



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**ANALYSIS OF THE FEASIBILITY AND BENEFIT
OF APPLYING ZERO TRUST PARADIGM
TO OPERATIONAL TECHNOLOGY SYSTEMS**

by

Meng Wee Song

September 2023

Thesis Advisor:
Co-Advisor:

Thuy D. Nguyen
Cynthia E. Irvine

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE September 2023	3. REPORT TYPE AND DATES COVERED Master's thesis	
4. TITLE AND SUBTITLE ANALYSIS OF THE FEASIBILITY AND BENEFIT OF APPLYING ZERO TRUST PARADIGM TO OPERATIONAL TECHNOLOGY SYSTEMS			5. FUNDING NUMBERS	
6. AUTHOR(S) Meng Wee Song				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) In response to evolving business demands, modern operational technology (OT) systems are increasingly exposed to external information technology (IT) environments. Consequently, their vulnerability to contemporary cybersecurity threats from legacy software and hardware necessitates proactive measures. While the Zero Trust (ZT) paradigm, outlined in NIST SP 800 207, has been embraced within IT systems, its use in OT systems remains largely uncharted. This work assessed the applicability of the ZT architectural model to modernize and secure critical OT systems. Our methodology commenced by defining requirements for OT systems, focusing on enabling remote access and bring your own device (BYOD). We then conducted threat modelling to identify potential vulnerabilities and formulated a cybersecurity policy for a water treatment plant. We designed the ZT-OT architecture, which applies the ZT tenets to protect a water treatment OT system. This architecture was evaluated against real-world use cases and preliminary results showed that a ZT approach can help mitigate vulnerabilities associated with remote access and BYOD threats in specific cases. Yet, limitations surfaced concerning legacy components and ZT effects on normal operation. This research advances security in water treatment OT systems across governmental and industrial domains, offering insights into ZT potential and challenges.				
14. SUBJECT TERMS zero trust, operational technology, industrial control systems, remote access, bring-your-own-device, BYOD			15. NUMBER OF PAGES 81	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**ANALYSIS OF THE FEASIBILITY AND BENEFIT OF APPLYING ZERO
TRUST PARADIGM TO OPERATIONAL TECHNOLOGY SYSTEMS**

Meng Wee Song
Civilian, ST Engineering
BE, National University of Singapore, 2016
MCS, National University of Singapore, 2018

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

**NAVAL POSTGRADUATE SCHOOL
September 2023**

Approved by: Thuy D. Nguyen
Advisor

Cynthia E. Irvine
Co-Advisor

Gurminder Singh
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In response to evolving business demands, modern operational technology (OT) systems are increasingly exposed to external information technology (IT) environments. Consequently, their vulnerability to contemporary cybersecurity threats from legacy software and hardware necessitates proactive measures. While the Zero Trust (ZT) paradigm, outlined in NIST SP 800 207, has been embraced within IT systems, its use in OT systems remains largely uncharted. This work assessed the applicability of the ZT architectural model to modernize and secure critical OT systems. Our methodology commenced by defining requirements for OT systems, focusing on enabling remote access and bring your own device (BYOD). We then conducted threat modelling to identify potential vulnerabilities and formulated a cybersecurity policy for a water treatment plant. We designed the ZT-OT architecture, which applies the ZT tenets to protect a water treatment OT system. This architecture was evaluated against real-world use cases and preliminary results showed that a ZT approach can help mitigate vulnerabilities associated with remote access and BYOD threats in specific cases. Yet, limitations surfaced concerning legacy components and ZT effects on normal operation. This research advances security in water treatment OT systems across governmental and industrial domains, offering insights into ZT potential and challenges.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	MOTIVATION	1
B.	RESEARCH APPROACH.....	2
C.	THESIS ORGANIZATION.....	3
II.	BACKGROUND	5
A.	OPERATIONAL TECHNOLOGY AND CYBERSECURITY	5
1.	Cybersecurity Issues in a Modern OT System	6
2.	Cybersecurity Controls for OT Systems.....	8
3.	OT-Related Cyber Incidents.....	10
4.	OT Systems Used in Water Treatment Process	11
B.	ZERO TRUST PARADIGM	13
1.	Tenets of Zero Trust	13
2.	Logical Components of Zero Trust	14
3.	Supporting Components of Zero Trust.....	15
C.	PRIOR WORK.....	16
III.	ZERO TRUST FOR A WATER PLANT.....	19
A.	CONCEPT OF OPERATIONS	19
1.	User Roles	19
2.	Operational Requirements.....	20
B.	THREAT MODEL	21
1.	Identify Requirements	21
2.	Identify and Assess Threats.	22
C.	ASSUMPTIONS.....	22
D.	CYBERSECURITY POLICY	23
E.	CYBERSECURITY REQUIREMENTS	23
F.	SECURE WATER TREATMENT PLANT ARCHITECTURE	23
1.	Securing Remote Connection.....	24
2.	Securing BYOD.....	25
3.	Securing Remote Connection and BYOD.....	26
4.	Zero Trust Design (ZT-OT)	27
IV.	ANALYSIS OF ZT-OT DESIGN	37
A.	A HYPOTHETICAL WATER PLANT	37
1.	Assumptions	37

B.	ANALYZING ZT-OT DESIGN	40
1.	Use Case 1 Analysis: Replacement of Reverse Osmosis Filter	40
2.	Use Case 2 Analysis: Abnormal Water Parameter During Afterhours.....	43
3.	Use Case 3 Analysis: Patching of the SCADA System.....	46
C.	STRENGTH OF ZT-OT	52
1.	Securing Remote Connection.....	52
2.	Securing BYOD.....	52
D.	WEAKNESS OF ZT-OT.....	53
1.	Reliance on Software Agent and Risk of Compromised Agent	53
2.	Compromised Trusted Zone	54
3.	Single Point of Failure	54
V.	CONCLUSION	57
A.	SUMMARY	57
B.	FUTURE WORK.....	58
	LIST OF REFERENCES.....	59
	INITIAL DISTRIBUTION LIST	63

LIST OF FIGURES

Figure 1.	Purdue Model Architecture for ICS. Source: [14]	9
Figure 2.	SUTD secure water testbed processes. Source: [24]	12
Figure 3.	SUTD secure water testbed system architecture. Source: [24].....	12
Figure 4.	NIST ZTA reference architecture. Source [25]	15
Figure 5.	SWAT architecture with secure remote connection without BYOD.....	24
Figure 6.	SWAT architecture with secure BYOD without remote connection.....	26
Figure 7.	SWAT architecture with secure remote connection and BYOD	27
Figure 8.	NIST SP800-207 Enclave Gateway Model. Source: [2]	28
Figure 9.	SWAT architecture with Zero Trust (ZT-OT).....	33
Figure 10.	Sequence diagram for Use Case 1: Replacement of reverse osmosis filter.....	42
Figure 11.	Sequence diagram for Use Case 2: Abnormal water parameter during afterhours	46
Figure 12.	Sequence diagram for Use Case 3: Patching of the SCADA system	51

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	ZT-OT logging requests classifications	35
----------	--	----

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AWWA	American Water Works Association
CCOP	Cybersecurity Code of Practice
CISO	Chief Information Security Officer
CSA	Cybersecurity Agency of Singapore
EDR	Endpoint Detection and Response
EWS	Engineering Workstation
IAM	Identity and Access Management
ICAM	Identity, Credential and Access Management
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IPS	Intrusion Prevention System
ISA	International Society of Automation
IT	Information Technology
NIST	National Institute of Standards and Technology
OT	Operational Technology
PDP	Policy Decision Point
PE	Policy Enforcement
PEP	Policy Enforcement Point
PIP	Policy Information Point
PLC	Programmable Logic Controller
PUB	Public Utilities Board of Singapore
S7	Siemens Step 7
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Incident and Event Management
SNMP	Simple Network Management Protocol
SOAR	Security Orchestration and Response
SOC	Security Operation Centre
SUTD	Singapore University of Technology and Design
SWAT	Secure Water Treatment

TPM	Trusted Platform Module
UEBA	User and Entity Behavioral Analytics
UEM	Unified Endpoint Management
VPN	Virtual Private Network
WTP	Water Treatment Plant
ZT	Zero Trust
ZTA	Zero Trust Architecture

ACKNOWLEDGMENTS

I would like to express my heartfelt thanks to my thesis advisors, Professor Thuy Nguyen and Dr. Cynthia Irvine. I am thankful and grateful for the guidance and support they have provided throughout this process. I have always enjoyed the intensity and creativity of the discussions that we had every week, where ideas were generated and always challenged.

Dr. Lim Woo Lip and Dr. Lee Shiang Long at Singapore Technologies have both been great assets and provided excellent support for my project and were always available when I required additional help.

I would also like to thank Mr. Goh Eng Choon for without him, I would not have been given the opportunity to partake in this amazing journey both at the National University of Singapore and the Naval Postgraduate School.

Then there is everyone who is in the Masters of Defense and Technology course who has shared laughter, hardship, and long nights over the entire course of 18 months. You guys have made the last 18 months amazing.

Being a foreign student, I am lucky to have the full support of my parents and siblings back home in Singapore to ensure that all is well. This has given me peace of mind to focus on and pursue my studies 9,000 miles away from home.

Most importantly, I am grateful for my wife, Hwee Ling, who provided me with all the love and support that I could have never dreamed of. Your trust and commitment in me during this time is more than I could ever ask for and I look forward to our future together. I am truly thankful to have you by my side.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Industrial control systems (ICS) are computer systems that control processes in critical sectors such as water treatment and reclamation; power generation and distributions; and train rail signaling [1]. These systems control processes such as chemical dosing, reading water levels, switching power transmission, and so on within these sectors. ICS belongs to a greater group of systems more commonly called operational technology (OT). OT systems, compared to their counterpart, information technology (IT) systems, prioritize reliability and robustness over flexibility, ease of use and cybersecurity, and can operate for decades before needing a replacement [1]. However, many OT systems were not designed with cybersecurity in mind and have depended on physical obscurity and network isolation for protection against cyberattacks.

The push for better operational efficiency, especially in the operation and maintenance of OT systems, has created a demand for OT systems to connect to external networks such as an enterprise IT network or the Internet. This allows centralized monitoring of various satellite OT sites from a central site or for supporting vendors to maintain proprietary components remotely, both of which can result in cost savings. Connecting a legacy system to the external network is inherently dangerous, yet many OT systems can only deploy network segregation as protection. This is due to the limited computing resources available to deploy protection mechanisms on legacy OT systems or limited bandwidth available on these legacy networks.

Personal devices are a second area of concern. Almost everyone carries a smart device today and some companies even promote use of personal devices for business purposes, a practice more widely known as bring your own device (BYOD). Use of these devices increase the risk of an insider attack, be it accidental or intentional, as they can bypass network segregation tools and physical protection to penetrate the network.

A. MOTIVATION

The concept of Zero Trust (ZT) is based on the notion that trust is never granted implicitly but must be continually verified [2]. This means that by default devices are not

trusted, even if they were previously verified, and thus, all access requests must be validated before being granted. In January 2022, the U.S. federal government issued a memorandum specifying a Zero Trust architecture (ZTA) strategy for its agencies [3]. ZTA is a cybersecurity approach to design and implement IT systems through strong identity verification, continuous device fingerprinting, and strict enforcement of access controls [3, 4].

Applying the Zero Trust paradigm to critical infrastructure is a topic that has been raised not only by the U.S. federal government but also mentioned in the Singapore cybersecurity strategy of 2021 [3, 5]. However, the feasibility and benefits of applying Zero Trust to OT systems have not been sufficiently addressed and remain largely unknown. Although the National Institute of Standards and Technology (NIST) has issued NIST SP800-82r3 to provide guidance and recommendations for applying Zero Trust to OT systems, that guidance is not detailed [1].

This thesis provides a security analysis of applying Zero Trust to OT systems used in the water sector. In particular, we ask: Can ZT enable secure external remote connection and allow personal devices to be used securely on the OT network? This thesis also asks: Can ZT be used to modernize and secure legacy OT systems without affecting normal operations?

B. RESEARCH APPROACH

This research started with a review of OT cybersecurity issues, Zero Trust and its tenets, a water treatment lab in Singapore University of Technology and Design (SUTD), and a six-part water treatment process. The latter formed the basis of our analysis of a water treatment plant OT system.

We then defined a concept of operations for a typical water treatment plant and developed a threat model to understand the risks associated with remote connectivity and BYOD. Next, we constructed a secure system architecture for a hypothetical water treatment plant, modelled after SUTD's Secure Water Testbed design, using the ZT paradigm.

We analyzed the ZT-OT design using three use cases to determine the effect of ZT on day-to-day water treatment operations. Advantages and disadvantages of ZT enforcement was also studied.

C. THESIS ORGANIZATION

Chapter II provides background information on OT systems, Zero Trust, and the water treatment process. Chapter III describes the process to develop the ZT-OT architecture for a water treatment plant. Chapter IV discusses our analysis of the ZT-OT design using a hypothetical water treatment system. Chapter V concludes the thesis and provides ideas for future work.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

This chapter describes OT systems and the cybersecurity threats that these systems face. The concepts, tenets, and key components of the Zero Trust paradigm [2] are also discussed.

A. OPERATIONAL TECHNOLOGY AND CYBERSECURITY

OT systems include subsystems that interact with physical environments such as industrial control systems [1]. OT systems automate and manage processes within critical infrastructures. Both the hardware and software of OT systems differ from those of IT systems, in that OT systems are built primarily for reliability rather than flexibility or security.

In the past, most OT systems were isolated from the Internet and are situated physically in remote locations. Examples are power plants and water plants. OT systems also often use vendor-specific, proprietary network protocols and components which, in the past, have deterred most attackers from targeting OT systems due to the complexity and time required to breach them. To understand the level of risk that an OT system has, we use the following equation [6]:

$$Risk = likelihood * impact$$

Impact is high as most OT systems are used in critical infrastructures and have direct impact on physical processes. In the past, the likelihood of an attack on an OT system was low, considering the challenges required to breach them. However, to meet increased demand for operational efficiency and various business needs, many OT systems are now connected to their enterprise IT networks and from there to the Internet. The primary driver for this IT-OT integration is to enable remote maintenance and centralized management of satellite sites. This inadvertently increases the likelihood of an OT system being successfully targeted by a malicious actor.

1. Cybersecurity Issues in a Modern OT System

Most OT systems are not designed for modern cyber threats, but are connected to the Internet, nonetheless. A common solution is to create a network perimeter around the critical and vulnerable system to block unwanted traffic. However, perimeter protections can be bypassed by insiders with physical access, as illustrated by the STUXNET worm [7].

The core component of an OT system, the programmable logic controller (PLC) [8], controls the physical process such as activating an actuator or reading a sensor. The supervisory control and data acquisition (SCADA) system is an architecture for centralized data acquisition and control of PLCs. Typical SCADA system hardware and software includes a control server, commonly called a SCADA server; communication equipment, such as cables or wireless equipment; and some PLCs [1]. PLCs and SCADA servers are usually built for reliability and robustness, not performance or flexibility. PLCs are often designed to operate for 10 to 15 years before a hardware change is required, in contrast to the four-to-six-year lifetime of an IT component, such as a Web server [1]. This creates a problem associated with the legacy OT systems that are still prevalent today. Legacy systems have a number of limitations, including limited computing resources and bandwidth, lack of auditing functionality, and lack of cybersecurity awareness.

a. Limited Computing Resources and Bandwidth

While OT systems can continue to function with legacy hardware and software, they lack the computing resources required to run modern security applications such as anti-virus software or software agents for endpoint detection and response. Limited computing resources also disallow active scanning processes such as vulnerability scanners, as these processes risk disabling a critical segment of the system.

Additionally, many OT networks include data links that use dial-up, radio or serial communications. These low-bandwidth data links necessitate careful control to avoid network congestion [9].

b. Lack of Audit Functionality

Asset discovery is the process of identifying and classifying devices that are found on the network, usually via the use of asset discovery tools [9]. These asset discovery tools initiate network requests to detect and verify the presence of devices within the network [9]. However, legacy components are often unable to handle network requests exceeding their originally designed capabilities, leading to potential identification issues.

The lack of security audit is also a concern for OT systems. Most OT systems audit operational activities and keep an operational log in a server (the Historian server in SCADA systems); they do not audit security functions [10]. The absence of security audit logs results in an inability to integrate with cybersecurity monitoring tools, such as Security Incident and Event Management (SIEM) applications [10].

c. Lack of Cybersecurity Awareness

Ani et al. [11]. conducted a survey of cybersecurity awareness among personnel working in an ICS environment. The sample size was 37 people. Of those surveyed, 62.2% were classified as having adequate cybersecurity knowledge while 37.8% were considered as either moderate or high risk in terms of their cybersecurity awareness. Nonetheless, the researchers reiterated the well-known fact that a successful cyber-attack often requires only one compromised person [11].

A compromised insider with administrative privileges can bypass any form of network perimeter or physical security that is put in place to prevent unauthorized access. This issue is further exacerbated in modern systems as many employees can now bring personal devices such as mobile phones and laptops to work. These external devices, which are unmanaged by the enterprise, increase the attack surface, as they can serve as entry points for malware or may accidentally bridge the OT network to the Internet.

2. Cybersecurity Controls for OT Systems

Due to the high risk and impact associated with OT systems, government and private entities have created security frameworks and guidelines with sector-specific recommendations for use by OT operators.

a. Purdue Security Model for ICS Systems

A notable reference model for designing ICS systems is the Purdue Reference Model for cybersecurity [12], shown in Figure 1. The Purdue Security Model consists of six levels, ranging from the physical processes at Level 0 to the enterprise network at Level 4 or 5 [13]. The idea behind the model is to isolate various functions to establish better security and operational controls. The model eliminates circular dependencies. For security controls, the model effectively provides network segregation and for operational controls, it allows upper layers to add features while allowing lower layers to function independently. (For example, Layers 0 and 1 can still operate even if Layer 2 is down because once configured, they do not depend on the capability of Layer 2.)

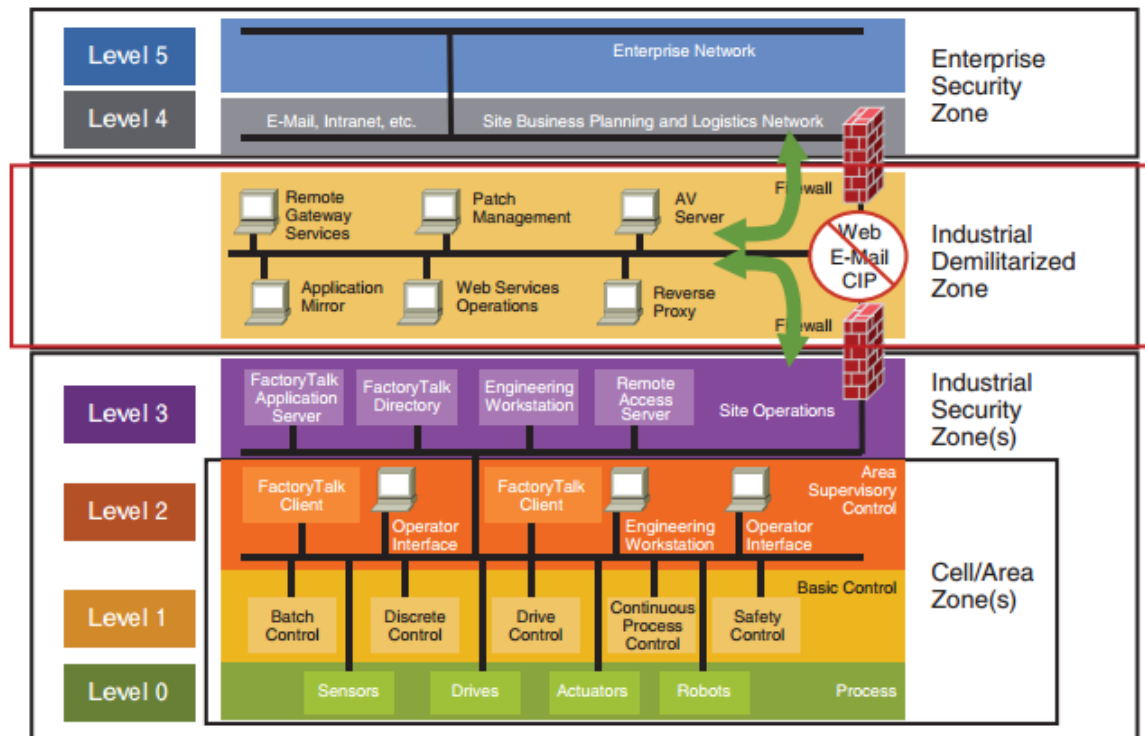


Figure 1. Purdue Model Architecture for ICS. Source: [14]

b. *Security Regulations for OT Systems*

The criticality and increased risk of OT systems have also moved government and cybersecurity entities to create regulations and guidelines for OT cybersecurity. Guidelines such as NIST SP800-82r2 [1] and Singapore’s Cybersecurity Agency (CSA) cybersecurity code of practice (CCOP) [15] are tailored for ICS specifically or have dedicated sections for ICS systems.

Also, sector-specific guidelines from the American Water Works Association (AWWA), the public utilities board of Singapore (PUB), and the Australian energy sector cybersecurity framework [16] have been created to provide more granular policies that addresses the unique nature of each sector.

Private entities have also provided or extended their technical frameworks or guidelines to include ICS-specific materials. Examples include the extension of the MITRE ATT&CK framework to include ICS techniques [17] and the International Electrotechnical Commission (IEC) 62443 standards from the International Society of

Automation (ISA) [18], which provide cybersecurity guidelines for automation and control systems.

3. OT-Related Cyber Incidents

A well-known OT attack is STUXNET. In 2010, STUXNET was found to have infected an Iranian nuclear plant and caused multiple centrifuge failures. The plant was infected via a removable drive used by maintenance personnel. This reinforces the point that a serious attack may be accidentally caused by an insider. The worm itself targeted the Siemens Step 7 (S7) protocol and involved exploits such as modifying system libraries, spoofing S7 variables, and installing signed drivers on Windows OS [7].

The Colonial Pipeline incident in May 2021 was a high-profile attack on an U.S. gas pipeline operated by Colonial Pipeline. Multiple U.S. agencies became involved, including the Federal Bureau of Investigation, the Department of Energy, and the Department of Homeland Security among many others [19]. A compromised virtual private network (VPN) endpoint, for which the methods of compromise are unknown, allowed attackers to infiltrate the network and move onto the OT network where billing systems were targeted and nearly 100 gigabytes of data was exfiltrated [20]. Although the oil pumping systems were still operational, Colonial Pipeline temporarily shut down on May 8, 2021, as a precaution to prevent the hackers from causing further damage. Service resumed after 5 days [20].

On April 2022, reports of a cyber-attack that affected OT systems supporting power grids in Ukraine surfaced during the Russia-Ukraine conflict. This attack used the malware INDUSTROYER.V2 to disrupt power grid operation in Ukraine [21]. INDUSTROYER.V2 was a variant of INDUSTROYER, well-known ICS malware that originally caused power outages in Ukraine in 2016 [21].

In recent years, attacks on U.S. water systems were also detected. In February 2021, a water treatment facility in Oldsmar, Florida was compromised. The facility was using legacy software and shared login credentials on top of enabling Remote Desktop Protocol [22]. In these attacks, hackers tried to increase dosage levels of sodium hydroxide, which is poisonous to humans [23].

4. OT Systems Used in Water Treatment Process

OT systems span many sectors and have different architectures and variants. Here we will focus on water treatment systems. A water treatment system is part of a larger water system, which includes water reclamation, water desalination and water distribution. Water treatment systems share similarities, especially in the logical layer, with water reclamation and water desalination systems.

Before becoming potable water for household or industrial use, water must first be collected either from rain or rivers, desalinated from sea water or reclaimed from used water. The collected water is then treated before being distributed. In most modern water treatment systems, a six-step process is adopted [24]:

- Process 1: Raw Water Processing
- Process 2: Chemical Dosing and Pre-treatment
- Process 3: Ultrafiltration
- Process 4: De-chlorination
- Process 5: Reverse Osmosis
- Process 6: Backwash

Figure 2 shows the Singapore University of Technology and Design (SUTD) Secure Water Testbed (SWAT), a scaled-down, six-step process water treatment facility built for research. Figure 3 shows the system architecture of the SWAT which simulates the IT and OT systems of a modern water treatment plant for research and experimental purposes.

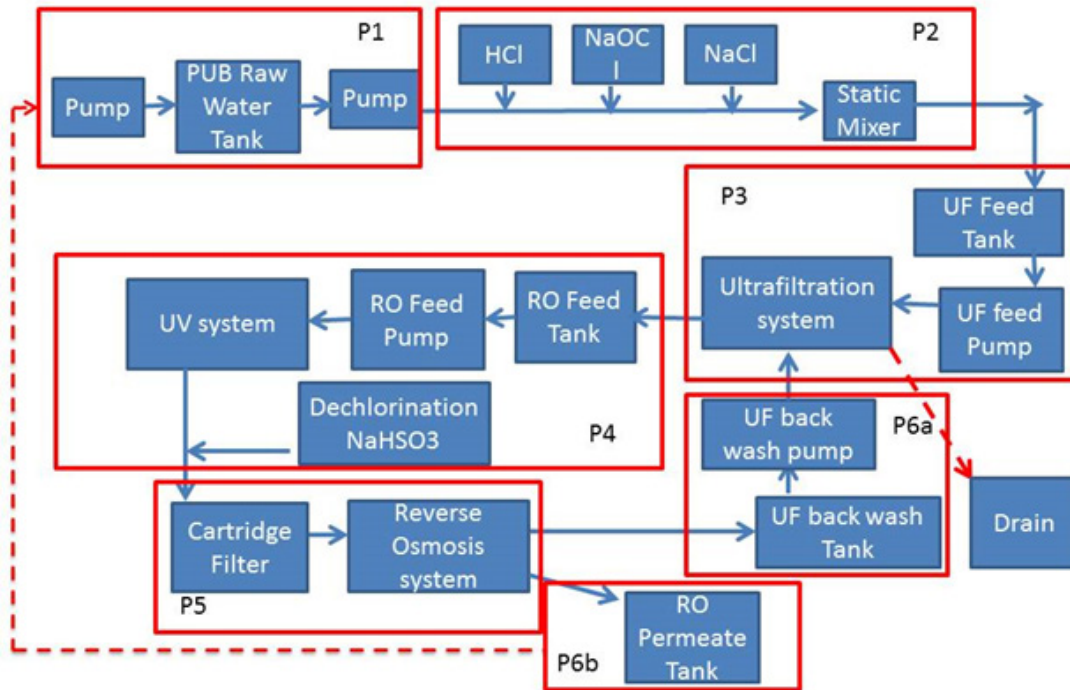


Figure 2. SUTD secure water testbed processes. Source: [24]

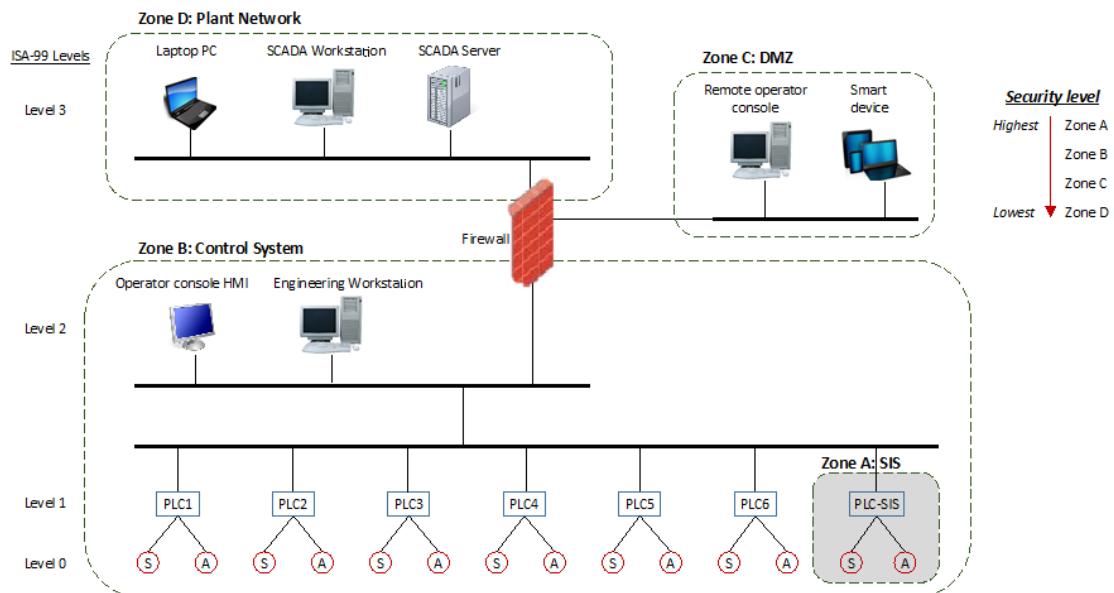


Figure 3. SUTD secure water testbed system architecture. Source: [24]

B. ZERO TRUST PARADIGM

The Zero Trust paradigm, also called Zero Trust Architecture (ZTA), differs from traditional access control approaches in that in this architecture, authentication is always active, even for previously verified devices and users. In ZTA, it is assumed that anything can be compromised at any time, and every action taken requires re-authentication. As with any paradigm, ZTA has many interpretations. In this work, we adopt the tenets and architecture of ZT described by NIST in NIST SP800-207 [2].

NIST SP800-207 defines the terms *subject* and *resource* as follows:

- Subject: a combination of user, application, services, and devices
- Resource: a combination of data, computing resources and applications, services [2]

1. Tenets of Zero Trust

The following seven tenets are formalized by NIST to define the core concepts of the ZTA approach. These tenets represent ideal goals. They may not all be fully realized for any given architecture.

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy; including the observable state of client identity, application and service, and the requesting asset, and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. [2]

The seven tenets defined by NIST are technology agnostic; various methods are available to implement them. This is particularly important when trying to apply an IT-based paradigm to an OT system or any non-enterprise systems, as there will be

differences. Nevertheless, these seven tenets require constant monitoring and logging of the entire network and constant knowledge of the risk posture of all subjects to correctly implement Zero Trust in a network.

2. Logical Components of Zero Trust

NIST has proposed the ZTA reference architecture (Figure 4) as a guideline for implementing ZTA. This model has three major components, namely the policy enforcement points(s) (PEP) [2], the policy decision point (PDP) [2], and the policy information points (PIP), which were recently added [25].

- **Policy Enforcement Point(s):** The PEP is implemented in-line between all resources and subjects. The PEP ensures that all access is authenticated and authorized based on the trust algorithm provided in the PDP [2]. NIST defines the trust algorithm as “the process used by the policy engine to ultimately grant or deny access to a resource” [2]. Examples of a PEP are a next-generation firewall or a proxy server [25].
- **Policy Decision Point(s):** As the name implies, the PDP provides a central point where all access decisions are made with reference to information provided by supporting components and data sources. The PDP can be a physically connected or a hosted engine but should be protected and out-of-band of the operational system.
- **Policy Information Point:** The PIP was recently added by NIST in the latest version of SP1800-35B. It provides the supporting components required by the PDP to evaluate its data and access decisions against [25].

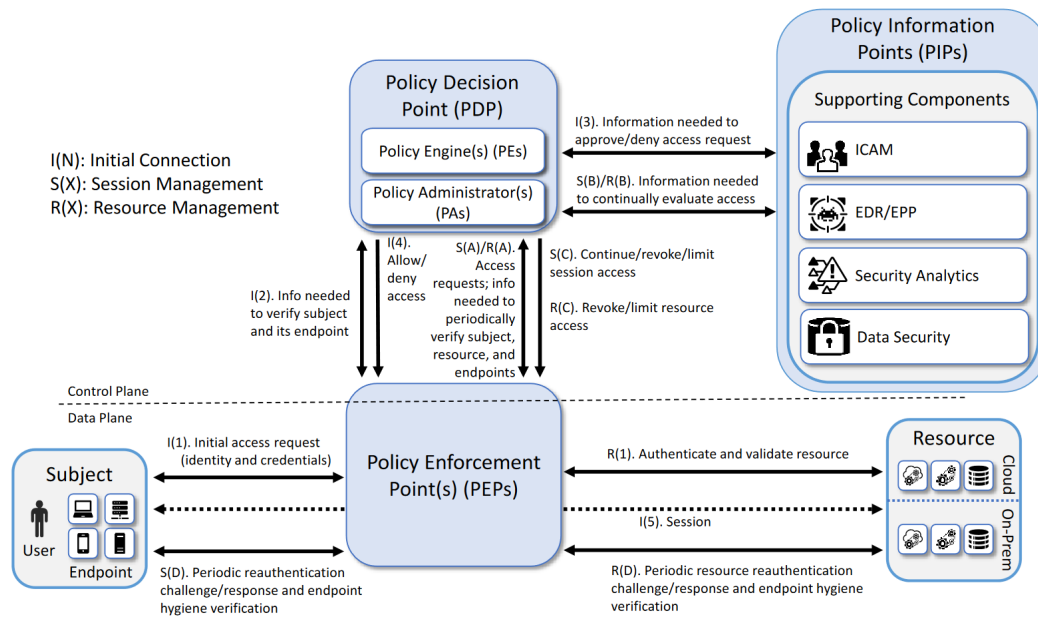


Figure 4. NIST ZTA reference architecture. Source [25]

3. Supporting Components of Zero Trust

The supporting components provide various types of telemetry and other information needed for the PDP to provide informed access decisions [25]. In Figure 4, four supporting components are identified by NIST for policy decisions to be made within the ZTA. They are:

a. Identity, Credential and Access Management (ICAM)

ICAM represents the realization of a collection of governance framework, policies, and mechanisms employed by an enterprise to govern account management and access control. These include identity and access management (IAM), use of multi-factor authentication, use of single sign-on, and identity governance to ensure compliance to regulations [25].

b. Endpoint Detection and Response (EDR)

EDR includes the governance framework, policies, and technology used by an enterprise to protect endpoints. These can include mechanisms for continuous diagnostics and mitigation, application protection, host-based protection (host-based firewall, host-

based intrusion prevention, etc.), malware protection, and mobile device management [25]. The list is not comprehensive, but all enterprise policies and technologies concerning endpoint protection fall under this category.

c. Security Analytics

The security analytics component combines all aspects of threat intelligence, network traffic monitoring, and enterprise monitoring to detect potential indicators of compromise [25]. This can include technologies such as Security Incident and Event Management (SIEM), Security Orchestration and Response (SOAR), network monitoring systems, traffic inspection, threat intelligence, user behavioral analysis, and analytics [25].

d. Data Security

The data security component includes enterprise policies, technologies, and governance frameworks that an enterprise uses to protect data at rest, at use, and in transit [25]. This includes protecting the confidentiality, integrity, and availability of data as well as all policies concerning data [25].

C. PRIOR WORK

The application of ZTA to OT network has been explored by several researchers. Boumhaout et al. [26]. analyzed the potential of using ZTA in critical infrastructure to secure every individual connection instead of just securing networks. The analysis considered a legacy system, third party vendors and industrial Internet of Things components within the network [26]. The paper also noted that the perimeter defense approach based on the Purdue model can be breached repeatedly. We agree that legacy systems are a major issue and that Zero Trust can be applied to provide a more proactive approach to cybersecurity. Nevertheless, our work explores using Zero Trust to enable additional functionality such as remote connection and BYOD, in addition to securing OT systems.

A method of using ZTA to secure remote access for maintenance within an industrial Internet of Things infrastructure was explored by Federici et al. [27]. That work

analyzed the implementation of ZTA within a software defined network consisting of both legacy and modern edge devices [27]. The paper suggested distributed PDPs for edge and network resources due to the difference in their criticality. The future work section of this paper indicates possible development of two-layered models to have multiple authorizations layers to address different levels of granularity [27]. This approach aligns with the work presented here as we are attempting to secure a system with varying levels of criticality. However, their work also did not address BYOD-related threats.

Teerakanok et al. [28]. analyzed challenges such as interoperability, proprietary data formats, user disruption and unmanaged devices when migrating legacy architectures to ZTA. Challenges in the implementation of ZTA such as the lack of standardization and vendor lock-in are discussed in their paper. The paper also mentioned challenges of handling unmanaged devices which is a considerable problem when considering implementing BYOD. Nevertheless, their work did not address the challenges of enabling remote access in legacy OT networks. Finally, the paper also explored generic steps and details that are useful in migrating to a Zero Trust architecture.

THIS PAGE INTENTIONALLY LEFT BLANK

III. ZERO TRUST FOR A WATER PLANT

This chapter describes the design of an OT system that enforces organizational security of a water treatment plant (WTP). The design steps include, in order, a concept of operations, threat model, assumptions regarding the system, description of the security policy to be enforced, and a high-level security architecture. We created a set of BYOD and remote access policies and assumptions for our water plant and used them to develop security requirements needed to design our secure OT architecture.

A. CONCEPT OF OPERATIONS

The objective of the WTP is to ensure a supply of clean water to its service area. A typical WTP has an IT-OT integrated network to allow for centralized monitoring. The system architecture of the WTP is based on the SWAT architecture in SUTD (Figure 3), which is based on the Purdue model. Our WTP contains both legacy OT and modern IT systems. Neither BYOD nor teleworking are allowed, and all operations are conducted on premises. The high-level objective of our design is to support both BYOD and telework.

1. User Roles

Both OT and IT systems have users. Only OT users are discussed in the work presented here. OT users include:

a. WTP IT Manager

- The WTP IT Manager manages the IT infrastructure and processes in the water plant. The role is responsible for all company-furnished equipment (CFE) issued to company personnel, including OT personnel.

b. OT Manager

- The OT Manager is responsible for ensuring water quality and flow of the WTP. The role is also responsible for all OT assets including sensors, actuators, PLCs, SCADA server, SCADA workstations, etc.

c. *OT Operator*

- The OT Operator ensures daily operation of the OT system and reports to the OT Manager. The role has access to the OT systems but requires explicit approval from the OT Manager to perform privileged operations.

d. *Plant Technician*

- The Plant Technician performs maintenance on hardware, such as sensors and actuators, in the WTP. The role has no network access to OT or IT systems.

e. *External Vendor*

- The external vendor works for the company that sells the OT system used in the WTP. The external vendor is contracted by the plant operator to build the OT system and provide maintenance services.

2. *Operational Requirements*

There are two operational requirements.

a. *Remote Connectivity*

The OT system must allow secure remote connections, which can enable teleworking, remote maintenance, and secure centralized monitoring of various satellite OT sites. Here, a remote connection is defined as a connection that traverses external networks such as a leased line or the Internet.

b. *Use of Personal Devices*

The OT system must allow personal devices in the plant premises. In addition to personal use, these devices can be used for WTP business and operations. Personal devices must be authorized prior to business use. These devices include handphones, tablets and laptops of employees and external contractors. Wearable devices are outside the scope of the water treatment plant scenario.

B. THREAT MODEL

Threat modelling is used to understand the security requirements that must be satisfied to enable remote connection and BYOD. It involves two steps: identification of functional requirements and identification of potential threats and the potential impact of those threats to the WTP.

1. Identify Requirements

In this section, we identify the functional requirements needed for our water treatment plant.

a. Remote Access Requirements

Functional requirements for remote access are taken from a document by the U.S. Department of Homeland Security and the UK Centre for the Protection of National Infrastructure (CPNI) entitled “Configuring and Managing Remote Access for Industrial Control System” [29]:

- The solution must ensure that resources can access their information and essential services from any location if required and allowed by policy.
- The solution must ensure that resources can access their information and essential services from multiple device categories.
- The solution must ensure that critical information is available for use at a moment’s notice, that the critical information is always accurate and complete, and that confidential information is provided only to those who require it. [29]

b. BYOD Requirements

We crafted our requirements based on the BYOD guidance by the National Cyber Security Centre of the United Kingdom [30]:

- Employees shall be permitted to perform business operations from their personal device with explicit approval.
- Personal devices shall be allowed for read operation on the OT network. Write operation shall not be allowed.
- Personal devices shall be enrolled prior to accessing company network.

- Attributes of personal devices and activity shall be monitored when accessing the company network.

2. Identify and Assess Threats.

The primary focus when addressing remote access centers on the initial access category of the MITRE ATT&CK framework for ICS systems [17]. Sub-categories within this category that are relevant to remote access are exploitation of public-facing applications, exploitation of remote services, external remote services, and remote services [17]. Enabling remote services in OT networks requires additional systems, such as a VPN server, that could potentially be exploited by adversaries. Moreover, enabling remote services also exposes the OT network itself to external threats.

Using the MITRE ATT&CK framework for ICS systems, the main focus for addressing BYOD is also in the initial access category [17]. Sub-categories within this category that are relevant to BYOD are replication through removable media, wireless compromise, and Internet accessibility of the device [17]. The overarching threat is that personal devices may potentially be used to transfer malware into the OT network (intentionally or accidentally) or may act as a bridge that links the OT network to an external network.

In both cases, the OT network is exposed to either external networks or external devices both of which can function as an entry vehicle into the OT network. While other categories such as evasion techniques and lateral movement are also of concern, they are downstream effects after the malicious actor has gained access to the OT network [17]. Compromised access to the OT network could result in disruption to water treatment operations or, worse still, lead to improper dosing of chemicals in the water.

C. ASSUMPTIONS

Our design was made with the following assumptions:

- All physical security policies will be enforced.
- The OT system includes legacy components that cannot be updated, patched, replaced, or removed.

- No cloud service is connected to the OT network.
- The WTP will be based in Singapore and regulated by the CCOP.

D. CYBERSECURITY POLICY

The defined concept of operations and threat model result in a cybersecurity policy for the WTP that has three elements.

- IT Manager, OT Manager, and OT Operator shall only have access to components in the network needed to complete their tasks and, for certain actions that affect the water treatment process, a series of authorizations shall be required,
- The system shall support both local and remote personnel, and
- Access to the OT system shall only be permitted to personnel with enterprise-issued devices or enterprise-installed agents.

These policies reflect the principle of least privileges and the principle of separation of duty. The policies also ensure that only authorized devices and personnel are allowed to access the enterprise network, either locally or remotely.

E. CYBERSECURITY REQUIREMENTS

The WTP must meet the security requirements of the CCOP [15].

Section 5.7 of the CCOP provides requirements for remote connection.

Section 5.11 of the CCOP provides requirements for portable computing devices [15]. Requirements in that section apply to all personal and company-furnished devices connected to the network.

F. SECURE WATER TREATMENT PLANT ARCHITECTURE

The WTP architecture is based on the SWAT architecture. Three separate architectures were created to address the following three scenarios:

1. Design 1: Securing remote connection without BYOD.
2. Design 2: Securing BYOD without remote connection.

3. Design 3: Securing BYOD and remote connection.

Security controls common to each design were identified.

For all three scenarios, the OT network is connected to the enterprise IT network via a secure leased line.

1. Securing Remote Connection

The security requirements for remote connection can be met by implementing a VPN server in Zone D (shown in Figure 5) to ensure that the connection is encrypted. The VPN server uses the existing IAM and domain controllers to manage its user accounts.

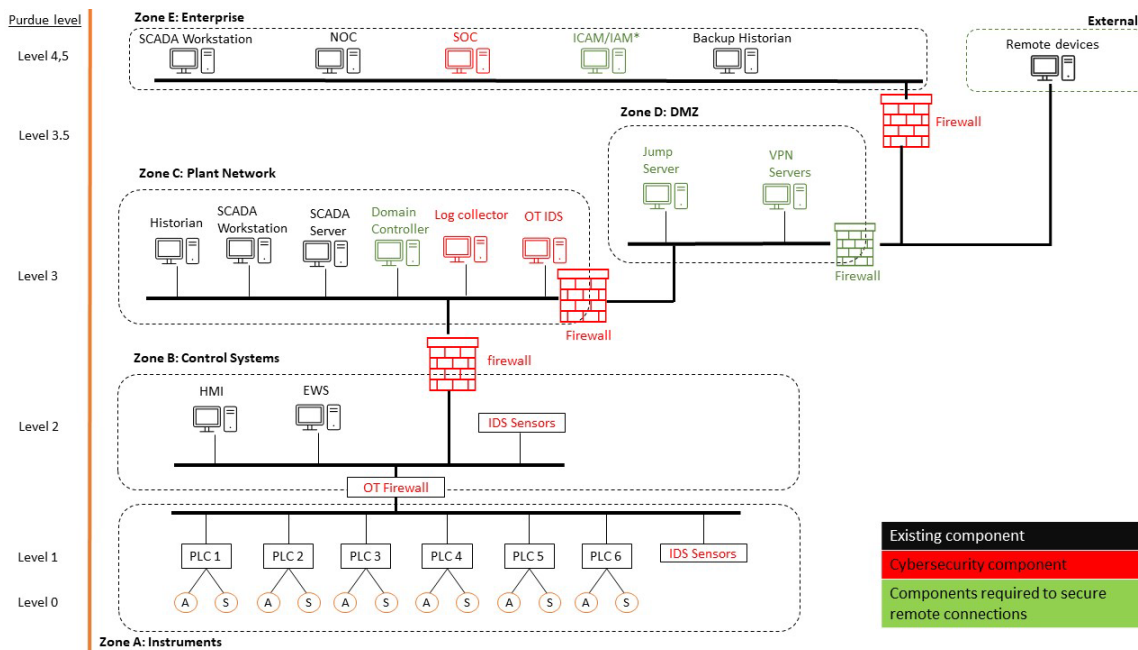


Figure 5. SWAT architecture with secure remote connection without BYOD

In Figure 5, existing OT and IT components are outlined in black. Components outlined in red are added to fulfill the security requirements of the CCOP. The firewalls are required to comply with Section 5.5 (Network Segmentation) and Section 5.6 (Network Security) of the CCOP [15]. The SOC, log collector and OT IDS are deployed

to comply with Section 6.1 (Logging) and Section 6.2 (Monitoring and Detection) of the CCOP [15].

Components outlined in green are required to secure remote connections; these may be new or existing components. The DMZ is replaced with a jump server and a VPN server to segregate the OT network from the Internet and to provide a single point of entry. These components are required to comply with Section 5.7 (Remote Connection) of the CCOP.

2. Securing BYOD

The security controls required to enforce security requirements for BYOD are:

- Device management solutions such as unified endpoint management (UEM) must be used to enroll and track all devices, including personal laptops and mobile devices. UEM supports both agent and agentless management of devices. UEM also facilitates the collection and aggregation of telemetry from managed devices in support of other tools, such as IDS and UEBA, that require device-specific data [31].
- Network filtering controls must be used to restrict network access to only authorized devices. Specifically, all network traffic within the company must be routed through a firewall.

Figure 6 shows the SWAT architecture updated with security controls to meet CCOP requirements and securing BYOD usage. Components outlined in black are existing components. Components outlined in red are added to fulfill security requirements of the CCOP [15]. Components outlined in blue are new or existing components required to enforce BYOD policies. Firewalls outlined in blue are intended to filter BYOD traffic on OT systems. In combination, the domain controller and ICAM act as the device management system. The UEM is part of the ICAM in the IT network.

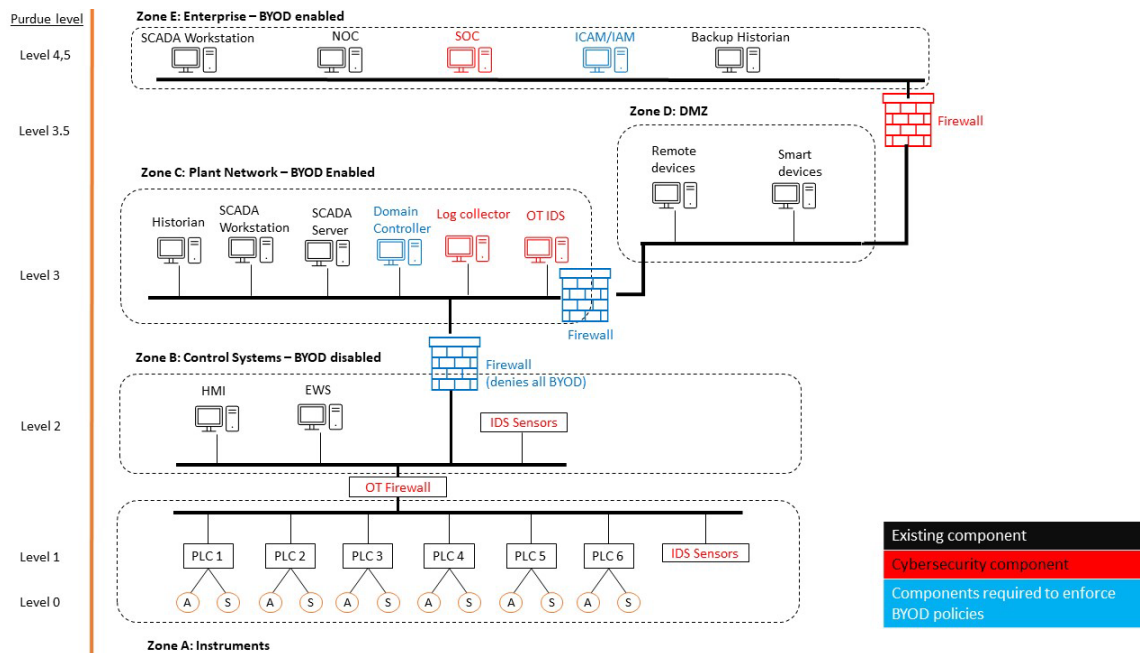


Figure 6. SWAT architecture with secure BYOD without remote connection

3. Securing Remote Connection and BYOD

Both remote connection and BYOD share security requirements in two areas:

1. User account and device management.
2. Network filtering controls.

Figure 7 shows a SWAT architecture conforming to the requirements set out in the CCOP that supports secured remote connection and BYOD usage. Components outlined in black are existing components and those outlined in red are components required to conform to the CCOP [15]. Components outlined in green are required for secure remote connections such as VPN and jump servers. Lastly, components outlined in purple are used to secure both BYOD usage and remote connections. In this design, there are no security controls dedicated solely for BYOD enforcement.

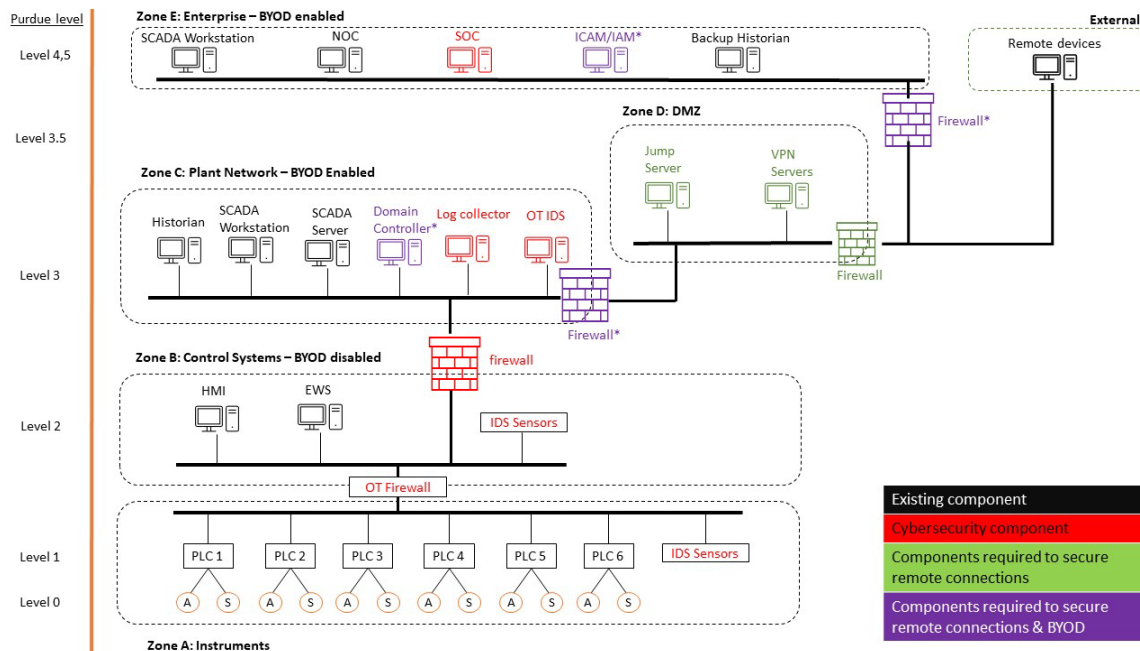


Figure 7. SWAT architecture with secure remote connection and BYOD

4. Zero Trust Design (ZT-OT)

Our analysis of the Zero Trust paradigm indicated that it is applicable to the remote access and BYOD requirements of the WTP. As mentioned in Section III.B, the main threat is in the initial access category which grants attackers their first entry point to the OT network. Zero Trust provides both strict access control and device control that can be used to mitigate this threat.

a. Understanding Zero Trust

Zero Trust as defined by NIST SP 800-207 [2] can have a direct impact on how the policy is shaped and can impact the final system architecture.

In this thesis, we refer to the process of evaluating security risk associated with a subject as *subject assessment*, and the outcome of this evaluation as the *risk profile* of the subject. The risk profile is computed using attributes such as: credentials used by the subject, data and time of access, geo-location of the device on which the subject run, firmware version of the device used by the subject, software installed on the device used

by the subject, type of data requested, connection type, authentication methods such as biometric or password, and so on [2].

Requesting access is defined as a subject, operated by someone or on behalf of someone, requesting a resource. Access is granted based on the risk profile of the subject and security attributes of the resource.

Figure 8 shows an enclave gateway deployment model from Section 3.2.2 of NIST SP800-207 [2]. A software agent installed on each device communicates with the PEP and provides information about the device such as IP address, port information, session key or other security artifacts for verification [2]. We separated our network into three enclaves based on the network criticality as follows:

- IT network zone,
- OT network zone, and
- Trusted zone, which contains legacy devices.

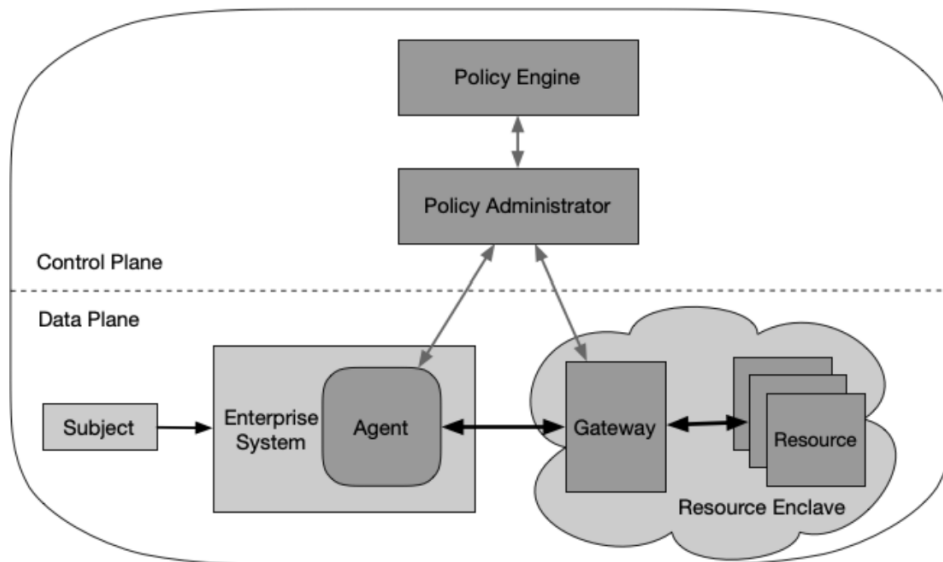


Figure 8. NIST SP800-207 Enclave Gateway Model. Source: [2]

Although NIST states that software agents are compulsory, their use is optional in our design. This provides the user flexibility when registering personal devices for business use.

For our design, we made three changes to the NIST recommendations with regard to software agents and network zones:

1. A company-controlled software agents will be installed on personal devices only if the owner agrees. This BYOD option requires that the device meets the operating requirements of the agent.
2. Use of a personal device without the software agent or its equivalent will only be allowed for read operations on non-critical systems.
3. We introduce the concept of *policy enforcement (PE) levels* to distinguish varying security requirements across different networks. This is required due to differences in criticality between IT and OT networks. Within IT and OT networks, different network segments may have different PE levels.

In addition, risk profiles are also given to subjects computed based on their attributes. Risk profiles are dynamic and continually assessed to determine whether a subject can continue to access a certain PE level.

b. Components Required for Zero Trust

To enable Zero Trust, the following components are required [2, 25]:

- Policy Enforcement Point
- Policy Decision Point
- Policy Information Point

The PEP restricts access to network zones and can be implemented by a firewall or as a separate component. Within a network zone, routing rules must also be implemented so that all requests for resources are routed to the PEP for verification.

The PEP then routes the request to the PDP, which uses information from the PIP and a trust algorithm to make access decisions. The PIP provides the information it collects from the following systems to the PDP:

- Identity, Credentials and Account Management (ICAM)
- Intrusion Detection System (IDS)
- User and Endpoint Behavior Analytics (UEBA)
- Multifactor Authentication
- Unified Endpoint Management (UEM)

This information parameterizes the trust algorithm used by the PDP to determine subject risk profile.

c. Access Policy for Zero Trust

- Three PE levels shall be assigned according to the criticality of each network zone:
 - PE Level 1
PE Level 1 is assigned to network zones with no OT functions.
 - PE Level 2
PE Level 2 is assigned to network zones with OT functions.
 - PE Level 3
PE Level 3 is assigned to network zones that cannot be secured by Zero Trust mechanisms. This includes legacy components, latency sensitive components, and components lacking the computational capacity to support Zero Trust.
- All subjects shall be assessed and given a risk profile before being granted access to any resource. A subject shall be assigned to one of the following

risk profiles after assessment: low risk, medium risk, high risk, or very high risk.

- Access to a PE level shall be based on the following policy:
 - For all PE levels, a risk profile for each subject shall be in effect for a period defined by the PE level or until a change in a subject attribute is detected, in which case, the subject shall be reassessed.
 - PE Level 1
 - Whitelisted subjects of low, medium, or high risk shall be allowed to access PE Level 1 network zones.
 - The PEP shall reassess the validity of access for all subjects after a configurable time frame. This time frame shall be defined by the enterprise access control policy.
 - All read and write requests shall undergo verification by the PEP, and only authorized requests shall be allowed access.
 - PE Level 2
 - Whitelisted subjects of low and medium risk shall be allowed to access network zones of PE Level 2.
 - Only approved devices with software agents shall be allowed to remotely connect to network zones of PE Level 2.
 - The PEP shall reassess the validity of access for all subjects after a configurable time frame. This time frame shall be defined by the enterprise access control policy.

- All read and write requests shall undergo verification by the PEP, and only authorized requests shall be allowed access.
- PE Level 3
 - Only whitelisted company-furnished equipment of low risk shall be allowed to access network zones of PE Level 3.
 - No remote connection shall be permitted.
 - No external devices shall be permitted.
 - The PEP shall reassess the validity of access for all subjects after a configurable time frame. This time frame shall be defined by the enterprise access control policy.
 - All read and write requests shall undergo verification by the PEP, and only authorized requests shall be allowed access.

d. ZT-OT Architecture

To implement the ZT-OT architecture, the enhanced SWAT design shown in Figure 3 is extended with the addition of PEP, PDP, and PIP components. A PEP is added at the boundary of all network zones. We termed the PEP in the IT network zone as Zone E PEP; the PEP in the OT network zone as Zone C PEP; and the PEP in the trusted zone as Zone B PEP.

There are two PDPs: an enterprise PDP and a plant PDP. The rationale for a local PDP is to ensure that each plant is operational even if the link between a water plant and the enterprise network is broken.

The PIP is a logical collection of components situated in the enterprise network and provides contextual information for use by the PDPs pertaining to each subject. We assumed that the PDP would cache the retrieved attributes for each subject it has

encountered for 24 hours, thus making verification involving the subject faster during the 24-hour interval.

Figure 9 shows the ZT-OT architecture with the PEP, PDP and PIP added in.

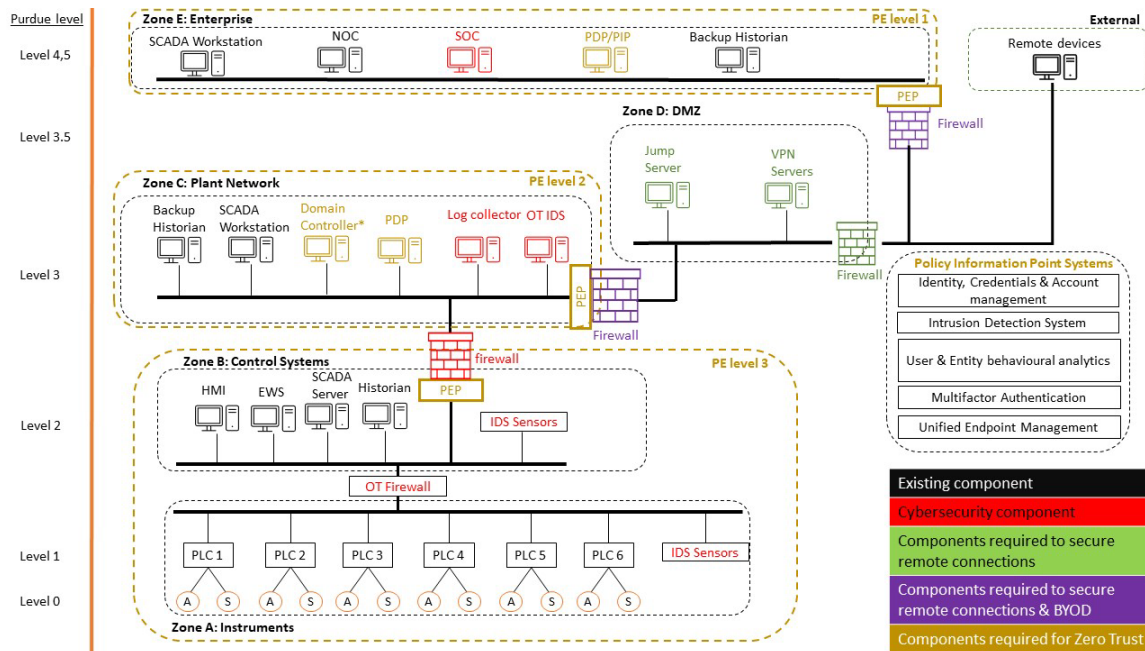


Figure 9. SWAT architecture with Zero Trust (ZT-OT)

In Figure 9, components shown in black are existing components, components in red are security controls required for CCOP, components in green are security controls required to secure remote connections, and components in purple are security controls required to secure both remote connections and BYOD user activity. Devices outlined in gold are either newly added security controls for implementing Zero Trust or existing security controls required for implementing Zero Trust.

In ZT-OT, the SCADA server and Historian server were moved from the plant network into the control network due to the addition of the PEP in the control system zone. This change in location is necessary to preserve the ability of the control network to function on its own even in the event of an outage of the plant network. By moving the

SCADA server and Historian server into the control network, the entire control systems network zone becomes self-reliant in the performance of water treatment operations.

e. Logging in ZT-OT

There are two kinds of logs in ZT-OT: process-related logs and cybersecurity logs. Process-related logs contain log entries associated with events generated by the SCADA systems. They provide historical information on SCADA operation and water parameters. Cybersecurity logs contain log entries for security-relevant events generated by operating systems and application software. These logs contain recorded information about various activities and events that are crucial for detecting and investigating security incidents.

In each water plant, process-related logs reside in the Historian in Zone B while cybersecurity logs are kept in the log collector in Zone C. For the DMZ and enterprise network, there is no process-related log and cybersecurity logs are kept in a log collector in the enterprise network. This enterprise log collector is part of the PIP.

Logs maintained by the Historian are also backed up to the Backup Historian in Zone C and Zone E. Incremental back up to the Backup Historian can be set to occur for every change made to the Historian or on a scheduled basis, such as every hour. Additionally, full back up of the Historian is scheduled to occur at less frequent intervals compared to incremental backups, such as every 24 hours. Offsite backups of logs will be carried out and retained in accordance with organizational policies.

In ZT-OT, all logging requests are verified by the respective PEP and PDP within their corresponding zones. Logging request excludes backing up of Historian logs to Backup Historians. Table 1 shows which PEP and PDP are involved in the verification of logging requests:

Table 1. ZT-OT logging requests classifications

	Process-related events	Cybersecurity events
Zone A devices	Logged in Zone B Historian.	Logged in Zone C log collector.
	No Zero Trust verification*.	Logging device verified by Zone B PEP and plant PDP.
Zone B devices	Logged in Zone B Historian.	Logged into Zone C log collector.
	No Zero Trust verification*.	Logging device verified by Zone B PEP and plant PDP.
Zone C devices	Logged in Zone B Historian.	Logged in Zone C log collector.
	Logging device verified by Zone B PEP and plant PDP.	Logging device verified by Zone C PEP and plant PDP.
Zone D devices	No process-related logs.	Logged in Zone E log collector.
		Logging device verified by Zone E PEP and plant PDP.
Zone E devices	No process-related logs.	Logged in Zone E log collector.
		Logging device verified by Zone E PEP and plant PDP.

*There is no verification as the device and Historian are within the trusted zone.

For Historian backups to the plant Backup Historian in Zone C, the request is verified by the Zone C PEP and plant PDP. Each Historian backup request sent to the enterprise Backup Historian in Zone E is verified by both Zone C and Zone E PEPs and both plant and enterprise PDPs.

The next chapter describes our analysis of common WTP operations and how Zero Trust affects these operations, which can help us determine its suitability, strength and weakness as applied to an OT system.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS OF ZT-OT DESIGN

This chapter discusses our analysis of the ZT-OT design as applied to a hypothetical water treatment system. Three use cases involving routine maintenance; after-hours, unscheduled remote, operations; and software patching were used for the analysis.

A. A HYPOTHETICAL WATER PLANT

Functionally, our hypothetical water plant is an instantiation of the water treatment plant (WTP) described in Chapter III. The OT system used in our water plant is based on the ZT-OT architecture described in Section III.F.4.d.

1. Assumptions

The following assumptions were made for the analysis:

- The scenarios used for the ZT-OT analysis only cover normal operation which includes both scheduled and unscheduled operations. Examples of scheduled maintenance are weekly filter changes. Examples of unscheduled operations are replaceable parts failures; these unscheduled operations are unplanned events but are not detrimental to WTP operation and can be remedied within a few hours.
- The scenarios do not cover emergency cases. Emergency cases are unplanned events which have detrimental effects on WTP operations. Examples are fire, floods, damage to key components such as pumps and turbines, etc.
- All user credentials are assumed to be valid.
- All device configurations are correctly implemented.
- Reactive measures such as incident response or business continuity are out of scope.
- The scenarios assume that all Zero Trust components are working as intended and are not subjected to any cyber-attacks.

- All devices connecting to the company network locally or remotely are either company-furnished equipment (CFE) or have CFE agents installed.
- All operational processes are assumed to succeed. Failure cases pertaining to ZT are included in the design analysis.

a. OT Manager

The OT Manager role oversees daily operations of the OT system to ensure the availability of clean water to the WTP's service area, these operations include software patching, hardware maintenance, and physical security. The role is responsible for controlling access to the OT system. It does not handle management of user accounts and service accounts [32], which is the responsibility of the IT Manager. WTP staff members with this role work at the water plant during office hours and may have access to the OT system remotely. The role is also responsible for requesting access period for external personnels.

In our scenarios, the OT Manager uses a CFE for both on-premises and off-site work. The OT Manager does not have an approved personal device for business use. The CFE used by the OT Manager is approved for remote access to the company network at any time of day.

b. OT Operator

The OT Operator role performs day-to-day operation in the water plant such as recording water and chemical levels and ensuring all systems perform as specified by the plant's operational requirements. During working hours, the OT Operator works at the plant and is usually situated in the control room. The OT Operator may also roam the plant and access the plant's networks via remote access from authorized devices. Remote connections may be established from any network, if they are initiated from an authorized device. The role may use CFE or a personal device for read access but is required to use CFE for write operations. The role requires approval from the OT Manager for all write operations.

In our scenarios, the OT Operator uses CFE while on premises and an authorized personal device at home. The role has approval to remotely access the plant network at any time of day using their CFE and authorized personal device.

c. Plant IT Manager

The Plant IT Manager role oversees the IT infrastructure of the water plant. This includes all network devices, IT servers, and all endpoints used by WTP personnel. The role also manages all personal device enrollment, remote connection authorization and agent installation. The role can grant or deny access to the network for all enrolled devices based on time periods.

In our scenarios, the IT Manager uses a CFE while on premises and an authorized personal device at home. The role has approval to remotely access the plant network using their CFE at any time of day.

d. Plant Technician

The Plant Technician role performs maintenance, servicing, and calibration for hardware components at Level 0 of the Purdue model [12]. The role does not have access to the plant network. WTP staff members in this role work closely with the OT Operator to ensure day-to-day operation of the WTP.

e. External Vendor

In our scenarios, the external vendor's service engineer uses a laptop that is pre-installed with a company-approved software agent to access the plant network locally or remotely. This laptop does not belong to the WTP and is considered an external device. Although this laptop has software agents installed, it is not authorized to connect to the company network, locally and remotely, until an access period has been granted. This access period is requested by the OT Manager and granted by the IT Manager.

While on premises, the vendor's service engineer is always monitored by plant personnel. When connecting to the WTP OT network remotely, the vendor action will be monitored by an OT Operator.

B. ANALYZING ZT-OT DESIGN

A WTP system typically has four modes of operation: maintenance, operational, standby, and manual mode. The three use cases in our analysis only affect the maintenance and operational modes.

- Case 1: Replacement of a reverse osmosis filter during a scheduled maintenance period. This use case simulates routine maintenance.
- Case 2: An OT Manager requests a water parameter check outside of normal operating hours. This use case simulates non-routine operations, remote connection, and usage of a personal device from a plant employee.
- Case 3: Patches to the SCADA system by the external vendor during an extended maintenance period. This use case simulates remote connection and use of a personal device by an external entity.

1. Use Case 1 Analysis: Replacement of Reverse Osmosis Filter

This use case represents a standard operating procedure during a scheduled period and how ZT-OT affects it. The involved actors are the OT Operator and OT Manager. All actions to change the reverse osmosis filter are performed on CFE within company premises.

This use case affects Zone A (Instruments), Zone B (Control Systems), and Zone C (Plant Network) as shown in Figure 9. Purdue Level 0, Level 1, Level 2, and Level 3 are affected. Figure 10 provides a graphical representation of the entire sequence of events. The operations are performed as follows:

1. The OT Operator submits a maintenance plan and task list to the OT Manager.
2. The OT Manager approves the maintenance plan and task list.
3. During the maintenance period, the operator successfully logs in to the SCADA workstation to initiate maintenance mode on the SCADA system.

This login goes through the Zone C PEP and plant PDP for verification and is logged to the Historian.

4. From the SCADA workstation, the OT Operator switches the SCADA system to maintenance mode. This command is routed through the Zone B PEP and plant PDP for verification before reaching the PLCs. The PEP verifies the device sending the command and the SCADA system is switched to maintenance mode. The command to switch mode is also logged by the SCADA system to the Historian.

The SCADA workstation may be deemed insecure by the PEP and be denied access. In this event, the IT Manager may check the logs to find out the reason why the SCADA workstation was deemed insecure by the PEP and perform a manual overwrite if deemed safe and necessary.

5. The filters are physically changed by the Plant Technician while the system is in maintenance mode. The OT Operator is sent an out of band notification by the Plant Technician once the work is completed and the OT Operator performs a system test. The system self-test request is routed through the Zone B PEP and plant PDP for verification before reaching the PLCs. The command to initiate the self-test and its results are logged by the SCADA system to the Historian.
6. After the system self-test succeeds, the OT Operator presents the results to the OT Manager and requests to switch the SCADA system to operational mode.
7. The OT Manager checks the result and approves the request.
8. The OT Operator logs in to the SCADA workstation and sets the SCADA system to operational mode. The login is routed through the Zone C PEP and plant PDP for verification while the command to set to operational mode is routed through the Zone B PEP and plant PDP for verification before reaching the PLCs. Both the login and the command to switch to

operational mode are logged by the SCADA system to the Historian. The SCADA system successfully switches over to operational mode.

9. The OT Operator checks all system parameters to ensure the system is running normally. It is assumed that the OT Operator is still within the allowed access period; hence, no reassessment of the SCADA workstation is required. However, command traffic is still routed to the Zone B PEP and plant PDP for verification. The OT Operator then updates the maintenance plan and presents it to the OT Manager for final sign off.

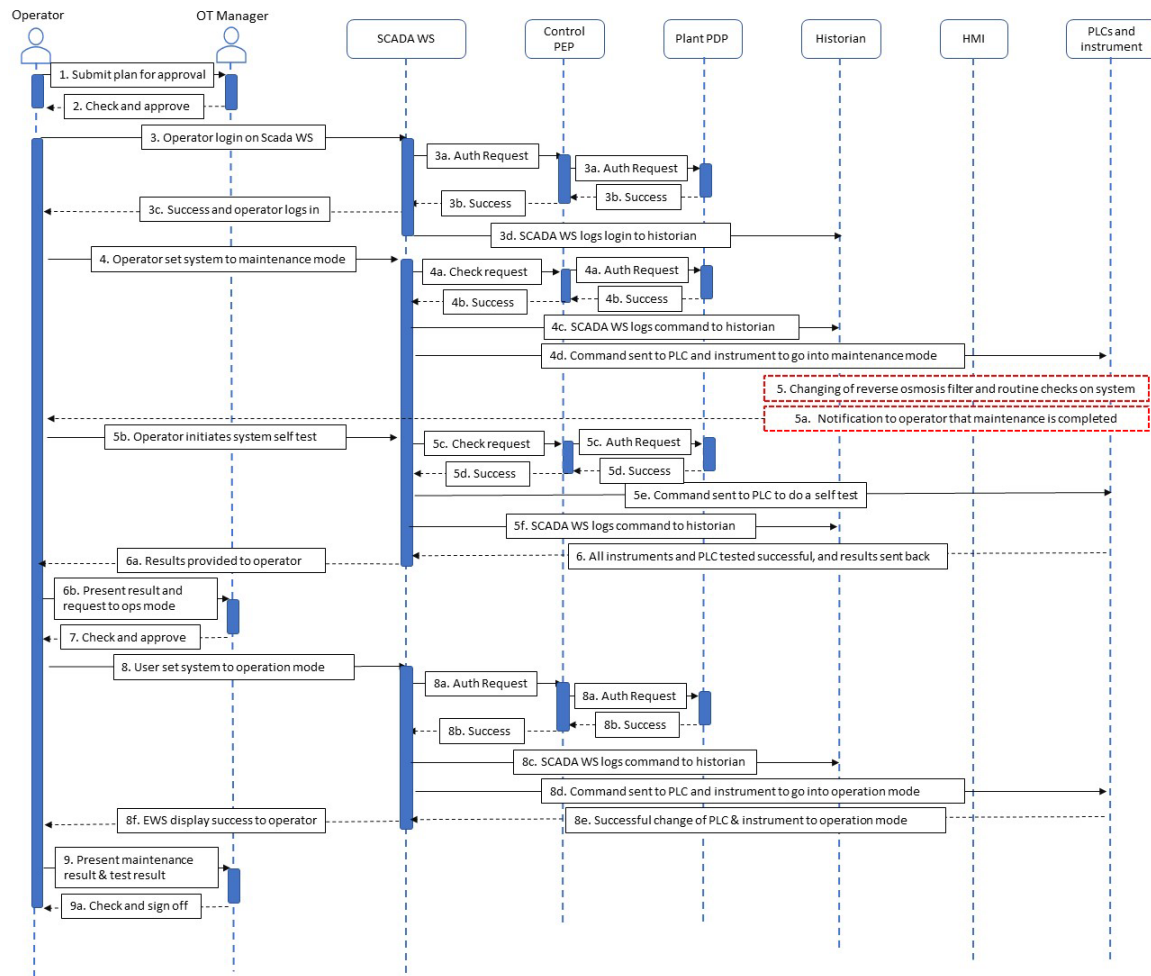


Figure 10. Sequence diagram for Use Case 1: Replacement of reverse osmosis filter

2. Use Case 2 Analysis: Abnormal Water Parameter During Afterhours

This use case presents a situation where abnormal water parameters are discovered after normal working hours. The involved actors are the OT Operator and OT Manager. Both BYOD and remote connection functionality are required as the OT Operator will operate from home using a personal device after hours. Plant Technicians will be stationed at the WTP premises for physical checks.

This use case affects Zone A (Instruments), Zone B (Control Systems), Zone C (Plant Network), Zone D (DMZ), and Zone E (Enterprise). This use case affects all Purdue levels from 0 to 5. Figure 11 provides a graphical representation of the entire sequence of events. The operations are performed as follows:

1. The OT Manager receives a report after office hours from the water regulators stating that a water parameter is abnormal although water is still safe for consumption.
2. The OT Manager requests the OT Operator to perform an ad-hoc check on the anomalous water parameter.
3. The OT Operator connects to the enterprise VPN on their personal laptop from his or her home network. The login to the VPN is routed to the Zone E PEP and enterprise PDP for verification. The PEP also assesses the risk profile of the operator personal laptop.

Upon successful login to the VPN, the OT Operator establishes a connection to the jump server and uses it to jump to the SCADA workstation. The jump request is routed to Zone C PEP and plant PDP for verification and subject assessment of the VPN Server.

Once connected to the SCADA workstation, the OT Operator then logs in to his or her plant account on the SCADA workstation. This login is routed to Zone C PEP and plant PDP for verification and subject assessment of the jump server. The login to the SCADA workstation is logged to the Historian.

At this point, three assessments are continuously performed for this remote connection every time a request is initiated:

- a. Zone E PEP will continuously assess the risk profile of the operator laptop that is connected via the VPN.
- b. Zone C PEP will continuously assess the risk profile of the VPN server used to connect to the jump server.
- c. Zone C PEP will continuously assess the risk profile of the jump server used to connect to the SCADA workstation.

The OT Operator then conducts a water parameter check and submits the findings to the OT Manager.

4. The OT Manager reviews the findings from the OT Operator and confirms there is indeed a problem with the water parameters. The OT Manager requests a SCADA system check to identify the fault.
5. The OT Operator sets the SCADA system to maintenance mode. This command is routed through the Zone B PEP and plant PDP for verification before reaching the PLCs. This command is also logged by the SCADA system to the Historian.

If the PEP verification for any subject in the remote connection chain fails, then a manual override may be initiated as described in Use Case 1.

Once the SCADA system is switched to maintenance mode, the OT Operator sends in a command for the system to perform a self-diagnostic test. This command is routed through the Zone B PEP and plant PDP for verification and logged to the Historian.

6. In this scenario, the test results indicate the issue is a faulty chemical injector. The OT Operator sends an out-of-band notification to the onsite Plant Technician to perform a physical check and repair. The Plant Technician notifies the OT Operator once this is completed.

7. While the remote connection (established in step 3) is still active, the OT Operator initiates another self-diagnostic test. The self-diagnostic test command is routed through the Zone B PEP and plant PDP for verification. The command to initiate the self-test and its results are logged by the SCADA system to the Historian. For this use case, it is assumed that the test will be successful.
8. The OT Operator then reports the test results to the OT Manager and requests to transition the SCADA system to operational mode.
9. The OT Manager approves the request to turn the SCADA system back to operational mode. The OT Manager also directs the OT Operator to retreat the tank of water that was reported as abnormal.
10. The OT Operator sends a command to set the SCADA system to operational mode. After the SCADA system successfully switches to operational mode, the OT Operator sends a command to restart the water treatment process. Both commands are routed through the Zone B PEP and plant PDP for verification before reaching the PLCs. Both commands are logged by the SCADA software to the Historian.

In Use Case 2, all remote access is constantly verified by the Zone C PEP (for access to the jump server and VPN server) and by the Zone E PEP (for the status of the operator laptop). In the Zero Trust paradigm, all components are assumed to be compromised and untrusted, which is why every node used for remote connection is checked, not just the endpoints.

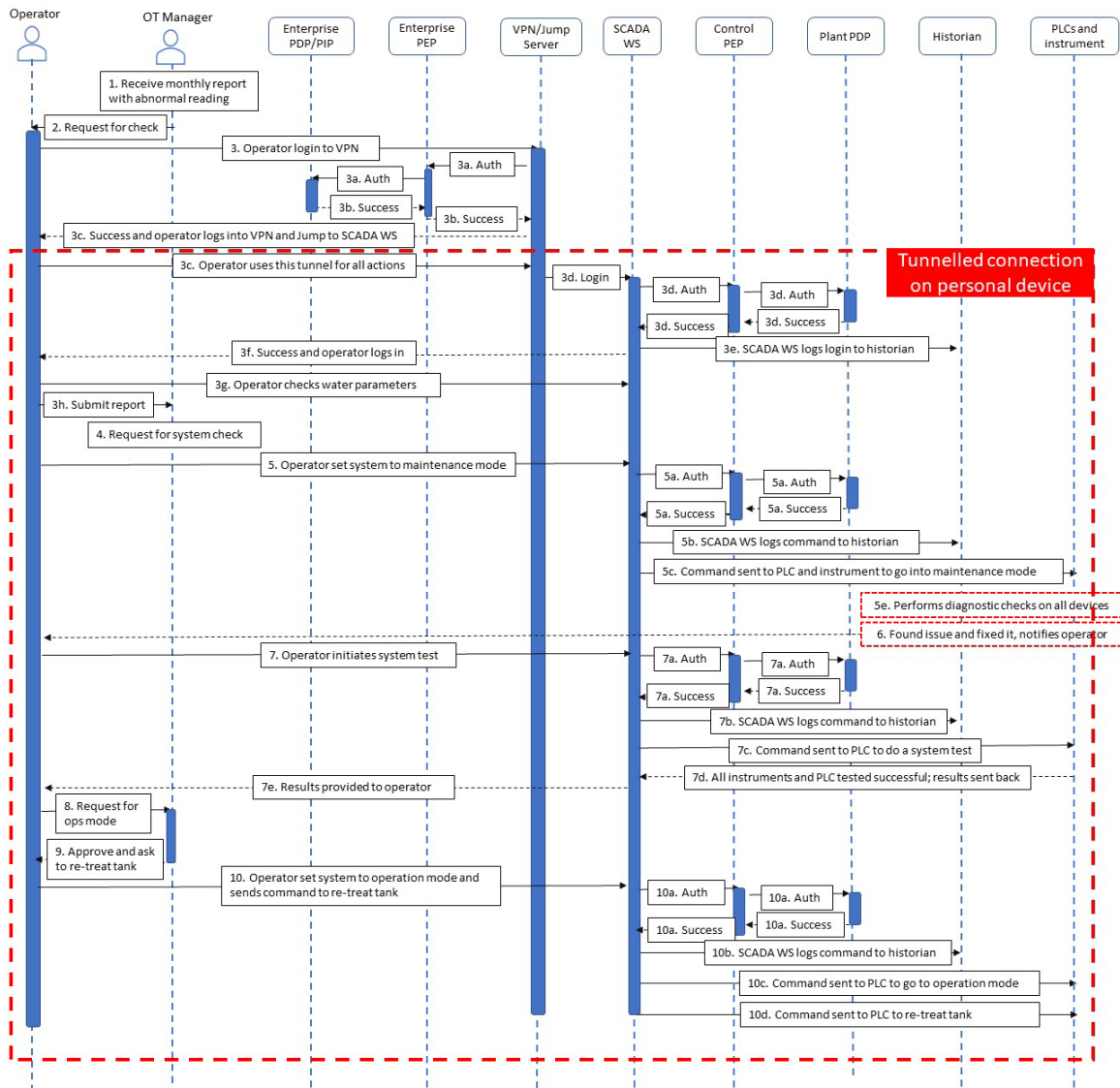


Figure 11. Sequence diagram for Use Case 2: Abnormal water parameter during afterhours

3. Use Case 3 Analysis: Patching of the SCADA System

Use Case 3 represents a case of granting temporary use of non-CFE and remote access.

This use case presents a situation where an external vendor conducts a system patch for the OT system during a predetermined maintenance period. The involved actors are the OT Operator, OT Manager, IT Manager, and external vendor's service engineer.

We also assume that the vendor has a laptop upon which a WTP-approved software agent for maintenance use has been preinstalled.

Remote connection functionality is required, as the vendor will use remote access to assess the system during the pre-patching phase. BYOD procedures are required as the vendor laptop is considered an external non-CFE device.

This use case affects Zone A (Instruments), Zone B (Control Systems), Zone C (Plant Network), Zone D (DMZ), and Zone E (Enterprise). This use case affects all Purdue levels from 0 to 5. Figure 12 provides a graphical representation of the entire sequence of events, and the operations are performed as follows:

This use case spans three separate phases: initial enrollment, information gathering day, and patch day.

a. Initial Enrollment Phase

1. The vendor informs the OT Manager of a system update patch. After analyzing the patch details and concluding that the patch is necessary, the OT Manager creates a work plan and schedules an extended maintenance period for the patch. The work plan consists of an information gathering phase during which the vendor remotely assesses the SCADA system before patching and a patching phase, where the latter must be conducted on site. In our scenario, the devices to be patched are all PLCs and the software to be patched are vendor-provided operating system.
2. The OT Manager informs the OT Operator of the work plan. Concurrently, he also submits a request to the IT Manager to temporarily enroll the vendor device for use during each phase.
3. The IT Manager contacts the vendor to request laptop information such as serial number, user ID, and agent ID. The IT Manager cross-checks this information with the authorized-device database (an example is the UEM) to ensure that the vendor device and user credentials are valid. The IT

Manager then assigns the two time periods when the vendor can access the plant network.

If the provided laptop information is invalid or cannot be found in the device database, the IT Manager will request that another laptop be installed with the agent and re-enrolled physically at the company premises. Alternatively, the external vendor can also conduct the information gathering and patching on a CFE; however, that would require the vendor to be physically present at the plant premises.

b. Information Gathering Phase -- Vendor Is Remote, Operator Is Onsite

4. During the predetermined maintenance period, the vendor connects to the enterprise VPN using their VPN account and pre-enrolled laptop. The login to the VPN is routed to Zone E PEP and enterprise PDP for verification and subject assessment of the vendor laptop.

Upon successful login to the VPN, the vendor establishes a connection to the jump server and uses it to jump to the SCADA workstation. For the vendor, the only jump connection available is the SCADA workstation. The jump request is routed to Zone C PEP and plant PDP for verification and subject assessment of the VPN Server.

Once connected to the SCADA workstation, the vendor then logs in to the SCADA workstation with a separate account for OT network. This login is routed to Zone C PEP and plant PDP for verification and subject assessment of the jump server. The login to the SCADA workstation is logged to the Historian.

5. Once logged in to the SCADA workstation, the vendor performs system checks necessary for the patch.

At this point, three assessments are continuously performed for this remote connection every time a request is initiated:

- a. Zone E PEP continuously assesses the risk profile of the vendor laptop for the VPN connection.
- b. Zone C PEP continuously assesses the risk profile of the VPN server for the connection to the jump server.
- c. Zone C PEP continuously assesses the risk profile of the jump server for the connection to the SCADA workstation.

c. *Patching Phase -- Both Vendor and Operator Are Onsite*

- 6. Prior to the actual patch, the OT Operator logs in to the SCADA workstation and sets the SCADA system to maintenance mode. These requests are routed through the Zone C PEP and plant PDP for verification and logged by the SCADA system to the Historian.

Steps 7 through 9 are performed by the vendor and monitored by the OT Operator.

- 7. The vendor physically connects the pre-enrolled vendor laptop to Zone B network. Upon connection, the software agent will initiate device authentication with Zone B PEP. If the PEP and plant PDP allow this request, the vendor is granted access to all PLCs that are designated to be patched.

If the pre-enrolled vendor laptop is considered insecure by the PEP, then a manual override will be performed as described in Use Case 1. Alternatively, the vendor may choose to use an authorized CFE to conduct the patching. In this case, the patch would have to be transferred via an authorized channel, such as an authorized external hard drive.

Steps 8 and 9 are conducted for every device that needs to be patched.

- 8. Once connected to the Zone B network, the vendor initiates a remote connection from their pre-enrolled laptop to the PLC to be patched. This remote connection may fail if the vendor laptop is deemed insecure by the PEP.

9. For each successful connection, the vendor loads the patch on the PLC and installs the patch. The Zone B PEP verifies the vendor laptop and the request to load the patch; however, the PEP does not have the capability to scan the patch.
10. The vendor informs the OT Operator that patching is complete and requests the OT Operator to run a system test. The OT Operator initiates a self-diagnostic test from the SCADA workstation. This command is routed through the Zone B PEP and plant PDP for verification before reaching the PLCs and logged in to the Historian. For this use case, we assume that the system self-diagnostic test succeeds.

The vendor logs off his account and disconnects the vendor laptop from Zone B network.

11. The OT Operator informs the OT Manager that patching is successful and presents the self-diagnostic test results. After reviewing the test results, the OT Manager directs the OT Operator to switch the SCADA system to operational mode.
12. The OT Operator sets the SCADA system to operational mode. This command is routed through the Zone B PEP and plant PDP for verification and is logged in the Historian.

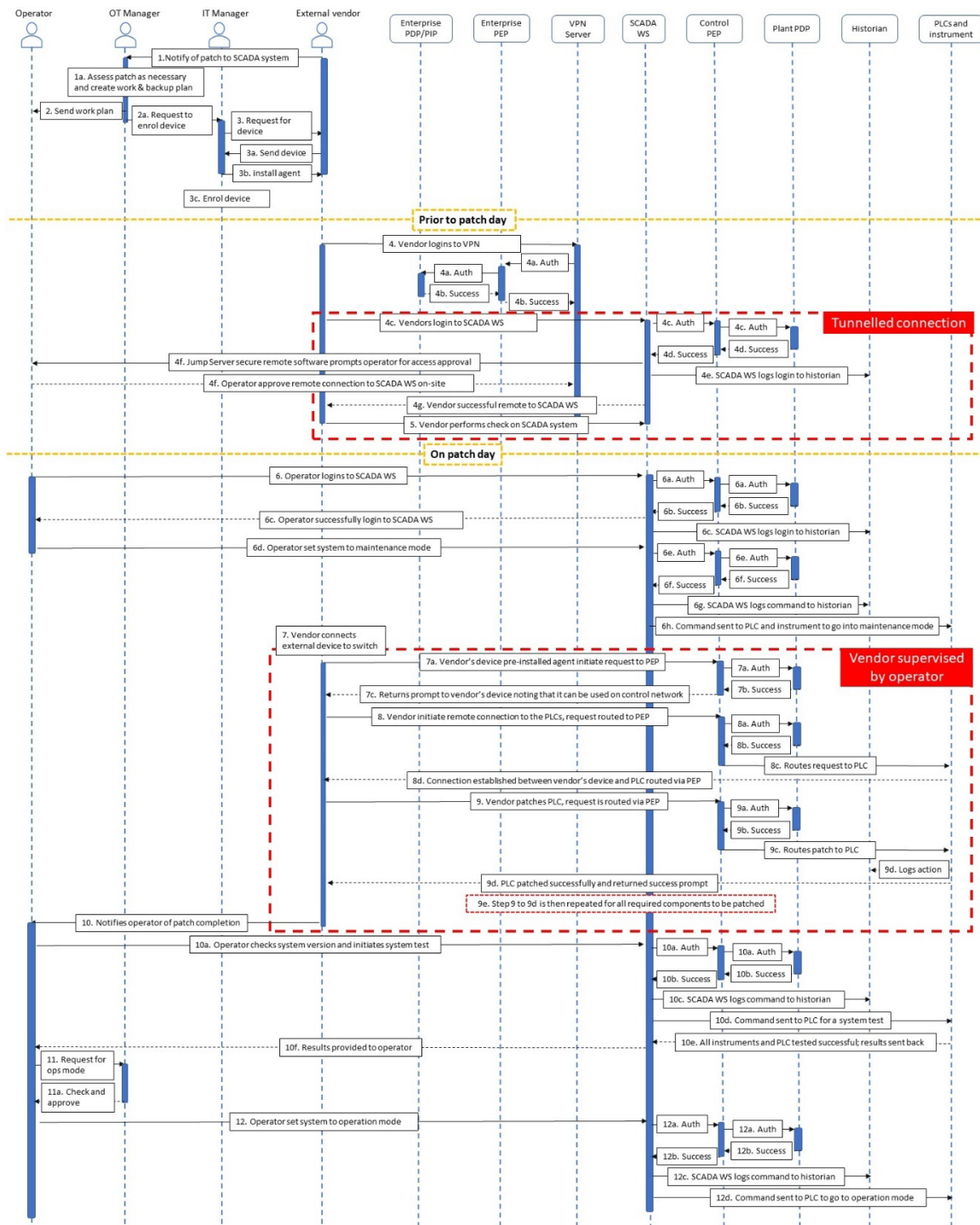


Figure 12. Sequence diagram for Use Case 3: Patching of the SCADA system

C. STRENGTH OF ZT-OT

1. Securing Remote Connection

In Use Case 2 and Use Case 3, Zero Trust provides continual assessment of all systems with remote connections, i.e., the OT Operator, the vendor laptop, the VPN server, and the jump host. Based on the MITRE ATT&CK ICS framework [17], this will help to mitigate the threats from exploitation of remote services and public facing applications.

Zero Trust allows for granular access control policies, such as specifying access periods and accessible devices or network zones. In our design, we created three policy enforcement levels to allow risk tolerance to depend on the criticality of the system and network. Proper access control policies and their enforcement is a mitigation method within the MITRE ATT&CK ICS framework [17], and applies to many of the threats identified for remote connection in Section III.B.

2. Securing BYOD

A strength of Zero Trust is the ability to perform security assessment on devices, in addition to user authentication. This helps to prevent compromised devices from accessing the system even if the user is authenticated. The ability to assess the security posture of each device provides an additional level of check before granting access. The checks are device agnostic and based solely on the device attributes used to enforce the security policy.

In ZT-OT, the PE levels serve as a form of network segmentation between the enterprise network, plant network and trusted zone network. Segmentation based on PE levels helps protect critical networks from unauthorized or unsecure devices.

Zero Trust can also help prevent bridging of networks. This is done by using the PEP to block access to the OT system from personal devices which are already connected to an unknown network. Information about unknown connections is obtained from the software agent installed in the personal device. This reflects the MITRE ATT&CK ICS

framework [17] in which network segmentation is a mitigation method for many BYOD threats identified in Section III.B, Threat Model.

D. WEAKNESS OF ZT-OT

In this section, we discuss potential weaknesses of ZT-OT and possible mitigations.

1. Reliance on Software Agent and Risk of Compromised Agent

Although the software agent is an optional component in our design, it is necessary for a subject to be able to access higher PE levels. Hence, most, if not all, CFE will come pre-installed with an agent and most employees may opt to have an agent installed on their personal devices for work purposes. This creates a dependency on the agent and its integrity. A spoofed agent may result in unauthorized access, or it may be blocked by malware from communicating with the PEP, which results in a denial of service.

A Trusted Platform Module (TPM) is a tamper-resistant integrated circuit built into devices that can be used to perform secure operations and protect sensitive information [33]. One method to reduce the risk of agent tampering is to allow installation only on devices with a TPM. Also, if the agent can only be installed by authorized personnel, the risk that the installation process is compromised is reduced. Furthermore, if only whitelisted devices are permitted to access certain resources, the effects of a spoofed agent trying to gain unauthorized access are reduced.

If the device is infected with malware that blocks agent communication, for example, blocking the port that the agent uses, then the only remediation might be to remove the malware or use a new device. In the OT sector, this is dangerous as it may potentially restrict access to stop the system during an emergency. For example, an emergency stop command to an overheating turbine may be blocked resulting in damage to physical environments.

2. Compromised Trusted Zone

In ZT-OT, a trusted zone is created to protect components that cannot interact with Zero Trust implementations. These include latency sensitive components and legacy systems (Purdue Level 0, Level 1, and potentially Level 2). The trusted zone may also contain physical sensors and actuators that have networking capabilities. Due to the criticality of devices found in the trusted zone, our hypothetical water plant assumes the highest PE level, Level 3, for this zone.

Despite the protection offered by ZT-OT, it is still possible that the trusted zone can be compromised. Compromise may be due to human errors such as misconfiguration or complacency (forgetting to lock the server room), zero-day exploits, vulnerabilities that create an attack vector into the zone, or direct physical access by a malicious insider. A compromised trusted zone is dangerous as it contains physical instruments which directly affect physical parameters of water treatment and can be manipulated to cause serious harm.

One mitigation strategy is to eliminate the concept of trusted perimeter and implement Zero Trust on all devices and networks. Further research into the possibility of implementing this interpretation of the Zero Trust paradigm on legacy devices and physical instruments will be required.

3. Single Point of Failure

In the ZT-OT design, all network traffic must be verified by a PEP. The PEP also relies on the PDP and PIP for access decisions. Any of these three components has the potential to become a singular point of failure, thereby jeopardizing the integrity of the entire network.

A PEP, PDP, or PIP could potentially be the target of denial-of-service attacks, which could arise either through deliberate actions of attackers or malicious insiders, or accidentally through careless insiders. Additionally, even actions from legitimate interconnected systems could contribute to a denial-of-service scenario. For example, a Zone B device might repeatedly attempt to establish a connection or sends an error

message to the SCADA workstation. This could flood the PEP, impeding its capacity to authenticate requests from other devices.

Robust mitigation strategies must be devised to protect the system against denial-of-service threats. One strategy would be to create backup PEP, PDP, and PIP. In ZT-OT, the complete SCADA system is situated in the trusted zone, which has no Zero Trust components. This setup helps to ensure that water treatment operations can continue, even in the event of failures in a Zero Trust component.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

This chapter summarizes the research and key findings of this thesis and provides a discussion regarding the application of Zero Trust on OT systems. Potential future works pertaining to this field is also explored.

A. SUMMARY

This thesis analyzed the feasibility and effectiveness of deploying the Zero Trust paradigm to OT systems in the water sector. We identified potential threats and, based on NIST's Zero Trust reference architecture, developed an OT architecture with Zero-Trust access control to support secure remote connections and authorized use of personal devices (BYOD). Using a hypothetical water treatment plant, we assessed our ZT-OT design in three use cases: routine maintenance, a non-routine check on water parameters, and scheduled software patching by vendors. Our analysis showed both strengths and weaknesses of implementing Zero Trust in OT systems.

We started with the hypothesis that the application of Zero Trust tenets and design can help modernize and secure legacy OT systems without affecting normal OT operations.

Findings from our research indicate that our ZT-OT design for a legacy water-treatment OT system can support secure both external remote connections and BYOD. Furthermore, the placement of the PEP and PDP components in the ZT-OT design can improve the security of legacy OT systems as they organically segment the OT network.

Nevertheless, certain aspects of ZT warrant further investigation. Specifically, the feasibility of applying the Zero Trust model to OT sectors other than water treatment. Another concern is that Zero Trust mechanisms might inadvertently block SCADA commands, which could adversely impact regular operations.

B. FUTURE WORK

The ZT-OT design utilizes a secured perimeter to protect legacy components, sensors, and actuators at Purdue level 0, 1 and 2. This means that the continuous verification tenet of Zero Trust is not applicable once a subject is authorized to enter the trusted zone network. As such, it is worth exploring the possibility of implementing Zero Trust on an OT network with legacy components to enable a full Zero Trust solution from Purdue Level 0 to Level 5. Furthermore, research to understand the effects of applying Zero Trust on OT components with limited computational resources or outdated operating system, or on entire legacy networks should be performed to formulate strategies for migrating both legacy and modern OT systems to a unified Zero Trust architecture.

NIST SP800-207 mentions the concept of de-perimeterization and that many definitions of ZT stress the concept of removing wide-area perimeter defense, such as an enterprise firewall [2]. While the architecture in the work presented here used network perimeter and segmentation as a form of defense-in-depth, analysis and research should be conducted to determine the possibilities of removing these network perimeters and the potential benefits that doing so may bring.

Another important topic to consider is logging and how Zero Trust may affect it. Logs are generated after an event has taken place and, if these logging requests are blocked by the PEP, there may be discrepancies in the audit trail. This challenge must be addressed when implementing Zero Trust both in IT systems and OT systems.

LIST OF REFERENCES

- [1] K. Stouffer et al., “Guide to Operational Technology (OT) Security: Initial Public Draft,” Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-82r3, Apr. 2022. Available: <https://doi.org/10.6028/NIST.SP.800-82r3.ipd>
- [2] S. Rose, O. Borchert, S. Mitchell, S. Connelly, “Zero Trust Architecture,” Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-207, Aug. 2020. Available: <https://doi.org/10.6028/NIST.SP.800-207>
- [3] White House. “Moving the U.S. government toward zero trust cybersecurity Principles,” Washington, DC, USA, 2022. Available: <https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>
- [4] Department of Defense, “DOD Zero Trust Strategy.” Accessed: Jan .05, 2023. Available: <https://dodcio.defense.gov/Portals/0/Documents/Library/DOD-ZTStrategy.pdf>
- [5] Cyber Security Agency of Singapore, “The Singapore Cybersecurity Strategy 2021,” Singapore, CSA, Oct. 2021. Available: https://www.csa.gov.sg/docs/default-source/csa/documents/publications/the-singapore-cybersecurity-strategy-2021.pdf?sfvrsn=809ced95_0
- [6] T. Olzak, “Risk management – Chapter 2,” Infosec Resources, January 20, 2012. Available: <https://resources.infosecinstitute.com/topics/application-security/risk-management-chapter-2/>
- [7] N. Falliere, L. O. Murchu, E. Chien, “W32.Stuxnet Dossier,” Symantec Corp., Cupertino, CA, USA, Symantec Security Response, 2011. Available: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
- [8] National Institute of Standards and Technology, “Programmable Logic Controller – Glossary | CSRC.” Accessed: Mar. 05, 2023. Available: https://csrc.nist.gov/glossary/term/programmable_logic_controller
- [9] A. Wedgbury and K. Jones, “Automated Asset Discovery in Industrial Control Systems – Exploring the Problem” in *3rd International Symposium for ICS & SCADA Cyber Security Research*, Sep. 2015. Available: <https://doi.org/10.14236/ewic/ICS2015.8>

- [10] X. Fan, K. Fan, Y. Wang, R. Zhou, “Overview of cyber-security of industrial control system,” in 2015 *International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, Aug. 2015. Available: <https://doi.org/10.1109/SSIC.2015.7245324>
- [11] U. D. Ani, H. He, and A. Tiwari, “Human factor security: evaluating the cybersecurity capacity of the industrial workforce,” *Journal of Systems and Info. Tech.*, vol. 21, no. 1, pp. 2–35, Mar. 2019, Available: <https://doi.org/10.1108/JSIT-02-2018-0028>
- [12] T. J. Williams, “The Purdue Enterprise Reference Architecture,” *IFAC Proceedings Volumes*, vol. 26, no. 2, pp. 559–564, Jul. 1993, Available: [https://doi.org/10.1016/S1474-6670\(17\)48532-6](https://doi.org/10.1016/S1474-6670(17)48532-6)
- [13] G. David, “Purdue Model Framework for Industrial Control Systems & Cybersecurity Segmentation,” Department of Energy, Washington, DC, USA, Topic Paper #4-14, 2019. Available: https://www.energy.gov/sites/default/files/2022-10/Infra_Topic_Paper_4-14_FINAL.pdf
- [14] A. Pascal, *Industrial Cybersecurity: Efficiency Secure Critical Infrastructure Systems*. Birmingham, UK: Packt Publishing, 2017. Available: <https://www.packtpub.com/product/industrial-cybersecurity/9781788395151>
- [15] Cyber Security Agency of Singapore, “Cybersecurity Code of Practice for Critical Information Infrastructure,” Singapore, CSA CCOP, Dec. 2022. Available: <https://www.csa.gov.sg/legislation/Codes-of-Practice>
- [16] Australian Government Department of Climate Change, Energy, the Environment and Water, “Australian Energy Sector Cyber Security Framework.” Accessed: Jan. 01, 2023. Available: <https://www.energy.gov.au/government-priorities/energy-security/australian-energy-sector-cyber-security-framework>
- [17] The MITRE Corporation, “Techniques – ICS | MITRE ATT&CK®.” Accessed: Jan. 03, 2023. Available: <https://attack.mitre.org/techniques/ics/>
- [18] International Society of Automation, “ISA99, Industrial Automation & Control Sys Security,” International Society of Automation, Research Triangle Park, NC, USA, ISA standards and Publications. Available: <https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99>
- [19] Department of Energy, “Colonial Pipeline Cyber Incident.” Accessed: Jan. 05, 2023. Available: <https://www.energy.gov/ceser/colonial-pipeline-cyber-incident>
- [20] Threat Hunter Team, “Attacks Against Critical Infrastructure: A Global Concern,” Symantec., Cupertino, CA, USA, 2021. Available: <https://symantec.broadcom.com/hubfs/Attacks-Against-Critical-Infrastructure.pdf>

- [21] D. K. Zafra *et al.*, “INDUSTROYER.V2: Old Malware Learns New Tricks,” Mandiant, April 25, 2022. Available: <https://www.mandiant.com/resources/blog/industroyer-v2-old-malware-new-tricks>
- [22] Cybersecurity and Infrastructure Security Agency, “Compromise of U.S. Water Treatment Facility,” Feb. 12, 2021. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-042a>
- [23] Republican Policy Committee, “Infrastructure Cybersecurity: Water Systems,” May 19, 2022. Available: <https://www.rpc.senate.gov/policy-papers/infrastructure-cybersecurity-water-systems>
- [24] Singapore University of Technology and Design, “Secure Water Treatment.” Accessed: Dec. 2, 2022. Available: <https://itrust.sutd.edu.sg/testbeds/secure-water-treatment-swat/>
- [25] National Institute of Standards and Technology, “Implementing a Zero Trust Architecture, Volume B: Approach, Architecture, and Security Characteristics,” Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 1800-35B, Dec. 2022. Available: <https://www.nccoe.nist.gov/sites/default/files/2023-07/zta-nist-sp-1800-35b-preliminary-draft-3.pdf>
- [26] E. B. Boumhaout, A. S. Danielsen, O. B. E. Pedersen, M. Shahid, “Towards Zero Trust for Critical Infrastructure,” Massachusetts Institute of Technology, Cambridge, MA, USA, 2020. Available: <https://courses.csail.mit.edu/6.857/2020/projects/2-Boumhaout-Danielsen-Pedersen-Shahid.pdf>
- [27] F. Federici, D. Martintoni, and V. Senni, “A Zero-Trust Architecture for Remote Access in Industrial IoT Infrastructures,” *Electronics*, vol. 12, no. 3, p. 566, Jan. 2023. Available: <https://doi.org/10.3390/electronics12030566>
- [28] S. Teerakanok, T. Uehara, and A. Inomata, “Migrating to Zero Trust Architecture: Reviews and Challenges,” *Security and Comm, Networks*, vol. 2021, article ID 9947347, May 2021, Available: <https://doi.org/10.1155/2021/9947347>
- [29] Centre for the Protection of National Infrastructure, “Configuring and Managing Remote Access for Industrial Control Systems,” Department of Homeland Security, Washington, DC, USA, Nov 2010. Available: https://www.cisa.gov/sites/default/files/recommended_practices/RP_Managing_Remote_Access_S508NC.pdf
- [30] National Cyber Security Centre, “Device Security Guidance for Bring your own device (BYOD).” Accessed Mar. 07, 2023. Available: <https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device>

- [31] K. Boeckl et al., “Mobile Device Security: Bring Your Own Device (BYOD),” Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 1800-22, Nov. 2022. Available: <https://www.nccoe.nist.gov/sites/default/files/2022-11/mdse-nist-sp1800-22-draft-2.pdf>
- [32] Microsoft, “Service accounts.” Accessed: Sep. 1, 2023. Available: <https://learn.microsoft.com/en-us/windows-server/identity/ads/manage/understand-service-accounts>
- [33] National Institute of Standards and Technology, “Trusted Platform Module (TPM).” CSRC. Accessed: Aug. 25, 2023. Available: https://csrc.nist.gov/glossary/term/trusted_platform_module

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Fort Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California



DUDLEY KNOX LIBRARY

NAVAL POSTGRADUATE SCHOOL

WWW.NPS.EDU

WHERE SCIENCE MEETS THE ART OF WARFARE