CHALMERS
UNIVERSITY OF TECHNOLOGY

UNIVERSITY OF GOTHENBURG

Regulation-Directed Cybersecurity Best Practices for Operational Technology Environments

Master's thesis in Computer science and engineering

PRAHITHA KAICHETTY
SREELEKHA VUPPALA

Department of Computer Science and Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
UNIVERSITY OF GOTHENBURG
Gothenburg, Sweden 2026

Master's thesis 2026

Regulation-Directed Cybersecurity Best Practices for Operational Technology Environments

PRAHITHA KAICHETTY
SREELEKHA VUPPALA

UNIVERSITY OF
GOTHENBURG

CHALMERS
UNIVERSITY OF TECHNOLOGY

Department of Computer Science and Engineering
Chalmers University of Technology
University of Gothenburg
Gothenburg, Sweden 2026

Regulation-Directed Cybersecurity Best Practices for Operational Technology Environments
PRAHITHA KAICHETTY
SREELEKHA VUPPALA

Supervisor: Dr. Haroon Elahi, Department of Computer Science and Engineering
Examiner: Morten Fjeld, Department of Software Engineering

Master's Thesis 2026
Department of Computer Science and Engineering
Chalmers University of Technology and University of Gothenburg
SE-412 96 Gothenburg
Telephone +46 31 772 1000

Abstract

Operational Technology (OT) systems refer to hardware and software used to monitor and control physical processes, devices, and infrastructure in industrial environments. These systems are typically designed for long operational lifecycles and are expected to function reliably over extended periods. In recent years, industrial sectors have increasingly integrated OT systems with Information Technology (IT) networks to enable digital transformation, improve data-driven decision-making, and support remote monitoring and control, thereby enhancing operational efficiency and connectivity. However, this integration also introduces significant cybersecurity risks. The incorporation of legacy OT systems into modern and continuously evolving IT environments makes them more vulnerable to cyberattacks and easier to exploit. Cyber incidents targeting OT systems can result in severe consequences, including physical damage to equipment, production disruptions, financial losses, safety risks to personnel, and loss of operational control. Consequently, OT environments have emerged as critical targets for malicious actors.

To address the growing cybersecurity threat landscape, the European Union has introduced the Network and Information Security Directive 2 (NIS2) Directive, which establishes standardized cybersecurity requirements for essential and important entities, including those in the manufacturing sector. Prior to the introduction of NIS2, the National Institute of Standards and Technology (NIST) cybersecurity framework has been widely adopted across industries as a best-practice guideline for managing cybersecurity risks. Most companies are required to meet the NIS2 requirements, however redesigning the security infrastructure from scratch is an expensive and complicated process. One possible approach to address this issue is to map NIS2 requirements to existing cybersecurity frameworks. In this thesis, NIST standards are mapped to the NIS2 Directive to identify compliance gaps and evaluate cybersecurity alignment within IT and OT environments. The associated risks in OT components are analyzed through the development of a Failure Modes and Effects Analysis (FMEA) table. Additionally, an OT and IT component checklist is created to ensure the adequacy mitigation and redundancy measures across systems.

This approach helps identify existing gaps, thereby improving overall security and strengthening compliance. Furthermore, it enables organizations to proactively address vulnerabilities and adapt to evolving cybersecurity threats.

Keywords: Operational Technology(OT), Security Standardization, Network and Information Systems Directive, Risk Analysis, Cybersecurity regulation

Acknowledgements

We would like to express our sincere gratitude to Dr. Haroon Elahi, our academic supervisor, for his invaluable guidance, consistent support and constructive feedback throughout our thesis.

Additionally, we are grateful to Morten Fjeld, our examiner, for his evaluation and feedback.

Prahitha Kaichetty, Sreelekha Vuppala, Gothenburg, 2026-06-24

Abbreviations

ACL	Access Control List
AI	Artificial Intelligence
CSF	Cybersecurity Framework
CSIRT	Computer Security Incident Response Team
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
EU	European Union
FMEA	Failure Mode and Effects Analysis
HMI	Human-Machine Interface
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
IDS	Intrusion Detection System
IIoT	Industrial Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
MAC	Media Access Control
MFA	Multi-Factor Authentication
MitM	Man-in-the-Middle
NIST	National Institute of Standards and Technology
NIS2	Network and Information Security Directive 2
OS	Operating System
OT	Operational Technology
OTP	One-Time Password
PLC	Programmable Logic Controller
RBAC	Role-Based Access Control
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SDN	Software-Defined Networking
SFAIR	Secure Framework for AI Regulation
SIEM	Security Information and Event Management
SOC	Security Operations Center
TCP	Transmission Control Protocol
TLS	Transport Layer Security
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
ZTA	Zero Trust Architecture

Contents

List of Figures

List of Tables

1

Introduction

Operational Technology (OT) systems are used to monitor and control industrial processes and play a vital role in modern industries, particularly in sectors such as manufacturing, energy, digital infrastructure and transportation [1]. These systems include components such as Supervisory Control and Data Acquisition (SCADA) systems, Programmable Logic Controllers (PLCs), and Distributed Control Systems (DCS), which directly interact with physical processes and infrastructure. OT systems, typically designed for isolated long operational lifecycles, were not originally designed with strong cybersecurity considerations [2].

Earlier cyberattacks were primarily focused on Information Technology (IT) networks; however, over time, the security posture of IT systems has significantly improved. In recent years, as many industries have increasingly integrated Information Technology (IT) with Operational Technology (OT) they have been exposed to cyber threats [3]. While this integration introduces notable improvements in cybersecurity and system capabilities, it also presents new challenges, particularly due to legacy OT systems that were not originally designed with security considerations in mind. Consequently, attackers have shifted their focus toward exploiting vulnerabilities in OT environments, leading to significant impacts on industrial operations. As the number and sophistication of such threats continue to increase, the European Union has introduced the Network and Information Security Directive 2 (NIS2) Directive, which establishes cybersecurity and risk management requirements for essential and important entities, including those operating in industrial and manufacturing sectors [4].

1.1 Problem Statement

Before NIS2 most industries were using NIST standards. The target organization may not be fully compliant with NIS2 requirements due to gaps between existing cybersecurity practices and regulatory expectations [5]. These gaps in security controls can introduce risks such as unauthorized access, vulnerabilities in legacy systems, safety hazards, operational disruptions, and potential data compromise. Therefore, a structured approach is required to systematically identify missing requirements and analyze the associated risks within operational technology (OT) and Information Technology (IT) environments.

1.2 Aim

The aim of this thesis is to help improve cybersecurity in Operational Technology(OT) environments by comparing the existing security framework based on National Institute of Standards and Technology (NIST) cybersecurity standards [1]. Specifically, the work focuses on mapping a security framework implemented in the target organization and based on NIST cybersecurity standards [6] to the requirement of the Network and Information Systems Directive 2 (NIS2) Directive [4] in order to identify gaps in coverage and recommend improvements.

1.3 Research questions

This thesis aims to answer the following research questions:

1. **What are the key cybersecurity risks in OT systems for production companies?**
   Identifying the most significant cybersecurity threats and vulnerabilities affecting OT systems in production environments helps establish an understanding of risks that may impact safety, system availability, and operational continuity. This provides a foundation for prioritizing security measures and risk mitigation efforts [7].

2. **What are the NIS2 compliance requirements relevant to OT environments?**
   Analyzing the NIS2 Directive requirements applicable to OT environments clarifies the regulatory obligations placed on industrial organizations [8]. This supports a structured interpretation of how NIS2 influences cybersecurity governance and risk management in production systems.

3. **How are the key cybersecurity risks being addressed in the target organization?**
   Describing existing cybersecurity practices and controls in the target organization provides insight into how OT related risks are currently managed in practice [9]. This helps assess the organization's current security posture and identify effective measures as well as potential weaknesses.

4. **What are the gaps in the current cybersecurity architecture of the target organization relative to NIS2 requirements?**
   Comparing the organization's existing OT cybersecurity architecture with NIS2 requirements highlights discrepancies between current practices and regulatory expectations [3]. This comparison supports the identification of areas where security improvements and compliance efforts are required.

5. **How can NIS2 compliance be effectively achieved in the target OT environment?**
   Formulating practical and implementable recommendations for NIS2 compliance supports the translation of regulatory requirements into concrete technical and

organizational measures. This enables improvements to OT cybersecurity while maintaining system availability and safety [3] and [8].

1.4 Challenges

1. Heterogeneity and complexity of Operational Technology(OT) environments: OT systems include a mix of modern and legacy technologies from different vendors, which increases system complexity and makes it challenging to generalise results and compare security measures in a structured way.
2. Limited availability of Operational Technology(OT) specific academic literature: Compared to IT security, fewer peer reviewed studies focus on OT cybersecurity, making it more difficult to identify relevant and high quality academic literature.
3. High level nature of NIS2 requirements: NIS2 defines cybersecurity obligations at a strategic and organizational level without prescribing concrete technical controls. Translating these abstract regulatory requirements into technically meaningful and analyzable OT security measures requires careful interpretation.

1.5 Contributions

In order to investigate the above research questions and meet study's goals a gap-analysis was performed. As a next step, the thesis analyzes risks associated with OT components using Failure Modes and Effects Analysis (FMEA) [10]. Based on this analysis, the objective is to provide practical and actionable recommendations to enhance cybersecurity in both IT and OT systems.

In addition, an OT and IT component checklist was developed to evaluate the cybersecurity posture of each component by analyzing the component type, associated threats, detection mechanisms, possible false negatives, mitigation measures, and redundancy controls. The checklist includes components such as Security Information and Event Management (SIEM), Human-Machine Interface (HMI), Virtual Local Area Network (VLAN), and firewalls [11], [12], [13] and [14]. This checklist supports a better understanding of security effectiveness and helps improve the target organization's overall cybersecurity resilience.

In short, this thesis makes the following main contributions:

- Mapping and Compliance Assessment Methodology (Section 3.2): The study develops a systematic mapping methodology to align existing National Institute of Standards and Technology (NIST) cybersecurity standards with the European Union's Network and Information Security Directive 2 (NIS2) requirements[15][4]. The comparative assessment between NIST CSF v2.0 and European Union cybersecurity standards presented in recent research literature [16] was referenced to understand the alignment, governance structure, and regulatory relationships between NIST frameworks and NIS2 requirements. This structured mapping as presented in the Appendix A.1 approach enabled the

identification of regulatory, governance, and compliance gaps within the target organization's existing cybersecurity architecture while ensuring traceability between established cybersecurity controls and NIS2 requirements.

- Provision of Checklist Instruments (Appendix A.3 and Appendix A.1): This study contributes by developing structured checklist instruments for both NIST-NIS2 compliance assessment and component-level cybersecurity evaluation within Operational Technology (OT) and Information Technology (IT) environments. The checklist development process was supported by the principles and guidance provided in the *NIST National Checklist Program for IT Products* [17], which emphasizes standardized security configuration checklists, risk-based tailoring, and compliance verification mechanisms. The developed instruments support cybersecurity evaluation, compliance verification, threat identification, mitigation assessment, and documentation processes across interconnected industrial environments for component-level security assessment.
- Empirical Risk Analysis of OT and IT Systems (Section 3.3) : This thesis performs an in-depth risk analysis of critical Operational Technology (OT) and Information Technology (IT) components using the Failure Mode and Effects Analysis (FMEA) method [18]. The risk assessment approach was supported by existing research on FMEA based cybersecurity analysis, industrial control system risk evaluation, and structured risk management methodologies [10], [19], [20]. The referenced studies explain that FMEA can be effectively applied within cybersecurity and industrial environments to systematically identify and prioritize potential failures and security risks using Risk Priority Number (RPN) calculations [10]. Research on Industrial Control Systems (ICS) and SCADA environments further highlights the importance of structured risk evaluation techniques for identifying vulnerabilities related to operational disruptions, malware attacks, unauthorized access, and infrastructure failures [19]. In addition, the NIST Risk Management Framework (RMF) provides a comprehensive and risk-based methodology for identifying, assessing, monitoring, and responding to cybersecurity risks across both Information Technology (IT) and Operational Technology (OT) systems [20]. By calculating the Risk Priority Scores for components such as Remote Terminal Units (RTUs), SCADA systems, and firewalls, the analysis identifies and prioritizes high-risk vulnerabilities related to unauthorized access, malware attacks, system failures, and detection limitations of the target organization A.2. This structured approach enables the evaluation of component-level failures and their potential impact on operational continuity, cybersecurity resilience, and regulatory compliance within OT and IT environments.
- Component-Level Security Evaluation Section (Section 3.4): This thesis develops a component-level security checklist for selected critical components within the target organization 3.5, including Security Information and Event Management (SIEM) systems, Human Machine Interfaces (HMI), Virtual Local Area Networks (VLANs), and firewalls. The checklist development process follows a structured assessment approach consisting of threat identification, detection mechanism evaluation, false negative analysis, mitigation assessment,

redundancy evaluation, responsible security team assignment, and checklist based documentation. The developed checklist systematically evaluates different threat categories, detection mechanisms, false negatives, mitigation strategies, redundancy measures, and responsible security teams associated with each component A.3. In addition, the assessment incorporates operational responsibilities across SOC Tier 1, SOC Tier 2, SOC Tier 3, Incident Response, Threat Hunting, Detection Engineering, and Endpoint Security teams to ensure clear accountability for threat monitoring, detection, analysis, and response activities. This structured component-level evaluation supports the identification of cybersecurity weaknesses, detection gaps, and operational limitations while improving overall security visibility, resilience, and incident response coordination within the Operational Technology (OT) and Information Technology (IT) environments of the target organization.

- Practical Recommendations (Chapter 6): Based on the identified compliance gaps and risk assessments presented in Chapter 5, this thesis provides practical recommendations to support organizations in achieving improved alignment with the NIS2 Directive and strengthening overall cybersecurity resilience within Operational Technology (OT) and Information Technology (IT) environments. The recommendations include strategic measures such as the adoption of the updated NIST SP 800-171 Rev.3 [21] standard to address evolving cyber threats, strengthen supply chain risk management, and improve the implementation of security controls. In addition, this thesis recommends the adoption of Zero Trust Architecture (ZTA) principles, including continuous authentication, least-privilege access control, network segmentation, micro-segmentation, and continuous monitoring, to reduce unauthorized lateral movement and improve protection across interconnected IT and OT infrastructures [22]. Furthermore, the recommendations incorporate Risk Priority Number (RPN) based mitigation strategies and component level security improvements for critical systems such as RTUs, SCADA systems, firewalls, and SIEM platforms to enhance threat detection, incident response, operational continuity, and regulatory compliance.

2

Background

This chapter presents the background work for the thesis, including a comprehensive literature review of relevant research papers.

2.1 Operational Technology (OT)

Operational Technology (OT) refers to the hardware and software systems used to monitor and control physical devices, processes, and events. These systems are responsible for detecting changes and directly influencing physical operations. OT environments form the backbone of critical infrastructure and industrial production. They include specialized components such as Supervisory Control and Data Acquisition (SCADA) systems, Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), sensors, and physical actuators [1].

In contrast to Information Technology systems, OT networks are designed to manage physical processes where safety and system availability are the highest priorities [23]. These systems often operate in real-time environments, where even very small delays or unexpected downtime can lead to serious consequences such as physical damage, financial loss, or risks to human life [2]. OT cybersecurity follows the (SCIA) model prioritizing Safety, Availability, Integrity, and Confidentiality to protect physical processes and industrial operations is illustrated in Figure 2.1.

2.2 Information Technology (IT)

Information Technology (IT) refers to the use of systems, networks, and hardware for handling data. It mainly focuses on collecting, processing, storing, and sharing digital information [24], [23]. A typical enterprise IT environment includes components such as personal computers, servers, enterprise applications, and networking devices such as routers and firewalls [23].

In the IT field, cybersecurity is based on three main principles known as confidentiality, integrity, and availability is illustrated in Figure 2.1. Among these, greater importance is usually given to confidentiality to ensure that sensitive information is protected from unauthorized access [3]. IT systems are generally designed to be easily accessible and regularly updated [23].

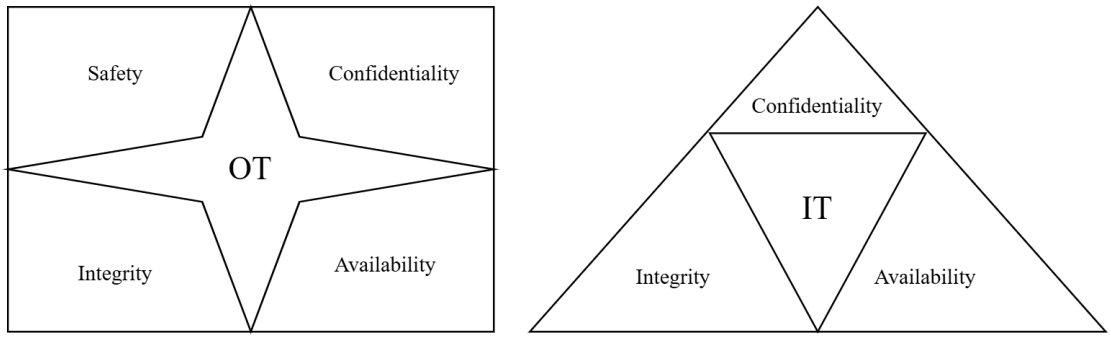

Figure 2.1: OT and IT security priorities

2.3 Industrial Cybersecurity Standards

The National Institute of Standards and Technology (NIST) is a non-regulatory agency of the United States Department of Commerce that develops standards, guidelines, and best practices to promote innovation and improve security across industries [15]. NIST is widely recognized for its contributions to cybersecurity, particularly through the development of frameworks and special publications that help organizations manage and reduce cybersecurity risks. These standards provide a structured and flexible approach for identifying, assessing, and mitigating security threats across information systems and critical infrastructure. Overall, NIST standards are globally adopted and serve as a foundation for implementing effective cybersecurity strategies in both public and private sectors [15].

Table 2.1: NIST Standards and Descriptions.

NIST Standard & Version	**Description**
NIST CSF 2.0	The NIST Cybersecurity Framework (CSF) 2.0 provides guidance to organizations to manage cybersecurity risks by offering a taxonomy of high-level cybersecurity outcomes[25].
NIST SP 800-37 Rev. 2	Risk Management Framework for Information Systems and Organizations detailing a system life cycle approach for security and privacy, including privacy and supply chain risk management[26].
NIST SP 800-39	Provides guidance for an integrated, organization-wide program for managing information security risk to operations, assets, individuals, and other entities[27].
NIST SP 800-53 Rev. 5	Provides a comprehensive catalog of security and privacy controls to address evolving threats, vulnerabilities, and technologies[28].
NIST SP 800-63B-4	Digital Identity Guidelines focusing on authentication and ensuring that a claimant is a valid subscriber interacting with systems[29].
NIST SP 800-64 Rev. 2	Assists agencies in integrating security considerations into the System Development Life Cycle (SDLC)[30].
NIST SP 800-88 Rev. 1	Provides guidelines for media sanitization to ensure secure disposal of information system data[31].
NIST SP 800-122	Guide for protecting the confidentiality of Personally Identifiable Information (PII) in federal systems[32].
NIST SP 800-160 Vol. 1 Rev. 1	Describes principles and processes for engineering trustworthy and secure systems[33].
NIST SP 800-161 Rev. 1	Provides guidance on cybersecurity supply chain risk management practices[34].
NIST SP 800-171 Rev. 2	Recommends security requirements for protecting Controlled Unclassified Information (CUI) in nonfederal systems[24].

Table 2.1 lists the NIST standards used by the target organization. These standards were reviewed to analyze how cybersecurity practices are implemented and aligned with established frameworks. The table 2.1 provides a summary of each standard and its relevance to this study.

2.4 NIS2 Directive

The Network and Information Systems 2 (NIS2) Directive (Directive (EU) 2022/2555) is a comprehensive legislative framework established to achieve a high common level of cybersecurity across the European Union [5]. It was introduced in response to the increasing digital transformation and interconnected nature of modern society, which have significantly expanded the cyber threat landscape. The directive replaces the earlier NIS1 Directive (Directive (EU) 2016/1148) [35], which was found to allow considerable variation in how Member States implemented cybersecurity requirements. This variation resulted in fragmented security practices and exposed certain sectors to cross-border cyber risks.

The directive requires Member States to establish coordinated national cybersecurity frameworks. This includes the development of national cybersecurity strategies, the designation of competent authorities and single points of contact, and the establishment of Computer Security Incident Response Teams (CSIRTs) [5]. In addition, the scope of the directive has been expanded to include medium and large organizations operating in highly critical sectors such as energy, transport, banking, and healthcare, as well as other important sectors including postal services, waste management, and digital service providers. Organizations are categorized as either essential or important entities based on their level of criticality and size, which determines the level of supervision applied to them [5].

At the operational level, the NIS2 Directive requires organizations to adopt a comprehensive risk management approach. This includes implementing policies related to incident handling, business continuity, supply chain security, the use of cryptography, and general cybersecurity practices, as outlined in Article 21 [5]. The directive also establishes strict reporting requirements for significant cybersecurity incidents under Article 23. Organizations must provide an initial warning within 24 hours, a formal notification within 72 hours, and a detailed final report within one month to the relevant authorities [5].

To ensure compliance, the directive grants regulatory authorities the power to conduct inspections, issue binding instructions, and impose significant administrative fines. For essential entities, penalties can reach up to 10 million euros or 2 percent of the global annual turnover, depending on the severity of non-compliance [5].

The directive defines its scope, governance, cooperation mechanisms, risk management requirements, and enforcement provisions across multiple articles. Articles 1 to 6 establish the subject matter, scope, classification of entities, and key definitions, while also allowing Member States to adopt stricter national measures. Articles 7 to

13 focus on national responsibilities, including cybersecurity strategies, competent authorities, crisis management, CSIRTs, and vulnerability disclosure mechanisms[5].

Articles 14 to 19 promote cooperation at European and international levels through cooperation groups, CSIRT networks, and large-scale incident coordination frameworks. Articles 20 to 25 define governance and operational cybersecurity requirements, including management responsibility (Article 20), cybersecurity risk management measures (Article 21), supply chain security (Article 22), incident reporting obligations (Article 23), certification schemes (Article 24), and standardization (Article 25)[5].

Articles 26 to 28 address jurisdiction and registration requirements, including entity registries and domain data accuracy. Articles 29 and 30 promote information sharing and voluntary reporting. Articles 31 to 37 define supervision and enforcement mechanisms, including regulatory oversight, inspections, administrative fines, and coordination with data protection authorities. Finally, Articles 38 to 46 cover implementation provisions, including delegation of powers, review requirements, amendments, repeal of the NIS1 Directive, and entry into force [5].

2.5 Literature Review

Existing research highlights significant challenges in securing operational technology (OT) environments, particularly due to the convergence of IT and OT systems. Studies indicate that this integration increases the attack surface and exposes legacy industrial systems to advanced cyber threats, including ransomware and targeted attacks on critical infrastructure [23], [36]. These works emphasize that traditional security mechanisms are insufficient for OT environments, and there is a growing need for resilient approaches that focus on detection, containment, and recovery rather than prevention alone.

From a regulatory perspective, several studies have examined the implementation of the NIS2 Directive and its impact on organizations. Research shows that compliance is particularly challenging in OT environments due to the IT/OT gap, differences in security practices, and limited availability of technical solutions [3], [37]. Furthermore, existing approaches suggest the use of frameworks such as ISO 27001 and assessment tools to support compliance efforts. However, these studies also indicate that cybersecurity maturity in OT systems remains relatively low, mainly due to legacy system constraints and insufficient resources.

Network segmentation has been widely proposed as a key strategy for improving OT security. Prior research demonstrates that segmentation techniques, particularly micro-segmentation, can significantly reduce lateral movement and limit the impact of cyberattacks [38], [36]. In addition, emerging technologies such as Software-Defined Networking (SDN) and automation are identified as promising solutions for implementing dynamic segmentation. Despite these advancements, existing studies highlight a lack of practical implementation guidelines tailored to organizational requirements, especially in complex OT environments.

Similarly, Zero Trust Architecture (ZTA) has been explored as an advanced security model for modern systems. Research categorizes ZTA into key components such as identity authentication, access control, and continuous trust evaluation, emphasizing the principle of "never trust, always verify" [39], [40] , [22]. While ZTA offers significant improvements over traditional perimeter-based security, studies identify several challenges, including system complexity, integration with legacy systems, and the absence of standardized migration frameworks. Existing frameworks propose structured and iterative approaches for ZTA implementation, but their practical application in OT environments remains limited.

Despite these contributions, several gaps remain in the current body of research. Existing studies often address cybersecurity techniques, regulatory frameworks, and architectural solutions independently, without providing a unified approach that integrates these aspects. In particular, there is a lack of methodologies that directly map regulatory requirements such as NIS2 to practical cybersecurity controls and risk analysis techniques within OT systems. Furthermore, challenges related to legacy infrastructure, operational constraints, and real-world implementation are not comprehensively addressed.

Therefore, there is a need for a structured and integrated approach that bridges the gap between regulatory compliance and practical cybersecurity implementation in OT environments. This study addresses this need by combining NIS2 mapping with risk analysis and component-level evaluation to provide a pratical recommendations for improving cybersecurity posture.

3

Methodology

This chapter presents the methodology adopted in this study to analyze the alignment between NIST standards and the NIS2 Directive and to assess cybersecurity risks in OT environments [5] and [15].

The research approach used in this study follows a structured methodology involving data collection, framework mapping, component-level security assessment, and risk evaluation to analyze the alignment between NIST standards and the NIS2 Directive and to assess cybersecurity risks in Operational Technology (OT) environments, as illustrated in Figure 3.1.

The methodology was designed to provide a systematic and comprehensive evaluation of the cybersecurity posture of the target organization. The study initially focused on collecting relevant data from multiple sources, including NIST cybersecurity standards, the NIS2 Directive, literature reviews, expert interviews, and system architecture information related to both IT and OT environments.This data served as the foundation for understanding existing cybersecurity practices, regulatory requirements, and operational dependencies within the target organization.

Based on the collected data, a structured mapping process was carried out to compare NIST standards with the requirements defined in the NIS2 Directive. In addition, component-level security assessment and Failure Mode and Effects Analysis (FMEA) were performed to identify vulnerabilities, evaluate risks, and analyze the effectiveness of existing security controls across critical OT and IT components. The overall methodology 3.1 supports the identification of compliance gaps, high-risk components, and areas requiring further cybersecurity improvements within the target organization.

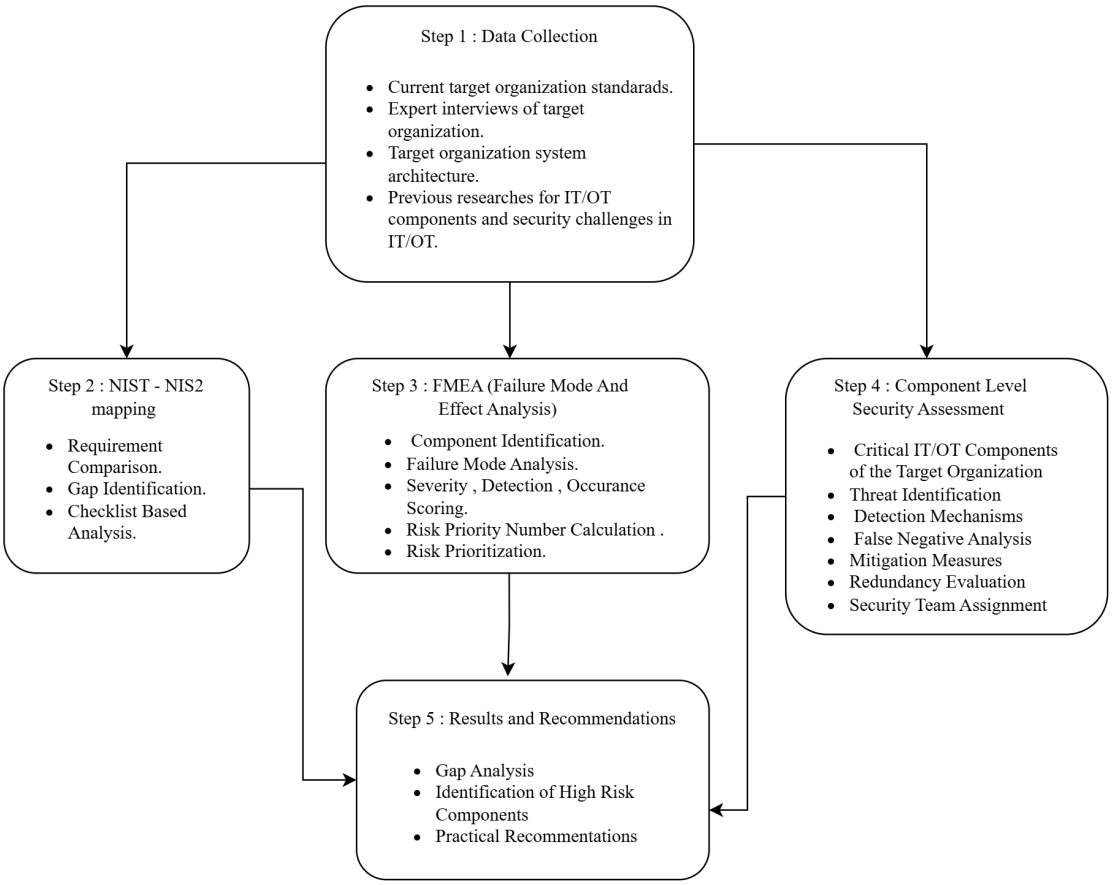

Figure 3.1: Research Methodology Process.

3.1 Data Collection

This study is based on multiple data sources, including cybersecurity standards, regulatory frameworks, system-level information, and expert insights, to ensure a comprehensive and structured analysis.

An interview with the cybersecurity team of the target organization was conducted to understand current security practices and awareness of NIS2 requirements. The findings confirmed that the organization primarily follows NIST-based approaches for managing cybersecurity.

Based on the above data, the NIST cybersecurity standards implemented by the target organization were considered as the baseline data for this study as discusssed in the Section 2.3. In addition, the NIS2 Directive was analyzed as the primary regulatory reference because it is a legally binding EU directive that establishes mandatory cybersecurity requirements, addressing a broad range of essential and important entities. The NIS2 Directive aims to harmonize cybersecurity requirements across EU Member States by establishing a common baseline of security measures, thereby improving consistency while still allowing national-level implementation. Relevant articles and requirements from the directive were systematically reviewed

and extracted to support the comparison and mapping process [5].

A systematic approach is followed for the mapping process. A literature review was conducted to examine existing studies, ensuring that the approach was aligned with established research[16]. Previous work, including comparisons between NIST CSF v2.0 and the NIS2 Directive, adopted a functional mapping approach by comparing NIST functions (Govern, Identify, Protect, Detect, Respond, and Recover) with corresponding NIS2 requirements based on similarities in objectives, control mechanisms, and expected security outcomes. This established approach was used as a reference to guide the mapping process. In addition, the mapping process is developed based on the NIST National Checklist Program [17] to support consistency and traceability throughout the mapping process.

Furthermore, system architecture data from the target organization, as illustrated in figure 3.5 the connection between IT and OT environments, illustrating basic segmentation through Demilitarized Zone (DMZs), Virtual Local Area Network (VLAN) and firewalls. It further higlights the communication pathways and secure interaction between IT system and OT devices. Data from the literature review was collected to identify key OT and IT components, along with their functional roles and interdependencies within the overall infrastructure. This data was specifically gathered to support subsequent component-level analysis and risk assessment using the Failure Mode and Effects Analysis (FMEA) approach.

3.2 NIST to NIS2 mapping

Based on the data collected, a mapping between the NIST cybersecurity standards used by the target organization and the requirements defined in the NIS2 Directive was performed. The purpose of this mapping is to evaluate the extent to which existing cybersecurity practices align with regulatory expectations and to identify potential gaps in compliance of the target organization.

The mapping process involved a systematic comparison of NIS2 requirements with relevant NIST standards [5] and Section 2.3. Each NIS2 requirement was analyzed and matched with corresponding NIST controls based on similarity in objectives, control mechanisms, and expected security outcomes.

To ensure a structured and consistent mapping process, a checklist-based approach is adopted for comparing NIS2 requirements with NIST controls. The development of the checklist was guided by the NIST National Checklist Program [17], which provides standardized procedures for creating, tailoring, and applying security configuration checklists. This approach supports systematic evaluation, improves traceability, and ensures that security requirements are assessed in a consistent and repeatable manner.

The mapping process was carried out as follows:

- Identification and selection of NIS2 requirements relevant to the operational and security context of the target organization.

- Extraction of applicable NIST standards and controls currently implemented within the target organization.
- Systematic comparison of NIS2 requirements with NIST controls to evaluate alignment in terms of control objectives, scope, and effectiveness.
- Association of specific NIS2 article numbers with corresponding NIST standards and control families.
- Documentation of the mapping results in structured checklist format to support analysis, traceability, and future reference.

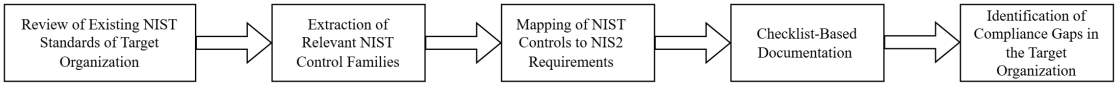

Figure 3.2: NIST to NIS2 mapping flow diagram

The detailed mapping tables, including the relationships between NIST standards, control families, and corresponding NIS2 articles along with their summaries, are presented in Appendix A.1. These tables provide a structured representation of how specific NIST controls align with NIS2 requirements, enabling a clearer understanding of coverage, overlaps, and potential gaps in compliance. The flow diagram of NIST to NIS2 mapping is illustrated in figure 3.2

3.3 FMEA-Based Risk Analysis

A structured risk analysis was conducted using the Failure Mode and Effects Analysis (FMEA) approach [18]. This step of the study aims to systematically identify potential failure modes within the system architecture of the target organization and evaluate their impact on cybersecurity, operational continuity, and regulatory compliance.

FMEA was selected due to its proactive capability to identify vulnerabilities, assess their severity, and prioritize mitigation strategies. In this study, the method was applied to both IT and OT components identified from the system architecture of the target organization, as well as components derived from the literature review. The overall FMEA process adopted in this work is illustrated in Figure 3.3.

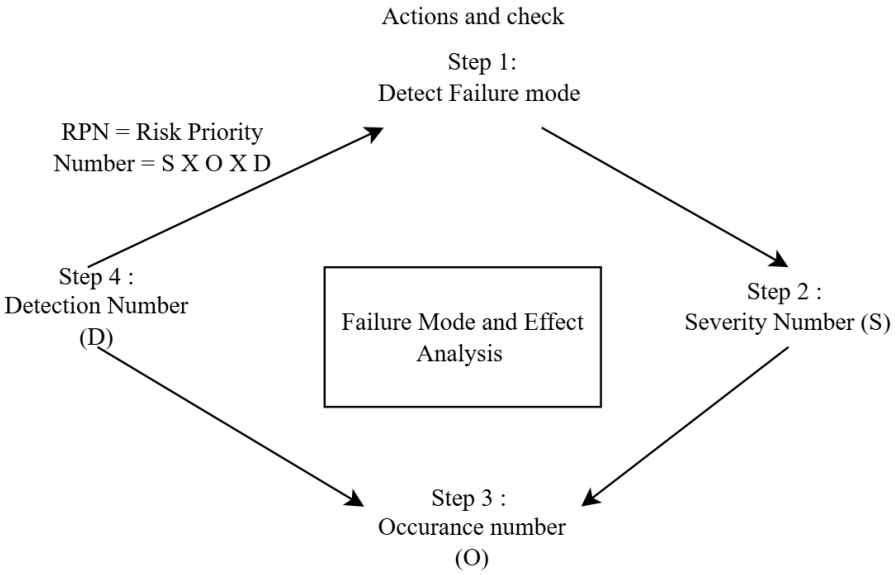

Figure 3.3: Failure Mode and Effects Analysis (FMEA) Process

3.3.1 FMEA Procedure

The FMEA process was carried out through a series of structured steps to ensure a systematic and comprehensive evaluation of potential risks[18]:

- **Component Identification:** Relevant IT and OT components were identified based on the system architecture of the target organization and supported by findings from the literature review.
- **Function Definition:** The primary function of each component was defined to clearly establish its role within the system, such as data acquisition, process control, communication, or security enforcement.
- **Failure Mode Identification:** Potential failure modes were identified for each component, representing possible ways in which the component may fail during operation.
- **Cause Analysis:** The underlying causes of each failure mode were analyzed, including hardware faults, communication issues, environmental factors, and cybersecurity vulnerabilities.
- **Effect Analysis:** The impact of each failure mode was evaluated at two levels:
  - **Local Effect:** Impact on the individual component.
  - **System Effect:** Impact on the overall system performance and operational processes.
- **Risk Priority Score:** A Risk Priority Score is a numerical score used in Failure Mode and Effects Analysis (FMEA) to measure and rank the risk associated with OT component.Using risk priority scores is a standard practice in academia and industry [19] and [10].

- **Risk Evaluation:** Each failure mode was assessed using three standard FMEA parameters:
  - Severity (S)
  - Occurrence (O)
  - Detection (D)
- **RPN Calculation:** The Risk Priority Number (RPN) was calculated using:

$$RPN = S \times O \times D$$

- **Risk Prioritization:** Failure modes were prioritized based on their RPN values, where higher values indicate greater risk and require more immediate attention.

3.3.2 FMEA Scaling Procedure

To ensure consistency in risk evaluation, a standardized rating scale was adopted for the three FMEA parameters: Severity (S), Occurrence (O), and Detection (D)[10]. Each parameter was assigned a numerical value ranging from 1 to 10, where higher values indicate greater risk impact, higher likelihood of occurrence, or lower detectability.

- **Severity (S):** Represents the impact of a failure on system performance, safety, and operational continuity.
- **Occurrence (O):** Indicates the likelihood or frequency of the failure occurring.
- **Detection (D):** Reflects the ability of existing controls to detect the failure before it affects the system.

To provide a clear and consistent basis for assigning these values, the rating scale used in this study is presented in Table 3.3 with the reference [10]. This structured scaling approach ensures consistency, repeatability, and objectivity in evaluating risks across different system components.

The Severity (S), Occurrence (O), and Detection (D) ratings for each IT and OT component were assigned using the standardized FMEA rating scale adopted from the literature [10]. The ratings were determined based on the identified failure mode, its potential impact on system operations, cybersecurity, and operational continuity.

For example, unauthorized access to a Remote Terminal Unit (RTU) is assigned a Severity rating of 9 because successful compromise of the RTU could enable attackers to manipulate operational processes, modify critical configurations, and potentially disrupt industrial operations, resulting in significant safety and operational consequences. An Occurrence rating of 7 is assigned because RTUs are often connected to communication networks and may be exposed to cybersecurity threats such as weak authentication mechanisms, misconfigurations, or network-based attacks, making unauthorized access reasonably likely. A Detection rating of 6 is assigned

because unauthorized access attempts may not be immediately identified by existing monitoring and security controls. In OT environments, limited visibility, legacy systems, and insufficient real-time monitoring capabilities can reduce the ability to detect malicious activities before they impact operations.

The RTU example is provided to illustrate the RPN rating assignment process. The same methodology and evaluation criteria were consistently applied across all identified IT and OT components.

The application of the FMEA methodology provides a comprehensive understanding of potential system vulnerabilities. The calculated RPN values enable the identification of critical risk areas, particularly those associated with cybersecurity threats such as unauthorized access and cyberattacks across IT and OT components.
The detailed failure analysis and corresponding risk assessment work is presented in Appendix A.2.

Rating Scale (1-10)	**Severity (S)**	**Severity of Effect (S)**	**Occurance (O)**	**Probable Failure Rate (O)**	**Detection**	**Criteria (D)**
10	Hazardous without warning	Highest severity ranking of a failure mode, occurring without warning and the consequence is hazardous.	Extremely high (inevitable failure)	≥ 1 in 2	Absolutely impossible	Design control does not detect a potential cause of failure or subsequent failure mode or there is no design control.
9	Hazardous with warning	Higher severity ranking of a failure mode, occurring with warning and the consequence is hazardous.	Very high	1 in 3	Very remote	Very remote chance the design control will detect a potential cause of the failure or subsequent failure mode.
8	Very high	Operation of system or product is broken down without compromising safety.	Repeated failures	1 in 8	Remote	Remote chance the design control will detect a potential cause of failure or subsequent failure mode.
7	High	Operation of system or product may be continued, but performance of system or product is affected.	High	1 in 20	Very low	Meager chance the design control will detect a potential cause of failure or subsequent failure mode.
6	Moderate	Operation of system or product is continued, and performance of system or product is degraded.	Moderately high	1 in 80	Low	Low chance the design control will detect a potential cause of failure or subsequent failure mode.
5	Low	Performance of system or product is affected seriously, and the maintenance is needed.	Moderate	1 in 400	Moderate	Moderate chance the design control will detect a potential cause of failure or subsequent failure mode.
4	Very low	Performance of system or product is less affected, and the maintenance may not be needed.	Relatively low	1 in 2,000	Moderately high	Moderately high chance the design control will detect a potential cause of the failure or subsequent failure mode.
3	Minor	System performance and satisfaction with minor effect.	Low	1 in 15,000	High	High chance the design control will detect a potential cause of failure or subsequent failure mode.
2	Very minor	System performance and satisfaction with slight effect.	Remote	1 in 150,000	Very high	Very high chance the design control will detect a potential cause of failure or subsequent failure mode.
1	None	No effect.	Nearly impossible	$\leq$ 1 in 1,500,000	Almost certain	Design control will almost certainly detect a potential cause of failure or subsequent failure mode.

Table 3.1: FMEA Rating Scale

3.4 Component level Security Assessment

This section provides a detailed assessment of security controls across critical system components, with a focus on identifying strengths and potential weaknesses in threat detection and response. Each component is evaluated based on its ability to address specific threat types, the mechanisms employed for monitoring and analysis, the effectiveness of mitigation and recovery strategies, and the assignment of dedicated teams responsible for monitoring, incident response, and system restoration.

The assessment adopts a structured methodology as illustrated in the Figure 3.4 that considers real-world threat scenarios, detection capabilities, and overall operational effectiveness, aligned with established cybersecurity frameworks such as [25] and [41]. Each component is systematically analyzed to understand how it detects and responds to cyber threats within dynamic and evolving environments .

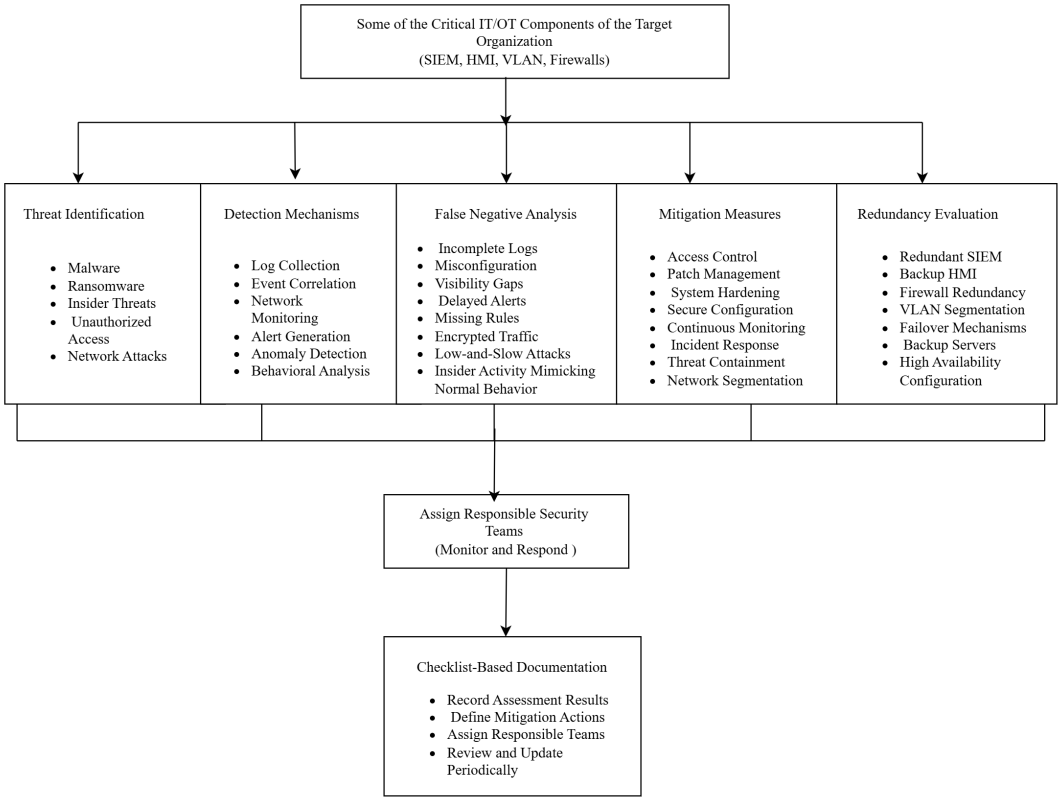

Figure 3.4: Component-Level Security Assessment Framework

The methodology is carried out through the following steps:

1. **Component Identification:** Identification and classification of system critical components such as eg: Security Information and Event Management (SIEM) and firewall systems based on their functional roles [42].
2. **Threat Mapping:** Identification of relevant cyber threats applicable to each component based on known attack vectors and operational context.

3. **Detection Mechanism Evaluation:** Examination of how each component detects threats using monitoring tools, log analysis, and behavioral techniques.
4. **Mitigation Strategy Assessment:** Evaluation of response actions implemented to contain, eliminate, or reduce the impact of identified threats.
5. **Redundancy and Resilience Evaluation:** Analysis of backup systems, failover mechanisms, and high-availability configurations to ensure continuity of operations.
6. **Dedicated Team Assignment:** Allocation of responsibilities to specialized teams for monitoring, incident response, and recovery to ensure accountability and efficiency.
7. **Consolidated Assessment:** Compilation of findings into a structured checklist to provide a comprehensive view of the overall security posture.

A key focus of this assessment is the identification and analysis of false negatives, where security mechanisms fail to detect malicious activity despite its presence. Such detection gaps may arise due to incomplete or misconfigured logging, delayed data ingestion, insufficient correlation rules, limited visibility across systems, or the use of encrypted communication channels. Additionally, attackers may exploit legitimate credentials or mimic normal system behavior, making their activities difficult to distinguish from authorized actions. Advanced techniques, such as low-and-slow attacks and stealthy lateral movement, further increase the likelihood of undetected threats. These challenges highlight the need for continuous monitoring, regular tuning of detection systems, and the integration of multiple data sources to enhance visibility and detection accuracy. Detailed component-wise analysis of threats, detection mechanisms, mitigation strategies, and redundancy measures is provided in Appendix A.3.

The inclusion of dedicated team assignments ensures that responsibilities are clearly defined across monitoring, detection, response, and recovery functions. Specialized teams, including security monitoring units, incident response teams, and network or system administrators, are assigned specific roles to ensure efficient handling of security events. This structured allocation of responsibilities improves coordination, reduces response time, and enables effective mitigation even in cases where threats are not immediately detected. A comprehensive breakdown of component-level responsibilities and corresponding controls is presented in Appendix A.3. Overall, this approach strengthens the security framework by combining technical controls with operational accountability and proactive risk management.

The Component checklist includes both OT and IT component namely Security Information and Event Management (SIEM), Human-Machine Interface (HMI), Virtual Local Area Network (VLAN), and firewalls.

- **SIEM:** Security Information and Event Management (SIEM) is a centralized security system that collects, monitors, and analyzes log data and security events from various devices and applications within an organization. Its main purpose is to detect, analyze, and respond to cyber threats in real time while

supporting incident investigation and compliance. SIEM is widely used in Security Operations Centers (SOC), network and cloud security monitoring, fraud detection, and cyberattack investigation. Its advantages include centralized visibility, faster threat detection, and improved incident response, while limitations include high cost, complex setup, false positives, and the need for skilled professionals to manage it [43] and [42].

- **HMI:** Human Machine Interface (HMI) is a centralized interface that enables communication between humans and machines in industrial and automated systems. Its main purpose is to monitor, control, and manage processes in real time through visual displays and alerts. HMI is commonly used in industrial automation, manufacturing, power systems, and transportation. Its advantages include improved efficiency, real-time monitoring, easier system control, reduced human error, and faster decision-making, while limitations include high implementation cost, cybersecurity risks, system dependency, complex configuration, and the need for trained personnel [44] and[12].
- **VLAN:** Virtual Local Area Network (VLAN) is a network segmentation technology that divides a physical network into multiple logical networks to improve security, management, and performance. Its main purpose is to separate network traffic, reduce broadcast domains, and enable secure communication between different groups or departments. VLANs are widely used in networks, data centers, industrial systems, and cloud environments. Their advantages include improved security, reduced network congestion, better performance, flexibility, and easier network management, while limitations include complex configuration, possible security risks from misconfiguration, dependency on managed switches, and the need for skilled administrators [45] and [46].
- **Firewall:** A firewall is a network security component that monitors and controls incoming and outgoing network traffic based on predefined security rules. Its main purpose is to protect systems and networks from unauthorized access, cyberattacks, and malicious traffic while allowing legitimate communication. Firewalls are widely used in enterprise networks, data centers, cloud environments, and industrial systems. Their advantages include improved network security, traffic filtering, access control, and threat prevention, while limitations include configuration complexity, performance impact, limited protection against internal threats, and the need for regular updates and skilled management [47] and[14].

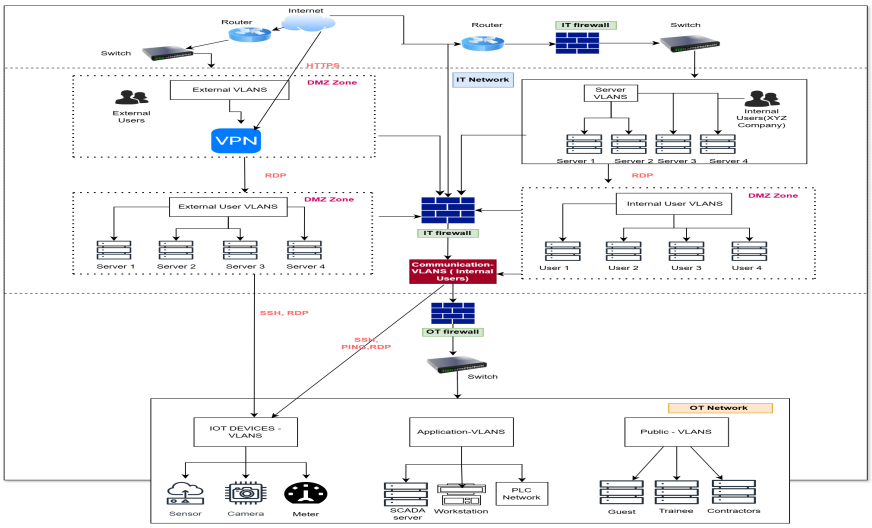

Figure 3.5: Network Segmentation Diagram: The figure illustrates the segmented IT and OT network architecture of the target organization, including VPN access, DMZ zones, VLANs, firewalls, SCADA systems, PLC networks, and IoT devices. Communication between IT and OT environments is controlled through SSH, RDP, HTTPS, and ICMP to improve security and reduce lateral movement.

4

Analysis

This chapter presents the analysis conducted in this thesis, focusing on three main areas. The mapping of NIST standards to the NIS2 Directive determines the level of alignment and identifies existing gaps. Cybersecurity risks in OT components are further analyzed using the FMEA method. In addition, a component-level analysis is provided through an OT and IT component checklist, outlining the corresponding mitigation and redundancy measures. This approach helps identfying existing gaps, thereby improving overall security and strengthening compliance.

4.1 NIST-NIS2 Mapping Analysis

The analysis of the mapping between opted NIST cybersecurity standards of the target organization and the NIS2 Directive demonstrates a strong alignment in technical and operational cybersecurity controls presented in Appendix A.1. Most of the NIST standards implemented within the target organization, including NIST SP 800-37, NIST SP 800-39, and NIST SP 800-53, show comprehensive coverage of NIS2 Articles 20, 21, and 23, which focus on governance, cybersecurity risk management, and incident reporting.

Specifically, standards such as NIST SP 800-63, NIST SP 800-64, and NIST SP 800-160 primarily align with Article 21, which addresses cybersecurity risk management measures. Similarly, NIST SP 800-88 and NIST SP 800-122 provide partial coverage of Articles 20 and 21, particularly in areas related to data protection and operational controls. NIST SP 800-161 and NIST SP 800-171 further reinforce alignment with Articles 20, 21, and 23 by addressing supply chain security and controlled information protection.

In addition, the NIST Cybersecurity Framework (CSF) 2.0 demonstrates broader alignment across multiple NIS2 articles, particularly Articles 7 to 25 and 29 to 37, covering governance, risk management, and operational security measures.

Overall, the findings indicate that NIST standards provide strong coverage of the technical and operational requirements of NIS2.

4.2 Gap Analysis

As discussed in the section 3.2 the mapping process of NIST standard with the NIS2 directive is carried out. This mapping aims to evaluate the alignment of current cybersecurity practices with regulatory expectations and to identify any compliance gaps in the targeted organization.

Despite the strong alignment, several gaps were identified where NIST standards do not fully address NIS2 requirements. These gaps are primarily related to regulatory, governance, and compliance aspects rather than technical controls.
Below Table 4.1 presents the unmapped NIS2 articles of the target organization with the NIST articles with the description of the articles.

Table 4.1: Missing NIS2 Articles of the Target Organization

S. No.	Articles	Description of the Articles
1	Articles 1 to 6 (General Provisions)	Covers the subject matter, scope, and key definitions of the directive. It categorizes entities into "essential" and "important" and requires them to submit their registration data to authorities.
2	Articles 26, 27, 28 (Jurisdiction & Registration)	Establishes rules for legal jurisdiction over digital entities and mandates the creation of registries. Requires specific digital providers to submit data for a central registry and requires domain registries to maintain accurate databases for lawful access.
3	Articles 38, 39, 40 (Delegated Acts & Review)	Outlines legislative procedures granting the power to adopt supplementary rules (delegated acts) and mandates a formal review of the directive's functioning by October 2027.
4	Articles 41 to 46 (Final Provisions)	Contains final legislative actions, including the deadline for Member States to transpose the directive into national law (October 17, 2024), repeal of the old NIS1 Directive, and official entry into force.

The analysis from the Table 4.1 highlights that NIST standards are primarily framework-driven and technical, whereas NIS2 includes legal, organizational, and regulatory obligations. As a result, key gaps exist in areas such as legal compliance, governance structures, enforcement mechanisms, and cross-border coordination.

4.3 FMEA-Based Risk Analysis

The Failure Modes and Effects Analysis (FMEA) provided a structured evaluation of cybersecurity risks across critical OT components A.2. The results indicate that several components exhibit high Risk Priority Numbers (RPN), highlighting significant vulnerabilities within the system.

The highest risks were observed in components such as Remote Terminal Units (RTUs), Supervisory Control and Data Acquisition (SCADA) systems, firewalls, data historians, and Security Information and Event Management (SIEM) systems. These risks are primarily associated with unauthorized access, malware attacks, detection failures, and data corruption.

Key observations include:

- RTU systems exhibit the highest risk severity in the FMEA analysis, with the highest (RPN = 378). The primary effect is unauthorized access caused by weak security controls, which could allow attackers to manipulate RTU configurations or process data remotely. Since RTUs directly control and monitor field operations, successful attacks may result in operational disruption, safety hazards, and loss of remote monitoring capabilities.
- SCADA systems show the second-highest risk level in the FMEA analysis, with (RPN = 336). The elevated risk is mainly associated with malware and ransomware attacks that can compromise centralized monitoring and supervisory control functions. Since SCADA systems are responsible for coordinating industrial operations, successful cyberattacks may disrupt operational visibility, interfere with process control, and affect the continuity and safety of industrial processes.
- Firewalls show a high cybersecurity risk in the FMEA analysis, with (RPN = 336). The major concern is the inability to identify sophisticated or encrypted malicious payloads, which may allow harmful traffic to bypass network security controls. Such weaknesses can expose OT devices to unauthorized access, lateral movement, and advanced cyber threats within the industrial network.
- Data historians are particularly vulnerable to data corruption and encryption caused by malware or ransomware attacks (RPN = 336). Since these systems store critical operational records, compromised data can affect system analysis, reduce decision-making accuracy, and delay incident response and recovery activities. This may lead to incorrect operational assessments, reduced visibility into system performance, and difficulties in identifying the root cause of failures.
- SIEM systems show a high cybersecurity risk due to failures in detecting advanced threats and malicious activities (RPN = 336). Misconfigured detection rules, outdated signatures, or delayed event analysis can allow cyberattacks to remain unnoticed within the network. This can delay incident response and allow attackers to move across IT/OT environments without detection. This may lead to security breaches may escalate, leading to operational disruptions, system downtime, and increased damage to critical infrastructure.

The analysis further reveals that several risks are characterized by high severity and low detectability, making them critical.This highlights the need for stronger monitoring mechanisms, improved threat detection capabilities, and enhanced security controls to reduce the overall cybersecurity risk within the OT/IT environment. The highest Risk Priority Number (RPN) identified for each component is illustrated in figure 4.1.

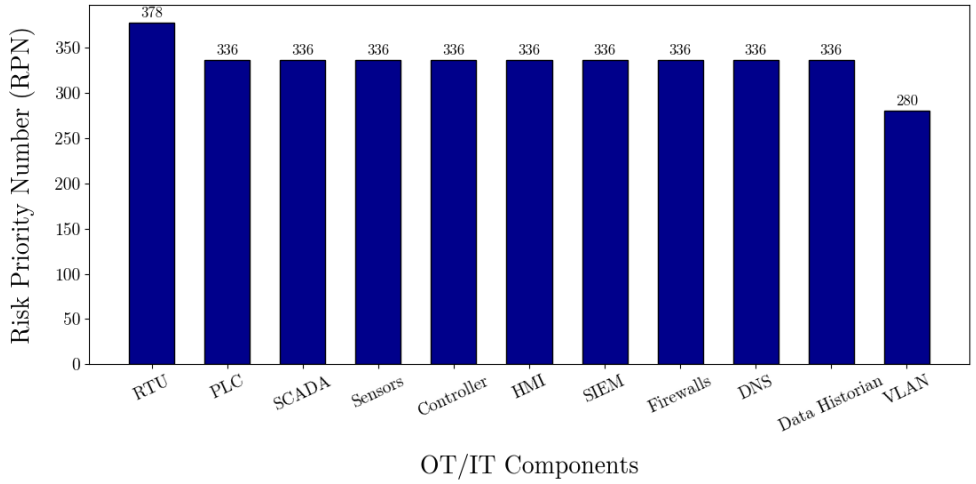

Figure 4.1: Maximum Risk Priority Number (RPN) Across OT/IT Components

4.4 Component-Level Security Analysis

The component-level checklist developed for Security Information and Event Management (SIEM), Human-Machine Interface (HMI), and Virtual Local Area Network (VLAN), and Firewall provided a structured approach to evaluate security controls across critical systems in the target organization [11], [12], [13] and [14]. It ensured that each component is assessed for its ability to detect threats, implement appropriate mitigation measures, and ensure redundancy for system availability. This analysis facilitated the evaluation of the checklist and supported effective decision-making within the targeted organization. The component-level assessment highlights both strengths and limitations in the current cybersecurity architecture presented in Appendix A.3.

4.4.1 Strengths

- Based on the component-level assessment checklist, the use of Security Information and Event Management (SIEM) is identified as a key strength within the targeted organization. The checklist enables a structured evaluation of how SIEM detects threats, handles potential false negatives, and supports mitigation strategies [43]. This checklist helps the organization clearly understand the effectiveness of its monitoring capabilities and identify any detection gaps. As a result, it supports informed decision-making, improves threat visibility, and enhances the target organization's ability to proactively manage cybersecurity risks.
- Firewalls are identified as a significant strength within the targeted organization, as their effectiveness can be evaluated using the assessment checklist. The checklist enables the analysis of firewall capabilities in terms of threat detection, mitigation measures and redundancy. By examining how security

rules are applied and identifying potential gaps such as missed threats, it provides a clear understanding of overall network security effectiveness [48]. This approach supports the target organization organization in strengthening its perimeter defenses, reducing unauthorized access, and making informed decisions regarding rule optimization and security improvements.

- VLAN implementation is identified as an important strength in enhancing network segmentation and security. The structured evaluation enables the target organization to assess how effectively VLANs limit threat propagation and support incident isolation measures [46]. By examining potential weaknesses, such as segmentation gaps or misconfigurations, the checklist helps improve network isolation and reduces the impact of security incidents. This contributes to a more resilient and controlled network environment [49].
- Human-Machine Interfaces (HMI) are identified as a strength in supporting operational monitoring and anomaly detection within the targeted organization. The assessment checklist enables the evaluation of threats, detection capabilities, and mitigation measures associated with HMI [12]. This provides insights into how HMI contributes to identifying abnormal system behavior and potential security issues. As a result, it enhances situational awareness, supports timely response to incidents, and improves overall operational security.

4.4.2 Limitations

- The checklist relies on predefined evaluation criteria, including detection capabilities, false negatives, mitigation, and redundancy. While this ensures consistency, it may not fully capture dynamic and evolving threats within the operational environment [50]. As a result, advanced or previously unseen attack scenarios may not be adequately reflected.

The overall analysis indicated that the organization had a strong technical cybersecurity foundation based on National Institute of Standards and Technology (NIST) standards; however, it lacked full alignment with NIS2 Directive regulatory requirements [15] and [3]. The primary gap was observed in governance, compliance, and regulatory alignment rather than in technical implementation. Failure Mode and Effects Analysis (FMEA) is a systematic method used to identify potential failures, assess their impact, and prioritize associated risks, thereby supporting proactive risk management through the evaluation of vulnerabilities [51]. In addition, component-level assessment is a structured approach used to evaluate the security controls and functionalities of individual system components, focusing on their contribution to threat detection, mitigation, and overall system protection.

5

Results

This chapter presents the results of the cybersecurity assessment conducted in this study. It includes the NIST-to-NIS2 mapping results, identified gaps, FMEA-based high-risk findings, risk distribution, key findings, and component-level security analysis results.

5.1 NIST-NIS2 Mapping Results

The table 5.1 below present the results derived from the analysis conducted using the checklist provided in Appendix A.1 of NIST with NIS2 mapping .The checklist was developed to systematically map NIST standards against the requirements of the NIS2 Directive. Each control and framework component was evaluated to identify alignment, overlaps, and gaps. The below Table 5.1 results highlight how existing cybersecurity standards of the target organization support regulatory compliance while also revealing areas where additional measures are required. This structured approach ensures traceability between technical controls and regulatory obligations, providing a clear basis for risk assessment and compliance evaluation.

Table 5.1: NIST to NIS2 Mapping

NIST Standard	**Mapped NIS2 Articles**
NIST SP 800-37	20, 21, 23
NIST SP 800-39	20, 21, 23
NIST SP 800-53	20, 21, 23
NIST SP 800-63	21
NIST SP 800-64	21
NIST SP 800-88	20, 21
NIST SP 800-122	21, 23
NIST SP 800-160	21
NIST SP 800-161	20, 21, 23
NIST SP 800-171	21, 23
NIST CSF 2.0	7–25, 29–37

5.2 Gap Analysis Results

The Table 5.2 below presents the gap analysis results derived from the checklist provided in Appendix A.1, which maps NIST standards to the NIS2 Directive requirements. The checklist was systematically used to identify areas where NIST frameworks do not fully address specific NIS2 obligations. Each control, process, and requirement was evaluated to determine missing coverage, partial alignment, or lack of direct mapping. Table 5.2 highlights the identified gaps, particularly in governance, regulatory compliance, and information-sharing provisions. These results indicate that while NIST standards of target organization provide strong technical and operational security controls, additional organizational and regulatory measures are required to achieve full NIS2 compliance. This gap supports a clearer understanding of compliance limitations and helps organizations prioritize improvements for aligning with NIS2 requirements.

Table 5.2: Unmapped NIS2 Articles

Articles	**Description of the Articles**
Articles 1–6 (General Provisions)	Covers the scope, subject matter, key definitions, and classification of entities as “essential” and “important”.
Articles 26–28 (Jurisdiction & Registration)	Defines jurisdiction rules, entity registration requirements, and maintenance of accurate registries and databases.
Articles 38–40 (Delegated Acts & Review)	Establishes delegated legislative powers and mandates periodic review of the directive implementation.
Articles 41–46 (Final Provisions)	Includes final implementation measures, repeal of NIS1, transposition deadlines, and entry into force of the directive.

5.3 FMEA High-Risk Results

The Table 5.3 below presents the high risk results identified through the Failure Modes and Effects Analysis (FMEA) conducted on key system components A.2. The analysis was performed using a structured checklist approach, where potential failure modes, their causes, and impacts were evaluated to determine risk levels. Each failure scenario was assessed based on Severity (S), Occurrence (O), and Detection (D) ratings, and the Risk Priority Number (RPN) was calculated to prioritize risks. Table 5.3 highlights the components with the highest RPN values, indicating critical vulnerabilities within the system. The results show that core operational technologies, such as RTU and SCADA systems, are particularly susceptible to cybersecurity threats, including unauthorized access and malware attacks. These findings emphasize the need for enhanced security controls, improved monitoring mechanisms, and stronger detection capabilities to reduce overall system risk and ensure resilient operations.

Table 5.3: High-Risk Components Based on FMEA

Component	Failure Mode	Impact	RPN
RTU	Unauthorized Access	Manipulation of processes causing disruption and safety risks	378
SCADA	Malware/Ransomware	Large-scale disruption of industrial operations	336
Firewalls	Payload Inspection Failure	Undetected malicious traffic	336
Data Historian	Data Corruption	Loss of operational insight	336
SIEM	Detection Failure	Undetected cyberattacks	336

5.4 Risk Distribution

The results indicate that high risks are concentrated in core OT components, while detection-related weaknesses contribute significantly to overall system risk. Core OT components tend to demonstrate greater risk levels because failures in these systems may directly affect system functionality and operational continuity. In addition, variations in RPN values across the analyzed components indicate that some systems require greater attention due to their potential impact on cybersecurity and system performance. This distribution of risk highlights the importance of prioritizing security and mitigation efforts toward higher-risk components to improve system reliability and cybersecurity resilience.

5.5 Key Findings

1. **NIST standards provide strong technical cybersecurity coverage:**

   The NIST Cybersecurity Framework provides comprehensive guidance for identifying, protecting, detecting, responding to, and recovering from cyber threats. It strengthens IT and OT security through structured controls and best practices. The framework mainly focuses on technical and operational cybersecurity measures rather than legal compliance requirements. Therefore, the target organization may still require additional regulations or frameworks to meet full compliance requirements.

2. **NIS2 introduces additional regulatory requirements not covered by NIST:**

   The NIS2 Directive emphasizes governance, accountability, incident reporting, supply chain security, and legal compliance. It also places greater responsibility on management to ensure cybersecurity preparedness and incident response. Unlike NIST, NIS2 includes mandatory compliance obligations for organizations. As a result, the target organization may face compliance gaps and increased regulatory risks if relying only on NIST.

3. **Significant gaps exist in governance and compliance areas:**

Gaps in cybersecurity governance, policies, and accountability can reduce the effectiveness of security measures. Limited oversight and unclear responsibilities may create inconsistencies in cybersecurity implementation. Organizations may face difficulties in maintaining regulatory compliance without proper governance structures. This can lead to poor coordination, compliance failures, and delayed responses to cyber incidents in the target organization.

4. **OT components present the highest cybersecurity risks:**

   OT systems are highly vulnerable because many legacy systems lack built-in cybersecurity protections and are difficult to update. These systems often prioritize operational continuity, limiting the use of frequent security patches and updates. Additionally, many OT environments have limited visibility and monitoring capabilities. As a result, cyberattacks on OT environments may disrupt operations, impact safety, and result in significant financial losses.

5. **Detection mechanisms are insufficient for advanced threats:**

   Current detection methods, especially signature-based systems, may have limitations in identifying advanced cyber threats. These threats can evade traditional detection approaches due to their unknown or evolving nature. Limited real-time monitoring further reduces the ability to identify threats quickly. This can delay threat identification and increase the severity of cyber incidents.

6. **IT-OT integration increases vulnerability exposure:**

   The integration of IT and OT systems improves efficiency by enabling better communication, automation, and data exchange. However, increased connectivity also expands the attack surface between networks. Differences in security requirements between IT and OT systems can make cybersecurity management more complex. As a result, vulnerabilities may increase, leading to operational disruptions and higher cybersecurity risks.

5.6 Component-Level Security Analysis Results

The following table presents the summarized results of the component-level security analysis detailed in Appendix A.3. This structured assessment evaluates the cybersecurity posture of critical IT and OT components within the target organization, specifically focusing on Security Information and Event Management (SIEM), Firewalls, Human-Machine Interfaces (HMI), and Virtual Local Area Networks (VLANs). Each component was analyzed to evaluate its capability to detect cyber threats, identify vulnerabilities such as potential false negatives (missed threats), and determine the mitigation and redundancy measures required to maintain operational continuity and system resilience [43], [12], [49] and [14].

Table 5.4: Results of Component-Level Security Assessment

Component	Key Threats Evaluated	Detection Mechanisms & Vulnerabilities	False Negatives (Missed Threats)	Mitigation & Redundancy Measures	Responsible SecurityTeams
SIEM	Policy violations, APTs, insider threats, ransomware, malware, and MitM attacks.	Uses correlation rules, behavioral baselines (UEBA), and supervised/unsupervised learning techniques.	Fails due to model drift, incomplete telemetry, static rules, or subtle attacks mimicking normal behavior.	**Mitigation:** Rule tuning, ML retraining, and standardized playbooks. **Redundancy:**Multiple correlation engines and offline/immutable backups.	SOC (Tiers 1, 2, 3), Detection Engineering, Threat Hunting, Incident Response, Endpoint Security, and IAM Teams.
Firewalls	DDoS, APTs, SYN Floods, ICMP Floods, and reconnaissance probing.	Uses static rule enforcement, packet header checks, AI anomaly detection, and stateful tracking.	Static rules miss dynamic attacks; high latency in virtual firewalls masks threats; slow-rate attacks bypass thresholds.	**Mitigation:** Dynamic updates via SDN, containerized architectures, and Moving Target Defense (MTD). **Redundancy:** Backup servers and parallel IDS containers.	Network Security Team, SOC, Cloud Security, Security Engineering, Threat Hunting, and IAM Teams.
HMI	Display manipulation, alarm suppression, unauthorized access, and legacy system exploits.	Threats materialize through compromised channels, weak authentication, or unpatched legacy OS vulnerabilities.	Attackers may suppress alarms or manipulate maintenance logs, causing delayed operator responses.	**Mitigation:** RBAC, MFA, system hardening, and data integrity validation. **Redundancy:** Redundant sensors, digital twins, and independent displays.	OT Security Team, SOC, IAM Team, OT Engineering, and Incident Response Teams.
VLAN	Switching loops, switch spoofing, double tagging, and ARP poisoning (MitM).	Attacks exploit misconfigurations, Dynamic Trunking Protocol (DTP), or multiple links causing broadcast storms.	Network isolation failures allow attackers to bypass segmentation and move laterally between IT and OT systems.	**Mitigation:** STP, port security, DHCP snooping, and disabling DTP/unused ports. **Redundancy:** Backup switches with identical VLAN/ACL configurations and redundant links.	Network Engineering, Network Security, SOC, IAM, and Incident Response Teams.

Key Findings

1. **Threat Detection Limitations and False Negatives:** The evaluation presented in the Table 5.4 demonstrated that advanced threats and subtle malicious activities can evade detection mechanisms, resulting in false negatives. This commonly occurs due to incomplete logging, reliance on static rule-based logic, encrypted malicious payloads, or sophisticated attackers mimicking legitimate user behavior within the network . These findings indicate that traditional signature-based detection systems are insufficient for identifying dynamic or previously unseen attacks.

2. **Component-Specific Vulnerabilities:** The component-level analysis identified significant vulnerabilities across critical IT and OT systems resulting from operational dependencies and IT/OT convergence. Key weaknesses include unpatched legacy operating systems in Human-Machine Interfaces (HMIs), high latency in virtual firewalls masking time-sensitive threats, and improper VLAN segmentation enabling lateral movement between IT and OT environments.

3. **Dynamic Mitigation Measures:** The assessment emphasized the importance of implementing robust mitigation mechanisms to address identified vulnerabilities and detection gaps. Recommended measures include continuous SIEM rule tuning, strict Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), and automated integrity validation processes to strengthen system resilience and reduce cybersecurity risks.

4. **Robust Redundancy Controls:** Reliable redundancy mechanisms were identified as essential for ensuring operational continuity and minimizing the impact of cyberattacks or component failures. Important measures include backup switches with identical Access Control List (ACL) configurations, cross-

validation using redundant sensors or digital twins, and maintaining offline immutable backups for rapid restoration following ransomware incidents.

5. **Dedicated Response Teams and Responsibilities:** The structured allocation of responsibilities to specialized teams such as SOC (Tier 1, Tier 2, and Tier 3), Incident Response, Threat Hunting, and Network Security teams was identified as a critical organizational defense mechanism. Clearly defined roles improve accountability, enhance coordination, and significantly reduce response times during cybersecurity incidents.

6

Recommendations

This chapter presents the recommendations derived from the findings and analysis conducted in this study. The recommendations focus on improving cybersecurity resilience, strengthening IT and OT security practices.

6.1 Gaps in NIST–NIS2 Alignment

Based on the analysis the identified gaps between NIST standards and the NIS2 Directive, several gaps remained at the policy level, particularly in areas related to legal provisions, governance structures, accountability, and enforcement mechanisms, as reflected in NIS2 Articles 1–6, 26–28, 38–40, and 41–46. A detailed table outlining the missing articles is provided in the Table 4.1

It is recommended that appropriate measures be introduced to cover these gaps identified in the NIS2 Directive. Furthermore, after implementing these measures, the gap analysis should be performed again using the same methodological steps to ensure that all identified gaps have been addressed and that no remaining gaps exist.

6.2 Adoption of NIST SP 800-171 Rev. 3

It is observed that the target organization had been using NIST SP 800-171 Rev. 2 (2021) to protect Controlled Unclassified Information (CUI) [24]. Rev. 2 provided a structured framework consisting of 110 security requirements across 14 control families, aligned with NIST SP 800-53B. It included clarified scope guidance, such as CUI isolation and defined isolation methods, along with minor editorial updates. However, the review indicated that adopting NIST SP 800-171 Rev. 3(2024) would be beneficial [21]. The updated revision offered enhanced and modernized security controls designed to address evolving cyber threats and reduce potential vulnerabilities that may not have been fully covered in the earlier version.

The recommendation to adopt NIST SP 800-171 Rev. 3 is based on its improved structure, enhanced control coverage, reduced the number of controls from 110 to 97 by consolidating and strengthening requirements. It also introduced 3 new control families: Planning, System and Services Acquisition, and Supply Chain Risk Management is provided in table A.8 , which addressed modern cybersecurity challenges not explicitly covered in Rev. 2. Furthermore, the inclusion of Organization-Defined

Parameters (ODPs), which are organization-specific values that must be defined for certain controls (e.g., frequency, thresholds, or limits), enabled the target organization to tailor security requirements, thereby improving adaptability and precision in implementation as presented in A.9.

Several security risks were identified in NIST SP 800-171 Rev. 2, including limited guidance on supply chain risk management, lack of explicit requirements for secure system acquisition, and ambiguity in control implementation due to generalized language. These gaps could lead to inconsistent security practices and increased exposure to risks, particularly from third-party dependencies and evolving cyber threats. NIST SP 800-171 Rev. 3 addressed these concerns by introducing dedicated controls for supply chain risk management, strengthening system acquisition requirements, and incorporating organization-defined parameters (ODPs) to ensure clearer and more precise implementation of security controls [21].

When the target organization adopted NIST SP 800-171 Rev. 3, an improvement in overall cybersecurity maturity and resilience was anticipated. The enhanced NIST SP 800-171 Rev. 3 was expected to provide stronger protection for CUI, improved risk management across the supply chain, and better alignment with federal cybersecurity standards. The advantages of using Rev. 3 included increased clarity in control implementation, greater flexibility through organization-defined parameters, improved audit readiness, and a more comprehensive defense against emerging cyber threats. As a result, the transition to newly revised NIST SP 800-171 Rev. 3 will be considered a strategic step toward achieving a more secure, scalable, and future-ready cybersecurity posture for the target organization [21].

6.3 RPN-Based Risk Mitigation for Critical Components

In the FMEA-based analysis, components with the highest Risk Priority Number (RPN) scores were considered to have greater cybersecurity vulnerabilities and therefore required immediate mitigation measures to reduce potential risks and strengthen the overall security of the OT system.

The Remote Terminal Unit (RTU) recorded the highest Risk Priority Number (RPN) score of 378, indicating the need for immediate mitigation measures [52]. To reduce the risk of unauthorized access, the following mitigation measures are:

- Stronger access control and authentication mechanisms ensure that only authorized personnel could access RTU functions.
- Role-Based Access Control (RBAC) to assign access permissions according to operational responsibilities, minimizing unnecessary privileges and limiting unauthorized activities.
- Secure authorization mechanisms to control user access and prevent unauthorized modification of RTU operations.

- Security hardening measures, including the reduction of unnecessary system functionalities and the implementation of a minimal operating environment, to minimize vulnerabilities and improve the overall security posture of RTUs.

The SCADA system recorded a Risk Priority Number (RPN) score of 336. To reduce the risk of malware and ransomware attacks through network vulnerabilities,the following mitigation measures are [53]:

- Implementation of network segmentation and isolation mechanisms to separate SCADA systems from external and corporate Information Technology (IT) networks, thereby minimizing unauthorized access and limiting the spread of malware across interconnected environments.
- Establishment of access control and authentication mechanisms to ensure that only authorized personnel could access SCADA systems and perform critical operational functions.
- Deployment of intrusion detection and continuous monitoring mechanisms to identify abnormal system behavior, suspicious network activities, and early indicators of cyberattacks targeting SCADA environments.
- Regular software updates and security maintenance practices to address known vulnerabilities and reduce the likelihood of malware exploiting outdated system components.

The Firewalls recorded a Risk Priority Number (RPN) score of 336. To reduce the risk associated with the inability to inspect malicious payloads caused by encrypted traffic,the following mitigation measures are:

- AI/ML-based anomaly detection to identify suspicious or unusual network behavior that may not be detected by traditional signature-based firewall mechanisms. This was suggested for detecting previously unknown and evolving threats [54].
- Enable Dynamic Policy Enforcement Firewall policies should be adaptive and updated in real time based on risk assessment and contextual factors such as user behavior, device posture, and network activity. This reduces dependency on static security policies that may become ineffective against changing threats [55].

The Security Information and Event Management (SIEM) system recorded a Risk Priority Number (RPN) score of 336. To reduce the risk associated with the failure to detect threats caused by misconfigured rules and outdated detection signatures,the following mitigation measures are:

- Integration of Artificial Intelligence (AI) and Machine Learning (ML)-based analytics within SIEM systems to improve anomaly detection and strengthen the identification of suspicious activities that may not be detected through conventional rule-based mechanisms [56].
- Continuous monitoring and behavioral analysis mechanisms to identify unusual network activities and deviations from normal system behavior, thereby

enhancing overall threat visibility and detection accuracy [56].

6.4 Monitoring Framework for Assessing the Regulatory Fitness of Security System

Recent research emphasizes that while governments and regulatory bodies are actively introducing comprehensive cybersecurity regulations, such as the European Union's NIS2 Directive[5] for critical infrastructure, the technical infrastructure required to practically enforce these regulations and continuously assess a system's regulatory fitness after deployment remains limited. High risk operational environments are dynamic in nature; therefore, relying solely on conventional one time security audits is often insufficient, as complex systems continuously evolve and their security posture may degrade over time.

To address this gap within the target organization's Operational Technology (OT) and Information Technology (IT) environments, it is recommended to implement an automated monitoring framework conceptually inspired by the Secure Framework for AI Regulation (SFAIR) [57]. Instead of performing static compliance checks, this approach can help enabling automatic and recurrent evaluations of deployed security controls.

For example, by integrating the NIST to NIS2 mapping framework and the component level security checklists developed in this thesis into an automated assessor monitor architecture, the organization can recurrently evaluate the operational capabilities of critical components such as RTUs, SCADA systems, and firewalls. The results of these recurrent assessments can be utilized to calculate regulatory fitness score to ensure the security system's ongoing regulatory fitness.

6.5 Zero Trust Analysis

Network Segmentation and Secure Data Transfer: Effective network segmentation and secure data transfer mechanisms are essential for reducing unauthorized access and Man-in-the-Middle (MITM) attacks within IT and OT environments [58]. At the *Organizational Level:* Organizations should transition from traditional VLAN architectures to Zero Trust Segmentation (ZTS) and micro-segmentation models to eliminate implicit trust across the network [59]. At the *Technical Level:* Micro-segmentation, Access Proxies, and Next-Generation Firewalls (NGFWs) should be utilized to regulate east-west traffic and continuously validate device identity and security posture [58], [37]. Secure communication should also be enforced through robust encryption algorithms, Trusted Platform Modules (TPMs), Trusted Execution Environments (TEEs), and Public Key Infrastructure (PKI) to ensure trusted data transfers [37]. At the *Operational Level:* Organizations should continuously monitor communication channels and maintain secure authentication and integrity validation practices across operational environments [59].

Secure Transfer of Data and Programs: The following practices are aligned with Zero Trust Architecture (ZTA) principles and support secure communication, access control, and data integrity within IT and OT environments [58]. At the *Organizational Level:* Organizations should enforce the principle of least privilege to minimize unauthorized access and accidental user errors [60]. At the *Technical Level:* Attribute-Based Access Control (ABAC), Function-Based Access Control (FBAC), automated data classification, Digital Rights Management (DRM), and Data Loss Prevention (DLP) mechanisms should be implemented to protect sensitive operational data [59], [40] and [60]. At the *Operational Level:* Continuous monitoring of critical files and configurations should be maintained to prevent unauthorized modifications and integrity violations during data and program transfers [58], [59].

Disaster Recovery and Incident Preparedness: The following practices are aligned with Zero Trust Architecture (ZTA) principles and support organizational resilience and rapid recovery during cybersecurity incidents within IT and OT environments [59]. At the *Organizational Level:* Organizations should adopt an "assume breach" mentality and establish incident response strategies aligned with Zero Trust principles [60]. At the *Technical Level:* Zero Trust Segmentation (ZTS) should be implemented to isolate critical assets and reduce the blast radius of cyberattacks. Enterprise IT, Operational IT, and Process Control environments should also support rapid logical or physical isolation during incidents [60]. At the *Operational Level:* Robust Backup and Recovery (B&R) mechanisms, incremental backups, and secure configuration management processes should be maintained to restore systems to validated operational states following disruptions [58], [40] and [60].

OT Security Monitoring and Zero Trust Adoption: Traditional OT security approaches based on static audits and perimeter firewalls are insufficient for modern interconnected industrial environments [58]. Organizations should implement continuous monitoring, real-time posture assessments, and Zero Trust Policy Decision Points (PDPs) to validate device compliance before granting access [60]. OT systems should also be integrated with SIEM, EDR/XDR, and UEBA solutions to improve anomaly detection and visibility across operational infrastructures [37] and [40]. Although challenges such as legacy systems and operational constraints slow adoption, Zero Trust Architecture (ZTA) significantly improves visibility, access control, threat containment, and cyber resilience within OT environments [59] and [58].

7

Discussion and Limitations

This chapter discusses the key findings of the study and analyzes the relationship between existing NIST cybersecurity standards and the regulatory requirements of the NIS2 Directive. It further evaluates the cybersecurity risks identified in integrated IT and OT environments through the proposed FMEA based assessment approach. Finally, the chapter outlines the main limitations of the thesis work.

7.1 Discussion

The results of this study highlight a clear distinction between technical cybersecurity implementation and regulatory compliance requirements. While the mapping between NIST standards and the NIS2 Directive demonstrates strong alignment in technical and operational domains, several gaps remain in governance, legal, and organizational aspects [15] and [4].

The strong alignment observed with Articles 20, 21, and 23 indicates that NIST standards provide a solid foundation for cybersecurity risk management, incident response, and system protection. This confirms that widely adopted frameworks such as NIST are effective in addressing core cybersecurity challenges in both IT and OT environments [61]. However, the absence of coverage for Articles 1-6, 26-28, and 38-46 reveals that NIST standards do not fully address regulatory compliance requirements, particularly those related to legal obligations, enforcement, and cross-border cooperation [8].

This gap can be attributed to the fundamental difference between NIST and NIS2. NIST is designed as a flexible, risk-based framework focused on technical controls and best practices, whereas NIS2 is a regulatory directive that enforces legal accountability, governance structures, and compliance obligations [20] and [4]. As a result, organizations relying solely on NIST may achieve strong technical security but still fall short of regulatory compliance.

The FMEA-based risk analysis further emphasizes the critical vulnerabilities present in operational technology environments [51]. High-risk components such as RTUs and SCADA systems demonstrate significant exposure due to legacy system design, lack of security mechanisms, and direct interaction with physical processes. These findings are consistent with existing literature, which highlights that OT systems prioritize availability and safety over security, making them attractive targets for

cyberattacks.

Another important observation is the limitation of detection mechanisms, particularly in systems such as SIEM and firewalls [42] and [47]. The presence of high RPN values associated with detection failures indicates that many cyber threats may remain undetected, especially those involving stealthy or low-and-slow attack techniques. This reinforces the need for improved monitoring, visibility, and advanced detection capabilities.

The integration of IT and OT systems further increases the complexity of cybersecurity management [3]. While integration enhances operational efficiency, it also expands the attack surface and introduces new vulnerabilities. This creates additional challenges in implementing consistent security controls across heterogeneous environments.

Despite the comprehensive approach adopted in this study, several limitations must be acknowledged. The analysis is based on a single target organization, which may limit the generalizability of the findings. Organizations may have different systems, security practices, and operational requirements. Therefore, the findings, mappings, and recommendations presented in this thesis are specific to the target organization and may need to be adjusted before being applied to other organizations. The recommendation presented in this thesis aim to support both regulatory compliance and overall cybersecurity posture of the target organization.

Additionally, the high-level nature of the NIS2 Directive requires interpretation, which may introduce subjectivity into the mapping process. To strengthen confidence in the mapping results, future research should incorporate independent validation procedures, inter-rater reliability assessments, and alternative mapping interpretations to better control subjective judgment and improve the robustness of the analysis[8]. Furthermore, the Failure Mode and Effects Analysis (FMEA) method relies on qualitative assessments, which may vary depending on expert judgment. Since the scores were assigned based on available architectural documentation and literature review rather than empirical penetration testing data, the resulting Risk Priority Numbers (RPNs) should be interpreted with caution as discussed in Sections 3.3 5. Therefore, the relative ranking of identified risks is considered more valuable for prioritizing mitigation efforts than the absolute RPN values themselves as discussed in Section 3.3.

7.2 Limitations

- **Limited Access to Sensitive Company Data:** One of the primary limitations of this research is the restricted access to highly sensitive and classified organizational data. Since target organization operates within a critical Operational Technology (OT) environment, certain network configurations, legacy vulnerabilities, and proprietary system details could not be fully disclosed for analysis. As a result, the gap analysis and FMEA assessment were based only on the accessible architectural information and documentation provided by the

target organization, which may limit the overall depth and granularity of the findings.

- **Scope Management:** To maintain the defined project scope and complete the research within the planned timeframe, the study was primarily limited to mapping existing NIST cybersecurity practices to NIS2 requirements and evaluating them using the FMEA methodology and making an component level security assessment. The proposed mitigation strategies and recommendations were therefore based on literature reviews, established standards, and expert insights. Furthermore, the analysis focused mainly on selected high risk OT and IT components identified during the study, rather than performing a complete assessment of all target organizational systems.

8

Conclusion

The European Union has introduced comprehensive regulatory measures, such as the NIS2 Directive, to establish a high common level of cybersecurity across essential and important entities, particularly as IT and OT environments increasingly converge [4]. Yet, structured methodologies to effectively translate these abstract regulatory requirements into practical, analyzable operational technology (OT) security measures remain limited.

In this thesis, key compliance challenges in OT environments were identified, and a structured methodology was proposed to align existing National Institute of Standards and Technology (NIST) frameworks with NIS2 regulatory obligations of the target organization in Section 3.2. A comprehensive NIST to NIS2 mapping checklist was introduced to evaluate regulatory fitness, and a Failure Modes and Effects Analysis (FMEA) table was developed to systematically assess cybersecurity risks in integrated IT/OT environments in Chapter . In addition, a component level security assessment checklist was designed to evaluate threat detection capabilities, mitigation strategies, and redundancy across critical infrastructure elements, including SIEM, HMIs, VLANs, and firewalls as developed in Chapter 3.

The evaluation demonstrated that existing NIST standards provide a strong foundation for technical and operational cybersecurity. However, significant gaps remain in governance, legal accountability, and regulatory enforcement mechanisms as results presented in Section 5. The practical utility of the FMEA based approach was validated by identifying critical high risk vulnerabilities in core legacy OT systems, such as RTUs and SCADA systems, emphasizing that current detection mechanisms are often insufficient against advanced cyber threats. Finally, to support regulatory alignment and assist industrial organizations in securing physical processes, structured and actionable recommendations were provided, including the adoption of the modernized NIST SP 800-171 Rev. 3 standard. These recommendations equip target organizations with strategies to proactively manage vulnerabilities, achieve NIS2 compliance, and improve overall cybersecurity resilience as presented in Chapter 6.

9

Future Scope

This chapter outlines potential directions for extending and improving the research presented in this thesis.

- **Empirical Validation and Penetration Testing:** Future research can focus on the practical implementation and validation of the proposed recommendation strategies within OT environments. This may include establishing controlled OT testbeds or conducting penetration testing on critical components such as RTUs, SCADA systems, and firewalls to evaluate the real world effectiveness of the recommended security controls against active cyber threats.
- **Expanding the Framework to Other Critical Sectors:** Since this research was conducted as a single industrial case study at the target organization future work can apply the proposed NIST to NIS2 mapping framework and FMEA methodology to other manufacturing environments and critical sectors such as energy, transportation, and healthcare. This would help evaluate the generalizability of the framework and support the development of a more standardized approach for NIS2 compliance across different industries.

Bibliography

[1] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, and V. Pillitteri, *Guide to Operational Technology (OT) Security*. Gaithersburg, MD, USA, Sep. 2023. DOI: 10.6028/NIST.SP.800-82r3. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/82/r3/final.

[2] Wikipedia contributors, *Operational technology*, Accessed: 2026-05-05, 2026. [Online]. Available: https://en.wikipedia.org/wiki/Operational_technology.

[3] N. Andersson, "The effect of the it/ot gap on the nis 2 implementation," M.S. thesis, Stockholm University, Department of Computer and Systems Sciences, 2023.

[4] European Parliament and Council of the European Union, *Directive (eu) 2022/2555 of the european parliament and of the council of 14 december 2022 on measures for a high common level of cybersecurity across the union*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555, OJ L 333, 27.12.2022, pp. 80–152, 2022.

[5] European Parliament and Council of the European Union, *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555, Official Journal of the European Union, OJ L 333, 27 December 2022, pp. 80–152, 2022.

[6] National Institute of Standards and Technology, "The nist cybersecurity framework (csf) 2.0," U.S. Department of Commerce, Tech. Rep. NIST CSWP 29, 2024, Published February 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[7] B. Hunorfi, "Cybersecurity of operational technology in critical infrastructures," *Belügyi Szemle*, vol. 73, no. Special Issue 1, pp. 183–198, 2025, Accessed: 2026-05-06. DOI: 10.38146/BSZ-AJIA.2025.v73.i1.pp183-198. [Online]. Available: https://www.researchgate.net/publication/393111322_Cybersecurity_of_Operational_Technology_in_Critical_Infrastructures.

[8] J. Ruohonen, "A systematic literature review on the nis2 directive," *arXiv preprint arXiv:2412.08084*, 2024, Accessed: 2026-05-14. DOI: 10.48550/arXiv.2412.08084. [Online]. Available: https://arxiv.org/abs/2412.08084.

[9] J. Parsola, "Cybersecurity risk assessment and management for organizational security," *NeuroQuantology*, vol. 20, no. 5, pp. 5330–5337, 2022, Accessed: 2026-05-06. DOI: 10.48047/nq.2022.20.5.nq22815. [Online]. Available: https://

pdfs.semanticscholar.org/5af8/15da2b581b0338fc3a8bf4ba3f8821334d75.pdf.

[10] S. K. Akula and H. Salehfar, "Risk-based classical failure mode and effect analysis (fmea) of microgrid cyber-physical energy systems," *arXiv preprint arXiv:2108.10349*, Aug. 2021, Accessed: 2026-05-06. DOI: 10.48550/arXiv.2108.10349. [Online]. Available: https://arxiv.org/pdf/2108.10349.

[11] S. Chinthala, *Analyzing the effectiveness of siem tools in threat mitigation: A qualitative study in cybersecurity*, Accessed: 2026-05-06, Dec. 2024. [Online]. Available: https://www.researchgate.net/publication/387538937_Analyzing_the_Effectiveness_of_SIEM_Tools_in_Threat_Mitigation_A_Qualitative_Study_in_Cybersecurity.

[12] D. McCoy, *Human-machine interface (hmi) vulnerabilities affecting maintenance decisions*, Accessed: 2026-05-06, Dec. 2025. [Online]. Available: https://www.researchgate.net/publication/398401787_Human-Machine_Interface_HMI_Vulnerabilities_Affecting_Maintenance_Decisions.

[13] Y. A. Makeri, G. T. Cirella, F. J. Galas, and A. O. Adeniran, "Network performance through virtual local area network (vlan) implementation & enforcement on network security for enterprise," *International Journal of Advanced Networking and Applications*, vol. 12, no. 6, pp. 4750–4762, 2021, Accessed: 2026-05-06. [Online]. Available: https://www.researchgate.net/publication/352961286_Network_Performance_Through_Virtual_Local_Area_Network_VLAN_Implementation_Enforcement_On_Network_Security_For_Enterprise.

[14] K. A. Sattar, K. Salah, M. H. Sqalli, R. Rafiq, and M. Rizwan, "A countermeasure to mitigate discovery of network firewall default rules," Dec. 2018, Accessed: 2026-05-06. [Online]. Available: https://www.researchgate.net/publication/329810902_A_Countermeasure_to_Mitigate_Discovery_of_Network_Firewall_Default_Rules.

[15] National Institute of Standards and Technology (NIST), *Nist computer security resource center glossary*, 2026. [Online]. Available: https://csrc.nist.gov/glossary.

[16] A. Gheorghe and M. Pătrașcu, "Cyber security frameworks (csfs): An assessment between the nist csf v2.0 and eu standards," in *Proceedings of the ESA Security Workshop*, Accessed: 2026-05-06, 2024. [Online]. Available: https://indico.esa.int/event/528/attachments/5988/10190/Cyber_Security_Frameworks_CSFs_An_Assessment_Between_the_NIST_CSF_v2.0_and_EU_Standards.pdf.

[17] S. D. Quinn and B. Heiserman, "National checklist program for it products: Guidelines for checklist users and developers," National Institute of Standards and Technology (NIST), Tech. Rep. NIST SP 800-70r5 (Initial Public Draft), 2025. DOI: 10.6028/NIST.SP.800-70r5.ipd. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-70r5.ipd.

[18] Wikipedia contributors, *Failure mode and effects analysis*, Accessed: 2026-05-01, 2025. [Online]. Available: https://en.wikipedia.org/wiki/Failure_mode_and_effects_analysis.

[19] H. Elahi, G. Wang, Y. Xu, and A. Castiglione, "On the characterization and risk assessment of ai-powered mobile cloud applications," *Computer Standards & Interfaces*, vol. 78, p. 103 538, 2021, Accessed: 2026-05-06, ISSN: 0920-5489. DOI: 10.1016/j.csi.2021.103538. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0920548921000337.

[20] National Institute of Standards and Technology, "Nist risk management framework (rmf) small enterprise quick start guide: A comprehensive, flexible, risk-based approach to managing information security and privacy risk," National Institute of Standards and Technology (NIST), Tech. Rep. NIST Special Publication 1314, Jul. 2024, Accessed: 2026-05-06. DOI: 10.6028/NIST.SP.1314. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1314.pdf.

[21] National Institute of Standards and Technology, "Protecting controlled unclassified information in nonfederal systems and organizations," U.S. Department of Commerce, Gaithersburg, MD, Tech. Rep. NIST SP 800-171 Rev. 3, 2024. DOI: 10.6028/NIST.SP.800-171r3. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-171r3.

[22] P. Phiayura and S. Teerakanok, "A comprehensive framework for migrating to zero trust architecture," *IEEE Access*, vol. 11, pp. 19 487–19 511, 2023. DOI: 10.1109/ACCESS.2023.3248622. [Online]. Available: https://ieeexplore.ieee.org/document/10043261.

[23] S. Kapoor, S. Kumar, and H. Vardhan, *Cyber security of ot networks: A tutorial and overview*, 2025. DOI: 10.48550/ARXIV.2502.14017.

[24] R. Ross, V. Pillitteri, K. Dempsey, M. Riddle, and G. Guissanie, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, Tech. Rep. NIST Special Publication 800-171 Revision 2, 2020. DOI: 10.6028/NIST.SP.800-171r2. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final.

[25] National Institute of Standards and Technology (NIST), *Cybersecurity framework (csf) 2.0*, 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[26] National Institute of Standards and Technology (NIST), *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy*, 2018. DOI: 10.6028/NIST.SP.800-37r2. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/37/r2/final.

[27] National Institute of Standards and Technology (NIST), *Managing information security risk: Organization, mission, and information system view*, 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf.

[28] National Institute of Standards and Technology (NIST), *Security and privacy controls for information systems and organizations*, 2023. DOI: 10.6028/NIST.SP.800-53r5. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

[29] National Institute of Standards and Technology (NIST), *Digital identity guidelines: Authentication and authenticator management*, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/63/b/4/final.

[30] National Institute of Standards and Technology (NIST), *Security considerations in the system development life cycle*, 2008. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-64r2.pdf.

[31] National Institute of Standards and Technology (NIST), *Guidelines for media sanitization*, 2014. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/88/r1/final.

[32] National Institute of Standards and Technology (NIST), *Guide to protecting the confidentiality of personally identifiable information (pii)*, 2010. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/122/final.

[33] National Institute of Standards and Technology (NIST), *Engineering trustworthy secure systems*, 2018. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final.

[34] National Institute of Standards and Technology (NIST), *Cybersecurity supply chain risk management practices for systems and organizations*, 2022. DOI: 10.6028/NIST.SP.800-161r1. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/161/r1/final.

[35] European Parliament and Council of the European Union, *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148, Official Journal of the European Union, OJ L 194, 19 July 2016, pp. 1–30, 2016.

[36] Z. T. Almulla and H. Rahman, "The role of network segmentation and micro-segmentation in operational technology security," in *2025 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, Fukuoka, Japan: IEEE, Feb. 2025. DOI: 10.1109/ICAIIC64266.2025.10920695. [Online]. Available: https://ieeexplore.ieee.org/document/10920695.

[37] T. Tuliainen, "Cybersecurity in operational technology networks: Nis2 as a guideline," Accessed: 2026-04-26, Bachelor's thesis, Jamk University of Applied Sciences, 2025. [Online]. Available: https://www.theseus.fi/handle/10024/888790.

[38] M. Kallatsa, "Strategies for network segmentation: A systematic literature review," Accessed: 2026-04-26, Master's thesis, University of Jyväskylä, Faculty of Information Technology, 2024. [Online]. Available: https://jyx.jyu.fi/handle/123456789/92952.

[39] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A survey on zero trust architecture: Challenges and future trends," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, pp. 1–13, 2022. DOI: 10.1155/2022/6476274. [Online]. Available: https://www.researchgate.net/publication/361335518_A_Survey_on_Zero_Trust_Architecture_Challenges_and_Future_Trends.

[40] M. Tsai, S. Lee, and S. W. Shieh, "Strategy for implementing of zero trust architecture," *IEEE Transactions on Reliability*, vol. 73, no. 1, pp. 93–100, 2024. DOI: 10.1109/TR.2023.3345665. [Online]. Available: https://ieeexplore.ieee.org/document/10301677.

[41] International Organization for Standardization, "Iso/iec 27001: Information security management systems," 2022.

[42] Wikipedia contributors, *Security information and event management*, Accessed: 2026-05-04, 2026. [Online]. Available: https://en.wikipedia.org/wiki/Security_information_and_event_management.

[43] A. F. Mgbemele, "Advancing cyber threat detection through siem-based automation and mitre att&ck aligned analytics: A systematic review," *Asian Journal of Research in Computer Science*, vol. 19, no. 1, pp. 233–254, 2026, Accessed: 2026-05-06. DOI: 10.9734/ajrcos/2026/v19i1816. [Online]. Available: https://journalajrcos.com/index.php/AJRCOS/article/view/816.

[44] Wikipedia contributors, *Human–computer/machine interaction*, Accessed: 2026-05-06, 2026. [Online]. Available: https://en.wikipedia.org/wiki/Human%E2%80%93computer_interaction.

[45] Wikipedia contributors, *Vlan*, Accessed: 2026-05-06, 2026. [Online]. Available: https://en.wikipedia.org/wiki/VLAN.

[46] M. A. Hossain, A. Al-Masud, B. Saha, F. Rabbi, and M. Helal, "Securing a network by using vlan, port security and access control list," *SEU Journal of Electrical and Electronic Engineering (SEUJEEE)*, vol. 5, no. 1, pp. 10–18, Jan. 2025, Accessed: 2026-05-06. [Online]. Available: https://old.seu.edu.bd/seujeee/downloads/vol_05_issue_01_January_2025/SEUJEEE-v5i1s2.pdf.

[47] Wikipedia contributors, *Firewall (computing)*, Accessed: 2026-05-06, 2026. [Online]. Available: https://en.wikipedia.org/wiki/Firewall_(computing).

[48] R. Ș. Lungu, O. A. Frasin, and C. V. Marian, "Design and implementation of lightweight virtualized firewalls for industrial cybersecurity and medical services," in *2025 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, Accessed: 2026-05-06, IEEE, 2025, pp. 47–52. [Online]. Available: https://ieeexplore.ieee.org/document/11193920.

[49] R. L. Bull, J. N. Matthews, and K. A. Trumbull, "Vlan hopping, arp poisoning, and man-in-the-middle attacks in virtualized environments," in *DEF CON 24*, Accessed: 2026-05-06, Aug. 2016. [Online]. Available: https://people.clarkson.edu/~jmatthew/publications/DEFCON-24-Bull-Matthews-Trumbull-VLAN-Hopping-ARP-MITM-in-Virtualized-WP.pdf.

[50] P. R. Kothamali and S. Banik, "Limitations of signature-based threat detection," 2025, Accessed: 2026-05-06. [Online]. Available: https://www.researchgate.net/publication/388494583_Limitations_of_Signature-Based_Threat_Detection.

[51] H. Liu, L. Liu, and N. Liu, "Failure mode and effect analysis (fmea) implementation: A literature review," *International Journal of Advanced Manufacturing Technology*, vol. 103, no. 9–12, pp. 4489–4537, 2019, Accessed: 2026-05-06. DOI: 10.1007/s00170-019-03594-6. [Online]. Available: https:

//www.researchgate.net/publication/333209894_Failure_Mode_and_Effect_Analysis_FMEA_Implementation_A_Literature_Review.

[52] J. L. Hieb, "Security hardened remote terminal units for scada networks," Accessed: 2026-05-06, Ph.D. dissertation, University of Louisville, 2008. [Online]. Available: https://scispace.com/pdf/security-hardened-remote-terminal-units-for-scada-networks-45k4g2j6x3.pdf.

[53] A. Ghosh, D. Das, and S. Roy, "Scada systems: Security concerns and countermeasures," *International Journal of Advanced Research in Computer Science*, vol. 14, no. 1, pp. 1–8, 2023, Accessed: 2026-05-06. [Online]. Available: https://www.researchgate.net/publication/368612018_SCADA_Systems_Security_Concerns_and_Countermeasures.

[54] G. B. Arote, V. S. Pratham Bhosale, and R. Khatri, "Ai-driven firewall: Dynamic threat detection research paper," Apr. 2026, Accessed: 2026-05-06. DOI: 10.13140/RG.2.2.34115.77602. [Online]. Available: https://www.researchgate.net/publication/404162392_AI-Driven_Firewall-Dynamic_Threat_Detection_Research_Paper.

[55] S. Kumar, H. Shanvi, R. Kumar, S. Kumar, D. Kumar, and B. Bhushan, "Ai-driven next-generation firewall for dynamic threat detection and zero trust implementation," *International Journal of Research and Innovation in Applied Science (IJRIAS)*, vol. 10, no. 12, pp. 672–682, Dec. 2025, Accessed: 2026-05-06. DOI: 10.51584/IJRIAS.2025.10120052. [Online]. Available: https://rsisinternational.org/journals/ijrias/view/ai-driven-next-generation-firewall-for-dynamic-threat-detection-and-zero-trust-implementation.

[56] S. Jangampeta, "Ai and machine learning in siem: Enhancing threat detection and response with predictive analytics," *International Journal of Artificial Intelligence & Machine Learning (IJAIML)*, vol. 1, no. 1, pp. 10–14, 2022.

[57] H. Elahi, N. Liu, J. Chen, and F. Zhang, "Toward a secure framework for regulating artificial intelligence systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 23, no. 1, pp. 1373–1389, Jan. 2026, ISSN: 2160-9209. DOI: 10.1109/tdsc.2025.3616288.

[58] C. Zanasi, F. Magnanini, S. Russo, and M. Colajanni, "A zero trust approach for the cybersecurity of industrial control systems," in *2022 IEEE 21st International Symposium on Network Computing and Applications (NCA)*, IEEE, Dec. 2022, pp. 1–7. DOI: 10.1109/nca57778.2022.10013559.

[59] S. Kaelble, *Zero Trust Segmentation For Dummies, Illumio Special Edition*. John Wiley & Sons, Inc., 2023, pp. 1–53, ISBN: 978-1-394-18168-1. [Online]. Available: https://www.illumio.com/resource-center/zero-trust-segmentation-dummies.

[60] Department of Defense, "Zero trust operational technology activities and outcomes," U.S. Department of Defense, Tech. Rep., 2025, pp. 1–28. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/ZT-OperationalTechnologyActivitiesOutcomes.pdf.

[61] J. L. Salas-Riega, Y. Riega-Virú, M. Ninaquispe-Soto, and J. M. Salas-Riega, "Cybersecurity and the nist framework: A systematic review of its implementation and effectiveness against cyber threats," *International Journal of Advanced*

Computer Science and Applications, vol. 16, no. 6, pp. 723–735, 2025, Accessed: 2026-05-06. DOI: 10.14569/IJACSA.2025.0160672. [Online]. Available: https://www.researchgate.net/publication/393423098_Cybersecurity_and_the_NIST_Framework_A_Systematic_Review_of_its_Implementation_and_Effectiveness_Against_Cyber_Threats.

A

Appendix 1

A.1 NIST Standards Mapping to NIS2 Articles

Table A.1: Mapping of NIST Standards to NIS2 Directive Articles

S. No.	NIST Standard & Version	Family	NIST Family Summary	NIS2 Article No.	NIS2 Article Summary
1.1	NIST SP 800-37 Rev. 2	Prepare	Prepare the organization to effectively manage cybersecurity risk	Article 20	Top management is responsible for approving and overseeing cybersecurity practices.
1.2	NIST SP 800-37 Rev. 2	Categorize	Determine system criticality based on confidentiality, integrity, and availability impacts	Article 21(2)(a)	Organizations must implement risk analysis and information system security policies.
1.3	NIST SP 800-37 Rev. 2	Select	Identify and tailor appropriate security controls based on system risk and operational requirements.	Article 21(2)(i),(h),(d)	(i) Entities use multi-factor authentication or continuous authentication and secure communications where appropriate; (h) entities implement policies and procedures for cryptography and encryption; (d) supply chain and third-party risks must be managed, including monitoring external service providers.
1.4	NIST SP 800-37 Rev. 2	Implement	Install and configure the chosen security controls so they work properly in the system.	Article 21(2)(i),(j)	(i) Strong authentication and secure communication practices must be used, including MFA where appropriate; (j) secure access control and personnel security measures must be enforced to ensure only authorized individuals access systems and data.
1.5	NIST SP 800-37 Rev. 2	Assess	Evaluate the effectiveness of implemented controls through testing, audits, and security assessments.	Article 21(2)(f)	Organizations must monitor networks and systems to detect suspicious activities, investigate security events, and respond to cybersecurity incidents.

S. No.	NIST Standard & Version	Family	NIST Family Summary	NIS2 Article number	NIS2 Article Summary
1.6	NIST SP 800-37 Rev. 2	Authorize	Senior management reviews risk and formally approves system operation based on acceptable risk levels.	Article 20	Top management is responsible for approving, overseeing, and being accountable for cybersecurity practices and preparedness.
1.7	NIST SP 800-37 Rev. 2	Monitor	Continuously observe system security, detect incidents, and update controls to address evolving threats.	Article 23, Article 21(2)(f)	(23) Entities must promptly report significant cybersecurity incidents to authorities; (f) organizations must monitor systems, detect suspicious activity, and respond to incidents.
2.1	NIST SP 800-39	Frame Risk	Set up how the organization will manage risk, including policies and overall approach.	Article 20	Top management is responsible for approving, overseeing, and being accountable for cybersecurity practices and preparedness.
2.2	NIST SP 800-39	Assessing Risk	Identify and understand risks by analyzing threats, vulnerabilities, and impacts.	Article 21(2)(a)	Organizations must implement policies on risk analysis and information system security to manage cybersecurity risks effectively.
2.3	NIST SP 800-39	Responding Risk	Take actions to reduce or manage risks using appropriate security measures.	Article 21(2)(e),(h),(i)	(e) Entities ensure security across system acquisition, development, and maintenance, including vulnerability handling and disclosure; (h) entities implement policies and procedures for cryptography and encryption; (i) entities apply cryptography and encryption where appropriate to protect sensitive information.
2.4	NIST SP 800-39	Monitoring Risk	Continuously check for risks and ensure security measures are working properly.	Article 21(2)(f)	Organizations must monitor networks and systems to detect suspicious activities, investigate security events, and respond to cybersecurity incidents.
2.5	NIST SP 800-39	Organization Level	Sets the overall security strategy, policies, and risk level decided by management for the whole organization.	Article 20	Top management is responsible for approving, overseeing, and being accountable for cybersecurity practices and preparedness.
2.6	NIST SP 800-39	Business Process Level	Applies security and risk management in daily business activities and processes to support safe operations.	Article 21(2)(a),(g)	(a) Organizations must implement policies on risk analysis and information system security; (g) entities implement cyber hygiene practices and training to reduce risks and improve awareness.
2.7	NIST SP 800-39	System Level	Implements and manages security controls in systems to protect data, networks, and operations.	Article 23, Article 21(2)(f)	(23) Entities must report significant cybersecurity incidents; (f) organizations must monitor systems, detect suspicious activity, and respond to incidents.

S. No.	NIST Standard & Version	Family	NIST Family Summary	NIS2 Article number	NIS2 Article Summary
3.1	NIST SP 800-53 Rev. 5	Access Control	Controls who can access systems and data. Ensures only authorized users are allowed.	Article 21(2)(i)	Entities use multi-factor authentication or continuous authentication and secure communications where appropriate.
3.2	NIST SP 800-53 Rev. 5	Awareness Training	Train employees on cybersecurity practices	Article 21(2)(g)	Basic cyber hygiene practices and cybersecurity training must be applied; these reduce human-related risks and improve awareness.
3.3	NIST SP 800-53 Rev. 5	Audit & Accountability	Records system and user activities to track actions and detect issues	Article 21(2)(f)	Organizations must monitor networks and systems to detect suspicious activities, investigate security events, and respond to cybersecurity incidents.
3.4	NIST SP 800-53 Rev. 5	Assessment, Authorization & Monitoring	Checks if security controls are working properly and continuously monitors system security	Article 21(2)(f)	Organizations must monitor networks and systems to detect suspicious activities, investigate security events, and respond to cybersecurity incidents.
3.5	NIST SP 800-53 Rev. 5	Configuration Management	Manages system settings securely and prevents unauthorized changes	Article 21(2)(e)	Security must be ensured across the lifecycle of systems, including acquisition, development, maintenance, and vulnerability handling.
3.6	NIST SP 800-53 Rev. 5	Contingency Planning	Prepares for system failures or attacks and ensures recovery	Article 21(2)(c)	Business continuity measures, including backups and disaster recovery, are required to ensure operations can resume quickly.
3.7	NIST SP 800-53 Rev. 5	Identification & Authentication	Verifies identity of users and systems before granting access	Article 21(2)(i)	Strong authentication and secure communication practices must be used, including multi-factor authentication where appropriate.
3.8	NIST SP 800-53 Rev. 5	Incident Response	Detects and responds to security incidents to reduce damage	Article 21(2)(b), Article 23	Processes must detect, manage, and respond to incidents; entities must also report significant cybersecurity incidents within defined timelines.
3.9	NIST SP 800-53 Rev. 5	Maintenance	Ensures systems are maintained securely during updates and repairs	Article 21(2)(e)	Security must be ensured across system lifecycle, including maintenance and vulnerability management.
3.10	NIST SP 800-53 Rev. 5	Media Protection	Safeguards digital and physical media to prevent unauthorized access or disclosure	Article 21(2)(e)	Security must be ensured across system lifecycle including secure handling of media and data.
3.11	NIST SP 800-53 Rev. 5	Physical & Environmental Protection	Protects physical locations and equipment from unauthorized access or damage	Article 21(2)(e),(j)	Systems must be physically protected and access restricted to authorized personnel.
3.12	NIST SP 800-53 Rev. 5	Planning	Defines security planning and policies for secure system management	Article 21(2)(a)	Organizations must implement policies on risk analysis and system security.

S. No.	NIST Standard & Version	Family	NIST Family Summary	NIS2 Article number	NIS2 Article Summary
3.13	NIST SP 800-53 Rev. 5	Program Management	Manages organization-wide security governance and strategy	Article 20	Top management is responsible for cybersecurity governance and accountability.
3.14	NIST SP 800-53 Rev. 5	Personnel Security	Ensures employees follow security policies and reduces insider threats	Article 21(2)(g)	Cybersecurity awareness and training must be implemented to reduce human-related risks.
3.15	NIST SP 800-53 Rev. 5	PII Processing & Transparency	Ensures proper handling and protection of personal data	Article 21(2)(e)	Security must be ensured across system lifecycle including protection of sensitive data.
3.16	NIST SP 800-53 Rev. 5	Risk Assessment	Identifies and evaluates risks to systems and data	Article 21(2)(a)	Organizations must implement risk analysis and security policies.
3.17	NIST SP 800-53 Rev. 5	System & Services Acquisition	Ensures security in system acquisition and development	Article 21(2)(e),(d)	Security must be ensured across lifecycle and supply chain risks must be managed.
3.18	NIST SP 800-53 Rev. 5	System & Communications Protection	Protects data during transmission and secures communications	Article 21(2)(h)	Policies and procedures for cryptography and encryption must be implemented.
3.19	NIST SP 800-53 Rev. 5	System & Information Integrity	Detects and corrects system errors and vulnerabilities	Article 21(2)(f)	Organizations must monitor systems to detect threats and respond to incidents.
3.20	NIST SP 800-53 Rev. 5	Supply Chain Risk Management	Manages risks from suppliers and third parties	Article 21(2)(d)	Supply chain risks must be assessed and monitored for security.
4.1	NIST SP 800-63B-4	Authenticator Types	Defines different ways users prove their identity, such as passwords, OTPs, biometrics, hardware tokens, and multi-factor authentication (MFA).	Article 21(2)(i),(j)	(i) Strong authentication and secure communication practices must be used, including MFA where appropriate; (j) secure access control and personnel security measures must be enforced to ensure only authorized individuals can access systems and data.
4.2	NIST SP 800-63B-4	Authenticator Assurance Levels (AAL)	Defines levels of authentication strength (AAL1, AAL2, AAL3) based on risk and required security.	Article 21(2)(i),(j)	(i) Strong authentication and secure communication practices must be used, including MFA where appropriate; (j) secure access control and personnel security measures must be enforced to ensure only authorized individuals can access systems and data.
4.3	NIST SP 800-63B-4	Authentication Lifecycle	Defines authentication processes across lifecycle stages based on required security levels.	Article 21(2)(i)	Strong authentication and secure communication practices must be used, including multi-factor authentication where appropriate.
5.1	NIST SP 800-64 Rev. 2	Initiation	Identify security requirements and risks at an early stage and plan system protection.	Article 21(2)(a)	Organizations must implement policies on risk analysis and information system security to manage cybersecurity risks effectively.

S. No.	NIST Standard & Version	Family	NIST Family Summary	NIS2 Article number	NIS2 Article Summary
5.2	NIST SP 800-64 Rev. 2	Development / Acquisition	Design or acquire systems with built-in security, including secure coding, configuration, and supplier evaluation.	Article 21(2)(e)	Security must be ensured across the lifecycle of systems, including acquisition, development, maintenance, and vulnerability handling.
5.3	NIST SP 800-64 Rev. 2	Implementation / Assessment	Deploy the system and test security controls to ensure they function correctly before use.	Article 21(2)(f)	Organizations must monitor systems to detect suspicious activities, investigate security events, and respond to cybersecurity incidents.
5.4	NIST SP 800-64 Rev. 2	Operations and Maintenance	Monitor and maintain system security during operation, including updates, patching, and incident handling.	Article 21(2)(b),(f)	(b) Processes must detect, manage, and respond to cybersecurity incidents to ensure recovery; (f) organizations must monitor systems, detect suspicious activity, and respond to incidents.
5.5	NIST SP 800-64 Rev. 2	Disposal	Safely remove systems and securely delete or transfer data to prevent unauthorized access or leakage.	Article 21(2)(e),(j)	(e) Security must be ensured across the system lifecycle, including secure disposal and vulnerability handling; (j) secure access control and personnel measures must ensure only authorized individuals access systems and data.
6.1	NIST 800-88r1	Media Sanitization	Establishes organizational duties for managing and handling media data throughout its lifecycle.	Article 20	Top management is responsible for approving, overseeing, and being accountable for cybersecurity practices and preparedness.
6.2	NIST 800-88r1	Media Sanitization	Outlines processes to render data on media inaccessible using Clear, Purge, or Destroy techniques based on data sensitivity before media leaves organizational control.	Article 21	Entities must implement cybersecurity risk-management measures to protect systems and reduce the impact of incidents.
7.1	NIST SP 800-122	Introduction to PII	Explains what PII is, how it is identified, and basic privacy concepts.	Article 21(2)(a),(j)	(a) Organizations must implement policies on risk analysis and information system security; (j) secure access control and personnel security measures must ensure only authorized individuals access systems and data.
7.2	NIST SP 800-122	PII Confidentiality Impact Levels	Defines sensitivity levels of PII and the impact of exposure, supporting risk assessment.	Article 21(2)(a)	Organizations must implement policies on risk analysis and information system security to manage cybersecurity risks effectively.

S. No.	NIST Standard & Version	Family	NIST Family Summary	NIS2 Article number	NIS2 Article Summary
7.3	NIST SP 800-122	PII Confidentiality Safeguards	Describes measures to protect PII, including policies, training, and security controls.	Article 21(2)(e),(h),(i)	(e) Security must be ensured across system lifecycle, including vulnerability handling; (h) entities implement policies and procedures for cryptography and encryption; (i) entities apply encryption to protect sensitive information.
7.4	NIST SP 800-122	Incident Response for PII Breaches	Explains how to detect, respond to, and recover from PII-related incidents.	Article 21(2)(b), Article 23	(b) Processes must detect, manage, and respond to cybersecurity incidents to ensure recovery; (23) entities must report significant incidents within defined timelines.
8.1	NIST SP 800-160 Vol. 1 Rev. 1	Security Requirements Definition	Defines security needs and requirements early in system design based on risks and threats.	Article 21(2)(a)	Organizations must implement policies on risk analysis and information system security to manage cybersecurity risks effectively.
8.2	NIST SP 800-160 Vol. 1 Rev. 1	Secure System Design	Integrates security into system architecture and design to prevent vulnerabilities.	Article 21(2)(e)	Security must be ensured across the lifecycle of systems, including acquisition, development, maintenance, and vulnerability handling.
8.3	NIST SP 800-160 Vol. 1 Rev. 1	Secure Implementation	Ensures systems are developed and implemented securely with proper controls.	Article 21(2)(e)	Security must be ensured across the lifecycle of systems, including acquisition, development, maintenance, and vulnerability handling.
8.4	NIST SP 800-160 Vol. 1 Rev. 1	Verification & Validation	Tests and evaluates whether security requirements are correctly implemented.	Article 21(2)(f)	Organizations must monitor systems to detect suspicious activities, investigate security events, and respond to cybersecurity incidents.
8.5	NIST SP 800-160 Vol. 1 Rev. 1	Secure Operation	Maintains system security during operation through monitoring and incident handling.	Article 21(2)(b),(f)	(b) Processes must detect, manage, and respond to cybersecurity incidents; (f) organizations must monitor systems and respond to threats.
8.6	NIST SP 800-160 Vol. 1 Rev. 1	System Resilience	Ensures systems can resist, recover, and continue functioning during attacks or failures.	Article 21(2)(c)	Business continuity measures, including backups and disaster recovery, are required to ensure operations can resume quickly.
9.1	NIST SP 800-161 Rev. 1	Supply Chain Risk Identification	Identifies risks from suppliers, vendors, and external service providers.	Article 21(2)(d)	Supply chain and third-party risks must be managed, including monitoring external service providers.
9.2	NIST SP 800-161 Rev. 1	Supply Chain Risk Assessment	Evaluates the likelihood and impact of risks introduced by third parties.	Article 21(2)(a),(d)	(a) Organizations must implement risk analysis policies; (d) supply chain risks must be assessed and monitored.

S. No.	NIST Standard & Version	Family	NIST Family Summary	NIS2 Article number	NIS2 Article Summary
9.3	NIST SP 800-161 Rev. 1	Supplier Security Requirements	Defines security requirements for vendors and includes them in contracts and agreements.	Article 21(2)(d),(e)	(d) Supply chain risks must be managed; (e) security must be ensured across system lifecycle including acquisition and development.
9.4	NIST SP 800-161 Rev. 1	Supply Chain Monitoring	Continuously monitors suppliers and third-party services for security risks.	Article 21(2)(f),(d)	(f) Organizations must monitor systems for suspicious activity; (d) supply chain risks must be continuously assessed.
9.5	NIST SP 800-161 Rev. 1	Supply Chain Incident Response	Handles incidents related to suppliers and coordinates response with external parties.	Article 21(2)(b), Article 23	(b) Incident response processes must be implemented; (23) significant incidents must be reported within defined timelines.
9.6	NIST SP 800-161 Rev. 1	Supply Chain Governance	Establishes policies and management oversight for supply chain security.	Article 20, Article 21(2)(d)	Article 20 requires management accountability; Article 21(2)(d) requires supply chain risk management and monitoring.
10.1	NIST SP 800-171 Rev. 2	Access Control (3.1.1)	Limit system access to authorized users, processes, and devices.	Article 21(2)(i)	Requires access control policies, human resources security, and asset management.
10.2	NIST SP 800-171 Rev. 2	Access Control (3.1.2)	Limit system access to permitted transactions and functions.	Article 21(2)(i)	Requires access control policies to manage risks to network and information systems.
10.3	NIST SP 800-171 Rev. 2	Access Control (3.1.3)	Control the flow of CUI in accordance with approved authorizations.	Article 21(2)(i)	Requires access control policies to prevent or minimize cybersecurity incidents.
10.4	NIST SP 800-171 Rev. 2	Access Control (3.1.4)	Separate duties of individuals to reduce risk without collusion.	Article 21(2)(i)	Requires human resources security and access control policies.
10.5	NIST SP 800-171 Rev. 2	Access Control (3.1.5)	Employ the principle of least privilege.	Article 21(2)(i)	Requires access control policies and human resources security.
10.6	NIST SP 800-171 Rev. 2	Access Control (3.1.6)	Use non-privileged accounts when accessing non-security functions.	Article 21(2)(i)	Requires access control policies as part of cybersecurity risk management.
10.7	NIST SP 800-171 Rev. 2	Access Control (3.1.7)	Prevent non-privileged users from executing privileged functions.	Article 21(2)(i)	Requires implementation of access control policies.
10.8	NIST SP 800-171 Rev. 2	Access Control (3.1.8)	Limit unsuccessful logon attempts.	Article 21(2)(i)	Requires implementation of access control policies.
10.9	NIST SP 800-171 Rev. 2	Access Control (3.1.9)	Provide privacy and security notices consistent with CUI rules.	Article 21(2)(i)	Requires implementation of access control policies.
10.10	NIST SP 800-171 Rev. 2	Access Control (3.1.10)	Use session lock with pattern-hiding displays.	Article 21(2)(i)	Requires implementation of access control policies.
10.11	NIST SP 800-171 Rev. 2	Access Control (3.1.11)	Automatically terminate user sessions after defined conditions.	Article 21(2)(i)	Requires implementation of access control policies.
10.12	NIST SP 800-171 Rev. 2	Access Control (3.1.12)	Monitor and control remote access sessions.	Article 21(2)(i)	Requires access control policies for remote access management.
10.13	NIST SP 800-171 Rev. 2	Access Control (3.1.13)	Use cryptographic mechanisms to protect remote access sessions.	Article 21(2)(h)	Requires policies and procedures for cryptography and encryption.

S. No.	NIST Standard & Version	Family	NIST Family Summary	NIS2 Article number	NIS2 Article Summary
10.14	NIST SP 800-171 Rev. 2	Access Control (3.1.14)	Route remote access through managed access control points.	Article 21(2)(i)	Requires strict access control policies to manage network security risks.
10.15	NIST SP 800-171 Rev. 2	Access Control (3.1.15)	Authorize remote execution of privileged commands and access.	Article 21(2)(i)	Requires access control policies to reduce cybersecurity risks.
10.16	NIST SP 800-171 Rev. 2	Access Control (3.1.16)	Authorize wireless access before allowing connections.	Article 21(2)(i)	Requires access control policies, human resources security, and asset management.
10.17	NIST SP 800-171 Rev. 2	Access Control (3.1.17)	Protect wireless access using authentication and encryption.	Article 21(2)(h),(i)	Requires encryption policies and access control policies.
10.18	NIST SP 800-171 Rev. 2	Access Control (3.1.18)	Control connection of mobile devices.	Article 21(2)(i)	Requires access control policies and asset management.
10.19	NIST SP 800-171 Rev. 2	Access Control (3.1.19)	Encrypt CUI on mobile devices and mobile computing platforms.	Article 21(2)(h)	Requires cryptography and encryption to protect network and information systems.
10.20	NIST SP 800-171 Rev. 2	Access Control (3.1.20)	Verify, control, and limit connections to external systems.	Article 21(2)(i)	Requires access control policies and asset management.
10.21	NIST SP 800-171 Rev. 2	Access Control (3.1.21)	Limit use of portable storage devices on external systems.	Article 21(2)(i)	Requires access control policies and asset management.
10.22	NIST SP 800-171 Rev. 2	Access Control (3.1.22)	Control CUI posted or processed on publicly accessible systems.	Article 21(2)(i)	Requires access control policies to manage security risks.
10.23	NIST SP 800-171 Rev. 2	Awareness and Training (3.2.1)	Ensure managers, administrators, and users are aware of security risks.	Article 21(2)(g)	Requires cybersecurity awareness and training.
10.24	NIST SP 800-171 Rev. 2	Awareness and Training (3.2.2)	Ensure personnel are trained to carry out security duties.	Article 21(2)(g)	Requires cybersecurity awareness and training.
10.25	NIST SP 800-171 Rev. 2	Awareness and Training (3.2.3)	Provide security awareness training on insider threats.	Article 21(2)(g)	Requires cybersecurity awareness and training.
10.26	NIST SP 800-171 Rev. 2	Audit and Accountability (3.3.1)	Create and retain system audit logs and records.	Article 21(2)(f)	Requires monitoring and evaluation of cybersecurity controls.
10.27	NIST SP 800-171 Rev. 2	Audit and Accountability (3.3.2)	Ensure actions of individual users can be uniquely traced.	Article 21(2)(f),(b)	Audit logs support incident investigation and accountability.
10.28	NIST SP 800-171 Rev. 2	Audit and Accountability (3.3.3)	Review and update logged events.	Article 21(2)(f)	Requires monitoring systems and responding to cybersecurity incidents.
10.29	NIST SP 800-171 Rev. 2	Audit and Accountability (3.3.4)	Alert when audit logging fails.	Article 21(2)(f),(i)	Audit records support accountability and monitoring of access to systems.
10.30	NIST SP 800-171 Rev. 2	Audit and Accountability (3.3.5)	Correlate audit records for suspicious activity investigations.	Article 21(2)(f),(a)	Audit mechanisms support risk assessment and security monitoring.
10.31	NIST SP 800-171 Rev. 2	Audit and Accountability (3.3.6)	Provide audit record reduction and report generation.	Article 21(2)(f),(c)	Monitoring logs supports incident detection and operational continuity.
10.32	NIST SP 800-171 Rev. 2	Audit and Accountability (3.3.7)	Synchronize internal system clocks with an authoritative source.	Article 21(2)(f),(h)	Protected audit logs support monitoring and integrity.
10.33	NIST SP 800-171 Rev. 2	Audit and Accountability (3.3.8)	Protect audit information and logging tools from unauthorized access.	Article 21(2)(f)	Audit logs must be available for authorized analysis and monitoring.
10.34	NIST SP 800-171 Rev. 2	Audit and Accountability (3.3.9)	Limit management of audit logging to privileged users.	Article 21(2)(f)	Audit processes support accountability and compliance investigations.

S. No.	NIST Standard & Version	Family	NIST Family Summary	NIS2 Article number	NIS2 Article Summary
10.35	NIST SP 800-171 Rev. 2	Configuration Management (3.4.1)	Establish and maintain baseline configurations and inventories.	Article 21(2)(a),(e),(i)	Baseline configurations support secure system settings and change management.
10.36	NIST SP 800-171 Rev. 2	Configuration Management (3.4.2)	Establish and enforce secure configuration settings.	Article 21(2)(i)	Only authorized users should modify system configurations.
10.37	NIST SP 800-171 Rev. 2	Configuration Management (3.4.3)	Track, review, approve, and log system changes.	Article 21(2)(e)	Configuration changes must be controlled and documented.
10.38	NIST SP 800-171 Rev. 2	Configuration Management (3.4.4)	Analyze security impact of changes before implementation.	Article 21(2)(e)	Configuration monitoring helps detect unauthorized or unexpected changes.
10.39	NIST SP 800-171 Rev. 2	Configuration Management (3.4.5)	Define and enforce physical and logical access restrictions for changes.	Article 21(2)(i)	Only approved applications and authorized changes should be allowed.
10.40	NIST SP 800-171 Rev. 2	Configuration Management (3.4.6)	Employ the principle of least functionality.	Article 21(2)(e)	Systems must be securely maintained through controlled updates and patches.
10.41	NIST SP 800-171 Rev. 2	Configuration Management (3.4.7)	Disable or prevent nonessential programs, functions, ports, and services.	Article 21(2)(e)	Least functionality reduces system attack surfaces.
10.42	NIST SP 800-171 Rev. 2	Configuration Management (3.4.8)	Apply deny-by-exception or permit-by-exception controls.	Article 21(2)(i)	Application control restricts software execution to authorized programs.
10.43	NIST SP 800-171 Rev. 2	Configuration Management (3.4.9)	Control and monitor user-installed software.	Article 21(2)(i)	Authorized asset use and inventory management support secure operations.
10.44	NIST SP 800-171 Rev. 2	Identification and Authentication (3.5.1)	Identify system users, processes, and devices.	Article 21(2)(i)	Requires identity management, access control, and asset management.
10.45	NIST SP 800-171 Rev. 2	Identification and Authentication (3.5.2)	Authenticate users, processes, or devices before access.	Article 21(2)(i)	Requires access control policies to manage system security risks.
10.46	NIST SP 800-171 Rev. 2	Identification and Authentication (3.5.3)	Use multifactor authentication for local and network access.	Article 21(2)(j)	Requires multi-factor or continuous authentication where appropriate.
10.47	NIST SP 800-171 Rev. 2	Identification and Authentication (3.5.4)	Use replay-resistant authentication mechanisms.	Article 21(2)(j),(i)	Requires MFA and access control policies.
10.48	NIST SP 800-171 Rev. 2	Identification and Authentication (3.5.5)	Prevent reuse of identifiers for a defined period.	Article 21(2)(i)	Requires access control policies and human resources security.
10.49	NIST SP 800-171 Rev. 2	Identification and Authentication (3.5.6)	Disable identifiers after a defined period of inactivity.	Article 21(2)(i)	Requires access control policies for system risk management.
10.50	NIST SP 800-171 Rev. 2	Identification and Authentication (3.5.7)	Enforce minimum password complexity and character changes.	Article 21(2)(i)	Requires access control policies.
10.51	NIST SP 800-171 Rev. 2	Identification and Authentication (3.5.8)	Prohibit password reuse for a specified number of generations.	Article 21(2)(i)	Requires access control policies.
10.52	NIST SP 800-171 Rev. 2	Identification and Authentication (3.5.9)	Allow temporary password use with immediate permanent change.	Article 21(2)(i)	Requires access control policies.
10.53	NIST SP 800-171 Rev. 2	Identification and Authentication (3.5.10)	Store and transmit only cryptographically protected passwords.	Article 21(2)(h)	Requires cryptography and encryption policies.
10.54	NIST SP 800-171 Rev. 2	Identification and Authentication (3.5.11)	Obscure feedback of authentication information.	Article 21(2)(i)	Requires access control policies.

S. No.	NIST Standard & Version	Family	NIST Family Summary	NIS2 Article number	NIS2 Article Summary
10.55	NIST SP 800-171 Rev. 2	Incident Response (3.6.1)	Establish an operational incident-handling capability.	Article 21(2)(b)	Requires incident handling to minimize incident impact.
10.56	NIST SP 800-171 Rev. 2	Incident Response (3.6.2)	Track, document, and report incidents to designated authorities.	Article 23	Requires phased reporting of significant incidents.
10.57	NIST SP 800-171 Rev. 2	Incident Response (3.6.3)	Test the organizational incident response capability.	Article 21(2)(b),(f)	Requires incident handling and assessment of cybersecurity risk-management measures.
10.58	NIST SP 800-171 Rev. 2	Maintenance (3.7.1)	Perform maintenance on organizational systems.	Article 21(2)(e)	Requires security in system acquisition, development, and maintenance.
10.59	NIST SP 800-171 Rev. 2	Maintenance (3.7.2)	Control tools, techniques, and personnel used for maintenance.	Article 21(2)(e)	Requires secure technical and organizational maintenance measures.
10.60	NIST SP 800-171 Rev. 2	Maintenance (3.7.3)	Sanitize equipment removed for off-site maintenance.	Article 21(2)(e)	Requires managing maintenance risks to protect data confidentiality, integrity, and availability.
10.61	NIST SP 800-171 Rev. 2	Maintenance (3.7.4)	Check diagnostic and test media for malicious code before use.	Article 21(2)(e)	Requires secure maintenance and vulnerability handling.
10.62	NIST SP 800-171 Rev. 2	Maintenance (3.7.5)	Require MFA and terminate sessions for nonlocal maintenance.	Article 21(2)(e),(j)	Requires secure maintenance and MFA or continuous authentication where appropriate.
10.63	NIST SP 800-171 Rev. 2	Maintenance (3.7.6)	Supervise maintenance activities by unauthorized personnel.	Article 21(2)(e)	Requires secure maintenance practices and organizational controls.
10.64	NIST SP 800-171 Rev. 2	Media Protection (3.8.1)	Physically control system media containing CUI.	Article 21(2)(i)	Requires limiting media access to authorized personnel.
10.65	NIST SP 800-171 Rev. 2	Media Protection (3.8.2)	Limit access to CUI on system media to authorized users.	Article 21(2)(i)	Requires secure storage and controlled access to sensitive data.
10.66	NIST SP 800-171 Rev. 2	Media Protection (3.8.3)	Sanitize or destroy system media before reuse.	Article 21(2)(i)	Requires restricted and authorized handling of media.
10.67	NIST SP 800-171 Rev. 2	Media Protection (3.8.4)	Mark media with necessary CUI markings.	Article 21(2)(h)	Encryption may protect data stored on physical or removable media.
10.68	NIST SP 800-171 Rev. 2	Media Protection (3.8.5)	Control access to media during transport.	Article 21(2)(i)	Requires protected media transport to prevent unauthorized access or loss.
10.69	NIST SP 800-171 Rev. 2	Media Protection (3.8.6)	Use cryptography for digital media during transport.	Article 21(2)(h)	Requires encryption to protect digital media in transit.
10.70	NIST SP 800-171 Rev. 2	Media Protection (3.8.7)	Control use of removable media on system components.	Article 21(2)(i)	Requires protection of physical media from unauthorized access or copying.
10.71	NIST SP 800-171 Rev. 2	Media Protection (3.8.8)	Prohibit portable storage devices without identifiable owners.	Article 21(2)(h)	Encryption may protect data on removable or portable media.
10.72	NIST SP 800-171 Rev. 2	Media Protection (3.8.9)	Protect backup CUI at storage locations.	Article 21(2)(i)	Requires media asset management and accountability.
10.73	NIST SP 800-171 Rev. 2	Personnel Security (3.9.1)	Screen individuals before authorizing access to systems with CUI.	Article 21(2)(j)	Requires personnel security and access control measures.

S. No.	NIST Standard & Version	Family	NIST Family Summary	NIS2 Article number	NIS2 Article Summary
10.74	NIST SP 800-171 Rev. 2	Personnel Security (3.9.2)	Protect systems during and after personnel actions.	Article 21(2)(j)	Requires personnel security and access control measures.
10.75	NIST SP 800-171 Rev. 2	Physical Protection (3.10.1)	Limit physical access to systems, equipment, and environments.	Article 21(2)(i)	Requires physical access control for authorized personnel.
10.76	NIST SP 800-171 Rev. 2	Physical Protection (3.10.2)	Protect and monitor physical facilities and infrastructure.	Article 21(2)(i)	Requires monitoring and protection of physical access points.
10.77	NIST SP 800-171 Rev. 2	Physical Protection (3.10.3)	Escort visitors and monitor visitor activity.	Article 21(2)(i)	Requires monitoring of visitors in controlled areas.
10.78	NIST SP 800-171 Rev. 2	Physical Protection (3.10.4)	Maintain audit logs of physical access.	Article 21(2)(i)	Requires logs of physical access to secure facilities.
10.79	NIST SP 800-171 Rev. 2	Physical Protection (3.10.5)	Control and manage physical access devices.	Article 21(2)(i)	Requires management of keys, badges, and physical access devices.
10.80	NIST SP 800-171 Rev. 2	Physical Protection (3.10.6)	Safeguard CUI at alternate work sites.	Article 21(2)(i)	Requires security protections for systems used at alternate locations.
10.81	NIST SP 800-171 Rev. 2	Risk Assessment (3.11.1)	Periodically assess risk to operations, assets, and individuals.	Article 21(2)(a)	Requires risk analysis and security policies.
10.82	NIST SP 800-171 Rev. 2	Risk Assessment (3.11.2)	Scan for vulnerabilities periodically and when new vulnerabilities are identified.	Article 21(2)(a)	Requires risk analysis and security policies.
10.83	NIST SP 800-171 Rev. 2	Risk Assessment (3.11.3)	Remediate vulnerabilities according to risk assessments.	Article 21(2)(a)	Requires risk-based remediation of cybersecurity weaknesses.
10.84	NIST SP 800-171 Rev. 2	Security Assessment (3.12.1)	Periodically assess security controls for effectiveness.	Article 21(2)(f)	Requires assessment of cybersecurity risk-management measures.
10.85	NIST SP 800-171 Rev. 2	Security Assessment (3.12.2)	Develop and implement plans of action to correct deficiencies.	Article 21(2)(a)	Requires actions to address identified cybersecurity risks.
10.86	NIST SP 800-171 Rev. 2	Security Assessment (3.12.3)	Monitor security controls on an ongoing basis.	Article 21(2)(f),(a),(b)	Continuous monitoring supports risk management, incident detection, and control effectiveness.
10.87	NIST SP 800-171 Rev. 2	Security Assessment (3.12.4)	Develop and update system security plans.	Article 21(2)(a)	Requires documentation and policies to manage cybersecurity risks.
10.88	NIST SP 800-171 Rev. 2	System and Communications Protection (3.13.1)	Monitor and protect communications at system boundaries.	Article 21(2)(f)	Requires monitoring of systems and network communications.
10.89	NIST SP 800-171 Rev. 2	System and Communications Protection (3.13.2)	Separate system components into security domains.	Article 21(2)(e)	Supports secure architecture and system lifecycle protection.
10.90	NIST SP 800-171 Rev. 2	System and Communications Protection (3.13.3)	Separate user functionality from system management functionality.	Article 21(2)(e)	Supports secure system architecture and internal separation.
10.91	NIST SP 800-171 Rev. 2	System and Communications Protection (3.13.4)	Prevent unauthorized information transfer through shared resources.	Article 21(2)(b)	Monitoring network activity supports incident detection.
10.92	NIST SP 800-171 Rev. 2	System and Communications Protection (3.13.5)	Use separated subnetworks for publicly accessible components.	Article 21(2)(e)	Requires secure network architecture and segmentation.

S. No.	NIST Standard & Version	Family	NIST Family Summary	NIS2 Article number	NIS2 Article Summary
10.93	NIST SP 800-171 Rev. 2	System and Communications Protection (3.13.6)	Deny network traffic by default and allow by exception.	Article 21(2)(e)	Requires control and restriction of unauthorized communications.
10.94	NIST SP 800-171 Rev. 2	System and Communications Protection (3.13.7)	Prevent remote devices from simultaneous external and non-remote connections.	Article 21(2)(e)	Boundary protection helps prevent unauthorized network access.
10.95	NIST SP 800-171 Rev. 2	System and Communications Protection (3.13.8)	Use cryptography to protect CUI during transmission.	Article 21(2)(h)	Requires encryption to protect sensitive transmitted information.
10.96	NIST SP 800-171 Rev. 2	System and Communications Protection (3.13.9)	Terminate network connections after sessions or inactivity.	Article 21(2)(i)	Requires access control and secure session management.
10.97	NIST SP 800-171 Rev. 2	System and Communications Protection (3.13.10)	Establish and manage cryptographic keys.	Article 21(2)(h)	Requires cryptographic protections for transmitted data.
10.98	NIST SP 800-171 Rev. 2	System and Communications Protection (3.13.11)	Use validated cryptography to protect CUI confidentiality.	Article 21(2)(h)	Requires cryptography and encryption to protect sensitive information.
10.99	NIST SP 800-171 Rev. 2	System and Communications Protection (3.13.12)	Prohibit remote activation of collaborative devices and indicate use.	Article 21(2)(e)	Requires secure communication protocols and system protections.
10.100	NIST SP 800-171 Rev. 2	System and Communications Protection (3.13.13)	Control and monitor the use of mobile code.	Article 21(2)(f)	Requires monitoring to detect suspicious activity and cybersecurity risks.
10.101	NIST SP 800-171 Rev. 2	System and Communications Protection (3.13.14)	Control and monitor VoIP technologies.	Article 21(2)(e)	Requires secure communications and network protection.
10.102	NIST SP 800-171 Rev. 2	System and Communications Protection (3.13.15)	Protect authenticity of communications sessions.	Article 21(2)(h)	Requires cryptographic protections for secure communications.
10.103	NIST SP 800-171 Rev. 2	System and Communications Protection (3.13.16)	Protect confidentiality of CUI at rest.	Article 21(2)(h)	Requires encryption to protect sensitive information at rest.
10.104	NIST SP 800-171 Rev. 2	System and Information Integrity (3.14.1)	Identify, report, and correct system flaws in a timely manner.	Article 21(2)(e)	Requires vulnerability handling and secure system maintenance.
10.105	NIST SP 800-171 Rev. 2	System and Information Integrity (3.14.2)	Deploy and update mechanisms to detect and protect against malware.	Article 21(2)(b)	Malware protection supports incident prevention and response.
10.106	NIST SP 800-171 Rev. 2	System and Information Integrity (3.14.3)	Monitor security alerts and advisories and take action.	Article 21(2)(f)	Requires monitoring and response to security threats.
10.107	NIST SP 800-171 Rev. 2	System and Information Integrity (3.14.4)	Update malicious code protection mechanisms.	Article 21(2)(e)	Requires secure maintenance and updates of protection mechanisms.
10.108	NIST SP 800-171 Rev. 2	System and Information Integrity (3.14.5)	Perform periodic and real-time scans of systems and files.	Article 21(2)(f)	Requires monitoring to detect threats and indicators of compromise.
10.109	NIST SP 800-171 Rev. 2	System and Information Integrity (3.14.6)	Monitor inbound and outbound communications for attacks.	Article 21(2)(f)	Requires monitoring systems and communications to detect attacks.

S. No.	NIST Standard & Version	Family	NIST Family Summary	NIS2 Article number	NIS2 Article Summary
10.110	NIST SP 800-171 Rev. 2	System and Information Integrity (3.14.7)	Identify unauthorized use of organizational systems.	Article 21(2)(f)	Requires monitoring systems for unusual activity and security alerts.
11.1	NIST CSF 2.0	Govern	The mission, stakeholder expectations, dependencies, and legal or regulatory requirements surrounding cybersecurity risk management decisions are understood.	Article 7	EU Member States must create and maintain a national cybersecurity strategy covering governance, risk assessment, incident preparedness, recovery, awareness, and national policies.
11.2	NIST CSF 2.0	Govern	Organizational priorities, constraints, risk tolerance, appetite statements, and assumptions are established, communicated, and used.	Article 7	EU Member States must create and maintain a national cybersecurity strategy covering objectives, priorities, governance, risk assessment, and incident preparedness.
11.3	NIST CSF 2.0	Govern	Cybersecurity roles, responsibilities, and authorities are established to support accountability and continuous improvement.	Articles 8, 20	Article 8 requires cybersecurity authorities and a coordination contact point; Article 20 makes management responsible and accountable for cybersecurity measures and training.
11.4	NIST CSF 2.0	Govern	Organizational cybersecurity policy is established, communicated, and enforced.	Articles 20, 21, 25	Article 20 assigns management responsibility; Article 21 requires risk-management measures; Article 25 promotes international standards and ENISA guidance.
11.5	NIST CSF 2.0	Govern	Cybersecurity risk management results are used to improve and adjust the risk management strategy.	Articles 18, 19, 20, 31–37	Articles 18 and 19 support EU-level risk review and peer review; Article 20 establishes management accountability; Articles 31–37 address enforcement, audits, penalties, and cooperation.
11.6	NIST CSF 2.0	Govern	Cyber supply chain risk management processes are identified, established, managed, monitored, and improved.	Articles 21, 22, 24	Article 21 requires risk-based cybersecurity measures; Article 22 supports EU supply chain risk assessments; Article 24 promotes certified secure ICT products and services.
11.7	NIST CSF 2.0	Identify	Assets such as data, hardware, software, and services are identified and managed.	Article 21	Requires appropriate and proportionate cybersecurity risk-management measures to protect systems, manage incidents, ensure continuity, secure supply chains, and reduce cyber threats.
11.8	NIST CSF 2.0	Identify	Cybersecurity risk to the organization, assets, and individuals is understood.	Article 21	Requires companies to implement cybersecurity risk-management measures to protect network and information systems and reduce incident impact.

S. No.	NIST Standard & Version	Family	NIST Family Summary	NIS2 Article number	NIS2 Article Summary
11.9	NIST CSF 2.0	Identify	Cyber threat intelligence is received from information sharing forums and sources.	Article 29	Encourages voluntary sharing of cyber threat intelligence, supported by ENISA guidance and competent authorities.
11.10	NIST CSF 2.0	Identify	Processes for receiving, analyzing, and responding to vulnerability disclosures are established.	Article 12	Establishes coordinated vulnerability disclosure through CSIRTs and a European vulnerability database managed by ENISA.
11.11	NIST CSF 2.0	Identify	Improvements to cybersecurity risk management processes, procedures, and activities are identified across all functions.	Article 19	Allows Member States to conduct peer reviews and provide recommendations to improve cybersecurity implementation and cooperation.
11.12	NIST CSF 2.0	Protect	Access to physical and logical assets is limited to authorized users, services, and hardware according to risk.	Article 21	Requires cybersecurity risk-management measures to protect systems, manage incidents, ensure continuity, and secure supply chains.
11.13	NIST CSF 2.0	Protect	Personnel are provided with cybersecurity awareness and training to perform their tasks.	Article 21	Requires cybersecurity risk-management measures, including awareness, training, incident response, continuity, and supply chain security.
11.14	NIST CSF 2.0	Protect	Data are managed according to the organization's risk strategy to protect confidentiality, integrity, and availability.	Article 21	Requires measures to protect network and information systems and reduce the impact of cyber threats.
11.15	NIST CSF 2.0	Protect	Security architectures are managed according to the organization's risk strategy.	Article 21	Requires proportionate cybersecurity risk-management measures to protect systems and ensure continuity.
11.16	NIST CSF 2.0	Detect	Assets are monitored to find anomalies, indicators of compromise, and adverse events.	Articles 10, 11	Articles 10–11 require CSIRTs to monitor threats, issue alerts, support incident response, perform vulnerability checks, and cooperate with stakeholders.
11.17	NIST CSF 2.0	Detect	Anomalies, indicators of compromise, and adverse events are analyzed to detect incidents.	Articles 10, 11	Articles 10–11 require CSIRTs to monitor threats, support incident response, issue alerts, and cooperate with companies and authorities.
11.18	NIST CSF 2.0	Respond	Responses to detected cybersecurity incidents are managed.	Articles 9, 21	Article 9 requires national cyber crisis response plans; Article 21 requires risk-based measures to manage incidents and ensure continuity.
11.19	NIST CSF 2.0	Respond	Investigations support effective response, forensics, and recovery activities.	Articles 10, 11	Articles 10–11 require CSIRTs to support incident response, vulnerability checks, alerts, and cooperation.

S. No.	NIST Standard & Version	Family	NIST Family Summary	NIS2 Article number	NIS2 Article Summary
11.20	NIST CSF 2.0	Respond	Response activities are coordinated with internal and external stakeholders as required by laws or policies.	Articles 13–17, 23, 29, 30	Articles 13–17 support EU cooperation; Article 23 requires major incident reporting; Articles 29–30 encourage voluntary information sharing and reporting.
11.21	NIST CSF 2.0	Recover	Restoration activities are performed to ensure operational availability after cybersecurity incidents.	Articles 9, 21	Article 9 requires national cyber crisis response plans; Article 21 requires cybersecurity measures for incident management and business continuity.

A.2 Failure Mode and Effect Analysis

Table A.2: Failure Analysis Table

S No.	Component	Function	Failure Mode	Cause	Local Effect (Component Level)	System Effect (OT Level)
1.1	PLC	Read sensor inputs	Incorrect input reading	Sensor malfunction or noisy signals	PLC processes inaccurate input values	Incorrect control actions, such as wrong temperature or pressure.
1.2	PLC	Read sensor inputs	Loss of input signal	Cable damage or communication failure	PLC does not receive input data	System may become unsafe without real-time data.
1.3	PLC	Ensure security	Unauthorized access	Weak authentication or poor access control	PLC configuration or logic may be modified	Industrial process may be manipulated.
1.4	PLC	Monitor temperature and control heater	Heater not turning off	Faulty logic or incorrect temperature data	Heater remains ON	Overheating, equipment damage, and fire risk.
1.5	PLC	Communicate with SCADA	Communication failure	Network, cable, or configuration issue	PLC becomes isolated	Operators lose monitoring and remote control.
2.1	RTU	Collect sensor data	Incorrect data collection	Faulty sensors or signal interference	RTU stores and transmits incorrect data	Control system makes wrong decisions, leading to improper process operation
2.2	RTU	Transmit data to SCADA	Communication failure	Network failure or signal loss	RTU cannot communicate with central system	Operators lose visibility and control of remote processes
2.3	RTU	Security	Unauthorized access	Weak security mechanisms	RTU configuration or data modified	Attackers manipulate processes, causing disruption or safety risks
2.4	RTU	Maintain operation	Power failure	Electrical issues or battery failure	RTU shuts down completely	Loss of remote monitoring, system downtime, service interruption
2.5	RTU	Execute control commands	Failure to execute command	Software issues or hardware malfunction	Commands from SCADA not implemented	Remote equipment fails to respond, causing process disruption
3.1	SCADA	Monitor system data	Loss of data visibility	Communication issues or system error	SCADA screen does not display real-time data	Operators cannot monitor process, causing delayed response and increased risk
3.2	SCADA	Data storage	Data loss	Storage failure or database crash	SCADA cannot store or retrieve historical data	Loss of traceability affecting analysis, audits, and decisions
3.3	SCADA	Communication	Network failure	Network issues with PLCs/RTUs	SCADA disconnected from field devices	Loss of monitoring and control, leading to operational disruption
3.4	SCADA	Security	Cyberattack (malware/ransomware)	Network vulnerabilities exploited by malware	SCADA system compromised or unavailable	Large-scale disruption and possible shutdown of critical infrastructure
3.5	SCADA	Send control commands	Incorrect command execution	Software bugs or configuration errors	SCADA sends incorrect instructions	Machines operate incorrectly, causing damage or unsafe conditions

S No.	Component	Function	Failure Mode	Cause	Local Effect (Component Level)	System Effect (OT Level)
4.1	Sensors	Measure physical parameter (e.g., temperature)	Incorrect measurement	Faulty or poorly calibrated sensor, or environmental interference	Sensor outputs incorrect data	PLC/RTU receives wrong information and makes incorrect control decisions, leading to unsafe conditions
4.2	Sensors	Power supply	Power failure	Electrical issues or battery depletion	Sensor shuts down and stops sending data	Loss of process visibility, leading to downtime or unsafe operation
4.3	Sensors	Security	Cyberattack	Attackers inject false signals through vulnerabilities	Sensor data is falsified	System makes wrong decisions, causing disruption or damage
4.4	Sensors	Security	Tampering	Physical or digital manipulation by unauthorized personnel	Sensor sends altered or false data	System operates on false information, leading to process manipulation or safety risks
5.1	Controller	Access control	Unauthorized access	Weak security controls	Controller logic or configuration is altered	System manipulation and security risks occur
5.2	Controller	Data processing	Incorrect data interpretation	Noise or calibration errors in sensor data	Controller processes incorrect values	System makes wrong decisions, leading to unsafe or inefficient operation
6.1	HMI	Data display	Incorrect data display	Software bugs, data corruption, or communication errors	HMI shows inaccurate information	Operators make incorrect decisions, leading to process errors or safety risks
6.2	HMI	Data display	No data display	Loss of communication with PLC/RTU or system failure	No real-time information displayed	Loss of situational awareness and delayed response to incidents
6.3	HMI	User input	Incorrect operator input	Human error or poor interface design	Wrong commands entered into the system	Process disruption or unsafe system operation
6.4	HMI	Access control	Unauthorized access	Weak authentication or poor security configuration	Unauthorized users access the system	System manipulation and cybersecurity risks
7.1	SIEM	Log collection	Log failure	Network issues, misconfiguration, or unsupported log formats	Security logs are not collected	Critical threats go undetected, increasing cybersecurity risks
7.2	SIEM	Data storage	Log storage failure	Database crash, storage limitations, or corruption	Logs are lost or inaccessible	Loss of forensic evidence and compliance issues
7.3	SIEM	Incident monitoring	Delayed detection	Processing delays or system overload	Alerts are generated late	Slow response leads to increased damage and downtime

S No.	Component	Function	Failure Mode	Cause	Local Effect (Component Level)	System Effect (OT Level)
7.4	SIEM	Threat detection	Failure to detect threats	Misconfigured rules or outdated signatures	Malicious activities remain undetected	Cyberattacks compromise IT/OT systems and disrupt operations
8.1	VLAN	Network isolation	VLAN segmentation failure	Improper configuration or hardware malfunction	Separation between networks is lost	Attacker may move laterally from IT to OT systems
8.2	VLAN	Policy enforcement	Misconfigured firewall or ACL rules	Incorrect security policies	Traffic filtering fails	Exposure of sensitive systems to cyber threats
9.1	Firewalls/ Boundary Protection Devices	Boundary protection and traffic filtering	Permissive rule sets allowing unauthorized traffic	Misconfigure, permissive rules, or failure to restrict outbound OT traffic	Isolation between zones fails, allowing unauthorized traffic	Malware propagates from IT to OT systems, exposing field devices to cyberattacks
9.2	Firewalls/ Boundary Protection Devices	Deep packet inspection (DPI)	Inability to inspect malicious payloads	Encryption masking payloads or lack of OT-specific protocol parsers	Malicious payloads go undetected	Exploitation of OT endpoints through covert or unrecognized malicious commands
10.1	DNS	Distributed control	Controller node failure	Hardware fault or software crash	Local controller becomes unavailable	Disruption of plant sections and possible production downtime
10.2	DNS	Process control	Control loop failure	Controller malfunction or configuration error	Control loops do not function correctly	Process instability, reduced efficiency, or unsafe conditions
10.3	DNS	Security issues	Unauthorized access	Weak authentication or poor access control	System settings or logic are altered	Manipulation of industrial processes and security breaches
11.1	Data Historian (IT/OT)	Data logging	Corrupted or encrypted data	Ransomware or weak IT/OT isolation	Logs become inaccessible	Loss of operational insight; possible precautionary system shutdown
11.2	Data Historian (IT/OT)	Performance analysis	Manipulated records	Unauthorized access or malware	Engineers receive false trends and statistical outputs	Poor failure prediction, inefficient operation, unexpected breakdowns
11.3	Data Historian (IT/OT)	Compliance reporting	Data loss or unavailable	Malware, ransomware, or hardware failure	Historian system unavailable or wiped	Loss of compliance capability, regulatory penalties, financial risk
11.4	Data Historian (IT/OT)	Incident forensics	Logs deleted	Attacker clears logs	Loss of historical forensic data	Delayed root-cause analysis and slower system recovery

Table A.3: Risk Assessment Table

S no.	**Component**	**Severity (S)**	**Occurrence (O)**	**Detection (D)**	**Risk Priority Number (RPN) = S*O*D**
1.1	PLC	9	5	6	270
1.2	PLC	9	4	2	72
1.3	PLC	8	6	7	336
1.4	PLC	10	4	6	240
1.5	PLC	7	5	2	70
2.1	RTU	6	5	6	180
2.2	RTU	7	5	2	70
2.3	RTU	9	7	6	378
2.4	RTU	8	4	2	64
2.5	RTU	8	4	4	128
3.1	SCADA	7	5	2	70
3.2	SCADA	6	4	2	48
3.3	SCADA	8	5	2	80
3.4	SCADA	8	6	7	336
3.5	SCADA	9	4	6	216
4.1	Sensors	9	5	6	270
4.2	Sensors	9	4	2	72
4.3	Sensors	8	6	7	336
4.4	Sensors	9	5	6	270
5.1	Controller	8	6	7	336
5.2	Controller	9	5	6	270
6.1	HMI	9	5	6	270
6.2	HMI	7	5	2	70
6.3	HMI	9	5	6	270
6.4	HMI	8	6	7	336
7.1	SIEM	7	5	4	140
7.2	SIEM	6	4	2	48
7.3	SIEM	8	5	6	240
7.4	SIEM	8	6	7	336
8.1	VLAN	8	5	7	280
8.2	VLAN	7	5	6	210
9.1	Firewalls	8	5	6	240
9.2	Firewalls	8	6	7	336
10.1	DNS	8	5	2	80
10.2	DNS	9	5	6	270
10.3	DNS	8	6	7	336
11.1	Data Historian (IT/OT)	8	6	7	336
11.2	Data Historian (IT/OT)	8	6	7	336
11.3	Data Historian (IT/OT)	6	5	2	60
11.4	Data Historian (IT/OT)	6	6	7	252

A.3 Component-Wise Security Checklist

A.3.1 Security Information and Event Management (SIEM)

Table A.4: SIEM Threat Detection and Security Assessment

S No.	SIEM Type	Type of Threat	How SIEM Detects Threat	False Negative (Missed Threats)	Mitigation	Redundancy	Responsible Security Team
1	SIEM	Policy violations	Uses predefined correlation rules to trigger alerts when specific conditions are met	Detection mainly depends on rule-based logic with limited contextual or behavioral support	Continuous tuning of correlation rules and updates to detection logic	Combines multiple correlation engines and backup logging mechanisms	SOC Tier 1 (Security Operations Center – Level 1)
2	AI/ML-Based SIEM	Advanced persistent threats, zero-day attacks, insider threats	Supervised learning identifies known malicious behavior; unsupervised learning detects anomalies; deep learning analyzes behavioral sequences	Model drift over time; dependence on training data quality; difficulty detecting subtle attacks	Continuous model evaluation, retraining, drift monitoring, and improved data quality	Combines rule-based detection with statistical analysis and machine learning techniques	SOC Tier 2 + Detection Engineering Team
3	UEBA-Integrated SIEM	Insider threats, credential misuse	Builds behavioral baselines and detects deviations using peer group analysis and risk scoring	Subtle attacks resembling normal behavior may not be detected	Continuous updating of behavioral baselines and refinement of risk scoring	Integrates behavioral analytics with SIEM correlation and contextual enrichment	SOC Tier 2 + Data Analysis Team
4	MITRE ATT&CK-Aligned SIEM	Multi-stage attacks and adversary techniques	Maps events to ATT&CK techniques using threat intelligence and behavioral detection engineering	Detection gaps when telemetry or log sources are incomplete	Log source auditing and ATT&CK gap analysis to improve visibility	Uses multiple data sources and detection techniques aligned with ATT&CK	Threat Hunting Team + SOC Tier 3
5	SOAR-Integrated SIEM	Complex attack campaigns and ransomware	Automates enrichment, investigation, and response using workflows and playbooks	Ineffective response if playbooks or detection triggers are poorly configured	Playbook standardization, continuous tuning, and maintaining human oversight	Combines SIEM detection, threat intelligence, and automated response workflows	SOC + Incident Response Team
6	SIEM	Phishing	Detects suspicious emails, unusual login attempts, and compromised credentials	Sophisticated phishing attacks may bypass detection	Reset passwords, block malicious links, and conduct employee awareness training	Restore affected email accounts and data from backups	SOC Tier 1 + SOC Tier 2
7	SIEM	Ransomware	Detects unusual file encryption, rapid file renaming, and suspicious programs	New or advanced ransomware may evade detection	Isolate infected systems, remove malware, and secure compromised accounts	Restore encrypted files from offline and immutable backups	Incident Response Team + SOC Tier 3
8	SIEM	Malware	Identifies harmful software through abnormal behavior and suspicious activities	Unknown or hidden malware may evade detection	Remove malicious software and update security tools	Restore systems using clean system image backups	SOC Tier 2 + Endpoint Security Team
9	SIEM	Unauthorized Access	Detects suspicious logins from unusual locations or devices	Attackers using stolen credentials may appear legitimate users	Reset passwords and enforce multi-factor authentication	Restore affected accounts using identity and access backups	IAM Team + SOC Tier 2
10	SIEM	Man-in-the-Middle (MitM) Attack	Analyzes network traffic, firewall logs, IDS alerts, and SSL/TLS certificates to detect anomalies	Detection may fail when attackers use spoofed certificates or encrypted traffic	Enforce HTTPS and secure network configurations	Restore systems from clean backups and reissue certificates	Network Security Team + SOC Tier 3

A.3.2 Firewall Systems

Table A.5: Firewall Threat Detection and Security Assessment

S No.	Firewalls	Type of Threat	How Firewall Detects the Threat	False Negative (Missed Threats)	Mitigation	Redundancy	Responsible Security Team
1	Traditional Hardware Firewall (IT/OT)	Distributed Denial of Service (DDoS), unauthorized access, malware infections	Relies on static rule enforcement, manual configurations, and static rule sets	Fails to identify new attack patterns dynamically because it relies on static rules and struggles with rapidly evolving network environments	Requires manual intervention to update security rules	Physical backup servers integrated into the traditional network topology	Network Security Team + SOC
2	VM-Based Virtual Firewall (IT/Cloud)	Standard network threats and attacks exploiting high processing latency	Inspects and filters incoming and outgoing Internet traffic utilizing full OS emulation and hypervisors	High CPU and memory consumption can lead to processing latency, potentially masking time-sensitive industrial threats	Transitioning to lightweight containerized virtualization to reduce processing overhead and latency	Virtual database and file backups connected via virtual switches	Network Security Team + Cloud Security Team
3	Containerized AI-Driven Firewall (Hybrid IT/OT)	Ransomware, DoS, Advanced Persistent Threats (APTs), and abnormal network behavior	Uses AI-based anomaly detection for real-time traffic analysis and Python/Scapy packet sniffing to inspect IP sources and protocols	May potentially miss threats originating from low-power IIoT edge devices if detection models are not optimized for edge computing	Software-Defined Networking (SDN) dynamically updates firewall rules based on AI threat intelligence	Parallel IDS container, logging and monitoring container, and continuous network probes/sensors	SOC + Security Engineering Team
4	Email Security Firewall (IT)	Phishing emails, malicious attachments, spam-based attacks	Scans email traffic for malicious links, attachments, and suspicious sender behavior	New phishing techniques or highly targeted attacks may bypass filters	Use advanced email filtering, user awareness training, and sandboxing	Backup email filtering systems and cloud-based email security	SOC + IAM Team
5	Firewall + IDS (Intrusion Detection System)	General DoS / DDoS attacks	Detection is performed using traffic analysis, attack signatures, and CPU/system metrics to identify abnormal traffic patterns	Intelligent or distributed attacks may blend with legitimate traffic, making detection difficult	Entropy-based detection, queue prioritization, and traffic filtering techniques	Combines multiple defense layers including firewall, IDS, and traffic analysis	SOC + Network Security Team
6	Packet Filtering Firewall	UDP Flood / ICMP Flood attacks	Checks packet header fields such as source/destination IP addresses and ports against ACL rules	Sophisticated or disguised traffic may pass through because only packet headers are inspected	Use proper rule configuration, filtering policies, and regular updates/patching	Works together with IDS and other network defenses for layered protection	Network Security Team
7	Stateful Firewall (Dynamic/Stateful Filtering)	SYN Flood attacks	Maintains active session tables and tracks TCP states to detect incomplete handshakes or abnormal connection requests	Distributed or slow-rate attacks may avoid threshold-based detection	Cryptographic client puzzles ensure only legitimate users receive service	Uses session tracking and layered defense mechanisms	Network Security Team + SOC
8	Firewall Systems (General)	Reconnaissance and probing attacks	Attackers send probe packets and analyze response timing to infer firewall rules	Probing traffic often appears legitimate and may not be detected as malicious activity	DIR-based random response delays prevent accurate rule discovery	Uses Moving Target Defense (MTD) strategies to dynamically change observable behavior	SOC + Threat Hunting Team

A.3.3 Human Machine Interface (HMI)

Table A.6: HMI Threat Detection and Security Assessment

S No.	HMI	Type of Threat	How this Threat Occurs	Mitigation	Redundancy	Responsible Security Team
1	HMI	Display manipulation	Attackers alter operational data shown on HMI systems through compromised communication channels, misleading operators about equipment conditions	Data integrity validation, secure communication using encryption, and anomaly detection	Cross-check with redundant sensors, digital twins, and independent displays	OT Security Team + SOC Team
2	HMI	Alarm suppression / false alarms	Attackers suppress critical alarms or generate false alarms, disrupting maintenance prioritization and operational response	Behavioral monitoring, secure system design, and operator training	Multiple alarm channels and independent monitoring dashboards	SOC Team + OT Security Team
3	HMI	Maintenance log manipulation	Maintenance logs and timestamps are modified to mislead maintenance planning or hide faults	Role-based access control (RBAC), authentication, and integrity verification	Cross-validation with secure historian systems and backup records	IAM Team + SOC Team
4	HMI	Threshold manipulation	Attackers modify alarm thresholds or system parameters, affecting predictive maintenance decisions	Role-based access control, anomaly detection, and system hardening	Independent validation of configurations and redundant monitoring systems	OT Security Team
5	HMI	Unauthorized access (weak authentication)	Shared accounts or weak passwords allow attackers to gain unauthorized access while appearing as legitimate users	Multi-factor authentication, individual accounts, and privilege separation	Monitor access across systems and verify actions through multiple interfaces	IAM Team + SOC Team
6	HMI	Legacy system exploitation	Outdated operating systems, unpatched software, and insecure plugins expose vulnerabilities to attackers	System hardening, regular patching, and migration from legacy systems	Backup systems and parallel secure environments to validate outputs	OT Engineering Team
7	HMI	Unexpected software installation	Unauthorized or malicious software is installed by users or attackers without approval	Isolate the system and remove unknown applications	Restore the system if integrity is compromised and implement application control policies	Incident Response Team + SOC
8	HMI	Malware infection (USB or untrusted downloads)	Malware is introduced through infected USB devices, downloaded files, or compromised software transferred from IT networks	Disconnect HMI from the network immediately and perform a security scan	Reinstall the system from a trusted image and restore clean backups while restricting USB usage	Incident Response Team + SOC

A.3.4 Virtual Local Area Network (VLAN)

Table A.7: VLAN Threat Detection and Security Assessment

S No.	VLAN	Type of Threat	How this Threat Occurs	Mitigation	Redundancy	Responsible Security Team
1	VLAN	Switching Loop	Multiple links between switches cause frames to loop continuously, leading to broadcast storms and network failure	Spanning Tree Protocol (STP) detects loops and blocks unnecessary paths	Maintain redundant links in blocked state and automatically activate alternate paths using STP recalculation	Network Engineering Team
2	VLAN	Default Gateway Failure	Misconfiguration of FHRP may delay or fail failover	First Hop Redundancy Protocol (FHRP) creates a virtual gateway shared by multiple routers	Use virtual gateway with multiple routers so traffic is automatically redirected through standby devices	Network Engineering Team
3	VLAN	Unauthorized Access	An unauthorized device connects to a switch port and attempts to access the network	Port security allows only specific MAC addresses and shuts down violating ports	Use redundant secure ports or backup switches with identical port security configuration	Network Security Team + SOC
4	VLAN	Network Vulnerabilities	Lack of segmentation and access control leads to multiple security risks	Combining VLANs, ACLs, and port security creates layered protection	Deploy redundant switches and routers with identical VLAN and ACL configurations	Network Security Team
5	VLAN	Weak Switch Authentication	Devices are automatically allowed network access without identity verification	Use NAC, enable port security, and restrict the number of devices per port	Disconnect unauthorized devices, restore configurations from backup, and verify policies	IAM Team + Network Security Team
6	VLAN	Private VLAN (PVLAN) Attack	A host bypasses PVLAN isolation using router MAC forwarding behavior	Use ACLs and VLAN ACLs to block unauthorized communication between hosts	Restore correct PVLAN configuration from backup and validate isolation	Network Security Team
7	VLAN	Improper Network Segmentation	Poor segmentation allows lateral movement and unauthorized access between sensitive systems	Use VLAN segmentation, firewalls, and ACLs with strict communication boundaries	Separate IT, OT, and HMI networks using redundant segmentation strategies	Network Security Team
8	VLAN	Switch Spoofing	Attackers exploit DTP to create unauthorized trunk links and gain VLAN access	Disable DTP and unused ports and manually configure trunk/access ports	Works when ports are in default mode; virtual switches may partially block the attack	Network Security Team
9	VLAN	Double Tagging	Frames containing double VLAN tags bypass VLAN isolation	Avoid native VLAN usage and secure trunk configurations	Requires trunk links and native VLAN; virtual switches may act as secondary switches	Network Security Team
10	VLAN	ARP Poisoning (MitM)	Attackers send fake ARP messages causing traffic redirection through malicious systems	Use DHCP snooping, Dynamic ARP Inspection (DAI), and ARP monitoring tools	Works in many environments without built-in virtual switch protections	SOC + Network Security Team
11	VLAN	VLAN Database Corruption	Human errors, rogue switches, or incorrect VTP updates overwrite VLAN databases	Disable unused VTP, use transparent mode, and apply VTP authentication	Restore VLAN database from trusted backups and verify segmentation before operations resume	Network Engineering Team + Incident Response Team

A.4 Additional Family Requirement in NIST SP 800-171 Rev.3

Table A.8: New Control Families in NIST SP 800-171 Rev.3 with ODPs

S.no.	Requirement Family	Rev 3 New Requirements	Requirement Description
1	Planning	03.15.01 Policy and Procedures	Develop, document, and disseminate to organizational personnel or roles the policies and procedures needed to satisfy the security requirements for the protection of CUI.ODP(Organization defined Parameters) 03.15.01.b:organization-defined frequency
		03.15.02 System Security Plan	Develop, review, and update a system security plan that defines system components, threats, and specific safeguards.ODP 03.15.02.b:organization-defined frequency
		03.15.03 Rules of Behavior	Establish rules that describe the responsibilities and expected behavior for system usage and protecting CUI.ODP 03.15.03.d: organization-defined frequency
2	System and Services Acquisition	03.16.01 Security Engineering Principles	Apply systems security engineering principles to the development or modification of the system and system components.ODP 03.16.01: organization-defined systems security engineering principles
		03.16.02 Unsupported System Components	Replace system components when support for the components is no longer available, or provide options for risk mitigation.(No ODPs present)
		03.16.03 External System Services	Require providers of external system services to comply with security requirements and monitor their compliance on an ongoing basis. ODP 03.16.03.a:organization-defined security requirements
3	Supply Chain Risk Management	03.17.01 Supply Chain Risk Management Plan	Develop, review, update, and protect a plan for managing supply chain risks associated with the system or system services.ODP 03.17.01.b:organization-defined frequency
		03.17.02 Acquisition Strategies, Tools, and Methods	Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks. (No ODPs present)
		03.17.03 Supply Chain Requirements and Processes	Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes, and enforce security requirements. ODP 03.17.03.b:organization-defined security requirements

Table A.9: Major Revisions and Additions in NIST SP 800-171 Rev.3

S.no.	Area of Change	Description of Revisions in Rev 3
1	Organization-Defined Parameters (ODPs)	Introduced ODPs in selected security requirements to increase flexibility and help organizations better manage risk. A new appendix was also added to list these parameters.
2	Security Requirements & Families	Modified requirements and families to reflect the security controls in the SP 800-53B moderate baseline. Added new security requirements, removed outdated or redundant ones, and grouped requirements where possible to improve understanding and efficiency.
3	Requirement Categorization	Completely eliminated the distinction between "basic" and "derived" security requirements.
4	Specificity & Language	Increased the specificity of the requirements to remove ambiguity, clarify the scope of assessments, and improve implementation effectiveness. Revised the requirements to be consistent with the security control language in SP 800-53.
5	Titles & Discussions	Added specific titles to all security requirements and restructured and streamlined the discussion sections for each requirement.
6	Tailoring Categories	Added new tailoring categories: Other Related Controls (ORC) and Not Applicable (N/A). Recategorized selected controls from the SP 800-53B moderate baseline using these new criteria and revised the tailoring tables in Appendix C.
7	Document Structure	Streamlined the introductory information in Sections 1 and 2, and revised the structure of the References, Acronyms, and Glossary sections for greater clarity and ease of use.