A COMPREHENSIVE SECURITY TESTING FRAMEWORK FOR PLC- BASED INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS

Cyber Security
Master's Degree Programme in Information and Communication Technology
Department of Computing, Faculty of Technology
Master of Science in Technology Thesis

Author:
Greeshma Swapnika Manubolu

Supervisors:
Tahir Mohammad (University of Turku)
Petri Sainio (University of Turku)
Imed Hammouda (Konecranes Global Oy)

June 2024

Master of Science in Technology Thesis
Department of Computing, Faculty of Technology
University of Turku

Subject: Cyber Security
Programme: Master’s Degree Programme in Information and Communication Technology
Author: Greeshma Swapnika Manubolu
Title: A comprehensive Security Testing Framework for PLC-based Industrial Automation and Control Systems.
Number of pages: 91 pages
Date: June 2024

The thesis focuses on developing a comprehensive security testing framework for Industrial Automation and Control Systems (IACS) based on Programmable Logic Controllers (PLCs). This framework aims to evaluate the security posture of PLC-based IACS systems using methods, tools, and best practices in security testing tailored to the specific characteristics of PLC environments. It leverages existing security standards such as the IEC 62443 standard. The methodology employed in this research is the Design Science methodology, serving as the systematic problem-solving strategy throughout the development of the framework. This methodology ensures the robustness and applicability of the framework within the domain of IACS. The framework encompasses various phases, including threat modeling, initial risk assessment, security testing tools and techniques, comprehensive risk evaluation, reporting mechanisms, and incident response planning.

Throughout the development process, adherence to the IEC 62443 standard is maintained, ensuring alignment with established industrial best practices and regulatory requirements. This adherence aims to bolster the security of IACS infrastructure and facilitate compliance with European Union (EU) regulations. Validation of the framework is achieved through its illustration to an Information Technology (IT) and Operational Technology (OT) asset within an industrial context. This research significantly contributes to advancing cybersecurity practices for security testing within industrial settings. By providing a structured methodology, practitioners are empowered to systematically inspect and enhance the security of PLC-based IACS systems.

The proposed framework's modular and independent nature makes it highly adaptable for deployment across various target systems. It conforms to recommended standards within the domain of IACS, aiming to establish secure and resilient industrial infrastructures capable of mitigating emerging cyber threats. Implementation of the framework's guidelines is anticipated to contribute to improved security and EU regulatory compliance within IACS environments.

Keywords: Security, Security testing, Security Standards, EU Regulations, Design Science Methodology.

Preface

I would like to express deep appreciation to Tahir Muhammad and Petri Sainio for the diligent supervision and invaluable assistance during my thesis. Their guidance was helpful in navigating the intricate details of the thesis.

I would also like to express gratitude to my advisor from Konecranes, Imed Hammouda, whose unwavering assistance and helpful critique were crucial in enhancing this thesis. Without the extensive conversations and insightful feedback provided by this person, the thesis would not have achieved its current level of scholarly rigour. I am profoundly grateful for his mentorship, which epitomises intellectual excellence.

Additionally, I am grateful to my Manager, Otso Karhu, at Konecranes, for giving me the opportunity to thoroughly explore this topic and for his consistent backing throughout.

Furthermore, I would like to extend my appreciation to my peers and co-workers for their immense proofreading efforts and for participating in intellectually intriguing discussions that enhanced the content of this project.

Finally, I want to express sincere gratitude to my cherished family for their steadfast support and encouragement. Their constant faith in my academic endeavours has provided me with tremendous fortitude and inspiration.

19.06.2024

Greeshma Manubolu

Table of contents

Abbreviations and Acronyms

CIA	Confidentiality, Integrity, and Availability
CRA	Cyber Resilience Act
DAST	Dynamic Application Security Testing
DDoS	Distributed Denial of Service
DSR	Design Science Research
IACS	Industrial Automation and Control Systems
IIoT	Industrial Internet of Things
NIS	Network and Information Systems
OT	Operational Technology
PERA	Purdue Enterprise Reference Architecture
PLC	Programmable Logic Controller
RED-DA	Radio Equipment Directive- Delegated Act
SAST	Static Application Security Testing
SL	Security Level
SL-A	Achieved Security Level
SL-C	Capability Security Level
SL-T	Target Security Level
SR	System Requirements
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Escalation of Privilege
SVV	Security verification and validation
TIA	Totally Integrated Automation

List of Figures

List of Tables

Glossary

Asset: physical or logical object having either a perceived or actual value to the IACS.

Authentication: Provision of assurance that a claimed characteristic of an identity is correct.

Availability: Property of ensuring timely and reliable access to and use of control system information and functionality.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Consequence: Condition or state that logically or naturally follows from an event

Control system: Hardware and software components of an IACS

Event: Occurrence of or change to a particular set of circumstances.

IACS Systems: Collection of personnel, hardware, software, and policies involved in the operation of the industrial process.

Impact: Evaluated consequence of a particular event.

Incident: Event that is not part of the expected operation of a system.

Integrity: Property of protecting the accuracy and completeness of assets.

Risk: Risk pertains to the potential for adverse outcomes.

Safety: The condition of being protected from or unlikely to cause danger, risk, or injury.

Security: The state of being free from danger or threat.

Security level: Measure of confidence that the IACS is free from vulnerabilities.

Security testing: A process intended to detect flaws in the security mechanisms

Threat: Circumstance or event with the potential to adversely affect operations, assets, control systems or individuals.

Vulnerability: Any weakness, flaw or gap in the security protocols or architecture of a system, network, or organization.

1 Introduction

Industrial Automation and Control Systems (IACS) play a key role in modern production facilities. On one hand, they provide real-time functionality to the connected field devices. On the other hand, they get more and more connected to local networks and the internet to facilitate use cases promoted by "Industry 4.0" [1]. After Stuxnet was reported in 2010, cyber security has become one of major concerns for the IACS industry.

Some of IACS systems are used for operating national critical infrastructures such as energy sector and power sector, any loss or damage to them may risk people's lives and safety, national security, economic vitality, societal well-being, and preservation [2]. The dynamic nature of cyber threats and the interplay between OT and IT systems present significant challenges in ensuring comprehensive cybersecurity of IACS systems making them susceptible to cyber-attacks by exploiting the vulnerabilities that further interrupt the automation processes.

The Programming and Logic Controllers (PLCs) are the complex embedded devices, considered the heart of IACS systems, often relies on an operating system. However, we don't need bugs or vulnerabilities to attack the PLCs [3]. It is easy to exploit its normal operation provided we have some access to the device. To avoid expensive business losses or production disruption due to misuse of the systems and PLCs, IACS manufacturers and integrators should protect their systems by planning a comprehensive security testing for their devices focussing on the defence-in-depth strategy.

1.1 Motivation

The motivation behind this research stems from the imperative to align with regulatory obligations and security best practices, particularly focusing on the role of a potential common standard as outlined in these regulations. Establishing this motivation lays the foundation for the ensuing research questions. Specifically, there arose a need for a company such as Konecranes, a global giant in crane manufacturing and material handling solutions, to evaluate the security of its PLC-based control systems to adhere to the regulatory requirements. The landscape is evolving rapidly with a deluge of upcoming regulations from the EU, such as the Machinery Regulation, Cyber Resilience Act (CRA), NIS2 (Network and Information Systems) directive, Radio Equipment Directive (RED), and others, all of which include cybersecurity-related mandates, provisions, and clauses.

Currently, Konecranes faces a gap of not having any existing framework to address this need. The motivation arises from this gap, underscoring the necessity for a comprehensive security testing framework. As a global entity, Konecranes anticipates navigating a myriad of forthcoming regulations across regions globally such as in the EU, China, the US, the UK, and the APEC region. The company seeks to ensure its PLC-based crane control systems comply with these regulations. Notably, these regulations provide the option for companies to adopt a harmonized standard - a common benchmark facilitating self-assessment for regulatory compliance.

Within this context, the IEC (International Electrotechnical Commission) 62443 standard emerges as the widely recognized standard globally for the security of IACS systems. This standard is closely aligned with the anticipated harmonized standard from the EU, which is yet to be published. Therefore, considering the IEC 62443 standard becomes pivotal for assessing PLC-based IACS systems globally. Simultaneously, the aim is not to overlook established security testing best practices, setting the stage for the Research Questions.

1.2 Research Problem

The primary research problem lies in the absence of a specialized security testing framework specifically designed for PLC-based IACS systems, aligned with the IEC 62443 standard. Existing frameworks and standards, while providing valuable insights, fail to address the unique security requirements and challenges inherent in PLC-based systems. Consequently, organizations face difficulties in conducting thorough security assessments and mitigating cyber risks effectively.

1.3 Research Questions and Objectives

The goal of this thesis is to develop and refine a comprehensive Security Testing Framework tailored specifically for PLC-based IACS systems. This framework aims to address the security challenges posed by PLCs within the broader context of IACS, focusing on enhancing cyber resilience, mitigating vulnerabilities, and ensuring compliance with relevant industry standards and regulations. Through a systematic approach, the thesis seeks to synthesize existing knowledge, adapt it to PLC-based systems, and align the framework with recognized security standards such as ISA/IEC 62443.

To address the research problem, the following key questions guide this study:

RQ 1: What are the essential components of a Security Testing Framework tailored to IACS ?

RQ 2: How can these components be adapted to address the specific security challenges posed by PLC-based IACS systems ?

RQ 3: In what ways can the framework be aligned with the principles of the security standards such as ISA/IEC 62443 standard ?

There are three corresponding objectives of this research:

1. To develop a comprehensive security testing framework specifically tailored to address the unique security requirements of PLC-based IACS systems.

2. To provide clear guidance on the implementation of the framework in compliance with the IEC 62443 standard.

3. To contribute a practical and effective tool that organizations can use to assess and improve the security posture of their PLC-based IACS environments, fostering a more resilient and secure industrial ecosystem.

To answer these research questions and meet the objectives, the research adopts a Design Science Research Methodology, which facilitates the iterative development and refinement of the security testing framework. The work will consist of multiple iterations in which a regulative cycle framework is applied. The goal of each iteration is to improve the solution based on the evaluation of the previous iteration. The regulative cycle in each iteration consists of five phases: problem investigation, solution design, design validation, implementation, and evaluation.

To gather comprehensive data and inform the framework development, a multi-faceted approach will be employed, leveraging various sources:

- Extensive Literature Review: Scholarly articles, industry reports, and standards documents were meticulously analyzed to glean relevant knowledge from the best practices.

- Focused Discussion Groups: Experts from diverse domains, including IEC 62443 specialists, PLC developers, security professionals, Safety experts and IACS practitioners, were engaged in focused discussions to gain critical insights and practical perspectives and had contributed to the contribute to the refinement of the security testing framework.

Discussions are held with security experts to identify the underlying challenges and required components of the framework while also receiving insight into the current state of the security testing processes. It also included investigating the global standards for IACS security.

1.4 Scope, Limitations and Delimitations

Through the development of an exhaustive security testing methodology, the scope of this master's thesis intends to contribute to the ongoing work to improve IACS security. The cybersecurity approaches and concepts on which the framework is built have been thoroughly verified, and it has been adapted to address the unique challenges and requirements encountered in IACS environments. Its goal is to provide companies with the resources that they need to proactively evaluate the security posture and thereby perform the comprehensive security testing of their systems, hence ensuring the robustness and security of essential infrastructure over time.

1.5 Structure of the thesis

The thesis comprises seven chapters. Chapter 1 introduces the research topic, motivation, research problem, objectives, and research questions. Chapter 2 highlights the theoretical background of PLC-based IACS systems, security challenges, relevant frameworks, standards, and EU regulations. Chapter 3 outlines the research methodology, employing the Design Science Research Methodology and iterative cycles. Chapter 4 presents the development of the security testing framework through iterations, illustrated with examples. Chapter 5 discusses the findings and outlines future work. Results and discussions are presented in Chapters 5 and 6, reflecting on the developed framework's effectiveness and implications. Finally, Chapter 7 concludes the thesis, summarizing the research findings and their implications for industrial cybersecurity and its significance on future research.

2 Literature Review and Background

2.1 The EU Regulations on Industrial Cyber Security

The EU Regulations on Industrial Cyber Security are set to be enforced, highlighting the need for organisations like Konecranes to adopt a robust security testing framework. This is crucial for Konecranes to ensure compliance with these regulations and maintain its competitiveness in the evolving landscape of industrial cybersecurity. The regulations aim to protect sensitive data and fortify critical infrastructure, making robust cybersecurity measures essential. As Konecranes navigates the terrain of compliance with these regulations, the selection of an appropriate security testing framework emerges as a strategic imperative. This section will explore the key aspects of the EU Regulations on Industrial Cyber Security and their implications.

2.1.1 The Cyber Resilience Act

The Cyber Resilience Act (CRA) is a crucial regulation in the EU's industrial cybersecurity sector, focusing on critical sectors like energy, transport, power, manufacturing, and waste management [4]. It aims to enhance the EU's ability to prevent, detect, and respond to cyber incidents effectively. Key cyber security requirements include risk management, prompt incident reporting, conformity assessment procedures, and vulnerability assessments. These requirements demand thorough security testing in industrial organizations, integrating risk management into risk assessments. By incorporating the CRA ideas into their cybersecurity defenses, industrial organizations can strengthen their industrial ecosystem.

2.1.2 NIS 2 (Network and Information Systems Directive)

The NIS 2 directive, enforced in January 2023, aims to enhance cybersecurity in both critical sectors like energy, transport, and health and important sectors such as manufacturing [5]. It mandates operators of essential services to implement security measures and report cyber incidents promptly. The directive emphasizes a comprehensive risk management approach, safe supply chains, frequent vulnerability assessments, strengthened security testing procedures, and consistent penetration testing, vulnerability scanning, and patching. Proactive regulation management and prioritizing security testing can help industrial organizations manage complex regulations and strengthen cybersecurity defenses.

2.1.3 Radio Equipment Directive - Delegated Act (RED-DA)

RED-DA came into force in March 2022, to improve the security of wireless devices in the EU market. It sets out cybersecurity standards, including secure boot, secure communication protocols, vulnerability management, and software upgrades [6]. Manufacturers must prove compliance through risk assessments, security testing, and conformity assessment procedures. Proactive compliance with EU cybersecurity standards is crucial for gaining a competitive advantage and enhancing industrial security. The Act must be considered alongside other requirements like NIS 2, and ongoing education and adjustment are necessary for successful management.

2.1.4 Machinery Regulation

Came into force in June 2023, this regulation [7] mandates manufacturers to consider cybersecurity when designing and manufacturing machinery. It emphasizes the need for robust measures to prevent potential cyber threats. The regulation requires risk-based cybersecurity, conducting risk assessments at various stages of the machinery lifecycle. It recommends that the security testing should align with risk assessments and focus on important functionalities and vulnerabilities.

Essential Safety Requirements (ESRs) cover cybersecurity aspects like secure communication methods, software upgrades, resistance to unauthorised access, incident reporting, and technical documentation. Proactive security testing is required, integrating testing across the machinery lifecycle, conducting regular penetration testing, software updates, and ensuring supply chain security. This proactive approach ensures compliance, reduces risks, and establishes trust in machinery.

2.1.5 EU Cyber Security Act

The EU Cybersecurity Act, enacted in June 2019, significantly enhances industrial security by increasing awareness and cooperation. It establishes the European Union Agency for Cybersecurity (ENISA) and the Cybersecurity Certification Framework, which certifies ICT products, services, and processes according to cybersecurity standards. The Act [8] encourages incident reporting and a culture of sharing information, requiring industrial stakeholders to stay updated on regulatory changes.

2.1.6 EU's Artificial Intelligence Act (AIA)

The AIA emphasizes ethical AI development, responsible usage, and cybersecurity. It requires AI systems to be designed with secure coding methods, vulnerability assessments, and penetration testing. The AIA [9] also emphasizes risk reduction strategies, data protection, and security transparency. It considers unified standards and certifications and continuous monitoring of the evolving cybersecurity environment for compliance and risk reduction.

The European Union (EU) has implemented various cybersecurity regulations to strengthen industrial security, protect sensitive data, and secure communications networks. However, these regulations do not prescribe a universal approach. Therefore, it is crucial to explore prevalent security frameworks and standards when formulating a compliance strategy for these regulations. The following section dives into the prevalent security frameworks and standards applicable to the IACS security.

2.2 Security Frameworks and Standards for IACS systems

IACS systems are vital in various industries, such as energy, manufacturing, and transportation, and their protection from cyber-attacks is crucial for their safety and continuity. However, organizations face the challenge of navigating cybersecurity compliance without a clear roadmap from regulations. Existing frameworks and standards, such as the Cybersecurity Framework (CSF) developed by the National Institute of Standards and Technology (NIST), the NIST 800-82 Guide to ICS Security, and ISA 99.02.01/IEC 62443: Security for IACS, are essential for organizations seeking to enhance their IACS security posture.

These frameworks offer structured approaches, best practices, and detailed specifications to help organizations navigate the complexities of cybersecurity. By exploring these frameworks and standards, organizations can uncover their unique strengths, considerations, and implications for securing their PLC-based IACS systems, equipping them with the knowledge and tools to make informed decisions for enhanced cybersecurity and regulatory compliance.

2.2.1 NIST Cyber Security Framework

The NIST-CSF [10] is a set of voluntary recommendations, standards, and best practices designed to help organizations improve their cybersecurity status. It offers a standardized method for addressing and communicating cybersecurity risks and goals across various industries. The CSF is organized into five fundamental functions: Identify, Protect, Detect, Respond, and Recover. It is adaptable and expandable, allowing organizations to customize its application to their specific requirements and risk profile.

The benefits of the CSF include enhanced cybersecurity posture, flexibility, communication, and a consistent language for cross-functional teams. However, it may not cover all industry-specific concerns related to IACS security. Therefore, aligning frameworks, addressing risks, and effectively incorporating CSF principles into the IACS security management system are crucial.

2.2.2 ISA/IEC 62443 Standard

ISA/IEC 62443 is a framework designed to help organizations implement robust cybersecurity protocols to protect their infrastructure assets from cyber threats [11]. It is based on risk, focusing on protecting critical assets based on their significance and potential vulnerabilities. The framework addresses security throughout the entire lifecycle of the IACS, from design and development to operation and maintenance. It establishes rules for shared responsibility for stakeholders like operators, integrators, and manufacturers.

Key aspects include technical criteria, process requirements, and certification schemes. IEC 62443 offers benefits such as enhanced security posture, reduced cyber threats, facilitation of trade and compliance with regulations, and a uniform language and methodology for IACS security. However, it has limitations such as complexity and lack of adaptability. Implementing all criteria can be challenging and resource-intensive, and it may not be suitable for all unique industry specifications. Therefore, IEC 62443 is not a universal solution, but must be tailored to IACS environments and potential risks.

2.2.3 IEC 27001/27002 Standards

ISO/IEC 27001 is a global standard that pertains to information security management systems (ISMS). Although not exclusive to IACS systems, it offers a structure for creating, executing, upholding, and enhancing an organization's information security management system.[12] Organisations can customise ISO/IEC 27001 to meet the cybersecurity requirements of IACS systems. ISO/IEC 27002 [13] offers guidance on how to put information security controls into practice. Although not exclusive to IACS systems, it provides a thorough collection of security measures that organisations can implement to safeguard the safety, confidentiality, integrity, and availability of information and physical assets.

2.2.4 Purdue model of secure control systems

A conceptual framework that divides systems into zones with differing security levels based on their criticality, promoting defence-in-depth techniques. This model was developed by Purdue University and is relevant to the IACS systems [14]. It may require adaption to unique IACS difficulties and demands but the model is simple and easy to understand, which helps with risk-based segmentation and makes it easier to create secure network architecture.

2.2.5 Cyber Security Capability Maturity Model (C2M2)

The C2M2 model is a versatile tool that can be customized to improve cybersecurity in IACS systems. It involves evaluating maturity using five C2M2 levels, providing guidance on 18 C2M2 practices, analyzing gaps between current practices and C2M2 requirements, and developing a roadmap for implementing essential security controls [15]. However, it may require specialized industry assistance, be resource-intensive, and have limited qualified assessors. Integrating C2M2 with other frameworks like IEC 62443 can create a more comprehensive strategy.

2.2.6 MITRE ATT&CK Framework

The adversary-centric approach offers significant insights into the behaviours and tactics of attackers, which contribute to the mapping of threats to specific mitigation techniques within the IACS environment [16,17]. It supports the understanding of attacker motivations and techniques, enables the integration of threat intelligence, and makes it easier to implement targeted defence strategies. It requires expertise for interpretation and application to specific IACS contexts and necessitates continuous monitoring and adaptation as TTPs are constantly evolving.

2.2.7 SANS Critical Security Controls (CSC)

It provides twenty security controls that are prioritised and specifically adapted for IACS environments with thorough implementation procedures and tools [18]. It provides actionable recommendations, is aligned with other frameworks, and prioritises controls based on their criticality for IACS. It necessitates customisation based on specific IACS risks and needs, as well as continuing effort for deployment, maintenance, and effectiveness assessment.

2.2.8 NERC Reliability Standards (CIP standards)

Although these standards cover a wider range of topics than cybersecurity, they do include security-related issues for a variety of critical infrastructure sectors, and they provide valuable best practices. Industry-specific guidance that goes beyond electric power and integrates with other NERC CIP standards [19] for a holistic approach is one of the strengths of this standard.

2.2.9 IEC 61508 Standard

It primarily addresses functional safety principles in industrial automation systems. These principles are crucial for the safety and security of IACS, with an emphasis on risk assessment and minimization. It provides a structured approach to safety-related systems, which enhances overall dependability and security, is one of the strengths of this system [20]. The primary emphasis is placed on functional safety, and integration with specialised cybersecurity frameworks is necessary to provide comprehensive protection.

Organizations must carefully evaluate their specific needs and objectives when selecting a security testing option for PLC-based IACS systems. The ISA/IEC 62443 framework offers a comprehensive solution, while NIST SP 800-82 provides guidelines for enhancing overall IACS security. ISO/IEC 27001 focuses on the IT side, establishing a robust Information Security Management System, while the IEC 62443 standard focusses on the OT side, providing a detailed specification for safeguarding the IACS systems.

Each framework has unique strengths, making the selection process complex yet crucial for strengthening cybersecurity measures. Considering Konecranes interest in securing its PLC-based crane control systems, the IEC 62443 standard emerges as the most pertinent choice. Therefore, we shall dive into the specifics of this standard in the subsequent section.

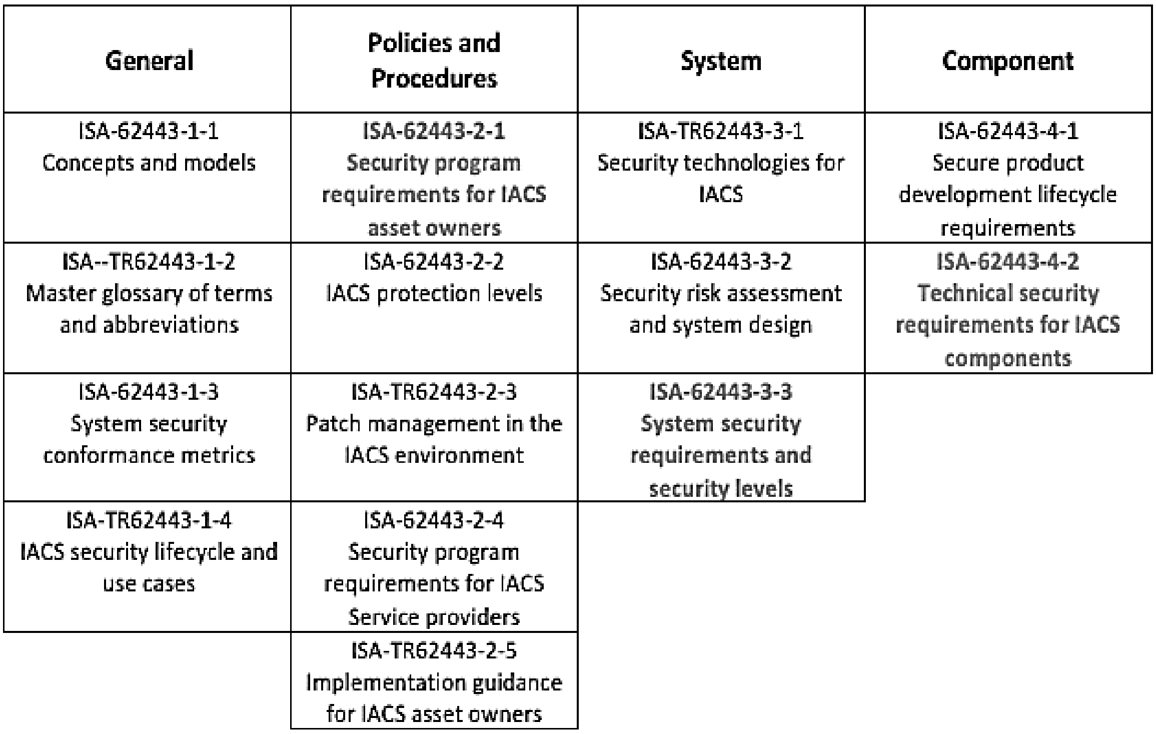
2.3 ISA/IEC 62443 standard

The ISA/IEC 62443 standard [21], developed by the International Society of Automation (ISA) and the International Electrotechnical Commission (IEC), is a widely recognized reference for OT security in various industries. It has been adopted by over 20 sectors and is crucial for ensuring the security and robustness of IACS. The ISA 99 standards committee, established by ISA, was later adopted by the IEC. The IEC 62443 series provides a comprehensive framework for assessing risks, establishing security policies, and implementing protective measures, directing organizations towards strong cybersecurity safeguards for critical infrastructure [58].

IEC 62443 is a set of standards designed to enhance cybersecurity of IACS systems by incorporating features like zone and conduit design, stringent access controls, and constant monitoring. It offers guidance on cybersecurity management systems and risk assessments in IACS/OT environments. The standards help organizations determine their security maturity, select security products and service providers, and enhance technical reports. It defines procedures for secure product design, security requirements, enhanced coding techniques, and risk-conscious deployment strategies.

The standards are structured into four parts as depicted in the Figure 1:

General section covers the introductory information, vocabularies, concepts, and example use cases. Policies and Procedures section includes security program requirements, patching procedures, and implementation guidance. System security section addresses risk assessment approaches, security requirement levels, and recommended technologies. Component security section focusses on product lifecycle and technical requirements for system component



General	Policies and Procedures	System	Component
ISA-62443-1-1 Concepts and models	ISA-62443-2-1 Security program requirements for IACS asset owners	ISA-TR62443-3-1 Security technologies for IACS	ISA-62443-4-1 Secure product development lifecycle requirements
ISA--TR62443-1-2 Master glossary of terms and abbreviations	ISA-62443-2-2 IACS protection levels	ISA-62443-3-2 Security risk assessment and system design	ISA-62443-4-2 Technical security requirements for IACS components
ISA-62443-1-3 System security conformance metrics	ISA-TR62443-2-3 Patch management in the IACS environment	ISA-62443-3-3 System security requirements and security levels	
ISA-TR62443-1-4 IACS security lifecycle and use cases	ISA-62443-2-4 Security program requirements for IACS Service providers		
	ISA-TR62443-2-5 Implementation guidance for IACS asset owners		

Figure 1: Structuring of the ISA/IEC 62443 standards

2.3.1 Zones, Conduits and Security levels

IEC 62443 is a standard for securing IACS systems, focusing on core concepts like Systems under Consideration (SuCs), Maturity Levels (MLs), Security Levels (SLs), zones and conduits

[22]. It classifies organizations with IACS systems into security zones [23] based on risk assessment and provides instructions on selecting these zones and determining SL implementation stages based on the determined ML. Asset owners can initially select a SuC and define pre-defined SLs to describe desired target security levels (SL-Ts), achieved levels (SL-As), and capability levels (SL-Cs). The Security Level scale, ranging from 0 to 4, is linked to these specific zones or levels.

These Security Levels are categorized as follows [24]:

SL 4: Protection against intentional violation using sophisticated means with extensive resources, specialized skills, and high motivation.

SL 3: Protection against intentional violation using sophisticated means with moderate resources, specialized skills, and moderate motivation.

SL 2: Protection against intentional violation using simple means with limited resources, basic skills, and low motivation.

SL 1: Protection against casual or coincidental violation.

Asset owners can apply security levels by dividing a system into "zones" and "conduits." Zones are physical asset groups with shared security requirements, while conduits are communication groupings that share the same security requirements and can represent communication tunnels between zones. Furthermore, to assist users in identifying the Security Level (SL) needed for each security zone, the standard 1-1 classifies seven Fundamental Requirements (FRs), which are then broken down into a set of system requirements to increase overall security (Table 1).

Table 1: Fundamental Requirements of IEC 62443-1-1 [27]

Fundamental Requirement (FR)	Subject
FR 1	Identification and Authentication control
FR 2	Use Control
FR 3	System Integrity
FR 4	Data Confidentiality
FR 5	Restricted data flow
FR 6	Timely response to event
FR 7	Network resource availability

These fundamental requirements are common throughout the standard and this taxonomy helps architects, engineers, and security professionals describe desired risk levels and mechanisms for achieving specific security objectives or Cyber Risk Reduction Factors.

2.3.2 IEC 62443 standard and Purdue model

IEC 62443 does not replace existing models such as ISA95 and Purdue (Figure 2); instead, it builds upon them, providing comprehensive coverage of cybersecurity and modern concepts. However, organizations seem to still find value in using ISA95 and Purdue models for specific security requirements, particularly in scenarios involving Industrial IoT devices [28] connected directly to the Internet or the cloud.

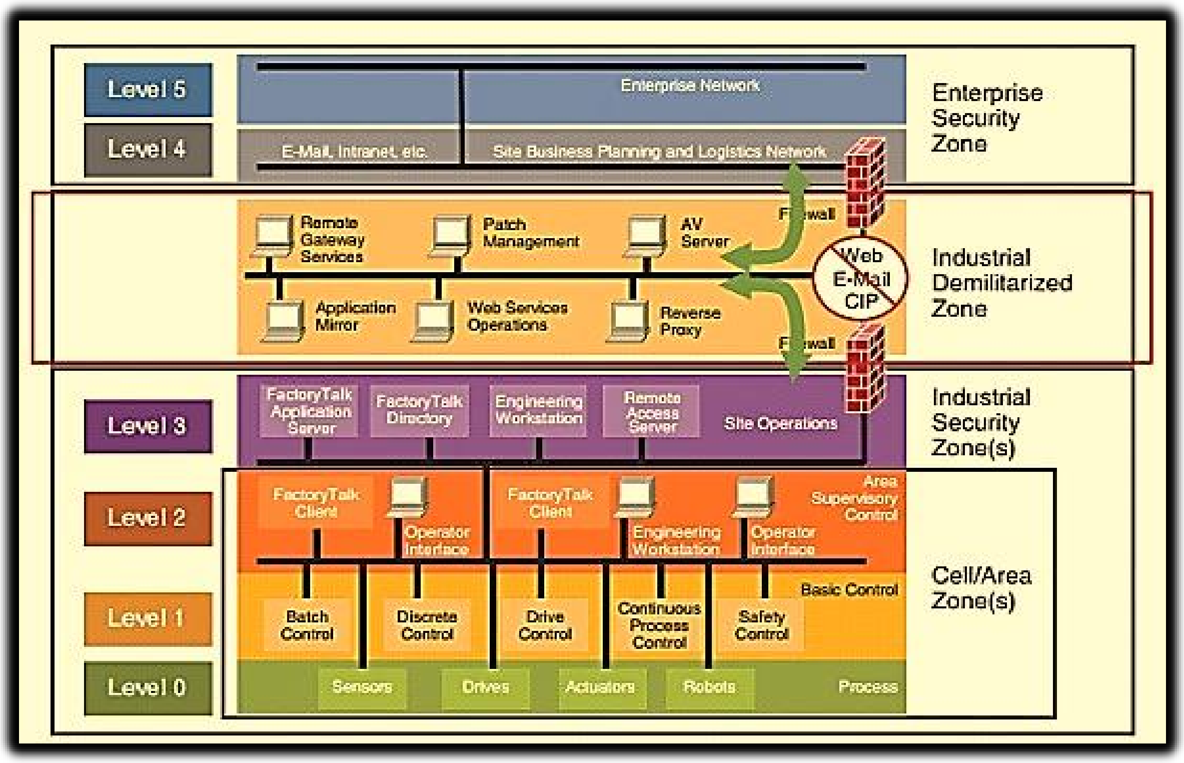


Figure 2: Purdue Architecture Reference Model [29]

2.3.3 IEC 62443 and Security testing

When it comes to the security testing context in the IEC 62443, SFS-EN IEC 62443-4-1:2018 , Chapter 3 covers terms, definitions, abbreviated terms, acronyms, and conventions about the security testing. Security verification and validation testing (IEC 62443-4-1-3.1.33) is to be conducted to evaluate the security of a component, product, or system within its intended security context and to confirm if it meets the security requirements and serves its security purpose. Security verification testing complements security validation testing by providing extra testing that emphasises the product's security context and defence in depth strategy. Fuzz testing (3.1.19), a process of creating malformed or unexpected data or call sequences to be consumed by the entity under test to verify that they are handled appropriately.

Unit testing (IEC 62443-4-1-3.1.39) is the process of verifying that an individual unit of computer software or hardware functions as intended. Automated verification, or testing, is typically carried out by computer test software. The standard also defines various testing activities (IEC 62443-4-1) under the category of System Validation and Verification (SVVs) as listed in Table 2, other than the static testing that the standard recommends it to be performed by the developers themselves to perform the static code checks [30]. It includes various tests for security requirements, threat mitigation, vulnerability testing, penetration testing and so on.

Table 2: Testing activities in the IEC 62443 standard

SVV	Subject
SVV 1	Security requirements testing
SVV 2	Threat mitigation testing
SVV 3	Vulnerability Testing, might be added to DevOps (recurring automated testing),
SVV 4	Penetration Testing (often it will be done by the subject matter expert consultants)
SVV 5	Independence of tester requirements

These are just some relevant features of the standard. Moving further, a foundational understanding is highly required about the PLC-based IACS system before considering the security aspects of it. So, the upcoming section delves into PLC architecture, the threat landscape, and the critical role of safety in securing these systems. This exploration aims to uncover vulnerabilities within these systems and identify key areas that require prioritized attention. Understanding these aspects is crucial for developing a comprehensive and effective security testing framework for PLC-based IACS systems.

2.4 PLC-based IACS Security

2.4.1 PLC Architecture

Programmable Logic Controllers (PLCs) are essential components of IACS systems. They manage physical processes and transmit data to higher levels for analysis [31]. PLCs are the backbone of any industrial system today specializing in control and automation in a variety of industries. A PLC system as depicted in Figure 3, will generally have 3 parts: CPU (or brain), I/O Modules and programming software. The CPU can best be described as the brain of any system as it executes the control logic programmed by the engineers.

Here, it processes inputs from various sensors and other devices (via the I/O Modules), takes into consideration the logic, and then finally sends outputs as signal to actuators and machinery. Meanwhile, the I/O Modules work together with the CPU to provide the link between devices in the physical world, so these modules help to their inputs and outputs to and from sensors and actuators.

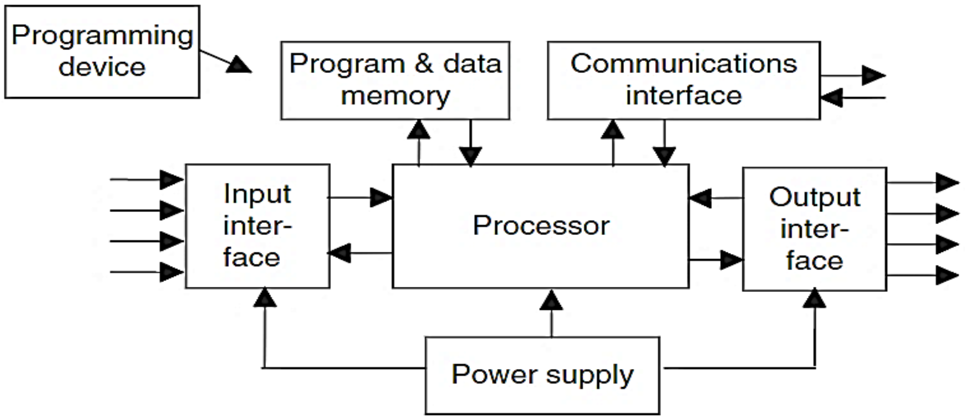


Figure 3: PLC Architecture

PLC architecture is a combination of hardware and software designed to provide efficient and reliable automation solutions for industrial processes. It includes communication interfaces, memory modules, and diagnostics. Communication interfaces allow PLCs to connect to other devices or systems, allowing data to be retrieved, synchronized, and exchanged across systems or networks.

Memory modules store PLC program and configuration settings, ensuring the integrity of automation logic even in power outages or system faults. Diagnostics monitor PLC status real-time, facilitating fault-finding and remedy on the plant floor, preventing costly downtime, and maximizing productivity. A PLC is hence the preferred, reliable, and flexible solution for industrial automation due to its ease of troubleshooting and design flexibility.

2.4.2 Threat landscape of PLC-based IACS systems

PLCs possess attributes that improve operational efficiency but also make them vulnerable to a wide range of cybersecurity attacks. The increasing interconnectivity and interdependence of PLCs in industrial ecosystems introduce new avenues for cyber-attacks [32,33]. PLCs and other IACS components are susceptible to various threats, including malware, cyber-attacks, ransomware, default credentials, network intrusions, man-in-the-middle attacks, DoS attacks, physical security concerns, supply chain vulnerabilities, insider threats, integration concerns, and outdated software and firmware.

Security incidents at the PLC level, such as Stuxnet, pose significant risks to critical infrastructure. Many critical infrastructures managed by IACS systems lack adequate security assessments against cyber-attacks. The threat landscape for PLCs is complex, involving targeted malware, ransomware, botnets, firmware vulnerabilities, network-based threats, physical security risks, insider threats, integration difficulties, and legacy systems. PLC protocols like UMAS, S7Comm, and Optocomm-Forth have exposed vulnerabilities [32] such as user program alteration, configuration breach, and authentication/access control infringement.

Unauthorized access to PLCs poses a significant threat to industrial operations which can be achieved through malware infection, compromised firmware upgrades, and manipulation of communication protocols. Insufficient safeguards against malware, lack of secure firmware updates, and weaknesses in PLC software contribute to the proliferation of harmful code. Vulnerabilities in the supply chain can compromise PLC components, resulting in compromised system integrity. The research [34] on PLC security reveals a complex array of risks and weaknesses within Industrial Automation and Control Systems. The most devastating threat to availability is DoS attacks.

One such example in the recent times is the vulnerabilities present in the Siemens devices. Siemens, a global manufacturer of industrial equipment, has been exposed to a vulnerability in its SIMATIC S7-1500 Programmable Logic Controllers (PLCs) by cybersecurity firm Claroty. The vulnerability allows attackers to extract global private keys, install malicious firmware, and potentially take full control of the devices. Researchers at Claroty and Red Balloon Security have also discovered multiple architectural vulnerabilities in the same PLCs, with over 100+ models susceptible in Siemens due to a cryptography error.

Siemens couldn’t fix it through software patches as the scheme is physically burned onto a dedicated chip. The hardcoded encryption keys could be exploited by nation-state attackers to bypass protection levels and perform sophisticated attacks on industrial devices using these PLCs.

Hence an effective IACS system requires strong defenses against these kind of peripheral and network attacks, timely application of security upgrades, insufficient patch management, and the unwillingness to stop operational operations for upgrades. PLC designers and programmers should focus on security aspects under the supervision of security experts to effectively deal with such potential dangers and weaknesses. To address these threats, a multi-layered approach involving technical controls, robust security policies, testing frameworks, procedures, ongoing monitoring and threat intelligence, and a culture of cybersecurity awareness throughout the organization is necessary.

2.4.3 Consequences of PLC Security Breaches on Operational Safety

It is also important to investigate the interconnection between security and operational safety in these systems. As we begin the second iteration of our security testing methodology designed for PLC-based IACS, this study seeks to comprehend the potential safety implications of security breaches in PLC-based IACS systems. There is a fundamental connection between security and safety in the field of industrial automation [35]. When it comes to PLCs overseeing crucial operations, the incorporation of security and safety measures becomes of utmost importance.

The vulnerabilities in PLC security can directly impact the safety of industrial operations and personnel. Unauthorized entry, alteration of control logic, or harmful code can pose security vulnerabilities and endanger industrial processes. To address these issues, a strong security-safety framework is needed. The research [35] suggests promoting integrated security-safety approaches, customizing risk assessments to incorporate specific security and safety factors. Cross-functional teams are crucial for security-safety efforts.

3 Methodology

The research methodology employed in this thesis is the Design Science Research (DSR) approach, specifically utilizing the Regulative Cycle Approach developed by Wieringa [36], also known as the engineering cycle. This choice of methodology is rooted in the nature of the thesis, which focuses on the development of a security testing framework for IACS systems. DSR is particularly suited for this research endeavour as it emphasizes the creation of innovative artifacts to solve real-world problems. Given the objective of designing a security testing framework, DSR provides a structured and iterative approach to develop, implement, and evaluate this solution.

The Regulative Cycle framework's [37] hierarchical organization further facilitates the implementation of the DSR methodology. Its systematic stages, from problem identification to solution design, testing, and refinement, align closely with the process of creating a security testing framework. Therefore, the adoption of the DSR methodology is a natural fit for this thesis, offering a rigorous and systematic approach to guide the development and evaluation of the proposed security testing framework for PLC-based IACS systems.

3.1 Design Science Approach

DSR is a methodical problem-solving methodology that emphasises combining theory and practice through iterative processes. It distinguishes between practical and knowledge-based challenges, which are complexly interlinked concepts. It involves addressing practical challenges by adjusting in the real world to meet stakeholder objectives. Knowledge-based challenges are addressed by formulating statements known as knowledge questions. The problems are organised in problem-solving cycles, where completing a practical challenge triggers the creation of a knowledge question and answering the question results in a new practical challenge.

Figure 4 illustrates a nested setup where options are evaluated based on the requirements of stakeholders. The criteria for evaluating the knowledge-based challenges are determined by examining them with respect to domain expertise. DSR assumes that developing artifacts like models, prototypes, and implementations while also learning more about real-world issues is the best way to do both. The questions what utility does the new artifact provide, and what demonstrates that utility are central to design science, as stated by Hevner et al. [38]. Artifacts are valuable because of the problems they solve, thus it's important to give thoughtful answers to these inquiries.

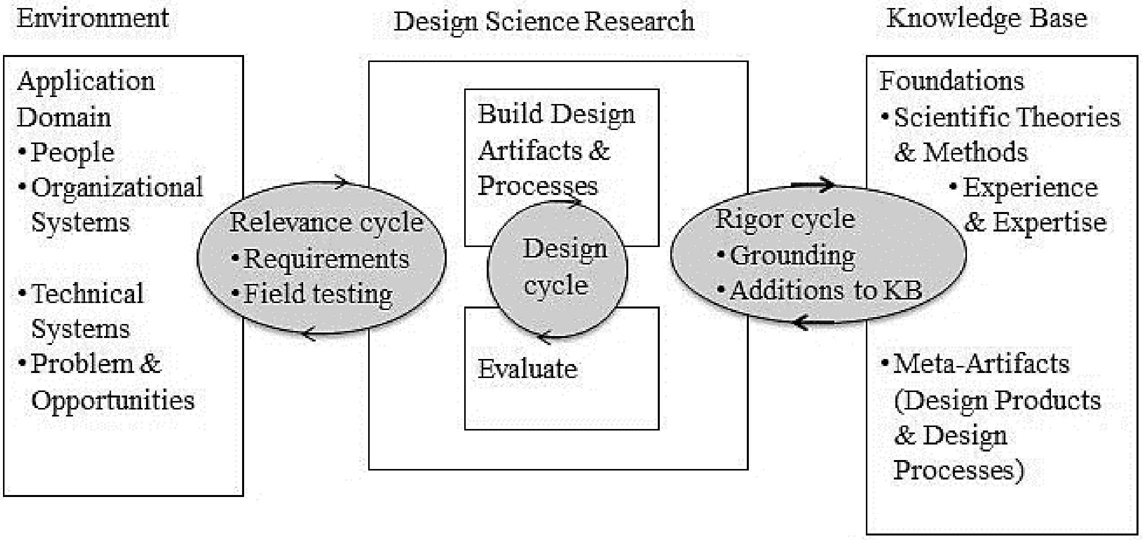


Figure 4: The Three-Cycle View of Design Science Research [39]

A useless artifact is one that has no bearing on the real world. If it doesn't solve a real-world issue, it's useless. Moreover, its claims of contribution are unfounded without adequate investigation. This thesis is a good fit for the Design Science Research approach since the major goal of DSR is to address practical problems, and the security difficulties faced by Konecranes in their crane control systems are inherently practical in nature.

Evaluating a created artifact correctly is crucial for learning from it. In DSR, it is crucial that the artifact shows evidence of innovation by either addressing an unaddressed problem or improving upon an existing solution. It is important for researchers to be able to convey their results to both technical and management audiences while doing design studies. Together, the design science process and the resulting artifact create a context within which researchers may apply a variety of analytical and empirical techniques in an ongoing effort to find workable answers to real-world issues.

3.2 Regulative Cycle Framework

This thesis utilizes Wieringa's regulative cycle paradigm [24], a four-stage framework for problem analysis, practical investigation, design validation, and implementation as shown in Figure 5. The framework is particularly useful in developing a Security Testing framework for ICS, as it provides a methodical and structured approach to solving research problems. The framework includes problem investigation, design, implementation, and evaluation of results, making it an invaluable guide for a systematic and structured approach to problem-solving.

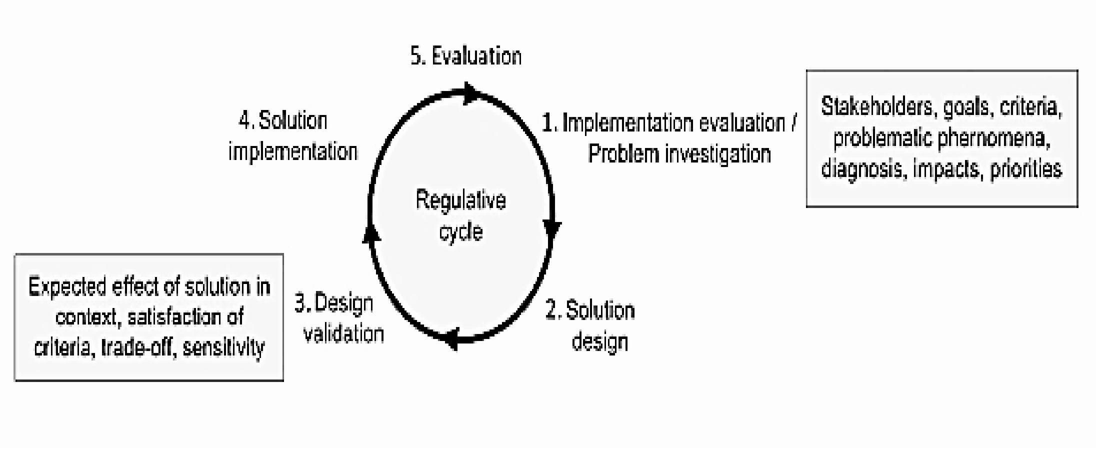

5. Evaluation
4. Solution implementation
1. Implementation evaluation / Problem investigation
Stakeholders, goals, criteria, problematic phernomena, diagnosis, impacts, priorities
Regulative cycle
Expected effect of solution in context, satisfaction of criteria, trade-off, sensitivity
3. Design validation
2. Solution design

Figure 5: Wieringa’s Regulative cycle [40]

3.2.1 Problem Investigation

The problem investigation phase aims to understand an existing issue through analysis and clarification. Four approaches are used: problem-driven, goal-driven, solution-driven, and impact-driven. The problem-driven approach diagnoses the issue, while the solution-driven approach investigates potential solutions using advanced technologies. The problem-driven investigation identifies specific challenges, emphasizing the importance of careful analysis. The security testing framework emphasizes the use of novel tools and approaches to fill gaps, focusing on preventative actions and developing new technologies to strengthen the IACS environment.

3.2.2 Solution Design

During the solution design phase, the objective is to design a plan that lays out the methods and mechanisms that will be used to achieve the goals that have been set by the stakeholders. To accomplish what needs to be done, the phase's conclusion will involve communicating the plan that has been proposed to the various stakeholders. In the current investigation, the problem investigation phase was completed before the solution design phase, and the author's ideas on how to address the identified challenges through a Security testing framework were taken into consideration during that phase.

3.2.3 Design Validation

It is necessary to move on to the design validation phase to validate that the design from the previous phase would bring stakeholders closer to their goals if the design is correctly implemented. During this phase, the following three knowledge questions, which were provided by Wieringa [26], are taken into consideration:

- On Internal validity: If this design were implemented in this problem's context, would it be able to satisfy the criteria that was identified in the investigation of the problem?

- On Trade-offs: How would the criteria be satisfied if slightly different designs were implemented in this context?

- On External validity, also known as sensitivity analysis: If this design were implemented in somewhat different contexts, would it still be able to satisfy the criteria?

3.2.4 Implementation

During this phase, the solutions that have previously been designed and validated are now put into action. The designed solution serves as a guide for determining the components that make up an implementation. It could be an early prototype, a finished software solution, or even just the testing of the system itself. During the implementation phase of this project, the security testing framework has been illustrated on each of IT and OT asset at the end of every iteration.

3.2.5 Evaluation

The Wieringa's regulative cycle framework, despite not having an official evaluation phase, was included in this study as it serves as a foundation for a new regulatory cycle. The evaluation process involved various stakeholders, using the Design Science methodology. The design phase involved literature review, stakeholder validation, implementation, and evaluation. The iterative approach ensured systematic refinement and enhancement of the framework, illustrating examples from both IT and OT domains within the IACS environment.

3.3 Data Collection Methods

A combination of focused group discussions with industry experts, an exhaustive review of security standards and frameworks, and a thorough analysis of research papers and scholarly articles were used as methods for collecting data. The research has been framed around a period of 7 months. There are three focus groups considered throughout the research. The focus group FG 1 constitutes PLC development engineers and security architects from the industry and the focus group FG2 includes members of FG 1 along with the safety experts who can provide their inputs on the Safety- Security choke points and the focus group FG 3 comprised of members of FG 1 along with the IEC 62443 standard experts to assist on the integration of framework to the standard. Each iteration has been mapped to the respective research question and a corresponding objective. At the end of each iteration, there is an artifact that is already available as shown in the Figure 6.

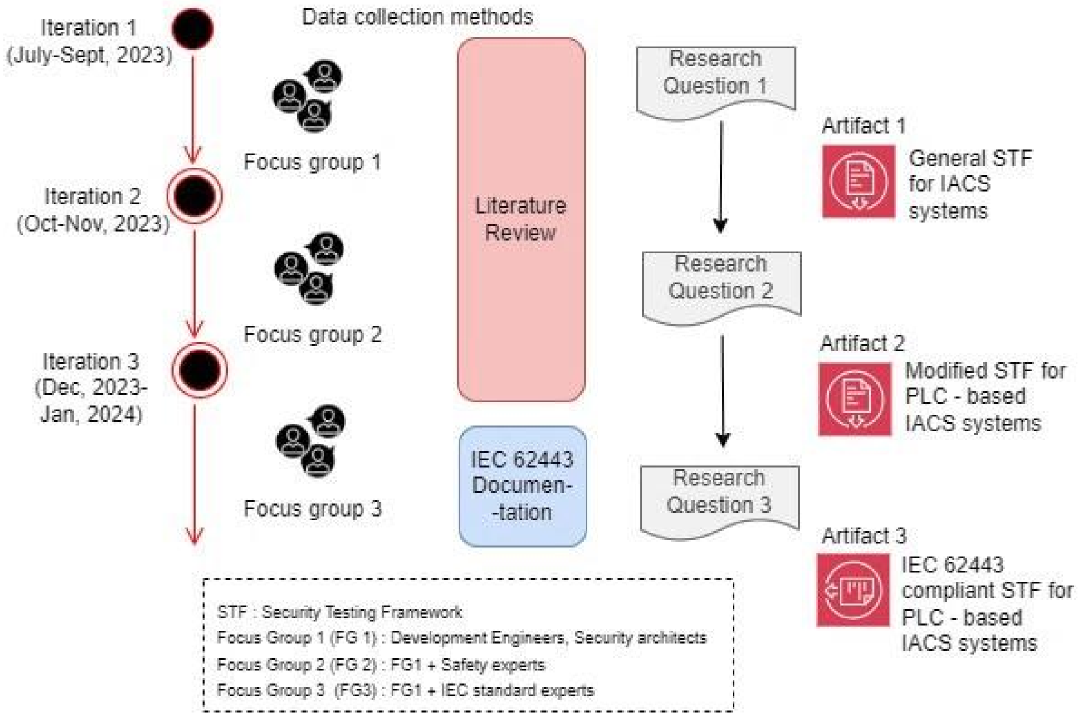

Iteration 1
(July-Sept, 2023)
Iteration 2
(Oct-Nov, 2023)
Iteration 3
(Dec, 2023-
Jan, 2024)
Data collection methods
Focus group 1
Focus group 2
Focus group 3
Literature Review
IEC 62443 Documen- -tation
Research Question 1
Research Question 2
Research Question 3
Artifact 1
General STF for IACS systems
Artifact 2
Modified STF for PLC - based IACS systems
Artifact 3
IEC 62443 compliant STF for PLC - based IACS systems
STF : Security Testing Framework
Focus Group 1 (FG 1) : Development Engineers, Security architects
Focus Group 2 (FG 2) : FG1 + Safety experts
Focus Group 3 (FG3) : FG1 + IEC standard experts

Figure 6: Data Collection Methods and Artifacts through each Iteration

3.3.1 Research Papers

Research papers and academic articles from various sources (as mentioned in Table 3), were meticulously reviewed to facilitate an exploration of the most recent advancements and emerging trends in IACS security testing. The literature review has been conducted in detail for forming a strong background for the work throughout the first two iterations. This enabled the development of a comprehensive and well-rounded security testing framework for IACS, which was then informed by the findings of this exploration. Network architecture of the PLC-based crane control system and cyber security documents of the crane control systems were also used to collect existing security posture about the crane control systems.

3.3.2 Focus Group Discussions

As an integral component of the Evaluation phase within the DSR methodology, focus group discussions were conducted to facilitate proper communication with stakeholders and to evaluate artifacts developed throughout each iteration. Given the qualitative nature of this study, focus group discussions emerged as a suitable method for gathering tool requirements.

In total, approximately 20 participants were involved in these discussions, organized into three distinct focus groups, as illustrated in the accompanying figure. Each discussion session was allotted a duration of approximately 2 hours, with numerous sessions convened with selected groups deemed pertinent to the study's objectives. While the exact number of questions posed during each session was not fixed, it varied depending on the dynamics and depth of the discussion. This iterative engagement approach allowed for comprehensive exploration of stakeholder perspectives and ensured thorough gathering of tool requirements essential for the advancement of the research.

Furthermore, the discussions provided an effective way to get insights into the opinions and thoughts of the various stakeholders about the framework implementation at the end of every iteration. The general security testing framework for IACS systems was evaluated by presenting it to security architects and engineers. For instance, the framework after each iteration was discussed, about the development of separate iterations for IT and OT.

The security specialists recommended an integrated methodology with domain-specific security testing strategies and an external Incident Response section to strengthen the framework. The difficulty in integrating a standardized framework across various IACS applications sparked discussions on practical implementation. The trajectory of the work was also deliberated, focusing on optimizing the framework for future iterations and addressing the requirements of PLC-based crane control systems. To ensure seamless integration, domain-specific modifications to the generic security testing paradigm were emphasized. The discussions were based on the framework synthesis and demonstrations in which the basic phases were presented, after which some fixed questions were asked from the participants. The sessions were recorded whenever necessary to revisit them.

3.3.3 The EU Journals on Various Regulations

For the study of various EU regulations, their deadlines, the key points, and implementation strategies were collected from the official EU journals, which has provided insights into how important it is to have a security testing framework for any organisation to be in place to meet the large number of regulations coming up in the next few years. The Table 3 lists the information sources used throughout the thesis:

Table 3: Major Information Sources

Information Source	Weblink
IEEE Xplore	https://ieeexplore.ieee.org/Xplore/
ACM Digital Library	https://dl.acm.org/
Springer	https://www.springerlink.com/
Academia	https://www.academia.edu/
ResearchGate	https://www.researchgate.net/
Science Direct	https://www.sciencedirect.com/
Finnish Standards Association	https://www.sfs.fi/
European Union	https://european-union.europa.eu

3.3.4 Research Validity

The thesis's construct validity is established through a thorough review of literature sources and the synthesis of a comprehensive security testing framework. The framework is structured and aligned with best practices and methodologies, ensuring robust and well-grounded construct validity. The internal validity of the research is strengthened through the iterative design process and adherence to design science research methodology. The framework's external validity is enhanced by considering the wider applicability and relevance of the proposed methodologies and tools to various IACS environments. The framework can be generalized across various IACS settings and addresses security concerns beyond the scope of the initial research. This ensures the framework's reliability and applicability across various IACS environments.

4 Iterations

In this chapter, the development process of the Security Testing Framework is described in iterations in the context of the regulative cycle framework.

4.1 Iteration 1 (Security Testing best practices)

The first iteration aims to synthesise a security testing framework that could cover most of the important phases of the general security testing framework for IACS systems gathered from the literature review of various security testing frameworks for Industrial security. The framework architecture has been designed carefully as a flow diagram that can be modified and finetuned with further iterations.

4.1.1 Problem Investigation

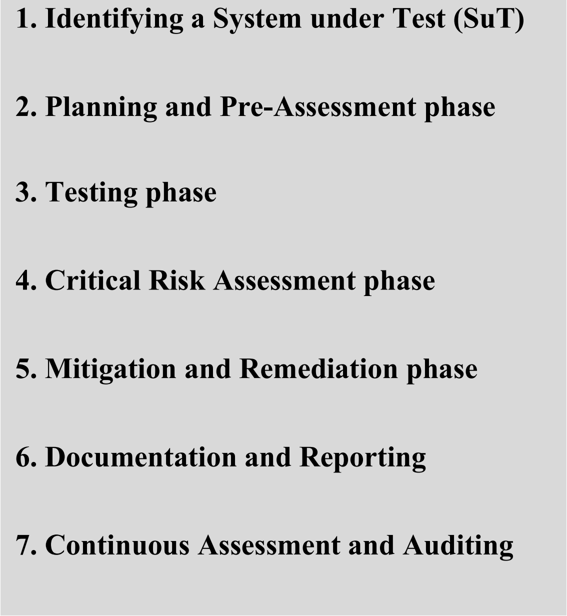
Konecranes recognized the need for a security testing framework to secure the crane core platform, especially considering mandatory EU regulations and the growing importance of security compliance. The focus is on improving the overall security posture of any IACS systems through several stages, with literature supporting each step and recommendations for the end user to achieve desired system security. The framework would provide a comprehensive security testing procedure tailored to the organization, allowing reusability of processes and tools while adhering to various EU regulations. The first step involved researching the issue and reviewing existing security testing literature

To design a Security Testing Framework tailored to IACS systems, the following research gaps were identified based on the existing literature and collaboration with the company's security specialists. It was observed that a very few frameworks can be customized for specific IACS needs, and the literature only provides a limited glimpse into the process of developing a comprehensive framework. The research identified several problems in the field of security of IACS systems [41, 42], including the lack of comprehensive security framework, standardized security measures within IACS, the evolving threat landscape in OT, legacy systems, comprehensive risk assessment procedures, basic security controls in many IACS systems, and inconsistent adherence to industry-specific standards and regulations. These gaps highlight significant challenges in addressing operational integrity and security and stress for having a comprehensive security testing framework equipped with real-time threat intelligence capabilities for organizations to successfully protect their IACS assets from potential cyber-attacks.

4.1.2 Solution Design

To address the above challenges in the IACS security, this iteration aimed to consolidate various literary sources to develop a comprehensive framework. In the process of synthesizing the framework for the solution design in Iteration 1, we began by investigating into the realm of IACS literature. This initial step allowed us to gain a comprehensive understanding of the critical components that constitute IACS systems.

Through an extensive review of existing literature [42-53], we identified the fundamental elements of the security testing framework for IACS systems as depicted in Figure 7. It was clear that the framework should include multiple phases to achieve a comprehensive security posture. The literature supports each phase, and recommendations are provided for stakeholders to choose the appropriate methodologies, tools, and techniques for effective security measures. The proposed security testing framework has been divided into the seven major phases as shown in Figure 7.



1. Identifying a System under Test (SuT)

2. Planning and Pre-Assessment phase

3. Testing phase

4. Critical Risk Assessment phase

5. Mitigation and Remediation phase

6. Documentation and Reporting

7. Continuous Assessment and Auditing

Figure 7: Phases of the Framework

System under Test (SuT) is a crucial component of any IACS system. It involves the selection of hardware, software, and network infrastructure that are essential for controlling and managing industrial processes. The Planning and Pre-Assessment Phase [54] involves critical activities such as Asset Discovery [55], Asset Identification, Asset Classification, Threat Modelling, Initial Risk Assessment, and Security Testing. The Threat Modelling Phase helps identify and assess potential threats using methodologies like STRIDE, DREAD, or PASTA [56-59]. The Initial Risk Assessment Phase evaluates identified risks based on severity and develops a robust risk response plan [60]. The Planning and Pre-Assessment Phase also sets the scope and objectives for security testing efforts.

The Comprehensive Security Testing Phase [44] is divided into four categories: Overall System Security Testing that includes Security Compliance Testing, Performance and Load Testing. IT-specific tests include Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), network vulnerability scanning, and configuration testing. OT-specific tests focus on process-specific vulnerability testing, firmware integrity checks, functional testing of critical processes, and operational testing under varying environmental conditions.

Common Testing for Both IT and OT ensures a holistic approach to security testing. The Critical Risk Assessment Phase is crucial in systematically assessing and managing risks within the SuT. This includes risk identification and classification, evaluation of risk exposure, impact analysis, prioritization of threats, assessment of existing security controls, calculation of residual risks, formulation of risk treatment strategies, and ongoing monitoring and review of risks.

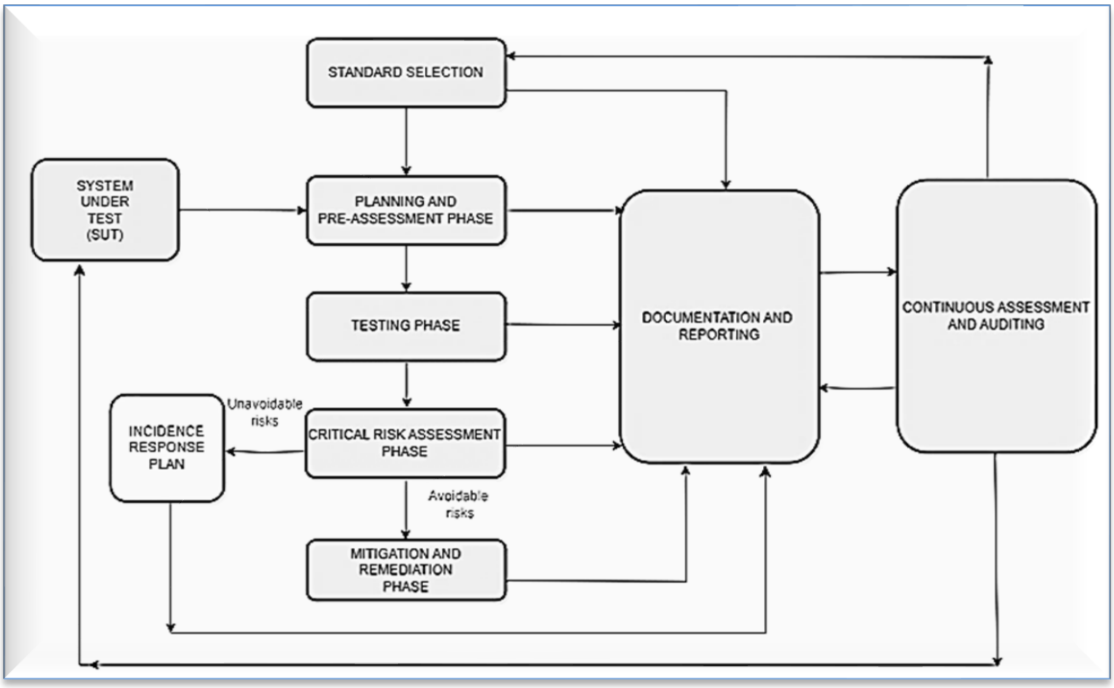

STANDARD SELECTION
SYSTEM UNDER TEST (SUT)
PLANNING AND PRE-ASSESSMENT PHASE
TESTING PHASE
DOCUMENTATION AND REPORTING
CONTINUOUS ASSESSMENT AND AUDITING
INCIDENCE RESPONSE PLAN
Unavoidable risks
CRITICAL RISK ASSESSMENT PHASE
Avoidable risks
MITIGATION AND REMEDIATION PHASE

Figure 8: Security Testing Framework for IACS systems

4.1.3 Design Validation

The Wieringa-proposed validation questions [61] were considered at this stage:

On Internal validity: Would this design, if applied to this problem context, meet the requirements stated in the problem investigation.

This evaluation of a security testing framework for IACS systems aims to determine if it meets the requirements outlined in the problem investigation. Iteration 1's design aligns with the primary objective of a structured, systematic, and comprehensive approach to assessing and enhancing the security posture of IACS systems. The framework includes critical phases such as Asset Discovery, Threat Modelling, Initial Risk Assessment, and Comprehensive Security Testing. Asset Discovery ensures meticulous identification and cataloging of hardware, software, and network infrastructure components within the System under Test (SuT), while Threat Modelling allows for a thorough examination and assessment of potential threats.

Initial Risk Assessment categorizes and evaluates risks based on severity, ensuring a robust risk response plan. Comprehensive Security Testing, segmented into IT-specific assets, OT-specific assets, and common testing for both domains, ensures a comprehensive examination of the SuT, addressing the multifaceted challenges posed by IACS. This framework provides a structured, systematic, and comprehensive security testing framework, drawing insights from literature and aligning with the objectives outlined in the investigation.

On Compromise: In what ways may somewhat altered designs, when applied here, nonetheless meet the requirements?

The security testing framework for IACS systems can be altered to meet the requirements outlined in the problem investigation. These adaptations include tailoring phases like Asset Discovery and Threat Modelling to suit the unique components and threat landscapes of diverse IACS environments. This allows for a targeted and effective approach to security testing. Flexible risk assessment approaches can be introduced to accommodate varying risk tolerances and priorities across different IACS systems.

The Comprehensive Security Testing Phase, designed as a modular framework, offers flexibility to customize testing modules based on individual IACS setup characteristics, ensuring scalability and resource efficiency. Additionally, adaptations can focus on incorporating specific modules or phases tailored to meet evolving regulatory requirements within the IACS domain. By ensuring compliance with industry standards and regulations, the altered designs of the security testing framework continue to enhance the security posture of IACS and meet the regulatory requirements outlined in the problem investigation.

On External Validity: Would this design still be acceptable if applied in somewhat different settings?

The security testing framework for IACS systems is a structured and systematic approach that can be applied in various settings. Iteration 1 of the framework offers key phases such as Asset Discovery, Threat Modelling, Risk Assessment, and Comprehensive Security Testing. The framework's adaptability is crucial when applied to diverse industrial environments with unique configurations. The modularity of the Comprehensive Security Testing Phase allows for customization of testing modules based on each IACS setup, ensuring its effectiveness across different settings.

Alterations to the design, such as tailoring the Threat Modelling Phase to address specific threats prevalent in different IACS contexts, enhance its acceptability in varied settings. The flexibility of risk assessment approaches allows adaptation to varying risk tolerances and priorities across different IACS systems, ensuring its relevance and effectiveness beyond its initial context. In conclusion, the security testing framework for IACS demonstrates potential acceptability in various settings within the IACS domain.

4.1.4 Implementation

The implementation part of the security testing framework for IACS systems was structured to offer a clear roadmap for organizations seeking to enhance their security posture. A comprehensive list of frameworks, tools, and techniques (Table 4) tailored to each phase of the framework has been provided.

Table 4: List of framework tools and techniques [54]

Phase	Framework /Models	Tools/ Platforms
Selecting SUT	Purdue model, IEC 62443 Standard, Zachman's framework	
Asset Identification	SCADA Security Architect (SSA) framework, ISA/IEC 62443 standard	Nessus, Shodan, IndustrialDefender platform
Asset discovery and management	Nozomi framework, At &T security tools, Applied risk tool	Axonius, Scrutiny, Claroty, Shodan,
Threat modelling	STRIDE, PASTA, DREAD, VAST,OCTAVE	MS threat modeling tool, OWASP Threat Dragon, Irius Risk tool, Threat modeler, ABB for ICS, PAS Cyber Integrity, and Kaspersky Industrial Cybersecurity
Initial Risk Assessment	OCTAVE Allegro, FAIR, NIST SP 800-30 Risk assessment software like TARA, and RiskWatch	Microsoft Security Risk Assessment Tool, OpenFAIR, Splunk, IBM QRadar, and ArcSigh, Nessus
Vulnerability scan	InsightVM	Nessus,OpenVAS, Qualys VMDR, RAPID7, BlackDuck
Penetration testing	Metasploit framework	BurpSuite, Wireshark, OWASP ZAP
SAST tools	Automated static test frameworks	Checkmarx, Fortify Static Code Analyzer, Veracode, SIGRID, SonarQube
DAST tools		Burpsuite, NetSparker, OWASP ZAP, Acunetix, WebInspect
Configuration testing		Tripwire, ManageEngine, Nipper, or Firemon.
End-point security testing		Cisco AnyConnect, Symantec Endpoint Protection, McAfee Endpoint Security, or CylancePROTECT
Incidence Response readiness testing	testing software: FireEye Helix, Splunk, IBM Resilient, D3 Security.	
Data Security testing	S/W	Digital Gaurdian, Varonis platform

This approach bridges the gap between abstract concepts outlined in the framework and practical actions that security teams can take to secure their IACS environments effectively. This ensures that security teams have a well-rounded set of options to choose from, aligning with the structured approach set forth in the framework.

Moreover, the inclusion of a range of tools such as Nessus, Metasploit, Wireshark, and compliance standards like NIST SP 800-30 and ISO/IEC 27005, provides practical guidance for security practitioners. These tangible resources empower organizations to make informed decisions and implement robust security measures within their IACS environments. This structured approach to the implementation part not only offers clarity and guidance but also enables the translation of theoretical concepts into actionable steps for securing critical industrial systems.

4.1.5 Evaluation

In the evaluation section of our security testing framework for IACS systems, we adopt an iterative approach to systematically refine and enhance the framework. The evaluation process is conducted by illustrating examples from both IT and OT domains within the IACS environment, ensuring a comprehensive assessment. Given the delicate nature of OT environments, caution is paramount when evaluating the framework in a real-world system. There is a potential risk that applying the framework could disrupt the industrial environment and compromise system availability. To mitigate these risks, a prudent and phased approach has been adopted.

This approach allows for careful validation of the framework's applicability and effectiveness, ensuring that any potential risks to the industrial environment are minimized. Furthermore, the general security testing framework undergoes initial validation by the security experts. Following this, attempts are made to illustrate the framework on selected assets, one from the IT domain and one from the OT domain respectively. This hands-on demonstration serves to showcase how the framework can provide comprehensive security for an IACS system while also ensuring that any adjustments or enhancements.

The security testing framework for the IACS system involves identifying and classifying IT asset (IDE) and OT asset (PLC controller) components based on their criticality within the industrial control framework. The Pre-Assessment phase helps identify and classify these assets, followed by the threat modeling phase to analyze potential vulnerabilities and security gaps. Specialized software like Microsoft Threat Modelling Tool and LINDUN are used for IT asset and OT asset analysis. We can prioritize IT asset (SQL injection) and OT asset (default password) vulnerabilities by mapping out potential attack vectors and employing methodologies like DREAD and STRIDE.

Initial risk assessment helps prioritize critical vulnerabilities, facilitating quantification of risks and developing appropriate response strategies. Secondary testing phases for IT and OT assets provide a thorough assessment of vulnerabilities . SAST and DAST tools are used to detect and mitigate SQL injection risks, enhancing the reliability and security of the IDE. The framework can also analyze the IDE's codebase and behavior using tools like Checkmarx and Acunetix. Process-specific vulnerability testing and firmware integrity checks are conducted for the PLC controller, eliminating the risk posed by default passwords. This comprehensive security evaluation ensures the safety and reliability of the IACS system.

These strategies can be used during the security testing phase. The next step is a thorough detailed risk assessment, where factors like attack surface, potential exploits, residual risks, and mitigation strategies are considered. The framework combines threat modeling, risk assessment, and comprehensive security testing to ensure the highest level of security in ICS systems. It provides a comprehensive assessment of IT and OT assets, improving the security posture and efficiently addressing identified vulnerabilities. The framework's application not only enhances individual components' security but also contributes to the overall fortification of the IACS system, ensuring resistance to potential cyber threats and vulnerabilities. The evaluation involved presenting the framework to security architects and engineers, who were given predetermined questions to gain perspective and identify areas for enhancement. The responses were generally positive and helpful.

A discussion was held regarding the potential need for two versions of the framework, one for IT and one for OT, due to the differing priorities observed in each domain. The security experts advised adopting an integrated methodology for the framework, with a thorough emphasis on tailoring security testing strategies for each specific domain, in addition to incorporating common tests. An additional suggestion entails the inclusion of an external Incident Response section that provides a comprehensive overview of recent attacks and incidents, along with a proposed management strategy for handling such occurrences.

Both recommendations were deemed highly valuable in the further iteration of the comprehensive security framework. Since Konecranes is interested into security testing of its

PLC- based crane control systems, the following knowledge question was raised in the session: " To what extent these practices are adapted to the PLC-based (crane) control systems? ". The feedback from the session was directly transferred as an input to the start of Iteration 2.

4.2 Iteration 2 (Security considerations of PLC-based IACS systems)

The Iteration 2 aims to refine and tailor the existing security testing framework to address the unique security considerations of PLC-based IACS systems. PLCs are crucial for control systems, governing industrial processes and critical infrastructure. Ensuring the security of PLC-based IACS systems is hence essential to protect operational safety, system integrity, and reliability. This problem statement lays the groundwork for developing a specialized security testing approach that aligns with PLC-based control systems, strengthening the overall security posture in industrial environments.

4.2.1 Problem Investigation

The primary focus is on applying the framework to the realm of PLC-based control systems. These systems, integral to the functioning of industrial processes, introduce a layer of complexity due to their intricate network of controllers, sensors, actuators, and communication protocols. The complexity inherent in PLC-based systems presents a significant challenge in ensuring their security resilience, requiring a tailored approach to address their unique vulnerabilities and threats [62] .

One of the central concerns in this iteration lies in the vulnerabilities prevalent in PLCs, which are often interconnected with various devices and networks. This interconnectedness exposes PLCs to a range of cyber threats, including unauthorized access, malware injection, and data manipulation. The potential impact of security breaches in PLC-based control systems cannot be understated, as such incidents can lead to production downtime, financial losses, and even safety hazards for workers and the surrounding environment. This underscores the critical need for robust security measures to safeguard the integrity, availability, and confidentiality of industrial processes reliant on PLCs.

Furthermore, the compliance landscape adds another layer of complexity, with industries operating PLC-based control systems mandated to adhere to stringent regulatory standards such as the IEC 62443 series, NIST SP 800-82, and ISO/IEC 27001. Compliance with these standards is not only a legal requirement but also crucial for maintaining trust and credibility in the industry. However, the existing gap in tailored security frameworks specifically designed for PLCs highlights the need for a comprehensive security testing framework in this iteration. This framework should be meticulously crafted to encompass asset discovery, threat modeling, risk assessment, and security testing methodologies, ensuring a holistic approach to addressing the security challenges unique to PLC-based control systems.

4.2.2 Solution Design

In response to the challenges posed by PLC based IACS, Iteration 2 focuses on refining the existing general security testing framework. Here are the major modifications and enhancements to the security testing framework for PLC-based IACS systems in Iteration 2:

4.2.2.1 Secure Communication Protocols for PLCs

Framework Phase: To be placed within the "Comprehensive Security Testing Phase" of the framework. After the "Initial Risk Assessment Phase" and before the "Critical Risk Assessment Phase".

Description: Secure communication protocols are crucial for maintaining data integrity, confidentiality, and authenticity in IACS systems, particularly for the PLCs. The introduction of protocols like OPC UA (Open Platform Communications Unified Architecture) and MQTT (Message Queuing Telemetry Transport) in Iteration 2 enhances the security testing framework. These protocols offer robust mechanisms to ensure data exchange between PLCs and connected devices remains secure throughout transmission.

They address various security concerns within IACS environments, ensuring data integrity, reliability, and accuracy of industrial processes. The framework provides guidelines and best practices for implementing OPC UA or MQTT within the PLC environment, including built-in security features like encryption, authentication, and data integrity checks. MQTT offers a lightweight and efficient communication method with support for Transport Layer Security (TLS) encryption. Validation methodologies are included to ensure the correct and secure implementation of these protocols.

Incorporating secure communication protocols into the framework significantly enhances the overall security posture of the IACS system, reducing the risk of data breaches, unauthorized access, or tampering. It also facilitates compliance with industry standards and regulations, as many mandates require secure communication protocols in industrial environments. Adopting best practices like OPC UA or MQTT ensures the confidentiality, integrity, and availability of critical industrial data, safeguarding operations against potential cyber threats.

4.2.2.2 Hardening PLC Firmware and Software

Framework Phase: To be placed within the "Comprehensive Security Testing Phase" and after the "Secure Communication Protocols for PLCs" phase and before the "Critical Risk Assessment Phase".

Description: The "Hardening PLC Firmware and Software" phase is a crucial part of the security testing framework for PLC-based IACS systems in Iteration 2. It aims to strengthen the security of PLCs by reducing vulnerabilities and enhancing resilience against cyber threats [24]. The framework introduces best practices for implementing security measures, such as the principle of least privilege, which limits the potential attack surface and minimizes the risk of unauthorized access to critical PLC functions. Key activities in this phase include identifying and disabling unnecessary services or protocols, regular firmware updates and patch management, and configuring secure default settings on PLCs.

Vulnerability scanning tools and penetration testing validate the effectiveness of these measures, while regular security audits and checks against established security baselines ensure PLCs are hardened against potential cyber threats. Therefore, this phase provides a systematic approach to strengthening the security posture of PLC-based IACS systems. By implementing security best practices, disabling unnecessary services, updating firmware, and configuring secure settings, organizations can mitigate risks, enhance resilience, and ensure the secure operation of their industrial processes.

4.2.2.3 Safety-Security Choke Points assessment

Framework Phase: As an input to the SuT identification and Planning and Pre-Assessment phase [63] ensures that these critical considerations are integrated into the early stages of the framework.

Description: This phase can be a crucial part of the security testing framework for PLC-based IACS systems. It focuses on identifying and assessing the intersections between safety and security measures within the IACS environment, particularly at critical points where compromises in security could potentially impact operational safety. Choke points are areas within the IACS where actions taken to enhance security may inadvertently impact safety, and vice versa. The framework emphasizes the need to evaluate these choke points to understand the potential risks they pose to the overall system.

By identifying these choke points, organizations can develop strategies to effectively manage and mitigate associated risks, including implementing safeguards and countermeasures to ensure security enhancements do not compromise the safety and integrity of industrial operations. The integration of risk assessment methodologies that consider both safety and security aspects is a key aspect of this phase [65]. Clear communication channels and protocols for reporting and responding to safety-security incidents are recommended to minimize the impact on industrial processes and personnel safety.

4.2.2.4 Secure Remote Access Management for PLCs

Framework Phase: This modification should be placed within the "Testing Phase" of the framework. After the "Initial Risk Assessment Phase" and before the "Critical Risk Assessment."

Description: The "Secure Remote Access Management for PLCs" phase of a framework aims to enhance the security of PLC-based IACS systems by addressing challenges related to remote access. The framework introduces guidelines for implementing Virtual Private Networks (VPNs) to ensure data confidentiality and protection from potential eavesdropping or interception. It emphasizes selecting VPN protocols that align with industry best practices and offer robust encryption standards to safeguard sensitive information [50]. Multi-Factor Authentication (MFA) mechanisms are introduced to bolster the authentication process for remote users, with detailed guidelines on configuring and managing MFA systems. Role-based access control (RBAC) policies define granular permissions and privileges for different user roles, ensuring access only to PLC functions and data necessary for their specific tasks.

Continuous monitoring and logging of remote access activities are also included, with regular audits and compliance checks recommended to ensure the remote access infrastructure remains aligned with industry standards and regulatory requirements. By implementing robust logging mechanisms, organizations can track and analyze remote access events, enabling timely detection and response to suspicious or unauthorized activities. Overall, the "Secure Remote Access Management for PLCs" phase offers a comprehensive approach to strengthening the security posture of PLC-based IACS systems.

4.2.2.5 Continuous Monitoring and Intrusion Detection for PLC Networks

Framework Phase: To be placed within the "Continuous Assessment and Auditing Phase" and after the "Incident Response Management Phase" and before the "Documentation and Reporting Phase".

Description: The "Continuous Monitoring and Intrusion Detection for PLC Networks" phase is a crucial part of the security testing framework for PLC-based IACS systems. It involves monitoring network traffic to detect potential security threats or anomalies. Real-time data packet analysis tools are used to detect abnormal or unauthorized activities, such as unusual data transfers or unauthorized access attempts. Intrusion Detection Systems (IDS) are deployed to automatically identify and alert on potential security breaches [67]. The framework also includes methodologies for detecting anomalies and deviations from normal network behavior, enabling organizations to respond promptly to potential threats and safeguard their critical industrial processes [68]. Configuration guidelines for IDS solutions tailored to PLC environments are available.

The security testing framework for PLC-based IACS environments can be improved by incorporating these major modifications. These changes aim to strengthen the overall security posture, mitigate risks, and ensure the reliable operation of PLC-based control systems in industrial settings. By strategically placing these modifications within the framework, organizations can establish a comprehensive and layered approach to securing their PLC-based IACS systems [69, 70]. The Security Critical Components focus on PLCs, communication modules, and associated software, with a focus on compliance with industry standards, particularly IEC 62443 and IEC 61508, to guide and validate the security measures implemented.

4.2.3 Design Validation

In the second iteration of the Design Validation phase, the framework underwent rigorous evaluation using Wieringa's validation questions and validation from the experts of Focussed Group (FG) 2. This systematic approach aimed to assess the framework's resilience and effectiveness in addressing the security challenges of PLC-based systems. The Wieringa [61] proposed validation questions considered at this stage:

On Internal Validity: Would this design, if applied to this problem context, meet the requirements stated in the problem investigation?

In evaluating the internal validity of the design for Iteration 2, it is crucial to assess its alignment with the identified problem context and requirements. The modifications introduced, such as the inclusion of secure communication protocols, hardening of PLC firmware and software, evaluation of safety-security choke points, secure remote access management, and continuous monitoring with intrusion detection, directly address the identified challenges in securing PLC-based IACS systems.

The design, if implemented, would meet the requirements stated in the problem investigation by providing a comprehensive and layered approach to security testing. By integrating these modifications into the framework, organizations can proactively mitigate potential vulnerabilities, unauthorized access, and cyber threats to the IACS environment. This ensures the integrity, confidentiality, and availability of critical industrial processes while aligning with the overarching goal of enhancing cybersecurity in PLC-based systems.

On Compromise: In what ways may somewhat altered designs, when applied here, nonetheless meet the requirements?

Somewhat altered designs within the framework for Iteration 2 would still meet the requirements by maintaining the core principles of enhanced security, safety, and compliance. For instance, if certain modifications are adjusted or expanded based on specific organizational needs or industry regulations, the framework remains adaptable and flexible. For example, organizations may choose to prioritize certain security measures over others based on their risk assessment, without compromising the overall effectiveness of the framework.

This allows for customization while ensuring that essential aspects such as secure communication, remote access management, and continuous monitoring with intrusion detection remain intact. Additionally, alterations to the design could involve the integration of additional security tools or technologies that better suit the organization's infrastructure or operational requirements. Despite these alterations, the framework retains its focus on strengthening the security posture of PLC-based IACS systems, thereby meeting the fundamental requirements of the problem investigation.

On External Validity: Would this design still be acceptable if applied in somewhat different settings?

The design for Iteration 2 maintains a level of generalizability that allows for its application in somewhat different settings beyond the specific context of the problem investigation. The modifications introduced, such as secure communication protocols, remote access management, and continuous monitoring with intrusion detection, are foundational principles of industrial cybersecurity. Thus, when applied in diverse industrial settings or sectors, the design remains acceptable and effective in enhancing the security of PLC-based IACS systems.

Whether in manufacturing, energy, transportation, or other critical infrastructure sectors, the framework provides a structured and adaptable approach to address common cybersecurity challenges. Moreover, the framework's emphasis on continuous assessment, risk mitigation, and compliance aligns with industry best practices and regulatory requirements across various sectors. This ensures that organizations can leverage the framework to enhance the security of their PLC-based IACS systems while adapting to different operational environments and industry-specific needs.

The framework is also subjected to scrutiny and feedback from IACS security experts (FG 2). These experts, with their domain-specific knowledge and experience, provided invaluable insights into the practicality and relevance of the adapted framework. Their feedback ensures that the framework remains robust and applicable in real-world scenarios, aligning with industry standards and best practices. By addressing these three questions posed by Wieringa and the expert recommendations, the design validation for Iteration 2 confirms the effectiveness, flexibility, and applicability of the security testing framework for PLC-based IACS systems.

4.2.4 Implementation

The implementation phase of Iteration 2 of the security testing framework for PLC-based IACS systems aims to provide a structured roadmap for organizations to enhance their cybersecurity posture effectively. Building upon the refined framework from Iteration 1, this iteration introduces significant modifications to address the specific challenges of PLC-based systems. A comprehensive toolkit of frameworks, tools, and techniques and implementation steps (Tables 5, 6, 7, 8, 9, 10) has been curated for each phase of the refined framework (Table 5), ensuring a practical and actionable approach to securing PLC-based IACS environments. This approach bridges the gap between theoretical concepts and tangible security measures, offering clear guidance for security teams.

Table 5: Secure Communication Protocols for PLCs

Implementation steps
- Identifying and selection of secure communication protocols such as OPC UA or MQTT.
- Configuring PLC communication channels to ensure encryption, authentication, and data integrity.
- Integrating testing methodologies to validate the effectiveness of the selected protocols.
- Deploying tools such as Wireshark for packet analysis and protocol testing.

Table 6: Hardening PLC Firmware and Software

Implementation steps
- Conducting vulnerability assessments to identify weaknesses in PLC firmware and software.
- Applying security patches and updates to mitigate known vulnerabilities.
- Disabling unnecessary services and ports to reduce the attack surface.
- Configuring secure default settings and access controls for PLCs.

Table 7: Evaluation of Safety-Security Choke Points

Implementation Steps
- Analysing potential intersections between safety and security.
- Identifying critical choke points where safety and security requirements converge.
- Developing strategies to mitigate risks without compromising safety or security.
- Integrating safety protocols and mechanisms

Table 8: Secure Remote Access Management for PLCs

Implementation Steps
- Implementing secure remote access tools such as VPNs and remote desktop protocols.
- Configuring role-based access controls (RBAC) to manage user permissions.
- Deploying multi-factor authentication (MFA) for enhanced access security.
- Conducting testing scenarios to validate the effectiveness of remote access controls.

Table 9: Continuous Monitoring and Intrusion Detection for PLC Networks

Implementation Steps
- Deploying network traffic monitoring tools to capture and analyze data packets.
- Implementing Intrusion Detection Systems (IDS) to detect and alert on suspicious activities.
- Configuring anomaly detection algorithms to identify deviations from normal network behavior.
- Integrating of SIEM (Security Information and Event Management) solutions for centralized monitoring.

This structured approach to implementation empowers organizations with a diverse toolkit of resources tailored to the specific security needs of PLC-based IACS systems. By delineating clear steps and providing practical guidance through the integration of tools such as Nessus, Metasploit, Wireshark, and compliance standards like NIST SP 800-30 and ISO/IEC 27005, organizations can make informed decisions and implement robust security measures.

The refined framework in Iteration 2 not only offers clarity and guidance but also enables the translation of theoretical concepts into actionable steps for securing critical industrial systems. Through this approach, organizations can effectively enhance the security posture of their PLC-based IACS environments while mitigating potential cyber threats and vulnerabilities of IACS in the face of evolving cyber threats and potential safety risks.

4.2.5 Evaluation

Evaluation is about the illustration of the framework and how each phase addresses the security needs of the IT (Siemens TIA Portal) and OT (Siemens S7 1500 PLC) assets within the system. The Siemens TIA Portal serves as the primary engineering software, while the S7 1500 PLC is a core component in industrial crane control processes. This initial step lays the groundwork for targeted security assessments and measures tailored to these specific assets. In the Planning and Pre-Assessment Phase, the modified framework includes the identification of potential threats and vulnerabilities specific to the Siemens TIA Portal and S7 1500 PLC. The threats are identified, assessed, and classified evaluation of risks associated with unauthorized access to the TIA Portal and potential vulnerabilities in the PLC firmware. The modification also adds the calculation of safety risks in parallel with security risks.

Table 10: Tools and techniques for Iteration 2 [60]

Phase	Technique	Framework/ Tools
Asset Inventory tools	CMDB, network scanners, reviewing system documentation and configuration files	Inventory management tools-CMDB, SCADAware Discovery, PLC configuration tools: Siemens TIA portal , Rockwell Automation studio 5000
Initial assessment	FMEA analysis	MITTRE ATT&ACK for ICS; Network scanners: Nmap, OpenVAS with industrial plugins: SCADAware, Industrial Defender; Wireshark, TCPdump, Busmaster
Threat modelling	STRIDE, FMEA, PASTA, DREAD ,attack surface analysis	Microsoft threat modeller
Initial risk assessment	Risk assessment frameworks	NIST CSF, IEC 62443, ISO 27001
Vulnerability assessment	Vulnerability scanning, Static analysis Dynamic testing analysis, Fuzzing,	Vulnerability scanners: TenableOT, Dragos X-series, CPPcheck, PVS-studio for PLC code analysis, Fortify, Coverity Modbus scanners (Modscan), ISuTest, , PLCSIM, Fuzzing tools: ICS fuzz, AFL, Peach fuzzer, PLC fuzzers (Radamsa, scapy)
Penetration testing	Code review for vulnerabilities, protocol fuzzing, black box testing, and white box testing, OWASP testing	Metasploit with ICS modules, Kali Linux
Risk assessment	Quantitative analysis Qualitative analysis	Risk assessment frameworks: NIST CSF risk matrix, Business Impact Analysis tools: FAIR, DREAD, Incidence Response simulation tools: SCADAware Cyber Range
Remediation	Vulnerability management Patch management Periodic vulnerability scans	VMPs (Vulnerability management Platforms)Tenable, Qualys, Rapid7 Microsoft SCCM, Red Hat Satellite
Reporting	Generate reports	Reporting platforms (Tenable)
Continuous monitoring	Issue tracking SIEM management IDS/IPS specific monitoring	Jira, Bugzilla; Splunk, ELK stack; Snort, Suricata ; Dragos, Nozomi networks

4.2.5.1 Threat Scenario (Unauthorized Access to TIA Portal)

Objective: To apply the modified Security testing framework for a comprehensive assessment to identify and mitigate the risk of unauthorized access to the TIA Portal, ensuring the integrity of industrial automation processes.

Application of Modified Framework

The TIA Portal, a crucial component of IACS at Kone cranes, uses advanced technologies to manage the movements, operations, and safety features of industrial cranes. It uses STRIDE and DREAD to identify and classify components, PLCs, HMIs, and engineering workstations to prevent threats like unauthorized access and manipulation. Risks associated with unauthorized access are assessed, including potential disruptions to PLC logic and unauthorized modification of HMI configurations. Testing methodologies validate encryption, authentication, and integrity of PLC communication channels for secure data transmission. Vulnerability scanners like Nessus identify vulnerabilities, while Security Compliance Testing ensures adherence to security standards.

Tools like Qualys assess endpoint security, focusing on workstations and devices connected to the TIA Portal. The FAIR framework is applied to identify critical risks associated with unauthorized access, emphasizing potential financial and operational impacts. Existing security controls are evaluated for effectiveness against unauthorized access. Role-based access controls are implemented to restrict unauthorized modifications to PLC configurations. Regular software updates and patching procedures are established to address vulnerabilities. The Crane Control Platform's security is paramount to prevent unauthorized access, manipulation, and cyber threats.

The illustration of security testing framework when applied to the crane control platform of an IACS system is as follows:

4.2.5.2 Threat Scenario 1: Security Threat - Unauthorized Control Access to Crane Control Platform

Objective: To evaluate and address the security threat of unauthorized control access to the Crane Control Platform with a primary focus on security.

Application of modified framework

The Siemens S7-1500 PLC is a critical component that requires careful security measures. The threat modelling frameworks STRIDE and DREAD can be used to identify threats like unauthorized control access and potential manipulation of motor controllers. Risks associated with unauthorized access can be assessed using tools like Metasploit and Siemens PLCSim. Specific procedures are implemented, including disabling unnecessary services, applying security patches, and configuring secure default settings. Network vulnerability scanning like Nessus can be used to assess vulnerabilities in the network infrastructure.

The exposure of the Siemens S7-1500 PLC to unauthorized control access can be assessed, focusing on potential impacts on operational efficiency. Risks can be analyzed, and role-based access controls can be implemented using TIA Portal. Snort as an intrusion detection system can be deployed to identify unusual patterns in control access. Code review and validation using tools like PLC Checker ensure control logic resilience against unauthorized manipulation. Regular audits of control access logs and security configurations using Siemens WinCC and collaboration with OT engineers can adapt security measures to evolving threats.

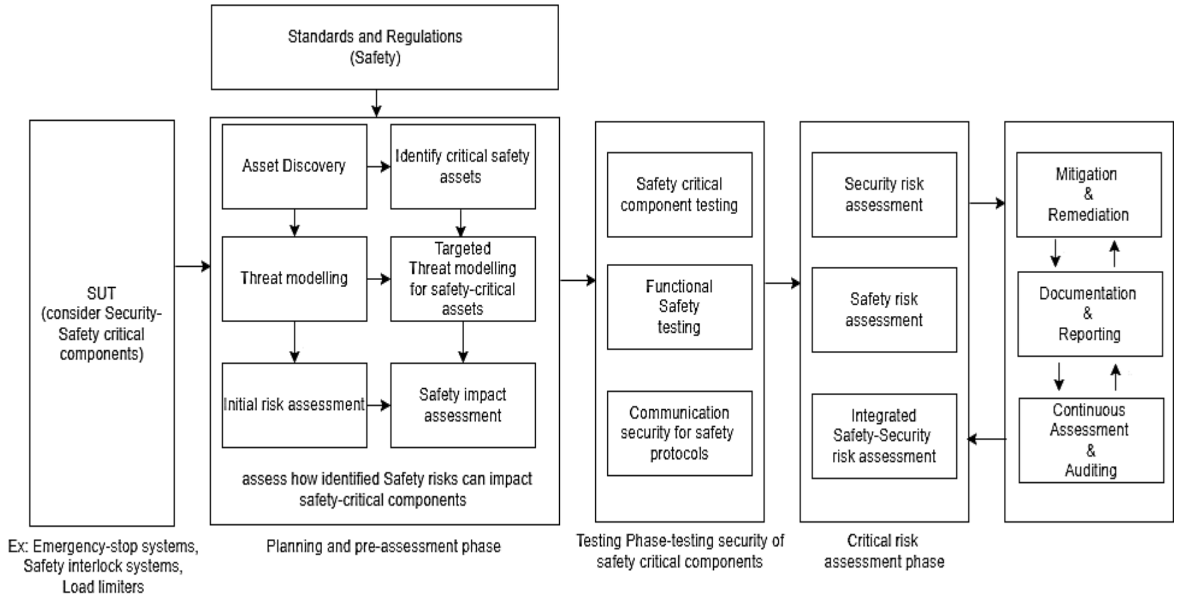

Standards and Regulations (Safety)
SUT (consider Security-Safety critical components)
Asset Discovery
Identify critical safety assets
Threat modelling
Targeted Threat modelling for safety-critical assets
Initial risk assessment
Safety impact assessment
assess how identified Safety risks can impact safety-critical components
Safety critical component testing
Functional Safety testing
Communication security for safety protocols
Security risk assessment
Safety risk assessment
Integrated Safety-Security risk assessment
Mitigation & Remediation
Documentation & Reporting
Continuous Assessment & Auditing
Ex: Emergency-stop systems, Safety interlock systems, Load limiters
Planning and pre-assessment phase
Testing Phase-testing security of safety critical components
Critical risk assessment phase

Figure 9: Application of Framework considering Safety implications on Security

4.2.5.3 Threat Scenario 2: Safety-Security Choke Point - Unauthorized Control Access with Safety Implications

Objective: To address a threat scenario where unauthorized control access to the Crane Control Platform has potential safety implications by integrating safety and security assessments.

In this case we consider safety implications of PLC-based control systems, when remotely accessed, that impact the security and vice versa. Figure 9 depicts an example walk-through of the framework at the safety and security choke points. Identifying Siemens S7-1500 PLC and safety-critical component such as emergency stop systems.

The framework for safety and security in a crane control platform involves identifying potential threats and implementing measures to protect critical processes. Threat modeling using

STRIDE and DREAD can identify unauthorized control access, leading to safety hazards. Initial risk assessment is conducted to assess risks associated with unauthorized access, focusing on potential safety hazards and disruptions. Operational testing with safety integration can be performed using tools like Metasploit to simulate unauthorized control attempts. Functional testing with safety implications is performed using Siemens PLCSim, while process-specific vulnerability testing with safety considerations is done using PILZ PAScal.

The critical risk assessment phase evaluates the exposure of the Siemens S7-1500 PLC and safety-critical components to unauthorized control access, analyzing potential consequences and cascading effects on critical processes. Role-based access controls are implemented using TIA Portal to restrict unauthorized access and deploy Snort as an intrusion detection system. A comprehensive code review and validation are conducted, prioritizing safety-critical elements. All safety and security considerations within the Crane Control Platform using TIA Portal project are documented, with a detailed report on implemented measures and regular audits. Collaborating closely with safety engineers ensures a holistic approach to security without compromising safety.

The discussions with the Focus Group 2 (FG 2) give valid inputs and the most relevant question faced in the session is that "How to integrate the IEC 62443 standard, the most recognized international standard for the IACS security into the framework ?" This question served as the knowledge question for the next iteration. By focusing on the alignment with IEC 62443 standards, Iteration 3 aims to elevate the security testing framework to meet internationally recognized benchmarks for IACS systems.

4.3 Iteration 3 (Integration of IEC 62443 standard into the framework)

Iteration 3 of the security testing framework development process builds upon the foundation laid in iteration 2, focusing on the integration of IEC 62443 standards and the establishment of a comprehensive testing framework. This iteration is particularly crucial for organizations like Konecranes, considering the approaching deadlines for several major cybersecurity regulations in the EU, including the Network and Information Systems (NIS2) Directive, the Radio Equipment Directive-Delegated Act (RED-DA), the Machinery Regulation, and the Cyber Resilience Act (CRA), the EU AI Act and so on. These regulations mandate robust cybersecurity measures for critical and essential infrastructure systems, including IACS systems.

Organizations must demonstrate compliance with these regulations to maintain their operational continuity and protect critical assets from cyberattacks. Since IEC 62443 standard has emerged as the leading framework for cybersecurity in IACS, providing a comprehensive set of guidelines for security requirements, controls, and risk management, adopting IEC 62443 as the cornerstone of the security testing framework, organizations can ensure that their IACS systems meet the stringent security requirements of the upcoming regulations.

The framework should align with IEC 62443 standards and incorporate a range of testing methodologies, including vulnerability scanning, penetration testing, compliance testing, performance testing, and so on [71]. Iteration 3 of the security testing framework development process is designed to address these critical requirements, empowering organizations to meet the impending deadlines and safeguard their IACS systems in the face of evolving cybersecurity threats. The objective for Iteration 3 is to enhance the security testing framework to align with the cybersecurity requirements of IEC 62443 for PLC-based IACS systems.

4.3.1 Problem Investigation

In our earlier iteration, we developed a security testing framework tailored for PLC-based Industrial Automation and Control System. Against the backdrop of emerging EU regulations concerning IACS cybersecurity, organizations are realizing the critical need for compliance. Compliance with these security regulations has evolved from a mere regulatory requirement to a strategic business imperative, essential for maintaining a competitive edge in global markets. The first step on this compliance journey often begins with a thorough security risk assessment. Hence, the imperative for a dedicated security testing framework designed to cater to the unique demands of IACS security.

However, one of the primary challenges faced is the necessity for a common standard to anchor our efforts. This challenge is met by turning to the internationally recognized ISA/IEC 62443 standard, which aligns closely with the anticipated harmonized standards being developed by the EU. This alignment provides a solid foundation for our framework, ensuring it remains in sync with evolving regulatory landscapes. Now, our focus turns to enhancing this security testing framework to align seamlessly with the cybersecurity requirements set forth by IEC 62443 for PLC-based IACS systems. Our research question, "How can the security testing framework be enhanced to align with the cybersecurity requirements of IEC 62443 for PLC-based IACS systems?" serves as a guiding light for our efforts in this third iteration.

This ensures that our development activities are focused on tackling the specific cybersecurity challenges posed by IEC 62443. The next challenge lies in the selection of the system under consideration for testing. The IEC 62443 standard recommends breaking down the entire system into distinct zones and conduits. While in previous iterations, we relied on the Purdue model for this purpose, the task now is to seamlessly integrate both the Purdue model and the Zone-conduit model in our framework.

Another challenge we face is how to effectively map the various phases of our framework to the corresponding sections of the IEC 62443 standard. This alignment ensures that our testing procedures are in perfect harmony with the best practices outlined in the standard, enhancing the robustness and relevance of our framework. Lastly, we aim to address the challenge of setting the appropriate security levels from the IEC 62443 standard to each phase of our framework.

This step ensures that our framework is capable of accurately assessing the security posture of PLC-based IACS systems across varying security levels, catering to the diverse levels of protection required. Each of these challenges has provided an opportunity for refinement and improvement in our security testing framework. By systematically addressing these challenges in this iteration, we aim to create a framework that is not only aligned with the stringent cybersecurity demands of IEC 62443 but also equipped to navigate the complex regulatory landscape of IACS cybersecurity with confidence and precision.

4.3.2 Solution Design

In addressing our 3rd research question, we meticulously tailored the security testing framework to precisely align with the cybersecurity prerequisites of the IEC 62443 standard. We began by recognizing the paramount importance of integrating the ISA/IEC 62443 standard within the context of the current landscape of myriad EU regulations affecting organizations [71]. A methodical mapping of these regulations against the standard to gain insights into their intersections was performed. With an in-depth study of the application of the standard in various other IACS domains as well [72, 73], the clarity emerged that the IEC 62443 standard stands out as the natural choice for anchoring IACS security protocols amidst the multifaceted requirements of EU regulations in case of Konecranes. Drawing upon these regulations as crucial inputs, we forged ahead to select the system under test (SuT).

Integrating the Purdue model with the Zone-conduit model of the IEC 62443 standard, our approach to SuT selection was meticulously designed for precision. Next, we meticulously mapped each phase of our framework to the relevant sections of the IEC 62443 standard, infusing depth, and coherence into our methodology. This strategic alignment not only fortified the foundation of our work but also ensured a seamless integration of industry best practices [74,75]. Finally, we strategically aligned the concept of Security Levels (SLs) to each phase of the framework. This deliberate move was aimed at enhancing our framework's capability to adeptly assess the security postures of systems across varying SLs.

This involved adapting the framework to include the following modifications:

4.3.2.1 Embedding the Zone-Conduit Model into the Purdue Enterprise Reference Architecture for the selection of SuT

Recognizing the IEC 62443 standard as the globally acknowledged benchmark for IACS security, our focus has been on understanding how its principles align with the diverse array of EU regulations. Through this exploration, it has become apparent that the ISA/IEC 62443 standard serves as an ideal starting point for organizations embarking on their security testing journey. By adopting this standard, companies can effectively navigate the complex landscape of IACS security while ensuring compliance with evolving EU regulations

The IEC 62443 standard is a crucial guide for conducting thorough security testing on systems. It recommends partitioning the system into zones and conduits (3-2), as introduced in IEC TS 62443-1-1, to better manage security considerations and assess risk for each zone and conduit. The Purdue Reference Architecture (PERA) serves as a foundational framework, excelling in structuring and organizing system components for efficient operation. However, the evolving landscape of cybersecurity threats necessitates further fortification.

The integration of the zone-conduit model, as outlined in the IEC 62443 standard, is necessary [76]. Zones represent areas of restricted access with high security, while conduits serve as controlled communication paths between zones. For example, in Layer 0, the enterprise zone is protected by a firewall, IDS, and IPS, while the internet conduit ensures secure communication with external networks. This strategic integration significantly reduces the potential attack surface, safeguarding critical assets from unauthorized access and cyber threats.

The zone-conduit model is integrated by mapping PERA layers to IEC 62443 security levels [76]. The system under Test (SuT) is described in terms of zones and conduits, and individual target SLs are assigned to these. The SRs and REs in this standard, along with their mapping to capability SLs (SL-Cs), are used to compile a list of requirements for the control system design. A given control system design can be checked for completeness, providing SL-As. The SRs are associated with the seven foundational requirements (FRs) described in IEC 62443-1-1. They define the requirements for control system capability security levels, zones and conduits, and appropriate control system target SLs for specific assets/zone-conduits.

The reference workflow diagram is considered to outline the primary steps required to establish zones and conduits and assess risks. As defined in IEC 62443-1-1 there are a total of seven FRs (3-3): Identification and authentication control (IAC), Use control (UC), System integrity (SI), Data confidentiality (DC), Restricted data flow (RDF), Timely response to events (TRE), Resource availability (RA).

This mapping is based on the criticality of the assets and the likelihood of attack at each layer. For instance, Layer 0, the enterprise layer, where critical assets reside, is assigned SL 4, the highest security level. Similarly, Layer 3, the sensors, and actuators layer, where the least critical assets are located, is assigned SL 1, the lowest security level. Within each PERA layer, distinct security zones and conduits can be defined, adhering to the IEC 62443 guidelines.

The integration of the zone-conduit model into the PERA offers several significant benefits such as enhanced security posture, granular risk management and stream-lined security testing and so on. However, to ensure the effectiveness of the integrated zone-conduit model, several implementation considerations should be addressed. First, the choice of communication protocols [75] is crucial, with secure protocols like TLS/SSL recommended for inter-zone communication. In Layer 2, where devices are tightly coupled, proprietary protocols may be employed. Next, the Access control mechanisms play a pivotal role in restricting access to zones and devices based on user permissions.

Role-Based Access Control (RBAC) is an effective approach [75], while strong authentication methods like two-factor authentication should be implemented for critical access points. Monitoring and logging capabilities are essential for tracking activities within zones and conduits. SIEM solutions help correlate events and identify anomalies, facilitating proactive threat detection. Continuous assessment is paramount to maintain the overall security posture of the zones and conduits. Vulnerability scanning, penetration testing, and other security testing methods [77] should be regularly conducted to identify and remediate vulnerabilities promptly

4.3.2.2 Consideration of various regulations

As the organization sets its sights on aligning with multiple EU regulations to meet stringent security requirements, the necessity for a unified standard becomes evident. Currently, the EU is actively working towards establishing a harmonized standard, yet its official release remains pending. Anticipated to parallel the robust principles of the IEC 62443 standard, this awaited EU standard promises a comprehensive framework for industrial control system security. The below Table 11 depicts the mapping of various EU regulations with parts of the standard that shows that the EU regulations are not too already on their way to the organizations, and it is quite good that most of the security requirements coming from these regulations can be mapped with the IEC 62443 standard.

Table 11: Mapping of the EU regulations with parts of the standard

EU Regulation	Requirements for IACS security	Alignment with IEC 62443 standard
Cyber Resilience Act (CRA)	Risk Assessment, Conformity assessment, Vulnerability reporting, documentation	Broadly aligns with many aspects of IEC 62443: security by design, risk assessment (3-2), incident response and vulnerability management
NIS 2 Directive (EU) 2022/2555	Comprehensive risk management, Incidents reporting within specific timeframes, security assessments of suppliers and third parties.	Strongly aligns with sections on risk assessment (3-2), incident response, supplier security, and security levels (3-3).
RED-Delegated Act (EU 2019/876)	Ensure confidentiality of communication and protection against unauthorized use, access, and modification of devices.	Aligns with IEC 62443 sections focused on secure communication and data integrity.
Machinery Regulation (Regulation (EU) 2019/1146)	Implement secure software development practices and measures to manage cybersecurity risks in the control systems of machinery.	May involve additional security considerations beyond IEC 62443 but aligns with the general principles of secure coding and vulnerability management.

4.3.2.3 Mapping the phases of the framework with the IEC 62443 standard

First, we have tried to establish a clear connection between the different phases of the Security Testing Framework to the relevant sections within the IEC 62443 standard. This mapping as illustrated in Table 12 usually helps to ensure that the testing activities are aligned with the established security best practices outlined in the standard. By pinpointing specific subsections within the relevant sections, this mapping provided a more granular understanding of how the framework activities align with the detailed requirements of the IEC 62443 standard.

By understanding this mapping and ensuring alignment with the IEC 62443 standard, organizations can conduct security testing in a comprehensive and standardized manner, ultimately strengthening the overall security posture of their PLC-based IACS environments. The Table 12 below establishes a clear connection between the different phases of the Security Testing Framework for PLC-based IACS and the relevant sections within the IEC 62443 standard.

Table 12: Mapping of Phases of the Framework with Parts of the Standard

Phase	IEC 62443 standard reference
Planning and Pre-Assessment phase (System security requirements definition and System documentation review)	IEC 62443-4-1: SRs and SSLs IEC 62443-4-1-2.1: Definition of SRs IEC 62443-4-1-2.2: Security zones and conduits IEC 62443-3-2: Process for developing and maintaining a security program for IACS
Asset Discovery Phase	IEC 62443-4-1 IEC 62443-4-1.3: System documentation
Threat Modelling Phase	IEC 62443-3-2.1
Initial Risk Assessment Phase	IEC 62443-3-2.4: Risk Assessment
Scope & Objectives	IEC 62443-4-1.2.1, 3-2.1: Security policy objectives
Comprehensive security testing phase	IEC 62443-4-2: Security risk assessment and system testing IEC 62443-4-2.2
Vulnerability assessment	IEC 62443-4-2.1
Penetration testing	IEC 62443-4-2.2.2
Critical risk assessment phase	IEC 62443-4-2: Security risk assessment and system testing IEC 62443-3-2.4.2: Impact assessment
Incidence Response Management, Remediation & Mitigation phase	IEC 3-3.1: Security incidence detection and response
Documentation & Reporting phase	IEC 62443-4-1.3: System documentation
Continuous Assessment & Auditing	IEC 62443-3-2.5

4.3.2.4 Threat Mitigation Testing

The framework has been modified by including the Threat Mitigation Testing in its treat modelling phase as integrating threat mitigation testing directly into the framework's threat modeling phase seemed to offer several advantages that align perfectly with the ISA/IEC 62443 standard. While the ISA/IEC 62443 standard doesn't explicitly mention about the threat mitigation testing, its emphasis on proactive security aligns perfectly with integrating this concept into threat modeling. .

This proactive approach allows for simultaneous identification of threats and evaluation of countermeasures, streamlining the process and ensuring targeted mitigation strategies. For instance, IEC 62443-4-1 calls for systematic approach to security throughout the IACS lifecycle, from design to decommissioning [74]. It stresses the importance of risk management which involves identifying threats, vulnerabilities, and potential consequences and evaluating security measures (Mitigation strategies) to address identified threats. So, integrating threat mitigation testing within threat modeling aligns with this concept by proactively assessing potential threats and vulnerabilities early on.

During the threat modeling, potential threats and attack vectors targeting the IACS system are identified. Simultaneously, mitigation strategies like access controls, network segmentation, or specific hardening measures are brainstormed for each threat. This evaluation considers the effectiveness of these countermeasures in preventing attacks and their potential impact on system performance. Based on this analysis, threats and mitigation strategies can then be prioritized, focusing resources on the most critical vulnerabilities.

Optionally, limited testing of promising mitigation strategies can be conducted in a non-critical environment for further evaluation. So, this integrated approach aligns with the standard's emphasis on risk-based security and "Defense in depth" strategies [79], ultimately fortifying defenses against potential threats and enhancing the overall security posture of the IACS system.

4.3.2.5 Detailed Risk Assessment

The framework developed has already defined a comprehensive risk assessment phase which includes form risk identification, assessment to mitigation. The standard also provides a similar guidance about the critical risk assessment per zone or conduit, whereby it introduces requirements in Clause 4 that are referred to as zone and conduit requirements (ZCR). So, the ZCR concept has been considered within the detailed risk assessment phase of the framework. ZCR 5 (3-2-4.6.1) discusses the detailed risk assessment [80] requirements for an IACS and provides rationale and supplemental guidance on each requirement.

The requirements in this ZCR apply to every zone and conduit. The mapping of various phases of the risk assessment in the framework has been mapped with the ZCR’s of 3-2 of the standard.

Almost all the phases remain the same, this framework recommends threat assessment along with the initial risk assessment phase unlike to the standard’s recommendation to have threat assessment as a part of detailed risk assessment phase which we would think as an optimal arrangement.

After the completion of threat mitigation testing and comprehensive testing phases, a critical stage commences: the detailed risk assessment. This phase relies on the combining the results obtained from prior assessments. Primarily, it integrates potential threats identified during the threat assessment with vulnerabilities uncovered through vulnerability assessments and testing procedures. Guided by best practices (e.g., ISA/IEC 62443), this phase emphasizes a meticulous review of existing Process Hazard Analysis (PHA) and associated risk assessments encompassing various domains.

These domains may include information technology (IT), functional safety, business continuity, and physical security. The evaluation progresses by determining the consequences and impact of identified risks (ZCR 5.3). Following this, a likelihood assessment (ZCR 5.4) is conducted to gauge the unmitigated risk likelihood (ZCR 5.5). This information, along with the impact assessment, contributes to the derivation of the Target Security Level (SL-T) for the asset or system under test (ZCR 5.6).

The process of assessing a system's vulnerability involves reviewing and updating vulnerabilities, calculating residual risks (ZCR), and maintaining meticulous documentation. This documentation serves as a comprehensive repository of identified risks and mitigation strategies, providing a valuable resource for future reference and risk management. The standard recommends adapting to detailed risk assessment methodologies, such as ISO 31000, NIST SP 800-39, and ISO/IEC 27005, provided the risk assessment requirements are met.

4.3.2.6 Alignment of phases with IEC 62443 Security Levels

The IEC 62443 framework was integrated by mapping security levels to framework activities. The framework was analyzed by referring to specific sections of the standard, outlining different security levels and their associated technical System Requirements and Requirement Enhancements. Activities within the framework were identified based on their type and depth of security, focusing on their purpose and impact. Activities were tabulated (Table 13) to map them to their corresponding security levels for a clear representation. Some activities were considered 'baseline' security practices, which can be adjusted based on the context, risk profile, and resource constraints of the IACS environment.

Although it is to be noted that the specific activities and their corresponding security levels may vary depending on the design and the specific security requirements of the IACS environment. This is how the security levels defined in IEC 62443 were effectively incorporated into the framework which can align the framework with industry best practices, demonstrate a clear understanding of security requirements for different risk levels and enable organizations make informed decisions when selecting and implementing security measures for their IACS environment and thereby facilitating communication and collaboration with stakeholders who understand the concept of security levels.

Table 13: Assigning the security levels to each phase of the framework

Framework Activity	**Description**	**Security Level 1 (SL1)**	**Security Level 2 (SL2)**	**Security Level 3 (SL3)**	**Security Level 4 (SL4)**
Asset Discovery and Classification	Identifying and classifying critical assets within the IACS environment.	✓	✓	✓	✓
Threat Modeling	Identifying potential threats and vulnerabilities.	✓	✓	✓	✓
Vulnerability Scanning	Identifying known vulnerabilities in system components.	✓	✓	✓	✓
Penetration Testing	Simulating real-world attack scenarios to identify exploitable vulnerabilities.		✓	✓	✓
Network Segmentation	Isolating critical assets on separate networks to limit attack spread.		✓	✓	✓
Endpoint Security	Implementing endpoint protection and detection solutions on devices.	✓	✓	✓	✓
Patch Management	Timely patching of vulnerabilities in system components.	✓	✓	✓	✓
Incident Response Planning	Developing and testing incident response procedure	✓	✓	✓	✓

The checkmark (✓) indicates that the activity is considered relevant for achieving the security objectives and requirements of that specific security level.

4.3.3 Design Validation

To validate the implementation of the enhanced security testing framework We actively sought feedback from stakeholders involved in the evaluation process, including IEC 62443 security experts, and industrial control engineers and IACS system owners to ensure that the framework meets their needs and aligns with their expectations. This feedback provided valuable insights into the framework's strengths and weaknesses, helping to guide further development and refinement. In addition to that,

during this phase Wieringa's validation questions were considered.

On Internal Validity: Would this design, implemented in this problem context, satisfy the criteria identified in the problem investigation?

The design implemented in this problem context aimed to address the specific criteria identified in the problem investigation. The need for a common standard to navigate the evolving landscape of EU regulations in IACS cybersecurity was recognized. By integrating the Purdue model from the previous iteration with the zone-conduit model of the IEC 62443 standard, we tailored the framework to align precisely with the cybersecurity requirements of IEC 62443. Threat modeling involves identifying potential threats and vulnerabilities, with mitigation testing integrated for efficiency and streamlining.

This approach eliminates the need for separate testing of countermeasures for potential threats, ensuring direct threat response. Risk-based prioritization ensures resources are focused on critical threats with effective countermeasures. By mapping the various phases of the framework with the parts of the standard and mapping the phases with the security levels from the standard, we directly satisfy the criteria established in our problem investigation, ensuring a targeted approach to security testing for PLC-based IACS systems.

On Trade-offs: How would slightly different designs, implemented in this context, satisfy the criteria?

Slightly different designs implemented in this context might have varying degrees of success in satisfying the criteria. For instance, if we had chosen not to integrate the Purdue model with the zone-conduit model of IEC 62443, the framework might not have been as closely aligned with the specific requirements of the standard. This could have resulted in a less precise approach to security testing, potentially missing key vulnerabilities or failing to meet the stringent standards set by IEC 62443.

Another approach for Integrating the security levels defined in IEC 62443 into the framework could have been linking the framework outputs to the security levels. By analyzing the results and outcomes generated by each phase or activity within the framework and evaluating how the outputs can relate to the security levels which might have led to different conclusions. Alternatively, a design that deviated significantly from integrating the standard might have provided a broader coverage of vulnerabilities but could have lacked the depth and specificity required for IEC 62443 compliance.

On External Validity: Would this design, implemented in slightly different contexts, also satisfy the criteria?

In considering the external validity of our design, we believe that this framework, implemented in slightly different contexts, would also satisfy the criteria. The integration of the Purdue model with the zone-conduit model of IEC 62443 provides a flexible yet standardized approach that can be adapted to various IACS systems across different industries. While the specific details of the systems may vary, the foundational principles of the IEC 62443 standard remain consistent. Therefore, this design should hold validity and effectiveness in other contexts where IEC 62443 compliance is a priority, ensuring a robust and tailored security testing framework for PLC-based IACS systems.

4.3.4 Implementation

Throughout our work iterations, we've consistently explored various tools and techniques suitable for implementing the security testing framework. While the fragile nature of the OT environment necessitates a phased implementation approach, we recognize the urgency to comply with impending regulations like CRA, NIS 2, and RED. The toolset discussed in previous iteration remains relevant across all phases. These tools have been carefully chosen for compatibility with the IEC 62443 standard and are well-suited for PLC-based IACS systems. This consistency reduces the need for additional tool selection in the current iteration3.

4.3.5 Evaluation

Evaluation of the iteration 3 is performed by the sample illustration of the modified framework to one each of IT and OT asset such as TIA portal and Crane control system respectively in the

Industrial Automation and Control System, assuming a threat/ vulnerability per asset. Considering a threat/vulnerability such as an unpatched vulnerability in TIA Portal allows an unauthorized attacker remote access to the system, potentially leading to data breaches, project manipulation, or disruption of critical control systems. Now, applying the Security Testing Framework that is aligned with IEC 62443 standard might appear something like this illustration:

To ensure security, IT and OT zones must be classified based on their criticality and potential impact. This involves defining system boundaries for TIA Portal and crane control systems, including their components, dependencies, and interfaces. IT assets have critical functionalities like engineering project creation, code compilation, communication with PLCs, network connections, software vulnerabilities, and user credentials. OT assets have critical functions like control of crane movement, safety interlocks, sensor data processing, emergency stop procedures, collision avoidance mechanisms, overload protection, and identified attack vectors.

A threat analysis is conducted to identify potential threats specific to each zone, considering vulnerabilities and attack vectors such as unauthorized access, data breaches, and manipulation of control commands. High-risk vulnerabilities are prioritized in critical zones, such as Zone 0. Vulnerability assessments can be conducted using tools and scanners to identify exploitable vulnerabilities in TIA Portal and crane control systems. High-risk vulnerabilities impact safety, operational continuity, and regulatory compliance.

Analyzing test results helps identify security gaps and potential corrective actions, prioritizing them based on risk assessment and aligning with security requirements in the System Security Requirements Specification (SSRS) as per IEC 62443 standard. Mitigation measures for security breaches in the IACS environment include patching vulnerabilities in the TIA Portal, implementing access control measures, and encrypting sensitive data. For the crane control system, these measures include patching the vulnerability, isolating the control system from non-critical systems, implementing multi-factor authentication, and enhancing physical security.

5 Results

This chapter presents the finished Security Testing Framework for the PLC-based IACS systems in alignment to the ISA/IEC 62443 standard, and the answers to the research questions. First, a detailed overview of the framework is provided after which the implementation and design are discussed, followed by the answers to the research questions.

5.1 Security Testing Framework

The primary outcome of this thesis is the development of a comprehensive Security Testing Framework tailored specifically for PLC-based IACS systems. This framework was designed to address the security challenges inherent in PLC-controlled environments, with a focus on enhancing the overall cybersecurity posture of critical industrial processes.

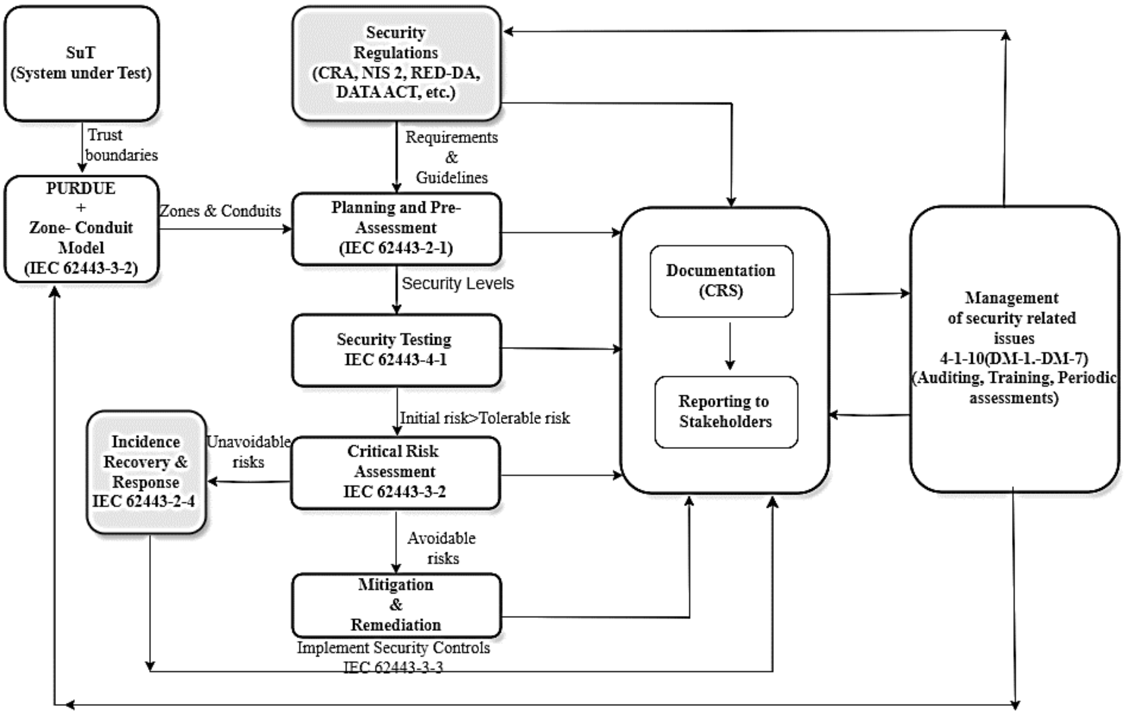

SuT
(System under Test)
Trust boundaries
PURDUE + Zone- Conduit Model (IEC 62443-3-2)
Zones & Conduits
Security Regulations (CRA, NIS 2, RED-DA, DATA ACT, etc.)
Requirements & Guidelines
Planning and Pre-Assessment (IEC 62443-2-1)
Security Levels
Security Testing IEC 62443-4-1
Initial risk>Tolerable risk
Critical Risk Assessment IEC 62443-3-2
Unavoidable risks
Incidence Recovery & Response IEC 62443-2-4
Avoidable risks
Mitigation & Remediation
Implement Security Controls IEC 62443-3-3
Documentation (CRS)
Reporting to Stakeholders
Management of security related issues 4-1-10(DM-1.-DM-7) (Auditing, Training, Periodic assessments)

Figure 10: Security Testing Framework as the result of the thesis

The Security Testing Framework (Figure 10) aims to provide organizations with a structured approach to identify, assess, and mitigate potential vulnerabilities within PLC-based IACS systems to safeguard the critical infrastructure from cyber threats by implementing targeted security measures and controls. . In a larger scope, the framework serves as a strategic tool for organizations seeking to fortify their IACS security posture, aligning with industry best practices and standards such as ISA/IEC 62443.

5.1.1 Identifying the SuT and the standard

The System Under Test (SuT) is a critical component within the IACS domain that undergoes a thorough security evaluation to assess its operational performance, security posture, and regulatory compliance. This process is crucial for establishing a robust IACS security posture and strategically targeting security testing efforts towards the most critical assets within the IACS infrastructure.

The selection process involves a methodology for categorizing resources, considering system criticality, regulatory compliance, and interdependencies. High-impact systems are prioritized due to their potential impact on safety, production, or environmental factors. Adherence to relevant security regulations, such as the ISA/IEC 62443 standard, guides the selection process. The selection process also considers perimeters and trust boundaries within the IACS network architecture. Standard selection provides a structured framework for conducting security testing, ensuring a well-defined SuT selection process.

5.1.2 Planning and Pre-Assessment phase

The Planning and Pre-Assessment phase sets the groundwork for effective security testing of IACS systems. Asset discovery, classification, system modeling, threat modeling, initial risk assessment, and risk mitigation strategies are crucial components of this phase as illustrated in Figure 16. By following a systematic approach, organizations can enhance the security posture of their IACS environments, reducing the risk of cyber threats and vulnerabilities.

5.1.2.1 Asset Discovery & Classification

Asset discovery involves the collection of information about interconnected technical assets within a network, facilitating effective management and monitoring. A comprehensive understanding of these systems is crucial for efficient asset detection and prioritization. Asset classification, aids in prioritizing security measures and resource allocation. An in-depth analysis of existing research on asset classification provided valuable insights into the methodologies and tools employed in this stage. Literature provides the practical implementations of scanning tools for asset discovery, which can be adapted into the framework.

5.1.2.2 System Model Development

Upon completing asset discovery and classification, the creation of a comprehensive system model, as suggested in [54], becomes pivotal. This model serves as a tool for simulating system behavior, identifying potential attack surfaces, and generating test cases to evaluate system resilience against cyber threats. Organizations can construct this system model by leveraging data gathered during the asset discovery phase, elucidating relationships between different subsystems. This simulation not only reflects the system's behavior but also effectively delineates potential attack surfaces. It enables the development of tailored security testing methodologies and strategies, specifically tailored for IACS environments.

5.1.2.3 Threat Modeling

With the establishment of a detailed system model, organizations can initiate proper threat modeling. Threat modeling, a critical analytical step, aids in identifying potential threats against the System under Test (SuT). While its application to cyber-physical systems requires more systematic elaboration, this approach is fundamental to implementing the secure-by-design principle.

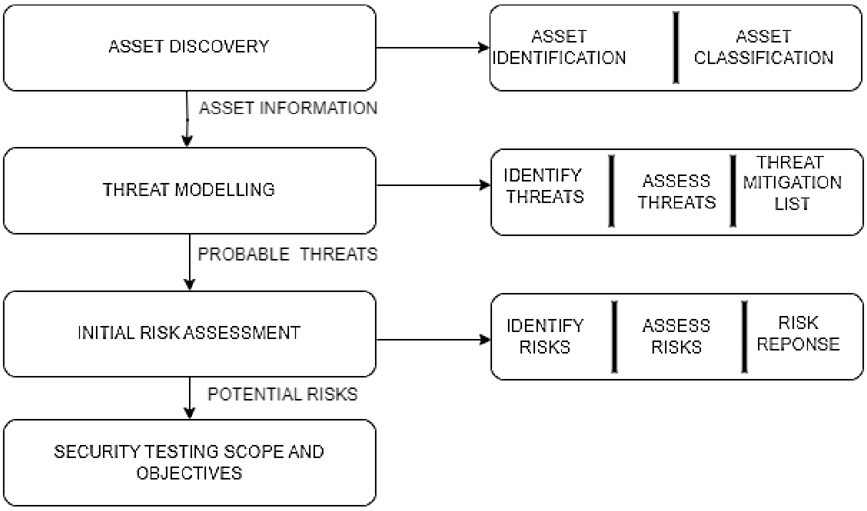


Figure 11 : Planning and Pre - Assessment Phase

Several popular approaches such as STRIDE, DREAD, PASTA, and LINDDUN offer diverse methods for threat modeling. Creating a cognitive map of threats specific to the IACS security strategy is valuable for classifying and prioritizing threats. Additionally, a novel threat model-driven security testing approach based on UML diagrams, can detect undesirable threat behaviours during runtime and be adapted for vulnerability testing.

5.1.2.4 Initial Risk Assessment

The results from threat modeling significantly contribute to the Initial Risk Assessment phase. This phase involves listing identified threats along with their severity. Leveraging these results, organizations can efficiently conduct the initial risk assessment, focusing on evaluating, prioritizing, and addressing identified risks within IACS systems.

For PLC-based IACS systems, the Initial Risk Assessment phase (Figure 11) provides a comprehensive understanding of system threats and vulnerabilities. Organizations may utilize various Risk Assessment frameworks such as NIST SP 800-82, ISO/IEC 27001, and the IEC 62443 series. Prioritization within the risk assessment process involves considering individual threat priorities and risk response strategies, highlighting potential network architecture flaws, software vulnerabilities, and security measure inadequacies. To address mitigated threats, organizations first define a risk matrix, considering factors such as the likelihood of threat occurrence, potential consequences of successful attempts, and existing security measures. T

his involves identifying risk factors and vulnerabilities, categorizing them by severity, probability of occurrence, and potential impact on operations, and prioritizing them based on safety, reliability, and functionality. With a general understanding of potential security risks, organizations can determine the focus areas during security audits. Risk identification involves discovering risks from potential threats, weighing possible outcomes and probabilities for each identified risk. An initial risk assessment includes reports summarizing risks, their potential impact, and proposed threat mitigation techniques.

A proposed process based on the IEC 62443 standard, leveraging the MITRE ATT&CK framework and Intel Threat Agent Library (TAL), can also be adapted for automated risk assessment [60]. Subsequently, a risk mitigation strategy is developed, outlining steps to reduce the impact of identified risks. This strategy suggests new security controls, revised operational methods, and other measures to enhance IACS security.

5.1.2.5 Scope and Objectives of Security Testing

Defining the scope and objectives of security testing for the System under Test (SuT) involves utilizing various technologies. Asset inventory aids in cataloguing all system assets, identifying potential vulnerabilities, and determining the testing scope. It directs attention to areas requiring thorough testing and specifies specific security objectives. Regulatory compliance tools help organizations understand relevant security standards and regulations, aligning testing objectives with compliance criteria.

5.1.3 Testing phase

The Testing Phase for PLC-based IACS systems involves a comprehensive evaluation of the system's security posture and resilience through various testing methodologies. Establishing an overall security testing strategy (Figure 12) is crucial, encompassing penetration testing, vulnerability scanning, security compliance testing, and performance/load testing.

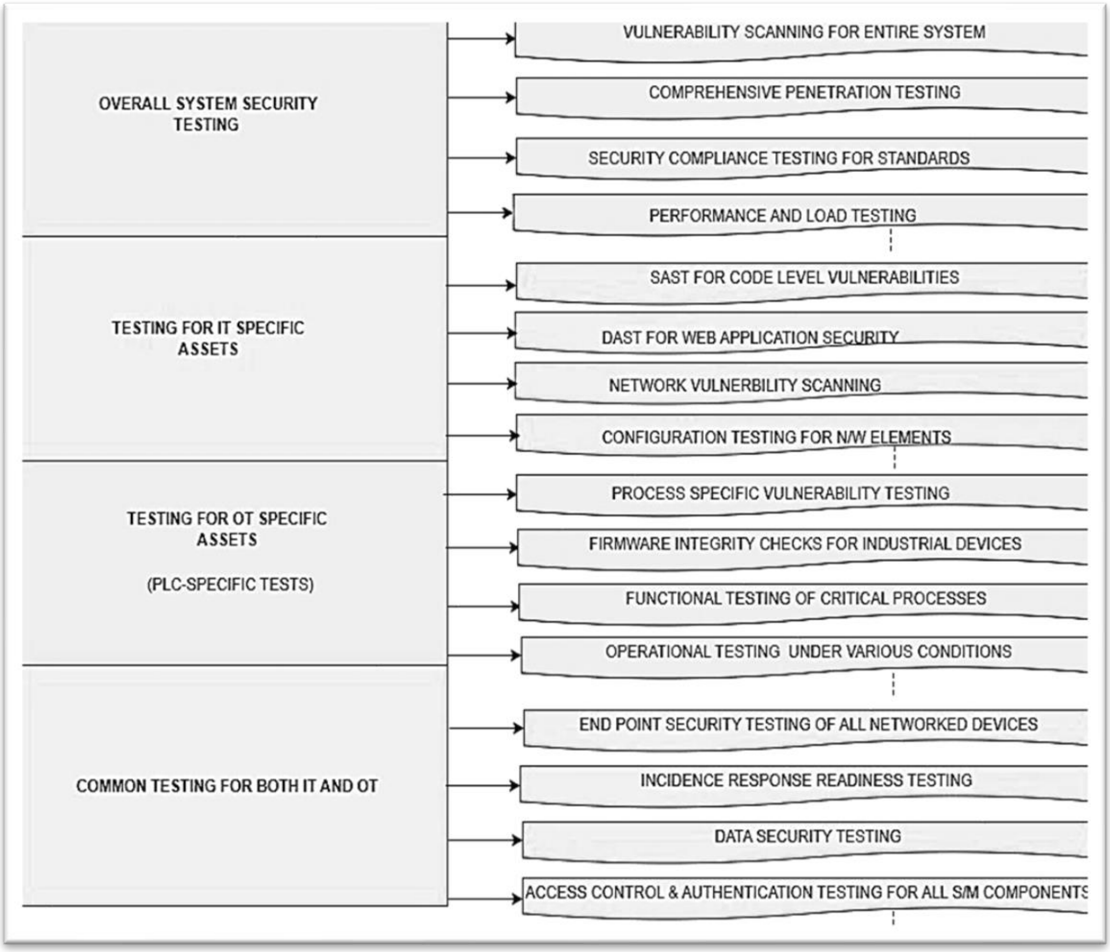

OVERALL SYSTEM SECURITY TESTING
VULNERABILITY SCANNING FOR ENTIRE SYSTEM
COMPREHENSIVE PENETRATION TESTING
SECURITY COMPLIANCE TESTING FOR STANDARDS
PERFORMANCE AND LOAD TESTING
TESTING FOR IT SPECIFIC ASSETS
SAST FOR CODE LEVEL VULNERABILITIES
DAST FOR WEB APPLICATION SECURITY
NETWORK VULNERBILITY SCANNING
CONFIGURATION TESTING FOR N/W ELEMENTS
TESTING FOR OT SPECIFIC ASSETS
(PLC-SPECIFIC TESTS)
PROCESS SPECIFIC VULNERABILITY TESTING
FIRMWARE INTEGRITY CHECKS FOR INDUSTRIAL DEVICES
FUNCTIONAL TESTING OF CRITICAL PROCESSES
OPERATIONAL TESTING UNDER VARIOUS CONDITIONS
COMMON TESTING FOR BOTH IT AND OT
END POINT SECURITY TESTING OF ALL NETWORKED DEVICES
INCIDENCE RESPONSE READINESS TESTING
DATA SECURITY TESTING
ACCESS CONTROL & AUTHENTICATION TESTING FOR ALL S/M COMPONENTS

Figure 12: Comprehensive security testing phase

Notably, the overall System Security Testing includes vulnerability scanning to identify issues such as outdated software, missing security patches, incorrect configurations, and open ports . These vulnerabilities are assessed based on their severity using the Common Vulnerability Scoring System (CVSS). Subsequently, penetration testing tools like Metasploit, Burp Suite, Kali Linux, and Nmap can be utilized to simulate potential cyberattacks and identify points of compromise within the system.

A critical aspect of the vulnerability scanning process is the meticulous examination of both authenticated and unauthenticated scans across the entire IACS network. This approach ensures a thorough identification of vulnerabilities that could pose risks to the system's integrity and functionality. The findings from these scans could be compiled into detailed reports, emphasizing the urgency of addressing the identified flaws promptly. Additionally, the use of black-box, white-box, and grey-box testing methodologies can aid in simulating various cyberattack scenarios and provides valuable insights into potential attacker methods.

IT-specific tests are integral to ensuring the security of IT assets within the IACS environment. These tests include Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST), network vulnerability scanning, fuzz testing, and configuration testing. Notably, SAST involves automated source code analysis to identify potential vulnerabilities, while DAST focuses on uncovering security flaws within actively used applications.

Tools such as Qualys and Rapid7 are essential for routine network vulnerability scanning, highlighting open ports, outdated protocols, and potential configuration errors. Moreover, specialized software like Tripwire, ManageEngine, Nipper, or Firemon enables comprehensive evaluations of network device configurations to ensure adherence to industry security policies.

For OT-specific tests targeting industrial processes and firmware components, specialized tools such as Wireshark and Modbus Poll are employed for process-specific vulnerability testing. These tools assess the security of industrial protocols and detect vulnerabilities within essential industrial processes, ensuring operational resilience and security. Additionally, Firmware Analysis Toolkit is utilized for regular integrity checks of industrial device firmware, identifying any signs of tampering or malicious implants. Functional testing of critical processes and operational testing under various environmental conditions further enhances the system's robustness and adaptability.

Common testing approaches for both IT and OT assets, including endpoint security testing, incident response readiness testing, data security testing, and access control, authentication, and authorization testing, ensure a unified and robust security framework across the entire IACS environment. These tests are aligned with industry standards such as NIST SP 800-53 and the

IEC 62443 series, providing comprehensive guidelines for establishing secure access controls and authentication protocols.

By integrating these diverse testing methodologies, organizations can conduct in-depth risk assessments to identify and mitigate potential risks within the PLC-based IACS system. These strategies enhance the system's security resilience, reduce vulnerabilities to cyber threats, and align with best practices recommended by industry standards.

Compliance with established IACS security standards, such as IEC 62443 or NIST SP 800-82, is paramount for safeguarding critical infrastructure. This includes rigorous security compliance testing to verify system conformance to predefined standards and regulations. Notably, tools such as Metasploit and Core Impact are employed to create simulated versions of real-world cyberattacks, enhancing the system's resilience against potential threats. Furthermore, protocol analyzers like Wireshark are utilized to monitor network traffic and detect anomalies or security vulnerabilities.

Stress testing plays a vital role in assessing the performance and scalability of the IACS system. By designing and executing load tests, organizations can evaluate how the system handles peak workloads without compromising performance. Continuous monitoring of response times, resource utilization, and system scalability enables proactive adjustments to optimize system performance.

Additionally, the implementation of stress testing methodologies will align properly with the recommendations of industry standards such as IEC 62443 and NIST SP 800-82. By integrating these diverse testing methodologies, organizations can conduct in-depth risk assessments to identify and mitigate potential risks within the PLC-based IACS systems. These strategies enhance the system's security resilience, reduce vulnerabilities to cyber threats, and align with best practices recommended by industry standards.

5.1.4 Comprehensive Risk Assessment

The security testing framework for IACS systems relies heavily on the results of the detailed risk assessment phase to guarantee the overall security posture is strong and reliable. A thorough risk assessment strategy is needed as is in Figure 13, one that investigates all aspects of the IACS environment, from the networks and devices to the protocols and operational assets. The framework seeks to provide a comprehensive understanding of the existing vulnerabilities and threats by conducting an extensive and systematic evaluation of potential risks, thereby allowing organisations to develop effective strategies for risk mitigation and management.

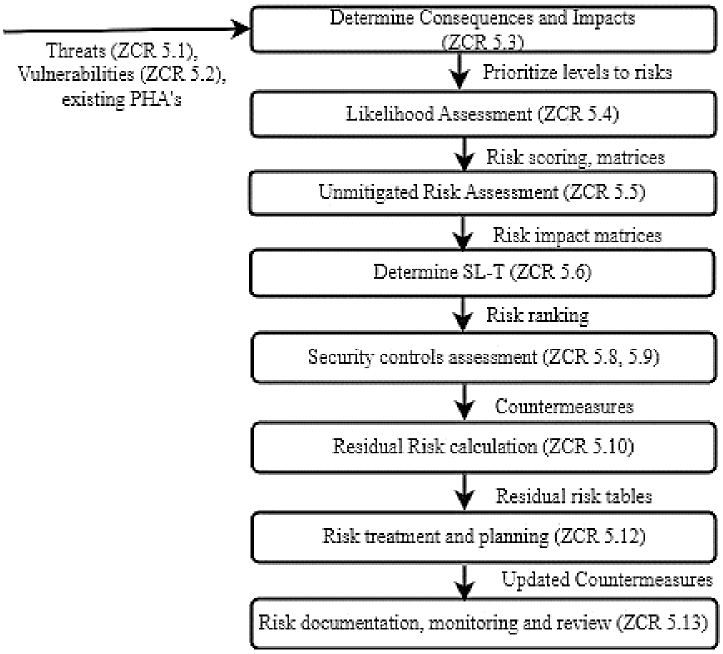

Threats (ZCR 5.1),
Vulnerabilities (ZCR 5.2),
existing PHA's
Determine Consequences and Impacts (ZCR 5.3)
Prioritize levels to risks
Likelihood Assessment (ZCR 5.4)
Risk scoring, matrices
Unmitigated Risk Assessment (ZCR 5.5)
Risk impact matrices
Determine SL-T (ZCR 5.6)
Risk ranking
Security controls assessment (ZCR 5.8, 5.9)
Countermeasures
Residual Risk calculation (ZCR 5.10)
Residual risk tables
Risk treatment and planning (ZCR 5.12)
Updated Countermeasures
Risk documentation, monitoring and review (ZCR 5.13)

Figure 13: Detailed Risk Assessment

This process helps analyze potential security issues and their effects. It involves analyzing vulnerabilities, threats, and repercussions of security breaches. Specialized tools and methodologies can be used to conduct a thorough analysis of the IACS infrastructure. Security assessment questionnaires tailored to the IACS environment ensure a comprehensive understanding of potential threats and gaps.

Vulnerabilities can be assessed for exposure and potential impact using tools like CVSS risk scoring matrices and surveys. This process helps businesses focus on the most pressing risks and evaluates the severity of potential security breaches, enhancing the overall understanding of the implications for IACS systems.

By using security control testing tools, we can assess the strength of the existing security measures and make any necessary adjustments to improve them. This in-depth analysis aids in revealing any loopholes or weak spots in the security controls, which can then be remedied to strengthen the overall security posture. In addition, determining the residual risk requires a thorough evaluation of the efficiency of the security controls in place to reduce the known threats. The risk assessment process can be further strengthened by making use of internationally recognised standards such as NIST SP 800-82, ISO/IEC 27001, and the IEC

62443 series. These standards provide structured and systematic approaches to managing and mitigating potential risks in the IACS environment.

Organizations can develop effective risk management strategies that align with industry standards and regulations. These frameworks provide comprehensive guidelines and best practices for addressing security concerns unique to IACS systems. Risk assessment involves using risk prioritisation matrices and ranking techniques to classify and rank threats based on severity and potential impact. This method helps allocate resources and prioritize risk response activities, improving risk management strategies and strengthening IACS security against vulnerabilities and threats.

5.1.5 Incident Response Phase

After conducting a thorough risk assessment, the phase of incident response within the IACS systems becomes pivotal. It necessitates the development of a tailored incident response plan, precisely outlining steps to take in case of a security breach or incident. To create efficient plans, organizations can utilize incident response planning methodologies and frameworks tailored for IACS environments. Furthermore, regular incident response training and simulations are crucial to ensure the response team is well-prepared to act swiftly and effectively.

Utilizing various incident response training tools and software solutions, teams can practice responding to realistic scenarios, including cyberattacks like ransomware or network breaches. These simulations refine their strategies and decision-making processes, bolstering readiness for diverse security incidents.

5.1.6 Mitigation and Remediation Phase

The Mitigation and Remediation phase is a crucial part of the incident response process for IACS systems. It involves the swift detection, containment, and resolution of security incidents. This phase involves the use of various tools and methodologies to address the root causes of the incident and prevent its recurrence. The primary strategy is the implementation of system and software patches and updates to mitigate vulnerabilities and rectify security flaws. This proactive approach reduces the potential for exploitation by malicious individuals or entities. The Mitigation and Remediation phase also involves the deployment of intrusion detection and prevention systems (IDPS), which continuously monitor network traffic to detect and respond to suspicious or malicious activities in real-time.

This proactive approach minimizes the risk of successful attacks and promotes a secure operational environment for critical industrial processes. Comprehensive security audits and assessments are also conducted to identify vulnerabilities or weaknesses within the system. These evaluations provide valuable insights for the development of targeted security controls and measures. Incident response playbooks and protocols are also adopted to ensure a swift and coordinated response in case of a security incident. By integrating these strategies and tools, organizations can establish a proactive and robust security posture for their IACS environments, fostering a culture of continuous improvement and vigilance towards security. This approach ensures the safety and reliability of critical industrial processes.

5.1.7 Documentation and Reporting Phase

Documentation and reporting procedures should be as thorough as possible throughout the earlier phases of risk management, including the Initial Risk Assessment and the Detailed Risk Assessment. These practices serve as the fundamental basis for efficient risk management. The maintenance of detailed records of identified risks, threat prioritization, and risk treatment strategies is required to maintain compliance with the standards established by NIST and IEC 62443 during these stages. Various EU regulations stress the importance of having proper documentation of all the required procedures [48] in order to pass the test of compliance.

By integrating this comprehensive documentation and reporting practices across the various phases of the security testing framework, it is possible to ensure a holistic approach to risk management and incident response. This gives organizations the ability to effectively identify, mitigate, and document security threats and vulnerabilities that exist within their IACS environment. This preventative strategy makes it easier to comply with regulations, encourages continuous improvement, and strengthens the overall security resilience of IACS.

5.1.8 Continuous Monitoring Phase

Continuous Assessment and Auditing Phase is an essential component that plays a role in maintaining compliance standards and securing the facility. Organizations can proactively identify and address security gaps, thereby fortifying the overall security posture of their IACS infrastructure, if they make use of robust assessment techniques and relevant tools. During this phase, it is essential to implement regular vulnerability assessments to identify potential security flaws and threats that may exist.

Tools such as OpenVAS and Nessus make it possible to perform continuous scans of networked devices and systems. As a result, these tools provide real-time insights into newly discovered vulnerabilities and potential attack vectors. The importance of conducting vulnerability assessments on a regular basis is brought to light by adhering to industry standards such as NIST and IEC 62443. This enables businesses to keep a watchful approach to the detection and mitigation of threats.

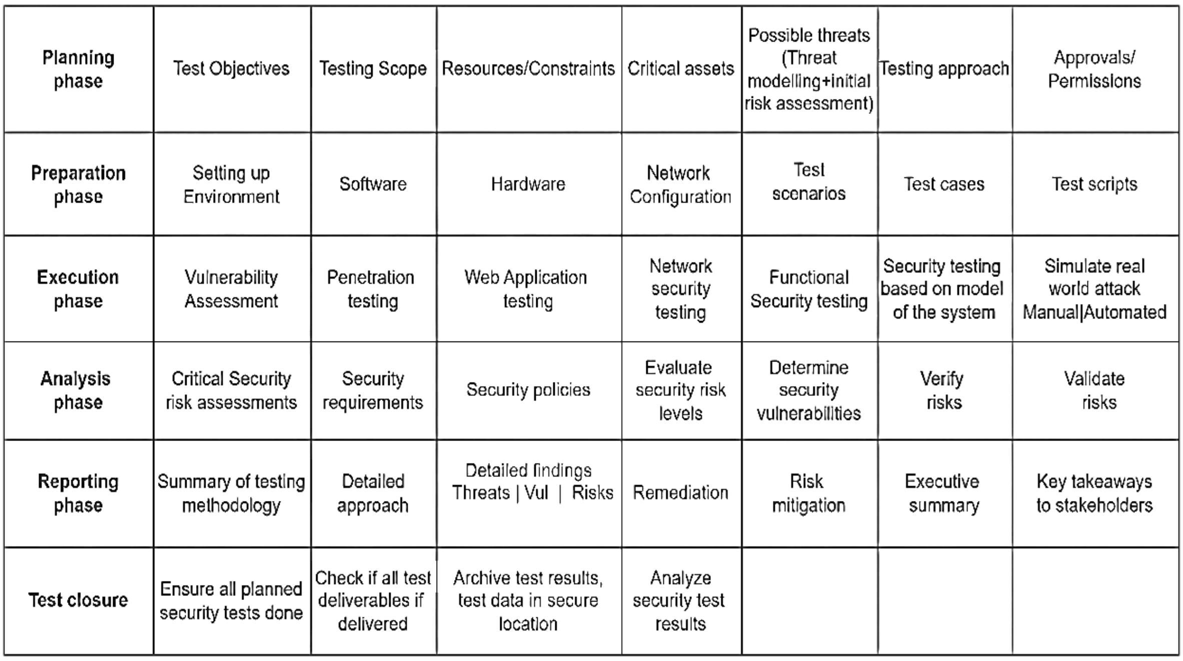
5.1.9 Feedback Loops

Feedback loops in the framework are crucial not only in determining the SuT and associated security standards, but also provide a dynamic and iterative methodology for enhancing the testing strategy and ensuring congruence with growing security requirements, especially when changes to the testing scope are needed. Feedback loops require continuous collaboration among stakeholders, including business executives, security professionals, system administrators, and developers.

They enable continuous assessment of potential risks and their implications for the SUT, enabling teams to identify vulnerabilities and prioritize critical assets. The cyclical nature of feedback loops helps teams enhance security objectives, identify critical components, determine appropriate security standards, and evaluate the need for additional measures. They ensure alignment with the organization's goals and align selected security measures with the strategic trajectory. Continuous evaluations of the scope of security testing optimize resource allocation. To help organizations follow all these phases of the proposed framework, a working template (Figure 14) has been designed which includes all the major phases and sub-phases has been created that can act as a Checklist for the organizations.

5.2 Security Testing Template

The Comprehensive Security Testing Framework is designed to provide a structured approach for evaluating and enhancing the security posture of IT and OT assets within an organization.



Planning phase	Test Objectives	Testing Scope	Resources/Constraints	Critical assets	Possible threats (Threat modelling+initial risk assessment)	Testing approach	Approvals/ Permissions
Preparation phase	Setting up Environment	Software	Hardware	Network Configuration	Test scenarios	Test cases	Test scripts
Execution phase	Vulnerability Assessment	Penetration testing	Web Application testing	Network security testing	Functional Security testing	Security testing based on model of the system	Simulate real world attack Manual|Automated
Analysis phase	Critical Security risk assessments	Security requirements	Security policies	Evaluate security risk levels	Determine security vulnerabilities	Verify risks	Validate risks
Reporting phase	Summary of testing methodology	Detailed approach	Detailed findings Threats | Vul | Risks	Remediation	Risk mitigation	Executive summary	Key takeaways to stakeholders
Test closure	Ensure all planned security tests done	Check if all test deliverables if delivered	Archive test results, test data in secure location	Analyze security test results			

Figure 14: Security Testing Framework working template

This framework encompasses a range of testing methodologies, tools, and best practices that can be formulated to a working template (Figure 14) that can guide the organisations to identify, assess, and mitigate security risks effectively.

5.3 Features of the Framework

The key features of this security testing framework, and how they contribute to a robust security posture for PLC-based IACS systems is discussed as follows:

The security testing framework for PLC-based IACS systems is designed to ensure robust security. It aligns with the IEC 62443 standard, incorporating comprehensive and multi-layered testing to maximize coverage and identify vulnerabilities. The framework prioritizes vulnerabilities based on their potential impact and likelihood of exploitation, allowing for focused mitigation and remediation efforts. It is adaptable to PLC-based systems, integrating knowledge of PLC architectures, communication protocols, and control logic.

The framework's planning phase defines the scope and objectives for the testing process, allowing it to be tailored to individual system needs. Continuous assessment and auditing ensure the framework adapts to evolving threats and maintains a robust security posture. The framework emphasizes incident response, with a dedicated incident response management component to minimize potential damage. The framework maps to relevant EU regulations like the CRA, NIS 2 Directive and RED-DA , ensuring compliance with data protection and critical infrastructure security standards.

The framework incorporates proactive measures, comprehensive evaluation, focused mitigation, quick incident response, traceability, auditability, and compliance with regulations. It also includes identifying assets, developing threat models, and conducting initial risk assessments to anticipate future threats. The comprehensive evaluation includes IT and OT aspects to minimise risks throughout the entire system. Established incidence response procedures reduce damage and operational interruptions. Documentation serves as a point of reference for previous evaluations and decision-making.

5.4 Workflow

The process involves selecting the SUT and the regulation that we are considering working with, identifying, and classifying all hardware, software, network devices, and data within a PLC-based IACS system. Potential threats are brainstormed and assessed, combining asset criticality with threats. Initial strategies are established, and clear goals for security testing are set. Tests are executed for overall system security, IT and OT specific tests, and common procedures.

Vulnerabilities are identified and assessed, and risks are categorized, ranked, and prioritized based on severity and likelihood. Procedures and actions are to be defined for effective response to security breaches. Detailed records of vulnerabilities, test results, recommendations, and remediation strategies need to be maintained. Regular re-assessments and audits are to be performed to identify changes and emerging threats.

5.5 Design

This security testing framework, designed to align with the IEC 62443 standard, offers a comprehensive approach to securing PLC-based IACS systems. It encompasses several essential phases, each fulfilling a specific role in the security assessment process. These components include:

The framework for securing PLC-based IACS systems involves a comprehensive approach to security. The initial phase involves thorough planning and Pre-Assessment activities, including asset discovery and classification, threat modeling, risk assessment, and setting scope and objectives for security testing. The framework uses a multi-layered approach to comprehensively assess the security posture of the system, identifying vulnerabilities and weaknesses across various components. A critical risk assessment is performed after comprehensive testing, identifying, and classifying risks, evaluating their potential impact, and prioritizing threats based on severity and likelihood.

Existing security controls are assessed, and residual risks are calculated after mitigation strategies are implemented. Risk treatment and planning define actions to address identified risks, and continuous monitoring and review ensure the effectiveness of risk management strategies over time. Additional components of the framework include incident response management, mitigation and remediation, documentation and reporting, and continuous assessment and auditing.

5.6 Implementation

Due to the highly fragile nature of crane control systems, the direct implementation of the developed security testing framework poses significant challenges and potential dangers. The intricate interplay of these systems requires meticulous handling to avoid disruptions that could impact critical processes. Therefore, it has become impossible for our organization to immediately implement the comprehensive framework.

Adding to this complexity is the impending wave of cybersecurity regulations emerging from the EU. Recognizing the necessity to comply with these regulations, our organization has made a strategic decision to approach the implementation of the security testing framework phase by phase. This phased approach will enable us to navigate through the intricate landscape of compliance requirements, ensuring a safer and more secure environment for our crane control systems.

In the current scenario, it is evident that early adoption of the framework could be premature, given the unique challenges posed by the crane control systems. However, Konecranes is acutely aware of the pressing need to act before it becomes too late or obsolete to implement robust security measures. Security compliance has already become a crucial business case, urging us to prepare diligently for the journey ahead.

Despite the inability to implement the framework directly, we have endeavoured to provide an illustrative walkthrough of its application using an IT and OT asset from the PLC-based crane control system. This example serves to highlight the framework's potential impact and the steps involved if implemented in real-time scenarios.

To embark on this journey towards implementation, Konecranes envisions this comprehensive approach:

Firstly, assembling an expert security team with a blend of IT and OT security expertise will be crucial. This team will play a pivotal role in understanding the complexities of the crane control systems and designing tailored security measures. Secondly, acquiring necessary tools such as vulnerability scanners like Nessus or OpenVAS, penetration testing tools like Metasploit or Kali Linux, and possibly SAST/DAST tools based on the system's programming languages will be essential. Standardized procedures will be established for each phase of the framework.

This includes activities like asset discovery using automated tools, employing methodologies such as STRIDE or PASTA for threat modeling, and utilizing a defined risk matrix for risk assessment. A thorough testing phase will ensue, where the framework will be applied to identify vulnerabilities and assess risks within the crane control systems. Following testing, a critical risk assessment will prioritize mitigation strategies and determine acceptable residual risk levels. Development of incident response plans, playbooks, and mitigation procedures will be crucial to effectively address vulnerabilities as they are identified. This may involve tools for vulnerability patching and configuration updates, continuous assessments and will ensure ongoing effectiveness against evolving threats and system changes.

Finally, creating a realistic testbed environment that replicates the production environment of the crane control systems will allow for realistic testing without impacting critical processes. This phased approach, while acknowledging the present limitations on direct implementation, sets the groundwork for a systematic and comprehensive security framework. By taking measured steps and preparing diligently, Konecranes aims to establish a robust security posture aligned with emerging cybersecurity regulations and the unique challenges posed by our crane control systems.

5.7 Answers to the Research Questions

RQ1: What are the essential components of a Security Testing Framework tailored to IACS environments?

The framework was developed by identifying and assessing critical components like PLCs, HMIs, SCADA systems, and network devices. The framework follows a structured approach, including planning, comprehensive testing, critical risk assessment, incident response, documentation, and continuous assessment. Threat modeling techniques are used to identify potential vulnerabilities, while vulnerability assessment tools identify system weaknesses. The framework includes various testing phases for IT and OT assets, a comprehensive risk assessment, incident response testing procedures, and meticulous documentation and reporting standards to document findings, recommendations, and compliance and auditing reports which concludes that it has addressed the RQ1.

RQ2: How can these components be adapted to address the specific security challenges posed by PLC-based IACS systems?

The Security Testing Framework has been adapted to address the security challenges of PLC-based IACS systems. It focuses on identifying vulnerabilities unique to PLCs, using OT-specific testing with specialized tools, tailoring risk assessment to operational impact, developing incident response plans for minimal disruption, and ensuring usability for diverse industrial automation teams. The framework also includes testing communication protocols commonly used in PLC environments, such as Modbus or Profibus, to verify secure configurations. The integration of specialized PLC-specific testing tools enhances the framework's efficacy in assessing PLC security, addressing RQ 2.

RQ3: In what ways can the framework be aligned with the principles of ISA/IEC 62443 standards while ensuring compliance with EU regulations?

The Security Testing Framework was developed to align with ISA/IEC 62443 standards and EU regulations. It incorporates concepts like the Security Levels, mapping each phase to relevant sections of the standard. The framework also incorporates Security Levels to tailor security assessments to the varying levels of protection and ensures compliance with evolving EU regulations concerning IACS cybersecurity, providing organizations with a roadmap for regulatory compliance. Continuous monitoring mechanisms enable organizations to adapt their security measures in a timely manner to ensure the framework is compliant with ISA/IEC 62443 standards while addressing specific security challenges inherent to PLC-based IACS systems and EU regulatory requirements which thereby answers RQ 3. The framework uses well-established methodologies, such as threat modelling, risk assessment, and a comprehensive testing phase, to identify and mitigate security vulnerabilities across IT and OT assets.

6 Discussion

This chapter discusses the study's results, including confirmed and refuted findings, interpretations, contributions, implications, limitations, and validity threats. The research problem was the lack of a security testing framework for crane control systems, specifically Konecranes. The framework was developed to address this issue, providing a comprehensive security assessment for the company. The framework was confirmed to provide all-round security for IACS systems, and no issues were found that would prevent its implementation or further improvement. The general security testing framework is a significant milestone in the thesis, providing a solid foundation for addressing concerns about IACS systems. It incorporates threat modeling for proactive risk assessment and comprehensive understanding of vulnerabilities.

The testing phase examines identified weaknesses, enabling the implementation of robust strategies to mitigate their effects. The framework's adaptability to various IACS environments highlights its potential as a practical solution across various industrial sectors. It emphasizes preventative security measures and encourages a culture of resilience. Compliance with industry standards and regulatory requirements ensures its relevance and application despite the ever-changing threat landscape. Although iterations demonstrate the framework's success, additional modifications and adaptations may be necessary to improve its implementation in IACS environments.

6.1 Revisiting the Research Questions

6.1.1 RQ 1

In the initial iteration of the thesis, Research Question 1 was meticulously explored through a comprehensive synthesis of existing literature on security testing frameworks for IACS systems. The methodology employed involved an exhaustive review of scholarly works to distil the essential components of such a framework. The resulting framework, as synthesized in Iteration 1, comprised elements such as asset discovery, threat modelling approaches, risk assessment methodologies, and recommended testing procedures and incident response mechanisms. These components have been meticulously integrated to ensure a comprehensive and multi-layered approach to security testing, aligning with industry best practices. Upon reflection, the iterative process of framework development highlighted the necessity of a robust architecture within IACS environments.

This framework, while designed to be broadly applicable to diverse IACS systems, was particularly focused on providing a foundational structure for understanding and implementing security testing practices. Its strengths lie in its adaptability across industries, offering a blueprint for organizations to enhance their cybersecurity postures. However, limitations were also identified, notably in the depth of coverage for specific attack vectors and the need for further validation in real-world industrial environments. However, Iteration 1 served as a crucial steppingstone, laying the groundwork for subsequent refinements and applications in the evolving landscape of industrial cybersecurity.

6.1.2 RQ 2

The second iteration of a thesis focused on applying a modified security testing framework to the theoretical landscape of PLC-based IACS systems. The thesis incorporated safety aspects into the framework, addressing the cyber-physical implications of potential threats and recognizing the critical intersection of cyber and operational safety within these systems. Building on the foundational components identified in the first iteration, it aimed to fortify systems against cyber-attacks and mitigate risks that could compromise operational safety. The framework was honed through theoretical assessments and example illustrations to detect vulnerabilities impacting both security and safety, ensuring a robust defense mechanism against evolving threats. This integration represents a significant advancement in aligning cybersecurity practices with operational resilience within PLC-based IACS systems.

6.1.3 RQ 3

In addressing Research Question 3, the third iteration of the thesis was more about the alignment of the security testing framework with the principles and requirements outlined in the ISA/IEC 62443 standard. This pivotal phase sought to harmonize the framework with the complex landscape of EU cybersecurity regulations, recognizing the significance of compliance in safeguarding IACS systems. By mapping each phase of the framework to the corresponding guidelines within the ISA/IEC 62443 standard, a structured approach was established to ensure adherence to recognized security best practices and the strategic integration of ISA/IEC 62443 principles into the framework, enhancing its robustness and effectiveness.

A notable addition was the incorporation of threat mitigation testing within the framework's threat modeling phase, aligning with the recommendations of the ISA/IEC 62443 standard to fortify defenses against potential threats. By considering the nuanced requirements of ISA/IEC

62443 and relevant EU regulations such as the NIS Directive and CRA, the framework not only meets stringent compliance standards but also enhances critical infrastructure security. This alignment underscores the thesis's commitment to developing a comprehensive and compliant security testing framework tailored to the unique challenges of PLC-based IACS systems within the regulatory framework of the European Union.

6.2 Contributions and Implications

The security testing framework for PLC-based IACS systems provides a comprehensive, adaptable, and standards-aligned approach to securing these critical industrial systems, improving their security posture, operational resilience, and regulatory compliance.

6.2.1 Contributions

This research contributes to the field of industrial cybersecurity by addressing a critical gap in existing frameworks and standards through the development of a specialized security testing framework for PLC-based IACS systems. By providing organizations with clear guidance on cybersecurity testing and compliance, this research empowers them to strengthen their cybersecurity posture and navigate the evolving regulatory landscape effectively. This thesis focuses on the development of a specialized Security Testing Framework specifically designed for PLC-based IACS systems.

The framework addresses unique challenges such as limited computing capabilities, exclusive communication protocols, and real-time operational requirements. It synthesizes existing literature, identifies essential components, and adapts them to the PLC context, providing a structured approach to assessing and enhancing the security posture of PLC-based IACS systems.

The framework also incorporates safety-security choke points, ensuring that security measures do not compromise the safety and integrity of critical industrial processes, enhancing the overall resilience of IACS systems. The framework is meticulously aligned with the internationally recognized ISA/IEC 62443 standard, ensuring compliance with best practices in IACS cybersecurity. The proposed framework offers a practical solution for organizations to strengthen the security of their PLC-based IACS systems by identifying vulnerabilities, conducting thorough testing, and providing mitigation strategies. It serves as a guiding resource for industry professionals, cybersecurity experts, and organizations operating in the IACS domain, providing a roadmap for implementing robust security measures tailored to the specific needs of PLC-based control systems. The contributions of this thesis extend beyond academic research, offering practical tools, methodologies, and guidelines to enhance the cybersecurity posture of PLC-based IACS systems.

6.2.2 Implications

The framework aims to enhance the security posture of the IACS systems by enabling organizations to identify vulnerabilities and take proactive measures to mitigate risks. This results in a more robust security posture, reducing the risk of cyberattacks and system disruptions. The framework also focuses on maintaining operational resilience by minimizing disruption to critical processes during assessments and mitigation efforts. It aligns with recognized standards and regulations, ensuring compliance with data protection and critical infrastructure security requirements. F

Furthermore, the framework contributes to standardization and best practices within the IACS domain by providing a well-defined approach to security testing. This approach fosters knowledge sharing and collaboration within the industry, creating a more secure environment for industrial automation systems.

The implications of this thesis on cyber safety and regulations are profound. Organizations adopting this framework can better protect their IACS environments, aligning with stringent data protection laws and critical infrastructure security mandates. Compliance with such regulations becomes more manageable, as the framework provides a systematic and comprehensive approach to security testing. In terms of research implications, our framework could be considered as a candidate for the harmonized standard framework, given its broader scope compared to the IEC 62443 standard.

The integration of security and safety within the framework also presents an area for further investigation. The notion of a "security and safety marriage" is explored within our work, demonstrating how both aspects can be integrated and implemented for extensive coverage. This aspect deserves careful study by the research community to explore its full potential and implications. For the industry, the framework offers practicality and effectiveness.

Companies like Konecranes are already planning to implement this framework to enhance their IACS security and comply with regulations. This adoption signifies a shift towards a more secure and standardized approach to industrial cybersecurity.

As organizations increasingly recognize the importance of cybersecurity in their operations, frameworks such as ours provide the necessary guidance and structure for effective implementation. Ultimately, the effectiveness of this framework in changing the world of industrial cybersecurity hinges on proper implementation and ongoing maintenance by organizations. It calls for the allocation of necessary resources and expertise to maintain a secure IACS environment, ensuring the resilience, integrity, and security of critical industrial infrastructure in our ever connected and digitized world.

6.3 Limitations

While the developed framework offers valuable tools for securing PLC-based IACS systems, there are certain limitations to consider before implementation: The Security Testing Framework developed in this thesis offers valuable tools for securing PLC-based IACS systems, but it has limitations before implementation. The framework has not yet been practically implemented in live IACS environments, which may introduce unforeseen challenges and nuances. It also lacks coverage of process security controls, which are crucial for regulatory compliance and overall system integrity.

Regulatory compliance requires adherence to rigorous process security requirements, and the framework may need to be extended to include process security testing and compliance. The framework should undergo regular updates to remain effective and adapt to new vulnerabilities and evolving regulatory landscapes. Resource and expertise constraints are also a concern, as implementing a comprehensive security testing framework requires substantial resources, technical expertise, and organizational commitment. Small and medium-sized enterprises (SMEs) or organizations with limited cybersecurity budgets may find it challenging to allocate resources for extensive testing and compliance efforts.

Addressing these constraints and providing cost-effective implementation strategies will be essential for broader adoption of the framework. By acknowledging these limitations, organizations can approach the framework realistically and take steps to mitigate them. While it's not a foolproof solution, the framework still offers valuable guidance and a structured approach for securing PLC-based IACS systems, ultimately contributing to a more secure and robust environment for critical industrial automation operations.

6.4 Validity Threats

This section defines validity threats of this study based on the definition by Runeson and Höst [43].

6.4.1 Construct Validity

The Construct validity addresses the gap between the concepts presented and the interpretations individuals may have of these concepts, essentially bridging the theory and practice divide. In the context of this research, it was crucial to ensure that the understanding of key concepts within the developed security testing framework was consistent among stakeholders. To mitigate this risk, various steps were taken. In focus group discussions and interviews, participants were probed on their interpretations and understanding of the framework's key components. This included questions about their opinions and perceptions of security testing methods, risk assessment techniques, and incident response planning.

Moreover, to ensure clarity and consistency, a clear and precise definition of each concept within the framework was provided. This helped align participants' interpretations with the intended meanings, reducing the risk of misinterpretation or misunderstanding. Additionally, examples and practical scenarios were shared to illustrate the application of these concepts in real-world industrial settings.

This approach not only aided in clarifying any ambiguities but also provided stakeholders with a practical understanding of how the framework could be implemented. By addressing potential discrepancies in understanding through clear definitions, practical examples, and active engagement with stakeholders, the research aimed to enhance the construct validity of the developed security testing framework. This approach helped bridge the gap between theory and practice, ensuring that the framework's concepts were accurately interpreted and applied in industrial contexts.

6.4.2 Internal Validity

To bolster internal validity, various strategies were implemented to address potential limitations and ensure the accuracy of the research findings. Recognizing the potential limitations of focus group discussions, private discussions were conducted with stakeholders to gather deeper insights and perspectives on the security testing framework. A diverse group of security engineers with varied backgrounds and expertise were carefully selected for the study. Their diverse perspectives provided a comprehensive evaluation of the framework's usability and effectiveness in different industrial settings.

Triangulation and member checking techniques were employed to confirm the reliability of the gathered information. Data from interviews, focus groups, and private discussions were cross verified, ensuring consistency and reducing the risk of bias. To mitigate the challenge of isolating the framework's impact on overall security posture, clear documentation of the IACS system's security baseline before implementation was emphasized.

This baseline serves as a reference for evaluating the framework's effectiveness. Implementing the framework in phases was suggested to allow targeted evaluation of its impact on specific components or functionalities of the IACS system.

6.4.3 External Validity

Firstly, the study evaluated a security testing framework within the context of a crane core platform in an industrial automation system. As such, the findings are specific to Konecranes and may not be directly generalizable to other IACS systems. To mitigate this limitation, documenting the customization process of the framework for this specific environment was emphasized. This documentation can serve as a valuable reference point for future adaptations and implementations in similar settings, enhancing the framework's potential for broader applicability.

Secondly, the validity of the framework could be affected by changes to industry standards such as ISA/IEC 62443 and EU regulations. To mitigate this risk, ongoing monitoring, and updates to the framework in alignment with evolving standards and regulations were recommended. This proactive approach aims to minimize inconsistencies or gaps in compliance and ensures the framework remains relevant and effective over time. Furthermore, while the study serves as a case study within a specific company, it also provides a foundation for further research and development in the automation industry.

Researchers and practitioners interested in a standardized approach to security testing can extract valuable insights and methodologies from this study. The framework's components and methodologies can be adapted and applied in diverse IACS settings, promoting a more systematic and rigorous approach to cybersecurity.

7. Conclusion

7.1 Summary

The study explored the Security Testing Frameworks specifically designed for PLC-based IACS security. It begun with an Introduction that emphasizes the importance of security in safeguarding industrial processes and the need for a specialized framework to combat evolving cyber threats. The theoretical background was presented in Chapter 2, provided an extensive literature survey on existing Security Testing Frameworks tailored for IACS. Sub-chapters delved into the nuances of security frameworks and standards specific to IACS security, including an analysis of EU regulations governing industrial cyber security.

Chapter 3 outlined the Design Science Research approach, providing a systematic framework for the design, development, and evaluation of the proposed Security Testing Framework. Chapter 4 describes the development process of the framework during three iterations in the regulative cycle framework, highlighting challenges, details, and results. Chapter 5 revisited the research questions and presents the results regarding the framework's illustration. Chapter 6 presented the findings, their fit with existing knowledge, limitations, threats to the validity, and mitigation strategies.

7.2 Concluding Remarks

In conclusion, this thesis developed a tailored Security Testing Framework for PLC-based IACS systems, aligning with ISA/IEC 62443 standards and EU cyber security regulations. Through iterative design and refinement, the framework now offered a structured approach to identifying and managing cyber threats in PLC-based IACS environments. The results provided a practical roadmap for organizations seeking to enhance the security of their critical industrial infrastructure. This collaborative effort bridges academia and industry, providing a tangible tool for identifying, mitigating, and managing cyber risks in real-world settings.

Looking ahead, the framework's potential for practical application is promising. Future research can explore its implementation across diverse industrial contexts, evaluating its effectiveness in bolstering resilience against cyber-attacks. Continuous updates and adaptations will be crucial to keep pace with evolving cyber security threats. This work contributes not only to the field of IACS security but also provides a valuable resource for organizations aiming to safeguard their critical systems. The insights gained and framework developed here lay a foundation for ongoing advancements in industrial cyber security, ensuring the reliability and security of industrial processes in the digital era.

7.3 Future Work

Future work on the Security Testing Framework for PLC-based IACS systems shall prioritize the integration of process security testing methodologies, with a keen focus on enhancing safety considerations within the framework. This entails delving into human-machine interactions, operational protocols, and physical security aspects to ensure a holistic approach to system security. By integrating safety assessments, the framework aims to provide a comprehensive view of vulnerabilities within the industrial process, enhancing overall system resilience against both cyber threats and potential safety hazards.

The framework can also be refined and expanded for its threat modeling techniques incorporating advanced methods such as attack tree analysis and dynamic, automatic threat modeling. These enhancements will offer deeper insights into potential attack vectors and practices, aiding in the prioritization of mitigation strategies based on the severity of threats. Additionally, the next phase of research shall focus on the practical implementation and validation of the framework in real-world PLC-based IACS environments. Collaborating closely with industry partners, the aim is to deploy the framework in operational settings to assess its effectiveness. This hands-on approach will gather valuable feedback from practitioners, allowing for usability enhancements and adjustments to better suit industrial needs.

Furthermore, a crucial aspect of future work involves automating the security testing process within the framework. This automation will streamline assessments and testing procedures, improving efficiency and accuracy in identifying vulnerabilities and potential threats. By automating key aspects, the framework can offer real-time insights into the security posture of IACS systems, enabling swift and proactive responses to emerging cyber risks. Integrating the framework with other relevant regulations and standards is also a priority for future research. This includes aligning the framework with emerging industrial security standards and regulations to ensure its compliance and relevance in the evolving cybersecurity landscape. Moreover, exploring its adaptation to emerging technologies like IoT and edge computing will expand the framework's applicability and effectiveness.

References

1. Pfrang, S., Meier, D., & Kautz, V. (2017). Towards a modular security testing framework for industrial automation and control systems: Isutest. In 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA) (pp. 1-5). IEEE.doi:10.1109/etfa.2017.8247727
2. Priya, N. (2022). Cybersecurity considerations for industrial IoT in critical infrastructure sector. International Journal of Computer and Organization Trends, 12(1), 27-36. doi:10.14445/22492593/ijcot-v12i1p306
3. Milinković, S. A., & Lazić, L. R. (2012). Industrial PLC security issues. In 2012 20th Telecommunications Forum (TELFOR) (pp. 1536-1539). IEEE.doi:10.1109/telfor.2012.6419513
4. Chiara, P. G. (2022). The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements: An introduction. International Cybersecurity Law Review, 3(2), 255-272.doi:10.1365/s43439-022-00067-6
5. Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. Computer Law & Security Review, 52, 105890.doi:10.1016/j.clsr.2023.105890
6. Giorgio Chiara, P. (2022). European Union· Commission Delegated Regulation (EU) 2022/30 Supplementing Directive 2014/53/EU on Radio Equipment: Strengthening Cybersecurity, Privacy and Personal Data Protection of Wireless Devices. European Data Protection Law Review (EDPL), 8(1). doi:10.21552/edpl/2022/1/15
7. Gallina, B., Olesen, T. Y., Parajdi, E., & Aarup, M. (2023). A Knowledge Management Strategy for Seamless Compliance with the Machinery Regulation. In European Conference on Software Process Improvement (pp. 220-234). Cham: Springer Nature Switzerland. doi:10.1007/978-3-031-42307-9_17
8. Kohler, C. (2020). The EU Cybersecurity Act and European standards: an introduction to the role of European standardization. International Cybersecurity Law Review, 1(1), 7-12.doi: 10.1365/s43439-020-00008-1
9. Wagner, M., Borg, M., & Runeson, P. (2023). Navigating the Upcoming European Union AI Act. IEEE Software, 41(1), 19-24.doi:10.1109/ms.2023.3322913

10. O'REILLY, P. A. T. R. I. C. K., & RIGOPOULOS, K. (2020). NIST/ITL CYBERSECURITY PROGRAM. NIST SPECIAL PUBLICATION, 800, 206.doi: 10.6028/NIST.SP.800-206
11. Leander, B., Čaušević, A., & Hansson, H. (2019). Applicability of the IEC 62443 standard in Industry 4.0/IIoT. In Proceedings of the 14th International Conference on Availability, Reliability and Security (pp. 1-8).doi:10.1145/3339252.3341481
12. Monev, V. (2020). Organisational information security maturity assessment based on ISO 27001 and ISO 27002. In 2020 International Conference on Information Technologies (InfoTech) (pp. 1-5). IEEE. doi:10.1109/infotech49733.2020.9211066
13. Sihwi, S. W., Andriyanto, F., & Anggrainingsih, R. (2016). An expert system for risk assessment of information system security based on ISO 27002. In 2016 IEEE International Conference on Knowledge Engineering and Applications (ICKEA) (pp. 56-61). IEEE.doi:10.1109/ickea.2016.7802992
14. Williams, T. J. (1994). The Purdue enterprise reference architecture. Computers in Industry, 24(2–3), 141–158. doi:10.1016/0166-3615(94)90017-5
15. Rea-Guaman, A. M., San Feliu, T., Calvo-Manzano, J. A., & Sanchez-Garcia, I. D. (2017). Comparative study of cybersecurity capability maturity models. In Software Process Improvement and Capability Determination: 17th International Conference, SPICE 2017, Palma de Mallorca, Spain, October 4–5, 2017, Proceedings (pp. 100-113). Springer International Publishing. doi:10.1007/978-3-319-67383-7_8
16. Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., & Lightman, S. (2022). Guide to operational technology (ot) security. National Institute of Standards and Technology: Gaithersburg, MD, USA.doi:10.6028/nist.sp.800-82r3.ipd
17. Kwon, R., Ashley, T., Castleberry, J., Mckenzie, P., & Gourisetti, S. N. G. (2020). Cyber threat dictionary using mitre att&ck matrix and nist cybersecurity framework mapping. In 2020 Resilience Week (RWS) (pp. 106-112). IEEE.doi:10.1109/rws50334.2020.9241271
18. Groš, S. (2021). A critical view on CIS controls. In 2021 16th International Conference on Telecommunications (ConTEL) (pp. 122-128). IEEE. doi:10.23919/contel52528.2021.9495982
19. Dolezilek, D., & Hussey, L. (2011). Requirements or recommendations? Sorting out NERC CIP, NIST, and DOE cybersecurity. In 2011 64th Annual Conference for Protective Relay Engineers (pp. 328-333). IEEE. doi:10.1109/cpre.2011.6035634

20. Bell, R. (2010). Introduction and Revision of IEC 61508. In Advances in Systems Safety: Proceedings of the Nineteenth Safety-Critical Systems Symposium, Southampton, UK, 8-10th February 2011 (pp. 273-291). London: Springer London.doi:10.1007/978-0-85729-133-2_16
21. Piggin, R. S. H. (2013). Development of industrial cyber security standards: IEC 62443 for SCADA and Industrial Control System security. In IET conference on control and automation 2013: Uniting problems and solutions (pp. 1-6). IET.doi:10.1049/cp.2013.0001
22. Kern, M., Taspolatoglu, E., Scheytt, F., Glock, T., Liu, B., Betancourt, V. P., ... & Sax, E. (2020). An architecture-based modeling approach using data flows for zone concepts in industry 4.0. In 2020 IEEE International Symposium on Systems Engineering (ISSE) (pp. 1-8). IEEE. doi:10.1109/isse49799.2020.9272013
23. Yang, J., Zhou, C., Tian, Y. C., & Yang, S. H. (2019). A software-defined security approach for securing field zones in industrial control systems. IEEE Access, 7, 87002-87016. doi: 10.1109/ACCESS.2019.2924800
24. Shaaban, A. M., Kristen, E., & Schmittner, C. (2018). Application of IEC 62443 for IoT components. In Computer Safety, Reliability, and Security: SAFECOMP 2018 Workshops, ASSURE, DECSoS, SASSUR, STRIVE, and WAISE, Västerås, Sweden, September 18, 2018, Proceedings 37 (pp. 214-223). Springer International Publishing. doi:10.1007/978-3-319-99229-7_19
25. Babu, B., Ijyas, T., Muneer, P., & Varghese, J. (2017). Security issues in SCADA based industrial control systems. In 2017 2nd International Conference on Anti-Cyber Crimes (ICACC) (pp. 47-51). IEEE. doi:10.1109/anti-cybercrime.2017.7905261
26. Alsabbagh, W., & Langendörfer, P. (2023). Security of Programmable Logic Controllers and Related Systems: Today and Tomorrow. IEEE Open Journal of the Industrial Electronics Society.doi:10.1109/ojies.2023.3335976
27. Ehrlich, M., Gergeleit, M., Simkin, K., & Trsek, H. (2019). Automated processing of security requirements and controls for a common Industrie 4.0 use case. In 2019 International Conference on Networked Systems (NetSys) (pp. 1-6). IEEE. doi:10.1109/netsys.2019.8854522
28. Dhirani, L. L., Armstrong, E., & Newe, T. (2021). Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap. Sensors, 21(11), 3901.doi:10.3390/s21113901

29. Green, B., Krotofil, M., & Hutchison, D. (2016,). Achieving ICS resilience and security through granular data flow management. In Proceedings of the 2nd ACM workshop on cyber-physical systems security and privacy (pp. 93-101).doi:10.1145/2994487.2994498
30. Bhattacharya, S., Hyder, B., & Govindarasu, M. (2022, September). ICS-CTM2: Industrial Control System Cybersecurity Testbed Maturity Model. In 2022 Resilience Week (RWS) (pp. 1-6). IEEE.doi:10.1109/rws55399.2022.9984023
31. Mlynek, P., Fujdiak, R., Mrnustik, P., Krena, B., & Apvrille, L. (2020). Co-Engineering Gap Analysis of ANSI/ISA-62443-3-3. International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems, 9(1), 1-9.doi:10.11601/ijates.v9i1.285
32. Sandaruwan, G. P. H., Ranaweera, P. S., & Oleshchuk, V. A. (2013). PLC security and critical infrastructure protection. In 2013 IEEE 8th international conference on industrial and information systems (pp. 81-85). IEEE.doi:10.1109/iciinfs.2013.6731959
33. Serhane, A., Raad, M., Raad, R., & Susilo, W. (2019). Programmable logic controllers based systems (PLC-BS): Vulnerabilities and threats. SN Applied Sciences, 1, 1-12. doi:10.1007/s42452-019-0860-2
34. Hajda, J., Jakuszewski, R., & Ogonowski, S. (2021). Security challenges in industry 4.0 plc systems. Applied Sciences, 11(21), 9785.doi:10.3390/app11219785
35. Pan, X., Wang, Z., & Sun, Y. (2020). Review of PLC security issues in industrial control system. Journal of Cybersecurity, 2(2), 69. doi:10.32604/jcs.2020.010045
36. Püllen, D., Anagnostopoulos, N., Arul, T., & Katzenbeisser, S. (2020). Safety meets security: Using IEC 62443 for a highly automated road vehicle. In Computer Safety, Reliability, and Security: 39th International Conference, SAFECOMP 2020, Lisbon, Portugal, September 16–18, 2020, Proceedings 39 (pp. 325-340). Springer International Publishing.doi:10.1007/978-3-030-54549-9_22
37. Offermann, P., Levina, O., Schönherr, M., & Bub, U. (2009). Outline of a design science research process. In Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology (pp. 1-11). doi:10.1145/1555619.1555629
38. Wieringa, R. (2009). Design science as nested problem solving. In Proceedings of the 4th international conference on design science research in information systems and technology (pp. 1-12). doi:10.1145/1555619.1555630

39. Hevner, A. R. (2007). A three cycle view of design science research. Scandinavian journal of information systems, 19(2), 4.
40. Wieringa, R. (2010). Relevance and problem choice in design science. In International Conference on Design Science Research in Information Systems (pp. 61-76). Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-642-13335-0_5.
41. Cook, A., Janicke, H., Maglaras, L., & Smith, R. (2017). An assessment of the application of IT security mechanisms to industrial control systems. International Journal of Internet Technology and Secured Transactions, 7(2), 144-174. doi:10.1504/ijitst.2017.087163.
42. Liu, K., Wu, Q., Geng, Y., Ma, R., & Wei, Q. (2022). A survey of proactive defense in industrial control system. In International Conference on Electronic Information Technology (EIT 2022) (Vol. 12254, pp. 785-790). SPIE. doi:10.1117/12.2640454.
43. Zhao, W., Xie, F., Peng, Y., Gao, Y., Han, X., Gao, H., & Wang, D. (2013). Security testing methods and techniques of industrial control devices. In 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (pp. 433-436). IEEE. doi:10.1109/iih-msp.2013.114
44. Dehlaghi-Ghadim, A., Balador, A., Moghadam, M. H., Hansson, H., & Conti, M. (2023). ICSSIM—a framework for building industrial control systems security testbeds. Computers in Industry, 148, 103906.doi:10.1016/j.compind.2023.103906
45. Atalay, M., & Angin, P. (2020). A digital twins approach to smart grid security testing and standardization. In 2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT (pp. 435-440). IEEE. doi:10.1109/metroind4.0iot48571.2020.9138264
46. Ahmadian, M. M., Shajari, M., & Shafiee, M. A. (2020). Industrial control system security taxonomic framework with application to a comprehensive incidents survey. International Journal of Critical Infrastructure Protection, 29, 100356. doi:10.1016/j.ijcip.2020.100356
47. Ani, U. P. D., He, H., & Tiwari, A. (2018). A framework for Operational Security Metrics Development for industrial control environment. Journal of Cyber Security Technology, 2(3-4), 201-237. doi:10.1080/23742917.2018.1554986
48. Babbar, G., & Bhushan, B. (2020). Framework and methodological solutions for cyber security in Industry 4.0. In Proceedings of the international conference on innovative computing & communications (ICICC). doi:10.2139/ssrn.3601513

49. Coppolino, L., D’Antonio, S., Giuliano, V., Mazzeo, G., & Romano, L. (2022). A framework for Seveso-compliant cyber-physical security testing in sensitive industrial plants. Computers in Industry, 136, 103589. doi:10.1016/j.compind.2021.103589
50. Guo, X., Xue, Y., Feng, T., Jiang, Y., & Yan, Y. (2023). Simulation Implementation and Verification of a Security Framework for ICS Based on SPD. Automatic Control and Computer Sciences, 57(1), 37-47. doi: 10.3103/S0146411623010042
51. Kim, H., Kim, S., Kwon, S., Jo, W., & Shon, T. (2019). A novel security framework for industrial iot based on isa 100.11 a. In Quality, Reliability, Security and Robustness in Heterogeneous Systems: 14th EAI International Conference, Qshine 2018, Ho Chi Minh City, Vietnam, December 3–4, 2018, Proceedings 14 (pp. 61-72). Springer International Publishing. doi:10.1007/978-3-030-14413-5_5
52. Ani, U. P. D., Watson, J. M., Green, B., Craggs, B., & Nurse, J. R. (2021). Design considerations for building credible security testbeds: Perspectives from industrial control system use cases. Journal of Cyber Security Technology, 5(2), 71-119. doi:10.1080/23742917.2020.1843822
53. Holm, H., Karresand, M., Vidström, A., & Westring, E. (2015). A survey of industrial control system testbeds. In Secure IT Systems: 20th Nordic Conference, NordSec 2015, Stockholm, Sweden, October 19–21, 2015, Proceedings (pp. 11-26). Springer International Publishing. doi:10.1007/978-3-319-26502-5_2
54. Sheikh, Z. A., & Singh, Y. (2022). A Hybrid Threat Assessment Model for Security of Cyber Physical Systems. In 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC) (pp. 582-587). IEEE. doi:10.1109/pdgc56933.2022.10053332
55. Thomas, A. M., Marali, M., & Reddy, L. (2022). Identification of assets in industrial control systems using passive scanning. In Computer Networks, Big Data and IoT: Proceedings of ICCBI 2021 (pp. 269-283). Singapore: Springer Nature Singapore. doi: 10.1007/978-981-19-0898-9_21
56. Jbair, M., Ahmad, B., Maple, C., & Harrison, R. (2022). Threat modelling for industrial cyber physical systems in the era of smart manufacturing. Computers in Industry, 137, 103611. doi:10.1016/j.compind.2022.103611
57. Sergeevich, B. A., Sergeevna, B. E., Nikolaevna, I. T., Vitalievich, K. S., Dmitrievna, M. V., & Gennadievna, S. M. (2022). The concept of the knowledge base of threats to cyber-physical systems based on the ontological approach. In 2022 IEEE International

Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON) (pp. 90-95). IEEE. doi:10.1109/sibircon56155.2022.10016783

58. Khalil, S. M., Bahsi, H., & Korõtko, T. (2023). Threat modeling of industrial control systems: A systematic literature review. Computers & Security, 103543. doi:10.1016/j.cose.2023.103543
59. Mashkina, I., & Garipov, I. (2018). Threats modeling and quantitative risk analysis in industrial control systems. In 2018 International Russian Automation Conference (RusAutoCon) (pp. 1-5). IEEE. doi:10.1109/rusautocon.2018.8501694
60. Zahran, B., Hussaini, A., & Ali-Gombe, A. (2021). IIoT-ARAS: IIoT/ICS Automated risk assessment system for prediction and prevention. In Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy (pp. 305-307). doi:10.1145/3422337.3450320
61. Wieringa, R. (2014). Empirical research methods for technology validation: Scaling up to practice. Journal of systems and software, 95, 19-31. doi:10.1016/j.jss.2013.11.1097
62. Coppolino, L., D'Antonio, S., Giuliano, V., Mazzeo, G., & Romano, L. (2022). A framework for Seveso-compliant cyber-physical security testing in sensitive industrial plants. Computers in Industry, 136, 103589. doi:10.1016/j.compind.2021.103589
63. Shokeen, R., Shanmugam, B., Kannoorpatti, K., Azam, S., Jonkman, M., & Alazab, M. (2019). Vulnerabilities analysis and security assessment framework for the internet of things. In 2019 Cybersecurity and Cyberforensics Conference (CCC) (pp. 22-29). IEEE. doi:10.1109/ccc.2019.00-14
64. Alanen, J., Linnosmaa, J., Malm, T., Papakonstantinou, N., Ahonen, T., Heikkilä, E., & Tiusanen, R. (2022). Hybrid ontology for safety, security, and dependability risk assessments and Security Threat Analysis (STA) method for industrial control systems. Reliability Engineering & System Safety, 220, 108270. doi:10.1016/j.ress.2021.108270
65. Staves, A., Gouglidis, A., Maesschalck, S., & Hutchison, D. (2024). Risk-based safety scoping of adversary-centric security testing on Operational Technology. Safety Science, 174, 106481. doi:10.1016/j.ssci.2024.106481
66. Lyu, X., Ding, Y., & Yang, S. H. (2019). Safety and security risk assessment in cyber-physical systems. IET Cyber-Physical Systems: Theory & Applications, 4(3), 221-232. doi:10.1049/iet-cps.2018.5068

67. Wolf, M., & Serpanos, D. (2017). Safety and security in cyber-physical systems and internet-of-things systems. Proceedings of the IEEE, 106(1), 9-20.doi:10.1109/jproc.2017.2781198

68. Hollerer, S., Sauter, T., & Kastner, W. (2022). Risk assessments considering safety, security, and their interdependencies in ot environments. In Proceedings of the 17th International Conference on Availability, Reliability and Security (pp. 1-8). doi:10.1145/3538969.3543814

69. Li, T., & Hankin, C. (2015). A Model-based Approach to Interdependency between Safety and Security in ICS. In 3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015). BCS Learning & Development. doi:10.14236/ewic/ics2015.4

70. Lyu, X., Ding, Y., & Yang, S.-H. (2019). Safety and security risk assessment in cyber-physical systems. IET Cyber-Physical Systems Theory & Applications, 4(3), 221–232. doi:10.1049/iet-cps.2018.5068

71. da Silva Oliveira, A., & Santos, H. (2022). Continuous industrial sector cybersecurity assessment paradigm: Proposed model of cybersecurity certification. In 2022 18th International Conference on the Design of Reliable Communication Networks (DRCN) (pp. 1-6). IEEE. doi:10.1109/drcn53993.2022.9758022

72. Heluany, J. B., & Galvão, R. (2023). IEC 62443 standard for hydro power plants. Energies, 16(3), 1452. doi:10.3390/en16031452

73. Leander, B., Čaušević, A., & Hansson, H. (2019). Applicability of the IEC 62443 standard in Industry 4.0/IIoT. In Proceedings of the 14th International Conference on Availability, Reliability and Security (pp. 1-8). doi:10.1145/3339252.3341481

74. Moyon, F., Beckers, K., Klepper, S., Lachberger, P., & Bruegge, B. (2018). Towards continuous security compliance in agile software development at scale. In Proceedings of the 4th International Workshop on Rapid Continuous Software Engineering (pp. 31-34). doi:10.1145/3194760.3194767

75. Dännart, S., Constante, F. M., & Beckers, K. (2019). An assessment model for continuous security compliance in large scale agile environments: exploratory paper. In Advanced Information Systems Engineering: 31st International Conference, CAiSE 2019, Rome, Italy, June 3–7, 2019, Proceedings 31 (pp. 529-544). Springer International Publishing. doi:10.1007/978-3-030-21290-2_33

76. Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. International journal of critical infrastructure protection, 9, 52-80. doi:10.1016/j.ijcip.2015.02.002
77. Hassani, H. L., Bahnasse, A., Martin, E., Roland, C., Bouattane, O., & Diouri, M. E. M. (2021). Vulnerability and security risk assessment in a IIoT environment in compliance with standard IEC 62443. Procedia Computer Science, 191, 33-40. doi:10.1016/j.procs.2021.07.008
78. Fockel, M., Merschjohann, S., Fazal-Baqaie, M., Förder, T., Hausmann, S., & Waldeck, B. (2019). Designing and integrating IEC 62443 compliant threat analysis. In Systems, Software and Services Process Improvement: 26th European Conference, EuroSPI 2019, Edinburgh, UK, September 18–20, 2019, Proceedings 26 (pp. 57-69). Springer International Publishing. doi:10.1007/978-3-030-28005-5_5
79. Schmittner, C., Shaaban, A. M., & Macher, G. (2022). ThreatGet: ensuring the implementation of defense-in-depth strategy for IIoT based on IEC 62443. In 2022 IEEE 5th International Conference on Industrial Cyber-Physical Systems (ICPS) (pp. 1-6). IEEE. doi:10.1109/icps51978.2022.9816864
80. Moyon, F., Beckers, K., Klepper, S., Lachberger, P., & Bruegge, B. (2018). Towards continuous security compliance in agile software development at scale. In Proceedings of the 4th International Workshop on Rapid Continuous Software Engineering (pp. 31-34). doi:10.1145/3194760.3194767