Spring 3-2024

Implementing a Zero Trust Architecture For ICS/SCADA Systems

Raven Sims

IMPLEMENTING A ZERO TRUST ARCHITECTURE FOR ICS/SCADA SYSTEMS

A dissertation submitted to Dakota State University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Cyber Operations

March 2024

By

Raven Sims

Dissertation Committee:

Dr. Yong Wang

Dr. Bhaskar Rimal

Dr. Edward M. Dennis

Dr. Edward P. Yakabovicz

Beacom College of Computer and Cyber Sciences

DAKOTA STATE UNIVERSITY

DISSERTATION APPROVAL FORM

This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Philosophy degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

Student Name: Raven Sims

Dissertation Title:
Implementing a Zero Trust Architecture For ICS/SCADA Systems

Graduate Office Verification: DocuSigned by: Abby Chowning F44C8D9E621C417... Date: 04/17/2024

Dissertation Chair/Co-Chair: DocuSigned by: Yong Wang 70AB505BC7B649E... Date: 04/17/2024
Print Name: Yong Wang

Dissertation Chair/Co-Chair: _____ Date: _____
Print Name: _____

Committee Member: DocuSigned by: Edward Dennis 5BEC844CFF91413... Date: 04/17/2024
Print Name: Edward Dennis

Committee Member: DocuSigned by: Bhaskar Rimal 917AA4B61574EF... Date: 04/18/2024
Print Name: Bhaskar Rimal

Committee Member: DocuSigned by: Ed Yakabovicz FBA65AC7CE66471... Date: 04/20/2024
Print Name: Ed Yakabovicz

Committee Member: _____ Date: _____
Print Name: _____

Submit Form Through Docusign Only
or to Office of Graduate Studies
Dakota State University

ACKNOWLEDGMENTS

A special thank you goes to Dr. Yong Wang, my dissertation committee chair and advisor. Thank you for the guidance and support during this long journey. I am also grateful to the dissertation committee members, Dr. Rimal Bhaskar, Dr. Edward Dennis, and Dr. Edward Yakabovicz. A special thank you goes to my mother, Beverly Anderson. Everything I am and ever hope to be, I owe to you. Thank you for preparing me for life, for convincing me that what I set out to do, I can achieve. Your love and guidance are what will lead me through the rest of my life. You will live in my heart forever.

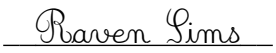
ABSTRACT

The American people depend significantly on Industrial Control Systems (ICS), which help enable critical infrastructures worldwide. These systems can deliver vital infrastructure services to provide essential capabilities worldwide. These Industrial Control Systems also contain many associated vulnerabilities that go unmitigated due to the complex nature of the systems. To strengthen and improve that cyber posture, a more proactive cyber approach utilizing a Zero Trust Architecture was analyzed as a solution to mitigate the risk. The ICS Purdue Model was interpreted as a potential framework for ICS architecture during the analysis. The ICS Purdue Model was then enhanced with Zero Trust controls as a possible cyber solution to mitigate the associated risks. Many of these systems are complex and have to maintain 24/7/365 operations. Because of the unique nature of these systems, they cannot be upgraded, or patched with modern-day cyber controls. This design science research study will investigate an Enhanced ICS Purdue Model with Zero Trust controls as an alternative approach to mitigate ICS cyber risks, rather than traditional cyber defense enterprise IT approaches.

DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions or writings of another. I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,



Raven Sims

TABLE OF CONTENTS

Dissertation Approval Form ii

Acknowledgments iii

Abstract iv

Declaration v

Table of Contents vi

List of Tables x

List of Figures xi

Chapter 1:

INTRODUCTION 1

1.1 Background of the Problem 3

1.2 Statement of the Problem with Motivation 4

1.3 Research Goals 4

1.4 Objectives of the Research 5

Chapter 2:

LITERATURE REVIEW 6

2.1 Cybersecurity Capability Maturity Model (C2M2) 7

2.2 Cybersecurity Framework 8

2.3 Zero Trust Architecture (ZTA) 10
2.4 Zero Trust Maturity Model 13
2.5 Zero Trust for Operational Technology 15
2.6 Overall Analysis of Published Work 15

Chapter 3:

RESEARCH METHODOLOGY **18**

3.1 Context 18
3.2 Research Problem 20
3.3 Research Design and Validation 20
3.3.1 Validation 21
3.4 Constructing the Validation Model 22
3.5 Sampling 23
3.6 Treatment Design 23
3.7 Measurement Design 24
3.8 Inference Design and Validation 25
3.9 Research Executing 25
3.10 Data Analysis 26
3.11 Data Collection 26

Chapter 4:

ICS PURDUE MODEL AND RISK ASSESSMENT **27**

4.1 Purdue Reference Architecture 27
4.2 ICS Purdue Model Reference Lab Environment 30
4.3 Verification of Lab Environment to ICS Purdue Model 32
4.4 Risk Assessment - ICS Purdue Model Architecture 33
4.4.1 Risk Identification 33
4.4.2 Risk Analysis 34

4.4.3 Risk Evaluation - ICS Purdue Model Architecture 35
4.5 ICS Purdue Model Risk Assessment Results 38
4.5.1 ICS Purdue Model Exploits 38
4.5.2 Enumeration 38
4.5.3 Gaining Access 41
4.6 Summary and Overall Security Risks of ICS Purdue Model 42

Chapter 5:

ENHANCED ICS PURDUE MODEL WITH ZERO TRUST CONTROLS AND RISK ASSESSMENT 46

5.1 Zero Trust Background and Motivation 47
5.2 Enhanced ICS Purdue Model and Reference Lab Environment 48
5.3 Verification of Lab Environment to Enhanced ICS Purdue Model 52
5.4 Enhanced ICS Purdue Model Exploits 53
5.4.1 Enumeration 54
5.4.2 Unable to Gain Access 55
5.5 Risk Assessment of Enhanced ICS Purdue Model and Results 56
5.6 Comparison Assessment of ICS Purdue Model and Enhanced ICS Purdue Model with Zero Trust Controls 57
5.7 Summary 58

Chapter 6:

IMPLEMENTING ENHANCED ICS PURDUE MODEL 61

6.1 Implementing the Enhanced ICS Purdue Model 61
6.1.1 Identifying Assets and Services 62
6.1.2 Policy Configuration 62
6.1.3 Network Segmentation 63
6.1.4 Policy Decision Point / Policy Enforcement Point Configuration . . 63

6.2 Summary 65

Chapter 7:

SUMMARY AND CONCLUSION **66**

7.1 Research Findings and Contributions 66

7.2 Research Challenges and Limitations 69

7.3 Future Work 70

7.4 Conclusion 71

References **73**

LIST OF TABLES

Table 2.1 Research Compare/Contrast Table 17

Table 3.1 Checklist for Research Context 20
Table 3.2 Design Problem and Knowledge Questions 20
Table 3.3 Construction of a Sample 24
Table 3.4 Measurement Design 25
Table 3.5 Research Execution Checklist 26
Table 3.6 Data Analysis Checklist 26

Table 4.1 ICS/SCADA Lab Components 30
Table 4.2 ICS Lab Network Configurations 32
Table 4.3 Lab Network Communication Paths 32
Table 4.4 Threats, Techniques, and Methods 34
Table 4.5 Vulnerability Alignment 36
Table 4.6 ICS Purdue Model Architecture Security Risks 37
Table 4.7 ICS Purdue Model Architecture Risk Score 38
Table 4.8 ICS Purdue Model Architecture Categorized Security Risks 44

Table 5.1 Enhanced ICS Model Lab Network Communication Paths 53
Table 5.2 Threats, Techniques, and Methods 54
Table 5.3 Enhanced ICS Purdue Model Risk Score 59
Table 5.4 Enhanced ICS Purdue Model Risk Score with Zero Trust Controls . . . 60

LIST OF FIGURES

Figure 2.1 NIST Cybersecurity Framework 1.1. [12] 9

Figure 2.2 NIST 800-207 Zero Trust Access Model. 11

Figure 3.1 Framework for Design Science 19

Figure 3.2 Engineering Process 21

Figure 4.1 ICS Purdue Model 28

Figure 4.2 ICS/SCADA Lab Hardware Components 31

Figure 4.3 Baseline ICS Purdue Model Network Diagram 34

Figure 4.4 Risk Assessment Matrix 35

Figure 4.5 ICS Purdue Model Architecture Risk Assessment 36

Figure 4.6 enum4linux - Enumeration 39

Figure 4.7 Kerbrute - Enumeration 40

Figure 4.8 Active Directory Users - Enumeration 40

Figure 4.9 HashCat - Enumeration 41

Figure 4.10 Popping a shell 42

Figure 4.11 Malicious Script 43

Figure 4.12 Empire - Interact 45

Figure 5.1 Purdue Model for ICS Security 47

Figure 5.2 Enhanced ICS Model 52

Figure 5.3 enum4linux - Enumeration 55

Figure 5.4 Enhanced ICS Purdue Model Risk Assessment Matrix 58

Chapter 1

INTRODUCTION

As the cyber landscape continues to evolve, operational technology must stay abreast of these changes to ensure no impacts on the American way of life. This research highlights the vulnerabilities within operational technology concerning Industrial Control Systems (ICS) and propose zero trust as a solution to defend these systems against the nation's greatest adversaries.

According to the Electric Power Research Institute (EPRI), zero trust is a cyber security concept that mitigates data and asset security risks. The traditional reactive cyber security defense measures cannot address risk reduction for cloud-based applications and insider threats because of the evolving cyber threat.

The National Institute of Standards and Technology (NIST) particular publication draft on zero trust offers the following definition: "Zero trust provides a collection of concepts and ideas designed to reduce the uncertainty in enforcing accurate, per-request access decisions in information systems and services in the face of a network viewed as compromised" [1]. Zero trust architecture is a cybersecurity plan that utilizes zero trust concepts to components within the IT infrastructure. This can include workflow planning, network configurations, and access control policies [2]. Therefore, a zero trust enterprise is the network infrastructure and operational policies within the enterprise zero trust architecture plan [2].

The EPRI definition of zero trust is tailored for utility OT environments. In these

mission-critical environments, product and process data must be protected from alteration to avoid performance disruptions in OT assets and their data networks. ERPI defines zero trust as a concept of continuous identity management based on the based on the identity of the entity and the context of the activity" [3].

According to the Cyber and Infrastructure Security Agency (CISA), critical infrastructure is defined as the infrastructure that provides essential services that fuel the society and economy [4]. This infrastructure has been deemed critical due to its impact on the American people if lost. If lost, the Energy sector includes infrastructure components vital to Americans' way of life. Therefore, ensuring these resources are protected with the appropriate cyber defenses is essential.

Guidelines and new policies have been developed for the Energy Sector to make risk-informed decisions to improve their cyber posture. Still, the referenced frameworks and guidelines are primarily based on enterprise IT solutions. The energy sector has a different problem with using ICS/SCADA systems. ICS/SCADA cannot have the same types of controls as enterprise IT components. Many of these systems do not have the computing power or the capability to have cyber controls placed on these mission-critical devices.

Without the appropriate cyber controls, these infrastructures can be left vulnerable to cyber-attacks [5]. The cyber controls that should be implemented to implement zero trust are both both physical and logical controls [6]. Implementing controls will lower the risk of losing resources and support a resilient cyber architecture to defend against a cyber attack. The energy sector needs to consider zero trust as a way to mitigate the vulnerabilities within the industrial control systems that support their power grid infrastructure.

1.1 Background of the Problem

Operational technology is the backbone of many mission-critical systems, including weapon systems, power grids, industrial processes, and many more [5]. Because of the mission-critical nature of the technology, it is often hard to remediate vulnerabilities found within the systems due to the downtime associated with the remediation. Due to the risk associated with the vulnerabilities found within such technologies, it is crucial for the industry to consider a new deployment strategy for these systems. The physical and logical controls of zero trust should be implemented to allow for a more proactive and granular approach to cybersecurity for these systems. Implementing controls will lower the risk of losing resources and support a resilient cyber architecture to combat a cyber-attack. It is essential for the industry to consider zero trust to mitigate the vulnerabilities within operational technology systems that support their mission-critical infrastructures. The Zero Trust Architecture (ZTA) is a model that can be followed within operational technology implementations that allow for the mitigation of risk and supports the need for these systems to be up 24/7/365 [7]. Meeting the mission need is significant, as the risk of exploitation often does not outweigh the value of mission-critical operations.

The National Institute of Standards and Technology (NIST) has defined operational technology as programmable devices that interact with the physical environment [2]. These systems/devices detect or cause a direct change by monitoring and controlling devices, processes, and events. Operational Technology includes industrial control systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems. NIST defines an industrial control system as information systems used to control industrial processes [2]. "Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, distributed control systems, and smaller control systems using programmable logic controllers to control localized processes" [2]. Examples of OT include Industrial Control Systems (ICS), Building Management Systems

(BMS), Fire Control Systems (FCS), and physical access control mechanisms. For the context of this dissertation, ICS, SCADA, and OT will be used synonymously throughout [8].

1.2 Statement of the Problem with Motivation

In many of these OT environments, product and process data must be protected from alteration to avoid performance disruptions [7]. Guidelines and new policies have been developed for the industry to make risk-informed decisions to improve its cyber posture. Still, the referenced frameworks and procedures are based mainly on enterprise IT solutions. Many solutions do not focus on mission criticality and the importance of maintaining system up-time during current operations. Therefore, current policies do not reflect the current need of the industry to maintain mission-critical operations [7].

This research explores zero-trust implementations to include specific technologies for mission-critical operational technology environments. By taking the time to understand how operational technology systems work, cyber professionals can better mitigate the risk of enterprises that use these types of systems. Because of the number of devices, sensors, and software utilized within OT, the attack surface is widespread.

1.3 Research Goals

Because of the vulnerabilities associated with operational technology, many Industrial Control Systems are left vulnerable to cyber attacks due to the lack of cyber controls that can be implemented. Zero Trust is an industry-standard framework that can be applied to operational technology to reduce cyber risk and ensure a resilient cyber architecture. This approach can help the utility industry transform its current reactive cybersecurity practices into a more proactive one. This approach allows the Energy sector to bake in zero trust and operational intelligence for a more cyber-resilient architecture. This

research focuses on mission-critical Operations Technology (OT) infrastructure, the vulnerabilities associated with such systems, and the utilization of Zero Trust to mitigate such vulnerabilities. This dissertation will seek to answer the following research questions:

- Could zero trust concepts be successfully applied to ICS/SCADA environments?
- What would the zero trust architecture be to effectively mitigate risks in the ICS/SCADA environment?
- What are the appropriate controls to pair with zero trust to ensure a resilient cyber architecture for ICS/SCADA environments?

1.4 Objectives of the Research

The research aims to determine how to properly secure ICS/SCADA environments within operational platforms such as the power grid. The research goals will identify a zero trust-based technical solution to protect industrial control systems from cyber-attacks. The research benefits industries where industrial control systems provide mission-critical operations.

An in-depth analysis of historical ICS/SCADA breaches has been done in the literature review to understand specific vulnerabilities to those systems and how adversaries established footholds into these types of systems. After the historical breaches are analyzed, a remediation solution is proposed in Chapter 5. The solution will discuss zero trust configurations within the network architecture to defend against cyber-attacks. The solution will then be verified in Chapter 6 by utilizing the Risk Management Framework (RMF) to assess the remaining risk within the SCADA system.

Chapter 2

LITERATURE REVIEW

An industry standard or guide to applying Zero Trust to Operational Technology has not been widely adopted, specifically in areas with a specific defense-in-depth architecture configuration. There have been few standards that tend to draw a complete picture of Zero Trust and Operational Technology. The referenced frameworks in the following paragraphs will provide a gap analysis of what is currently available in industry as reference architectures for ICS/SCADA systems and zero trust.

The purpose of this research is to bring awareness to the vulnerabilities within ICS/SCADA systems and how zero trust can be implemented outside of an enterprise IT environment. These findings will serve as a foundation for connecting zero trust architecture frameworks and apply it to the ICS Purdue Model for ICS/SCADA systems.

The research reviews the defense-in-depth model, network segmentation, tool configuration, and continuous monitoring needed to ensure cyber resiliency within ICS/SCADA systems. This technological approach can be utilized across organizations with ICS/SCADA systems. This research allows for specific configurations to be listed in detail to allow cyber engineers to understand specific technologies that can be utilized to apply cyber resiliency within their aging ICS/SCADA environments.

This chapter will provide a review of current research related to zero trust and ICS/SCADA systems. The strategy for this literature includes understanding zero trust and the current implementation recommendations in industry. After the researcher has gath-

ered that understanding, the researcher will focus on applying zero trust to ICS/SCADA systems. The depth of the literature found reflects a time period of approximately five years.

2.1 Cybersecurity Capability Maturity Model (C2M2)

Within the *Cybersecurity Capability Maturity Model (C2M2)*, the Federal Government has made great efforts to increase the cyber posture of the Energy Sector by developing the Electricity Subsector Cybersecurity Capability Maturity Model (C2M2). The C2M2 helps private sectors evaluate their cybersecurity controls and assess their maturity against a framework. With this framework, industry is able to prioritize and improve cybersecurity controls based on their environment requirements [9]. The Office of Cybersecurity, Energy Security and Emergency Response (CESR) released guidance to help the energy sector establish or align their risk management programs with the NIST CSF. The Department of Energy (DOE) developed a Risk Management Process (RMP) specifically tailored for the energy sector. Within this process, managing cybersecurity risk is highlighted as critical to the organization's success. Without effectively managing risk, the sector is incapable of carrying out its mission. The RMP was designed to manage risk within an environment and to help organizations make informed decisions to improve their cyber posture [9].

Guidelines and new policies have been developed for the Energy Sector to make risk-informed decisions to improve their cyber posture, but the referenced frameworks and guidelines are largely based on enterprise IT solutions. The energy sector has a different problem with using ICS/SCADA systems. This specific work does not highlight the ability to utilize zero trust, nor does it detail what tools and/or technologies could be considered to mitigate risk for the Energy Sector. The research provided by the author will take those considerations in to present a complete and detailed standard for OT.

2.2 Cybersecurity Framework

On May 27, 2021, the Department of Homeland Security (DHS) Transportation Security Administration (TSA) department announced new cybersecurity requirements for critical pipeline owners due to ransomware attacks on major petroleum pipelines [10]. Due to the cyber-attacks, President Barack Obama issued Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*. This EO led to the development of the *NIST Cybersecurity Framework (CSF)*. The CSF allows organizations to manage cybersecurity risk for the components directly involved in the delivery of critical infrastructure services [11].

The Cybersecurity Framework is broken into three components: Framework Core, Implementation Tiers, and a Framework Profile. The Framework Core represent the industry standards, guidelines and policies that allow for communication within the system [11]. The Core establishes a process for organizations to Identify, Protect, Detect, Respond, and Recover from cyber security incidents. The Implementation Tiers provide context on how risks are viewed within an organization and the current processes used to manage risk [11]. The Tiers allows the organization to assess the strength of their cybersecurity process and tools from Tier 1, Partial; Tier 2, Risk Informed; Tier 3, Repeatable; and Tier 4, Adaptive. The Framework Profile is the alignment of standards, guidelines, and practices to the Framework Core implementation scenario [11]. Organizations can use "profiles" to assess their current cyber posture to identify areas to improve their cyber posture. Figure 2.1 describes the continuous process of the CSF and how this process needs to be continuously applied to allow for the mitigation of risks.

The *NIST Cybersecurity Framework* is a technology-neutral process that outlines the most effective ways to manage risk. Like the research developed by the author in this dissertation, the NIST CSF is only a recommendation as ICS owner will need to manage their own risk based on the risk tolerance that is identified within the organization. NIST

Figure 2.1: NIST Cybersecurity Framework 1.1. [12]

CSF and the work proposed by the author are not intended to replace any existing policies within organizations but rather to allow for an assessment of current tools, technologies, and procedures to assess areas of improvement. The NIST CSF can serve as the building block for a new cybersecurity program or a enabler to improve an existing program, developing cyber requirements for external partners, or identify gaps in current processes [11].

The *NIST Cybersecurity Framework* is a great starting point for ICS organizations to learn about how to assess risk within their organization. Because NIST CSF is vendor

agnostic, it misses a lot of technical details that need to be included. This includes the appropriate technical controls that need to be applied. The example technical controls in the document only highlight enterprise IT examples that do not apply within ICS/SCADA systems.

2.3 Zero Trust Architecture (ZTA)

Zero Trust is not a new framework. NIST has published foundational reference documents highlighting zero trust concepts. NIST SP 800-207 sets the framework for Zero Trust Architecture (ZTA). This literature explains the foundational concepts of zero trust principles and gives high-level deployment models within enterprise IT. NIST defines Zero Trust (ZT) as a "collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised" [1]. This is important because zero trust is not a simple technology that can be purchased and installed within your network. Zero Trust is a collection of concepts and principles that enable a strategy to generate a zero trust architecture as a plan to be implemented within a network. Within this work, NIST focuses on authentication, authorization, and minimizing trust zones. They have done this by developing a "Zero Trust Access" model, which is highlighted in the Figure 2.2.

"The network will ensure that the user or service requesting access to resources is authentic and the request is valid by utilizing policy decision points or policy enforcement points (PDP/PEP)" [1]. The PDP/PEP contains dynamic risk-based policies that allow the entity to access the requested resource. All traffic beyond the PEP has a common level of trust or "implicit trust zone" [1]. The PDP/PEP cannot apply additional policies beyond its location in the flow of traffic. To allow the PDP/PEP to be as specific as possible, the implicit trust zone must be as small as possible. Zero trust provides a set of

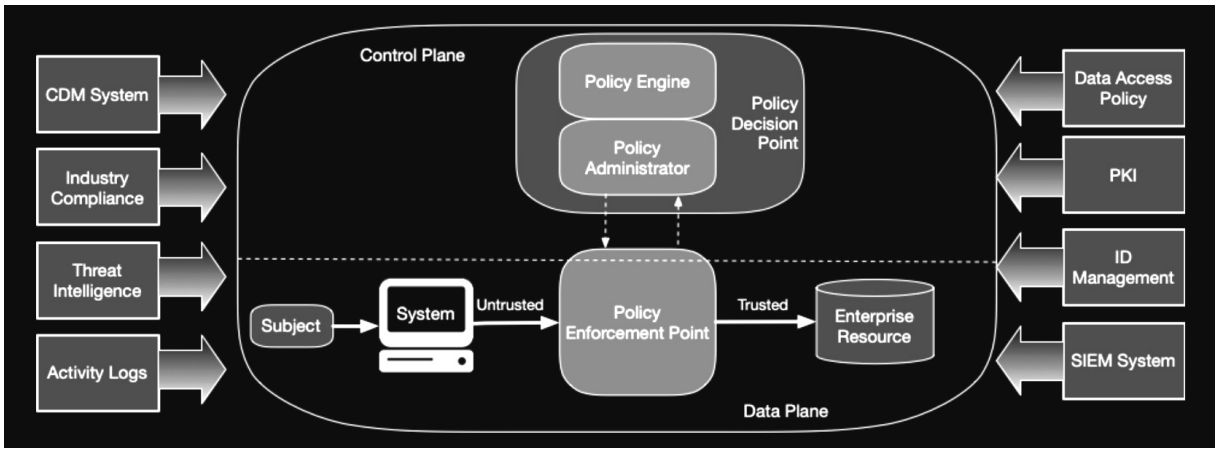


Figure 2.2: NIST 800-207 Zero Trust Access Model.

principles and concepts around moving the PDP/PEPs closer to the resource. The idea is to explicitly authenticate and authorize all subjects, assets, and workflows that make up the enterprise.

The founding principles in implementing a zero-trust architecture are defined by NIST as "tenets". These tenets are outlined below:

- All sources and services are considered resources.
- Communications are secured regardless of network location.
- Access to resources is granted on a per-session basis to ensure that appropriate security checklists have been followed.
- Resource access is determined by policy.
- Nothing is inherently trusted.
- Authentication and authorization are strictly enforced before granting access.
- Event logs are collected regarding the current state of assets, network infrastructure and communications to be able to proactively defend against cyber-attacks. [12]

NIST Special Publication 1800-35, Implementing a Zero Trust Architecture acknowledges that there is no single zero trust solution. This publication outlines many different

scenarios in which zero trust implementations can be applied. They highlight specific technologies, but their research still forgets to mention operational technology implementations. Because NIST is a non-regulatory federal agency within the U.S. Department of Commerce, they are vendor agnostic and do not recommend specific technologies [2]. Because of the lack of mention of specific technologies, the authors' research will be integral to closing this gap.

Augmenting Zero Trust Network Architecture to enhance security in virtual power plants, focuses on the energy sector and the application of zero trust to a virtual power plant [13]. This paper does a great job at highlighting the energy sectors problems and goes into great research about previous breaches to critical infrastructures. The research on the application of tools and technology is still vague. Since this research is solely focuses on the Energy sector, the authors research will ensure that the ZT approach can be applied in multiple environments.

Zero-Trust Model for Smart Manufacturing Industry, takes a look at utilizing zero trust for "serverless applications running on containers, mobile endpoints, IoT, and cyber-physical systems" [14]. The paper introduces Smart Manufacturing, also known as Industry 4.0. "Smart manufacturing focuses on the end-to-end digitization of all physical assets and integration into digital ecosystems with value chain partners" [14]. The paper also goes into existing cybersecurity countermeasures for smart manufacturing which include: cryptographic techniques, intrusion detection systems, security training and Incident Management, security with Software-Defined Networking (SDN), artificial neural network for threat detection, and blockchain security in smart manufacturing. The material covers general security considerations for implementing zero trust within operational technology. The paper then proposes a zero trust security model for manufacturing devices. This paper does not include specific technology implementation to include specific configurations for tools. This research was also very dedicated to smart manufacturing environments.

Zero Trust User Access and Identity Security in Smart Grid Based SCADA Systems
Smart grid-based systems are apart of modernized critical infrastructures. These infrastructures are used across the world to operate in various critical sectors, including electricity services, nuclear stations, transportation systems, hospital services, waste management, water services, etc. [15]. The modern smart grid technology includes both operational technology (OT) and information technology (IT) components. The convergence of both has introduced new security challenges for the operations of the systems in terms of its safety, reliability, efficiency and stability. The security perimeter is completely redrawn with the OT and IT convergence. The need of the hour is for new approaches towards security that are innovative and will ensure the security of critical infrastructures. The traditional approach of perimeter-based security defense is obsolete with the convergence of OT and IT. The Zero Trust model for user access and identity is based on concept of "Never Trust but Always Verify" that enable organizations to secure the critical infrastructures by ensuring only trustworthy and validated components are allowed into the network. The perimeter-centric security architecture is replaced by Zero Trust model to ensure and enable security and access decisions for devices, identity and user context to be enforced dynamically. It also ensures that only authorized and authenticated users and devices can access the network, systems, applications, and data. In this paper we are proposing Zero Trust User Access & Identity Security model that can be implemented in smart grid based SCADA systems.

2.4 Zero Trust Maturity Model

CISA's Zero Trust Maturity Model is a roadmap for agencies to reference to aid in the transition into a zero trust architecture for their enterprise. The maturity model contains five pillars: Identity, Device, Network, Application Workload, and Data. Each pillar also includes general details regarding Visibility and Analytics, Automation and Orchestration,

and Governance" [4].

The Identity pillar focuses on functions to uniquely define users or entities [4]. This approach is similar to identity access management with core components in least privilege and multi-factor authentication. The Device pillar refers to any hardware asset that can connect to a network [4]. This can include internet of things (IOT) devices, mobile phones, laptops, servers, and others [4]. This pillar focuses on the integrity of devices and ensuring that an organization is aware of all assets across its enterprise. The Network pillar "refers to an open communications medium, including agency internal networks, wireless networks, and the Internet, used to transport messages" [4]. This pillar focuses on network segmentation and protection of network traffic. The fourth pillar, Application Workload include agency systems, computer programs, and services that execute on-premise, as well as in a cloud environment [4]. This pillar focuses on extending zero trust into the development and deployment of applications to minimize the attack surface. The final pillar, Data, refers to organizations protecting the data within the enterprise. This includes data-at-rest and data-in-transit. Agencies should identify, categorize, and inventory their data to ensure a complete understanding of the data types and better understand the risk associated with data loss.

After reviewing the pillars provided by CISA, they are also focused on zero trust for enterprise IT. CISA's *Zero Trust Maturity Model* includes three stages: traditional, advanced, and optimal. The traditional stage includes manual configurations and static policies. The Advanced stage includes centralized visibility and policy enforcement. The Optimal stage includes fully automated processes and dynamic policy enforcement. In the combination of both the pillars and maturity levels, operational technology is not included in the model.

2.5 Zero Trust for Operational Technology

According to *Zero Trust Considerations for Utility OT Cyber Security Strategies*, OT cyber and IT cyber are drastically different cyber security practices. In the IT world, security measures data ex-filtration. Meanwhile, for OT cyber security, the focus is on altering product or process data. The alteration of products or process data can impact the performance of systems, applications, or devices. This publication understands the difference between environments as they relate to OT and IT, but this research does not go into detail regarding specific OT implementation to enable Zero Trust.

NIST Special Publication 800-82r3, *Guide to Operational Technology (OT) Security* provides guidance for establishing secure operational technology (OT) while addressing OT's unique performance, reliability, and safety requirement [2]. This publication goes into great detail regarding the system design of the OT system, including human machine interfaces (HMI), remote terminal units (RTUs), programmable logic controllers (PLCs), etc. This work does not include zero trust as a mitigation mechanism for risk for OT systems. This document explains best practices and general outlines for OT security but it does not go into specific technology implementation or suggest zero trust as an enabler for OT security as this research will do.

2.6 Overall Analysis of Published Work

This literature review analyzed information regarding operational technology, ICS/SCADA, and zero trust and found significant gaps in research when utilizing zero trust as a framework for mitigating risks within ICS/SCADA environments. Many of the references, went into great detail regarding risk assessments and how to mitigate risks within enterprise IT environments but they did not reference the tools/technologies that will be needed to mitigate risk with the OT environment. Table 2.1 incorporates all of the

findings to compare and contrast the identified work against the proposed work by the author.

Table 2.1: Research Compare/Contrast Table

Title	**Findings**	**Gaps**
C2M2	Maturity model for risk assessments	No specific information regarding the tools/technologies needed to mitigate risk. Reference also does not mention Zero Trust as a mitigation implementation
CSF	Risk assessment model for Enterprise IT systems	Certain methodologies do not apply to OT systems. Reference also does not mention Zero Trust as a mitigation implementation
ZTA	Explains the foundational zero trust concepts	Does not explain how the technology can be implemented within OT
Zero Trust Maturity Model	Assessment model used for transitioning organizations to zero trust	Does not include applications to OT environments, and this work also does not go into tools/technologies that can be utilized to implement zero trust within OT environments
Zero Trust Considerations for Utility OT Cyber Security Strategies	Mentions the difference between OT and IT	Does not detail specific OT implementation technologies to enable zero trust
Guide to OT	Provides guidance for establishing secure OT	Does not include zero trust as a mitigation mechanism for OT risk and does not go into specific technology/process implementations
Augmenting Zero Trust Network Architecture to enhance security in virtual power plants	Applies zero trust to the energy sector	Does not go into specific technologies utilized to implement zero trust. The author also does not go into test results to prove that the mitigation strategy works for ICS/SCADA systems.
Zero-Trust Model for Smart Manufacturing Industry	Zero Trust approach was explored to include principles, architecture, and implementation procedure. Proposed a zero trust model to be applied to the smart manufacturing industry.	Application of zero trust to the energy sector. Listing of tools/technology that can be utilized within the energy sector.

Chapter 3

RESEARCH METHODOLOGY

This chapter will define the research design needed to develop an inter-operative set of tools and configurations needed to implement zero trust for ICS/SCADA systems. The experiment, data collection, solution approach, and validation methodologies will be discussed in detail.

Research designs are plans for research that help enable decisions from assumptions to detailed methods of data collection and analysis [16]. A Design science *single-case mechanism experiment* will be utilized for this project. "A single-case mechanism experiment is a test of a mechanism in a single object of study with a known architecture" [17]. A single-case mechanism experiment is a test of a case where the researcher can manipulate the case and explain the responses. Within this project, the researcher will introduce penetration tests to manipulate the case and validate that the proposed zero trust framework for ICS/SCADA systems mitigates vulnerabilities within the environment.

3.1 Context

"Design science is the design and investigation of artifacts in context" [17]. To do a data science project, you must understand the major components, object of study, and activities. The object of study is investigating the artifact in context. This project's object of study is the newly proposed zero trust framework for ICS/SCADA systems. For the design activity, the social context is researchers, cyber engineers, and SCADA system operators. The goal of the project is to define the tools and configurations needed to

implement a zero trust architecture for ICS/SCADA systems. This will allow for the mitigation of risk and vulnerabilities for the environment. The knowledge context is the referenced work we discussed in the Literature Review. "The knowledge context consists of existing theories from science and engineering, specifications of currently know designs, useful facts about currently available products, lessons learned from the experience of researchers in earlier design science projects, and plain common sense" [17]. The interaction of these activities allow for a strengthen design to mitigate the risks within ICS/SCADA environments. Figure 3.1 highlights the interactions of the objects and major activities within design science to solve a problem.

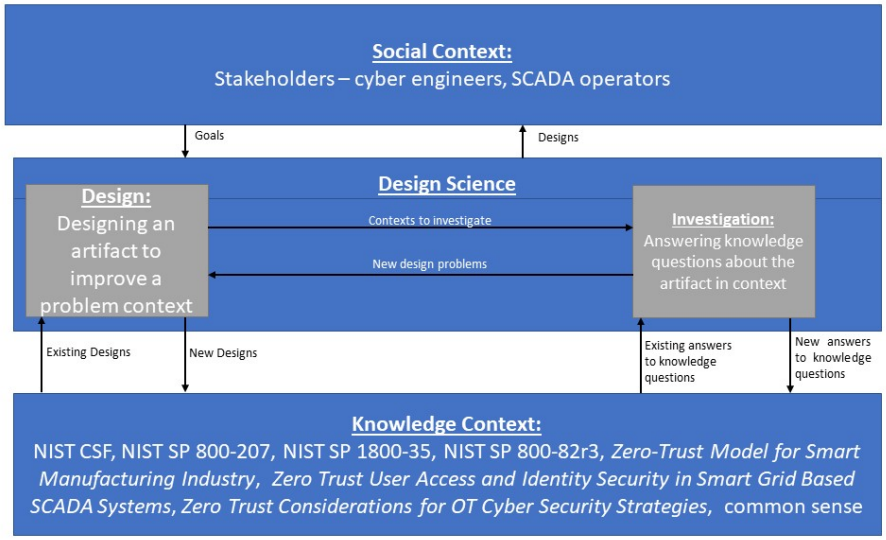


Figure 3.1: Framework for Design Science

The artifacts within this project are designed to interact with the problem context to improve the problem. In the Implementing Zero Trust for ICS/SCADA systems project, a zero trust framework was developed that allows cyber security engineers to mitigate risk within ICS/SCADA environments. The method is an artifact, and the context consists of cyber engineers who want to mitigate risks within the ICS/SCADA environment [17].

The ICS/SCADA zero trust architecture framework developed in the ZTA for ICS/S-

CADA project will be tested with open source tools. Table 3.1 provides context on the *knowledge goal, improvement goal, and knowledge context.*

Table 3.1: Checklist for Research Context

Knowledge Goals	**Improvement Goals**	**Current Knowledge**
Determine tools and framework to apply zero trust to ICS/SCADA systems Determine migration strategy for legacy ICS/SCADA systems	Development of new technology frameworks	Current research of zero trust and ICS/SCADA systems

3.2 Research Problem

Design problems force a change within the real world and require an analysis of stakeholder goals [17]. For this project, the design problems are the vulnerabilities within ICS/SCADA systems. Knowledge questions do not force a change in the real world but enables information gathering about how the world is [17]. The knowledge questions for this project are presented in Table 3.2.

Table 3.2: Design Problem and Knowledge Questions

Design Problem	**Knowledge Question**
Design an architecture that mitigates risk for ICS/SCADA system.	Is the risk mitigated down to an acceptable level?
Design a technical implementation plan for cyber engineers to implement for ICS/SCADA systems	Is the solution affordable for organizations?

3.3 Research Design and Validation

The *engineering cycle* is a rational problem-solving process that consists of: *problem investigation, treatment design, treatment validation, treatment implementation, and im-*

plementation evaluation. Figure 3.2 highlights all of the stages in the context of this project.

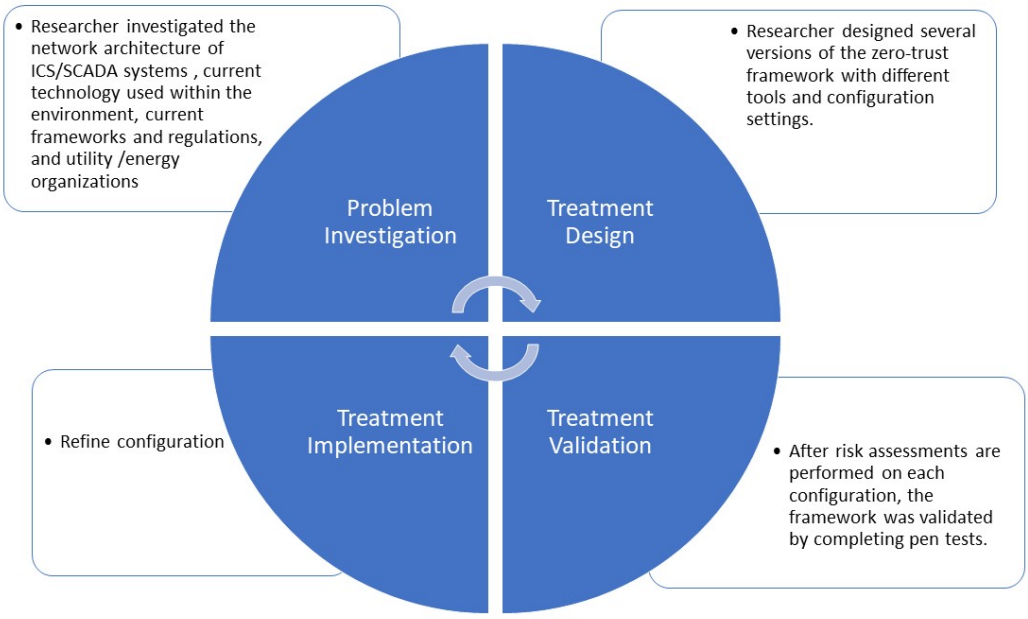


Figure 3.2: Engineering Process

The goal of *Treatment Implementation* is to evaluate the solution after it has been applied to the original design problem. *Treatment Validation* allows the researcher to validate the solution to justify that it will truly mitigate risk within ICS/SCADA environments. *Treatment Design* is the overall design of the proposed solution to mitigate risks within ICS/SCADA environments. *Problem Investigation* is the overall evaluation of the defined problem with ICS/SCADA systems.

3.3.1 Validation

Validation allows the researcher to predict how an artifact will interact with its context, without actually observing it within the real world [17]. Within this project, the researcher has predicted that zero trust mitigations at each network architecture level will mitigate risks within ICS/SCADA environments. In validation research, the researcher will expose

a mock ICS/SCADA system in a lab to various penetration tests to evaluate if the zero trust controls successfully defend against the tests. An unsuccessful test will expose the ICS/SCADA system to risk. This overall process is called a *single-case mechanism experiment*.

3.4 Constructing the Validation Model

Validation research develops a design theory of an artifact in context that allows the researcher to predict what would happen if the artifact were transferred to its intended environment [17]. The validation model helps the researcher predict how the solution will interact with ICS/SCADA systems within the real world. "A validation model consists of a model of the artifact interacting with a model of the problem context" [17].

A defined set of penetration tests was executed to observe how the system responds aligned to the *ICS Purdue Model Framework*. This project will test the zero trust controls within the *ICS Purdue Model Framework*in an ICS/SCADA environment. The validation model will comprise each layer of the *ICS Purdue Model* using a zero trust control. The risks within the *ICS Purdue Model* will be reduced once the zero trust controls are applied within the lab environment. By contrast, penetration tests executed without zero trust configurations enabled will show a significant increase in vulnerabilities within the system. This phenomenon will be explained by the specific tools and configurations used in the architecture of the system, as well as of the architecture of the ICS/SCADA system, in which zero trust methodologies were not applied.

The lab environment was configured with tools aligned to the *ICS Purdue Model* to mimic the industry framework for an industrial control system. Virtualization will be utilized to to mimic an SCADA environment. The hardware components to mimic an industrial control system will be a signal light tower and PLC. The following software was utilized to mimic the environment as recommended by *Pentesting Industrial Control*

Systems :

- VMWare ESXI
- Ubuntu ISO
- Windows 7 ISO
- Kali Linux ISO
- Koyo Click Software
- Koyo Click hardware power supply and PLC
- Physical network switch
- Selector Switch Station Box
- Industrial Signal Tower Lamp

3.5 Sampling

Within this research, the sampling was done subsequently in a process of analytical induction. After defining the zero trust framework and formulating knowledge questions, a case is selected from the results of the experiments that were conducted and studied. After continuous re-evaluation, the zero trust framework was updated until risk is reduced within the ICS/SCADA environment. Further detail of the induction of samples and sample validity is outlined in Table 3.3.

3.6 Treatment Design

An experimental treatment is the treatment of an object of study by the researcher in order to find out the effects of the proposed treatment [17]. Exposing the zero trust

Table 3.3: Construction of a Sample

Induction Strategy	**Sample Validity**
Tools will be inducted into the framework based on the results of the risk assessment. After multiple tools are evaluated, the best of breed solution will be selected if the tool lowers risk within the environment	Tools that do not lower risk will not be considered within the sample for evaluation.

framework to a simulated context (*i.e., penetration tests)* in order to learn if the tools can be applied within an ICS/SCADA environment and also discover if the tool can appropriately mitigate risks within the environment is an experimental treatment of the framework.

In this project, the scenarios are all combinations of zero trust frameworks. No treatment instruments are needed other than the necessary penetration tests to evaluate the applicability of controls. The treatment scenarios are intended to be similar to real-life breaches to assess which tools are most promising in the intended context to be selected for adoption into the framework. The researcher will have complete control of all factors that could influence the validation model. This will improve support for causal inference and analogic inference to real-world conditions.

3.7 Measurement Design

Measurement requires the definition of measured variables and scales. Table 3.4 outlines the data sources, variables, measurement instruments, and measurement schedules.

The researcher made sure the lab mocked a real-world ICS environment and implemented the best practices of the ICS Purdue Model that will be detailed in Chapter 4 [8]. This increases construct validity. Measurements of the results after the experiment will be used to support the tools selected within the zero trust framework appropriately

Table 3.4: Measurement Design

Variables	**Data Sources**	**Measurement Instruments**	**Measurement Schedule**
Results of Risk Assessment and penetration test	Software/hardware components within the ICS/SCADA system	Risk Assessment Matrix, Penetration test scenarios. The results will be stored within a separate laptop,	Risk assessment and penetration test will be completed before and after the zero trust tool is installed and implemented

mitigate risks within the environment.

3.8 Inference Design and Validation

"Single-case mechanism experiments are case based, and inferences from them are done in three steps: description, architectural explanation, and generalization by analogy" [17].

In this project, descriptive inferences will be the development of graphs, charts, and tables with digestible information displaying the experiment results. The researcher will not add additional data during the data preparation or data transformation phases.

Data will be entered into a risk assessment matrix for qualitative data analysis. The data will be cleaned to ensure missing data is not captured within the overall depiction.

3.9 Research Executing

The researcher will document the study's observations as the experiment is executed. Examples of the documentation notes are in Table 3.5.

Table 3.5: Research Execution Checklist

What happened?	**Unexpected Events?**	**Observation notes**
Will be completed at research execution	(Y/N)	Will be completed at research execution

3.10 Data Analysis

Table 3.6 checklist will be utilized to ensure the data from the experiment is collected consistently after each test.

Table 3.6: Data Analysis Checklist

Descriptions	**Explanations**	**Generalizations**	**Answers**
List Data prep steps	Explanations and validity	Will the results be valid in other cases?	Answer to knowledge questions

3.11 Data Collection

Log analysis will determine if the cyber tools selected can recognize adverse events within the ICS/SCADA system. The analysis of logs will also allow us to evaluate if the penetration attack was successful or if the cyber controls implemented could protect the ICS/SCADA system from an adverse attack. The tool evaluation phase will consist of finding open-source tools within each layer of the ICS Purdue Model that can be configured with zero trust policies. The open-source tool will be installed in the lab.

Chapter 4

ICS PURDUE MODEL AND RISK ASSESSMENT

Ackerman defines an Industrial Control System as a diverse set of control systems and instrumentation used in industrial production technology to achieve a common goal [8]. An Industrial control system includes: Programmable Logic Controllers (PLC), Human Machine Interface (HMI), Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Safety Instrumented Systems (SIS) [8]. These systems can be found nationwide in weapon systems, platforms, and power plants.

4.1 Purdue Reference Architecture

The security framework surrounding these systems is known as the Purdue model (Figure 4.1). This model was adopted from the Purdue Enterprise Reference Architecture (PERA) model as a concept model for ICS network segmentation [8]. This model is an industry standard for setup and configuration of ICS systems. The Purdue model shows the the interconnections and inter dependencies of the ICS system [8]. The PERA divides the ICS architecture into three zones and six levels defined in Figure 4.1:

- Enterprise
  - Level 5: Enterprise Network
  - Level 4: Site Business and Logistics

- Industrial Demilitarized Zone (IDMZ)
- Manufacturing Zone / Industrial Security Zone
  - Level 3: Site Operations
- Cell/Area Zone
  - Level 2: Area Supervisory Control
  - Level 1: Basic Control
  - Level 0: Process

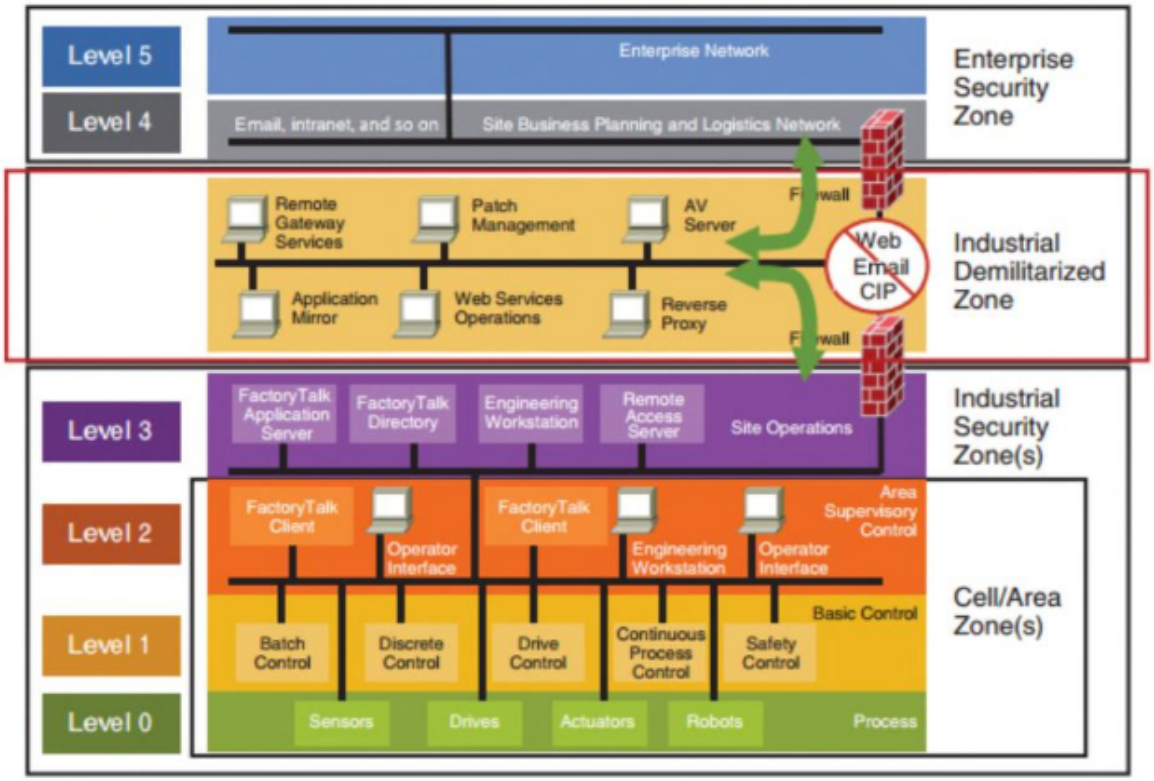


Figure 4.1: ICS Purdue Model

The *Enterprise Zone* is where business systems live like ERP and SAP [8]. These systems take data from systems lower in the model and use the accumulated data to report on the overall production status of the environment [8]. This zone relies on the

connectivity within the ICS networks to ensure that the production data is accurate and visualizes the appropriate information to drive business decisions [8].

The *Site Business and Logistics Zone* is where all the IT systems within the network live [8]. These systems support the production process in a plant [8]. These systems report production statistics for corporate systems [8]. Systems in this layer are enterprise applications like database servers, application servers, file servers, and email clients. [8].

Between the *Enterprise Zone* and the *Industrial Zone* lies the IDMZ. The IDMZ allows users to securely connect networks with different security requirements IDMZ [8]. "This is an information sharing layer between the business or IT systems in levels 4 and 5 and the production or OT systems in levels 3 and lower" [8]. The IDMZ is a broker between the two layers and serves as an extra layer of protection within the model that prevents direct communication between the IT and OT systems [8].

The *Industrial Zone* is where processes live [8]. This zone is subdivided into four levels: *Level: Site Operations, Level 2: Area supervisory control, Level 1: Basic Control, and Level 0: The process* [8]. Systems that support plant wide control and monitoring functions are within Level 3. The view function of the system lies within this level. The view function allows the operator to watch the current state of the system in real-time [8]. This allows the operator to make business decisions or perform corrective actions on the system. If an attacker can change the operator's view of the system's status, the attacker can control the complete process of the ICS [8].

The *Cell Area Zone* is where monitoring happens [8]. The monitoring function is often part of a control loop [8]. This function will monitor critical values, such as pressure, temperature, etc. [8]. "Systems typically found in Level 2 include HMIs (standalone or system clients), supervisory control systems such as a line control PLC, engineering workstations, etc." [8]. If an attacker can control the value that the monitor function is monitoring, the reaction to the function can be manipulated [8].

The control system is housed in Level 1, and this system is what makes actuators

engage, valves open, and motors run [8]. The control actions can be initiated by an operator changing a set point on an HMI screen or an automated response as part of the process control [8]. If an attacker can manipulate the values within the control system, the control function can be circumvented from the intended actions of the device [8].

Level 0 is where the actual process is performed and where the product is made [8]. This is a critical system component, as a minor disruption at this layer can cause grave damage to operations [8].

4.2 ICS Purdue Model Reference Lab Environment

Virtualization was utilized to align the lab environment to the Purdue Model Reference Architecture. Each component of the lab had a unique function in order to mimic the industrial control environment as recommended by *Pentesting Industrial Control Systems*. Table 4.1 highlights the functionality of each component.

Table 4.1: ICS/SCADA Lab Components

Software/OS	**Function**
Ubuntu OS	SCADA Machine used to view communications within the PLC
Windows 8.1 OS	Engineering workstation to mimic the operator workstation that interacts with the PLC
Kali Linux	Machine used to perform penetration tests on the equipment in the lab to ensure the zero trust architecture is capable of defending against attacks
Koyo CLICK Software	An open source engineering programming software that will be installed on the PLC machine.
Selector Switch Station Box	Used to toggle power on/off to the I/O on PLC
Industrial Tower Lamp	Used to display visual feedback from the toggling of I/O on PLC

These elements will serve as the baseline of the *ICS Purdue Model*. With the Koyo CLICK Programmable Logic Controller (PLC) in Figure 4.2 the researcher can mimic the PLCs often found in the field. The PLC contains the hardware and software used to automate industrial electromechanical processes, such as control of machinery on factory

(a) PLC - C0-10ARE-D

(b) Industrial Tower Lamp

(c) Selector Station Box

Figure 4.2: ICS/SCADA Lab Hardware Components

assembly lines. The C0-10ARE-D model obtained for the purpose of this research contains the CPU and a fixed set of I/O points in a compact form factor. This specific PLC has an ethernet port that supports Modbus TCP and EtherNet/IP protocols and one RS-232 serial comm port. The unit has eight stackable I/O modules connected to the PLC to expand the system to multiple capabilities.

The PLC is wired to the selector station switch that controls the lights on a tower lamp. The green selector switch controls the green light on the tower lamp, the turn key switch controls the yellow light on the tower lamp, and the red button controls the red light on the tower lamp. The PLC controller and selector switch station were wired and then programmed by the Koyo CLICK software to perform these functions. The Koyo CLICK software writes software to the PLC that controls the operations of each signal within the PLC. Koyo CLICK is similar to more mainstream vendors such as Siemens, Rockwell, and Schneider. The Koyo CLICK software was configured to trigger the functionality below from the industrial tower lamp. These configurations are simple for this lab's purpose but can mimic the same behavior in the field, such as opening and closing valves on a water plant, etc. [18]. These configurations are highlighted in Table 4.1.

After the hardware components are setup and are communicating with each other through out the environment, the network was defined according to the recommendations found within in the *Purdue Model for Industrial Control Systems* because it is an industry standard when setting up ICS/SCADA networks [19]. The network topology for the lab is highlighted in Table 4.2.

Table 4.2: ICS Lab Network Configurations

Purdue Model	**IP Address**	**Device**
Level 5 - Enterprise	172.16.0.2	Domain Controller
Level 4 - Site Business Systems	n/a	Router/Firewall
Level 3 - Operations and Control	192.168.3.10	Windows 8.1 Workstation
Level 2 - Localized Control	192.168.2.10	SCADA system (Ubuntu 18.04)
Level 1 - Process	192.168.1.10	PLC and Industrial Tower Lamp

4.3 Verification of Lab Environment to ICS Purdue Model

To verify that the lab environment is aligned to the *ICS Purdue Model*, the researcher used firewalls and routers to separate each zone according to the *ICS Purdue Model*. To verify the configurations, the researcher used network protocols to ping the devices in the different layers to ensure that each layer was independent in communication as highlighted in Table 4.3:

Table 4.3: Lab Network Communication Paths

Reference Architecture Layer	**Communication With**
Enterprise Zone	Industrial Demilitarized Zone
Industrial Demilitarized Zone	Industrial Security Zone, Enterprise Zone
Industrial Security Zone	Cell/Area Zone, Industrial Demilitarized Zone
Cell/Area Zone	Industrial Security Zone

4.4 Risk Assessment - ICS Purdue Model Architecture

The researcher configured the lab environment according to the *ICS Purdue Model* and performed a risk assessment on the baseline lab infrastructure to determine the risk posture of the *ICS Purdue Model*. Each assessment was based on the controls within the *Enterprise, Operations, and Process* layers of the *ICS Purdue model*. Risk assessments are used to identify, estimate, and prioritize risk for organizational operations [20]. The risk assessment will be used to identify the following:

- Threats to the *ICS Purdue Model*
- Vulnerabilities
- Impact
- Harm
- Likelihood

4.4.1 Risk Identification

The first step in a risk assessment is identifying all assets and resources within the scope of the assessment [21]. Since this is a lab environment, the assets have already been identified and illustrated in Figure 4.3. The most critical assets within the network are the Active Directory server, SCADA Machine, PLC, and connected tower lamp. The identification of applicable attacks to ICS/SCADA systems are also important. We will use Table 4.4 for the associated attacks to evaluate against ICS/SCADA systems.

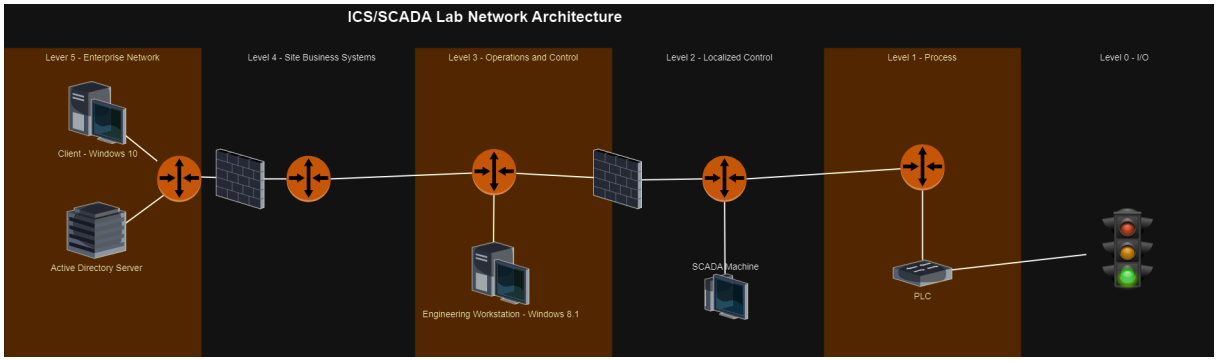


Figure 4.3: Baseline ICS Purdue Model Network Diagram

Table 4.4: Threats, Techniques, and Methods

Threat	**Vulnerability**	**Location**	**Description**
Authorized Access	Basic Authentication Vulnerability	AD Server	Attacker is able to harvest credentials and pivot through the network
Unauthorized Code Execution	Non-sanitized or restricted user input	Operator Console	Attacker is able to gain command and control of the network
Unauthorized devices connected to machine	Networking Misconfiguration	Firewalls, Routers	Adversary are able to maintain access without detection. Possibly exfiltrating data
Denial of Service	Network Misconfiguration	Operator Console	Leads to misconfiguration of PLC and/or losing control of PLC and connected device
Unauthorized Access	Basic Authentication Vulnerability	Enterprise Systems	Attacker can gain insights into the network and possibly exfiltrate data

4.4.2 Risk Analysis

During the *Risk Analysis* phase, the researcher was able to analyze risks and determine the potential impact or *likelihood* to the *ICS Purdue Model* using the risk assessment matrix shown in Figure 4.4. In a risk assessment, "risk likelihood is the probability that a given threat is capable of exploiting a given vulnerability" [21]. Likelihood or probability, in this case, was ranked from 1 - 4. 1 was the "Improbable", while 4 was

"Frequent". The impact or severity in our case was ranked from 1 - "Negligible" to 4 - "Catastrophic". "Impact refers to the magnitude of harm to the organization resulting from the consequences of a threat exploiting a vulnerability" [21]. The impact of the availability, integrity, and confidentiality of the ICS/SCADA system will be assessed in each *Threats, Techniques, and Methods* scenario in Table 4.4. The overall Risk Assessment Matrix Template provided by AllVoices is highlighted in Figure 4.4.

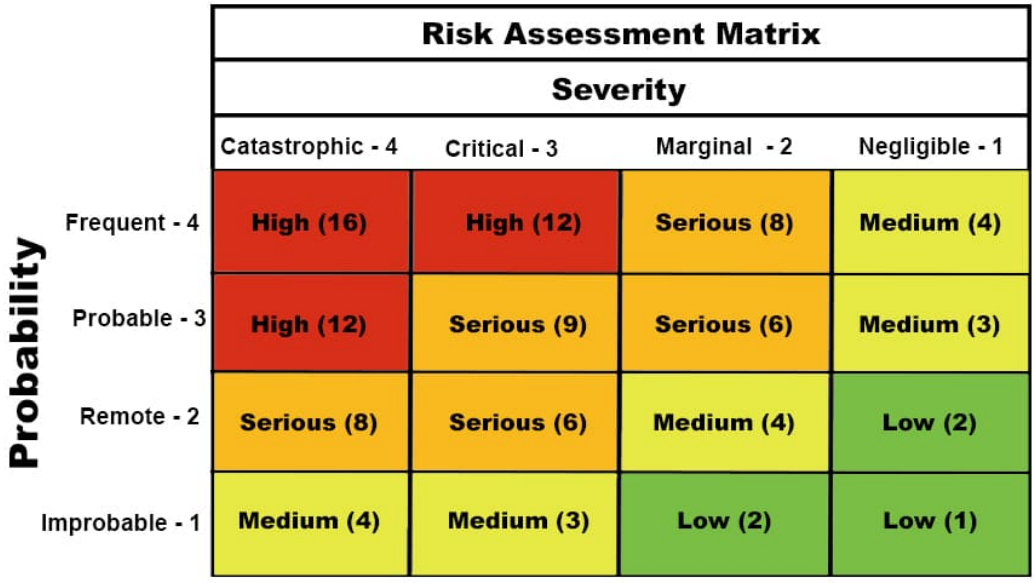


Figure 4.4: Risk Assessment Matrix

4.4.3 Risk Evaluation - ICS Purdue Model Architecture

During the *Risk Evaluation* phase, the researcher completed a risk matrix of the *ICS Purdue Model Architecture* and prioritized the risks based on the risk score received from the risk analysis. A risk impact score will be calculated by multiplying the probability times the likelihood of the event occurring. When doing this type of evaluation, it is important to understand that risk cannot be deleted. Organizations only have the option to *avoid, transfer, or mitigate* the risk identified in the figures below.

Risk mitigation is when security controls are deployed within the environment to reduce the likelihood or impact of the event occurring [21]. For the purpose of this research, all risks will be mitigated with zero trust security controls. However, even with utilizing zero trust, a system with no inherent risk does not exist. There is always risk leftover called *residual risk* [21]. The purpose of this assessment is to mitigate the risk of the *ICS Purdue Model Architecture* by utilizing zero trust controls. Table 4.5 highlights the identifier for each associated vulnerability within Figure 4.5. Table 4.6 highlights the existing security controls inherent in the architecture aligned to the risk score and ICS Purdue Model Layer.

Table 4.5: Vulnerability Alignment

Identifier	Vulnerability
X1	Authorized Access
X2	Unauthorized Code Execution
X3	Unauthorized devices connected to machine
X4	Denial of Service
X5	Unauthorized Access

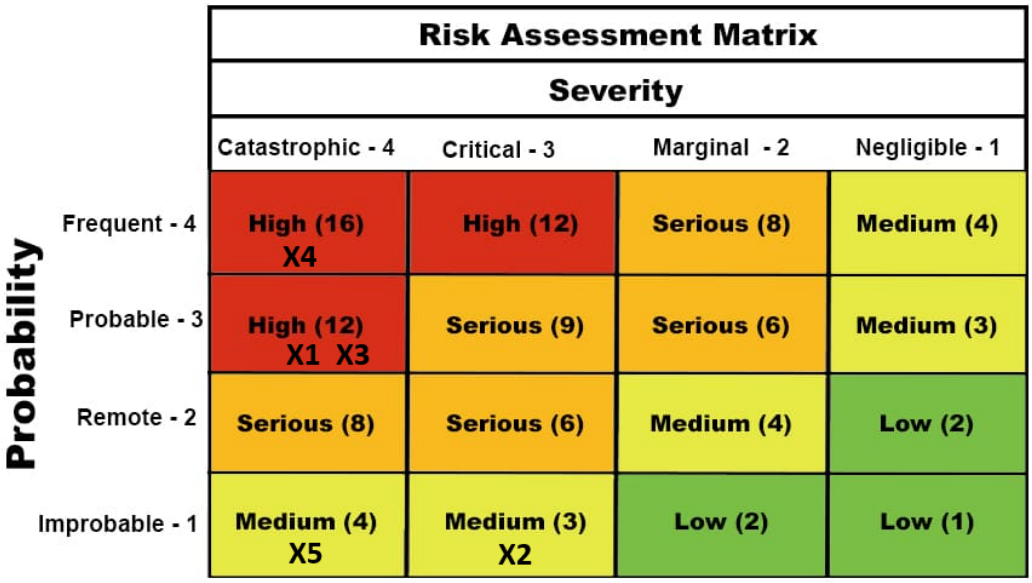


Figure 4.5: ICS Purdue Model Architecture Risk Assessment

Table 4.6: ICS Purdue Model Architecture Security Risks

Identifier	Risk Scenario	Existing Controls	ICS Purdue Model Layer	Current Risk Score
X1	Authorized user gains access to system he or she does not have a need to know on (i.e. Admin assistant gaining access to PLC controller)	Limited Role Base Access Control	Enterprise Zone / IDMZ	12 - HIGH
X2	Unauthorized code is executed on operator workstation to gain command and control of the ICS/SCADA system	Firewall between the two environments	Industrial Security Zone	3 - MEDIUM
X3	Unauthorized command and control network connected to ICS/SCADA network	Firewalls	Cell/Area Zone	12 - HIGH
X4	Denial of Service attack is executed on devices within the environment from command and control network	Firewalls / Routers	Cell/Area Zone	16 - HIGH
X5	Unauthorized access to the enterprise network	Limited Role Based Access Control and Authentication mechanisms	Enterprise Zone	4 - MEDIUM

4.5 ICS Purdue Model Risk Assessment Results

The final step of the risk assessment process is to document all risks assessed in the previous section in a risk register [21]. Table 4.7 outlines what penetration tests were completed to satisfy the outcome of these risk scores before zero trust principles were applied to mitigate risk effectively. It is important to understand that this was a qualitative assessment of risk and that risk scores are subjective to the person who is performing the assessment. The risk assessment results are highlighted in Table 4.7.

Table 4.7: ICS Purdue Model Architecture Risk Score

Identifier	Risk Score
X4	16 - HIGH
X1	12 - HIGH
X3	12 - HIGH
X5	4 - MEDIUM
X2	3 - MEDIUM

4.5.1 ICS Purdue Model Exploits

The researcher was able to successfully exploit the *ICS Purdue Model*. The researcher did this by stepping through enumeration, which highlighted specific details about the target system. By utilizing this information, the researcher could gain command and control of the Industrial Control System within the environment. Sections 4.5.2 and 4.5.3 detail the specific attacks the researcher used to breach the *ICS Purdue Model Architecture*.

4.5.2 Enumeration

Enumeration is the listing of details specific to the target that allows the attacker to gain access to the system [22]. *Enum4linux* is an enumeration command within the Kali distro that allows for target information such as domain, IP address, and known usernames to

be displayed in clear text for the researcher to have additional information to build an attack profile as shown in Figure 4.6.

In Figure 4.6, the researcher has discovered the domain name of the ICS network (LabCorp). Using the information in the enumeration scan, we can run *Kerbrute* against the usernames identified: *administrator, guest, krbgt, domain admins, root.* The researcher also added additional usernames based on the reconnaissance efforts that were previously explained. After running the *Kerbrute* linux package, the researcher found that 2 usernames were valid from the username file, *administrator@labcorp.local* and *allison@labcorp.local* as shown in Figure 4.7.

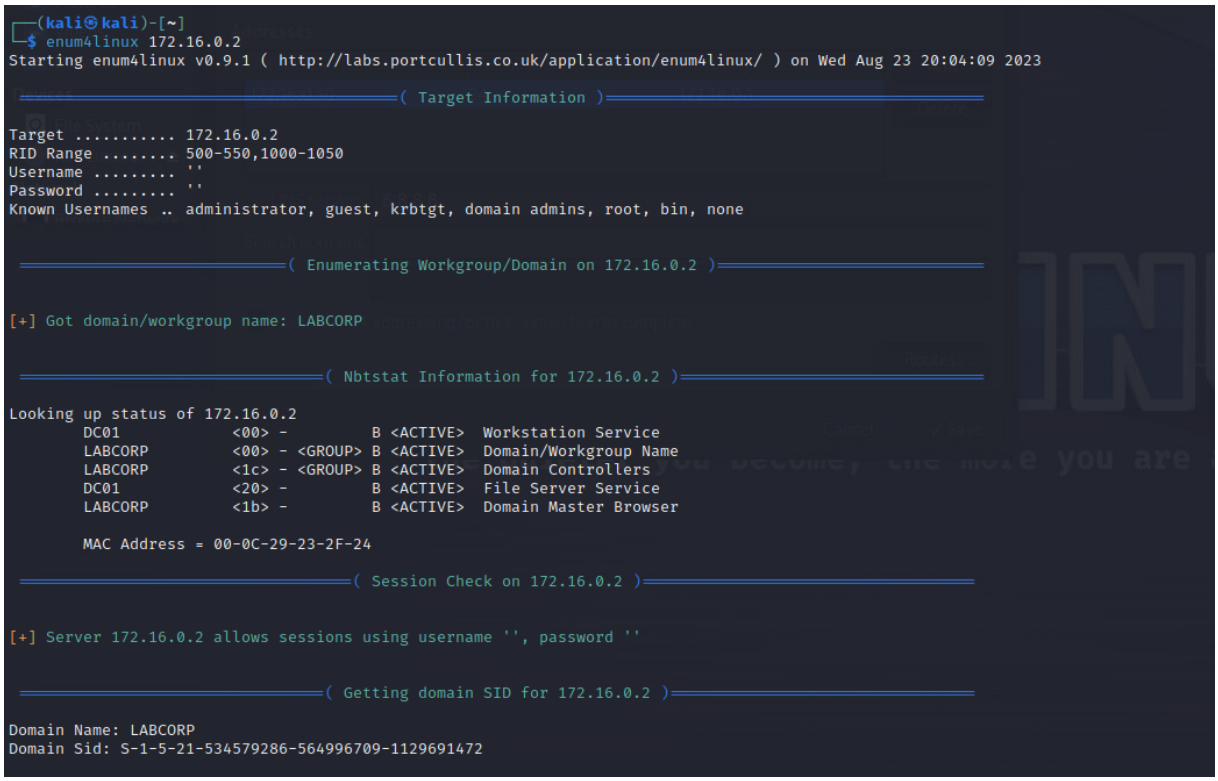


Figure 4.6: enum4linux - Enumeration

The *Impacket* linux package allowed the researcher to discover if kerberos preauthentication was disabled on the identified usernames. found that the *Administrator* user does have kerberos preauthentication disabled. The *Allison* account did not have kerberos preauthentication disabled, therefore the impacket package can extract the ker-

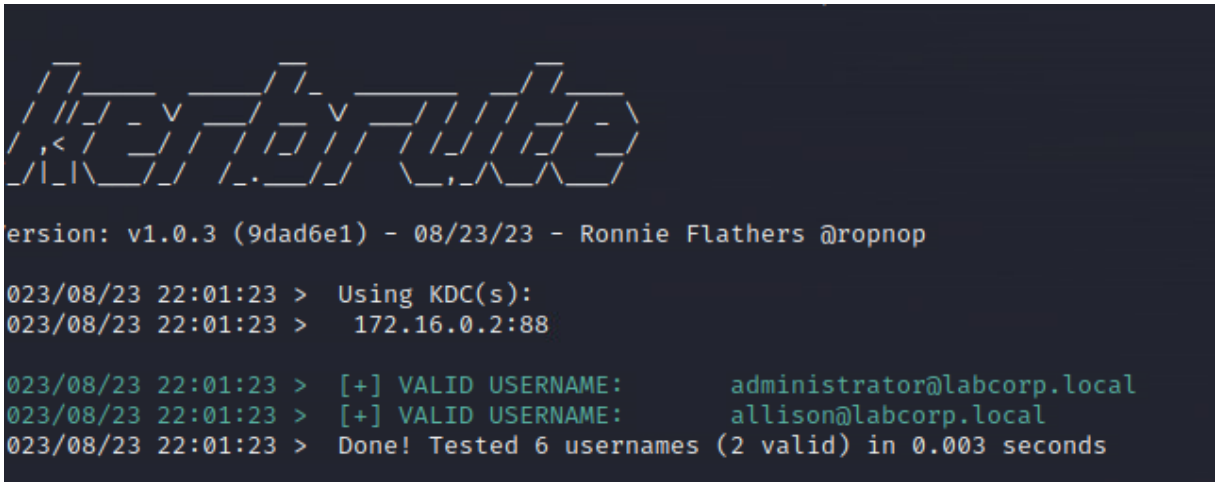


Figure 4.7: Kerbrute - Enumeration

beros preauth hash from the username to enumerate additional users within the domain as depicted in Figure 4.8.

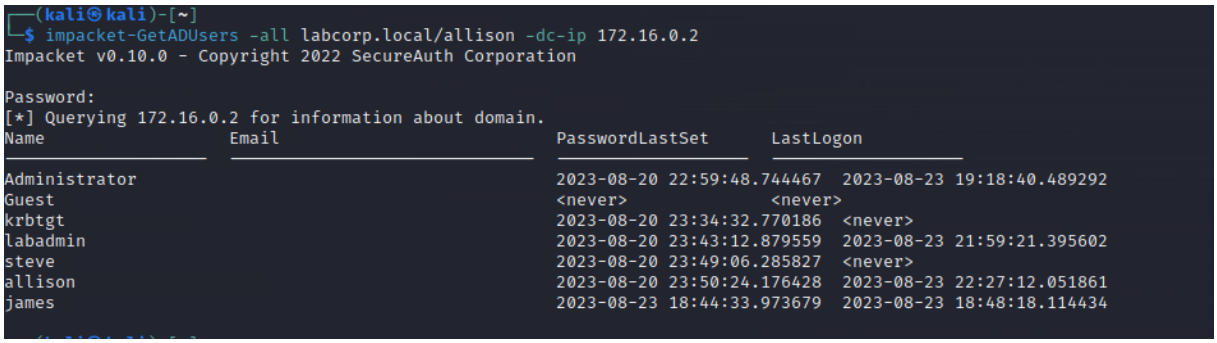


Figure 4.8: Active Directory Users - Enumeration

The kerberos preauthentication hash was also utilized to crack the password for the *allison@labcorp.local* user account. Figure 4.9 shows that the password for the account is *Password2*. Since the researcher has identified an account to utilize within the ICS network, she can use this account to penetrate the ICS network.

For the complexity of the lab, it is assumed that internal network access was already gained through a form of social engineering or phishing attack.

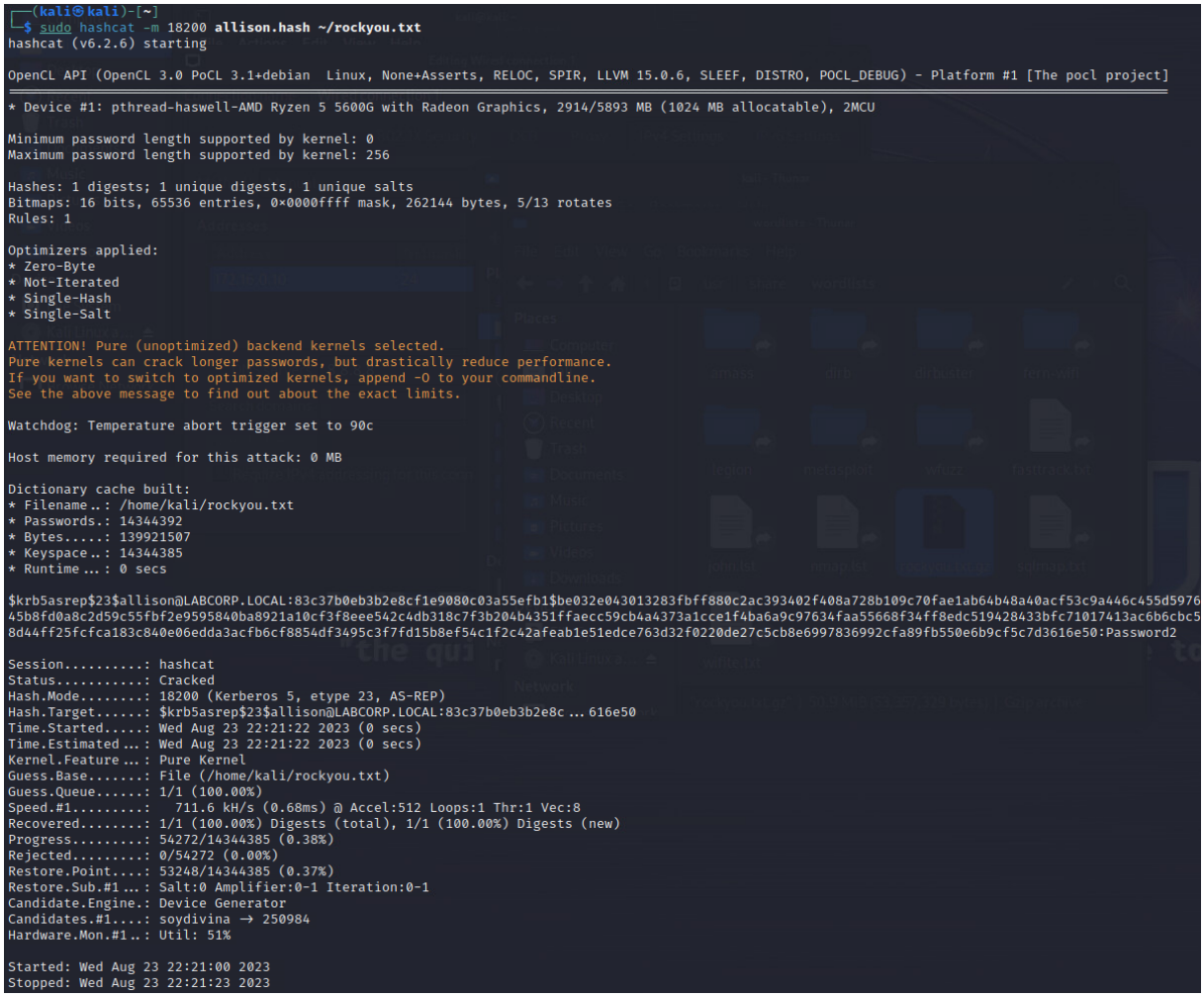


Figure 4.9: HashCat - Enumeration

4.5.3 Gaining Access

The researcher utilized *Evil-WinRm* to gain access to the target system as shown in Figure 4.10. The intelligence collected within the *Enumeration* section aided the researcher in executing a shell on the target system. With this access, the attacker has established a foothold in the system. Since this is not access to the ICS/SCADA machine that is connected at the *Industrial Security Zone* of the ICS model, the researcher has to escalate privileges and navigate to the appropriate level of the network to successfully carry out an attack. The target zone is Level 3, Operations and Control.

The researcher was able to gain access to the enterprise network. *Empire* was utilized

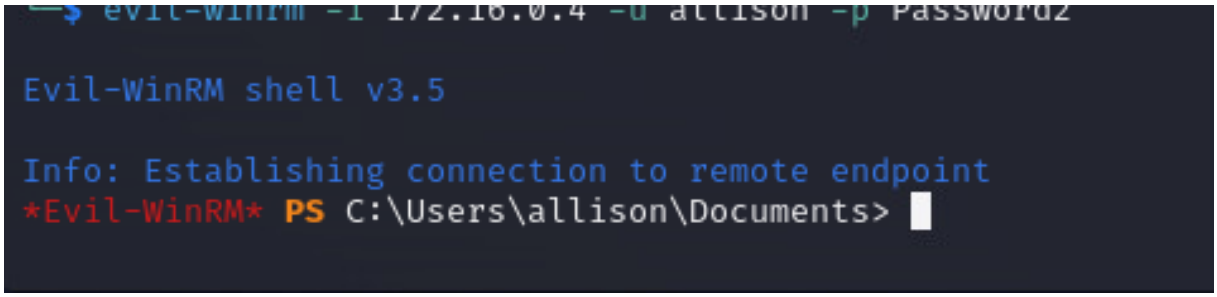


Figure 4.10: Popping a shell

to build a command and control server, allowing the researcher to harvest credentials, find exploitable services, and gain elevated privileges. After the researcher established a shell with the target system, they were able to create an exploit to gain command and control of the system utilizing empire shown in Figure 4.11. This exploit allowed the researcher to gain additional information regarding the networked environment to continue to gain access to the ICS/SCADA system as shown in Figure 4.12. The researcher could enumerate additional users within the *labcorp.local* domain and escalate privileges to the Domain Administrator account. This account allowed the researcher to access the Operator machine within Layer 2 of the *ICS Purdue Model*. Gaining access this deep into the network allows the researcher to manipulate the ICS/SCADA system that is connected to the operator workstation. This is a successful breach of the system.

4.6 Summary and Overall Security Risks of ICS Purdue Model

In summary, the researcher gained access by exploiting the *Enterprise Zone* of the ICS Purdue Model. The researcher could then pivot into the *Cell/Area Zone* to gain command and control of the system. At this level, the researcher could have full control and manipulate data at the process level to cause grave damage to the ICS.

The risk assessment of the *ICS Purdue Model Architecture* shows vulnerabilities within

Figure 4.11: Malicious Script

the model if applied without additional controls. Zero Trust will be utilized as additional compensating controls to complement the ICS Purdue Model architecture. Adding these controls can mitigate the risks within the ICS Purdue Model. Table 4.8 highlights the overall security risks of the *ICS Purdue Model Architecture*:

Table 4.8: ICS Purdue Model Architecture Categorized Security Risks

Risk Category	**Risk Scenario**	**ICS Purdue Model Layer**
Unauthorized Access to system	Authorized user gains access to system he or she does not need to know on (i.e., Admin assistant gaining access to PLC controller)	Enterprise Zone / IDMZ
Code Execution	Unauthorized code is executed on the operator workstation to gain command and control of the ICS/SCADA system	Industrial Security Zone
Man in the Middle	Unauthorized command and control network connected to ICS/SCADA network	Cell/Area Zone
Denial of Service	Denial of Service attack is executed on devices within the environment from the command and control network	Cell/Area Zone
Password Attack	Unauthorized access to the enterprise network	Enterprise Zone

```
(Empire: usestager/multi_launcher) > interact 89CSB5ZY
(Empire: 89CSB5ZY) > info

Agent Options
```

session_id	89CSB5ZY
name	89CSB5ZY
listener	http
host_id	1
hostname	DC01
language	powershell
language_version	5
delay	5
jitter	0.0
external_ip	172.16.0.4
internal_ip	172.16.0.4
username	LABCORP\allison
high_integrity	True
process_id	4484
process_name	powershell
os_details	Microsoft Windows Server 2019 Standard Evaluation
nonce	8107097610354096
checkin_time	2023-08-31T00:20:14+00:00
lastseen_time	2023-08-31T00:25:56+00:00
parent	

Figure 4.12: Empire - Interact

Chapter 5

ENHANCED ICS PURDUE MODEL WITH ZERO TRUST CONTROLS AND RISK ASSESSMENT

The researcher has implemented and tested zero trust security controls to complement the *Purdue Model for ICS Security Model* architecture shown in Figure 5.1. The controls described below were applied to the lab environment and tested against the penetration test scenario defined in the previous chapter to determine applicability and validation. The researcher has divided the solution into the following categories aligned to the *Purdue Model for ICS Security Model* shown in the figure below: Enterprise Zero Trust (Level 5/4), Operations Zero Trust (Level 3/2), Process Zero Trust (Level 1/0). Each network section will have specific controls that enable a zero trust architecture. To come to a definitive solution for the zero trust implementation strategy for ICS/SCADA systems, the applicable logs will be evaluated to validate the control, and the penetration test will be completed.

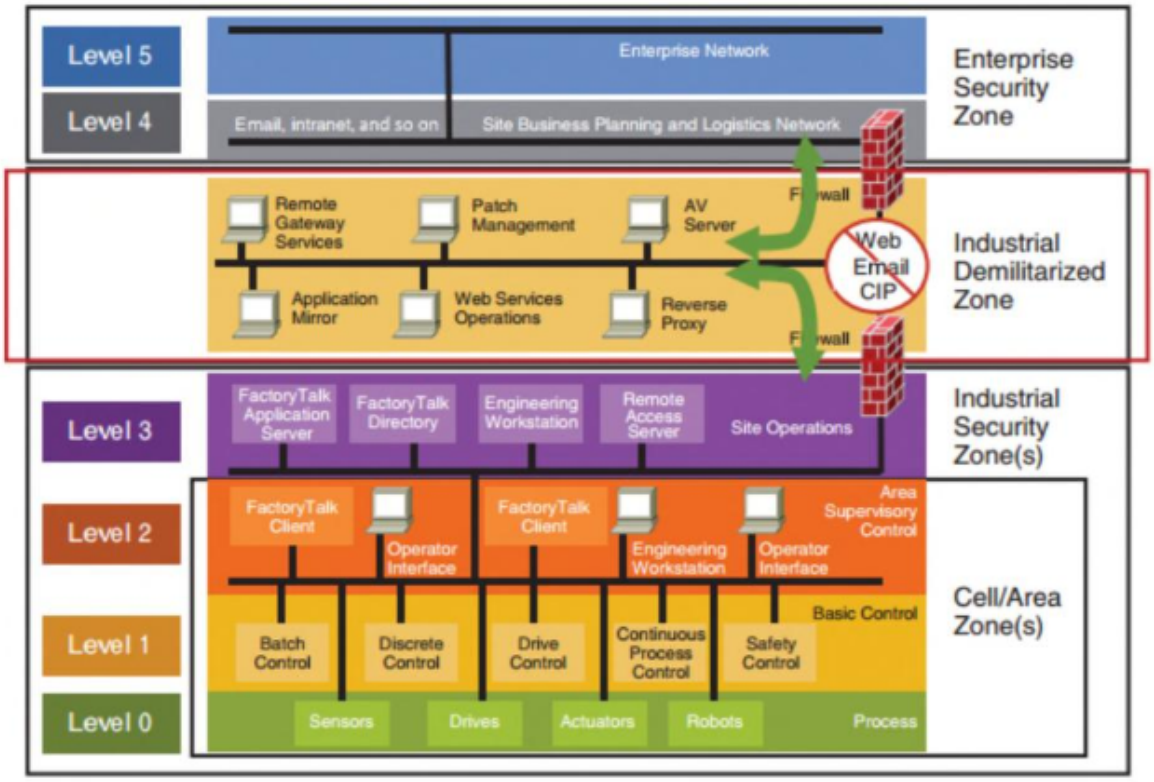


Figure 5.1: Purdue Model for ICS Security

5.1 Zero Trust Background and Motivation

NIST published foundational reference documents highlighting zero-trust concepts. *NIST SP 800-207* sets the framework for Zero Trust Architecture (ZTA). This literature explains the foundational concepts of zero trust principles and gives high-level deployment models within enterprise IT. It is important to understand how zero trust is defined to further understand the researchers' proposed solution for ICS/SCADA systems. Zero trust is a cybersecurity framework that is tailored for resource protection [1]. The central premise of the framework is that "Trust is never granted implicitly but must be continually evaluated" [1]. NIST has also defined ZTA [1] as an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. This is important because zero trust is not a simple technology that can be

purchased and installed within a network, especially within an ICS/SCADA environment. Zero Trust is a collection of concepts and principles that enable a strategy to generate a zero-trust architecture as a plan to be implemented within a network.

NIST focuses on authentication, authorization, and minimizing trust zones within the publication. Zero trust architecture is an end-to-end approach to enterprise resource and data security encompassing identity (person and nonperson entities), credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure [1]. The initial focus should be restricting resources to those needing access and granting only the minimum privileges (e.g., read, write, delete) needed to perform the mission. This methodology allows only authorized users or subjects to access resources or data and excludes all other components [1]. Therefore, as it pertains to ICS/SCADA systems, this can enable the control between the operator console and the ICS/SCADA system.

5.2 Enhanced ICS Purdue Model and Reference Lab Environment

The *Enterprise* layer of the *Purdue Model for ICS Security* is where your enterprise IT systems live (i.e., email, intranet resources, etc.). This layer of the model was the main target when developing the penetration test, which was highlighted in the previous chapter. Breaching this one specific layer allowed the researcher to pivot into deeper layers of the network to gain access to command and control of the ICS/SCADA system.

The recommended controls at this layer include: Risk based multi-factor authentication, identity protection, and next-generation endpoint security to verify a user or systems identity [23]. Corporate assets such as email and data should also be protected through encryption [23]. The traditional IT security approach employed within the network automatically trusted users and endpoints within the organization's perimeter. Therefore,

when the researcher obtained valid credentials, the researcher could pivot to any location within the network. Having the appropriate controls at this layer allows for the reduction of risk and protection against insider threats.

With this zero trust security recommendation, organizations with ICS/SCADA systems must baseline their current infrastructure to validate that the appropriate users and devices have the appropriate privileges and attributes. An enforcement policy will also need to be created that incorporates the risk of the user and device before granting access [1]. NIST refers to this type of transaction as a *Policy Decision Point (PDP)* or *Policy Enforcement Point (PEP)* [1]. The PDP/PEP contains dynamic risk-based policies that allow the entity to access the requested resource. All traffic beyond the PEP has a standard level of trust or implicit trust zone. The PDP/PEP cannot apply additional policies beyond its location in the traffic flow. The implicit trust zone must be as small as possible to allow the PDP/PEP to be as specific as possible. Zero trust provides a set of principles and concepts around moving the PDP/PEPs closer to the resource. The idea is to explicitly authenticate and authorize all subjects, assets, and workflows that make up the enterprise.

Implementing this control will be a continuous effort by the organization that elects to implement this control. All access requests and attributes must be continuously reviewed to ensure that legitimate requests are not blocked due to risk profile and/or data attributes assigned to the subject [23]. Analytics like AI/ML should be used within the network to determine common network paths and completely map what assets communicate to specific resources or data.

The *Operations* layer of the *Purdue Model for ICS* is where the site operations systems (i.e., operator HMI terminals, engineering workstations, and ICS/SCADA system software) live within the network. This layer of the model is where the control for the heart of the ICS/SCADA systems lives. Therefore, the systems in this layer should be protected at all costs. If an attacker has access to the *operations* layer, he or she can

cause grave damage to the system [24]. Access to operational systems is usually granted based on implied trust [24]. This was observed as the researcher was able to breach the trust zone by using stolen credentials of one of the operators, in the previous chapter.

To protect the *Operations* layer, the researcher recommends an Industrial Demilitarized Zone (IDMZ) or micro-segmentation of the assets within the operations layer to further protect the high critical asset from the rest of the network [24]. Micro-segmentation will include the use of firewalls and highly granular access and identity policies. To protect the ICS/SCADA system from the risk of the *Enterprise* layer to create a boundary between the two areas, called an IDMZ [24]. The IDMZ will create a buffer between the operations workstations and the enterprise systems. These two layers should not inherently trust each other, therefore, granular risk based access will be utilized at this layer as well (i.e. PDP/PEP). This boundary should use network and application security controls to manage data flow between the two zones.

The *Process* layer of the *Purdue Model for ICS Security* is where the core of the ICS/SCADA systems live (i.e., actuators, sensors, etc.). Gaining command and control of this layer starts by gaining access to the *Operations* layer. Messages from the *Operations* layer are received by the I/O systems at this layer. The cyber issue with sensors is that the data received at this layer could be incorrect, leading to incorrect control decisions [25]. Since the ICS/SCADA protocols are widely available online, an attacker can learn what type of data can lead to ICS/SCADA control system errors. An example would be if an attacker could spoof the data to manipulate what is seen on the operator's HMI [25]. This will make the operator believe everything is operating normally on the system. Corrupt sensor data could be injected at the sensor itself (Level 0), communication networks between sensor and PLC (Level 1), at the PLC, communications between the PLC and the Level 2 computers, or in the ICS applications at Level 2 [25].

The recommended security control at this layer is authentication of the source system and data integrity [25]. The data integrity solution is called Process Variable Detection

(PVAD). PVAD assesses the Level 0 sensor data risk and determines false data [25]. GE developed a product called *Digital Ghost* that solved this concern. GE was able to develop a digital twin that mapped all system communications and allowed for the identification of rogue sensor data based on the state of the process reported by other sensors. Digital Ghost then calculated what the corrupt sensor value should be and sent that information to the operator [25]. Another method for monitoring the security between the operations layer and the process layer is to create a separate Level 0 monitoring network and compare the sensor data to the reported data from Level 2 received from the Level 0 monitoring network [25]. Example solutions in this area are *SIGA OT Solutions, Cynalytica, Fortiphyd, and Mission Secure.* Actuators are an endpoint in which they do not verify commands but execute whatever is given to them, regardless of the source [25]. To gain more control in this area, actuators need to employ the following:

- Secure Boot
- Authentication of control commands - CIP Secure/Modus Security
- Deep packet inspection firewall

These controls will allow for a more granular approach to securing critical assets. Using a Secure Boot process will prevent DoS attacks from attackers by corrupting the firmware on the actuator. Modbus security allows for the authentication of control commands at the source [25]. A deep packet inspection firewall will restrict access to the devices within Levels 1 and 2 [25]. Examples of a deep packet inspection firewall are: Tofino, M-Guard, and OTfuse [25]. These technologies are usually embedded into the Ethernet card of the PLC. All of the controls of the enhanced model are depicted in Figure 5.2.

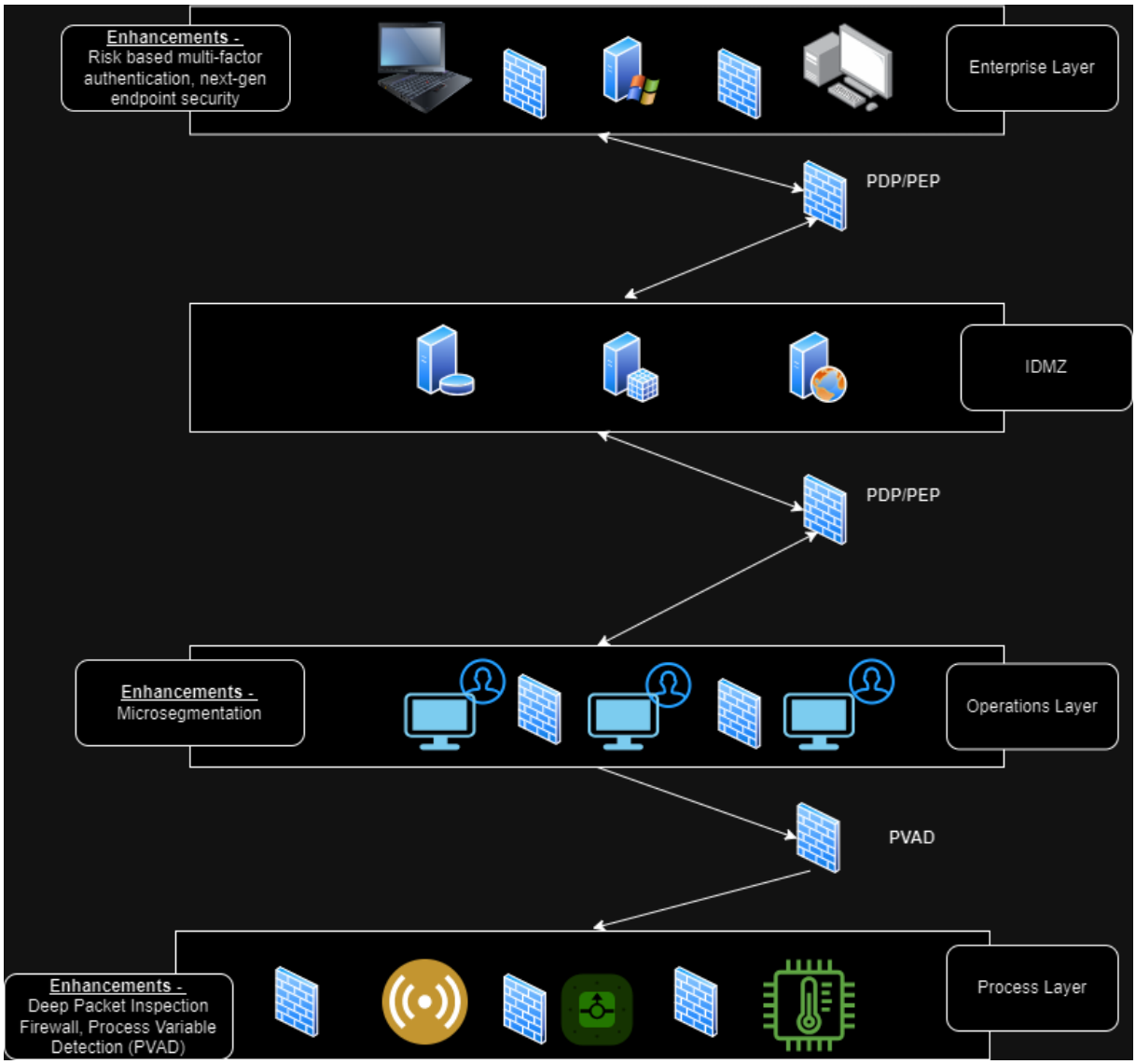


Figure 5.2: Enhanced ICS Model

5.3 Verification of Lab Environment to Enhanced ICS Purdue Model

To verify that the lab environment is aligned to the *Enhanced ICS Purdue Model*, the researcher used firewalls and routers to separate each zone according to the *Enhanced ICS Purdue Model* figure for the PDP/PEP, scripts were utilized to assign risk-based scores to the assets to understand communication paths. If the communication path

was unknown or undocumented with the firewall settings, the packets were automatically dropped. Scripts were also utilized for the risk-based multi-factor authentication in the Enterprise layer. The scripts assigned numeric values to users and higher risk users weren't allowed to access certain assets. To verify the configurations, the researcher used network protocols to ping the devices, ran Wireshark to document network flow in the different layers to ensure that each layer was independent in communication as highlighted in Table 5.1.

Table 5.1: Enhanced ICS Model Lab Network Communication Paths

Reference Architecture Layer	**Communication With**	**Pass-Through Layer**
Enterprise Layer	IDMZ	PDP/PEP
Industrial Demilitarized Zone	Operations Layer, Enterprise Layer	PDP/PEP
Operations Layer	Process Layer, IDMZ	PDP/PEP, PVAD
Process Layer	Operations Layer	PVAD, Deep Inspection Firewall

5.4 Enhanced ICS Purdue Model Exploits

Penetration test scenarios were completed after enhancing the ICS Purdue model. Even in the Enhanced ICS Lab environment configuration, the most important assets within the network are the Active Directory server, SCADA Machine, PLC, and connected tower lamp. The identification of applicable attacks to ICS/SCADA systems are also important. Table 5.2 was used for the associated attacks to evaluate against ICS/SCADA systems.

The researcher was not able to successfully exploit the *Enhanced ICS Purdue Model* utilizing the same penetration test scenarios in the following paragraphs. As done previously, the researcher stepped through enumeration, which highlighted specific details about the target system. By utilizing this information, the researcher could gain command

Table 5.2: Threats, Techniques, and Methods

Threat	Vulnerability	Location	Description
Authorized Access	Basic Authentication Vulnerability	AD Server	Attacker is able to harvest credentials and pivot through the network
Unauthorized Code Execution	Non-sanitized or restricted user input	Operator Console	Attacker is able to gain command and control of the network
Unauthorized devices connected to machine	Networking Misconfiguration	Firewalls, Routers	Adversary can maintain access without detection. Possibly exfiltrate data
Denial of Service	Network Misconfiguration	Operator Console	Leads to misconfiguration of PLC and/or losing control of PLC and connected device
Unauthorized Access	Basic Authentication Vulnerability	Enterprise Systems	Attacker can gain insights into the network and possibly exfiltrate data

and control of the Industrial Control System within the environment. The paragraphs below detail the specific attacks the researcher used to attempt to breach the *Enhanced ICS Purdue Model Architecture*.

5.4.1 Enumeration

Enum4linux was used as previously describe in the penetration test scenario discover target information such as domain, IP address, and known usernames as shown in Figure 5.3. For the complexity of the lab, the researcher did not enable perimeter protections and also assumed that the attacker was on the same LAN network as the ICS system. This will be assumed because in industry, many attackers use social engineering attacks to breach that first layer of protection.

In Figure 5.3, the researcher has discovered the domain name of the ICS network (LabCorp). Using the information in the enumeration scan, the researcher is still able to run *Kerbrute* against the usernames identified: *administrator, guest, krbgt, domain*

admins, root. The researcher was unable to run the *Kerbrute* linux package, as this feature was disabled.

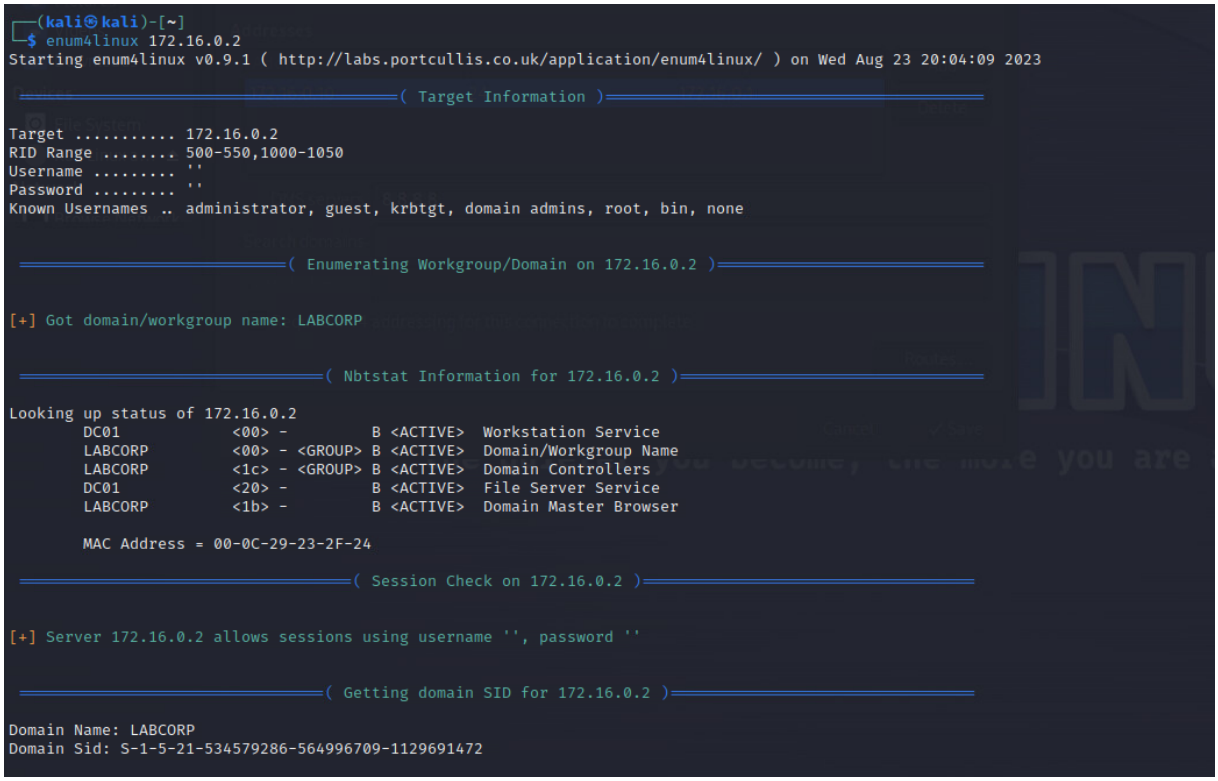


Figure 5.3: enum4linux - Enumeration

The researcher was unable able to use *Impacket* linux package to discover if kerberos preauthentication was disabled on the identified usernames due to the endpoint security now on the endpoint devices. The normal kerberos preauthentication hash would not have worked in this case due to multi-factor authentication also being enabled on the usernames. Because of this, the attacker was never able to breach a valid account with administrator rights to gain command and control of the system.

5.4.2 Unable to Gain Access

The researcher attempted to utilize *Evil-WinRm* to gain access to the target system but was unsuccessful. For the complexity of the lab, the researcher disabled multi-factor authentication and endpoint security to allow for the next phase of penetration tests.

After disabling the control, the researcher executed a shell on the target system. With this access, the attacker has established a foothold in the system. Since this is not access to the ICS/SCADA machine that is connected at the *Industrial Security Zone* of the ICS model, the researcher has to escalate privileges and navigate to the appropriate level of the network to successfully carry out an attack. The target zone is Level 3, Operations and Control.

The researcher was able to gain access to the enterprise network. *Empire* was utilized to build a command and control server, allowing the researcher to harvest credentials, find exploitable services, and gain elevated privileges. This was because the enhanced ICS/Purdue Model controls were disabled to allow for the researcher to continue with the applicable testing.

After the researcher established a shell with the target system, they were able to create an exploit to gain command and control of the system utilizing empire. This exploit allowed the researcher to gain additional information regarding the networked environment to continue to gain access to the ICS/SCADA system. The researcher could enumerate additional users within the *labcorp.local* domain and escalate privileges to the Domain Administrator account. Even with the Domain Administrator account, the researcher was not able to reach the Operator machine within Layer 2 of the *ICS Purdue Model* due to the PDP/PEP now separating the layers.

5.5 Risk Assessment of Enhanced ICS Purdue Model and Results

Overall, after implementing the zero trust controls, risk of ICS/SCADA systems did reduce to an acceptable level. The overall risk score of the environment was a 23 compared to 47 when zero trust principles were not applied as shown in Figure 5.4. The section below analyzes what penetration test was executed and also what control was introduced to

mitigate the risk of the execution. After the zero trust mitigations were applied, none of the penetration tests were able to execute as originally designed for the baseline system which essentially lowered the risk of the overall system as shown in Table 5.3.

The zero trust controls implemented within the *Enterprise* layer of the *Purdue Model for ICS* were: risk based multi-factor authentication, identity protection, and next-generation endpoint security, and data encryption. These controls provided protection against the researcher gaining access to data to compromise credentials within the *Enterprise layer*.

The zero trust controls implemented within the *Operations* layer of the *Purdue Model for ICS* was an Industrial Demilitarized Zone (IDMZ) by utilizing a virtual firewall within the lab network to protect the high critical assets from the rest of the network. The virtual firewall had granular risk based access control policies configured into the firewall to limit access between the two zones.

The zero trust controls implemented within the *Process* layer of the *Purdue Model for ICS Security* was authentication of the source system with a deep packet inspection firewall. Authentication allowed for the authentication of control commands at the source. The deep packet inspection firewall restricted access to the devices within Levels 1 and 2.

5.6 Comparison Assessment of ICS Purdue Model and Enhanced ICS Purdue Model with Zero Trust Controls

The selected zero trust controls from the researcher ultimately mitigated the risks within the *Purdue Model for ICS Security*. As with anything with risk, risk cannot be deleted only mitigated to reduce the risk posture of the system. Therefore, even with the selected controls within the Enhanced Purdue Model for ICS Security risk still remains within the

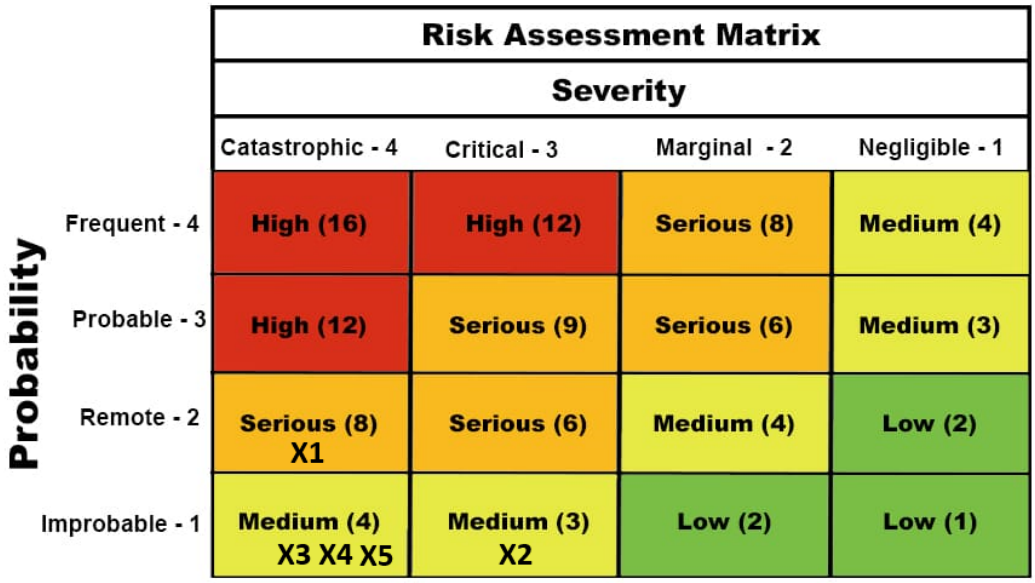


Figure 5.4: Enhanced ICS Purdue Model Risk Assessment Matrix

architecture. Table 5.4 outlines the remaining risk of the model.

5.7 Summary

Overall, the zero trust controls selected was able to protect the lab network against the pre-defined penetration tests that were previously executed. The Penetration tests described in Chapter 4, were identified as potential ways to circumvent the current network controls. Determining how likely those tests will succeed in industry and the impact they may have to the organization's environment is key within the risk assessment. Each penetration test was unable to execute and either did not succeed or did not yield any results that allowed the researcher to gain more information regarding the network to execute an attack.

Table 5.3: Enhanced ICS Purdue Model Risk Score

Identifier	**Risk Scenario**	**Zero Trust Control / Configuration**	**New Risk Score**
X1	Authorized user gains access to system he or she does not have a need to know on	Risk-based multi-factor authentication, PDP/PEP	8 - SERIOUS
X2	Unauthorized code is executed on operator workstation to gain command and control of the ICS/SCADA system	IDMZ, PDP/PEP	3 - MEDIUM
X3	Unauthorized command and control network connected to ICS/SCADA network	Secure Boot, PDP/PEP, IDMZ, PVAD	4 - MEDIUM
X4	Denial of Service attack is executed on devices within the environment from command and control network	PDP/PEP, IDMZ	4 - MEDIUM
X5	Unauthorized access to the enterprise network	Risk based multi-factor authentication, endpoint AV on client machines, PDP/PEP	4 - MEDIUM

Table 5.4: Enhanced ICS Purdue Model Risk Score with Zero Trust Controls

Identifier	Risk Scenario	Zero Trust Control / Configuration	Old Risk Score	New Risk Score
X1	Authorized user gains access to system he or she does not have a need to know on	Risk-based multi-factor authentication, PDP/PEP	12 - HIGH	8 - SERIOUS
X2	Unauthorized code is executed on operator workstation to gain command and control of the ICS/SCADA system	IDMZ, PDP/PEP	3 - MEDIUM	3 - MEDIUM
X3	Unauthorized command and control network connected to ICS/SCADA network	Secure Boot, PDP/PEP, IDMZ, PVAD	12- HIGH	4 - MEDIUM
X4	Denial of Service attack is executed on devices within the environment from command and control network	PDP/PEP, IDMZ	16- HIGH	4 - MEDIUM
X5	Unauthorized access to the enterprise network	Risk based multi-factor authentication, endpoint AV on client machines, PDP/PEP	4-MEDIUM	4 - MEDIUM

Chapter 6

GUIDANCE ON USING ENHANCED ICS PURDUE MODEL

The Enhanced ICS Purdue Model is focused on protecting data, services, enterprise assets, users, and nonhuman entities that request information from ICS/SCADA resources. To implement these types of protections, access to resources is minimized to only the users and nonhuman entities identified as needing access to the resources. The requests of these entities are continuously authenticated and authorized to ensure that their identity is validated [26]. The Enhanced ICS Purdue Model compliments a Zero Trust cybersecurity architecture that is based on zero trust principles [1]. These principles are foundational for preventing data breaches and limiting lateral movement within a system.

6.1 Implementing the Enhanced ICS Purdue Model

Implementing the Enhanced ICS Purdue Model can mitigate the threats industrial control systems face. This enhanced model focuses on the needs of industrial control systems by implementing a network-centric data security strategy that provides specific access only to authorized individuals and/or resources. This addresses the security flaw within the original ICS Purdue Model where data only needs to be protected from outside of the organization. The Enhanced ICS Purdue Model allows for all internal processes to

be authenticated as well to ensure that specific actions are authorized. This allows for proactive cyber defenses to combat the ever-evolving cyber threat the these systems face.

6.1.1 Identifying Assets and Services

The first step in implementing the Enhanced ICS Purdue model is identifying the assets, data, and services on the network. It is also important to identify the network's most critical data, assets and network flows. Within the researcher's lab, the ICS/SCADA components within the network were identified, as well as any associated services, data and network paths. Identifying the critical data and assets also allows you to identify traffic flow and what components are being used within the network. By understanding the behavior of the components within the network, an organization can determine and enforce the policy that ensures secure access to resources.

6.1.2 Policy Configuration

According to *NIST 800-207, Zero Trust Architecture*, Zero Trust Privilege is the concept of granting least privilege access based on verifying the identity, context, and risk of the request. Zero Trust Privilege is designed to handle the complexity of requesters that the ICS systems will receive. It will be important for organizations to identify these requests to understand better how their system communicates.

These requesters can be machines, services, application programming interfaces (APIs), or users [1]. The controls implemented within the lab environment were risk-aware and built upon machine learning (ML), artificial intelligence (AI), and user and entity behavior analytics (UEBA). These technologies allow the ICS/SCADA systems to stay proactive against potent cyber-attacks and detect anomalies in user and entity behavior patterns that may indicate a threat or compromise.

Zero trust policies allow for the understanding of the network flow. Within the lab environment, zero-trust policy was used to whitelist resources authorized to have access

to other resources. With this type of approach, only authenticated and authorized sources are to communicate at all layers of the OSI model. This model attempts to account for all instances of attempted authorization attacks by continually verifying identification and authorization.

6.1.3 Network Segmentation

To be able to effectively apply the Enhanced ICS Purdue Model, the networks within ICS/SCADA systems need to be segmented. Segmentation can be built using a next-generation firewall that creates a micro perimeter around the attack surface. The researcher was able to identify its systems and devices according to the types of access they allow and the categories of information they process.

The segmented networks will be the trust boundaries within the lab environment that allow other security controls to enforce a zero-trust philosophy. Between the trust, boundaries should be firewalls. These firewalls will limit access between the networks. The only traffic allowed should support the needs of the ICS environment. Application inspection technology should also be added to these firewalls at the trust boundary. This allows for the firewall to inspect the contents of the pack to ensure that the traffic being passed has the expected content.

6.1.4 Policy Decision Point / Policy Enforcement Point Configuration

Within the Enhanced ICS Purdue Model, there will be a separation of the communication flows used to control the network and application/services. This will be separated into a control plane for network control communications and a data plane for application/service communication flows. The control plane will be used by ICS/SCADA components to maintain and configure assets. This will also include granting or denying access to

resources. The data plane will be used for communication between software components within the ICS/SCADA system.

The lab network was configured to ensure that the user or service requesting access to resources is authentic and the request is valid by utilizing policy decision points or policy enforcement points (PDP/PEP). The PDP/PEP contains dynamic risk-based policies that allow the entity to access the requested resource. All traffic beyond the PEP has a common level of trust or implicit trust zone [1].

The PDP/PEP cannot apply additional policies beyond its location in the traffic flow. To allow the PDP/PEP to be as specific as possible, the implicit trust zone must be as small as possible. Zero trust provides a set of principles and concepts around moving the PDP/PEPs closer to the resource. The idea is to explicitly authenticate and authorize all subjects, assets, and workflows that make up the enterprise.

The policy decision point (PDP) [1] is broken down into two logical components: the policy engine (PE) and the policy administrator (PA). The policy engine is responsible for granting access to the resource for the requester. The PE uses policy and external sources as its logic source to enforce the appropriate actions of the trust algorithm. The policy engine makes and logs the decision, and the policy administrator executes the decision. The PA is also responsible for establishing and/or shutting down the communication path between a subject and a resource. It would generate any session-specific authentication and authentication token or credential used by a client to access an enterprise resource. If the session is authorized and the request authenticated, the PA configures the PEP to allow the session to start. If the session is denied, the PA signals the PEP to shut down the connection.

6.2 Summary

To effectively migrate to the Enhanced ICS Purdue Model, a phased approach is recommended. The organizations data and assets need to be identified to be able to implement the architecture properly. Without a thorough understanding of an organization's current architecture and the risks associated with that architecture, the organization will not be able to enter a phased approach of implementing an Enhanced ICS Purdue Model.

The organization looking to implement this model needs to have a thorough understanding of its infrastructure to ensure that the PE enforces accurate policy decisions. Incomplete infrastructure awareness would lead to the PE denying legitimate requests for resources and can lead to cost and schedule impacts for the organization.

Chapter 7

SUMMARY AND CONCLUSION

ICS/SCADA systems are a mission critical technology with specific mission objectives that separates itself from traditional IT technology. Many of the guidelines and policies introduced by NIST and other agencies are based on generic enterprise IT approaches. This approach is not sufficient enough to address the vulnerabilities within ICS/SCADA systems and address the mission critical nature of the operational technology that are utilized in mission operations. The Enhanced ICS Purdue Model is a proactive solution that will increase the cyber posture of OT environments and effectively mitigate risk. Protecting mission critical operational technology is very important to our nation and the cyber architecture protecting OT should be resilient in nature to withstand cyber-attacks. The Enhanced ICS Purdue Model can augment OT's current security architecture to enhance cyber posture.

7.1 Research Findings and Contributions

The purpose of this research is to bring awareness to the vulnerabilities within the ICS Purdue Model which is the industry standard for ICS/SCADA systems for configuration. Additional cyber controls need to be considered to mitigate risk of the ICS Purdue Model. ICS/SCADA systems are utilized in many organizations across the United States, from manufacturing, weapon systems, power grids and many more. The goal of the research is

to develop an Enhanced ICS Purdue model to address the gaps within the current ICS Purdue Model.

The researcher has implemented and tested zero trust security controls to compliment the *Purdue Model for ICS Security Model* architecture. The controls below were applied to a lab environment and tested against the penetration test scenario defined in the previous chapter to determine applicability and validation. The researcher has divided the solution into the following categories aligned to the *Purdue Model for ICS Security Model* shown in the figure below: Enterprise Zero Trust (Level 5/4), Operations Zero Trust (Level 3/2), Process Zero Trust (Level 1/0). Each section of the network will have specific controls that enable a zero trust architecture.

The *Enterprise* layer of the *Purdue Model for ICS* is where your enterprise IT systems live (i.e. email, intranet resources, etc.). The recommended controls at this layer include: risk based multi-factor authentication, identity protection, and next-generation endpoint security to verify a user or systems identity [23]. Corporate assets such as email and data should also be protected through encryption [23]. Having the appropriate controls at this layer allows for the reduction of risk and also allows for protection against insider threats.

With this zero trust security recommendation, organizations with ICS/SCADA systems need to baseline their current infrastructure to validate that the appropriate users and devices have the appropriate privileges and attributes. An enforcement policy will also need to be created that incorporates risk of the user and device before granting access [1]. NIST refers to this type of transaction as a *Policy Decision Point (PDP)* or *Policy Enforcement Point (PEP)* [1]. The PDP/PEP contains dynamic risk-based policies that allow the entity to access the requested resource. All traffic beyond the PEP has a common level of trust or implicit trust zone. The PDP/PEP cannot apply additional policies beyond its location in the traffic flow. The implicit trust zone must be as small as possible to allow the PDP/PEP to be as specific as possible. Zero trust provides a set of principles and concepts around moving the PDP/PEPs closer to the resource. The idea

is to explicitly authenticate and authorize all subjects, assets, and workflows that make up the enterprise.

The *Operations* layer of the *Purdue Model for ICS* is where the site operations systems (i.e. operator HMI terminals, engineering workstations, and ICS/SCADA system software) live within the network. To protect the *Operations* layer, the researcher recommends an Industrial Demilitarized Zone (IDMZ) or microsegmentation of the assets within the operations layer to further protect the high critical asset from the rest of the network [24].The IDMZ will create a buffer between the operations workstations and the enterprise systems. These two layers should not inherently trust each other, therefore, granular risk based access will be utilized at this layer as well (i.e. PDP/PEP). This boundary should use network and application security controls to manage the flow of data between the two zones.

The *Process* layer of the *Purdue Model for ICS Security* is where the core of the ICS/SCADA systems live (i.e. actuators, sensors, etc.). Gaining command and control of this layer starts by gaining access to the *Operations* layer. Messages from the *Operations* layer are received by the I/O systems at this layer. Bad sensor data could be injected at the sensor itself (Level 0), communication networks between sensor and PLC (Level 1), at the PLC, communications between the PLC and the Level 2 computers, or in the ICS applications at Level 2 [25]. The recommended security control at this layer is authentication of the source system and data integrity [25]. The data integrity solution is called Process Variable Detection (PVAD). PVAD assesses the risk of Level 0 sensor data and determines false data [25]. Another method for monitoring the security between the operations layer and the process layer is to create a separate Level 0 monitoring network and compare the sensor data to the reported data from Level 2 received from the Level 0 monitoring network [25]. Example solutions in this area are *SIGA OT Solutions, Cynalytica, Fortiphyd, and Mission Secure.* Actuators are an endpoint in which they do not verify commands but just execute whatever is given to them, regardless of the source

[25]. In order to gain more control in this area, actuators need to employ the following:

- Secure Boot
- Authentication of control commands - CIP Secure/Modus Security
- Deep packet inspection firewall

These controls will allow for a more granular approach to securing the most critical assets. Using a Secure Boot process will prevent DoS attacks from attackers by corrupting the firmware on the actuator.

This research will contribute to the ICS Purdue Model and other NIST operational technology guidance that has been released. This research offers a different perspective to secure ICS/SCADA systems outside out the Enterprise IT perspective which can be limited in its ability to protect operational technology due to the mission critical nature of their operations.

7.2 Research Challenges and Limitations

With the understanding of how important the 24/7/365 nature of these assets are, it is important that those limitations are considered when developing a cyber security strategy to protect mission critical assets. This research became challenging when looking for industry standard equipment. The researcher was able to find one but it was not connected to a real mission critical platform. This limited the research because there was no connection to how much real damage the penetration tests could do if truly in an operational scenario. Many ICS/SCADA systems are also aged and maybe way pass their end-of-life (EOL) maintenance schedule. This also presented a challenge to the researcher because the researcher could only locate PLC controllers that were still being produced and had a maintenance contract associated with them. There are many special scenarios as it

pertains to ICS/SCADA systems as it will be extremely difficult to process each scenario within the researcher's lab.

7.3 Future Work

In the future, to further enhance the ICS Purdue Model, the researcher can look to develop trust algorithms to enable automation and heuristics within the ICS Purdue Model. A trust algorithm (TA) is used by the policy engine to grant or deny access to resources. The policy engine takes input from multiple sources. The priority set by the PE regarding what data source is of higher importance can be configured by the energy sector. After the assessment has been made against the external sources, the PE passes its decision to the PA to be executed [1]. The decision is then logged and should be ingested by SIEM technology. If the decision is a "deny access," or if the PE gives the PA a signal to terminate the connection based on external sources, the PA will issue the terminate command to end communications [1]. The trust algorithm for ICS/SCADA systems will be utilized as an evaluation method in which requests are evaluated in relation to other requests by the same entity.

By utilizing a contextual criteria-based TA, ICS/SCADA systems can set qualified attributes that must be met before access is granted to a resource. These criteria is set across the enterprise and can be tailored for specific ICS/SCADA systems within the enterprise. Access will be granted to the specific resource only if certain attributes are met. The contextual aspect of the TA allows for the requester's recent history to be evaluated in the evaluation process [1]. This approach gets into behavior analytics because if the requester does not normally request access to the specific resource, this can be seen as a red flag to the security operator and can be logged for further analysis or implicitly denied based on the policy set. Contextual criteria-based TA's can mitigate threats that are "low and slow attacks". These are attacks where an attacker stays close to a "normal" set of

access requests for a compromised subject account or insider attack [1]. An example of how a contextual TA can be configured within an mission operations environment, is if an operator is making requests to the PLC controllers within the ICS/SCADA system after normal business hours, it can flag the communication as a potential attack. The granularity of this logic can be adjusted if too many false positives are detected. There will be a "tuning" phase of this type of configuration because the system will need to get adjusted to what normal communications of the system are. Criteria may need to be adjusted to ensure that the policies are enforced while still allowing the operational technology's mission to function.

7.4 Conclusion

In conclusion, there have been great strides to secure ICS/SCADA systems. Many of the guidelines and policies introduced by NIST and other agencies are based on a generic enterprise IT approach. This approach is not sufficient enough to address the vulnerabilities within ICS/SCADA systems and address the specific issues that these platforms face with their mission specific requirements. The Enhanced ICS Purdue Model is a proactive solution that will increase the cyber posture of ICS/SCADA systems and effectively mitigate risk. Protecting ICS/SCADA systems is very important due to the systems these platforms support. Many of these systems are apart of the critical infrastructure that have 24/7/365 operational requirements. The Enhanced ICS Purdue Model can augment organization's current security architectures to enhance its cyber posture. This will allow for them to transition some of their aged and unsupported systems within their infrastructures into modern-day technology, more resilient to cyber-attacks.

This granular approach to cybersecurity will allow organization's with ICS/SCADA systems to decrease risk within their network and ensure a resilient approach to continually providing the operational services that these systems provide today. This is required in

today's forever-changing cyber environment because of the adversaries that ICS/SCADA systems face. The adversary will only get stronger with their approaches, so it is important for ICS/SCADA systems to become proactive and embrace cyber resiliency within their cyber architectures.

References

[1] A. Kerman, M. Souppaya, S. Symington, K. Scarfone, and W. Barker, *Implementing a zero trust architecture draft*, en, Dec. 2022. [Online]. Available: https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf.

[2] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, and S. Lightman, "Guide to operational technology (ot) security," *NIST Special Publication*, vol. NIST SP 800-82r3 ipd, pp. 41–133, 2022. DOI: https://doi.org/10.6028/NIST.SP.800-82r3.ipd.

[3] N. Andravous, *ZERO TRUST SECURITY: A Complete Guide* (ITpro collection). BPB PUBLICATIONS, 2022, ISBN: 9789355512512. [Online]. Available: https://books.google.com/books?id=LXM3zwEACAAJ.

[4] *Zero trust maturity model — cisa*. [Online]. Available: https://www.cisa.gov/zero-trust-maturity-model.

[5] S. Durbin, *Securing industrial control systems: The what, why and how*, Sep. 2022. [Online]. Available: https://www.forbes.com/sites/forbesbusinesscouncil/2022/08/30/securing-industrial-control-systems-the-what-why-and-how/?sh=61390d627f25.

[6] T. Macaulay and B. Singer, *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS*. CRC Press, 2016, ISBN: 9781466516113. [Online]. Available: https://books.google.com/books?id=YBM3cwTNwj0C.

[7] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, and S. Lightman, "Guide to operational technology (ot) security," *NIST Special Publication*, r3, vol. 800, no. 82, Apr. 2022. DOI: 10.6028/nist.sp.800-82r3.ipd.

[8] P. Ackerman, *Industrial Cybersecurity: Efficiently secure critical infrastructure systems*. Packt Publishing, 2017, ISBN: 9781788395984. [Online]. Available: https://books.google.com/books?id=FhlKDwAAQBAJ.

[9] *Cybersecurity capability maturity model (c2m2)*, Jun. 2022. [Online]. Available: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

[10] *Dhs announces new cybersecurity requirements for critical pipeline owners and operators*, May 2021. [Online]. Available: https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators.

[11] *Framework for improving critical infrastructure cybersecurity*, en, Feb. 2014. [Online]. Available: https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[12] K. Stine, "Framework for improving critical infrastructure cybersecurity, version 1.0," *NIST*, vol. 1.1, Apr. 2018. DOI: 10.6028/nist.cswp.1.

[13] A. Alagappan, S. K. Venkatachary, and L. J. B. Andrews, "Augmenting zero trust network architecture to enhance security in virtual power plants," *Energy Reports*, vol. 8, pp. 1309–1320, 2022, ISSN: 2352-4847. DOI: https://doi.org/10.1016/j.egyr.2021.11.272. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352484721014190.

[14] B. Paul and M. Rao, "Zero-trust model for smart manufacturing industry," *Applied Sciences*, vol. 13, no. 1, 2023, ISSN: 2076-3417. DOI: 10.3390/app13010221. [Online]. Available: https://www.mdpi.com/2076-3417/13/1/221.

[15] A. W. Mir and K. R. Ram Kumar, "Zero trust user access and identity security in smart grid based scada systems," in *Proceedings of the 12th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2020)*, A. Abraham, Y. Ohsawa, N. Gandhi, *et al.*, Eds., Cham: Springer International Publishing, 2021, pp. 716–726, ISBN: 978-3-030-73689-7.

[16] J. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications, 2014, ISBN: 9781452226101. [Online]. Available: https://books.google.com/books?id=4uB76IC_pOQC.

[17] R. Wieringa, "Design science methodology for information systems and software engineering," in *Springer Berlin Heidelberg*, 2014.

[18] P. Smith, *Pentesting Industrial Control Systems: An ethical hacker's guide to analyzing, compromising, mitigating, and securing industrial processes*. Packt Publishing, 2021, ISBN: 9781800207288. [Online]. Available: https://books.google.com/books?id=hzZKEAAAQBAJ.

[19] P. Ackerman, *Industrial Cybersecurity: Efficiently monitor the cybersecurity posture of your ICS environment*. Packt Publishing, 2021, ISBN: 9781800205826. [Online]. Available: https://books.google.com/books?id=olZBEAAAQBAJ.

[20] G Stoneburner, A. Goguen, and A. Feringa, *Risk management guide for information technology systems*, en, Jul. 2002. DOI: https://doi.org/10.6028/nist.sp.800-30.

[21] M. Cobb, *How to perform a cybersecurity risk assessment in 5 steps: Techtarget*, Nov. 2022. [Online]. Available: https://www.techtarget.com/searchsecurity/tip/How-to-perform-a-cybersecurity-risk-assessment-step-by-step.

[22] M. Walker, *CEH Certified Ethical Hacker: All-in-one exam guide*, 4th ed. McGraw-Hill Education, 2019.

[23] K. Raina, *What is zero trust security? principles of the zero trust model*, Apr. 2023. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/.

[24] J. Newton, *The importance of an idmz in a perimeterless world*, Mar. 2021. [Online]. Available: https://www.rockwellautomation.com/en-us/company/news/blogs/idmz-perimeterless-world.html.

[25] D. Peterson, *Recommended security controls for level 0 and level 1*, Mar. 2021. [Online]. Available: https://dale-peterson.com/2021/03/30/recommended-security-controls-for-level-0-and-level-1/.

[26] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, *Zero trust architecture*, en, Aug. 2020. DOI: https://doi.org/10.6028/NIST.SP.800-207. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930420.