADA nodes internal communication through its Giga Transceiver Network Interface Card (GTNET).

ISAAC has four substations that are segmented into different VLANs. These four substations help emulate real-world power utility substations, which are geographically distributed. Each substation consists of the following:

1. A Schweitzer Engineering Labs (SEL) 3620 Ethernet Security Gateway, which serves as the substation's firewall to enable: secure connectivity between the substation internal network and the external SCADA network, audit trail provisioning, and IED password management.

2. A SEL-2740S Software Defined Network (SDN) Switch, for providing Ethernet communication and centralized traffic flow.

3. A SEL-5056 Software-Defined Network Flow Controller, to provide traffic engineering flow control for the SDN switch.

4. Two substations have SEL-411L Protection and Control System Relays, to enable: line current differential protection, breaker failure detection, and traveling-wave fault locator.

5. Two substations have SEL-487B Protection Relays, for providing busbar protection and breaker monitoring.

6. A SEL-2240 Axion, which provides a modular I/O control solution that consists of: SCADA remote terminal, fault recorders, IEC 61850 GOOSE concentrator, trip coil monitors, distributable Phasor Measurement Unit (PMU) serving IEEE C37.118.1a-2014 compliant synchrophasor data, event recorder, and SCADA data concentrator.

7. One SEL-3530 Real-Time Automation Controllers (RTAC). Additional relays can be placed in the substation as needed.

An SEL-2488 satellite synchronized network clock integrates the PoT to the Global Navigation Satellite System (GNSS). GNSS distributes precise time, coordinated with universal time (UTC), via multiple output protocols, including Inter-range Instrumentation Group-B (IRIG-B) and the Network Time Protocol version 4 (NTPv4) with an accuracy of about ±40 nanoseconds (ns) on an average and ±100ns at peak. Precise timing is provided to relays, IEDs, and PMUs. Precise timing is an important requirement for synchrophasor functionality. Additionally, the SEL-2241 RTAC module on the SEL-2240 Axion can serve synchrophasor data and act as a Phasor Data Concentrator (PDC). Functionalities of the PDC are to: 1) concentrate synchrophasor data from several PMUs that are compliant with IEEE C37.118 protocol; 2) time-tag and archive the data to create wide-area systems' measurement; and 3) provide situational awareness at the control center. Measurement signals from the outstation devices are processed by the automation controllers within the substation using DNP3 SCADA Protocol, for real-time information exchange using DNP3 SCADA protocol.

2.1.3 ISAAC's SCADA Control Component

A SCADA enterprise center, located in the SCANVILLE module, provides a facility for remote human monitoring and control of the outstation devices and the overall ISAAC testbed. To simulate a modern enterprise center, General Electric (GE) SCADA applications were installed on x64 server operating systems. The GE applications suite consists of the following: 1) GE iFIX SCADA, acting as SCADA master and a Human-Machine Interface (HMI) server; 2) GE Webspace, which facilitates advanced control and visualization capabilities; 3) GE Web HMI, a model-based HMI, that is used to improve situational awareness; and 4) GE Historian - for data collection, storage and aggregation of SCADA measurements. A Catapult DNP3 OPC [OLE (Object Linking and Embedding) Process Control (OPC)] driver was installed on the GE iFIX server, to provide control devices with an easy and reliable method to process SCADA-specific protocols. The OPC drivers also provides communication between master-slave device pairings. SCADA control actuation is triggered when an automation controller writes data to the OPC server. The OPC server updates the outstation device state with the actuator command if needed, to produce a state change in the electrical process of the RTDS devices. Such an OPC update can be conducted through either the intervention of a human operator or automatic SCADA data tags.

A highly visible, wall-mounted display is installed in the Power lab Testbed enterprise room, using an IRIG-B synchronization with SEL-3401 digital clock. The clock provides time with an accuracy of ±100ns. The SCADA servers are segmented into separate network enclaves, to ensure the enforcement of access control policies within ISAAC. The substation devices and the RTDS hardware are managed using an out-of-band management VLANs on a dedicated, Open Systems Interconnection model (OSI)

Layer-3 management switch.

2.1.4 ISAAC's Cyber Components

The cyber architecture of ISAAC depicts commonly used information technology and security components in critical infrastructure systems. The TCP/IP suite is used for wired network communication and the IEEE 802.3 based Ethernet protocol is used for wireless connectivity [Wireless connectivity is not available for ISAAC connected devices]. The RS-232 serial communication protocol is also used for inter-connectivity between some legacy control devices. Using networking devices is necessary for a SCADA network to establish a communication channel for the environment. A few substations use the Inter-Control-Center Protocol (ICCP), to facilitate data exchange over Wide Area Networks (WAN), between different utility control centers.

ISAAC consists of a variety of networking devices, which enable communication between power and cyber equipment, over a physically air-gapped communication channel. OSI Layer-3 switches are used to provide network routing. The routing decisions made by OSI Layer-3 switches are based on: 1) the source and destination addresses, and 2) Access Control Lists (ACLs). The Layer-3 switches also provide a reduction in broadcast domains through VLAN mechanisms. The Layer-3 switches interconnect the RADICL, SCANVILLE, PoT, and IRON networks. Atthe substation level, network firewalls, with stateful and deep packet inspection, provide secure network access to substation devices.

ISAAC's SCANVILLE module is capable of providing visualization data representing all instances of: SCADA servers, network VLANs, infrastructure management and automation applications. The visualization data can be used to conduct critical infrastructural security analytics research. SCANVILLE utilizes a set of security monitoring tools such as: Security Information and Event Monitoring (SIEM) and Network Intrusion Detection System (NIDS), to provide real-time security monitoring and data analytics.

Media Access Control Security (MACSec), an IEEE 802.1AE compliant security technology, is planned for encrypting the communication between the SCANVILLE, RADICL, PoT, and IRON. MACSec uses AES-256 bit ciphers, to provide secure communication for almost all types of traffic on Ethernet links, and it identifies and prevents external security threats such as denial of service, intrusion, man-in-the-middle, and playback attacks [15]. [This MACSec approach has been implemented between the testbed switches.]

Chapter 3: Utilization and Security Considerations for ISAAC

In this chapter, we discuss the current and potential utilization of the testbed. We also outline the security considerations employed to ensure the Confidentiality, Integrity, and Availability (CIA) of devices installed within the testbed infrastructure.

3.1 ISAAC's Current Utilization

The Idaho CPS Smart Grid Cybersecurity Testbed (ISAAC) components are fully implemented. The simulation devices, substation components and industrial SCADA software are deployed in the Power lab Testbed (PoT). The Securing Cyberphysical systems ANalytics, Visualization, IoT, and machine Learning Laboratory of Enquiry (SCANVILLE) and Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL) are also functional with ongoing efforts to inter-connect the laboratories in a federated architecture, using a high-speed network channel. While the ongoing inter-laboratory integration is being finalized, researchers leverage ISAAC to conduct cybersecurity research by using a localized server infrastructure within PoT. Experiments to validate several research works have been conducted using ISAAC's current implementation. [This connectivity has been implemented after publication].

Amarasinghe et al. created a microgrid simulation and a cyber-network, which is connected to the microgrid [16]. They used ISAAC's SCADA, visualization and cybersecurity capabilities to generate experimental results. The experiments dealt with analysis of network data and included collecting packet streams from ISAAC's communication channel, during a Denial of Service (DoS) attack on ISAAC. As a result of the experiments, a machine-learning-based framework for data-driven health monitoring of CPS was also created [16].

Penkey et al. created a system model containing distributed resources, which are connected to a utility grid [17]. For creating their model, Penkey et al. used an earlier implementation of ISAAC-PoT's simulation component, automation controller, and relays. Their model also analyzed the capability of a utility system, when handling severe contingencies such as: extreme weather, natural disasters, major generation failure, loss of transmission lines, and cyber-attacks [17].

ISAAC's adaptability was demonstrated by Chilukuri et al., who modeled a thermal power-generating station using an earlier version of ISAAC's simulation and PoT components [18]. Their model also aimed to improve the reliability and security of the generation station protection schemes. This was achieved by proposing an approach to enhance the performance and coverage of backup protection schemes, using sampled values of the IEC 61850 standard. This model also introduced a synchronism element checking mechanism to address the challenges involved in generator protection schemes [18].

A number of cybersecurity research projects are ongoing, which are slated to make extensive use of ISAAC's capabilities. These research projects are related to the improving resiliency and risk assessment of CPS, detection of stealth cyber-attacks against state estimation, and application of machine learning to detect false data injection in CPS [6].

3.2 ISAAC's Potential Utilization

3.2.1 Real-Time Cyber Attack Simulation Using RADICL

RADICL facilitates hands-on teaching and research in the areas of information assurance, cyber-defense, and modern computing platforms and networks [19]. The laboratory provides a secure and contained environment that facilitates forensic investigation, penetration testing, and experimental analysis, aimed at securing critical infrastructure. As such, RADICL has the ability to strengthen critical infrastructure by enabling conduct of experimental, realistic, and sophisticated cyber-attacks against ISAAC. In addition, RADICL enables researchers to develop realistic red team versus blue team exercise environments that depict practical threat scenarios. RADICL also facilitates educational teaching exercises for critical infrastructure cyber-defense classes

3.2.2 Visualization and Security Analytics using SCANVILLE

SCANVILLE provides real-time visualization data for the overall ISAAC testbed. SCANVILLE is vital for emulating a real-world enterprise center of a critical infrastructure utility. SCANVILLE provides a human operator with comprehensive overall system data, that can be used to conduct security prognostics. Visualization data can also be used to: 1) monitor the overall system for device and environmental well-being; 2) detect real-time attacks; and 3) identify trends, to support better decision making.

SCANVILLE consists of: 1) security and automation control monitoring screens; 2) networking equipment that are typically found in an automation control utility; and 3) a monitoring and visualization platform. The human operator of SCANVILLE can assess and regulate violations when simulating threats and adversarial incidents. Such functionality can be used to understand the "under-attack" behavior and response of critical infrastructure and its' networks. Visualization and security analytic tools of SCANVILLE module include: vulnerability scanner, SIEM, Lightweight Directory Access Protocol (LDAP) server, Elasticsearch, Logstash Kibana, Intrusion Detection System (IDS), transmitters, and monitoring screens.

3.2.3 ISAAC's Experimental Capabilities

ISAAC facilitates building capacity in the area of developing practical and realistic CPS security research. ISAAC also provides a realistic emulation environment for comparative testing and validation of different CPS security research approaches. ISAAC can be used to demonstrate and investigate vulnerabilities, exploit them, and assess their impact in a realistic environment that emulates a real-world power utility's SCADA network. ISAAC also facilitates an experimental environment that can be used in a CPS cyber-defense training curriculum. Examples of teaching usage are: 1) vulnerability assessment for vendor-specific devices; 2) threat modeling and risk analysis of possible cyber-attacks; 3) intrusion detection training; and 4) learning forensic techniques for analyzing the aftermath of an attack on a real time distribution system.

Some examples of experimental capabilities provided by ISAAC are: 1) simulation of holistic CPS organizational models, such as METICS Acme Corp. model [9]; 2) the simulation of real-world attack case studies, such as false data injection attacks on state estimation [20] and replay attacks; 3) simulation of best-effort damage mitigation models [21]; and 4) security evaluation of power grid using the RTDS.

3.2.4 Remote Utilization

We have also completed plans and designs to enable us to expand the ISAAC testbed to other branch campuses across the State of Idaho. This connection will be by means of an OSI layer 2 Tunneling protocol on the Idaho Regional Optical Network (IRON). IRON is a high-speed fiber-optic backbone that facilitates advanced interconnectivity and networking amongst public institutions in Idaho and other Northern Tier States [22]. IRON is currently expanding its backbone link capacity to 100Gbps. For ISAAC, the current plan is that all cross laboratory VLANs will be mapped one-to-one into a virtual VLAN in IRON. This expansion may also enable the testbed to grow by adding laboratories at other academic and research institutions across the State of Idaho and the Northwest.

Chapter 4: Experiment and Formal Model Validation

In this chapter, we discuss an attack scenario-based validation of ISAAC using a 21 bus microgrid system, a simulated infrastructure scenario and experimental attack cases.

4.1 Experimental Validation Using an Attack Scenario

ISAAC uses a Real Time Digital Simulator (RTDS) to create a real-time virtual power system simulation environment which aids in studying the impact of control events on the physical layer. To explain the working of the testbed, we present a single line diagram of a 21 bus microgrid system with breakers on connected lines. The microgrid system simulates the power flow, including disturbances, and transmits information using Distributed Network Protocol 3 (DNP3). The microgrid system is simulated on the RTDS and connected to external devices through analog and digital channels to achieve hardware-in-the-loop simulations. The grid has two hydro generators, which are modeled using RTDS library components. These components include the IEEE type 1 Excitation system, IEEE type 1 Governor system, and several voltage-behind-reactance modeled sources to supply energy to the loads. Figure 4.1 shows the single line diagram of the 21-bus microgrid system.

To create a holistic hardware-in-the-loop emulation, several components have to be simulated as a close-enough simplified model to save resources for the critically required components such as DNP3 block, transformers, breakers, and various buses as nodes. The required components have been adjusted to meet the resource limitations, and allow later introduction of new components in the system. Since the data generated by the power system must be sent over the networking devices, the RTDS GTNET (Gigabit Transceiver Network Interface) card is used. We have created and configured a DNP3 transcription created on set parameters in a built in component in the RSCAD (Realtime Simulated and Computer Aided Design) draft to match network parameters of the connected Ethernet interfaces.

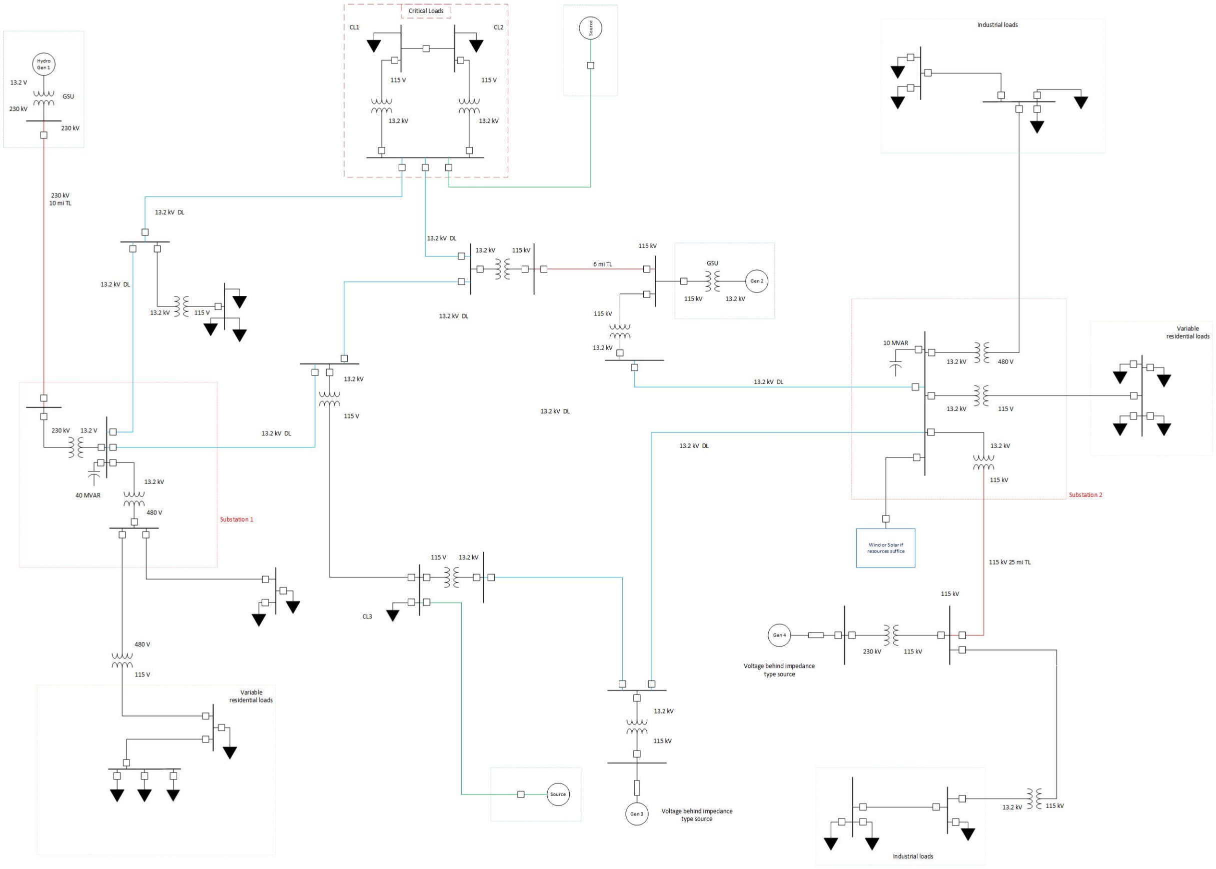


Figure 4.1: Single-Line Diagram of ISAAC's 21-Bus Microgrid Model.

The DNP3 block is configured to act as a master-slave system, to which unsolicited polls are sent by the microgrid controller. A RTAC (Real-Time Automation Controller) device, acting as a slave-server, receives the data from the RTDS. A DNP points list is created for all the variables available in the power system model and shared between the intercommunicating devices. These variables are then mapped to the sources from components where the data is captured for the simulated model in the microgrid controller. Table 4.1 shows an excerpt of the points list created on the RTAC, to map a few of the needed variables for the physical data.

Table 4.1: DNP3 Points List Map For Intercommunicated Variables

S/N	Client DNP Point	Server Map	Point Name
87	Client_DNP.AI_00087	Map_DNP.AI_00087	S1) N49
88	Client_DNP.AI_00088	Map_DNP.AI_00088	S1) N50
89	Client_DNP.AI_00089	Map_DNP.AI_00089	S1) N51

We validate[d] the ISAAC testbed by performing attack scenario-based experiments. Due to manpower and access time restrictions, an exhaustive analysis of all possible cyber-attacks is not feasible. Therefore, we demonstrate an attack scenario that is commonly encountered by CPS in the real world. The attack scenario consists of two experiments: a network reconnaissance campaign, followed by an Address Resolution Protocol (ARP) poisoning attack. In our scenario, we play the role of an attacker.

Our attack scenario adopts the following threat model: an outside attacker has gained remote access to the microgrid communication network using a spear phishing attack on company employees. The attacker is able to compromise a company employee and has access to the employee's remote authentication credentials. The attacker gains access to microgrid's engineering console by pivoting the compromised employee's credentials through the corporate network. Through the engineering console, the attacker obtains access to the SCADA servers and substation control network. Figure 4.2 depicts a visual representation of our attack scenario.

4.1.1 Experiment 1: Network Reconnaissance Campaign

In a CPS environment, an attacker can capture and analyze packets, including ones from the control network. Through packet analysis, the attacker can map a network and gather information about devices connected into the network. The attacker is then able to analyze the devices and find a device which is vulnerable to exploitation. Network reconnaissance and other related activities are important to carry out an attack. Reconnaissance also informs an attacker about the potential reward of successfully executing an attack.

In the first stage of this experiment, we record network traffic from multiple vantage points on the corporate network. By sniffing network packets of the captured traffic, the attacker is able create a list of vulnerable hosts and protocols, which can be used in subsequent attack stages. In the second stage of this experiment, the attacker scans for vulnerable live services running on vulnerable hosts. The attacker performs these scans by launching a series of NMap (Network Mapper) scans. The attacker also captures network-based operational control data to passively analyze the network layout.

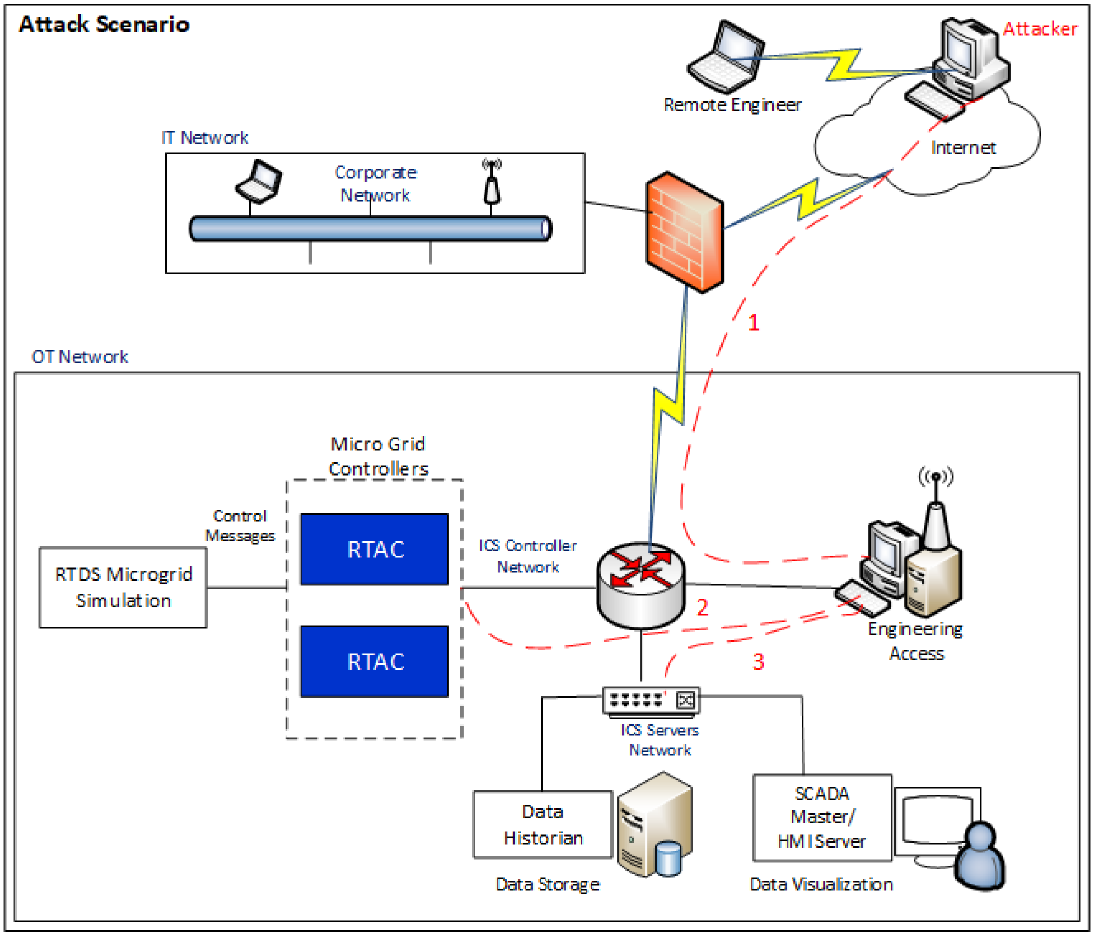


Figure 4.2: Visual Representation of the Attack Scenario Used to Validate ISAAC Testbed.

Results: The attacker was able to understand the topology of operational control network. Passive data containing protocol messages and network activity logs were collected. The attacker was also able to ascertain valuable CPS operational data from the control network's data.

4.1.2 Experiment 2: Address Resolution Protocol (ARP) Poisoning Attack

Devices that need to communicate on an Ethernet network broadcast Address Resolution Protocol (ARP) queries to other devices for obtaining their MAC (Media Access Control) addresses. In this experiment, an attacker injects malicious ARP packets in the network.

Using Ettercap, we launch a man-in-the-middle attack and disrupt the communication on the network. The disruption is carried out by sending ARP requests/replies to devices in the microgrid network, which poisons their ARP cache. We perform the same attack on the control network, the SCADA network, and other critical networks. Once all the ARP caches are poisoned, the controllers send their packets to us. We can then, in turn, can carry out further attacks or modification on the packets.

Results: The attacker was successful in sending malformed packets to the devices connected to the compromised networks. We are also successful in blocking packet flow to components, like the Data Historian. As shown in Figure 4.3, the Historian stopped receiving data after we executed the ARP attacks. In addition, the SCADA Human-Machine Interface (HMI) also displayed no data during the attack duration. Using a packet sniffer, the attacker observed several retransmission packets on our attack-machine during the attack phase. The attacker was also successful in using ARP poisoning to confuse the measurement processing and storing features from field devices to the HMI. Normal operations resumed soon after we stopped the attacks. Recreating similar attacks on real world CPS networks could result in serious catastrophic consequences, such as: economic loss, damage to equipment, or a local blackout.

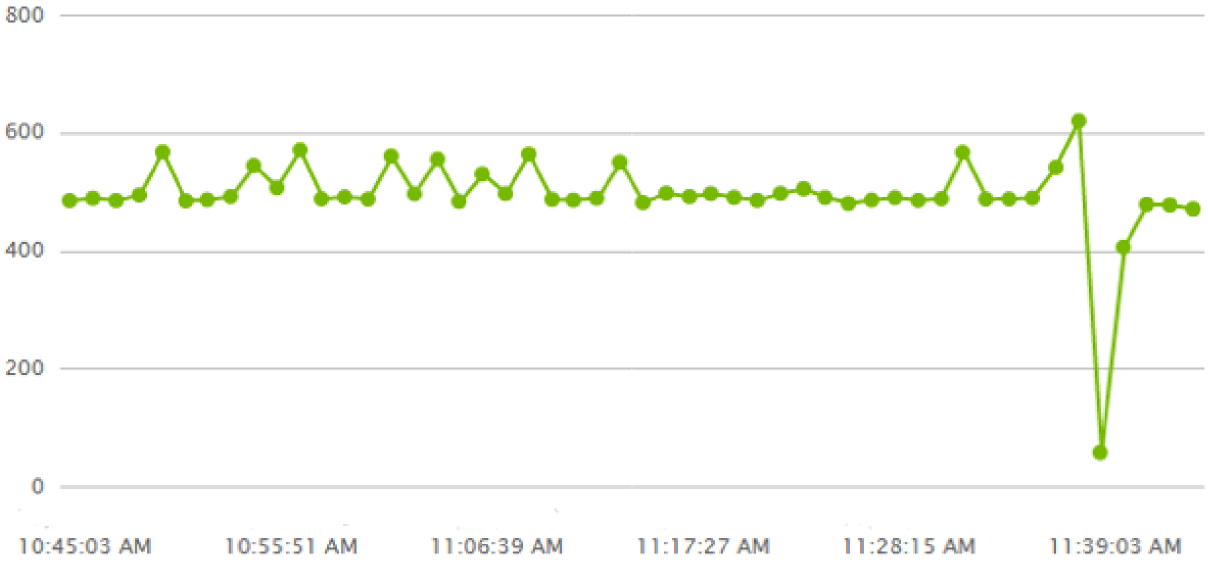


Figure 4.3: Historian Receive Rate During an ARP Attack.

In addition to our attack scenario-based validation discussed here, ISAAC has also been previously used for CPS security research and education programs [16], [18], [17] . While cybersecurity experiments are considered important, it is worthwhile to note that security is not the only objective of the ISAAC testbed. ISAAC is planned to be utilized as a platform to: 1) conduct multiple CPS research programs (as discussed in Section 1.3) and 2) teach hands-on CPS related concepts.

4.2 Formal Validation Using the Purdue Reference Model

In this section, we map the ISAAC testbed with the Purdue Model for Control Hierarchy Logical Framework (Purdue reference model) [23].

The Purdue Model for Control Hierarchy is an industry adopted model developed by the International Society of Automation (ISA-99) from the Purdue Enterprise Reference Architecture [23]. It is a standard benchmark for CPS architectures using logically segmented zones to secure the enterprise and the CPS network zones to form an integrated enterprise architecture. The model consists of six levels which are: 1) Level 5: Enterprise network; 2) Level 4: Site business and logistics; 3) Level 3: Site operations; 4) Level 2: Area supervisory control; 5) Level 1: Basic control; 6) Level 0: The process.

ISAAC was designed as a multi-level, tier-based, and hierarchical smart grid testbed to meet all the requirements of the Purdue reference model. When mapped to the model, ISAAC consists of the following architectural layers: Level 0: simulated instrumentation field devices; Level 1: protection and control devices; Level 2: substation supervisory control; Level 3: control center and supervisory control applications with management networks; Levels 4 and 5: System operations and corporate IT infrastructure, respectively. ISAAC's architectural layers enable us to simulate several realistic attack-defend scenarios to study smart grids at each level and to observe the corresponding impact of control events on the physical layer. Figure 4.4 shows the mapping of ISAAC testbed to the Purdue reference model.

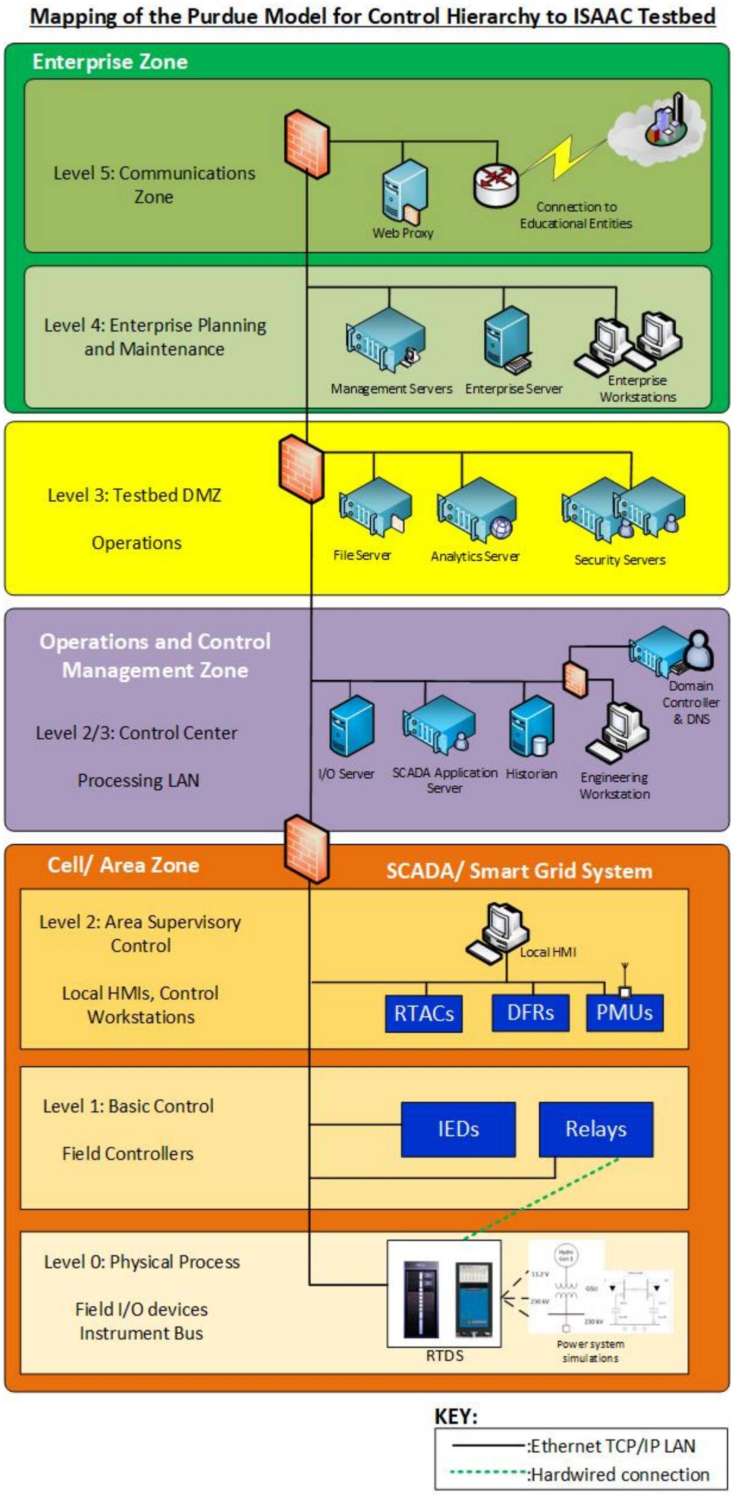


Figure 4.4: Mapping Between ISAAC Testbed and the Purdue Reference Model.

Chapter 5: Design and Architecture Enhancements

The Confidentiality, Integrity, and Availability (CIA) of devices installed in the Idaho CPS Smart Grid Cybersecurity Testbed (ISAAC) network plays a significant role in ensuring the overall security of the ISAAC network against cyber attacks. This section summarizes ISAAC's security considerations. In this chapter, we outline design and architecture enhancements to ensure the CIA triad for the testbed and its environment in two sections: i) implemented enhancements; and ii) recommended enhancements.

5.1 Implemented Design Enhancements

5.1.1 Network Segmentation and Isolation

To provide design-level defense, ISAAC's network was classified into sub-networks. Sub-networking creates functionally segmented and isolated networks. Virtual Local Area Networks (VLANs) and De-Militarized Zones (DMZ) with stringent access control policies were created to improve security, performance, and create better access control. Power lab Testbed (PoT) substations, Real TIme Digital Simulator (RTDS) hardware, Reconfigurable Attack-Defend Instructional Computing Laborator (RADICL), and PoT servers each can be segmented into separate VLANs so that researchers can also look at poorly implemented examples. Each VLAN has an explicitly-defined access control list. To prevent exfiltration of experimental research activities to other networks, we deploy containment using physical and logical link isolation. The isolated containment results in a virtually air-gapped or air-locked ISAAC environment, where communication is highly controlled.

We implemented PFSense, a network packet filtering firewall and router based on FreeBSD, to enforce logical segmentation of experiments. The router provides features such as load balancing, threat management and many more. It segments ISAAC substations, RTDS, Supervisory Control and Data Acquisition (SCADA) and Security servers into distinct logical VLANs and facilitates the segmentation and isolation of experiments. Figure 5.1 shows the experiment isolation architecture for ISAAC.

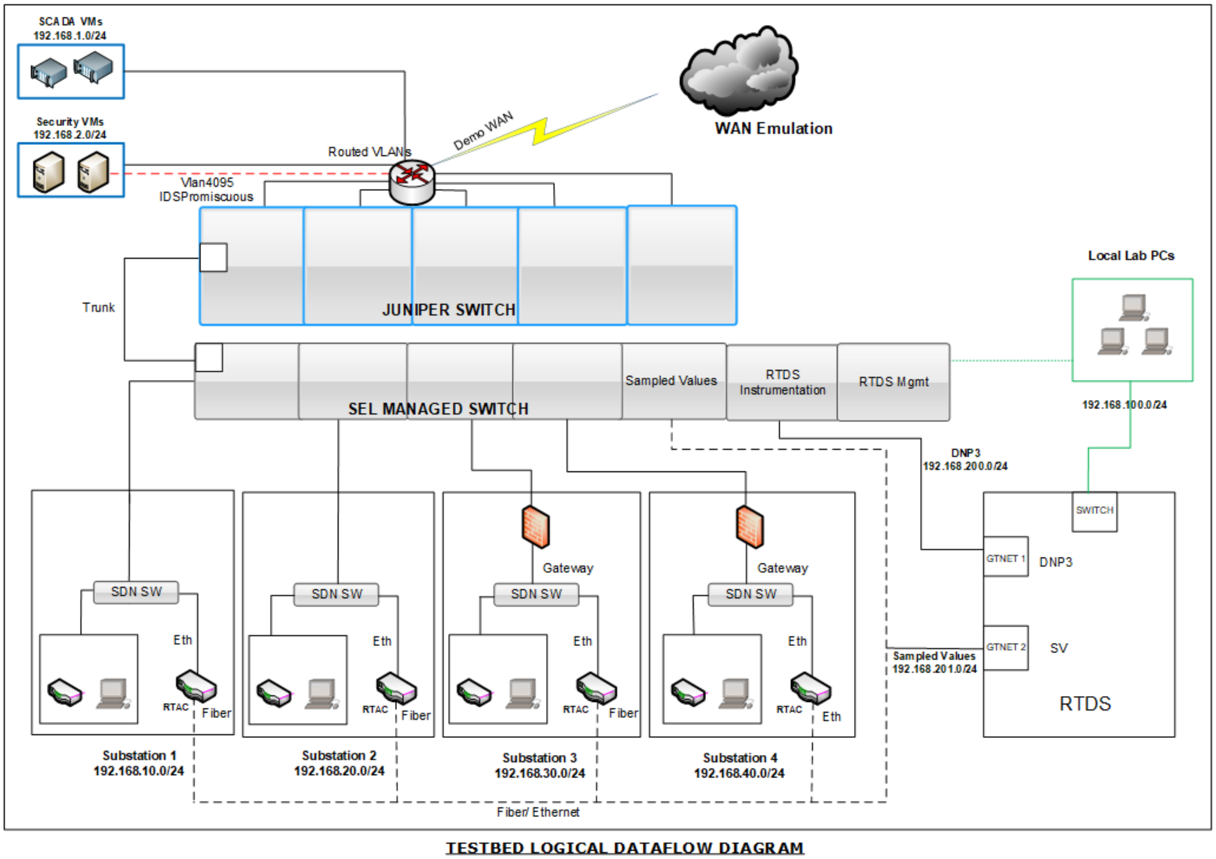


Figure 5.1: Diagram of Logical Isolation of Substations Using a Network Router.

In Figure 5.2, we outline the detailed experiment isolation architecture currently in use within ISAAC's environment. We ensure the deployment of a unique packet filter per experiment to facilitate re-configurable and contained set of unique experiment.

5.1.2 Firewalls

To provide perimeter-level defense, firewalls are widely deployed. ISAAC's firewalls also prevent direct egress and ingress connections between an external network and the experimental environment. Stringent access control lists are configured between communicating devices to prevent exfiltration and infiltration of unauthorized external connections.

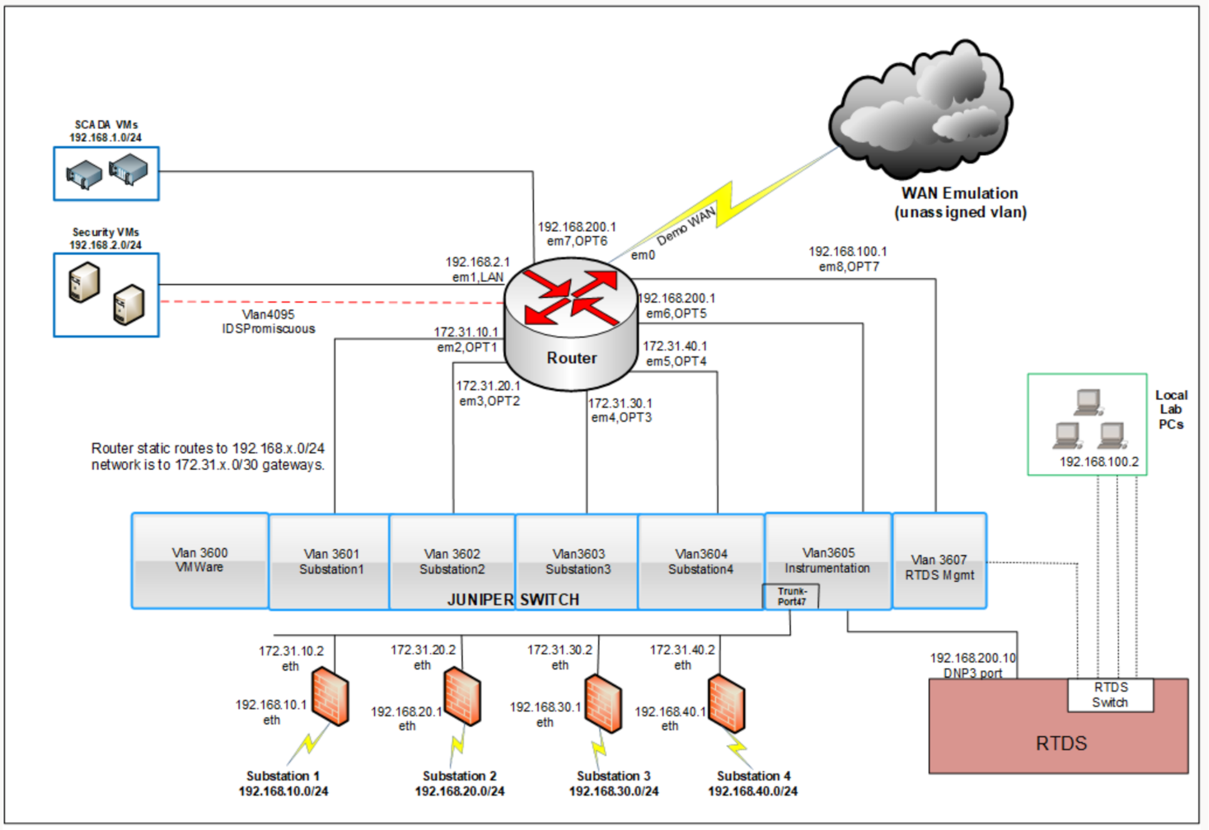
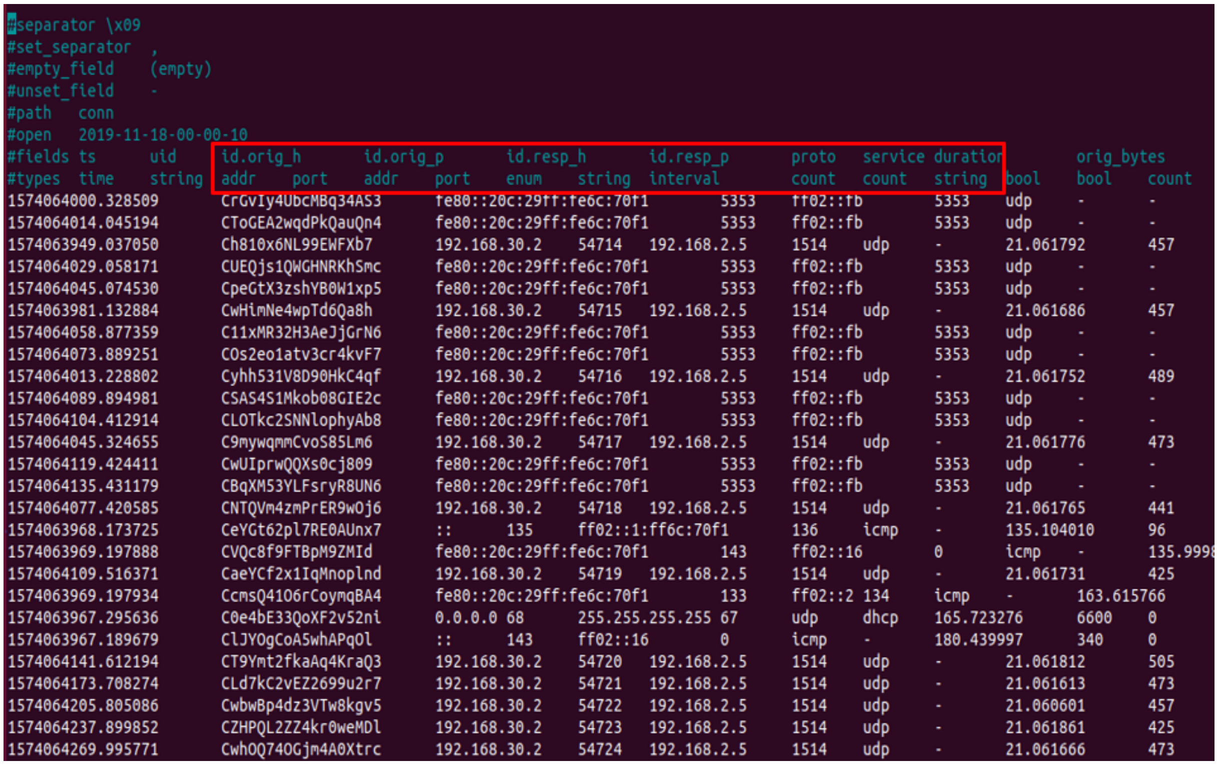


Figure 5.2: Diagram of Experiment Isolation Using a Network Router.

5.1.3 Intrusion Detection

To provide real-time security and monitoring, an IDS is deployed in transparent mode. We implemented Zeek IDS cluster deployed in cluster mode. The IDS integrates to the network switches through port mirroring and Switched Port Analyzer (SPAN). Using an IDS, network usage policies can be enforced by analyzing a copy of all network packets. IDS can also be used to addresses various attack vectors from real cyber-attacks that may target SCADA operating systems, protocols, and networks within ISAAC. Strict NIDS rules are implemented to detect anomalies between critical network zones and the Internet. Through the use of NIDS, experiments that try to exceed their authorized network scope can be immediately stopped and further review would be conducted to re-validate such experiments. Figure 5.3 shows a sample connection log from the IDS.



```
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   conn
#open   2019-11-18-00-00-10
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   service duration        orig_bytes
#types  time    string  addr    port    addr    port    enum    string  interval        count   count   string  bool    bool    count
1574064000.328509       CrGvIy4UbcMBq34AS3      fe80::20c:29ff:fe6c:70f1        5353    ff02::fb        5353    udp     -       -
1574064014.045194       CToGEA2wqdPkQauQn4      fe80::20c:29ff:fe6c:70f1        5353    ff02::fb        5353    udp     -       -
1574063949.037050       Ch810x6NL99EWFXb7       192.168.30.2    54714   192.168.2.5     1514    udp     -       21.061792       457
1574064029.058171       CUEQjs1QWGHNRKhSmc      fe80::20c:29ff:fe6c:70f1        5353    ff02::fb        5353    udp     -       -
1574064045.074530       CpeGtX3zshYB0W1xp5      fe80::20c:29ff:fe6c:70f1        5353    ff02::fb        5353    udp     -       -
1574063981.132884       CwHimNe4wpTd6Qa8h       192.168.30.2    54715   192.168.2.5     1514    udp     -       21.061686       457
1574064058.877359       C11xMR32H3AeJjGrN6      fe80::20c:29ff:fe6c:70f1        5353    ff02::fb        5353    udp     -       -
1574064073.889251       COs2eo1atv3cr4kvF7      fe80::20c:29ff:fe6c:70f1        5353    ff02::fb        5353    udp     -       -
1574064013.228802       Cyhh531V8D90HkC4qf      192.168.30.2    54716   192.168.2.5     1514    udp     -       21.061752       489
1574064089.894981       CSAS4S1Mkob08GIE2c      fe80::20c:29ff:fe6c:70f1        5353    ff02::fb        5353    udp     -       -
1574064104.412914       CLOTkc2SNNlophyAb8      fe80::20c:29ff:fe6c:70f1        5353    ff02::fb        5353    udp     -       -
1574064045.324655       C9mywqmmCvoS85Lm6       192.168.30.2    54717   192.168.2.5     1514    udp     -       21.061776       473
1574064119.424411       CwUIprwQQXs0cj809       fe80::20c:29ff:fe6c:70f1        5353    ff02::fb        5353    udp     -       -
1574064135.431179       CBqXM53YLFsryR8UN6      fe80::20c:29ff:fe6c:70f1        5353    ff02::fb        5353    udp     -       -
1574064077.420585       CNTQVm4zmPrER9wOj6      192.168.30.2    54718   192.168.2.5     1514    udp     -       21.061765       441
1574063968.173725       CeYGt62pl7RE0AUnx7      ::      135     ff02::1:ff6c:70f1       136     icmp    -       135.104010      96
1574063969.197888       CVQc8f9FTBpM9ZMId       fe80::20c:29ff:fe6c:70f1        143     ff02::16        0       icmp    -       135.9998
1574064109.516371       CaeYCf2x1IqMnoplnd      192.168.30.2    54719   192.168.2.5     1514    udp     -       21.061731       425
1574063969.197934       CcmsQ4106rCoymqBA4      fe80::20c:29ff:fe6c:70f1        133     ff02::2 134     icmp    -       163.615766
1574063967.295636       C0e4bE33QoXF2v52ni      0.0.0.0 68      255.255.255.255 67      udp     dhcp    165.723276      6600    0
1574063967.189679       ClJYOgCoA5whAPqOl       ::      143     ff02::16        0       icmp    -       180.439997      340     0
1574064141.612194       CT9Ymt2fkaAq4KraQ3      192.168.30.2    54720   192.168.2.5     1514    udp     -       21.061812       505
1574064173.708274       CLd7kC2vEZ2699u2r7      192.168.30.2    54721   192.168.2.5     1514    udp     -       21.061613       473
1574064205.805086       CwbwBp4dz3VTw8kgv5      192.168.30.2    54722   192.168.2.5     1514    udp     -       21.060601       457
1574064237.899852       CZHPQL2ZZ4kr0weMDl      192.168.30.2    54723   192.168.2.5     1514    udp     -       21.061861       425
1574064269.995771       CwhOQ74OGjm4A0Xtrc      192.168.30.2    54724   192.168.2.5     1514    udp     -       21.061666       473
```

Figure 5.3: Screenshot of Connection Logs From Zeek IDS.

5.1.4 Air-gaps and Regular Updates

ISAAC's network segments are virtually air-gapped from the enterprise network of the University of Idaho. The infrastructure of SCANVILLE, RADICL, and PoT modules are currently manually maintained with the latest security updates. A dedicated substation VLAN segment is also used for testing firmware updates, prior to deploying such updates on ISAAC devices.

5.2 Recommended Design Enhancements

5.2.1 Web Proxy

For patch management and other critical services requiring Internet connectivity, a web proxy with Internet filtering, antivirus, antispam, and statistic engine features is recommended to be deployed in reverse proxy mode. The web proxy would provide controlled and restricted Internet access. Through its update caching enforcement feature, the web proxy server can fetch the necessary security updates from the Internet and locally distribute such updates to ISAAC servers and endpoints. The web proxy eliminates a need to directly expose ISAAC to the Internet and implements the air-lock or virtual air-gap.

5.2.2 Node Re-Imaging

All of RADICL's virtual machine instances and endpoint nodes are re-imaged upon completion of experimental activities. The re-imaging process includes formatting and deallocation of operating system files and data on endpoint nodes, which prevents reuse of data. New images from virtual machine templates are re-deployed for subsequent experiments. We recommend a similar re-imaging strategy for critical components of ISAAC that may be contaminated after an infectious experiment.

5.2.3 Planned ISAAC Security Assessment

A security assessment and evaluation of ISAAC should be planned to verify acceptability of ISAAC's security threshold. Potential assessors/evaluators could be Idaho National Labs (INL) or Pacific Northwest National Labs (PNNL).

Chapter 6: Related Work

Cyber-physical testbeds are becoming an important part of Cyber-Physical Systems (CPS) security studies and pre-production deployment evaluation. There exist several testbeds that are focused on cybersecurity of Supervisory Control and Data Acquisition (SCADA) systems. This section highlights testbed environments that have been developed for evaluating the SCADA part of a CPS organization.

The United States National SCADA Testbed (NSTB) program facilitates experimental research and discovery, and development of methodologies to address energy sector's critical security vulnerabilities [24]. The NSTB program is a collaboration and consists of several laboratories. These partner laboratories offer expertise to secure SCADA and distributed control systems. The NSTB program also offers testing and research environments, examples of which are: the Idaho Critical Infrastructure Test Range, the Pacific Northwest Electricity Infrastructure Operations Center, and the Sandia Center for SCADA Security. Such environments provide next-generation testbeds, including the state-of-the-art visualization and modeling tools. The Idaho National Laboratory's (INL) Critical Infrastructure Test Range, a part of the NSTB, includes an electric grid and cybersecurity testbed with 15 Real Time Digital Simulator (RTDS) racks to simulate a real-world power grid [25].

Ashok et al. describe the system architecture of a security testbed using simulation data derived from Internet Scale Event and Attack Generation Environment (ISEAGE) [26]. Benzel et al. developed and evaluated the experimental capability of the DETER testbed [27]. DETER consists of several experimental nodes built with Emulab suite and operates in two-clustered federated sites at University of Southern California and University of California at Berkeley. Biswas et al. introduce the development of a smart grid testbed for PMU and PDC testing [28]. Biswas et al.'s testbed implements industry standard SCADA software and devices and it is used for real world utility-security evaluation. Davis et al. describe a testbed developed using the PowerWorld power simulation and the Realtime Immersive Network Simulation Environment (RINSE) suite [29]. Davis et al.'s testbed simulates parallel large-scale networks and is a part of the Trustworthy Cyber Infrastructure for the Power Grid (TCIP) consortium.

They provided attack descriptions and demonstrate the vulnerability of network clients to a Distributed Denial of Service (DDoS) attack.

Benzel et al. present the DETER (cyber DEfense Technology Experimental Research) testbed infrastructure and its experimental program for conducting cybersecurity research [27]. Ashok et al. describe the system architecture and experimental capabilities of a security testbed using cyber attack simulations, derived from Internet Scale Event and Attack Generation Environment (ISEAGE) [26]. Koganti et al. present a virtual testbed, which can simulate man-in-the-middle attacks against an CPS [30]. Jillepalli et al. present a stockholder-based risk assessment model for CPS security [3].

Korkmaz et al. also describe an industrial control systems security testbed and propose a couple of experiments [31]. The experimental focus of Kormaz et al.'s testbed is on time delay attacks.

The Idaho CPS Smart Grid Cybersecurity Testbed (ISAAC) stands out from the other testbeds because of its capability: 1) to simulate of real cyber attacks using the Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL); 2) to provide an integrated visualization and security analytics tools using the Securing Cyberphysical systems ANalytics, Visualization, IoT, and machine Learning Laboratory of Enquiry (SCANVILLE); and 3) to provide distance collaboration and learning facility with multiple geographically distributed research and educational entities, using the Idaho Regional Optical Network (IRON). Another distinctive feature of ISAAC is that its design considers both, research and teaching, as points of focus.

Chapter 7: Future Work

The Idaho Cyber Physical System (CPS) Smart Grid Cybersecurity Testbed (ISAAC) testbed is fully functional except the integration to Idaho Regional Optical Network (IRON). There are few technology implementation, policies and procedures that need to be implemented or created in order for it to reach its full potential and usage.

We intend to integrate the testbed to the Idaho Regional Optical Network (IRON) to facilitate the use of the testbed by other campuses of the University of Idaho. Efforts are also ongoing to define security policies for data management: on-boarding, processing, collection and sharing of data; and testbed utilization policies. We also intend to define procedures for: i) experiment setup and teardown; ii) identity management and access control; and iii) testbed modification for experimental use-cases and improvements; iv) exporting data for external collaboration; and v) secure access for remote research collaboration.

We also proposed a few design enhancements highlighted in Section 5.2. The enhancements include the use of: i) web proxy for security updates and internet access; ii) node re-imaging for containment and device refresh; and iii) planned security assessment to verify acceptability of ISAAC's security threshold against secure architectural design principles and threat assessment.

—-

Chapter 8: Summary and Conclusions

Cyber Physical Systems (CPSs) are increasingly becoming attractive targets for multiple threat actors. Creation of secure CPS involves practical deployment of cutting edge CPS security research results. To do that, CPS research must be performed, tested and validated on a real-world CPS environment. Cyber-physical testbeds for CPS are becoming increasingly necessary to analyze and secure CPS organizations. These testbeds need to be comprehensive enough to simulate realistic attack-defend scenarios. ISAAC, the Idaho CPS Smart Grid Cybersecurity Testbed, is one such comprehensive testbed.

In this thesis, we discussed the limitations of being able to validate and test research on real-world CPS utilities. We presented the design, architecture and functional explanations of ISAAC: Idaho CPS Smart Grid Cybersecurity Testbed, an environment which emulates a realistic power utility. The ISAAC modules and components are fully implemented and functional while the inter-laboratory integration is on-going.

Validating the testbeds with realistic experiments and a formal reference model is just as necessary as constructing the testbed. We mapped ISAAC testbed to the Purdue reference model. We also presented a validation of ISAAC testbed with an experimental attack-scenario. Our results showed that ISAAC has the capability to emulate realistic scenarios. We hope that the ISAAC testbed will help the CPS community in analyzing and subsequently, securing their organizations against cyber-attacks.

Finally, we discussed the security considerations involved in the design enhancement and build process of ISAAC. We have presented current and potential utilization areas of ISAAC. We also discussed similar related projects and discussed the differences between these related works and ISAAC. When fully integrated, ISAAC will enable CPS research and educational capacity at locations across the State of Idaho.

References

[1] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A.-R. Sadeghi, M. Maniatakos, and R. Karri, “The cybersecurity landscape in industrial control systems,” *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1039–1057, May 2016. [Online]. Available: https://doi.org/10.1109/JPROC.2015.2512235

[2] C.-C. Sun, C.-C. Liu, and J. Xie, “Cyber-physical system security of a power grid: State-of-the-art,” *Electronics*, vol. 5, Jul 2016.

[3] A. A. Jillepalli, F. T. Sheldon, D. Conte de Leon, M. A. Haney, and R. K. Abercrombie, “Security management of cyber physical control systems using NIST SP 800-82r2,” in *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, Jun 2017, pp. 1864–1870. [Online]. Available: https://doi.org/10.1109/IWCMC.2017.7986568

[4] The Department of Homeland Security of the United States of America, “Critical infrastructure sectors,” Online, Nov 2018. [Online]. Available: https://www.dhs.gov/critical-infrastructure-sectors

[5] C. Glenn, D. Sterbentz, and A. Wright, “Cyber threat and vulnerability analysis of the u.s. electric sector,” Tech. Rep., Dec 2016. [Online]. Available: https://doi.org/10.2172/1337873

[6] A. A. Jillepalli, D. Conte de Leon, M. Ashrafuzzaman, Y. Chakhchoukh, B. K. Johnson, F. T. Sheldon, J. Alves-Foss, P. Tosic, and M. A. Haney, “HESTIA: Adversarial modeling and risk assessment for CPCS,” in *2018 14th International Wireless Communications and Mobile Computing Conference (IWCMC)*, Jun 2018, pp. 226–231. [Online]. Available: https://doi.org/10.1109/IWCMC.2018.8450297

[7] Symantec Corporation, “2018 internet security threat report,” Online, Mar. 2018. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

[8] Cisco Systems, Inc., “Cisco 2018 annual cybersecurity report,” Online, Feb 2018. [Online]. Available: https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf

[9] A. A. Jillepalli, D. Conte de Leon, B. K. Johnson, Y. Chakhchoukh, I. A. Oyewumi, M. Ashrafuzzaman, F. T. Sheldon, J. Alves-Foss, and M. A. Haney, "METICS: A holistic cyber physical system model for ieee 14-bus power system security," in *2018 13th International Conference on Malicious and Unwanted Software (MALCON)*, oct 2018. [Online]. Available: https://doi.org/10.1109/MALWARE.2018.8659367

[10] A. A. Jillepalli, D. Conte de Leon, I. A. Oyewumi, J. Alves-Foss, B. K. Johnson, C. L. Jeffery, Y. Chakhchoukh, M. A. Haney, and F. T. Sheldon, "Formalizing an automated, adversary-aware risk assessment process for critical infrastructure," in *2019 3rd IEEE Texas Power and Energy Conference (TPEC)*, Feb 2019, pp. 1–6. [Online]. Available: https://doi.org/10.1109/TPEC.2019.8662167

[11] P. Ackerman, *Industrial Cybersecurity.* Packt Publishing, 2017.

[12] S. Caltagirone, P. Ortman, S. Melton, D. Manz, K. King, and P. W. Oman, "Design and implementation of a multi-use attack-defend computer security lab," in *Proceedings of the 39th Hawaii International Conference on System Sciences (HICSS-39)*, vol. 9. Kauai, Hawaii, U.S.A.: IEEE Computer Society, Jan 2006, p. 220c. [Online]. Available: https://doi.org/10.1109/HICSS.2006.115

[13] RTDS Technologies, "Real time digital power system simulator," Online, Dec 2019. [Online]. Available: https://www.rtds.com

[14] "14 Bus Power Flow Test Case," https://www2.ee.washington.edu/research/pstca/pf14/pg_tca14bus.htm, Apr 2018.

[15] "ISO/IEC/IEEE international standard for information technology – telecommunications and information exchange between systems – local and metropolitan area networks – part 1ae: Media access control (MAC) security - AMENDMENT 2: Extended packet numbering." [Online]. Available: https://doi.org/10.1109/ieeestd.2015.7457578

[16] K. Amarasinghe, C. Wickramasinghe, D. Marino, C. Rieger, and M. Manic, “Framework for data driven health monitoring of cyber-physical systems,” in *2018 Resilience Week (RWS)*. IEEE, Aug 2018. [Online]. Available: https://doi.org/10.1109/RWEEK.2018.8473535

[17] P. Penkey, M. Alla, B. K. Johnson, and T. R. McJunkin, “Improving transmission system resilience using an automation controller and distributed resources,” in *2016 Resilience Week (RWS)*. IEEE, Aug 2016. [Online]. Available: https://doi.org/10.1109/rweek.2016.7573313

[18] S. Chilukuri, M. Alla, and B. K. Johnson, “Enhancing backup protection for thermal power generating stations using sampled values,” in *2017 North American Power Symposium (NAPS)*. IEEE, Sep 2017. [Online]. Available: https://doi.org/10.1109/naps.2017.8107323

[19] D. Conte de Leon, A. A. Jillepalli, V. J. House, J. Alves-Foss, and F. T. Sheldon, “Tutorials and Laboratory for Hands-On OS Cybersecurity Instruction,” *Journal of Computing Sciences in Colleges*, vol. 34, no. 1, Oct 2018. [Online]. Available: https://dl.acm.org/citation.cfm?id=3280489

[20] M. Ashrafuzzaman, Y. Chakhchoukh, A. A. Jillepalli, P. Tosic, D. Conte de Leon, F. T. Sheldon, and B. K. Johnson, “Detecting stealthy false data injection attacks in power grids using deep learning,” in *2018 14th International Wireless Communications and Mobile Computing Conference (IWCMC)*, Jun 2018, pp. 219–225. [Online]. Available: https://doi.org/10.1109/IWCMC.2018.8450487

[21] M. Ashrafuzzaman, H. Jamil, Y. Chakhchoukh, and F. T. Sheldon, “A best-effort damage mitigation model for cyber-attacks on smart grids,” in *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, vol. 02, Jul 2018, pp. 510–515. [Online]. Available: https://doi.org/10.1109/COMPSAC.2018.10285

[22] Idaho Regional Optical Network, “Iron- about us,” Online, Apr 2018. [Online]. Available: http://ironforidaho.net/about-us/

[23] T. J. Williams, “The purdue enterprise reference architecture,” *Computers in Industry*, vol. 24, no. 2-3, pp. 141–158, Sep 1994. [Online]. Available: https://doi.org/10.1016/0166-3615(94)90017-5

[24] "National scada test bed: Fact sheet," Online, Apr 2018. [Online]. Available: https://www.energy.gov

[25] "Idaho national laboratory: Grid resilience," Online, Apr 2018. [Online]. Available: https://www.inl.gov/research-programs/grid-resilience/

[26] A. Ashok, A. Hahn, and M. Govindarasu, "A cyber-physical security testbed for smart grid," in *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW '11.* ACM Press, Oct 2011. [Online]. Available: https://doi.org/10.1145/2179298.2179320

[27] T. Benzel, R. Braden, D. Kim, C. Neuman, A. Joseph, K. Sklower, R. Ostrenga, and S. Schwab, "Experience with DETER: a testbed for security research," in *2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, 2006. TRIDENTCOM 2006.* IEEE, Mar 2006. [Online]. Available: https://doi.org/10.1109/tridnt.2006.1649172

[28] S. S. Biswas, J. H. Kim, and A. K. Srivastava, "Development of a smart grid test bed and applications in PMU and PDC testing," in *2012 North American Power Symposium (NAPS).* IEEE, Sep 2012. [Online]. Available: https://doi.org/10.1109%/naps.2012.6336362

[29] C. M. Davis, J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol, "SCADA cyber security testbed development," in *2006 38th North American Power Symposium.* IEEE, Sep 2006. [Online]. Available: https://doi.org/10.1109/naps.2006.359615

[30] V. S. Koganti, M. Ashrafuzzaman, A. A. Jillepalli, F. T. Sheldon, D. Conte de Leon, and B. K. Johnson, "A virtual testbed for security management of industrial control systems," in *2018 12th International Malicious and Unwanted Software Conference (MALCON)*, Oct 2017, pp. 85–90. [Online]. Available: https://doi.org/10.1109/MALWARE.2017.8323960

[31] E. Korkmaz, A. Dolgikh, M. Davis, and V. Skormin, "Ics security testbed with delay attack case study," in *MILCOM 2016 - 2016 IEEE Military Communications Conference*, Nov 2016, pp. 283–288. [Online]. Available: https://doi.org/10.1109/MILCOM.2016.7795340

[32] I. A. Oyewumi, A. A. Jillepalli, P. Richardson, M. Ashrafuzzaman, B. K. Johnson, Y. Chakhchoukh, M. A. Haney, F. T. Sheldon, and D. C. de Leon, "Isaac: The idaho cps smart grid cybersecurity testbed," in *2019 IEEE Texas Power and Energy Conference (TPEC)*, Feb 2019, pp. 1–6. [Online]. Available: https://doi.org/10.1109/TPEC.2019.8662189

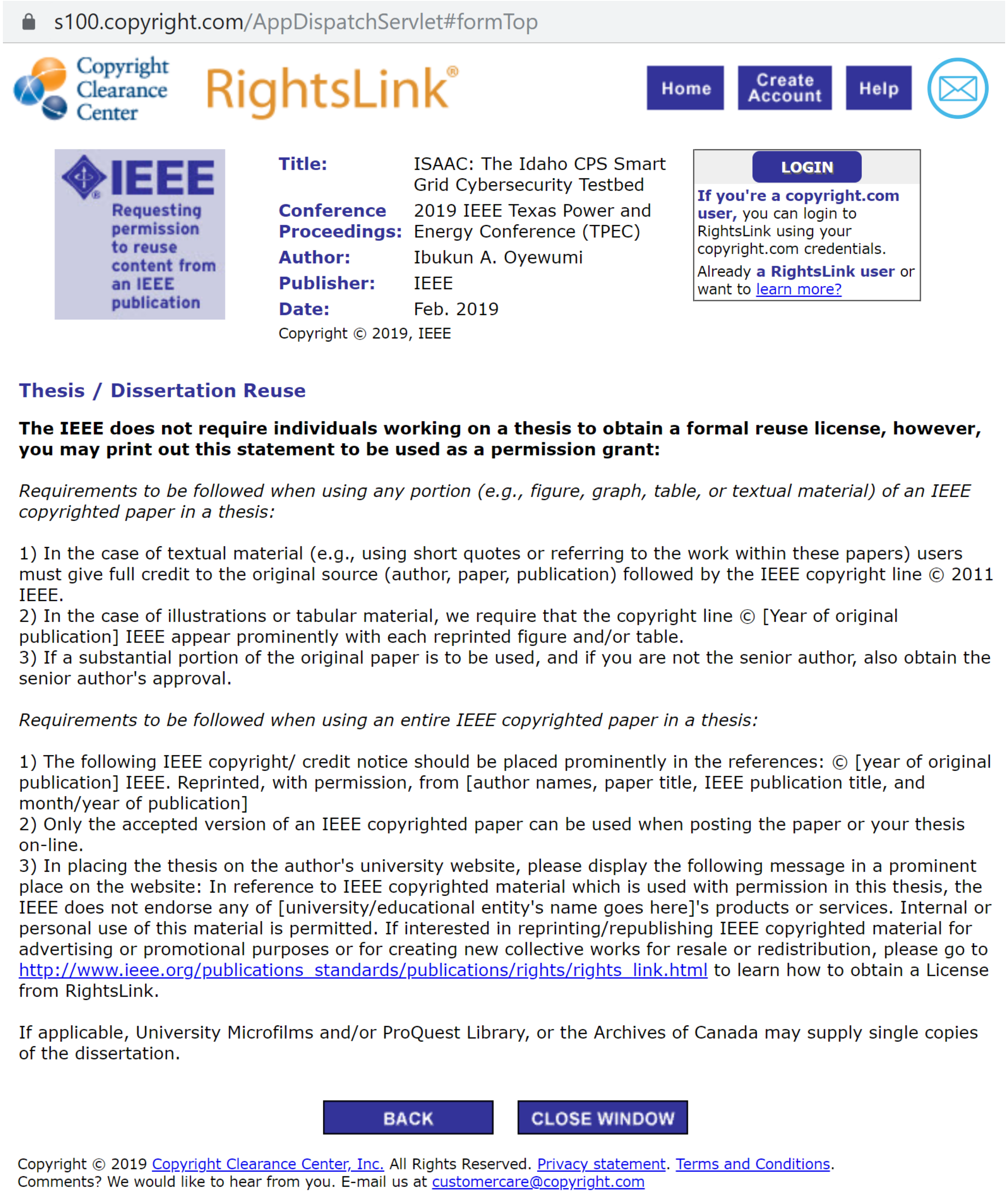
[33] I. A. Oyewumi, H. Challa, A. A. Jillepalli, P. Richardson, Y. Chakhchoukh, B. K. Johnson, D. Conte de Leon, F. T. Sheldon, and M. A. Haney, "Attack scenario-based validation of the idaho cps smart grid cybersecurity testbed (isaac)," in *2019 IEEE Texas Power and Energy Conference (TPEC)*, Feb 2019, pp. 1–6. [Online]. Available: https://doi.org/10.1109/TPEC.2019.8662168

Appendix A: Copyright and Credit Notice

As listed in the Section 1.4, some of the content of this thesis is currently copyrighted by the Institute of Electrical and Electronics Engineers Inc. (IEEE). Permission for reproduction of complete article, towards use in theses/dissertations has been given by the IEEE, provided the following statements are placed in the theses. Figures A.1 and A.2 provides proof of this permission. The content of these reproduced articles has been changed to suit the format of a thesis; instead of a scholarly article. The numbering of figures and listings has changed, due to being reproduced in this thesis. However, the figures and listings, and their captions themselves remain unchanged. Also, some paragraphs may have gone through minor edits resulting from the thesis review and editing process. There are also present in this thesis chapters, figures and paragraphs not present in the publications. This is due to work performed after paper submission and publication, and also not included due to conference proceedings length limitations.

Chapter 2 of this thesis ©2019 IEEE. Reprinted, with permission. Citation: I. A. Oyewumi et al., "ISAAC: The Idaho CPS Smart Grid Cybersecurity Testbed," 2019 IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 2019, pp. 1-6. doi: 10.1109/TPEC.2019.8662189 [32].

Chapter 3 and Chapter 4 of this thesis ©2019 IEEE. Reprinted, with permission. Citation: I. A. Oyewumi et al., "Attack Scenario-based Validation of the Idaho CPS Smart Grid Cybersecurity Testbed (ISAAC)," 2019 IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 2019, pp. 1-6. doi: 10.1109/TPEC.2019.8662168 [33]. For portions not copyrighted by IEEE or any other publisher (as of the date of this publication), and for this thesis as a whole; copyrights are retained by the author. Permission for not-for-profit and academic use is granted. For any other right to copy, transfer, reprint, republish, or for-profit use; permission must be sought from the author (Ibukun A. Oyewumi).


s100.copyright.com/AppDispatchServlet#formTop
Copyright Clearance Center
RightsLink®
Home
Create Account
Help
IEEE
Requesting permission to reuse content from an IEEE publication
LOGIN
BACK
CLOSE WINDOW

Title: ISAAC: The Idaho CPS Smart Grid Cybersecurity Testbed

Conference Proceedings: 2019 IEEE Texas Power and Energy Conference (TPEC)

Author: Ibukun A. Oyewumi

Publisher: IEEE

Date: Feb. 2019

Copyright © 2019, IEEE

If you're a copyright.com user, you can login to RightsLink using your copyright.com credentials.
Already **a RightsLink user** or want to learn more?

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

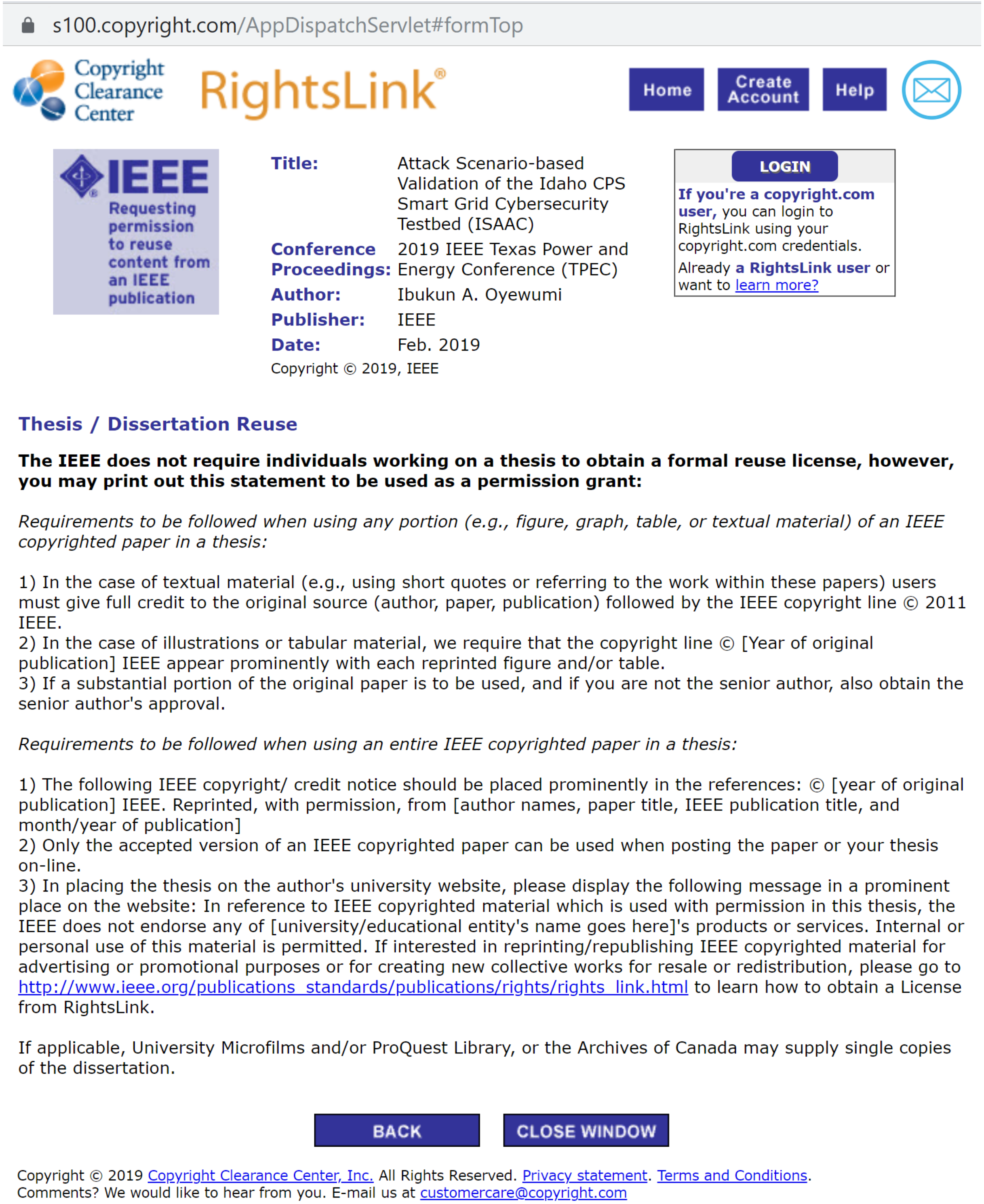
1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

Figure A.1: Permission from IEEE to Reproduce an Article as Chapter 2 of This Thesis.


s100.copyright.com/AppDispatchServlet#formTop
Copyright Clearance Center
RightsLink®
Home
Create Account
Help
IEEE
Requesting permission to reuse content from an IEEE publication
LOGIN
BACK
CLOSE WINDOW

Title:	Attack Scenario-based Validation of the Idaho CPS Smart Grid Cybersecurity Testbed (ISAAC)
Conference Proceedings:	2019 IEEE Texas Power and Energy Conference (TPEC)
Author:	Ibukun A. Oyewumi
Publisher:	IEEE
Date:	Feb. 2019

Copyright © 2019, IEEE

If you're a copyright.com user, you can login to RightsLink using your copyright.com credentials.
Already **a RightsLink user** or want to learn more?

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

Figure A.2: Permission from IEEE to Reproduce an Article as Chapter 3 of This Thesis.