UNIVERSITY OF TURKU

Cybersecurity Standard-Based Model for IT/OT Converged Environments

Cyber Security

Master's Degree Programme in Information and Communication Technology

Department of Computing, Faculty of Technology

Master of Science in Technology Thesis

Author:

Kimi Uutela

Supervisors:

Petri Sainio

Jouni Isoaho

May 2025

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin Originality Check service.

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

Subject: Cyber Security
Programme: Master's Degree Programme in Information and Communication Technology
Author: Kimi Uutela
Title: Cybersecurity Standards-based Model for IT/OT Converged Environments
Number of pages: 184 pages
Date: May 2025

This thesis addresses the cybersecurity challenges posed by the convergence of Information Technology (IT) and Operational Technology (OT) in industrial environments. The aim is to develop a practical cybersecurity framework that supports secure operations, regulatory compliance, and risk management in mixed IT/OT systems. The research is based on an extensive analysis of internationally recognized standards such as the IEC 62443 series, ISO 27001, and the EU NIS2 Directive, comprehended by industrial reference architectures including PERA, RAMI 4.0, and IIRA, and a review of recent academic and industry research.

The thesis proposes a modular cybersecurity framework structured into six control domains: Network, Hardware, Software, Redundancy, Governance and Compliance, and Security. This structure allows organizations to organize their cybersecurity practices systematically across industrial environments. The results show that existing standards, despite their varied scopes, can be interpreted and integrated to support a unified governance and control model for IT/OT environments.

The thesis concludes that a domain-based structure offers a practical and clear methodology for implementing cybersecurity controls in industrial operations. The work highlights the need for continuous assessment and adaptation of cybersecurity measures due to evolving threats and addresses limitations in harmonization across existing industrial cybersecurity standards.

Keywords: Industrial Cybersecurity, IT/OT Convergence, Cybersecurity Framework, Risk Management, Industrial Control Systems, Operational Technology Security, Cybersecurity Standards, Critical Infrastructure Protection

Acknowledgements

I want to express my gratitude to the University for supporting my academic and professional growth over the years, creating an environment that allowed me to balance my studies and work successfully. It has been invaluable. I extend my special thanks to my supervisors, Jouni Isoaho and Petri Sainio, whose guidance, encouragement, and insightful feedback were essential throughout the thesis process.

I am especially thankful to Tomi Airo and my colleagues at Consolis for their continued support throughout my professional journey, which began in 2015. Having started my professional life at the age of 14, this thesis culminates nearly a decade of growth within the same organization. Their mentorship, encouragement, and possibilities not only shaped my professional development but also played a key role in sparking my interest in computer science, ultimately guiding me toward this field of study. It has been a privilege to grow within the company, deepen my expertise, and pursue higher education simultaneously. Their flexibility and understanding in accommodating my academic goals alongside my professional duties played a significant role in making this thesis possible.

The practical nature of this research has been deeply informed by real-world challenges faced throughout my time in industrial environments. I am grateful for the opportunity to connect academic inquiry with operational realities, which enriched both the outcomes of this thesis and my personal growth.

Lastly, I want to thank my friends for their support, encouragement, and understanding during my university years. I am deeply grateful to my family for their enduring patience and belief in me through the good and more challenging times.

Table of Contents

1 Introduction

The convergence of Information Technology (IT) and Operational Technology (OT) has become one of the most defining transformations in industrial environments. This digital evolution is characterized by the growing interconnection of traditional operational systems such as programmable logic controllers (PLCs), industrial networks, sensors, and supervisory control and data acquisition (SCADA) systems with IT platforms, including cloud infrastructure, enterprise resource planning (ERP) systems, and data analytics platforms. This integration enables increased automation, real-time data-driven decision-making, and improved operational efficiency. However, it also introduces new risks and vulnerabilities due to the exposure of previously isolated systems to broader threat landscapes.

Cybersecurity in industrial settings has become an increasingly urgent priority as organizations face the dual challenge of maintaining operational continuity while safeguarding against an expanding array of cyber threats. The rise in targeted attacks against critical infrastructure, such as ransomware campaigns and supply chain intrusions, demonstrates the evolving threat landscape. These developments underscore the importance of structured security governance spanning IT and OT domains. While many international standards offer security guidance, few provide a comprehensive blueprint for integrating controls across the technical and organizational boundaries in complex industrial environments.

To address this gap, this thesis explores how industrial organizations can design a comprehensive IT/OT cybersecurity environment model that is grounded in internationally recognized standards, acceptable to different operational contexts, and aligned with real-world requirements. The goal is to synthesize a flexible and modular framework that supports organizations in implementing cybersecurity practices in a traceable, scalable, and context-aware manner.

The framework developed in this thesis is built upon a foundation of key cybersecurity and risk management standards, including the IEC 62443 series, ISO 27001, ISO 31000, ISO 27005, and the EU's NIS2 Directive. Additionally, modern industrial reference architectures such as the Reference Architectural Model for Industry 4.0 (RAMI 4.0), the Industrial Internet Reference Architecture (IIRA), and the Purdue Enterprise Reference Architecture (PERA) are reviewed to align structural design with prevailing industrial practices.

The outcome of this thesis is a domain-based control structure consisting of six areas: Network, Hardware, Software, Redundancy, Governance and Compliance, and Security. These domains were chosen based on both theoretical analysis and practical considerations, ensuring that the framework is applicable across diverse industries and technological environments. Each domain allows for focused analysis and control implementation, enabling organizations to manage cybersecurity at multiple IT/OT landscape layers.

To guide this, the thesis addresses the following research questions:

1. How can industrial organizations develop a comprehensive IT/OT cybersecurity framework that balances security, operational efficiency, and regulatory compliance?

2. What are the main challenges and best practices for standardizing IT/OT infrastructure across diverse industrial facilities, and how can these be addressed using existing standards and models?

3. How does IT/OT integration impact cybersecurity postures in industrial environments, and what strategies can organizations adopt to mitigate emerging risks while enhancing interoperability and resilience?

The structure of this thesis progresses logically from contextual understanding to practical application. Chapter 2 begins with a foundational overview of the industrial system, laying the groundwork for understanding the complexity and implications of IT/OT convergence. Following this, Chapter 3 introduces the regulatory and technical standards that form the basis of the proposed framework, drawing from both cybersecurity and risk management domains. Chapter 4 presents the rationale for the six-domain framework structure, offering justification for the chosen areas of focus based on theoretical alignment and practical relevance. In Chapter 5, the framework is applied across the identified domains, illustrating implementation strategies and mapping relevant technical controls. Chapter 6 expands on the discussion by reflecting on framework adoption, maturity levels, and broader industrial trends, incorporating observations from academic literature and real-world practices. Finally, Chapter 7 draws together the key findings, addresses the research questions in detail, and highlights directions for future exploration.

Through this structure, the thesis aims to deliver a usable, standards-aligned framework that addresses the security challenges of modern industrial environments while promoting clarity, modularity, and adaptability across various organizational and technological contexts.

2 Automation in Industrial Technologies

Industrial systems form the foundation of modern manufacturing and infrastructure operations. These systems encompass a diverse range of components, technologies, and architectures designed to support the reliable, safe, and efficient functioning of industrial processes. Historically, these systems have been engineered with a focus on high availability, deterministic behavior, and real-time responsiveness, which distinguishes them from traditional IT systems. While IT systems prioritize confidentiality and data processing, industrial systems place the highest emphasis on uptime and integrity of physical processes. Industrial environments typically consist of OT, which encompasses hardware and software used to control physical devices and processes [1], [2]. This includes systems such as Programmable Logic Controllers (PLCs), Supervisory and Data Acquisition Systems (SCADA), and Distributed Control Systems (DCS), and the related software [1], [2]. These components interact with the physical environment through field devices such as sensors and actuators, forming closed feedback loops that ensure continuous process controls. In addition to these, Human-Machine Interfaces (HMIs) enable operators to interact with and monitor ongoing industrial operations.

Earlier in the 2000s, OT and IT were technically and organizationally separated. However, as the digital era has transformed, organizations recognize the need for IT and OT to collaborate more closely [3]. IT and OT are converging, and communication technologies and classifications of cybersecurity concerns are driving the need for collaboration between these environments. This is already evident in organizations, as 38% have reported a shared IT-OT cybersecurity budget, with a significant portion allocated to technologies such as segmentation and access control across the environment [4]. The phenomenon we are observing is often referred to as IT and OT convergence in academic literature. Industrial application platforms are nowadays required to communicate with the information infrastructure. The advantages are evident in areas like automation and computing platforms, with numerous open communication servers, edge computing solutions, and applications in deep learning, machine learning, and artificial intelligence already available [3]. All of this occurs as IT integrates with OT through autonomous systems and machine virtualization. A roadmap connecting IT and OT systems is now more essential than ever, and creating a security-focused strategy is vital for organizations.

To manage the complexity of such environments, industrial systems are often structured using hierarchical models, with the Purdue Enterprise Reference Architecture (PERA) being one of the most widely adopted models [5]. This model segments systems into five levels – from Level

0 (physical processes) to Level 4 (enterprise planning) – to provide functional separation and facilitate the implementation of network segmentation and security controls [5]. The lower levels (0-2) are primarily concerned with physical processes and control logic, while the upper levels (3-4) integrate production with enterprise systems, such as ERP or MES [5]. Later, the same model was used in ISA/IEC 62443, ISO, and NIST standards [3]. Most organizations (72%) are mapping their control systems to recognized security frameworks such as NIST and IEC 62443 [4]. Similar notices are made in academic literature, where industrial control systems that span across IT and OT make traditional IT-focused risk assessment insufficient [6]. It is emphasized that single-dimensional evaluations are not enough, and there are proposed methodologies for OT specific functionalities and cyber-physical interactions [6]. This underscores the importance of established standards in guiding modern industrial network security practices but also highlights the intrinsic complexity of industrial environments, where security cannot be detached from safety, reliability, and operational continuity.

Purdue's model, however, does not come without its limitations. The increasing convergence of IT and OT systems renders this strict segmentation impractical. The demand for real-time data exchange between enterprise and control layers has grown in modern industrial environments. Organizations are increasingly adopting cloud-based solutions for ICS environments. Traditional segmentation models are being reevaluated to accommodate new architectures and ensure security resilience across IT and OT environments. Emerging technologies like Industrial IoT (IIoT) and cloud computing blur the lines between the traditional Purdue layers, requiring new network segmentation and security approaches. Due to the growing need for data exchange between enterprise and control layers, organizations spend more money on shared IT-OT cybersecurity budgets to bridge the gap between traditional network segmentation. These technologies introduce complexities not considered in the original Purdue model, prompting organizations to adapt the model to accommodate more flexible and dynamic architectures. With traditional Purdue segmentation, 55% of organizations in 2024 ranked network protections, including boundary protection, as a top priority, reflecting the critical need to limit incident spread across all IT and OT infrastructure layers [4]. For example, by isolating the OT environment from the IT environment, the Purdue model ensures that potential breaches in the IT layer do not immediately compromise critical control systems at lower levels [3]. The segregation approach is necessary, especially for essential infrastructure sectors and employee safety. Due to the hierarchical nature of practice, this approach has

become an effective way to break down OT environment solutions, providing better system management in complex environments.

In the past, these systems were largely air-gapped, with little to no external connectivity. This isolation served as a thick set for security. However, with the emergence of Industry 4.0 and digital transformation initiatives, industrial systems are increasingly integrated with IT networks to support features such as predictive maintenance, real-time analytics, and remote diagnostics. However, industrial cyber-physical systems now combine computing and network capabilities with physical processes to enhance operational flexibility and efficiency [7].

Another big driver in the industrial field is the Internet of Things (IoT), specifically the Industrial Internet of Things (IIoT) [8]. The basic idea of the IoT is to attach technology to devices that have not been on the internet in the past. The purpose of the IIoT is to receive information from machinery in real-time, which helps with maintenance and process optimization, for example. There are already clear signs of the increasing number of IoT devices in industrial networks, which poses a challenge in managing networks in production facilities. Active nodes in the network increase, and signals in the production facilities increase [8]. With the rising number of IIoT devices, visibility remains a challenge; only 5% of organizations claim to have visibility over OT activities, which is a surprising decrease from previous years [9]. Interference in the signals across the production facility might cause unwanted movements in the machinery or signal blockage; interference at the premises must be managed better than the business is most likely prepared to.

Adopting IIoT platforms further accelerates this integration by enabling ubiquitous sensing and data-driven automation. In addition to the PERA model, several modern architectural frameworks have been introduced to support the evolution of industrial systems within the context of Industry 4.0. Notably, the Industrial Internet Reference Architecture (IIRA) and the Reference Architecture Model Industrie 4.0 (RAMI 4.0) models aim to bridge the operational and informational domains [10], [11]. IIRA, developed by the Industrial Internet Consortium, emphasizes cross-sector interoperability and business-driven design, while RAMI 4.0 integrates lifecycle and hierarchy dimensions to map all relevant layers of a smart factory.

These changes bring substantial benefits, including cost reduction, improved productivity, and increased system transparency. However, they also introduce new challenges, particularly around interoperability and cybersecurity. Legacy systems, often not designed for modern threats, coexist with new technologies, creating heterogeneous environments that are difficult

to secure uniformly. Moreover, long device lifecycles and proprietary communication protocols continue to limit the ability to apply standard IT security measures. The increasing heterogeneity in industrial environments necessitates standardized interfaces and protocols for seamless communication across layers [11]. In response to these challenges, there are research and development efforts focused on enhancing the intelligence and adaptability of industrial systems. Frameworks like OPC UA, AutomationML, and the Asset Administration Shell have emerged to support interoperability, enabling consistency across devices and platforms [11]. Digital twins, edge computing, and artificial intelligence are being applied to improve process optimization, fault prediction, and incident response. Such technologies are pushing the environment forward, reducing downtime, and enhancing resilience by enabling real-time decision-making and automated anomaly detection [12]. However, the research highlights that the lack of semantic standardization remains a significant bottleneck for industrial integration [11].

Despite the technological advancements, the critical nature of industrial systems demands a cautious and measured approach to digital integration. As stated in the 2024 SANS State of ICS/OT Cybersecurity report, the expanding connectivity of OT systems has exposed them to a broader threat landscape [4]. The report also highlights that the most common attack vector is now IT-to-OT lateral movement, where compromised IT assets provide a pathway into critical OT environments. The number of reported intrusions into industrial control systems has increased significantly in 2024, with nearly one-third of organizations experiencing six or more intrusions in the past year alone and almost two-thirds having experienced three or more intrusions [9]. This represents a significant increase from previous years, attributed to the growing convergence of IT and OT systems, as well as the heightened exposure that industrial networks face from external threats [9]. The number of global industrial control system safety incidents has increased since 2012, coinciding with the rise in internet users. This risk is compounded by insufficient visibility and monitoring in many industrial networks, with over half of organizations reporting limited situational awareness [4]. These developments underscore the importance of adopting robust, layered security architectures tailored to the unique requirements of industrial systems. Studies and standards recommend implementing defense-in-depth strategies, network segmentation, and continuous monitoring to safeguard critical infrastructure [13]. Current market studies also highlight the effect, as the Fortinet OT Cybersecurity Report points out, achieving cybersecurity in OT is not merely a technical

challenge, but an organizational one that requires collaboration across IT, engineering, and executive leadership [9].

2.1 Challenges in IT/OT Converged Environments

Today's industrial systems combine electrical systems and networking parts, which are integrated with automation, supervisory control, and data acquisition systems, making them highly complicated [14]. Originally, industrial control system security implementations were primarily vulnerable to local threats due to the location of the components, which were not connected to any networks [15]. Today, however, these systems are increasingly utilizing more reliable and standardized IT technologies. Originally, industrial systems were designed to control processes locally and had to be safe and reliable, rather than secure. As industrial systems evolve from traditionally isolated infrastructures into digitally integrated ecosystems, the convergence of IT and OT introduces a range of new challenges [15]. While the integration is driven by objectives such as increased efficiency, centralized data collection, remote monitoring, and predictive maintenance, it simultaneously exposes legacy OT environments to the threat landscape of IT systems.

Industrial computing underwent a revolution, like any other computing and communication field, in the 2000s. The ICT aspects of our lives have significantly expanded our insights and changed nearly every aspect of our lives. Industrial fields are also hanging on to this IT boom. The term "cyberphysical system" was first introduced in 2006, used to demonstrate the increasingly important areas of computing physical processes [7]. In 2020, the European Commission initiated public-private partnership operations under the "Factories of the Future" initiative, and the German Federal Ministry of Education and Research also adopted the Industry 4.0 name [8]. The current trend in industry requires more interconnectivity, connectivity, interoperability, and flexibility to adapt to the solutions that industrial applications are receiving to optimize production processes. ICS environments with cloud adaptations have been on the rise, and their growth increased by 39% in 2024. However, most of these solutions were only for telemetry and disaster recovery [4]. As we explore AI solutions, only 10% have connected their ICS systems to utilize AI in the environment, which reflects a cautious approach to emerging technologies due to security and reliability concerns [4]. The demand for solutions is already high, but it is expected to increase in the coming years as more PLCs and machinery are connected to the internet.

In 2024, 73% of organizations reported experiencing cyber intrusions affecting both IT and OT systems, illustrating the scale of exposed industrial environments [9]. Threats that they were never expecting to encounter, so they do not have a defense against them. Secondly, commercial solutions are often used to replace the original industrial control systems with new hardware. The vulnerabilities of commercial solutions can be exploited without specialized knowledge of industrial control systems [15]. A crucial example of this can be found in the statistics that commercial IT devices were among the primary attack vectors for ICS solutions in 2024, allowing attackers to bypass traditional ICS defenses and exploit these systems through traditional vulnerabilities [9]. To exacerbate this situation, organizations often opt for standard IT security protection for industrial systems that do not adapt or cannot be effectively integrated into industrial environments. Security through obscurity is no longer a suitable defense [15]. Threats to any control system can vary and originate from numerous sources, including governments, malicious intruders, complex systems, or accidents. Protecting the integrity of industrial systems and their data is essential not only for worker safety but also for the continued success of organizations. Thirty-nine percent of organizations have addressed this by placing the responsibility for ICS systems under a CISO, which reflects a movement toward centralized security management that can better address cross-domain vulnerabilities [4].

One of the primary challenges of IT/OT convergence is the fundamental differences in priorities and design assumptions. As stated in the CIA triad, IT environments traditionally prioritize confidentiality, integrity, and availability, whereas OT environments are designed around availability, safety, and deterministic control. As a result, applying standard IT security controls, such as frequent patching, network scanning, or endpoint detection, can disrupt OT processes. According to the SANS 2024 ICS/OT cybersecurity report, over 40% of organizations refrain from applying patches on time due to the fear of operational disruption, even when known vulnerabilities are identified [4]. The legacy nature of OT systems adds to this complexity. Many industrial control systems still in use today were designed decades ago, using proprietary protocols and hardware that lack built-in security features. Their long lifecycles and closed ecosystems mean that retrofitting modern security measures is technically and economically challenging. These limitations are taken further when older OT networks are connected to enterprise IT systems or the cloud, creating new attack surfaces to OT platforms. As an example, this was the technique used in high-profile incidents such as the TRITON and Colonial Pipeline attacks in 2024 [9].

In addition to technical issues, IT/OT convergence introduces governance and organizational challenges. OT teams often have deep domain expertise in industrial processes but lack exposure to cybersecurity frameworks, while IT teams are more familiar with risk management and digital threats but lack the understanding of physical process constraints. The cultural and operational divide can hinder incident response, risk assessment, and policy development. Bridging this gap requires collaborative governance models, joint training initiatives, and integrated operational workflows [10]. Visibility and monitoring clearly pose significant difficulties as well in converged environments. While IT networks often utilize centralized logging, intrusion detection systems, and Security Information and Event Management (SIEM) tools, such solutions may not be compatible with OT protocols or devices. The SANS 2024 report reveals that only 44% of organizations report having full visibility into their OT assets, leaving significant blind spots [4]. The lack of visibility and situational awareness impedes both proactive defense and timely response to incidents.

Another key concern is the supply chain security. Third-party service providers, integrators, and equipment manufacturers play critical roles in converged architectures. Ensuring the security of third-party entities becomes essential, especially when remote access or software updates are involved. NIS2 directive emphasizes this point by requiring essential entities to manage risks to address supply chain dependencies, urging organizations to assess the cybersecurity practices of their suppliers [16]. Compliance with regulatory standards in a converged context is increasingly complex. Standards such as ISO 27001 and IEC 62443 provide structured frameworks for implementing cybersecurity practices in IT and OT environments; however, their alignment and practical integration often remain fragmented, resulting in issues. This leads to inconsistent semantics, delayed integration, and difficulty in lifecycle traceability when devices or components are sourced from different vendors. For example, ISO 27001 defines requirements for information security management systems, while IEC 62443 delves into the responsibilities of asset owners, secure development, and component-level protections. Harmonizing the standards to support real-world convergence is a challenge that many organizations are trying to address, but it would also require global harmonization [11].

Furthermore, architectures such as the PERA, IIRA, and RAMI 4.0 aim to structure IT/OT systems; however, practical adoption still encounters barriers due to system incompatibilities and inconsistent implementation [5], [10], [11]. The conclusion is that IT/OT environments bring substantial operational benefits but also introduce a multifaceted set of challenges to

manage. These not only stand ground in technological integration and legacy limitations, but also in compliance. Recognizing and addressing these challenges early in the design and development of converged environments helps to build a better future. As digital transformation accelerates, organizations must adopt holistic, cross-disciplinary strategies to ensure that the convergence of IT and OT enhances productivity and safety, rather than compromising them.

3 Research Methods

With the landscape of industrial environments constantly evolving, standardization plays a critical role in ensuring consistent, interoperable, and secure operations. Industrial systems, particularly those that integrate IT and OT, face unique challenges due to their complexity, heterogeneity, and criticality. International standards offer structured methodologies for managing cybersecurity risks across these domains. Their adaptation helps organizations align with best practices, regulatory requirements, and industry expectations. The framework developed in this thesis is built on a combination of globally recognized standards that address technical, organizational, and regulatory dimensions of cybersecurity. As mentioned earlier, there is no universal harmonizing standard that can help organizations manage such environments. However, combining global standards with a harmonizing model is the closest approach organizations can take at this time.

The IEC 62443 series, developed by the International Electrotechnical Commission in collaboration with the International Society of Automation (ISA), is the most comprehensive standard specifically focused on security in industrial automation and control systems. IT addresses the full lifecycle of industrial systems and defines roles for asset owners, system integrators, and product suppliers. The framework is modular and layered, which enables its application across diverse use cases in manufacturing, energy, and critical infrastructure sectors. One of the key strengths of IEC 62443 is its defense-in-depth model, which is specifically tailored to the unique characteristics of OT environments. The standard introduces a classification of security levels based on the risk profile and criticality of the asset, helping organizations prioritize their security investments. It includes detailed technical and process requirements, such as those in IEC 62443-3-3, which defines system-level security requirements, and IEC 62443-2-4, which addresses service provider responsibilities. The standard also aligns well with widely accepted industrial reference architectures like the Purdue model, making it a practical tool for segmenting and securing complex environments of today. IEC 62443 was selected for this thesis due to its domain specificity, wide industry adoption, and comprehensive coverage of lifecycle and technical security requirements. Its design enables the development of secure-by-design industrial systems while maintaining operational continuity and securing the systems of today.

ISO 27001 provides a globally recognized framework for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS).

Although initially developed for traditional IT environments, its structured, risk-based approach and emphasis on governance make it highly relevant for managing security in converged IT/OT ecosystems. The standard prescribes a process-oriented methodology that begins with defining the scope of the ISMS, followed by the identification, assessment, and treatment of risks. It emphasizes the importance of continual improvement, monitoring, and performance evaluation to maintain system resilience over time. ISO 27001 also supports integration with other ISO management systems such as ISO 9001 (quality management) and ISO 31000 (risk management), offering a coherent framework for aligning cybersecurity with broader organizational goals. The implementation of ISO 27001 is guided by a control set detailed in Annex A, which is further elaborated in ISO 27002. These controls span a wide range of security domains, including supplier relationships, access management, incident response, and business continuity. In this thesis, ISO 27001 serves as the foundation for enterprise-wide governance and strategic risk management, completing the technical depth of IEC 62443.

The Network and Information Security Directive (NIS2), adopted by the European Union in 2022, represents a significant regulatory milestone for strengthening cybersecurity across essential and important sectors. It requires that organizations implement both technical and organizational measures to manage cybersecurity risks, with a strong emphasis on supply chain security, vulnerability management, and incident response. The directive applies to a wide range of sectors, including manufacturing, transportation, energy, and digital infrastructure, making it directly relevant to industrial organizations. Its requirements are aligned with both ISO 27001 and IEC 62443, particularly in areas such as governance, risk management, and business continuity. NIS2 mandates board-level accountability for cybersecurity and includes provisions for enforcement, such as audits and penalties for non-compliance. NIS2 was included in this thesis because it formalizes many best practices and transforms them into legal obligations for EU-based entities. Its regulatory nature makes it a critical consideration for any organization operating in or supplying to critical infrastructure sectors within the European Union.

Beyond the three principal standards described above, this thesis incorporates several additional standards and frameworks to enhance the depth and practical relevance of the proposed model. These supplementary documents address key dimensions, including risk management, incident response, industrial safety, third-party assurance, and domain-specific concerns. Their integration into the framework ensures coverage of both strategic and operational areas. One critical addition is ISO 27005, which offers a structured approach to conducting information

security risk assessments. This includes asset identification, threat and vulnerability analysis, and selection of appropriate risk treatment options. It is particularly effective in complex, converged environments where IT and OT must be evaluated together. To support enterprise-wide risk thinking beyond cybersecurity, ISO 31000 provides a comprehensive methodology for integrating risk management into business strategy and operational decision-making. Then, in the domain of incident preparedness and response, ISO 27035, Parts 1 and 2, are referenced. These documents outline how organizations should structure their incident detection, response, and learning processes. They provide guidance on integrating third-party roles into incident workflows, a crucial consideration in industrial systems where vendors, contractors, and support personnel often operate jointly.

To address sector-specific concerns, ISO 27019 is highlighted for its tailored control objectives within the energy sector, extending the ISO 27002 to industrial process environments, which is a valuable addition. ISO 27011, in combination with the telecom-focused perspective, offers relevant parallels for managing networked industrial systems. With the IEC 62443 family itself, various sub-standards provide detailed direction for specific roles and system layers. IEC 62443-2-1 defines cybersecurity program requirements for asset owners, and IEC 62443-2-4 specifies integration and maintenance obligations for service providers. IEC 62443-3-2 supports risk-based design through zone-conduit modelling, and IEC 62443-3-3 prescribes security requirements for industrial automation and control systems. And finally, IEC 62443-4-2 defines technical capabilities expected in industrial control components.

Several architectural models are referenced to see where and how these controls apply. PERA (Purdue Enterprise Reference Architecture) remains the foundation for structuring industrial networks into functional layers. RAMI 4.0 (Reference Architecture Model Industrie 4.0) adds vertical and horizontal interoperability dimensions, especially for smart factories. Meanwhile, the Industrial Internet Reference Architecture (IIRA) provides a modern, layered model to map IT/OT system functionality and stakeholder roles. In addition to standard literature, the thesis draws on academic and applied research accessed through platforms such as IEEE Xplore. These sources include recent contributions to industrial cybersecurity, Zero Trust models in OT, anomaly detection, and risk modelling in ICS and IIoT networks.

These articles add contemporary insight and support the practical relevance of selected standards. Taken together, the supporting standards and references used in this thesis provide a layered, role-oriented, and future-conscious basis for cybersecurity in industrial systems. They

enable integration across lifecycle stages and technical components while supporting strategic governance and regulatory obligations.

4 Foundation and Structure of the Model

To address the multifaceted cybersecurity challenges in converged IT/OT environments effectively, this thesis proposes a structured control model divided into six primary domains: Network, Hardware, Software, Redundancy, Governance and Compliance, and Security. These domains are not arbitrary; they are the result of an analysis of industrial systems architecture, operational understanding, and the layered requirements embedded within relevant cybersecurity standards, while also incorporating the operational knowledge of the writer. As discussed in Chapter 3, this structure is directly derived from the architectural considerations and control requirements outlined in international standards, such as IEC 62443-3-2, ISO/IEC 27001, and the PERA model, which emphasize segmentation, modular control layers, and lifecycle-oriented risk management [5], [17], [18]. This structure aims to make complex cybersecurity concerns more accessible and operationally actionable for businesses, especially in interconnected yet resource-constrained industrial environments.

Industrial environments are composed of diverse and tightly coupled systems, necessitating a modular approach to control and risk management. This perspective is supported by IEC 62443-3-2, which introduces zone and conduit modeling to segment environments based on function and risk, and by ISO/IEC 27001 Annex A, which promotes structured security domains for asset classification, access control, and operational resilience, where security cannot be treated as a monolithic or centralized function [17], [18]. Rather, effective cybersecurity requires the ability to compartmentalize different asset categories and risk zones. By breaking down the cybersecurity approach into six distinct domains, the framework enables a more focused analysis of each system layer or component, the mapping of standard-specific controls for different levels or requirements, a clear assignment of responsibilities across multidisciplinary teams, and ease of communication with both technical and non-technical stakeholders. The modularity aims to reflect how real-world operations are typically structured, with each area having different technical requirements, support functions, and risk profiles. The design choice is further validated by trends noted in the latest reports, highlighting lateral movement, encrypted command-and-control channels, and active directory (AD) manipulation as common post-compromise behaviors best mitigated through domain controls [19].

A key enabler of the six-domain framework is a foundational asset management function that connects these layers and ensures consistency in governance and operational decisions. As emphasized in ISO 27001 and IEC 62443-2-1, accurate and continuously updated asset

inventories are essential for implementing risk-aware control strategies. The interdependencies between components, like network infrastructure support software functions or how hardware failure impacts redundancy, necessitate a central point of visibility and control. Asset management ensures traceability of security requirements, simplifies change management, and enables organizations to understand the criticality of systems in both IT and OT environments. As detailed in Chapters 2 and 3, failing to establish an integrated asset view undermines the ability to ensure the complexity of industrial ecosystems. This gap is being increasingly exploited, with threat actors performing automated scanning of services like RDP, Modbus TCP, and SIP at a rate exceeding 36,000 attempts per second, emphasizing the urgency of proactive asset visibility [19].

The structured breakdown supports both top-down and bottom-up cybersecurity planning. From a top-down view, it facilitates management understanding and prioritization. From a bottom-up angle, it supports engineers and administrators in implementing tangible controls and measuring compliance. The structure also promotes key qualities that are seen as essential to effective and adaptable cybersecurity implementation. First, it offers flexibility, allowing organizations to begin implementing controls in areas where they already possess maturity or where the risks are most critical, supporting pragmatic and prioritized decision-making. Second, the structure ensures traceability, meaning that every control implemented can be clearly linked back to the corresponding requirements from applicable standards, enhancing accountability and auditability. Finally, the model is scalable, as it can accommodate emerging technologies and requirements, such as 5G, AI-driven automation, or zero-trust architecture, by integrating them into the most relevant domain without requiring a complete overhaul of the model. Supporting the need for such modular frameworks, recent research highlights the fragmented nature of governance across IT and OT in industrial domains [20]. It is highlighted that there is a lack of empirical validation and real-world harmonization between IT-focused standards and OT operational requirements [20]. The work points to disjointed security ownership, cultural gaps, and a tendency to rely on compliance-driven practices without a unified risk strategy [20]. Validating the need for a holistic, standard-bridging structure such as one proposed here.

The selected structure is a practical interpretation of best practices derived from international cybersecurity standards, academic literature, and real-world deployment considerations across industrial domains. By combining these diverse sources, the framework accommodates the technical complexity and operational diversity found in converged IT/OT environments. This

approach enhances relevance and facilitates compliance with regulatory expectations, particularly in highly regulated sectors such as energy, manufacturing, and critical infrastructure. The framework's structure allows organizations to align their internal controls with external benchmarks while adapting to their specific technological landscape and maturity level. The framework encourages strategic alignment and operational applicability, ensuring that security efforts are not siloed but are integrated across disciplines and system layers. Ultimately, promoting clarity in role assignments, modular implementation of controls, and comprehensive risk coverage are essential qualities for maintaining security in today's rapidly evolving environments.

5 Environment Model

The implementation of cybersecurity practices across industrial IT/OT environments requires a structured and standards-aligned approach. Building on the foundation laid in earlier chapters, this chapter introduces a detailed control model divided into six domains: Network, Hardware, Software, Redundancy, Governance and Compliance, and Security. Each domain represents a core focus that is essential to securing the complex and interconnected components of modern industrial environments.

The structure of this environment draws from key international standards such as IEC 62443, ISO 27001, ISO 27005, ISO 31000, and the NIS2 Directive. It is further informed by architectural frameworks like PERA, RAMI 4.0, and IIRA, ensuring that both technical and governance aspects are addressed. The chapter highlights references to these standards and models to illustrate how the framework supports traceability, regulatory alignment, and operational resilience.

Table 1 summarizes the main standards and frameworks associated with each domain area discussed in this chapter to aid clarity.

Table 1: Visualization of the key standards and frameworks

Domain	**Key Standards and frameworks referenced**
Network	IEC 62443-3-2, IEC 62443-3-3, PERA, RAMI 4.0, IIRA, Selected academic papers
Hardware	IEC 62443-2-1, IEC 62443-4-2, ISO 27001
Software	IEC 62443-4-1, IEC 62443-4-2, ISO 27001, ISO 27002
Redundancy	IEC 62443-3-3, IEC 62443-2-4, IEC 61850, Academic research
Governance and Compliance	ISO 27001, ISO 27005, ISO 31000, NIS2 Directive, IEC 62443-2-1
Security (Operational Security)	IEC 62443-3-3, IEC 62443-2-1, ISO 27035

5.1 Network Domain: Segmentation, Resilience, and Monitoring

The network domain forms the foundational layer in securing industrial IT/OT environments. In converged systems, networks connect assets across traditional organizational boundaries, bridging operational and enterprise domains. Consequently, network architecture is critical in enabling segmentation, resilience, and monitoring capabilities that support secure operations.

This section builds upon the architectural concepts from PERA, RAMI 4.0, and IIRA models to emphasize structured communication flows, functional zoning, and lifecycle management. It also applies requirements and best practices derived from IEC 62443-3-2 and IEC 62443-3-3, which outline the segmentation, access control, and monitoring principles essential for robust industrial cybersecurity.

The framework discussed here reflects both traditional static designs and emerging approaches such as Software-Defined Networking (SDN), which offers dynamic and programmable control of network security. The section pays particular attention to ensuring network architectures align with security objectives such as system availability, data integrity, and operational continuity.

5.1.1 Network Architecture, Design, Segmentation, and Zoning

Network segmentation and zoning are essential to cybersecurity in OT and industrial networks. Network architecture works as a foundation for securing operations while allowing the adaptability and integration of OT solutions. Standards provide some guidelines for how network architecture in operational environments should be done, but of course, this has to be adapted into practical implementation. Purdue Enterprise Reference Architecture (PERA) is often referred to as the go-to network segmentation architecture in industrial practices [17]. Complementary to PERA, modern reference architectures such as RAMI 4.0 and the Industrial Internet Reference Architecture (IIRA) also provide layered models tailored for Industry 4.0 and industrial internet systems. RAMI 4.0 combines lifecycle, hierarchy, and functional layers to contextualize assets and communication pathways, while IIRA highlights functional domains and stakeholder viewpoints that align with structured segmentation and modular security design [10], [11]. However, as industrial environments evolve and adopt IIoT and remote connectivity, more dynamic and granular models are gaining relevance. Zero Trust Network Architecture (ZTNA) offers a modern complement by introducing identity-based segmentation and continuous verification principles [21]. Especially in converged IT/OT environments, ZTNA supports micro-segmentation that adapts to operational context, enabling more resilient protection against lateral movement across zones [21]. PERA model provides a detailed model for defining security levels within each zone based on the risk and criticality of the assets [22], [23]. The Purdue model offers a hierarchical structure for industrial networks that breaks them down into segments, as the standard proposes. The benefit of the model is that it allows for a structured, layered network model that can have tailored security at each level, restricting access

across layers and protecting critical and more risky OT assets from IT-based threats [17]. Based on ISO 27002, it is recommended that organizations implement strict access control policies, limit communication between network segments, and use secure methods to manage data flow across the security zones [24]. Following the guidance of RAMI 4.0, which introduces structured hierarchy levels—from field devices up to enterprise planning—segmenting industrial networks into such levels supports both operational clarity and security containment. IIRA similarly advocates for isolating communication paths between functional domains to reduce systemic risk [10], [11].

Table 2: Hierarchical levels of the network [5], [10], [11], [21], [23].

Layer	Name	Description
Layer 0	Process Control	Physical processes and field devices that interact directly with the environment.
Layer 1	Basic Control	Localized control systems, such as PLCs and RTUs, that perform automation tasks based on sensor inputs and actuator outputs.
Layer 2	Supervisory Control	Systems like SCADA and DCS provide monitoring, supervisory control, and data acquisition from Layer 1 and Layer 0 devices.
Layer 3	Operations Management	Systems supporting production workflows, manufacturing execution systems, batch management, and quality assurance.
Layer 3.5	Industrial Demilitarized Zone (DMZ)	Secure zone isolating enterprise IT systems from OT networks, hosting jump servers, patch management servers, and data historians.
Layer 3.5	Management	Network security management systems, remote monitoring portals, and industrial cybersecurity tools operating across the IT/OT boundary.
Layers 4 & 5	Enterprise & Cloud Solutions	Business IT systems and external cloud platforms are used for business management, supply chain coordination, and data storage.

Network segmentation should be broken down as in Table 2. There should be layers for all hierarchical levels of the process.

Layer 0—Process control represents the physical process itself. This includes sensors, actuators, and other devices that are directly in touch with physical processes. It is a foundational layer that has to be strictly isolated, with minimal communication to higher layers to protect against interference.

Layer 1—Basic control represents the layer housing controllers and PLCs that execute the core control functions. For example, to spin the mixer, this layer interfaces with the level 0 device, monitors, and manages the physical process. This level must stay isolated from IT-level networks to maintain the integrity of control operations.

Layer 2— Supervisory control houses supervisory systems like SCADA and HMIs. These systems require access to data from control layers but must be secured to avoid exposing lower-level systems to potential threats.

Layer 3— The operations management layer includes systems that support plant operations, such as manufacturing execution systems (MES). Layer 3 works as a bridge between OT and the IT environment; here, housed devices require access to a higher-level IT network and to the OT supervisory network.

Layer 3.5—The Industrial Demilitarized Zone (DMZ) is a controlled buffer zone between OT and IT networks. It is instrumental in filtering data exchange, ensuring that OT devices are protected from IT-originating threats and that only essential data is shared across zones. The DMZ aims to facilitate secure communication between OT and IT, allowing for critical data (like production metrics) to flow to enterprise systems without exposing OT assets to IT network traffic. This isolation layer reduces the risk of lateral movement. This aligns with IIRA's emphasis on defined interfaces between domains and RAMI 4.0’s security-by-design approach, both of which aim to prevent the propagation of threats across layered architectures [10], [11]. Components placed in the DMZ might vary but often include data historians, jump servers, protocol converters, or edge devices. Data historians are used to gather and store OT data for IT applications. This can be analytics, for example. This way, there is no need for IT-OT integration. Jump servers securely manage OT systems by logging in through the DMZ, where access to OT solutions can be carefully controlled and monitored. Protocol converters can translate OT-specific protocols like MODBUS into IT-compatible formats, enabling better

and more secure data exchange across IT and OT systems. Edge can be seen as one kind of protocol converter as well, but the benefit of Edge lies in the computing that can be done before entering enterprise solutions. For example, Edge could generate reports for ERP solutions and deliver them from the analytics gathered locally. Strict access control policies should be deployed to access the DMZ. This is because it acts as an interface to all OT access and information, and malicious access can cause safety risks and lead to significant facility downtime.

Layer 4&5—Enterprise and cloud solutions house systems like ERP and IT applications. These are relevant to local area operations because OT systems often want to be integrated for broader organizational needs. These layers are separated from OT layers, and access to the data on layers 4 and 5 should only pass through the DMZ layer.

While the PERA model works as a basis for network segmentation, it is still important to acknowledge the key elements of network architecture and design. Beyond traditional segmentation models, redundancy and routing design are also integral to maintaining availability in industrial environments. Standards such as IEC 62443-3-3 emphasize system availability and resilience through architectural design, while IEC 61850—commonly used in power systems—supports high-availability communication protocols like PRP (Parallel Redundancy Protocol) and HSR (High-availability Seamless Redundancy) [22], [25]. Additionally, recent literature explores the use of SDN to implement programmable segmentation and adaptive failover. In contrast to static models like PERA, SDN introduces the agility required for dynamic, time-sensitive networks in smart factories, allowing reconfiguration in response to failure or threat without manual intervention. One of these is the ideology of the system under consideration (SUC), which identifies industrial and automation control system assets, security perimeters, and access points in the architecture. SUC ideology works by the demarcation of industrial network boundaries and mapping data flows between enterprise and OT systems. Having a clear understanding of what system we are talking about and what kind of network architecture has to be built around it gives a better chance for good security, architecture, and defining perimeters. Standards require organizations to clearly identify the SUC, including the demarcation of the security parameters and identification of the access points [17].

We also need to identify zones and conduits based on the Purdue model. Zones would be logical groupings of assets based on their security needs, like the ones in the Purdue model, but that

can be extended. Secure conduits also mean secure communication channels between the zones, which could mean implementing firewalls, IT/OT DMZ for secure interaction, and segmenting business IT (levels 4-5) from OT networks (levels 0-3). By industrial standards, organizations are required to group industrial and automation control system assets into zones or conduits based on risk, and it is also said that assets can be grouped into zones that are logically or physically separated from business systems [17]. The same goes for assigning network security level targets. Security level targets define minimum security requirements for each zone. This could mean assigning higher security level targets for critical OT systems and enforcing different security level targets for enterprise, control, and safety networks. The secure level targets are crucial for communicating the level of protection required for each zone and are recommended by the standards to be set for an organization [17].

Risk-based network segmentation falls into the same category as security-level targets; the Purdue model is the basis for network segmentation, but industrial standards recommend risk-based segmentation as well, which would mean separating control networks and implementing security policies based on the risk assessments done on the systems. The recommendation falls under the same security level targets, but it is highlighted that the organization should determine security level targets for each zone based on risk analysis and required protection levels [17]. Suppose a system's risk level differs a lot from the other systems, either by leaving them too exposed or causing the system to be too exposed. In that case, assigning separate network risk mitigation should be considered. An industrial demilitarized zone is one of the most important aspects of keeping hold of the security level targets and zones in the OT network. A DMZ is a buffer zone between IT and OT networks to secure data flow. Its design principle is to allow one-way communication from OT to IT and vice versa, while we can also enforce deep packet inspection firewalls to filter data. While business and industrial automation control system assets should be separated, the standards do not discuss the demilitarized zone. However, it is required to transfer traffic between IT and OT systems, which is common in today’s digital age [17].

The boundaries that we set for our architecture in terms of segmentation and zoning can be either logical boundaries or physical boundaries. Logical boundaries refer to network segmentation done by using VLANs, firewalls, and SDN. Physical boundaries include air-gapped systems, isolated OT infrastructures, and secured physical access points. The design principles clearly define demarcation points between IT and OT networks while ensuring and securing entry and exit points with monitoring systems and using documented access for logical

and physical boundaries. Logical boundaries are highlighted in the industrial standards as they delineate the boundary between the zone or conduit and the rest of the system, and the documentation of each physical access point is recommended for monitoring and data flow security for each zone [17]. In addition to boundary enforcement, modern standards such as IEC 62443-3-3 emphasize the importance of real-time anomaly detection for maintaining system integrity [22]. Network monitoring and intrusion detection have become vital components of the architecture, especially as communication pathways grow in complexity.

AI-driven monitoring approaches—such as Convolutional Neural Networks (CNNs) and Fuzzy Neural Networks (FNNs)—are increasingly used to identify deviations from normal behavior within network traffic [26], [27], [28]. These technologies help detect sophisticated, context-aware threats that may bypass traditional signature-based detection. This monitoring not only supports forensic readiness but also enhances proactive defense against lateral movement and zero-day attacks within segmented industrial networks. While physical and logical boundaries are one thing, so is protecting external connections. This would mean having separate security measures for devices that connect to external networks, like remote access gateways, cloud interfaces, and supplier/vendor access, and they are required to be in a separate zone. This would, in practice, mean the IT/OT DMZ that aims to restrict remote access to pre-defined, monitored channels and use encrypted tunnels with authentication. The standards state that devices that connect via external networks should be grouped into a separate zone [17].

For OT networks, it is also essential that the network stays the same and does not really vary. That is why industrial standards often think that temporarily connected devices should be in different zones. Portable devices such as maintenance laptops and mobile devices introduce security risks and should be isolated from permanent control networks. This would mean creating a quarantine zone for external or temporary devices and enforcing strict access control policies for device connectivity. It is stated that devices that are permitted to make temporary connections should be grouped into a separate zone [17]. The same ideology follows for wireless network segmentation. Wireless devices and networks are inherently more vulnerable to eavesdropping and unauthorized access, requiring a separate security strategy. Design-wise, this would mean assigning wireless devices to dedicated zones separate from wired networks and utilizing firewalls, access control lists, and encryption for wireless communications. The standards state that wireless devices should be placed in one or more zones separate from wired devices [17].

The segmentation of safety-critical systems is also seen as different from the others. Safety-related industrial automation and control system assets shall be grouped into zones that are logically or physically separated from zones with non-safety-related assets. Safety-related systems require a higher level of security due to the consequences of system failure [17]. The safety instrumented systems should be separated from other systems to ensure fail-safe operations. This would mean using dedicated safety instrumented system zones that restrict communication with other networks and implementing redundant safety measures in isolated safety zones.

Documentation of network architecture, segmentation, and zoning is also essential to the success of network infrastructure. System architecture diagrams are one way of showing the overall IT and OT environment and its infrastructure. Network topology diagrams define how assets connect across zones and conduits logically and physically, and security documentation includes risk assessments and compliance reports. If we have to set design principles for documentation, it would be clear documentation, flow diagrams, and records of all security controls. Ensuring clear documentation of network segmentation helps with staying up-to-date with the current setup. Flow diagrams are good for visualizing critical data traffic, and a record of all security controls implemented in each network zone is essential for maintaining security. The organization is required to produce SUC documentation already, as well as system inventory, architecture diagrams, network diagrams, and dataflows that can be used to illustrate industrial and automated control systems [17].

The implementation of the design principles basically involves segmentation and zoning, risk-based zone assignments, industrial demilitarized zones, and security level targets. This should be enough design principles to carry the network architecture a long way. The same ideologies might not have all the necessities for traditional homogenous IT networks, but those principles can be transferred into IT networks. The network architecture requires consistency across the network to be a success, but starting with the listed points is a good start. Segmentation and zoning implementation would basically mean isolating IT and OT networks, separating safety systems, restricting wireless access, and protecting external access. These give organizations a good network segmentation platform to continue, but just the ideology doesn’t build a picture. You still need risk-based understanding and micro-segmentation inside a network, but well-defined network segmentation and zoning reduce some cyber risks and ensure operational resilience.

5.1.2 Perimeter Security and Firewalls

Perimeter security and firewalls play a crucial role in industrial networks, defining the security boundary of industrial networks and the system's security under consideration. Industrial standards require organizations to clearly define their security perimeters and access points, ensuring proper zoning and segmentation to protect against cyber threats [17]. The core of perimeter security is defining the security perimeter. The security perimeter refers to logical or physical boundaries that are set to protect industrial systems from external threats. Basically, it is the list of methodologies that we have applied to the environment to keep it safe. Perimeter security also means clearly identifying and documenting all entry and exit points, using firewalls, intrusion detection/prevention systems, and access control measures, and even implementing segmentation policies between IT and OT networks. As previously stated, the organization should clearly identify the System Under Consideration (SUC), including demarcation of the security perimeters and identification of access points [17].

The exact perimeter security ideology follows the already-stated importance of industrial firewalls and DMZs. Firewalls are network security devices that monitor and control incoming and outgoing traffic based on a given set of rules. This is essential for us because setting security perimeters would mean understanding what type of firewalls we have – network layer firewalls, stateful inspection firewalls, or application layer firewalls. This is essential for industrial environments where we might want to change how the network is handled depending on the SUC. Where DMZs step in is also tied to firewalls. DMZs are built buffer zones between business IT networks (Level 4/5) and industrial control networks (Level 0-3). We need firewalls to create this buffer zone between IT and OT, and be that element that enforces strict access controls and inspection so that direct IT issues do not affect the OT environment. The ideology here is set by the standards that assets shall be grouped into zones that are logically or physically separated from business or enterprise assets, and devices permitted to make external network connections should be grouped into separate zones [17]. Firewalls are often the easiest choice for organizations to secure the perimeter. As stated, firewalls are our secure communication paths, “conduits” connecting and grouping communication channels between zones. A conduit itself is a logical grouping of communication channels between zones. The design principle is that firewalls should be placed at conduit boundaries to inspect and filter traffic while enforcing encryption at the latest, and firewalls are required for the logical or physically separated zones [17].

The firewall rule and policy enforcement are a bit different for OT networks – for critical networks, we should define what traffic is allowed or blocked based on predefined rules the design principles for OT networks could be listed as using a default-deny strategy, which would mean blocking all traffic except explicitly allowed or implementing role-based access control for firewall management, and regularly auditing and updating firewall rules for misconfigurations. This would go in line with the industrial standards regarding the access requirements for network zones and the security level targets that have to be set for industrial and automation control systems [17]. As already stated, the wireless network requires additional points, as it requires a separate security zone from wired devices [17]. Wireless networks increase attack vectors, requiring additional measures. These would include, first of all, matching the requirement of isolating wireless networks from wired control networks, utilizing high-end encryption, Mac filtering, and secure SSID policies, and finally, ensuring that there is a firewall between all wireless and wired communications.

Best practices for perimeter security and firewalls are crucial for maintaining effectiveness. This involves defining security perimeters—specifically entry and exit points—and thoroughly documenting the network. Firewalls should serve as conduits, with zones segmented through firewall-controlled pathways, and DMZs should be implemented to separate IT and OT using deep packet inspection and proxies. Additionally, isolating firewalls for wireless zones is important, along with restricting remote access by creating dedicated zones with strict firewall regulations. These measures contribute to establishing a robust perimeter security and firewall framework. Securing industrial networks is about protecting our employees and processes, necessitating practical steps, although the underlying principles remain straightforward.

5.1.3 Network Access Control (NAC) and Authentication

Network access control and authentication are critical components for industrial cybersecurity. With network access control, we ensure that only authorized devices and users can access the industrial network. For industrial networks, it is essential to control network access, manage credentials, and enforce authentication policies to mitigate cybersecurity risks. It all starts with defining access control policies, which means establishing who is allowed to access and which resources under what conditions. For network security, role-based access control stands for the rules that define which roles are allowed for what resources and under what conditions. It fulfills all the requirements while following least privilege access to limit user permissions, ensuring that security measures are met, and enforcing multi-factor authentication on critical systems is

also recommended. Standards recommend Access control within zones and between accesses, and it is recommended to implement various security countermeasures for industrial environments [17].

Authentication mechanisms for the network are also what is under consideration here. Enforcing strong password policies where passwords must be applied and utilizing smart cards or biometric authentication in high-security areas would be recommended. A small yet still important thing is to understand different authentication methods for systems and humans in network access. Network access authentication could mean device authentication for IoT and industrial endpoints, like MAC filtering, for example. The key takeaway is to understand the threat environment through analysis and include identity verification for access control in the assessment, because with the right authentication, anyone can access the environment [17]. It is also generally recommended to enforce authentication and authorization policies for system access in industrial environments, and this applies to networks [17]. The access control implementation would mean that devices are checked before they can connect to the network. This could mean implementing 802.1X authentication for authorized devices and users in wireless and wired networks and quarantining non-compliant devices that are attempting to use NAC enforcement policies. This means that temporarily connected and unknown devices will not be granted access to critical security zones, and the logical environment will enforce access control mechanisms as required by standards [17].

And finally, remote access and secure authentication are also one thing that needs to be considered with network access controls. Remote access introduces additional security risks, and the environment should be strictly controlled. This would mean the usage of VPNs would be limited with multi-factor authentication, third-party vendor access would be limited to predefined time slots, and session monitoring and logging would be done for remote connections. Remote access is required to be modeled as a separate security zone with its own security requirements, and it is also said that remote access should require strong authentication mechanisms and encryption; therefore, listing it under NAC Lists [17].

5.1.4 Remote Access Security

Remote access introduces significant risks to OT networks if not properly managed. Industrial standards often mandate that remote accesses are treated as a separate zone with its own security requirements, ensuring strict authentication, encryption, and monitoring controls [17]. While the topic has already been discussed in a couple of sectors, it is better to be safe than sorry. As

said, remote access is required to be set into a separate zone, logically or physically separated from the core industrial network, to prevent unauthorized access to primary operations. So here are two takeaways for the design of an OT environment: one is that remote connections should be isolated from control system networks, and the second is that this can be solved by establishing a dedicated remote access security zone, for example, an industrial DMZ.

For remote connections, secure authentication mechanisms to ensure only authorized users can establish remote connections become even more crucial in industrial environments. This could mean implementing multi-factor authentication for all remote connections and enforcing strong password policies with certificate-based authentication. Security measures are demanded to enforce strong authentication and authorization for system access, and remote access should require that, as well as encryption [17]. Data transmitted through remote connections should be encrypted, meaning the usage of VPNs like IPsec and SSL/TLS for remote connections and end-to-end encryption should be enabled for all remote connections. This prevents eavesdropping and tampering with the data packets during transmissions.

For remote connections, role-based access cannot be emphasized enough. Remote users should only be granted access to specific assets necessary to do their job functions. This would mean that if the organization is utilizing multiple third parties, each function only receives access to its own function and assets. Role-based access and the principle of least privileged access ensure minimized risk, improved security, and compliance. To comply with IEC 62443-3-2, all industrial remote access must implement role-based access controls, ensuring that remote users are granted only the minimum necessary permissions required for their task [17]. And as well as the access should be in place, so should monitoring and logging of remote sessions. All remote access sessions should be logged and monitored to detect potential security incidents. This is a preventative method that ensures that we detect anomalies as they occur. In practice, this would mean recording session activities in centralized log management systems and analyzing those remote session logs for anomalies and potential intrusions. Industrial standards require that remote access connections should be monitored and logged for security auditing purposes [17].

The best practices for remote access security lie in separating remote access zones, enforcing multi-factor authentication, encrypting remote connections, monitoring and logging remote sessions, and implementing role-based access controls. Remote access security is a critical component of industrial cybersecurity. The best practice implementations are highly

recommended and also required to comply with the IEC 62443-3-2 standard. By pushing these steps forward, organizations can increase the network's security posture and limit risks from remote connection components.

5.1.5 Intrusion Detection and Prevention Systems

Intrusion detection and prevention systems are critical components of industrial cybersecurity with the aim of helping organizations detect, prevent, and respond to cyber threats. Industrial standards outline requirements for intrusion monitoring, anomaly detection, and automated response mechanisms within industrial networks [17]. Intrusion detection systems monitor network traffic for malicious activity or policy violations, logging and alerting relevant teams when threats are detected. In practice, this would mean deploying network-based intrusion detection systems to monitor traffic between security zones, implementing host-based intrusion detection systems on OT assets, and ensuring continuous monitoring with real-time alerting systems. The standards require a description of the threat environment that affects the SUC, and they require both current and emerging threats, while they also mandate that organizations should leverage threat intelligence services to enhance detection capabilities [17].

The same goes for intrusion prevention systems and automated response. Intrusion prevention systems actively block detected threats based on a set of predefined security rules. Since intrusion prevention systems are a fundamental security countermeasure, intrusion prevention system deployment is mandated as part of an organization's cybersecurity framework under IEC 62443 [17]. This would mean configuring signature-based and behavioral anomaly detection systems, implementing automated responses like isolating infected devices, and integrating the intrusion detection and prevention logs with security information and event management systems. As well as having these systems in place, it is essential to know where they should be deployed. Intrusion detection and prevention systems should be deployed at key network segments, such as conduits between security zones. The design principle is to deploy intrusion prevention systems at external network points and deploy network-based intrusion detection systems at conduit boundaries. While the organization is mandated to group assets into zones or conduits as determined by the risks, they are mandated to ensure there are no breaches [17].

While intrusion detection and prevention systems are there, it's not the only requirement. The systems should be updated with real-time threat intelligence. This is mandated by the standards by understanding the threat environment with both current and emerging threats [17]. In practice, what teams can do is subscribe to information sharing and analysis centers that share

knowledge of various cybersecurity matters, such as threats. There is also ICS-CERT, which specializes in industrial control system threats. An organization can also aim to ensure that systems utilize machine learning-based anomaly detection. Logging and incident response integration are integral for proper intrusion detection and prevention. Logs should be correlated with security events to facilitate incident investigation and also help with incident response. This would mean storing logs in centralized security event management systems and implementing real-time alerting mechanisms. The standards state that security measures should enforce logging and monitoring policies for detecting security breaches [17].

Intrusion detection and prevention systems are essential for protecting industrial networks from cyber threats. We've gone through the deployment of industrial detection systems at network perimeters, utilizing intrusion detection systems for automated threat prevention, integrating threat intelligence sources to process, and implementing centralized logging and security event and information management systems. With this, organizations should be able to align with relevant standards of the field but also improve their security posture and preventative methods for cybersecurity.

5.1.6 Encryption and Secure Communication

Encryption and secure communication in IT and OT environments ensure data confidentiality, integrity, and authenticity. Encryption is a critical way of preventing eavesdropping, data manipulation, and unauthorized access, which is essential in critical infrastructure. Encryption refers to transforming data into an unreadable format without the correct cryptographic key. Secure communication is achieved through cryptographic protocols, access controls, and authentication methods that safeguard network transmissions. In industrial settings, integrating these measures is crucial for preventing data interception and unauthorized access while facilitating secure remote access to industrial systems and safeguarding our industrial environments.

We should start with data encryption at rest and in transit. Data encryption while in transit and at rest is required by industrial standards, but is also recommended for data protection [22], [24]. Data at rest encryption in industrial environments would mean encrypting SCADA logs, historical process data, and database records, and utilizing the AES-256 encryption standard for that. It would also mean applying disk encryption for industrial endpoints where applicable. Data in transit would mean utilizing secure communication paths between industrial control systems, from IT environments to OT environments and vice versa. Ensuring that data

encryption is applied during rest and transit is essential for data security. While we are talking about networks, it would mean focusing on encrypted protocols to replace legacy communication methods. For daily life, this could mean replacing Telnet with SSH or FTP with SFTP or changing DNS queries to encrypted DNS queries. Recommendations are clear with secure protocols for network transactions, and the aim is to secure protocols as well as remote access communications [22], [24].

Securing industrial protocols might become trickier, but options are available for most use cases. For example, OPC UA utilizes TLS-based authentication for PLC and SCADA communication, and the same goes with secure Modbus, which is encrypted but still seen as old in the field. There is also MQTTS communication instead of MQTT, and DNP3-SA added cryptographic authentication to DNP3-based SCADA systems. Options are available, industrial standards often require that control system communication protocols be encrypted, and security standards recommend secure authentication methods [24], [29]. The same goes for virtual private networks (VPNs) and secure tunneling methods. Encryption is also required for industrial environments and is strongly advised for general network access [24], [29]. Encrypting network traffic for remote and site-to-site communications is essential for security. It can be done by implementing SSL VPNs, SSH Tunnels, and IPsec VPNs.

Certificate-based authentication and public key infrastructure offer security through digital certifications and cryptographic key pairs; they aim to ensure trust between devices, users, and systems. Public key infrastructure works with certificates issued by a certificate authority, verifying the legitimacy of entities in a networked environment. Certificate-based authentication utilizes public key infrastructure to ensure that only trusted entities can access systems and data. Encrypting the data in transit eliminates the weakness of traditional password-based authentication and reduces the risk of credential and data theft. Challenges in the industrial environment might be with resource-constrained devices and ensuring security. Industrial standards require certificate-based authentication for secure communications, while also secure IT practices recommend public key infrastructure for managing cryptographic certificates [22]. With Public Key Infrastructure, we also need to ensure that encryption key management and best practices are being followed. This would mean ensuring secure storage, rotation, and distribution of cryptographic keys, not only for certificates. This could mean the usage of hardware security modules, regular key rotation, lifecycle management, and role-based access controls for key usage. While certificate-based authentication is required, so is secure

key management in industrial control system environments alongside the recommended key management policies for cryptographic security [22], [24].

While protocols handle a lot of traffic encryption, we also need to ensure that wireless communications are secure, and that is done by staying up to date on wireless security trends and encrypting Wi-Fi and RF communications to prevent eavesdropping. This could mean utilizing WPA3 instead of WPA2, even though they can be cracked, but WPA3 requires more effort, or utilizing the restriction of MAC filtering to our advantage. It is also recommended to use RF shielding to prevent interference and jamming attacks. Suppose wireless communication is required in OT networks by the systems. In that case, it is also necessary to protect those wireless networks with similar efforts, and it is also advised to use strong wireless encryption standards like WPA2 and WPA3 [22], [24].

Secure cloud and edge communications are the same as encrypting remote and site-to-site traffic and encrypting data transfers between industrial control systems, IoT devices, and cloud services. End-to-end encryption would do this between cloud-stored data and data sent to the cloud, utilizing the zero-trust network access principles by enforcing encryption and authentication before accessing systems. One solution to this would be secure edge gateways that ensure encrypted communication between cloud and enterprise services and industrial networks. If there are cloud-based industrial control system applications, the requirement for encryption is forced, but also, generally, data encryption for cloud environments is recommended [24], [29].

The implementation of encryption and secure communications should be quite straightforward. Finding out the use cases for your environment and pointing out the best practices is often an intricate process with newer technologies, as long as you have the hardware to support the outlining. This could mean listing Secure remote access methods – Like VPN (IPsec, SSL) with Zero Trust network access, Cloud and IoT security – Usage only with TLS and secure protocols, Wireless Network Security should be applied with WPA3 and MAC filtering, ICS Protocol security should only include secure protocols when possible. As long as those topics are listed as a general organizational policy, the applicability should follow. Encryption and secure communication are vital sources for protecting IT and OT networks from cyber threats, ensuring data integrity, and securing industrial communication channels. By applying the previously discussed strategies, organizations can more effectively demonstrate their data integrity and theft prevention efforts.

5.1.7 Network Monitoring and Threat Detection

Network monitoring and threat detection are fundamental cybersecurity measures in industrial control systems to detect anomalies, identify threats, and prevent cyber incidents before they cause operational disruptions. For industrial networks, standards outline requirements for continuous monitoring, threat intelligence, and ensuring real-time responses [17]. Network monitoring, in our case, would mean continuous monitoring, keeping up with network traffic, logs, and activities to detect anomalies in industrial network environments. By design, this would mean deploying security information and event management systems, using industrial intrusion detection systems to monitor specific traffic for our industrial networks, and performing a baseline network behavior analysis to further help detect anomalies. As the standard requires organizations to stay up to date on current and emerging threats, the requirement falls under continuous monitoring [17].

Anomaly and threat detection is a great part of ensuring that you stay up to date on upcoming services and standards. It also requires organizations to stay on top of this. It is stated that organizations should leverage threat intelligence services to enhance detection capabilities [17]. This entails recognizing network activities that are suspicious or malicious, differing from normal behavior. This would mean implementing AI-driven threat detection to identify possible zero-day attacks on organizations' networks while correlating network anomalies with known threat intelligence feeds. While organizations are collecting this data, it is essential to have correlating network logs from firewalls, intrusion detection and protection services, and endpoint security tools. As stated earlier, this would mean centralizing logs to SIEM platforms for real-time analysis and utilizing automated alerts for high-priority security incidents. Standards require organization security measures to enforce logging and monitoring policies for detecting security breaches across zones [17].

Incident response integration with network monitoring and anomaly detection is essential for rapid mitigation of incidents. This would mean automating incident response workflows for detected threats within the organization and ensuring that forensic data retention also supports post-incident investigations. Incident response and automated threat mitigation are mandated under IEC 62443-3-2, requiring organizations to integrate real-time security monitoring with structured mitigation workflows to minimize industrial security risks [17]. The best practices for network monitoring and threat detection ensure that the organization stays on top of its cybersecurity. While standards mandate continuous monitoring, threat intelligence integration,

and automated response mechanisms to detect and mitigate threats, it should also be in the organization's best interest to try to act on incidents as soon as possible. By implementing effective monitoring strategies, organizations can gain enhanced visibility into their environments, allowing them to identify anomalies and strengthen their cybersecurity posture.

5.1.8 Network Redundancy and High Availability

Network redundancy and high availability are important for ensuring continuous operations and resilience against system failures in industrial networks. Standards often outline the requirement for redundancy planning, failover mechanisms, and resilience strategies, not only for operational safety but also for operational continuity in industrial networks [17], [30]. While business continuity standards and ISO 27001 provide general perspectives on IT availability and resilience, this chapter focuses more on OT environments [18], [30].

Network redundancy involves deploying multiple network paths to prevent a single point of failure. Industrial standards discuss the risk of network failures and the need for maintaining industrial process continuity, but do not hand out simple recommendations [17]. If a network failure is something that stalls the industrial process, it is highly recommended to include redundancy in the architecture. Business continuity standards recommend that organizations identify risks and opportunities that can affect their ability to deliver products and services during disruptive incidents [30]. While redundancy would mean implementing multiple network pathways for critical segments and hot-standby links with automatic failover mechanisms, ring topologies, or mesh networking, it is highly recommended to evaluate the risks of network downtime by conducting a business impact analysis or defining high availability requirements based on the risk exposure to the business. Regardless, the availability of IT/OT networks should be assessed and prioritized based on risk levels. ISO 27001 mandates organizations to set disaster recovery policies with recovery time objectives and recovery point objectives for critical systems – if that is seen in the risk management as a network, then it should be applied. Disaster recovery plans must include actions and regular testing for critical system availability [18].

Industrial standards highlight the requirement for automatic recovery and failover mechanisms. With the network, this would mean the utilization of the spanning tree protocol or the rapid spanning tree protocol to ensure that network loops do not cause failures. But it would also mean deploying multi-homed industrial gateways and implementing automatic switching to backup links upon detecting network failure. To comply with IEC 62443-3-2, organizations are

required to implement failover mechanisms and automatic recovery solutions, ensuring that network disruptions do not impact industrial operations [17]. Similar points are raised with business continuity standards, with the statement that organizations should determine solutions for ensuring business continuity by defining resilience, recovery, and redundancy requirements for critical operations [30]. This would mean setting minimum viable uptime requirements for industrial networks and implementing failover mechanisms to avoid downtime in the first place. High availability requirements are also pointed out in the ISO 27001 standard, with high availability assurance for critical network resources to remain accessible even in the event of cyber incidents or failures [24]. The fault tolerance is highlighted in ensuring network resilience through backup and redundancy. This would mean establishing active-active failovers for network components in OT environments and implementing an automated switchover. Organizations are mandated to establish information security continuity measures to ensure operational resilience [18].

Redundant communication channels are one point that is pointed out in both industrial standards and business continuity standards. Industrial networks should use multiple independent communication channels to ensure availability. This would mean implementing wired and wireless communication paths and utilizing multiple internet providers. To mitigate risks, industrial standards recommend this, but business continuity mandates communication pathway redundancy to maintain operational continuity [17], [30].

However, Industrial standards are the only ones that require monitoring and fault detection for systems, including networks. IEC 62443-3-2 mandates that continuous monitoring and fault detection systems be integrated into industrial networks [17]. This means that the network should have proactive monitoring systems to detect faults and automatically respond to failures. Being implemented would mean real-time monitoring tools to monitor network pathways and failover systems, and predictive maintenance for network components to avoid failures in the first place. Network redundancy and high availability ensure uninterrupted operations for the organization, and it is recommended to implement redundant network paths, failover automation, multiple communication channels, high availability resources, and continuous monitoring for a more resilient environment.

5.1.9 Wireless and IoT security

Wireless and IoT security is highlighted for protecting industrial networks from unauthorized access, data breaches, and cyber threats. Industrial wireless devices and IoT solutions increase

attack surfaces, making it essential to implement network segmentation, encryption, authentication, and monitoring to secure these systems. Industrial standards provide good security guidelines for wireless and IoT devices, focusing on network zoning, device isolation, and security controls, but also ISO 27002 and ISO 27035-1 support this [17], [24], [31].

Suppose we begin with wireless device isolation and segmentation. Wireless networks must be logically or physically separated from wired networks to reduce attack exposure and protect information in systems and applications [17], [24]. This would mean zoning wireless networks in separate security zones and wireless access points to be treated as conduits and secured with firewalls. The zoning must include security controls to separate wireless and wired devices. While zoning gives us a good head start on static network security, it surely does not ensure it. It is also stated that devices temporarily connected to the SUC should be grouped into separate zones [17]. This would mean that wireless connections have to be in separate zones and that connections not included in the critical OT system infrastructure should be zoned differently. This could mean zoning additional features like tablets or IoT sensors to a different zone and enforcing security requirements on them as well. This could mean unique authentication credentials, role-based access control, or restricting protocols in a specific network zone. This is also supported by the ISO 27002 standard, which states that networks must be managed and controlled to prevent unauthorized access [24]. ISO standards recommend mitigating the risks by implementing a zero-trust network policy so that every device is treated as an external connection before authentication [24].

Wireless encryption and secure communication in general over wireless networks are recommended to be encrypted, which also applies to IoT communications. Encryption is done to prevent eavesdropping, data manipulation, and man-in-the-middle attacks. ISO 27002 recommends additional security measures for wireless communications, highlighting encryption in general, but Industrial standards require wireless encryption to mitigate the added risks of wireless networks [17], [24]. The same goes for remote access tools to wireless and IoT devices. The connections to wireless and IoT devices must be encrypted and secured with multi-factor authentication. As required by IEC 62443-3-2 and ISO 27002, remote connections to industrial IoT and wireless networks must be protected using MFA and encryption to prevent unauthorized access and data interception.

Finally, wireless must be monitored, as well as any other network, with additional security measures due to increased exposure. Wireless and IoT networks must be monitored

continuously for atleast unauthorized access, rogue access points, and security anomalies. This would mean deploying wireless intrusion detection systems to detect rogue access points and log all network traffic from IoT devices for real-time threat detection. It is stated that wireless networks must implement additional security measures due to their increased exposure to threats, and intrusion detection systems should be implemented to identify and respond to network-based threats, including unauthorized access points [17], [24].

Wireless network security and IoT security become a critical component of industrial network cybersecurity as they expand the threat landscape exponentially, with their broadcast nature, lack of physical boundaries, and varying security postures of connected devices. Standards mandate wireless device isolation, access controls, encryption, secure remote access, and continuous monitoring to protect industrial environments from cyber threats, and those are the best practices. A sound mitigation of cybersecurity risks with wireless network connections shrinks organizations' threat landscape to a minimum. Organizations must implement layered security controls that address vulnerabilities at the network, device, and application levels to effectively mitigate the risks associated with wireless. That can mean implementing zero trust architecture, adaptive authentication and role-based access controls, wireless network hardening and encryption enforcement, anomaly detection, and strict network access controls with device whitelisting. Securing wireless ensures industrial control system resilience while enabling the benefits of wireless devices.

5.1.10 Industrial Network Security

Industrial network security focuses on protecting our critical control systems, industrial automation environments, and OT networks from cyber threats, unauthorized access, and operational disruptions. Traditional IT environments must ensure confidentiality, integrity, and availability, whereas in industrial networks, we must focus first on maintaining the availability and integrity of systems and processes, with confidentiality being less critical. Reliability over the processes is of new importance. While protecting the environment, we must ensure real-time communications, deterministic communication, and resilience. Industrial standards provide a framework for risk assessment, security zoning, and countermeasures to help organizations mitigate cyber threats, reduce vulnerabilities, and establish a strong security posture regardless of the environment [17].

The first step for industrial networks is risk-based security zoning and network segmentation. Industrial networks must be segmented into security zones based on risk, asset criticality, and

communication needs. The design principle requires the usage of zones and conduits to enforce security boundaries between IT and OT systems, while it also means isolating critical assets to prevent lateral movement of cyber threats and to ensure process continuation. Standards require zoning to be based on a formalized cyber risk assessment to determine the security requirements of each segment, while also requiring organizations to partition the system into zones and conduits to control access and reduce the risk of security breaches [17]. Zoning is the first step in defining network perimeter security, and securing boundaries is where zoning starts. Industrial networks must have secure boundaries, ensuring that external traffic does not directly interact with industrial control or OT systems. The organization must clearly define security perimeters and access points for industrial networks while ensuring communications, if necessary [17]. This would mean deploying firewalls, demilitarized zones, and intrusion detection/prevention systems to protect industrial networks with the restriction of external access to OT or industrial control systems.

While we must ensure the availability of industrial networks as our priority, it does not mean that security is dismissed. Communications between industrial devices must be secured to prevent tampering, spoofing, and unauthorized interception. While not possible with all systems, it should still be an aim. The usage of cryptographic measures is recommended for industrial systems alongside other security controls to prevent unauthorized access and tampering [22]. The system should be able to provide the capability to protect the integrity and confidentiality of transmitted data [29]. The standard for industrial automation control systems mandates that industrial networks utilize secure protocols for communication between devices to mitigate cybersecurity risks, yet it is not always applicable [22]. With encryption, we need to be able to apply strict access control measures for users, devices, and applications that interact with industrial networks. In practice, this is best applied with role-based access control and the least privilege principle for network users. Strict access controls would also mean implementing multi-factor authentication for remote access to industrial networks. Access to industrial networks should be limited according to established security zones, and access control policies need to be enforced, with remote access requiring multi-factor authentication for network entry [17], [29].

Industrial networks also can't avoid monitoring. The organization should implement real-time security monitoring and event logging to detect and respond to cybersecurity threats in industrial networks [17], [22]. Industrial networks should be no exception; they must have real-time monitoring, anomaly detection, and threat intelligence capabilities to stay up to date on

security incidents. This means deploying security information and event management solutions for log analysis and correlation, as well as implementing intrusion detection systems and industrial threat intelligence platforms to detect abnormal activity. While monitoring is essential, the organization should also act to minimize exposure to security vulnerabilities. This could mean disabling unused services and ports to reduce attack surfaces and setting up secure baseline configurations for all industrial network assets, including industrial switches, access points, and other network devices. Industrial standards mandate that network assets be configured with a security baseline that minimizes vulnerability exposure [17].

Securing an industrial network requires a layered defense approach, but also needs a predefined incident response plan to ensure rapid containment of cyber threats. Industrial standards require an assessment to evaluate the efficacy of countermeasures aimed at minimizing the likelihood or consequences of incidents. This includes automated network segmentation and failover mechanisms to ensure network availability during such occurrences. In practice, this would mean defining escalation procedures for industrial security incidents, automated containment actions, and conducting regular tabletop exercises and penetration testing to validate response effectiveness. By implementing the layers through segmentation, perimeter security, access controls, monitoring, and secure configuration, the organization should be able to ensure resilience against cyber threats and unauthorized access. A proactive, defense-in-depth strategy gives an organization a good overall security posture while mitigating risks efficiently in an increasingly connected industrial environment.

5.1.11 Compliance and Regulatory Requirements for Network Security

Industrial networks are required to adhere to compliance and regulatory requirements to ensure that security aligns with international, national, and industry-specific cybersecurity frameworks. The requirements dictate how the organization manages risk assessment, zoning and segmentation, incident response, and continuous monitoring. To have good IT-OT compliance and governance, we must focus on the security mandates for industrial control systems, OT in general, and the convergence of IT and OT environments.

Compliance and governance start with establishing baselines. Cybersecurity requirements specification is one document for all applicable security regulations, countermeasures, and compliance requirements based on possibly government-mandated regulations like NIS2, industry-specific guidelines, or industrial cybersecurity standards. Any relevant cybersecurity regulatory requirements that apply to the SUC should be included in the cybersecurity

requirement specification, and the organization must be able to identify applicable legislative, regulatory, and contractual requirements related to information security [17], [18]. In the cybersecurity requirement specification, the organization must also use a rational approach to prioritize security controls and network segmentation strategies based on legal and regulatory mandates. This would mean a risk-based approach to the topic. Conducting a formal cybersecurity risk assessment to determine the required security levels for network zones would be preferred. Ensuring that security zoning aligns with compliance requirements to enforce access control and segmentation policies, and maintaining documentation for audits and regulatory reviews to demonstrate compliance with cybersecurity frameworks. Standards require the security level for each zone or conduit to be determined based on a detailed cybersecurity risk assessment, and organizations are mandated to apply a structured approach to managing cybersecurity risks, incorporating compliance obligations into risk assessments [17], [32].

While we have already opened the door for discussion about network segmentation and access control, industrial network security compliance often requires segmentation policies that align with regulatory security levels and access controls that come with it. To tackle this, organizations should aim to segregate business IT and OT assets into separate network zones with distinct security policies and limit communication between network segments based on risk classification and regulatory requirements. Implementing network access control to enforce role-based policies and restrict unauthorized devices in the network is highly recommended. A grouping of industrial automation and control systems into security zones and conduits based on risk and compliance requirements is recommended by the standards, but also establishing access control policies to manage access to networks and systems based on business and security requirements is mandated [17], [24].

With network governance and compliance, there also come regulatory requirements for incident response and monitoring. The organizations are mandated to ensure compliance with incident response to facilitate fast recovery, continuous monitoring for visibility, and logging for traceability and accountability. Practically, this means implementing security information and event management solutions to support real-time network monitoring, ensuring network logging mechanisms to support forensic investigation and regulatory audits in the environment, and making sure that incident response plans align with compliance mandates, including the NIS2 directive requirements or other regulatory requirements for significant cybersecurity incidents. Industrial and security standards require that organizations implement continuous

monitoring and logging for compliance with security policies and regulatory requirements. Still, the establishment of an incident response framework is also necessary to align with industrial, incident, and industry standards [17], [33].

To initially obtain and maintain regulatory compliance, organizations must establish a process of regular audits, governance policies, and security assessments. This means conducting network security audits to ensure potential compliance with IEC 62443 and ISO 27001 controls and maintaining audit logs for regulatory review, ensuring traceability of security events. Standard documentation of security policies and governance frameworks is often an easy way to demonstrate compliance with legal mandates as well. To comply with standards, organizations must first define their tolerable risk level and ensure alignment with regulatory cybersecurity requirements, and then conduct compliance audits to ensure that the cybersecurity measures align with business, business continuity, and disaster recovery policies and efforts [17], [30]. The process of auditing and reviewing the environment ensures continuous improvement and that efforts are made towards a safer tomorrow.

5.2 Hardware Domain: Securing Physical Assets and Infrastructure

The hardware domain focuses on the physical components and embedded devices that constitute industrial IT/OT environments. In critical operations, hardware assets such as controllers, networking devices, servers, and field equipment form the backbone of system functionality and resilience. Securing these assets is fundamental to ensuring the integrity and availability of industrial operations.

This section leverages standards such as IEC 62443-2-1 and IEC 62443-4-2 to define requirements for asset management, device hardening, and secure component design. It also incorporates elements from ISO 27001 related to hardware asset control and risk treatment. The framework emphasizes principles such as hardware inventory, secure configuration, role-based physical access control, and lifecycle management to mitigate vulnerabilities associated with industrial hardware.

By addressing hardware at the device and system levels, this domain supports a broader objective of achieving defense-in-depth strategies throughout the industrial environment.

5.2.1 Hardware Asset Inventory

Hardware asset inventory is a crucial part of any environment. By having a good asset inventory, you ensure visibility, management, and security of all hardware assets within an organization while supporting operational continuity, compliance, and risk management at the same time. It is often considered to be one of the cornerstones of good IT management. Everything starts with an overview—where are we now? A comprehensive, up-to-date list of all hardware assets used in IT and OT environments should be covered. It should include detailed information about each asset to the point that it is identifiable in the mass. Providing a good background of the assets provides good visibility and reduces the risk of unmanaged or unauthorized hardware on the operational grounds. An up-to-date inventory also helps with maintenance, lifecycle management, and security by ensuring all assets are accounted for and monitored.

We can build a good base for a hardware asset inventory by narrowing it down to inventory scope coverage and asset attributes. Asset attributes should be a detailed record of information about each hardware asset for accurate tracking and management [24]. They should have at least details like the asset name and description, Manufacturer, Model and serial number, location, Asset owner and custodian, date of acquisition, and warranty expiration. Detailed documentation of each asset might seem like a lot to do, but it will significantly help lifecycle management. This could also physically mean using barcodes or QR codes on devices to tag devices and streamline inventory management. Inventory scope and coverage matter as much as the details themselves. Defining the scope of inventory to include required IT and OT hardware such as servers, PLCs, SCADA systems, routers, sensors, and field devices is essential. Identifying and listing all the network devices, as well as including portable devices like laptops that are used in operational processes, is essential. Starting small and building up to a complete list of good asset inventory builds for a good foundation on the operational grounds. Asset identification and classification are a part of modern cybersecurity management and should be considered while creating and maintaining a hardware asset inventory [23], [24].

Using software tools to automate asset tracking, monitoring, and reporting is recommended. Deploying CMDB tools for IT and OT management is recommended. The environment should be able to handle OT and IT assets, as they vary quite a bit from the traditional CMDB toolset usage environment. Using the asset discovery tools efficiently to identify devices connected to the network automatically is recommended, but it also clears out the clutter and possible

duplicate entries in the database [24]. The tool should be capable of manual inserts, as many of the assets in the OT might never be network-connected in legacy environments, but tracking those devices is as crucial as network-connected ones. Utilizing the tools to the fullest leverages automated tools to maintain, monitor, and upkeep an asset database [24]. Proper lifecycle management processes require integrating hardware asset inventory with lifecycle management. This process should include procurement, maintenance, and decommissioning of the hardware at hand. In lifecycle management, you should be able to track and schedule replacements and upgrades proactively. You should also be able to plan for the secure disposal of obsolete devices, which includes data wiping and product recycling. The lifecycle management of industrial assets is as important as any IT asset in addressing operational and cybersecurity risks in daily operations [23].

Regular audits of the hardware asset inventory can help clear up removed devices and inventory items that do not belong there. Regular audits also ensure that the inventory is accurate and current [24]. The audit should focus on the automated tools' performance, whether they are detecting new or removed devices in the network and updating the inventory accordingly. Scheduling inventory audits at the locations helps to verify physical and digital records, and planning these, for example, quarterly, could make a difference. Regular reviews and conversations around hardware asset inventory improve inventory accuracy and upkeep, but can also improve the chances of demonstrating compliance with regulatory and industry standards [18], [22], [24]. Providing a good record of audits to meet the requirements of regulations is always better. Utilizing the inventory data to generate reports for management and external auditors helps to point out that the organization is upholding the requirements for a specific standard. Detailed asset inventories are required for compliance with information security management, but they are also needed as part of system integrity measures for industrial control systems [22].

Asset information also needs to be integrated into incident response. What assets are affected, and what are their dependencies? We can utilize our hardware asset inventory to quickly locate and isolate compromised hardware during a cybersecurity incident. Still, it can also help us identify replacement devices to minimize downtime during hardware failures. Asset visibility is crucial when managing security incidents, but it will also help the organization manage its environment [34]. While this information can be essential, ensuring proper security and access controls for the inventory data to prevent unauthorized access is vital. Personnel should only have access based on the principle of least privilege, and data should be encrypted. The

inventory data is sensitive information as it covers the IT ground, revealing potential vulnerabilities in the environment. Securing inventory data as a part of broader information security measures is recommended [24].

5.2.2 Hardware Lifecycle Management

Hardware lifecycle management focuses on effectively managing the lifecycle of IT and OT assets from procurement to disposal. Lifecycle management ensures operational efficiency, cost-effectiveness, and security while minimizing risks associated with outdated or poorly maintained equipment. It involves tracking and managing hardware assets through their lifecycle stages: procurement, deployment, operation, maintenance, and decommissioning. We must ensure that hardware remains operational and secure throughout its lifecycle at industrial facilities. This way, we can reduce unplanned downtime and associated risks, especially in the OT environments. Proper lifecycle management supports the factory's budgeting, planning, and regulatory compliance. Lifecycle planning can educate businesses on reasonable, knowledgeable risks instead of making decisions without proper knowledge.

The hardware lifecycle management can be broken down into five core stages: procurement, deployment, operation, maintenance, decommissioning, and disposal. Procurement is selecting and acquiring the hardware assets that meet organizational and operational needs. OT hardware must be defined to ensure compatibility with existing systems on factory grounds. Vendor evaluation for reliability, support, and compliance with standards like IEC62443 must also be evaluated [24], [35]. Rather than having a standard list of products that must fit the environment, we should investigate the required features in the environment and compare providers accordingly. After that, the business unit can decide which road to take. Deployment means configuring and integrating the hardware into the IT/OT environment or factories. The process should outline practicalities like secure installation methods, such as device hardening, which can mean, for example, disabling unused ports and protocols in the equipment. Hardening the environment, especially in IT/OT, can be seen as crucial; even though it makes the organization a bit clumsier, it allows for better change management and control over the environment, which is required in IT/OT environments. The deployment process also stands as a vital inventory function, and separate deployment practices, which include configuration and access control, are advised [24]. Verifying that all new hardware is inventoried and labeled before deployment is crucial for inventory upkeep.

A similar simple process is an operation that outlines hardware maintenance in daily operations to ensure optimal performance and security. Practical examples of this could be real-time monitoring to track performance metrics like CPU utilization and temperature usage. This way, by spotting the anomalies, we can remotely tell if something is out of line, and by setting alerts on the monitoring, we can prevent possible hardware failure beforehand. Monitoring and maintaining the integrity of operational assets is recommended [22]. Maintenance goes hand in hand with the operation phase, conducting preventive and corrective maintenance to extend hardware longevity and reliability in the environment. This could mean scheduling maintenance checks for critical OT systems like PCLs and SCADA hardware or replacing worn-out components such as fans or power supplies to prevent further failures. Preventive maintenance is recommended for critical systems to ensure availability [24]. Finally, decommissioning and disposal would be a phase of safely retiring outdated or end-of-life hardware to prevent future security risks and environmental hazards. Performing secure data wiping or physical destruction of storage devices to avoid data leaks would be preferred, and partnering up with certified e-waste recycling companies to dispose of hardware sustainably. Proper disposal methods ensure that no sensitive information is leaked, and compliance is assured, but securely decommissioning industrial hardware is recommended through safety measures [23], [24].

As we've described the stages of hardware in hardware lifecycle management, we've also noticed that key processes are needed in the mix. We can break that down into three methods: Asset tracking, Risk and Obsolescence management, and integration with redundancy strategies. Asset tracking means continuously monitoring hardware throughout its lifecycle to ensure accurate inventory and effective management of the hardware. This could mean anything from asset management software to tracking hardware, including deployment status, location, and lifecycle stage. The updates to inventory should be made by monitoring when the hardware is repaired, replaced, or retired. Asset tracking helps to maintain the organization's cybersecurity readiness [23]. Risk and obsolescence management is also a crucial part of cybersecurity, which builds upon managing and being knowledgeable about the risks related to hardware and obsolete hardware [24]. This could mean developing a hardware refresh plan to replace devices nearing end-of-life or end-of-support. It can also mean monitoring vendor updates for firmware and security patches to avoid vulnerabilities as they come. Integrating hardware lifecycle management with redundancy strategies is another crucial part of lifecycle planning [22]. In practice, this would mean procuring redundant servers and network devices

to minimize single points of failure and testing failover systems as a part of hardware lifecycle management.

Security considerations across the lifecycle should be a part of daily operations. Organizations should validate hardware for compliance with security certifications like IEC 62443 during procurement and assess supply chain risks [23]. In operations, regular vulnerability scanning procedures and penetration tests are implemented to ensure the environment's integrity. Ensuring secure configuration during firmware updates is just a part of the security mindset of daily operations [23]. Disposal would mean applying secure wiping protocols or physically destroying sensitive components while documenting decommissioning processes to maintain audit trails. Time after time, this is mentioned, but continuous improvement and feedback should be integrated into the processes. Utilizing input from hardware performance and incidents to refine lifecycle management practices should be considered. Analyzing hardware failure reports to improve future procurement decisions and incorporating lessons learned from decommissioning audits to enhance disposal procedures is recommended. Carrying out continuous improvement and feedback processes through the hardware lifecycle management would be beneficial regardless of the environment [34].

5.2.3 Physical Security Controls for Hardware

Physical security controls for hardware ensure that the IT and OT assets are protected against unauthorized physical access, tampering, theft, or environmental hazards. In industrial environments, hardware often supports essential processes, and physical security is a cornerstone of a robust security and safety framework. With physical security, we need to define measures and mechanisms to protect hardware assets from physical threats, which ensures their integrity, availability, and security. This is the cornerstone of preventing unauthorized access to PLCs at the factory, SCADA servers, and network equipment. Reducing risks associated with hardware theft, sabotage, or environmental damage can help businesses ensure a return on investment.

Physical security controls are broken down into four core components: Access control mechanisms, surveillance systems, physical barriers, and environmental protection. Access control mechanisms restrict and monitor access to critical hardware areas. This could mean using badge readers, biometric systems, or keycard access to server rooms or control centers to prevent unauthorized access. Implementing mantraps or airlock systems to prevent tailgating into secure areas is also recommended [24]. Implementing physical access control mechanisms

would be beneficial if we discuss environments that might cause operational disruptions or risk employee safety if not used correctly [23]. Surveillance systems can monitor hardware environments to deter unauthorized access and document incidents. This could mean installing CCTV cameras with remote monitoring capabilities in possible control rooms, data rooms, and warehouses. Integrating cameras with motion detection and alert systems can maintain monitoring and logging for access [24].

Physical barriers involve employing structural measures to protect hardware from unauthorized access, which is advised [24]. This could mean practically locking network cabinets and control panels with padlocks or electronic locks, or installing fences and gates around outdoor equipment. Environmental protection protects hardware from ecological hazards like temperature fluctuations, humidity, and power surges. Utilizing industrial-grade enclosures to shield hardware from dust, moisture, or vibrations is required in industrial environments. Installing temperature and humidity sensors in server rooms can help detect environmental anomalies, and installing uninterruptible power supplies can prevent hardware damage during power outages. Managing environmental controls ensures system integrity in industrial environments and the longevity of the systems at hand [22].

Monitoring systems help to detect and respond to physical security incidents in real time [24]. Like any detection and monitoring system in cybersecurity, organizations should also include similar detection systems for physical security. Organizations can implement tamper-evident seals on hardware enclosures to detect unauthorized access attempts or alarm systems that trigger alerts for unauthorized access or when the environmental threshold is breached. This could be set to something like high temperatures. Security training is crucial for employees and contractors to follow physical security and safety guidance around the factory and conduct regular security drills with personnel [18]. Hence, they know how to respond when physical security is breached and restrict access to sensitive areas to authorized personnel only based on role-based access policies.

Integrating physical security with cybersecurity is crucial to bringing total success to the security plan. Combining physical and cybersecurity measures for a unified approach can help mitigate physical threats and protect hardware. Our electronic equipment can be analyzed through minor physical breaches. The stages that the computer is in can be explored from the power output. Meetings can be heard through the walls [36]. Integrating physical security with cybersecurity is recommended [35]. This can be done by integrating access control logs into

security information and event management (SIEM) systems. Surveillance systems can be integrated with intrusion detection systems to detect and alert to a threat. This way, organizations can be ready to respond to combined threats. Combining physical and logical controls for enhanced security in industrial systems is also recommended [35]. Redundancy measures should be in place for physical security as well [24]. Implementing redundant security methods ensures that security measures remain in place in case of a failure. This can mean anything from backup power sources for access control systems to dual-layer mechanisms like badge readers in critical areas.

Like with anything, regularly reviewing and auditing your own physical security controls is recommended to ensure the effectiveness of the measures [24]. Setting security controls to a test alongside other testing can be a quick and easy way to ensure the effectiveness of systems. Performing penetration tests to identify vulnerabilities in physical security can also be an effective way to audit and review the areas that require improvement. Finally, documenting and reporting physical security measures is important. This could mean maintaining logs of critical areas, including time, date, and personnel details, which is beneficial for tracking down potential internal threats. Documenting security incidents and setting corrective actions brings the organization closer to better security practices [18]. Physical security controls are essential for covering critical hardware in IT/OT environments. Still, by implementing robust measures aligned with standards, organizations can ensure better integrity, availability, and security for their assets.

5.2.4 Redundant and Backup Hardware

Redundant and backup hardware ensures the continuity of operation in industrial environments by mitigating risks from hardware failures. Redundancy offers failover mechanisms for critical components, while backup hardware is an immediate replacement. The importance is evident: minimizing disruptions in critical industrial processes and enhancing system resilience against hardware failures or maintenance downtime. The topic of redundant and backup hardware can be broken down into two simple issues. Redundant systems have hardware operating in parallel or standby mode to ensure seamless failover across similar hardware. This can be in Active-Active redundancy mode, where the load is shared and taken over if one fails. The other alternative is active standby, where the backup system remains on standby and activates automatically upon failure of the primary system. With backup hardware, we are talking about physically kept devices that are ready for deployment when primary components fail. Practical

examples could be pre-configured spare devices that are kept on-site for immediate deployment or hot-swappable components like storage drives, power supplies, and cooling units. Backup resources are crucial for business continuity planning, but redundancy is also heavily supported for ICS components, and redundancy is the core of availability management [22], [24], [30].

The types of redundant and backup hardware we discuss depend heavily on the systems we are working with. Generally, however, we can say that network equipment, for one, is highly recommended to be redundant [23]. Deployment can mean using layer three switches in a high-availability configuration, Firewalls in high-availability configurations, and dual WAN routers for redundant internet connections. For ICS cybersecurity management, network redundancy is a key topic [23]. The same goes for redundant servers and storage systems that ensure continuous data access and processing [24]. Using redundant storage solutions can protect systems against data loss and hardware failure. With RAID configurations, organizations can simultaneously protect against hardware failure and redundancy. Power supplies are also highlighted in any discussions around industrial environments. Redundant power supplies ensure that hardware remains operational during power disruptions. Installing dual power supplies in critical devices like PCLs and SCADA controls is recommended [22]. Backup generators and UPSs can provide power during outages and mitigate possible power spikes.

The deployment strategies for how we implement hardware redundancy and or backup might differ. High-availability configurations are one way to handle system availability so that redundant systems are configured to fail over to minimize downtime. This could mean the usage of load balancers to distribute traffic across multiple servers in active-active setups or implementing heartbeat protocols to monitor and activate standby systems during failures. High-availability configurations are often recommended for critical services and systems [24]. Another way to handle deployment could be backup hardware readiness, which means having backup hardware pre-configured and stored securely for rapid deployment. This would mean minimizing the downtime. It is crucial that the strategy involves storing a pre-configured device, regularly updating backup devices, and maintaining the process to ensure hardware compatibility and testing [30].

Regular hardware testing and maintenance ensure that redundant and backup solutions remain operational. Monthly failover drills for redundant systems are recommended, and testing backup hardware annually verifies functionality and compatibility [23], [30]. Testing and maintenance for backup and redundant systems is also viewed as highly important. If the

backup or redundant system isn't working when it is needed, we are facing no return on the investment of having those systems. Encouraging regular testing of backup and redundant systems is more than recommended, but highlighting testing as a part of the hardware lifecycle is crucial [23]. Integrating redundant and backup methodologies into disaster recovery and continuity plans is also advised [33]. Defining the procedures for deploying backup hardware in response to hardware failures is recommended. Also, redundant systems are integrated into recovery time objectives. Generally, redundancy and backup processes should be built into incident response and disaster recovery processes.

Monitoring and documenting these processes is a way to track and maintain the success of redundant and backup hardware solutions. Monitoring tools should be used to track the health of redundant systems and identify potential issues beforehand. At the same time, maintain detailed documentation of backup hardware configurations and locations. Monitoring and documenting redundant and backup systems as part of the overall asset management is recommended [24]. Redundant and backup hardware is essential for ensuring high availability and operational continuity in IT/OT environments. By implementing redundancy in critical systems and maintaining ready-to-deploy backup hardware, organizations can minimize downtime and mitigate the impact of hardware failures.

5.2.5 Monitoring and Maintenance of Hardware

Monitoring and maintenance of hardware is to ensure the reliability, security, and longevity of IT and OT systems by detecting issues early on and performing proactive maintenance on hardware to prevent failures. The importance is highlighted in industrial environments where hardware supports critical processes on the factory grounds. Monitoring, by our definitions, means continuous observation of hardware performance, health, and status to identify potential issues. Maintenance is a regular activity to keep the hardware in optimal condition, including preventative and corrective actions for hardware. In IT/OT environments where unplanned downtime is unwanted, we can prevent downtime by proactively identifying and addressing hardware issues; we also extend the lifespan of critical systems and minimize repair or replacement costs, which can be beneficial as industrial systems tend to have longer lifespans. And by monitoring and maintenance, we support compliance with operational and cybersecurity standards.

If we break down monitoring and maintenance into parts, we can see that there is performance monitoring, environmental monitoring, and preventive maintenance. We aim to track key

metrics for performance monitoring to assess hardware performance and detect system anomalies. This could mean CPU usage, memory utilization, and disk I/O for servers and workstations. We can track communication latency and throughput for network devices and determine if we are seeing an unexpected amount of traffic or latency through the OT network. Hardware performance tracking helps track anomalies in hardware, which, therefore, can help maintain system integrity and availability [22], [24]. However, it is also essential to monitor critical systems for security management. We should also observe environmental conditions to ensure the hardware operates within safe parameters. This could mean installing additional temperature, humidity, and vibration sensors in data cabinets or industrial facilities. Environmental monitoring should be considered part of hardware lifecycle management, as it may extend the hardware lifecycle in industrial environments [23]. Predictive maintenance refers to scheduled activities to reduce the likelihood of hardware failure in the field. This could mean cleaning dust from cooling systems, replacing filters, and performing controlled firmware updates on devices to address security vulnerabilities. Predictive maintenance is recommended, especially for critical systems, to ensure their availability [24]. Corrective maintenance is referred to as the repair or replacement of hardware components after detecting issues. This usually means replacing worn-out drives or power supplies before they fail and addressing hardware errors indicated by the monitoring systems. Corrective maintenance is intended to support operational continuity [22].

The tools and technologies used in hardware monitoring matter as well. We should utilize monitoring tools to track hardware health and performance, as it is too heavy to do it manually. Automating the process will help the organization in the long term, and deploying industrial-specific monitoring solutions in OT equipment is recommended [24]. Automation and automated monitoring tools help organizations with the efficiency and accuracy of maintenance. Predictive maintenance technologies can also help organizations identify potential failures based on historical data and real-time monitoring. This could mean implementing data-collection devices to track operational equipment to collect data on machinery or using vibration analysis to anticipate wear in mechanical components. Predictive maintenance is a way to enhance continuity and maintenance planning for organizations [30].

Scheduling maintenance and how we proceed during emergencies should also be predefined. Setting a regular maintenance schedule to follow a structured schedule for hardware maintenance activities helps with maintenance consistency and accountability [24]. This could mean anything from monthly health checks on PLCs and SCADA systems alongside other

maintenance or scheduling a quarterly inspection to go over data cabinets, cooling, and power systems in an industrial plant. Alongside maintenance schedules, we should have predetermined emergency maintenance procedures and establish procedures to ensure rapid support in case of unexpected hardware failures [33]. Developing a workflow for swapping out failed components and maintaining on-call staff or third parties for immediate repairs to critical hardware can be beneficial.

As a maintenance and upkeep topic, it is highly beneficial to integrate maintenance into incident response plans, business continuity plans, and disaster recovery plans for rapid recovery. This could include testing hardware failover mechanisms during scheduled maintenance and validating backup systems during preventive maintenance activities. Maintenance plays a crucial role in continuity and recovery planning, making its integration into the process highly important [30]. It is also recommended that monitoring and maintenance activities be integrated into security policies [23]. For example, ensure that we log and audit all maintenance activities to detect possible unauthorized access and utilize secure remote monitoring tools. The importance of secure maintenance practices can be seen in industrial environments where a protocol error can lead to financial losses or a loss of human life.

On top of this, we need to ensure sufficient documentation and reporting of monitoring and maintenance. Maintaining detailed and well-maintained records of all maintenance activities, including actions taken and outcomes, helps an organization direct its maintenance activities. This could mean documenting firmware updates and their impact on system performance, or logging corrective actions such as component replacements or repairs, and their suspected causes. Documenting maintenance activities promotes accountability in the organization [24]. In addition to documenting maintenance records, we must use reports to review hardware performance and identify trends or recurring issues. Generating monthly reports on network device uptime and maintenance activities helps organizations steer toward better availability, and using trend analysis to predict and address recurring hardware failures can help. Regularly reviewing and reporting are encouraged to refine security and maintenance processes in the organization [18].

5.2.6 Secure Configuration and Access Control for Hardware

Secure configuration and access control for hardware ensure that IT/OT hardware is set up securely and protected against unauthorized access, which can reduce the risk of vulnerabilities and system compromises. The importance of properly setting up the devices is evident in

industrial environments where hardware directly influences physical processes and operational safety. Secure configuration refers to the process of applying security controls, disabling unnecessary features, and hardening hardware devices to minimize exposure to threats. As with access control, we refer to mechanisms and policies that regulate who can access and modify hardware configurations and operations. In industrial environments, the benefits and importance are clear: prevent unauthorized changes to critical infrastructure, reduce the attack surface by eliminating default or unnecessary settings, and ensure accountability through controlled access to hardware devices.

The foundation of secure configuration and access control comprises five key areas: hardware configuration hardening, access control policies, physical hardware access controls, secure firmware management, and logging and auditing for access control. Hardware configuration hardening refers to strengthening the default configuration of hardware to minimize vulnerabilities. Practically, this means disabling unused ports and services on network switches and PLCs, removing default credentials and applying strong, unique passwords, or restricting physical ports to prevent unauthorized data transfer. Critical components and their configuration should be hardened as part of a broader security strategy, and secure configuration is recommended, especially for industrial components [22], [24].

Implementing strict access control policies to define and enforce access rights for hardware components is also recommended [24], [35]. This could mean using role-based access controls to limit user privileges based on roles and responsibilities or enforcing the principle of least privilege, where users only have access to the resources necessary for their role. It could and should also mean using multi-factor authentication to access hardware management consoles where applicable. Access control policies tailored to ICS environments are recommended, while role-based access controls minimize unauthorized hardware interaction. Physical access control for hardware also falls under the same access control policies. Preventing unauthorized access to hardware devices in offices and industrial environments should be applied. Using locks and digital tools to have entry systems for server rooms and data cabinets is recommended, such as physically securing any critical hardware in environments with locked cabinets. Organizations could use tamper-evident seals for hardware enclosures. Physical access controls protect critical assets, as do access control policies overall. Physical access restrictions should be emphasized as part of OT security programs [23], [24].

Secure firmware management refers to maintaining the integrity of firmware and BIOS configurations on hardware devices. Practically, this could mean updating firmware and BIOS updates to patch vulnerabilities, verifying firmware authenticity using vendor-signed updates, or disabling bootloader modifications to prevent unauthorized firmware changes. Secure firmware management practices are standard for industrial control systems, and patching is recommended for any IT and OT hardware alongside secure management [22], [24]. Finally, for the fundamentals, logging and auditing of access controls are required. Ensuring visibility into hardware access activities for accountability and threat detection is crucial. Practically, this would mean event logging on all access attempts on critical hardware devices, implementing centralized logging tools to monitor these logs, and conducting regular audits of the access logs to detect potential suspicious behaviors. Logging and monitoring are generally recommended for any critical access, and continuous monitoring should be a part of security management programs for IT and industrial environments [23], [24].

How we implement these practices in our environment is crucial. The standards recommend specific strategies for deploying secure practices. Secure default configuration is one of those strategies. Establishing a secure default configuration for all newly deployed hardware ensures that security best practices are pre-configured [24]. This could mean practically having a configuration ready on new devices that changes the default credentials before placing hardware into deployment and disabling unused interfaces and services during installation. Secure configuration defaults have to be set for the organization to follow. Using configuration management tools to automate and manage hardware configurations at scale is recommended, helping organizations become more adaptable [24]. This could mean using Infrastructure-as-Code tools for standardized configurations and implementing configuration management databases to track hardware configurations at large. The use of configuration management tools helps with the standardization of secure configurations and helps organizations push those ideas into reality. Network segmentation and isolation limit hardware exposure through the network and isolated zones. Practically, this would mean creating isolated zones for different types of equipment and isolating them with separate VLANs. It would also mean implementing DMZs to restrict traffic between IT and OT environments, requiring traffic restrictions. Network segmentation minimizes hardware exposure and is recommended by the standards [23].

Maintenance and review of secure configurations are as essential as setting them up in the first place. Organizations need to set regular security audits for the hardware configurations and access policies so that they will be reviewed and re-evaluated regularly [24]. This could mean

security audits for hardware assets or penetration testing to identify misconfigurations. Recommendations for security reviews and audits are clearly outlined. Also, organizations need to ensure that configurations are backed up and recoverable when needed. Organizations must maintain backup copies of hardware configurations for quick recovery after failures or attacks. Organizations can automate configuration backups for critical systems like PLCs and SCADA servers, and those backups need to be stored in secure, offline locations to prevent tampering. Regular backups are part of resilience planning; building them properly can help with business continuity and everything else [24], [30].

Finally, proper documentation and policy enforcement ensure that secure configuration and access control standards are consistently applied. Developing a secure configuration baseline policy for all new devices is recommended, as well as maintaining an access control policy that defines roles, permissions, and enforcement mechanisms in different areas [18], [22]. Policy creation is one of the keys to bringing the changes and formalizing configuration and access control policies for industrial environments to ensure visibility, accountability, and security. Secure configuration and access control for hardware are critical for safeguarding the IT/OT systems from unauthorized access and misconfigurations. By implementing secure default settings, strict access control policies, regular audits, and leveraging automation tools, organizations can significantly reduce attack surface and maintain operational security.

5.2.7 Incident Response and Recovery Hardware

Incident response and recovery hardware ensures that IT/OT systems can respond effectively to security incidents, hardware failures, or operational disruptions while minimizing downtime and ensuring system integrity. Incident response and recovery hardware are essential to hardware management in industrial environments where operational continuity is paramount for the business. Incident response hardware refers to specialized equipment designed to detect, isolate, and contain incidents, which may include security breaches or system failures. Conversely, recovery hardware consists of backup and failover systems that are utilized to restore normal operations following an incident. Why this matters to IT/OT systems is that it reduces downtime and operational disruptions during security incidents while also ensuring faster system recovery and protecting critical infrastructure and data integrity, but it also aligns with business continuity and disaster recovery strategies.

We will break down the incident response and recovery process for hardware into five key components: incident detection, isolation, containment, backup and recovery, forensic analysis,

and communications and coordination. Each element plays a crucial role in the hardware's overall incident response and recovery strategy. Incident detection hardware is most often first in line for incidents. These first-line devices and tools are designed to detect anomalies and potential incidents in real time. These can be intrusion detection systems and intrusion prevention systems, or network traffic analyzers and packet capture devices that help to keep our environment safe by actively monitoring it. Monitoring is recommended, and it is advised to set up hardware for it in industrial environments and as a general part of security operations [22], [24]. Along with the first security responders are isolation and containment hardware – The equipment used to isolate compromised systems during security incidents or daily operations. Practically, this means hardware responsible for network segmentation, like firewalls and managed switches, physical disconnection mechanisms for isolating OT systems, like airgaps in the systems, or endpoint detection and response tools capable of isolating infected devices. Isolation and segmentation are big parts of the incident response and are heavily recommended strategies to isolate incidents [35].

What comes after the incident is most often backup and recovery hardware – the hardware resources that are used to restore system functionality after an incident. Practical examples are redundant servers and pre-configured failover settings, PLCs on-site for immediate replacement, and disaster recovery hardware that can be stored in separate locations. It all comes down to maintaining backup systems and ensuring business continuity during incidents. The importance of redundant and backup systems for critical industrial systems is also highlighted in the standards [22], [30]. Alongside backup hardware, forensic and analysis hardware are used for forensic analysis after a security incident to understand root causes. This could be just a regular workstation with specialized hardware or write blockers preserving the integrity during analysis. Forensic analysis is recommended as part of incident response for root cause identification [33]. Finally, we have communication and coordination hardware supporting secure communication during and after an incident for coordination. This would mean secure communication channels for incident response teams or air-gapped laptops for secure data recovery. Secure communication channels must be available in the event of an incident [24].

To implement incident response and recovery hardware, we need to keep in mind four different topics: readiness and accessibility, hardware redundancy planning, testing and validation, and secure storage and maintenance of response hardware. All of these have a role in the implementation and are needed in the process. Readiness and availability ensure that response

hardware is ready for use and easily accessible when needed. This could be practically maintaining an incident response kit with spare network devices, storage media, and possible forensic tools, or storing backup hardware in secure but accessible locations with controlled access. The recommendation is to prepare recovery resources for rapid deployment during incidents and understand the meaningfulness of the preparation work in daily operations [30]. The same applies to hardware redundancy planning, which involves designing systems with redundant hardware to ensure operational continuity during incidents. This is typically the dual SCADA server configuration that includes load balancing, failover mechanisms, redundant power supplies, and battery backups (UPS) for critical hardware. Implementing hardware redundancy is essential to maintain operational integrity [22].

The redundancy and incident response also boil down to secure storage and maintenance of the response hardware. Storing the hardware securely in a separate facility with separate physical security controls is recommended, but regularly inspecting and testing spare PLCs, Servers, and network devices for integrity is also recommended. Securing backup hardware against tampering and environmental damage is critical, as they are the hardware that we rely on in incident response [24]. This is where testing and validation come into play as well. Regularly testing and validating the effectiveness of incident response and recovery hardware is critical. When we trust our process on these devices, we must ensure they can be used. This could mean quarterly failover tests for redundant hardware configurations or testing backup hardware restoration processes to ensure that we can recover with the current systems. It is recommended to schedule testing for all backup and recovery resources, as well as to test the incident response measures in industrial control system environments [23], [30].

There is no clear standing for these hardware resources as individual parts of hardware. However, the hardware resources must align with formal incident response processes to ensure redundant and efficient incident response hardware. The practical stance on this could mean that we include hardware failover protocols in the organization's incident response plans or assign roles for specific hardware resources during an incident. This could mean network isolation through managed switches, for example. Defining hardware response steps with a broader incident response plan framework is recommended [24], [31]. Integrating the solution is important, but it is equally essential to maintain records of all incident responses and recovery hardware, including testing outcomes and usage reports. Documenting procedures, from hardware configurations to recovery processes, is crucial. Additionally, keeping an inventory of spare and recovery hardware with detailed locations is necessary. Maintaining this

documentation not only ensures operational continuity but also enhances security [24]. Incident response and recovery hardware is crucial for maintaining resilience in IT/OT environments. By implementing redundant systems, backup hardware, and forensic tools, organizations can significantly reduce downtime and improve their security posture during critical incidents.

5.3 Software Domain: Application Security and Lifecycle Management

The software domain addresses the critical role of software components in industrial IT/OT systems, ranging from control applications and embedded firmware to enterprise-level management tools. As industrial environments increasingly depend on software for automation, data processing, and remote operations, ensuring the security and resilience of software becomes paramount.

This section builds upon the principles outlined in IEC 62443-4-1 for secure software development and IEC 62443-4-2 for secure component design. It also integrates control requirements from ISO 27002, focusing on secure coding practices, vulnerability management, configuration security, and software patching.

Special emphasis is placed on ensuring the integrity of industrial software throughout its lifecycle, from development through deployment and maintenance. Organizations can minimize risks associated with unauthorized access, manipulation, and operational disruption by establishing a structured approach to software security.

5.3.1 Software Inventory Management

Software inventory management involves maintaining a comprehensive and up-to-date record of all software assets within an IT and OT environment. A good software inventory can ensure visibility, compliance, security, and effective software lifecycle management. All of these are critical not only for operational efficiency but also for cybersecurity. Software inventory management is the process of cataloging and managing all software components used in an organization, including applications, operating systems, firmware, and licenses. This is important for IT and OT environments because it provides visibility into the software landscape, reduces shadow IT risks, and helps track software versions, updates, and end-of-life information; this is all essential for vulnerability management, incident response, and compliance with standards. We can break down the core components of software inventory

management into inventory scope and coverage, software asset attributes, software inventory tools and automation, and software inventory maintenance audits.

We should start with the inventory scope and coverage. It is important for the business to clearly define the types of software included in the inventory. This could mean, in practice, including both IT and OT software components such as SCADA systems, HMIs, PLC firmware, databases, and endpoint security tools. Having a solid coverage of the IT and OT software gives the organization good visibility of the landscape. It is recommended to have full asset visibility for effective cybersecurity in an industrial environment, but also maintain a complete inventory of software assets for risk management [23], [24]. While the scope plays an important role, it is also important to identify the key data points for effectively tracking and managing software assets. Setting a solid base of software asset attributes can help the organization manage the landscape. The key attributes should be defined so that you have knowledge of the software name and version, vendor and support contact information, installation location and device association, license type, expiration and compliance status, and patch and update history. Tracking key asset attributes confirms the organization's view of the software assets and ensures complete visibility [24].

Software inventory management requires quite a bit of effort, but it also requires tools and automation to make daily life easier. We need to implement automated tools for real-time software discovery and inventory management. This could mean using tools like Lansweeper, SolarWinds, or Tenable to automate software discovery and tracking. Implementing asset tagging for easier software identification is also a good practice. Monitoring software integrity continuously and encouraging automation for efficient software inventory management is recommended [22], [24]. Just having tools and the knowledge of software inventory up to date is not enough. Keeping the inventory accurate and updated through regular reviews and audits is essential. That is why we have software inventory maintenance and audits. This could mean regular software inventory audits to identify unapproved or outdated applications and remove software from the inventory that no longer aligns with operational needs or security policies. It is recommended that periodic audits be conducted to ensure inventory accuracy and ongoing inventory validation for industrial systems [24], [35].

Software lifecycle management should also be integrated into the daily operations and security. Four main points should be considered: procurement and approval, patch and update management, version control and change management, and end-of-life and decommissioning

management. We should start with procurement and approval. The goal is to ensure that only approved software is added to the inventory. To have this in practice, we would need a formal approval process before purchasing new software so that we can verify vendor security compliance in cases of OT software and IT. It is imperative to prioritize security considerations during the software procurement process [24]. The procurement process is essential for any managed environment and must be rigorously enforced. It is imperative to prioritize security considerations during the software procurement process. Patch and update management is also vital for security purposes. We need to be able to track and apply security patches and updates systematically. Systematic patching should be done to maintain secure configurations on the equipment [22]. This could mean automating patch management for IT systems while scheduling controlled updates for OT environments or testing patches in sandbox environments before deployment in production environments.

While we have established procurement processes, we still require version control and change management. We need to maintain version histories and manage changes carefully to avoid disruptions. Well-maintained records of software versions and changes help the organization prevent issues and ensure compliance [24]. Practical uses could be version control tools for critical software, especially in OT configurations, or implementing a formalized change control process for major software updates. While managing our software versions, we must also ensure proper end-of-life and decommissioning management. It is important to identify and manage software that is approaching the end of support. This would mean identifying software reaching EOL and planning for secure replacements or upgrades, or creating decommissioning plans for safe removal, including data wiping and compliance checks. Managing obsolete software helps reduce security risks for the organization and ensures business continuity [24].

Overall, security considerations in software inventory management should be considered. It could mean Software whitelisting and blacklisting, secure configurations management, and license compliance and management. Whitelisting and blacklisting is a simple definition of which software is approved or restricted within the environment. Having an application whitelist for OT and ICS environments is recommended [35]. This is particularly important for OT environments and control systems, as it aims to prevent unauthorized or risky software installations in any situation. Secure configuration management is also a great part of security integration. Ensuring that software is configured according to the security best practices is essential for security posture. Secure baseline configurations are recommended for OT systems [22]. In practice, it applies baseline configurations for operating systems and control software,

regularly auditing configurations for unauthorized changes. Also, license management and compliance are a great part of security integration. Ensuring that all software is legally licensed and compliant with contractual agreements is highly recommended for compliance [24]. This can mean maintaining a licensing database with expiration alerts and avoiding using unlicensed or unauthorized copies of software by staying up to date with providers.

Software inventory should also be integrated with incident response and business continuity plans. Ensuring that software inventory data supports incident response and business continuity efforts can be integral for the organization. Asset inventories should be used for continuity planning, but software visibility is also critical during incident response [30], [34]. Practically, this could mean using software inventory to identify vulnerable software during a security incident or ensuring that essential software configurations are backed up and recoverable. Documentation is vital for maintaining a comprehensive record of the software inventory and associated management processes. This could mean keeping historical logs of all software installations and updates and generating periodic reports about software status, compliance, and patch levels. Detailed documentation is recommended for compliance and audit purposes [24]. Software inventory management ensures complete visibility and control over software assets, supporting operational efficiency, compliance, and security across IT/OT environments. Implementing secure practices can help reduce software-related vulnerabilities and improve operational resilience in the long run.

5.3.2 Access Control and Authentication for Applications

Access control and Authentication for applications ensure that only authorized users and systems can access and interact with applications. This is critical for the security of IT and OT environments, where applications control sensitive operations and store valuable data across the production. Access control stands for the process of defining and enforcing permissions for users, systems, and methods to interact with an application. Authentication stands for verifying the identity of users or systems before granting access to an application. By implementing proper access controls and authentication, we ensure accountability by tying actions to authenticated users or systems, reducing the attack surface by enforcing strict access rules, and monitoring and protecting sensitive applications from unauthorized access. Components of access control and authentication can be broken down into five core pieces: Role-based access controls (RBAC), Principle of Least Privilege (PoLP), Multi-factor Authentication (MFA), network segmentation and access control lists (ACLs), and Single Sign-on (SSO) and

centralized authentication. By focusing on these, we cover a lot of access control ground but also get familiar with authentication methodologies.

Role-based access control is used to restrict access based on user roles and responsibilities. Practically, this could mean just granting operators only access to the HMI screens they need. At the same time, administrators have full configuration access or can create separate roles for maintenance teams, limiting access to configuration or diagnostic tools. Role-based access control should be a standard for industrial control systems, and implementing role-based access to restrict unauthorized interactions is recommended [22], [24]. Another great practice to have is the principle of least privilege – the ideology is to grant users and systems only the permissions they need to perform their tasks. The principle of least privilege is recommended across all access policies in an organization [24]. This could mean limiting SCADA users to read-only access unless they require control permissions across the layers or preventing third-party vendors from accessing production systems beyond their specific tasks. Through networks, this would mean network segmentation and access control lists in networks. Enforce network-level access control to limit application exposure. Segmentation and ACLs for networks and application security are recommended [22]. This could mean restricting access to OT applications like PLC management tools to specific subnets or VLANs. This also means limiting external traffic to application-specific ports.

Multi-factor authentication adds one more layer of authentication to strengthen access security. Practically, this could mean combining a password and a hardware token to access SCADA systems or implementing phone authentication for critical applications. MFA authentication is recommended for all remote and local access to industrial systems; however, it is also recommended for high-risk applications and systems [24], [35]. Single sign-on and centralized authentication are mechanisms that streamline secure access. This could mean implementing SSO with an AD for IT and OT applications and using Lightweight Directory Access Protocol (LDAP) or Remote Authentication Dial-In User Service (RADIUS) servers to manage user authentication across multiple applications. Centralized authentication streamlines access controls and minimizes security vulnerabilities throughout the organization, making it a standard recommendation [24].

As for authentication mechanisms, there should be strong password policies. Enforcing secure password practices for all application users helps with the organization's security posture. This could mean over 14-character-long complex passwords with alphanumeric and special

characters, and implementing password expiration policies for periodic updates. Enforcing strong password policies is one step of the way, as enforcing secure password practices like password management systems and tools [24]. Certificate-based authentication is also a good use of digital identity management. With certificate-based authentication, we can use digital certificates to verify systems or user identities. Digital certificates can vary from user authentication with TLS certificates to certificates required for communication with OT applications. Certificate-based authentication is recommended for critical systems [22].

At the application level, we also need to define security features. Granular permissions are one way to handle application-level permissions. It means defining permissions at a detailed level within an application. This could mean configuring SCADA software to allow specific users access to only specific system tag views or alarms in the system. We can grant reporting users read, write, or execute permissions at the database level. This allows groups that need to modify data in case of incidents on the industrial floor to do so, while reporting tools and users can only view the data. Fine-grained access controls for application security are especially highlighted in industrial applications [23]. While we should also have fine-grained access controls for applications, we should also focus on logging and audit trails. Maintaining records of access and activity within applications can help organizations in administrative actions for auditing [24]. This may involve anything from activating application logging to monitoring user activities and alterations to essential parameters such as SCADA systems. Additionally, integrating application logs with SIEM tools allows for centralized monitoring and alerts.

Alongside everything else, access controls need maintenance and review. Organizations should have a periodic access review to regularly review and update access permissions to align with user roles and organizational needs. This should mean performing quarterly audits of user access to OT applications, removing unnecessary permissions, and revoking access for inactive users or terminated employees, alongside the termination. Periodic reviews of access permissions help the organization maintain security [24]. Access controls should also be integrated into the incident response process to isolate compromised accounts or systems quickly. This could mean implementing account lockout policies for repeated failed login attempts or using automation to disable user accounts during suspected breaches. Rapid isolation of compromised accounts and systems should be a part of the incident response process [34].

Documentation and policy enforcement are what make access controls stick in an organization. Developing and enforcing policies for access control and authentication across applications enhances an organization's security posture. The importance of documented policies is stressed while formalizing access control measures for industrial environments [18], [22]. Practically, this means creating a formal access control policy for applications that define roles, permissions, and authentication requirements and documenting all changes to an application's access permissions and authentication configurations. Access control and authentication for applications are crucial in IT/OT environments as they help organizations protect their environments from unauthorized access and maintain operational integrity. Organizations can secure their applications effectively by carrying out robust role-based access, MFA, secure configurations, and periodic reviews.

5.3.3 Software Development and Secure Coding Standards

Software development and secure coding standards focus on creating robust, secure, and reliable software to minimize vulnerabilities and risks in IT/OT environments. A secure development environment guarantees operational safety, cybersecurity, and compliance with regulatory and industry standards. Defining what development and coding standards mean is essential, as we are splitting this into two. With software development standards, we mean frameworks and practices that guide the development process, ensuring quality, maintainability, and compliance. Meanwhile, secure coding standards are guidelines for writing code that reduces vulnerabilities and protects against common security threats. The importance in IT/OT environments lies in preventative action for security vulnerabilities, such as injection attacks, buffer overflows, and improper input validation. It ensures that critical software is resilient against cyberattacks and operational errors while aligning with global industry standards.

Three components form software development and secure coding: a secure software development lifecycle, Secure coding guidelines, and vulnerability and risk management. If we are starting off with a secure software development life cycle, it involves integrating security practices into each phase of the software development lifecycle. It would mean requirement analysis, design, implementation, testing, deployment, and maintenance, as well as security practice in each and every one of them. Secure development lifecycle processes are standard for industrial systems, but they are also recommended to be considered for all software assets as well [24], [37]. Secure coding practices walk hand in hand with a secure software development life cycle. Secure coding practices practically mean adopting coding practices to

reduce vulnerabilities in software. This could mean validating all user inputs, avoiding exposing sensitive system information in error messages, ensuring robust authentication, and using strong encryption for data in transit and at rest. Secure coding practices enhance ICS software resilience, but OWASP also provides secure coding practices that are widely adopted guidelines [22], [38]. We also need to consider vulnerability and risk management during software development. Proactively identifying, assessing, and mitigating software vulnerabilities during development and use is a good foundation for secure software. This could mean the usage of tools like Static Application security testing or dynamic application security testing, then prioritizing vulnerabilities using frameworks like the Common Vulnerability Scoring System. Risk management is recommended for software vulnerabilities and the organization's security posture [34].

Testing and validation are a foundation for software development and secure coding standards. With security testing, we verify that the software meets the security requirements and is free from vulnerabilities. Performing penetration testing on web applications and OT control surfaces is an easy way to make sure software is as ready as it is. Utilizing fuzz testing to identify unexpected behavior of software is also recommended. Focusing on security testing in industrial software environments is a key foundation of secure industrial environments [29]. Utilizing automation for testing can easily streamline and enhance the testing processes as well. This could mean using CI/CD pipelines to automate static code analysis and unit testing while also utilizing dependency scanning tools, which can help identify vulnerabilities in third-party libraries. Automated testing improves software reliability and security, which is highly recommended by secure practices [24].

To ensure compliance and the usage of standards in secure development, we should align with secure coding standards in industrial environments to ensure compliance for ICS software [37]. Practically, this could mean using MISRA, which provides best practice guidelines for the safe and secure application of embedded control systems and standalone software, or adopting CERT secure coding standards for languages in use. For regulatory compliance, we need to ensure that software development aligns with applicable regulatory requirements. This could mean adhering to GDPR requirements for data protection or complying with NIS2 for security in critical infrastructure applications. It is advisable to check compliance with legal, regulatory, and contractual obligations [18].

As secure development and coding are not something you can expect from everyone, it is important to train developers with the skills and knowledge to write secure code. This could mean conducting workshops on OWASP's top 10 vulnerabilities and mitigation strategies or hands-on training in secure coding practices, showcasing to programmers what it means in different coding languages and what the consequences can be. Security awareness is highly important, and training should also be provided for developers, not only users [24]. Threat awareness is also a significant part of training. Keeping development teams informed about emerging threats and vulnerabilities helps organizations stay current with the latest trends. This could mean sharing regular threat intelligence reports, reviewing the sources and what they mean, or including security updates in team meetings or training sessions. Encouraging the integration of threat awareness in organizations enhances incident management processes and security awareness [34].

Software documentation and version control with secure repositories are as important for secure software development and coding practices as anything. This means maintaining comprehensive documentation for secure software development processes and using version control systems to manage code securely and track changes. The importance of maintaining detailed records for compliance and security is highlighted, as well as having proper version control as part of secure development practices [18], [24]. This means documenting software designs, configurations, and security testing results while maintaining a secure change log for tracking updates and patches. Version control means hosting code on secure platforms and applying access controls and encryption to repositories containing sensitive code. Software development and secure coding standards are essential for creating a secure, resilient, and compliant environment. Organizations can reduce risks by integrating secure development practices, adhering to coding standards, proactively managing vulnerabilities, and improving internally developed software reliability.

5.3.4 Patch Management and Software Updates

Patch management and software updates are essential for maintaining the security, reliability, and performance of any IT/OT system. Properly managing patches and updates ensures that vulnerabilities are mitigated, systems remain compliant, and operational risks are minimized. Patch management is understood as the process of identifying, testing, deploying, and verifying patches to address security vulnerabilities, bug fixes, or performance enhancements in software. Software updates are broader updates that may include new features, improvements, and critical

patches to software. The importance of IT/OT Environments is evident: we must protect the environments against known vulnerabilities and maintain compatibility with evolving technologies and standards while ensuring system integrity and minimizing operational disruptions in OT environments. It's a lot to ask, but manageable with the correct processes and procedures.

We can break down the core components of patch management and software updates into five components: patch identification and prioritization, patch testing and validation, patch deployment and updates, patch monitoring and verification, and handling unpatched systems. Patch identification and prioritization is the first part, identifying patches and updates from vendors or open-source communities and prioritizing them according to the systems. This could mean subscribing to vendor notifications and using scoring systems to prioritize patches systematically for critical updates. It is emphasized that organizations monitor vendor notifications for security patches in ICS environments, but also evaluate the criticality of patches based on the risk and impact of the patches [23], [24]. The same systematic approach goes for testing and validation of patches, testing and validating patches in a controlled environment to verify their impact on the system functionality. It means going the extra mile of setting up test environments mirroring the production environment and conducting regression testing to ensure new patches do not introduce other issues. Patch testing is advised to ensure compatibility and integrity, while pre-employment testing is also advised for patches in critical systems [22], [24].

Patches and updates must also be deployed; safely deploying them into production systems with minimal disruption can be tricky. Practically, staggered deployment to non-critical systems first, then apply to critical systems during planned downtime. Controlled deployment processes for industrial environments are recommended and encouraged to minimize disruptions during updates [29], [30]. Controlled patching also means that you must monitor the patches to ensure they are successfully applied and that the intended issues are resolved. Validating patch deployments ensures asset inventory maintenance, but monitoring software updates also ensures system performance and security [22], [24]. After patches are identified, tested, deployed, and monitored, there is only one left: the unpatched systems. The organization needs to implement compensating controls for systems where patches cannot be applied. This could mean using network segmentation as a part of protection or deploying prevention systems to monitor and block threats targeting unpatched vulnerabilities. Additional protections and measurements are recommended for systems with known vulnerabilities [29].

The patch management process is key to handling patches properly. Organizations should have a patch management policy; defining a formal policy for managing patches and updates across IT and OT systems helps organizations with consistency and accountability [24]. Practically, this would mean establishing patching schedules for non-critical and critical systems with roles, responsibilities, and escalation procedures. Organizations should also link the patch management process with software and hardware inventories. Patch management should be supported by an accurate software inventory [23]. This would mean using configuration management databases to track software versions and patch statuses and identifying high-priority systems for patching based on criticality and exposure. Patching can become more manageable with automated tools. Organizations should aim to automate part of the patch management lifecycle to increase efficiency and reduce human error [24]. For organizations, this could mean using tools like WSUS, SCCM, or Ansible to automate patch discovery and deployment for IT systems; OT environments often require specific patching solutions for industrial devices.

OT environments don't come without challenges. OT environments bring a lot of special considerations to prevent disruptions while managing patches. The unique challenges in industrial systems should not be dismissed and should be considered [23]. This would mean planning updates during maintenance windows to minimize operational impact and communicate with the business that it has to be done. You should also address vendor-specific restrictions for PLCs. The OT environments come with a lot of legacy systems as well. Patching legacy systems can be complex due to a lack of vendor or machine support. The legacy system risks should be addressed by compensating controls for unpatched systems [24]. This could mean employing virtual patching in the network or gradually phasing out unpatchable systems and replacing them with modern alternatives.

As for the records of patch management, maintaining a detailed set of records of all patches that have been applied to systems is essential. Tracking patch release dates, deployment dates, and associated vulnerabilities allows for visibility in the environment and trackability. It is recommended that patch documentation be maintained for audit and compliance purposes, but it is also essential for forensics and accountability [24]. The reporting and metrics also go hand in hand with the documentation. Using reports to track patching effectiveness and compliance gives management a reason to support patching efforts in environments. Generating monthly reports of the percentage of systems patched and compliance with SLAs helps organizations. However, monitoring the meantime to patch for critical vulnerabilities also gives the

organization a good measurement of security posture. Regular reporting is recommended to assess the effectiveness of security processes inside an organization [18]. Patch management and software updates are essential for maintaining security, compliance, and reliability in industrial environments. If an organization follows best practices, like prioritizing patches, testing updates, and implementing compensation controls for unpatchable systems, the organization can achieve a safeguarded infrastructure around the business.

5.3.5 Application Security Controls and Hardening

Application security controls and hardening involve implementing measures to protect applications from threats and vulnerabilities. Doing this ensures the integrity, confidentiality, and availability of applications in the industrial environment, where they often control critical processes or handle sensitive data. Application security controls are measures to prevent, detect, and respond to security threats that target applications. At the same time, hardening is the process of reducing the surface of applications' attacks by eliminating vulnerabilities and applying best security practices. This way, we can secure essential industrial operations and mitigate risks of exploitation from common vulnerabilities, enhancing resilience against cyberattacks and ensuring compliance with security standards.

The foundation of application security controls and hardening lies in five things: logging and monitoring, encryption and data protection, input validation and sanitization, access control and authentication, and secure configuration. Suppose we start with a secure configuration, which means applying a secure baseline configuration to reduce application vulnerabilities. This could mean anything from disabling unnecessary features and services to enforcing strong passwords and encryption on any application available. It can also mean enforcing secure configurations for web servers hosting OT applications. Establishing and adhering to a baseline would ensure the security of configurations on essential applications and improve application integrity, which is advisable [22], [24]. Access control and authentication should go hand in hand with the secure configuration of an application. Ensuring that there is limited access to applications from authorized users and systems only. This could mean utilizing role-based access control to define user roles and permissions, implementing multi-factor authentication, and enforcing account lockouts after multiple failed login attempts. Access control mechanisms are supported for secure application use in industrial environments and in IT environments for application security [24].

Since we can limit who uses the application and what features we have, we should also prevent malicious inputs from compromising applications. This is where input validation and sanitization come into play. Organizations should aim to validate user inputs for critical applications against expected formats such as length, type, and range. Applications can use parameterized queries to protect against SQL injection attacks, or we can sanitize inputs to prevent cross-site scripting vulnerabilities in web applications. Input validation is highly recommended to prevent application vulnerabilities, but input validation is also highlighted as a critical control against injection and cross-site scripting attacks [24], [39]. In addition to input validation, we must use encryption to protect data processed, stored, or transmitted by applications. The organization should aim to encrypt sensitive data in transit using TLS and at rest using AES-256 at least for now. Industrial systems typically require encryption for compliance; however, encryption is also recommended as a critical measure for safeguarding sensitive data [22], [24]. As we aim to protect applications, we should also know what is going on inside the applications. Tracking application activity to detect suspicious behavior and aid in incident response can help the organization predict system errors and act as a preventative measure for cyberattacks. Integrating application logs into security information and event management tools helps with organizational monitoring. Logging and monitoring are recommended to identify and respond to security incidents, which includes logging industrial systems as part of a cybersecurity program [23], [24].

There are several ways to harden your software solutions; however, when hardening is discussed, it usually implies removing unused features, secure coding practices, and patch management. Removing unused features is simple: disabling debugging and developer tools in production environments and removing sample files, default scripts, and unused modules. The work amount is not much, but the result will be a smaller attack surface. Minimizing unnecessary functionality to improve security in an industrial environment is recommended [29]. Secure code practices are often also discussed as a preventative measure – Writing code and reviewing the code to prevent security vulnerabilities. This could mean static code analysis in the early stages of development to identify early vulnerabilities or implementing peer reviews for critical application code changes. Secure development practices are essential for industrial software development, but secure coding should be a part of application security practices [24], [37]. Patch management is also seen as a regular hardening technique, so regularly updating to address application vulnerabilities is effective. Timely patching of applications can address vulnerabilities early on, and patch management is often required to maintain secure applications

in industrial fields [22], [24]. Scheduling patches for critical applications is easy, and testing patches in staging environments should be a regular part of testing procedures.

Integration of application security controls and hardening with security frameworks can improve the security organizations' approach to application security. This can be done with threat modeling and risk assessment, or compliance with security standards. For threat modeling and risk assessment, we want to identify and address potential threats to applications during the design phase of the application. This could mean utilizing frameworks like STRIDE or DREAD for threat modeling and assessing the risk of third-party integrations like APIs, Plugins, or platforms. Guidelines for risk management are provided in ISO 27005, and they include application threats [34]. Standard compliance is another great way to improve an organization's security posture. Ensuring that applications are built with industry regulations should be the organization's goal. This could practically mean adherence to the IEC 62443 standard for industrial applications. Compliance is a critical component of application security, and it is highly recommended [18].

As with anything, the environment needs to have detailed documentation for secure application configurations. This means creating configuration baselines for critical IT and OT applications, including access control settings and encryption protocols. Document changes to application configurations should be signed alongside others as part of change management. Maintaining secure configuration documentation helps in the long term with the environment and its adaptability, but also helps with auditing [24]. Regularly reviewing the documentation and applications themselves ensures compliance with set security policies and points out abnormalities. This could mean annually having security assessments of the environment or using third parties to perform audits to verify compliance or the status of the environment. Regular auditing of industrial applications should be a standard as part of cybersecurity management, but also for continuous improvement [23], [24]. Application security controls and hardening aim to protect IT/OT environments from vulnerabilities and cyber threats. By securing configurations, implementing access control, validating inputs, and hardening application code, organizations can strengthen their cybersecurity stance while also minimizing the unnecessary attack surface.

5.3.6 Monitoring and Logging for Application Activity

Monitoring and logging for application activity are to ensure that application behavior is continuously tracked, anomalies are detected, and security incidents can be investigated

effectively. Logging and monitoring are critical for compliance, security, and operational reliability in industrial environments. Monitoring is the real-time collection and analysis of application activity to detect anomalies, performance issues, and security threats. Logging systematically records events, errors, and transactions with applications to provide historical data for audits, forensic investigations, and troubleshooting. With monitoring and logging, we aim to enhance security by detecting unauthorized access, application misuse, and potential cyberattacks early. This will support compliance with regulatory frameworks by maintaining an audit trail and providing visibility into application health and performance for proactive maintenance and upkeep.

By separating the essential principles—logging strategy and implementation, key events to record, real-time monitoring and anomaly detection, log storage and retention, and log analysis and correlation—we establish a robust foundation for effective monitoring and logging. Starting with the core question strategy, establishing a structured approach to logging application events is recommended to ensure completeness and usability while maintaining the cybersecurity of industrial applications [22], [24]. Defining log categories, authentication attempts, configuration changes, errors, and security events separately can help organize the strategy, but standardizing log formats also helps ensure consistency across applications. While strategy is important, so is identifying the key events that should be recorded for security and operational insights. This could mean recording privilege escalation, tracking policy violations, blocking intrusion attempts, or API calls. Security-related events should be captured for forensic analysis, but logging security incidents for incident response management can also be helpful [23], [34]. Continuous monitoring is seen as integral to detecting suspicious activity and security threats. This could mean deploying SIEM tools to analyze logs in real-time and using behavioral analytics to detect deviations from normal usage patterns. Real-time monitoring is recommended for early threat detection, but it is also encouraged for industrial applications to detect threats [22], [24].

Log storage and retention also have to be set. Defining retention policies for application logs to ensure compliance and forensic readiness is essential, but not making the active log files too big is necessary. Storing logs for a minimum of one year for compliance with industry regulations is advised, but it is also suggested to align with local laws and regulations [35]. Implementing log archiving and secure storage for logs to prevent tampering or loss is suitable for a monitoring and logging strategy. It is essential to maintain audit logs for security and compliance, but it is also advised that logs be stored securely to prevent unauthorized

modifications [18], [35]. Storing and retaining the logs go hand in hand with analysis and correlation. Using tools to correlate logs from multiple sources to detect complex security incidents is recommended. This could mean integrating firewall, application, and network traffic logs for correlation in SIEM systems and implementing log-based analysis with machine learning to identify patterns indicating cyber threats. Log correlation is recommended to detect sophisticated attacks, and advanced log analysis is recommended for industrial security monitoring [22], [24].

How we monitor our equipment is also essential; we should perform performance and security monitoring, as well as user behavior analytics. We should monitor application availability, response times, and resource usage for performance monitoring. Performance monitoring is supported to ensure system reliability [24]. In practice, this would mean application performance monitoring tools to track resource usage and set automated alerts for high resource utilization or service outages. Security monitoring is essential alongside performance monitoring. Tracking security-related activities in applications to detect potential threats early on is recommended. Implementing security monitoring for critical applications is seen as vital in industrial environments [22]. Practically, this means intrusion detection for unauthorized application access or file integrity monitoring to detect unauthorized changes in critical files. User behavior analytics go hand in hand with security monitoring. Analyzing user behavior to detect insider threats and compromised accounts is recommended to enhance security monitoring [24]. This means practically tracking deviations from standard logging patterns or using anomaly detection algorithms to identify unauthorized privilege escalation attempts.

Monitoring and logging processes should also be integrated into IT processes, especially incident detection and response. The integration comes with automated alerts and responses that should be set for monitoring. Configuring real-time alerts to detect and respond to security incidents is integral for organizations. Automating incident detection and response is highly recommended [34]. This could mean implementing automated lockouts or using automated script execution to isolate environments. Incident investigation and forensics are also necessary. Logs can be used to investigate security incidents and provide forensic evidence, which can help the organization explain events. This could mean retaining detailed access logs for forensic analysis after a breach or using log correlation tools to reconstruct attack timelines. Detailed logging is essential for incident response in industrial environments [18].

How we store, review, and handle audits around monitoring is essential as well. Regularly reviewing logs to ensure compliance and detect anomalies is a standard practice. This could mean conducting weekly log reviews for high-risk applications or performing annual security audits on log retention policies. Periodic log reviews ensure compliance but also guarantee that the organization stays ahead of the issues [24]. A standard overview of the logs also ensures that the logging practices align with legal and industry regulations. Going through and checking back up with the rules helps to maintain compliance through security monitoring [18]. Retaining logs for GDPR or NIS2 compliance is a practical example of following the standards. Monitoring and logging for application activity provides critical visibility into security, performance, and operational issues in IT and OT environments. Organizations can detect and respond to incidents effectively with a structured approach, real-time monitoring, and automated analysis.

5.3.7 Backup and Recovery for Critical Applications

Backup and recovery for critical applications ensure continuity by protecting essential software systems from data loss, corruption, or cyber incidents. In IT and especially in OT environments, applications such as SCADA, MES, and ERP systems must remain operational or be quickly restored after an outage. For backup, we are creating copies of application data, configurations, and states for later restoration. Recovery is the process of restoring backed-up data or system configurations to resume normal operations. Rapid recovery from cyber incidents, against accidental deletions, hardware failures, and corrupt software updates, is essential in IT and OT environments, but also supports regulatory compliance and auditability.

As with anything, backup and recovery for critical applications starts with a backup strategy and planning. Defining policies and procedures for backing up critical applications is a start. Implementing a policy covering frequency, retention, and encryption requirements while categorizing applications based on criticality ensures real-time backups for essential systems. It is recommended to define backup strategies aligned with business continuity, but systematic backup management is also encouraged in industrial environments [22], [30]. Another crucial aspect to set is the backup types and frequency. It is essential to select appropriate backup styles based on the application's criticality. Full backups have a complete copy of all data and configurations, incremental backups only save changes since the last backup, and differential backups store changes since the previous full backup. Daily incremental backups and weekly full backups are recommended for mission-critical applications, while snapshot-based backups

should be the choice for database-intensive applications. Backup frequency based on risk and business continuity requirements is also recommended in industrial environments for application resilience [22], [30].

We also need to store the backups—ensuring that backups are stored safely and protected against cyber threats is critical for recovery scenarios. Practically, this could mean using air-gapped offline backups to prevent ransomware attacks and implementing encryption for backup files to protect sensitive data. It is recommended to encrypt stored backups to prevent unauthorized access and to store them in a protected, tamper-proof environment [22], [24]. This location should also be redundant, meaning geographic redundancy, to prevent data loss due to site-specific failures. A rule of thumb is to have three backup copies: primary, onsite, and offsite. A separate geographic location prevents regional disasters affecting all copies, which is advised by geographic redundancy for business continuity [30]. A final core for application backup and recovery is application configuration and state backup, backing up data, application configurations, and states. Practically, this could mean separating PLC configurations or HMI profiles from operational data or using configuration version control systems to track changes in critical OT applications. Maintaining backups of industrial software configurations is highly recommended [35].

Recovery strategies and testing are as essential as backup strategies. They start with setting recovery point objectives and recovery time objectives. Each application needs acceptable data loss and recovery times. This could mean setting recovery point objectives to, for example, one hour for real-time operational applications and defining recovery time objectives to 15 minutes for mission-critical database servers. Defining recovery point objectives and recovery time objectives is a key to business continuity metrics, but setting recovery objectives for critical industrial systems is also required [22], [30]. Automated and rapid recovery mechanisms are here to help organizations meet these recovery objectives. Implementing automated recovery solutions to minimize downtime and for rapid incident response is recommended [31]. Practicalities around this could mean disaster recovery processes that are automated or hot standby systems for real-time failover of critical applications.

Periodic backup testing and validation are key to ensuring that your recovery will be tested once it is needed. Regularly testing and validating backup integrity and ensuring recovery procedures help organizations ensure the effectiveness of backups, and verification of backup processes is required in industrial environments [23], [30]. While it is quite simple to dismiss it, it is also

highly recommended. Performing quarterly tests to verify that backups can be restored successfully is one way of handling it, but also conducting cyber resilience drills simulating ransomware recovery can help organizations ensure backup effectiveness. Training drills go hand in hand with incident response and disaster recovery, which should be integrated into the recovery process. Backups are vital components of incident response and recovery plans and should be handled accordingly. Including backup restoration protocols in cybersecurity incident response plans could be one way to do it, but also defining escalation procedures beforehand can ensure the organization's faster recovery during system outages. Security incident response frameworks are advised to include backup recovery [33].

For backup and recovery, we also need to set security controls, which would mean ensuring data integrity, tamper protection, access control, and authentication. With data integrity and tamper protection measures, we are ensuring backups are immutable and protected against tampering. This could mean using write-once and read-many storage to prevent modifications and monitoring backups for unauthorized access or corruption. It is advised to have integrity controls to protect backup data, and integrity verification is recommended in industrial environments [22], [24]. One way is to implement access control and authentication mechanisms to backup systems. Restricting access prevents unauthorized modifications. Access controls and recovery tools are recommended to secure backup storage [24], [35]. This means implementing role-based access control for backup administrators and requiring multi-factor authentication to access backup systems.

Forming the backup documentation and the backup policy are keys to maintaining a comprehensive policy, enforcing it, and documenting backup and recovery. This could mean creating backup runbooks specifying schedules, storage locations, and procedures, and documenting recovery steps and dependencies for critical applications. The ISO 27001 requires documentation for IT and OT backup policies [18]. This also guarantees partial compliance with industry regulations, but not all of them. Ensuring that backup policies meet regulatory requirements is recommended. This should be checked against relevant regulations or standards, such as NIS2 or ISO compliance, and storing logs in a secure and tamper-proof environment ensures compliance. Compliance verification is required for any standard and business continuity plans [30] Critical application backup and recovery are essential to maintaining operational resilience in IT/OT environments. Organizations can ensure continuity and cybersecurity by implementing secure, redundant backups, automated recovery solutions, and periodic testing.

5.3.8 Incident Response and Recovery for Software Applications

Incident response and recovery for software applications are critical components of cybersecurity efforts and business continuity. They ensure that software applications can quickly detect, respond to, and recover from security incidents such as cyberattacks, data breaches, and system failures. Incident response is identifying, containing, eradicating, and recovering from security incidents affecting software applications. In contrast, recovery is restoring the affected software applications to normal operational states after an incident. The importance of IT and OT environments lies in the protection of mission-critical applications from cyber threats while ensuring compliance with regulatory and cybersecurity standards, reducing downtime, and mitigating financial and reputational damage.

Breaking down incident response and recovery, it all comes down to incident detection and identification, incident response plan, containment and eradication of threats, recovery and restoration, and finalizing post-incident analysis. Starting with incident detection and identification, rapidly detecting security events affecting software applications is crucial. Using intrusion detection systems to monitor for unauthorized access to applications helps, and implementing real-time anomaly detection for applications with automated alerts will enhance the incident detection and identification process. Proactive detection mechanisms are key for incident identification and monitoring, and detection is supported in industrial software applications [22], [31]. The incident response plan is also critical for the incident response, as it has a predefined process for responding to software-related incidents. This could include developing a software incident response plan with clear roles, responsibilities, and escalation paths, and defining incident categories with tabletop exercises to test incident response readiness. ISO 27035 provides guidelines for incident handling and response strategies, and in industrial environments, it is recommended to have structured incident response planning [23], [33].

After an incident, how we contain and eradicate the threats is crucial to recovery. Isolating infected applications or containers is essential to prevent lateral movement, and having clear steps is also vital. Containment and eradication also mean applying patches to mitigate exploited vulnerabilities and revoke compromised user credentials. Rapid containment measures are recommended for industrial applications, but effective containment strategies are also encouraged to minimize damage [22], [31]. Containment and eradication go hand in hand with recovery and restoration procedures. Restoring applications to a secure and functional state

should follow the same efforts as the containment and eradication efforts. This would mean having clear, verified backups to fix applications, conducting post-incident security scans, and an automated rollback mechanism that can restore software versions of failed updates. Business continuity highlights the requirements for application recovery, but industry standards also require vendors to provide secure recovery capabilities for industrial applications [30], [35]. What happens post-incident is learning. This could mean conducting reviews and forensic investigations to prevent recurrence. It could also mean conducting root cause analysis, updating software development policies based on findings, and sharing findings with threat intelligence platforms if necessary. Post-incident learning is a great chance to refine response plans, and it is advised, but also continuous improvement is key for cybersecurity incident response [23], [33].

Incident response has to be integrated with security controls and business continuity. This would mean proactive security measures to reduce incident impact, which would mean strengthening software security to minimize attack surfaces. This could mean utilizing zero trust principles to verify application access at all times or implementing code integrity monitoring. Proactive application security measures are required for solid cybersecurity [24]. Cybersecurity is also visible in cyber threat intelligence and incident prevention. This could mean using intelligence-driven insights to anticipate and mitigate future incidents. Proactively, this could mean subscribing to frameworks and CVE databases for vulnerability tracking across the IT teams and conducting threat hunting on application logs or network traffic. Proactive measures are encouraged using cyber threat intelligence for incident prevention [31]. Finally, backup and recovery have to be integrated into incident response, which is integral to the incident response process. This means ensuring immutable backups for ransomware tampering or predefining disaster recovery failover for mission-critical applications. Ensuring incident response is integrated with business continuity ensures business continuity planning alignment, and it ensures secure backup recovery for critical industrial applications [22], [30].

Documenting and compliance seal the deal for incident response. Incident documentation and reporting are vital for legal, compliance, and forensic purposes. It is also good for the continuous learning efforts, but also for transparency in the organization. Having a detailed incident log with timestamps, affected systems, and remediation steps, but also reporting major security incidents to regulators, aligns with compliance efforts. The recommendation is to maintain structured incident reports but also have incident documentation as part of vendor security responsibilities [33], [35]. Compliance with regulatory requirements means ensuring

that software incident response processes comply with industry regulations and standards. Recovery policies should align with business continuity and NIS2 requirements, and you should maintain audit logs for security controls applied during incidents [16]. ISO 27001 requires compliance with cybersecurity policies for incident response [18]. Incident response and recovery for software applications ensures that organizations can detect, mitigate, and recover from software-related security incidents early on and effectively. Implementing robust detection systems, structured incident response plans, and reliable recovery processes can minimize downtime and enhance an organization's cybersecurity resilience.

5.3.9 Third-party and Supplier Software Security Management

Third-party and supplier software security management ensures that the software we acquire from external vendors, contractors, or open-source repositories meets security requirements before implementing it into IT and OT environments. Mitigating risks such as supply chain attacks, insecure dependencies, and unauthorized software modification in critical environments is essential. Supplier security management ensures vendors follow security best practices in software development and deployment. In contrast, third-party software security management evaluates, monitors, and secures software from external vendors. The importance lies in preventing supply chain attacks like Kaseya and Log4j, unauthorized software modifications, outdated components, and backdoors, and ensuring regulatory compliance.

The third-party and supplier software security management starts with vendor risk assessment and security evaluation. Assessing security risks associated with third-party software providers ensures that security requirements are met. This could mean conducting vendor security audits to ensure compliance with IEC 62443 standards or asking suppliers to complete security questionnaires before procurement. The industrial standards define security requirements for suppliers of industrial software, but also IT standards advise on third-party security risk management [24], [35]. Defining security clauses in contracts for third-party software suppliers is essential to fulfill the security requirements. In practice, this could mean requiring vendors to provide a software bill of materials listing all dependencies, including service-level agreements for patching vulnerabilities, or mandating compliance with secure software development lifecycle principles. Integrating security clauses in vendor contracts is highly supported, and in industrial environments, it is recommended to have secure software development lifecycle practices from suppliers [24], [37].

While supplying software is quite simple, so is changing the software during delivery. Ensuring software integrity during delivery is essential. This could mean requiring digital signatures for software executables to verify authenticity or using hash verification to confirm file integrity before installation. Software integrity verification is essential in industrial environments, but also for incident management, as it is used to check integrity and detect unauthorized modifications [17], [33]. Open-source software security management aligns with software integrity verification. Assessing and securing open-source components that are used in third-party software is highly recommended. It is encouraged to proactively monitor third-party software for vulnerabilities and securely integrate external software components [29], [31]. Open-source software security management is exactly that – Utilizing software component analysis tools to scan for known vulnerabilities and maintaining open-source policy that defines approved repositories and licensing compliance.

The secure deployment of third-party software is as essential as any other point. Implementing security controls before deploying third-party applications is part of deploying software with secure configurations. Controlling third-party software access in industrial environments and deploying it with secure configurations is crucial [22], [24]. Practically, this means performing static and dynamic application security testing before deployment, applying zero trust architecture principles to isolate third-party applications, and restricting third-party software execution. Regarding security, it is also essential to have third-party applications patched and updated. This could mean establishing a third-party patch management policy that would require vendors to provide updates within, for example, 30 days of vulnerability disclosure. There are a lot of ways of handling this, like regular software audits or virtual patching. Timely patching of third-party software vulnerabilities is recommended, along with vulnerability remediation for external software used in industrial environments [22], [24]. Like regular audits help detect unpatched third-party applications, we should also have monitoring and threat detection for third-party software. Integrating third-party applications with security information and event management systems is one way to go, as well as using endpoint detection and response solutions to monitor third-party software activities. Real-time monitoring of third-party software application risks is encouraged in terms of incident management, and it is recommended to log and monitor external software in industrial environments [23], [31].

Implementing security measures for third-party and supplier software can be a bit tricky. However, there are solutions for this, and Zero Trust is highly recommended. This would mean assuming that no third-party software is inherently trustworthy in IT and OT environments. In

practice, this could mean implementing network segmentation to isolate third-party applications from the core operational networks or implementing MFA for access to third-party software management interfaces. Industrial standards highly support the principle of least privilege for third-party software [22]. While ensuring our environment handles these programs accordingly, we also need to ensure that software suppliers follow secure software lifecycle processes. This could mean requiring vendors to follow IEC 62443 secure development lifecycle practices and auditing software supply chain partners to ensure secure coding and testing standards. A secure development lifecycle is essential in industrial environments, but for IT environments, it is also required for organizations to verify supplier security measures [18], [37]. If we require something from suppliers, we should also be ready to verify their actions. Regularly auditing and assessing vendor security compliance, for example, annually, could help with third-party risk assessments. This could also mean requiring vendors to provide certifications as proof of security compliance. In industrial environments, suppliers are required to undergo cybersecurity audits, and periodic third-party risk assessments are recommended [24], [35].

However, we still need to verify our handling of third-party software providers with a policy. Defining clear security policies for third-party software helps organizations align with the understanding of what is crucial and why we should handle third parties differently. This means developing a third-party risk management policy with specific approval processes for software acquisitions. It also means maintaining a vendor security requirements document that would outline acceptable security controls for the organization. Standards often require formal security policies, but also underline the business's efforts towards a safer environment [18]. Third-party and supplier software security management can greatly mitigate risks associated with external software providers, which is often a lot. By implementing vendor risk assessments, software integrity verification, continuous monitoring, and secure deployment policies, organizations can align with standards but also ensure the security of third-party software.

5.4 Redundancy Domain: Ensuring Availability and Failover

The redundancy domain focuses on ensuring the availability and resilience of industrial IT/OT systems through duplication, failover mechanisms, and robust network and infrastructure design. Given the criticality of continuous operations in industrial environments, minimizing single points of failure is essential to maintaining service continuity and reducing operational risks.

This section references high-availability concepts from IEC 62443-3-3, redundancy principles from IEC 61850 within industrial control systems, and selected insights from academic research into SDN applications for industrial contexts. It addresses strategies such as redundant networking, failover paths, clustered server architectures, and resilient communication frameworks.

By implementing structured redundancy at the network and system layers, organizations enhance their capacity to withstand faults, targeted attacks, or environmental disruptions, thus supporting operational reliability and cybersecurity resilience.

5.4.1 System and Network Redundancy

Redundancy in systems and network design ensures that critical functions remain operational despite failures or disruptions. This principle is vital for OT environments, where uptime is crucial for safety and operational continuity. I've broken this down into four main categories: system redundancy, network redundancy, failover mechanisms, and periodic testing and validation. The redundancy benefits are pretty clear – Enhanced availability, improved resilience against single points of failure, and business continuity. By focusing on this aspect, we can build a robust framework for the continuous operation of OT and IT systems from an industrial point of view.

System redundancy refers to duplicating critical hardware, software, or systems to maintain factory operations in case of component failures. This means redundant SCADA servers, database clusters, and storage arrays; for controllers, backup PLCs to take over the control functions if the primary PLC fails, and for power supplies, this will mean dual power supplies or uninterruptible power supplies for critical systems to avoid power-related downtime. Application of the principle might not be that simple in legacy operational systems, but this could mean hot standby PLCs that immediately take over control of the operations without manual interventions or mirrored data storage for SCADA systems to protect the data integrity. Redundancy is recommended, especially for ICS architectures, but it should be applied to any critical system at the factory [22], [24]. It is advised to take proper measures to ensure the availability of critical information systems [22], [24].

Network redundancy always ensures uninterrupted communications by using alternative network paths or redundant communication links. Redundancy is often discussed as a part of maintaining the availability of critical network services [24]. This could mean failover-

configured switches and routers take over during hardware or link failures. It could also mean using multiple communication lines between OT devices and control systems to ensure connectivity in case of path failure. Rapid Spanning Tree Protocol (RSTP) is recommended because it prevents network loops while also providing redundancy by rerouting data if a path becomes unavailable. The Media Redundancy Protocol is often used in industrial Ethernet networks for rapid failover between redundant paths. We should design control networks with redundant rings or star topologies to prevent single points of failure. We should also use redundant gateways for secure and continuous IT-OT integration. Highlighting the importance of secure and redundant network designs supports system resilience, but redundancy should also be a part of a broader strategy to maintain the availability of critical infrastructure [22].

Failover mechanisms are also a critical part of system redundancy and are often emphasized to be used to minimize disruption during outages [30]. Failover mechanisms allow systems or networks to automatically switch to backup components in case of failure, minimizing downtime. In networks, RSTP is a type of protocol that helps with failover mechanisms. There are a couple of ways of handling failover mechanisms: one is active-passive failover, and the other is Active-Active failover. In the case of Active-Passive failover, a secondary system is idle but ready to take over when the primary system fails. In active-active failover, multiple systems operate simultaneously, sharing the load, with one taking over fully if another one fails. These can be implemented in OT by having SCADA servers with an active-passive cluster to ensure continuous availability or by deploying redundant network paths in the factory for PLC communication links.

While implementing these failovers and redundancy operations, we must ensure that the systems and redundancy mechanisms function as expected and meet operational expectations and requirements. This is done by regular failover drills for redundant PLCs, SCADA systems, and overall systems. We can also simulate network disruptions to validate alternate communication paths to critical points. Testing seals the deal for redundancy; it should be a part of the security and availability controls of the organization, and testing is also crucial for maintaining industrial cybersecurity programs and tests [23], [24].

5.4.2 Disaster Recovery Planning

Disaster Recovery Planning (DRP) ensures that critical systems, data, and operations can be quickly restored after a disruption. Planning ahead minimizes downtime and prevents long-term impacts, especially in OT environments where continuous operation is crucial. Disaster

recovery planning involves creating a structured approach to restore operations and systems after a major disturbance. These major disturbances can be anything form cyberattacks to natural disasters or equipment failure. SCADA systems and PLCs often require immediate recovery to avoid production halts or safety hazards. Having a disaster recovery plan also ensures that the company is compliant with industry standards and guarantees customer expectations for high availability and reliability [22], [30].

The core components of disaster recovery planning are data backup and restoration, system redundancy, and disaster recovery sites. Disaster recovery sites ensure that the company can continue operations regardless of one site being lost, and standards provide guidance on how to set up recovery sites as part of a comprehensive Disaster Recovery Strategy [30]. Recovery sites can be hot, warm, or cold depending on the recovery time objectives. Co-operation with the organization is required to set realistic expectations for disaster recovery, and defining Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) is crucial. Redundant systems and components enable operations to continue while primary systems are being restored. This is a point being highlighted for a broader part of the disaster recovery strategy for industrial cybersecurity. A disaster recovery plan includes having these failover servers and duplicate PLCs so that the operations can continue regardless of the situation. Data backup and restoration require regular backups of critical OT data, including configuration files, control programs, and system logs. Ensuring backups are securely stored off-site or in cloud environments for accessibility during local disruptions. Forming a backup and restoration policy is crucial for the continuation of operations and is part of business continuity management. Business continuity and industrial standards highlight the importance of backups as core components of business continuity and to maintain operational integrity [22], [30].

Incident detection and escalation are highlighted in disaster recovery planning. Proactive monitoring helps organizations detect potential disruptions before they escalate further. A proper incident response framework also enables organizations to define escalation procedures that clearly specify roles, responsibilities, and communication protocols for responding to incidents. Breaking down incident response into processes that can be integrated into disaster recovery plans ensures timely action during disruptions without causing disorganization. Information security standards outline the need for detailed incident response processes, which are integrated with disaster recovery plans to ensure timely action and mitigation [31], [33].

While incident detection and escalation play a significant role, so do the testing and validation of the disaster recovery plan. Regular simulations of disaster recovery can help the organization with the validation of the disaster recovery plan. Still, it can also help to identify gaps and update the disaster recovery plan processes. Conducting routine disaster recovery drills tests the effectiveness of backup and restoration procedures and helps the organization set expectations. Simulating scenarios like ransomware attacks, equipment failure, and natural disasters can help organizations prepare in multiple ways and expand their disaster recovery plan. Periodic validation is seen as a crucial part of maintaining the effectiveness of disaster recovery routines, and the testing is also stressed in terms of business continuity and disaster recovery readiness [24], [30].

How we handle disaster recovery depends highly on the recovery time and point objectives. The business continuity standard also highlights these methodologies for determining correct recovery time objectives and recovery point objectives, which serve as indicators for businesses to determine the importance of a system [30]. For example, recovery time objectives define the maximum acceptable downtime for a system. The recovery time objective guides the actions based on the system's critical rating. The recovery point objective identifies the maximum tolerable data loss during a disaster. This determines how often backups are made and how storage is being handled. Determining these is crucial for the organization and would be a good approximation regardless of the disaster recovery planning. Using these methodologies, you can set the expectations for service level agreements and other organizational processes to align better in the case of incidents.

Integrating a disaster recovery plan into a business continuity plan can help the organization move forward with a broader ideology. While disaster recovery is just a part of business continuity that is focused on explicitly restoring systems, a business continuity plan focuses on broader operational resumption. Industrial standards and information security standards provide their perspectives on the topic, as well as highlighting operational integrity during cyber incidents and recovery, and ensuring secure recovery processes post-incident [22], [24]. Ensuring collaborative work between IT, OT, and business management helps organizations achieve business continuity goals in the long run. In addition, including ransomware recovery measures such as offline backups and secure restoration protocols in the disaster recovery plan can help organizations better prepare for a ransomware incident, regardless of its severity. Implementing redundant pathways and access control systems to reduce vulnerabilities during recovery is also recommended.

All in all, the disaster recovery plan boils down to documentation and communication. Maintaining clear, comprehensive documentation of disaster recovery plans, different scenarios, step-by-step procedures, contact lists, and resource requirements builds confidence in the business's continuity, even in the case of disasters. Defining communication strategies to inform stakeholders and coordinate recovery actions during a disaster can make a huge difference. In the 2024 NIS2 regulation, it is mandated that critical infrastructure organizations must establish business continuity strategies, have sufficient incident handling, and report incidents within 24 hours, with a detailed incident notification within 72 hours [16]. The upcoming regulations and the standards in the past highlight the importance of documenting and communicating as a part of disaster recovery planning [16], [24]. And it can be seen as a foundation for it.

5.4.3 High Availability Systems

High availability refers to systems and components engineered to deliver reliable performance and continuous operation. Continuous operations are often measured as a percentage of uptime, but 99% is usually insufficient for critical systems. In OT networks, downtime could cause serious production halts, safety risks, or financial losses. If we look at 99% of uptime, the services are down daily for 14 minutes and 24 seconds. Yearly, that would make over three and a half days of downtime. If the downtime comes at unpredictable times, this could mean three days of work time lost in a year. Financials are not excellent on that, but what about the safety risks this might cause? If we cannot trust a system, should we trust our lives with it? If we added 0.99% to that uptime, we would reduce the yearly downtime to 52 minutes from three and a half days. High availability ensures seamless operations, especially for OT systems.

The core components of high-availability systems can be broken down into two parts. One is a redundant system design, which ensures redundant components, and the second is redundant network paths. Redundancy is generally highlighted in network design and industrial standards as a part of cybersecurity management and business continuity, which are recommended when designing industrial control systems and critical operations [22], [23], [24]. These are the same components that we explained earlier. High-availability services should always have redundant components throughout the architecture to ensure an uninterrupted operation, but the same goes for network paths. If one path of communication fails, we need to be able to keep the data flowing within the OT network with redundant pathways.

As well as redundant components, the same goes for failover mechanisms in high-availability systems. A secondary or backup system that automatically takes over the system must be installed when the primary system fails. Often, in the IT world, this can be a failover DNS server for continuous network communication. In terms of automation, this could be a hot standby PLC to ensure uninterrupted control. Failover mechanisms are generally emphasized as part of business continuity planning [30]. Clustering services can also handle failover. Clustering involves multiple systems working together to appear as a single system that shares the workload. When there is a failure in one node, the other will continue to maintain the workload. This can be seen as an active-active way of handling redundancy. Industrial standards support clustering as part of system-level redundancy strategies and are often implemented in industrial settings [22].

High-availability systems rely heavily on consistent and up-to-date data across systems. This is achieved by synchronization and backups. Practical examples of this can be seen in the synchronization of SCADA databases across redundant servers and with the use of RAID configurations in workstations. RAID configurations offer redundant workstation storage with data mirroring across the hard drives. Industrial standards stress that data synchronization and backup are essential for an organization's resilience, while including data integrity and availability are the key elements of high availability system design [22], [30].

Regular testing is essential to ensure that high-availability systems operate as intended during unexpected failures or disruptions. Organizations should not shy away from rigorously testing their failover mechanisms; instead, they should treat it as a proactive strategy to validate system resilience. Simulating failover scenarios under controlled conditions not only helps identify potential weaknesses but also builds confidence in the robustness of the implemented architecture. This is particularly critical in industrial environments such as factories, where Supervisory Control and Data Acquisition (SCADA) servers and redundant systems are expected to deliver uninterrupted operation. By conducting routine recovery drills, organizations can assess and refine their response capabilities in the face of disruptions, whether they stem from hardware malfunctions, software errors, or network outages. These exercises are invaluable in validating uptime objectives and ensuring that redundancy mechanisms function correctly when needed most. Regular testing plays a crucial role in supporting broader business continuity strategies and strengthening cybersecurity postures, aligning with established business continuity standards, such as ISO 22301, as well as industrial cybersecurity frameworks like IEC 62443 [23], [30]. These standards emphasize the importance of validating

system behavior under stress and ensuring that operational processes can withstand and recover from adverse events.

The availability metrics for high-availability systems mean that a metric is followed for system optimization and understanding the performance of high-availability systems. Setting up metrics like Mean Time Between Failures (MTBF) and Mean Time To Recovery (MTTR) helps organizations measure system reliability and recovery efficiency. Information security standards typically emphasize the use of availability metrics for system optimization [24]. Automating human processes can also help to reduce human error and ensure rapid recovery during system failures, which is also promoted by industrial standards [22]. Automating failover configurations for redundant servers could be handled with automation, such as scripting to restore network connections in the case of a path failure. Implementing automation can enhance redundancy and reduce the IT/OT team's manual intervention in production.

5.4.4 Data Backup and Restoration

Data backup refers to creating copies of data or configurations for safekeeping, while restoration involves retrieving the once-backed-up data and resuming operations after a disruption. OT operations are critical, and backups are there mainly to prevent data loss from unexpected incidents like ransomware attacks, hardware failures, or misconfigurations. With data backups and restoration, we are trying to ensure rapid recovery of critical systems, minimizing downtime. By following the principles of the standards, organizations can achieve robust, secure, and effective backup and restoration strategies tailored to their needs.

The core data backup and restoration components are backup frequency and scheduling, backup types, and storage location. If we start with backup storage, backups should be stored securely in multiple locations to protect against localized disruptions. With On-site backups, we can prioritize faster recovery of minor incidents, and the usage could be more frequent. With Off-site backups, we could protect against site-wide disasters. Generally, it is recommended to have diverse storage for critical geographical backups [24]. A common saying is that having three copies of your data on two different media types and at least one copy kept off-site is recommended. Different backup strategies address various operational needs – we can classify these into three types: Full Backup, Incremental Backup, and Differential Backup. Full backup stores all data and configurations, ideal for periodic comprehensive backups. Incremental backup saves only data that has changed since the last backup, reducing storage requirements and backup times. Differential backup captures changes since the previous full backup,

balancing the storage use and recovery speed. Diversified backup strategies enhance the organization’s resilience, and setting up different strategies can make the organization more agile [30]. Then, how often these backups are taken depends on the business. Regular backups of critical systems and data are recommended when they help with system integrity and availability [22], [24]. Regular backups are essential to minimize data loss and ensure that recent system states are recoverable. Using modern technologies can streamline and enhance the backup processes [24]. For example, snapshot-based backups rapidly capture system states at a specific moment. Cloud-based solutions can offer scalability and off-site storage, while deduplication techniques enable optimized storage usage [24].

Regardless of the backup strategies, restoration processes ensure that the backups taken can be quickly and reliably used to resume operations. Predefining restoration workflows that include roles, tools, and timelines helps the organization achieve a successful restoration. Testing restoration processes regularly ensures data integrity and compatibility and offers IT teams good practice in the case of data loss. The documented and tested restoration process ensures operational continuity, and detailed recovery planning minimizes the hassle and, thus, the downtime, and is recommended [23], [24]. While the recovery process is important, it is also important to have the backups secured from unauthorized access, corruption, and theft. The security of the backups is as important as anything. Encrypting data to safeguard it from unauthorized access and ransomware is recommended, and strict access controls restrict backup handling to authorized personnel [22], [24]. Preferably, use the principle of least privilege in the process.

Testing and backup were already mentioned, but regularly testing backups ensures that they are functional, Sufficient, and compatible with the systems. Performing restoration drills would be good practice for critical systems and their configuration. Validating the system can save you time in the case of an accident and ensure that the incremental backups can be combined with full backups, and seamless restoration can be achieved regardless of the scenario. Testing different combinations of scenarios can help IT teams communicate and train them to be less dependent on a single person. Organizations' business continuity plans should emphasize validating backup and restoration processes through regular testing scenarios [30]. Testing recovery is again a critical part of maintaining cybersecurity readiness in an organization [23].

Integrating backups into disaster recovery planning is crucial, just as everything that comes to business continuity is. Backups are central to disaster recovery strategies as they ensure that

data and systems can be quickly restored after a major incident. Aligning backup schedules to match the Recovery Point Objectives (RPOs) determined in disaster recovery is crucial to ensuring smooth disaster recovery. Also, integrating workflows with broader disaster recovery processes is recommended. ISO 27035 connects backup and restoration with incident response plans and facilitates rapid recovery during cyber incidents [31], [33]. Business continuity standard ISO 22301 recommends maintaining thorough documentation as a part of business continuity [30]. Well-maintained records of backup schedules, methods, and restoration attempts make an excellent foundation for backup processes. All restoration attempts, including time taken and success rate, are essential for review and improvement of the process. If an organization cannot trust the backup and restoration efforts, there is no point in having them. Specifying the need for backups for various solutions is crucial for continuity.

5.4.5 Incident Response and Business Continuity Integration

Incident response is a structured approach to detecting, managing, and resolving security incidents to minimize impact on the organization's operations. As OT systems often control critical infrastructure in manufacturing plants, downtime or a compromise could result in safety risks or economic loss. Integrating redundancy functions into incident response can help the business with business continuity efforts while threats are being mitigated. Business continuity aims to ensure the uninterrupted availability of critical functions and systems during and after a disruption.

The core components of incident response and its integration into business continuity are basically a unified response and recovery framework, and risk assessment and prioritization accordingly. Organizations should strive to establish a unified framework for incident response and business continuity, ensuring a coordinated approach to managing disruptions. A practical example of this could be an incident response plan that triggers automatic failover mechanisms to maintain system availability and redundant connection paths to systems during the incident resolution phase. Business continuity also promotes the alignment between incident response and continuity strategies, while ISO 27035 provides a framework [31]. For risk assessment, the organization needs to be able to identify and prioritize critical systems to ensure redundancy mechanisms and, in this way, ensure that continuity measures are focused on high-impact areas. Industrial standards recommend the practice, especially for shaping redundancy and continuity strategies [23]. This could mean doing yearly risk assessments to classify systems by criticality

and assigning redundant resources accordingly. Reporting and communication can be set beforehand, so everyone knows where to find information during disruptions.

Effective incident detection should be triggered by default redundancy mechanisms, ensuring continuity while resolving the problem. This could involve using automated scripts to switch communication paths during network anomalies or utilizing intrusion detection systems that can initiate failover to redundant systems when a threat is detected. This is part of monitoring and redundancy, but having redundancy as part of the incident handling process can significantly benefit businesses by utilizing their redundancy infrastructure [22], [24]. Leveraging redundant systems is often overlooked. Incident response procedures should include actions for managing and validating redundant systems during disruptions. In practicalities, this could mean anything from a check-up procedure to validate the redundant systems before initiating failback to the primary component, to switching operations to backup servers or PLCs while investigating and resolving issues with primary systems. Usage and involvement are the keys to redundant systems. As we increase the usage of redundancy mechanisms in incident response, we are also integrating the process into business continuity and minimizing downtime during incidents [33]. Regular testing of the redundancy mechanisms can be reduced if the systems and mechanisms are used actively. Of course, testing and conducting specific drills to involve the failover scenarios are recommended, which can also improve the incident response actions [23], [30].

As long as communication and coordination are handled well and redundant communication tools are used to maintain coordination during a system's failure, incident response can be quick and thorough. Implementing secure communication channels for incident management teams is beneficial, but also ensuring that you do not prioritize just one channel is crucial to maintaining business continuity [24]. After incidents, it is recommended that the team analyze incidents to refine the integration of redundancy, incident response, and continuity strategies [33]. This can help the team review the performance of redundant systems during incidents and identify gaps or delays in activating the redundant systems. Revisiting the incident can also help teams update response plans to address the weaknesses observed during the incident. Post-incident analysis is a great way to improve response and continuity measures. Finally, integrating the redundancy measures with business continuity management ensures that the critical systems in the organization's operations are covered [30]. It can be anything from simple redundant power supplies and communication paths to secondary SCADA servers that activate

automatically during hardware failures. Integrating and involving technical measures to ensure business continuity is an easy way to improve business resilience.

5.4.6 Supply Chain and Vendor Continuity

In supply chain and vendor continuity, we focus on ensuring that critical components, services, and materials provided by third parties remain available regardless of disruptions. Generally, we have specialized hardware, software, and support services in OT. There is a clear need for business continuity to ensure redundancy in supply chain processes and vendor relationships. In supply chain and vendor continuity, we define strategies to mitigate risks associated with vendor dependency and ensure availability. Especially in the industrial environment, we want to focus on essential hardware such as PLCs, SCADA components, and specialized hardware. By doing this, we reduce the risk of operational downtime caused by delays in receiving critical components or vendor support.

Supply chain and vendor continuity consist of diversification of vendors and vendor risk assessment. Engaging multiple vendors for critical components and services reduces the dependency on a single supplier and enhances resilience against supply chain disruptions [30]. Ensuring you can source PLCs and control system components from two or more manufacturers with compatible specifications would be beneficial. Establishing relationships with local and global vendors can address geographic disruptions for the organization. Through vendor risk assessment, organizations can evaluate the reliability and resilience of vendors to ensure they meet requirements during disruptions, a practice often advocated as part of supply chain security methods [24]. Assessing the supplier's financial stability, redundancy in their supply chains, and disaster recovery capabilities helps mitigate the risks within the supply chains. Regular vendor risk assessments can be seen as a part of supply chain security.

Managing the supply chain is one thing, but organizations should also manage their inventory and stockpiling. Maintaining solid stock levels of critical components would ensure that even during supply chain disruptions, the organization has already invested in parts and can utilize the parts from inventory. Stockpiling critical parts for OT systems, like sensors, actuators, and communication devices, is often highlighted to support continuity efforts [23]. Inventory should be monitored and maintained, and the market should be monitored in cases of more extended shortages. Having that additional supply chain helps in retaining that inventory of critical supplies. Identifying and contracting backup suppliers for necessary hardware and services is not going to hurt organizations; it will make them more ready for the future. The work

beforehand to see if the supplier meets quality and compatibility requirements would be good. Establishing supply chains mitigates the risks from single supplier dependencies [30].

Contractual and service-level agreements ensure vendors' commitment to defined service levels even during disruptions. Including clauses for disaster recovery support, guaranteed delivery times, and penalty provisions for SLA failures is generally seen as a good practice. In a contract, an organization can require and support suppliers to maintain their redundancy mechanisms. Incorporating security and continuity requirements into vendor agreements is generally recommended and approved best practice [24]. Vendors should also be regularly assessed to ensure alignment with continuity objectives and KPIs. KPIs are a good way to evaluate vendor reliability, delivery times, and incident response efficiency. Monitoring vendors' performance and evaluating the alignment with business goals is recommended [24]. While assessing suppliers, it is also good to ensure the alignment with organizational needs in the business continuity plans. Sharing critical requirements, such as minimum stock levels and response times, with vendors is viewed positively [30]. If vendors deliver services, it is good to join a continuity planning exercise to validate alignment and readiness with suppliers.

Leveraging technology can also help with supply chain security, management, and continuity. Implementing supply chain management software to track orders, predict shortages, log inventory, and identify alternative suppliers is recommended. Most organizations have ERP and purchase management systems, which can be leveraged to become a supply chain management system. Naming inside the ERP might vary depending on the software. It is also good to predefine emergency sourcing protocols for sourcing critical components and services of the production. This can be anything from a simple list of approved vendors for emergency procurement to establishing a fast-track approval process for alternate suppliers. Establishing emergency sourcing protocols is seen as a vital part of continuity planning [30].

5.4.7 Critical Systems Testing and Validation

Critical systems testing and validation ensure that the redundancy mechanisms we set in place work as intended during disruptions. In OT environments, regular testing and validation are essential to maintaining the reliability of production plants. Simple tests can reduce downtime and ensure a seamless transition between primary and redundant systems. For OT, the importance lies primarily in activating failover systems, validating the integrity and performance of redundant systems, and identifying gaps and weaknesses inside redundancy strategies before incidents occur.

As core components, we define system integrity checks, performance tests, and redundancy validation as the most crucial elements in OT. System integrity checks verify the integrity of redundant systems' configurations, data, and components. This involves testing the synchronization of PLCs with real-time data from primary systems and checking the data consistency between separate controlling machinery or SCADA servers. Integrity checks confirm the effectiveness of redundancy mechanisms and ensure data and system reliability, which should be highlighted [23]. In terms of performance testing, we assess the performance of critical systems under redundant configurations to ensure they meet operational requirements [24]. This includes load-testing SCADA systems during failover scenarios to maintain performance metrics from both an internal and supplier perspective. During testing, we should also simulate high network traffic on redundant communication paths to verify throughput to critical systems and ensure the low latency required by operational systems. Finally, for redundancy validation, we must ensure that all redundant systems can take over seamlessly during failures. An unnoticed transition is challenging to achieve, but ensuring that operations can continue regardless of the production phase is essential for operational technologies. Testing failover PLCs, connections, and management device failures is an effective way to validate redundancy measures. This also allows development teams to enhance their processes and move forward. The validation of redundancy mechanisms, performance testing, and system integrity checks are all proposed standards for ensuring good system availability during disruptions [22]. Proper testing strategies also assist the organization in forming a business continuity plan in a long-term environment [30].

Scenario-based testing is a good way to simulate real-world scenarios to evaluate the readiness of critical systems. Practically simulating a network failure to test the automatic activation of redundant connections is recommended, and performing power failure drills to evaluate UPS and redundant power supplies is preferred. Encouraging scenario-based testing ensures readiness inside and outside the factory. Diversifying failure scenarios can build resilience within the organization and ensure that necessary monitoring and protocols are in place safely [30]. Overall, backup validation and restoration settings have a place in scenario-based testing. Restoring configurations from recent backups in different scenarios can ensure their usability in real-world scenarios while providing recovery times against predefined recovery time objectives. Regular validation, testing, and restoration support availability management should be considered when managing critical systems [24]. Regular testing schedules are also preferred to ensure the ongoing readiness of redundant systems. This could be monthly or yearly as long

as the schedule is there. Conducting failover drills regularly ensures that operations have a guarantee that continuity and redundancy measures are functioning as intended [30].

Tools and automation are also recommended to streamline testing and ensure consistency between the tests. Practically deploying monitoring tools that can simulate network failures and evaluate failover mechanisms. Automated scripts can test the synchronization between servers and databases and prove that the redundancy measures are working. Overall, utilizing technology in testing can prove compelling and help the organization move forward [24]. Post-test review can help the organization identify weaknesses in the redundancy strategies and move the organization towards necessary improvements [33]. Documenting each test result can help analyze activation times for redundant systems and assist with corrective actions. Generating standardized testing templates to document failover performance is recommended [30]. Compiling these reports to highlight the improvements in redundancy strategies over time can help businesses maintain an exemplary process for business continuity management. Adhering to standards can help a company with testing procedures and align the business with industry best practices.

5.5 Governance And Compliance Domain: Policies, Risk Management, and Regulatory Alignment

The governance and compliance domain establishes the management frameworks, policies, and oversight structures necessary to coordinate cybersecurity efforts across industrial IT/OT environments. Strong governance ensures that organizational processes support technical controls, while compliance mechanisms align operations with legal, regulatory, and contractual requirements.

This section draws from ISO 27001 for information security management systems, ISO 27005 for risk management, ISO 31000 for enterprise risk governance, and incorporates obligations from the NIS2 directive for critical infrastructure operators. It also aligns with organizational governance principles outlined in IEC 62443-2-1.

Emphasis is placed on defining roles and responsibilities, managing third-party risks, setting security objectives, and ensuring continuous improvement through audits and assessments. Effective governance and compliance practices are the backbone of sustainable cybersecurity resilience in complex, multinational industrial environments.

5.5.1 Security Governance Framework

A security governance framework establishes the policies, processes, roles, and responsibilities required to manage cybersecurity risks inside an organization and ensure regulatory compliance in industrial networks. With the Security governance framework, we aim to align organizations' objectives with cybersecurity mandates, providing a structured approach to risk management, compliance, and security oversight. International standards like IEC 62443, ISO 27001, ISO 31000, and NIS2 guide managing governance and outline principles to help organizations integrate cybersecurity into operational and strategic decision-making that ensures resilience against cyber threats while maintaining regulatory compliance.

The core principles are quite straightforward: a structured security governance framework should be based on four key pillars: leadership and commitment, security policies and compliance requirements, Risk management and Continuous Improvement, Accountability, and security oversight. Starting from leadership and commitment, Security governance must be led by executive leadership and enforced through clear policies, roles, and responsibilities. Risk management standards clearly mandate leadership commitment to risk management, ensuring that security is integrated into governance and decision-making processes [32]. Industrial standards specify that security governance must be integrated into ongoing processes, driven by executive management and operational leadership [23]. Next up are security policies and compliance requirements – organizations must develop and maintain a cybersecurity policy framework that defines security mandates, regulatory obligations, and risk mitigation strategies. ISO 27001 mandates that security policies are formally documented and aligned with business objectives [18]. Industrial standards also require organizations to define cybersecurity policies that establish security baselines, access control, and monitoring mechanisms for organizations [22].

Risk management standard ISO 31000 also emphasizes a risk-based approach to governance, requiring organizations to integrate risk management into governance, leadership, and strategy [32]. For organizational risk management and improvement, this would mean that security governance should be risk-driven, leveraging cybersecurity risk assessments to ensure that security measures align with business impact and criticality. This would ensure that decisions around cybersecurity are made with clear reasons for mitigating risks while aligning with business decisions. Industrial standards also require organizations to conduct risk assessments to define security levels for industrial networks, set control measures for environments to

mitigate the risks, acknowledge the environment's scenario, and ensure governance [17]. Finally, accountability and oversight – The organization needs to set clear security accountability and oversight roles that must be assigned across IT, operational grounds, and the organization's executive leadership. ISO 27001 requires organizations to set these security responsibilities and also establish oversight committees [18]. There should be accountable personnel to handle organizational security, preferably more than one, with an oversight committee that ensures topics are considered and managed. Industrial standards also mandate that asset owners, system integrators, and service providers maintain defined security roles and responsibilities inside and outside the organization [35].

The security governance framework must ensure compliance with global, national, and industry-specific cybersecurity regulations. For manufacturing organizations, this clearly signifies essential frameworks such as IEC 62443—Industrial Cybersecurity, ISO 27001—Information Security Management, ISO 31000—Risk Management, and the NIS2—EU Cybersecurity. Embracing these standards is crucial for robust security and risk management. Relevant to our security governance framework, industrial cybersecurity standards define industrial control systems requirements, including secure network segmentation, access control, and monitoring, as well as guidance for implementing security governance, defining roles, and establishing security policies [22], [23]. Information security management standards mandate the implementation of information security management systems, requiring organizations to document security policies, conduct risk assessments, monitor security compliance, and outline security controls, including access control, network security, and incident management [18]. Risk management provides governance principles for integrating cybersecurity into business risk management, ensuring security is embedded into the organization's strategic decision-making [32]. The EU cybersecurity directive mandates cybersecurity governance for critical infrastructure and industrial sectors, requiring organizations to implement proper incident response and reporting mechanisms, continuous monitoring and threat detection, and supply chain security requirements [16]. Regulatory audits, reviews, and third-party assessments support organizational compliance status and validation. Generally, it is recommended that processes be maintained for continuous evaluation and improvement. Security governance must ensure proper documentation of security policies, governance frameworks, and compliance documents while aligning with all mandates.

As mentioned already, continuous monitoring and incident response requirements are one of the requirements. Security governance must enforce continuous monitoring and incident

response readiness to detect and respond to cyber threats. This would mean implementing real-time monitoring, log correlation, and forensic logging to meet regulatory compliance requirements like IEC 62443, which mandates organizations to have continuous security monitoring [23]. When it comes to incident response and regulatory reporting, Security governance must enforce incident response plans that comply with Incident management standards, NIS2, industrial standards, and industry regulations. It is mandated for organizations to implement an incident response framework that ensures timely containment, investigation, and mitigation of cybersecurity threats [23].

A good security governance framework provides strategic direction, risk-based security controls, regulatory compliance, and incident response readiness for organizations while complying with standards. When properly implemented, the organization can establish a resilient and secure industrial environment, ensuring governance measures support practical implementation. Furthermore, aligning security governance with business objectives builds up a safety and security-first culture, where ensuring cybersecurity is not just a technical concern but a part of operational resilience and continuity. Regular assessments and continuous improvement initiatives help organizations to adapt to evolving threats, maintaining a proactive and preventative security posture.

5.5.2 Regulatory Compliance and Standards Alignment

Regulatory compliance and standards alignment aim to help organizations align with regulatory requirements and standard alignment with a structured approach. The ideology is to help organizations comply with regulatory frameworks while aligning with international cybersecurity standards. This dual focus ensures that organizations not only meet legal obligations but also adopt best practices to enhance their overall security posture. With this integration, organizations can better manage risks and protect sensitive information from evolving cyber threats.

Starting with a compliance framework for industrial networks, Organizations must establish a structured compliance framework aligning industrial cybersecurity with regulatory, legal, organizational, and contractual requirements. The key compliance areas could be Industrial automation and control system security (IEC 62443), Information Security management (ISO 27001), Operational resilience and business continuity (ISO 22301), Risk management (ISO 31000), Critical infrastructure cybersecurity regulation (NIS2), and Organizational cybersecurity policy. Industrial standards state that any relevant cybersecurity regulatory

requirement that applies to the system under consideration must be in the cybersecurity requirement specification [17]. With the aim of aligning organizational governance to cover regulatory requirements as well as the industrial standardization requirements. Information security management best practices are also used to ensure organizational compliance with legal, regulatory, and contractual requirements related to information security [18]. Forming a structured methodology to ensure compliance is highly recommended.

Risk-based ideology is another topic that follows standards in an organization's everyday business. Regulatory compliance mandates risk-based security zoning, requiring organizations to classify network zones based on cybersecurity risks. The risk-based approach does not end there, as risk management standards require examination internally and externally, including regulatory requirements and implementation of risk management in all parts of the organization [32]. This would mean risk assessments to define security zones and conduits, aligning security controls with compliance mandates to enforce the segmentation approach, and documenting and maintaining zoning records. Industrial standards mandate organizations to perform detailed risk assessments to determine required security levels for each network zone and conduit [17].

Security governance and policy compliance must be considered when we are talking about regulatory compliance and standards alignment. As previously discussed, a Security governance framework is what organizations must develop to align cybersecurity policies with compliance obligations across legal requirements, standards, and organizational requirements. Governance measures are required to define risk ownership and security responsibilities, integrate compliance requirements into IT-OT governance structures, and develop security policies that align with IEC 62443, ISO 27001, and NIS2, which are relevant to the organization's environment. Risk management standards require that governance structures ensure risk accountability and oversight to meet compliance obligations, while industrial standards also require that asset owners implement cybersecurity programs to align with regulatory and compliance requirements [23], [32].

Governance must also consider compliance with incident response and continuous monitoring regulations. Industrial standards state that organizations must implement security countermeasures that align with regulatory requirements, including real-time monitoring and incident response [17]. Incident response standards mandate the establishment of an incident response framework that includes regulatory reporting obligations [31]. Based on this, compliance frameworks must require organizations to maintain real-time security monitoring

and incident response capabilities. This, in practice, would mean implementing security information and event management for real-time monitoring, logging mechanisms, and log retention for forensic investigation and compliance audits, and alignment with incident response mandates that can be given by, for example, ISO 27035 and NIS2. From a governance perspective, this would mean including security monitoring in policies and ensuring they stay in place.

That's where auditing, compliance validation, and continuous improvement come in. Organizations need to conduct regular security audits to ensure they comply with cybersecurity regulations and internal requirements. Industrial standards state that asset owners must review and approve cybersecurity risk assessments to ensure compliance with security governance policies [17]. Information security management standards state that organizations must conduct compliance reviews to ensure security policies align with regulatory mandates [18]. Enforcement of compliance may involve conducting regular security audits to evaluate adherence to internal standards, IEC 62443, and ISO 27001. It also includes documenting security controls and governance frameworks for regulatory assessments, along with mechanisms for continuous improvement to respond to changing regulatory or policy demands.

A robust regulatory compliance framework goes beyond being a mere checklist; it is a crucial component of industrial cybersecurity on dynamic platforms. By aligning with global standards and regulatory needs, organizations enhance resilience, refine risk management, and maintain the protection of their vital infrastructure. Integrating governance, risk management, incident response, and ongoing monitoring not only bolsters compliance readiness but also elevates an organization's cybersecurity maturity. Conducting regular audits and adapting to changing regulations ensures security measures remain relevant and effective, thereby supporting sustainable compliance and industrial resilience.

5.5.3 Risk Management and Assessment

Risk management is a systematic approach to identifying, assessing, and mitigating organizational risks that might impact its objectives. The objective of Risk management and assessment is to ensure that cybersecurity risks in IT/OT environments are properly managed to protect industrial control systems, critical infrastructure, and operational resilience. Risk is defined in risk management as the effect of uncertainty on objectives, which can be expressed in terms of risk sources, potential events, their consequences, and their likelihood [32]. Industrial standards mandate OT environments to perform a cybersecurity risk assessment in

the system under consideration to identify the worst-case unmitigated cybersecurity risk that could result from the disruption of mission-critical operations, attaching the risk management into our framework for IT and OT environments [17].

The risk management framework and governance must first be built. Organizations must integrate risk management into their governance model to align with corporate strategy, regulatory mandates, and cybersecurity frameworks [32]. This means establishing a risk management framework that includes risk management in different processes across the organization, with consistent integration into all processes as well as the governance model. Industrial standards require organizations to compile a thorough and pragmatic list of potential threats to conduct a security risk assessment [17]. This implies that risk management processes must be integrated across all operational areas. With a Risk management framework, there also needs to be risk leadership and accountability. Top management must demonstrate leadership and commitment to risk management by issuing risk policies, allocating resources, and ensuring risk communication. This aligns with the standard requirement of integrating risk management into all organizational activities, allowing resources and ensuring proper communication [32]. Information security policies for risk management should be defined, approved by management, published, and communicated across the organization, which also applies to risk governance [18]. This would mean that risk governance must include board-level oversight of cybersecurity risks and compliance.

Risk identification and categorization are also being shed light on by governance. Risk identification involves systematically recognizing potential threats and vulnerabilities to business objectives, industrial control systems, and IT/OT environments. Identifying and categorizing risks would mean setting risk categories to include financial, operational, regulatory, technological, and security risks. It would also mean assessing risks that are associated with insider threats, supply chain vulnerabilities, and emerging cyber threats. Standards facilitate risk identification by helping to find, recognize, and describe risks that may either assist or hinder an organization in reaching its goals. Additionally, industrial standards mandate the creation of a list detailing potential threats to the assets found within the zone or conduit [17], [32].

Risk analysis and evaluation are vital components; they encompass understanding the nature and scale of risks by evaluating their probability, impact, and exposure. Risk likelihood and impact assessments are the beginning of this. Organizations must evaluate the likelihood and

potential consequences of identified risks. The risk matrix methodology is commonly used to assess threats ranging from low to extreme risk levels. The risk matrix works by assessing the likelihood of a risk and determining the harm severity of a risk. By placing these in the matrix, the organization can determine the severity of set risks. However, it is commonly known that organizations may need to create their own or tailor an existing risk matrix depending on the business scale and its impacts. Risk management standard states that risk analysis should involve a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls, and their effectiveness [32]. Industrial standards recommend risk assessments to compare risk to organizations' tolerable risk and, therefore, determine if mitigation is required [17]. Comparing initial risk to tolerable risk is also required – organizations must determine whether existing controls sufficiently mitigate risk or if additional safeguards are needed. While industrial standards recommend comparing the risk to a tolerable level, it also sets a comparison to understand set risks and accept them – not all risks have to be mitigated. Risk management standards recommend evaluating risks based on risk levels in established criteria to determine if additional risk treatment is needed [32].

Once risks have been analyzed, organizations must develop treatment plans to reduce the likelihood and impact through proactive security controls. This would mean implementing risk mitigation measures like Industrial networks must implement firewalls, IDS/IPS, encryption, and zero-trust architectures to mitigate cyber threats. Security controls should align with risk severity levels and be continuously updated based on shifting risk ground. Risk management standards recommend selecting the most appropriate options for reducing risk while considering the effectiveness of the set options and resource allocation [32]. This means that organizations select the best viable option to mitigate the risk effectively without using too many resources. Industrial standards also mandate organizations to identify and mitigate cybersecurity risks for risks that exceed acceptable levels [17].

Finally, Risk monitoring and compliance audits are essential parts of risk management processes as well. Risk management is an interactive process that requires continuous monitoring, reassessment, and compliance audits. It's explicitly stated that monitoring and review should be planned and incorporated into all steps of the risk management process to track effectiveness and detect risks [32]. This would mean having ongoing risk monitoring and reporting methodologies so that organizations can periodically evaluate their risk management framework to align with emerging threats and possible changes to the environment. Automated security monitoring tools are also recommended to continuously assess risks in the

environment, meaning security information and event management systems, threat intelligence feeds, or network anomaly detections. Industrial standards also mandate documentation and communication of the results of risk assessments to key stakeholders for governance and compliance reasons [17].

Effective risk management is essential for securing industrial control systems and critical infrastructure. Organizations can proactively protect against cyber threats by systematically identifying, assessing, and mitigating risks. An integrated risk management framework ensures alignment with corporate strategies and regulatory requirements. While not all risks require mitigation, organizations should establish acceptable risk levels and treatment strategies based on security priorities. Risk treatment is a continuous process, necessitating ongoing monitoring and compliance audits. Effective risk management involves strategic leadership, governance oversight, and technical safeguards, ultimately enhancing security and ensuring long-term protection.

5.5.4 Policy Development and Enforcement

Defining cybersecurity policies for IT and OT environments can be a bit tricky. Effective governance starts with clear, management-approved security policies that cover both IT environments and OT environments. For IT environments, we focus on standards like ISO 27001, which requires that top management establish an information security policy that sets objectives and commitments for the organization [18]. For OT-centric environments, we must focus on standards like IEC 62443 that stress the need for an OT security management system that provides organizations with policies, procedures, and best practices tailored for industrial control systems, which could mean site-specific policies [17]. Together, the policies must address the unique requirements of corporate IT systems and industrial OT systems while ensuring the security of environments and enforcement across organizations.

The standards also offer governance models for security policy implementation. Adopting recognized frameworks provides a structured model for developing and implementing security policies. Picking from our standards for IT and OT, they offer a well-defined governance structure for both sides. Utilizing the standards helps organizations to build robust governance structures for cybersecurity management [17], [18]. Governance structures are often established per standardization efforts for information security management systems or for OT per industrial cybersecurity management systems to ensure that policies are systematically rolled

out and maintained across the enterprise. Risk management standards also state that governance provides the rules, processes, and practices needed to achieve an organization's purpose [32].

Regulatory requirements should be included in policy frameworks and the creation of policy frameworks as well. Cybersecurity policies should incorporate and reflect relevant laws, regulations, and industry mandates. In information security standards, it is mandated that policies reflect a commitment to satisfy other requirements related to information security, ensuring legal and regulatory obligations are built into the governance framework [17], [18]. Legal mandates are also forced upon from NIS2, which mandates that organizations' risk management measures include policies on risk analysis and information security, which underscores that regulatory requirements must be molded into internal policies from the start [16]. Aligning the corporate policies with standards and regulations provides consistency and legal compliance across the environments.

Once policies are in place, organizations must enforce them through controls and procedures. This involves a combination of technical measures like firewalls, network segmentation, access control systems, and monitoring tools, with administrative measures like procedures, training, and audits to ensure adherence to those standards. Industrial standards recognize that cybersecurity measures are a combination of technical and non-technical measures [17]. In practice, this means implementing tools that automatically enforce rules like password policies or network access rules, as well as management oversight like approval procedures and training to uphold the security policy in IT and OT environments. Industrial standards also mandate that security policies have to define and enforce authentication, access control, and user management requirements [17]. Which again just highlights the need to ensure compliance with a combination of technical and administrative points.

As already covered, effective enforcement covers areas like network protection, user access, and continuous monitoring. Organizations should aim to deploy policy-driven network segmentation and firewall rules to isolate critical OT networks and critical IT assets as well. Access control policies must be strictly applied – for example, NIS2 calls for human resources security, access control policies, and asset management as baseline measures in the directive [16]. The strict access control measures are also mandated by information security and industrial standards that require role-based access control with the least privilege principles[17], [18]. This means enforcing least privilege access, multi-factor authentication, and strict account management to ensure compliance with policy. Monitoring and detection mechanisms are also

mandated to be used to watch for policy violations or incidents to ensure compliance continuously [18]. These technical controls are guided by policy and ensure that the rules on paper are actively upheld in day-to-day operations.

Enforcement extends to how organizations prepare and respond when incidents or non-compliance occur. Cybersecurity policies should define incident response plans and remediation actions so that when a breach or policy violation happens, there is a clear, enforced process to address it. Industrial standards and NIS2 reinforce this – NIS2 includes incident handling as a required capability in risk management measures [16], [17], [31]. This means organizations must have policy-backed procedures for detecting, reporting, and recovering from security incidents. Having actions like isolation of affected systems, escalation to incident response teams, and post-incident reviews in policies ensures a consistent and compliant reaction in day-to-day business. Enforcement in incident response does not only mean preventing the incidents but also executing the proper corrective actions dictated in the policy in a timely manner. Policy-driven response helps organizations limit damage and restore secure operations quickly and within expectations [31].

Governance requires verifying that policies are being followed and are effective. Regular audits – internal and external – are essential enforcement tools for this. Information security mandates that the organization must conduct internal audits to provide information on the information security management system, and enforce internal audits [18]. These internal audits review technical controls and procedures in both IT and OT environments to ensure they align with the established policies and standards. Often, organizations schedule audits or assessments quarterly or annually to check compliance with key policy areas such as access control, network security baselines, and configuration standards. The same requirement is found in industrial standards, where security policies must be reviewed periodically to ensure effectiveness and alignment with industry standards [35]. Audit findings must be reported to management, and any non-compliance should trigger corrective actions as required by the policy framework and its enforcement.

Beyond these snapshots, we call audits, continuous monitoring mechanisms help organizations to ensure ongoing compliance with policies. Automated compliance monitoring tools like security information and event management systems can track system configurations, user activities, and network traffic against policy rules in real-time. The practice of active monitoring aligns with NIS2 and ISO 27002, which both mandate organizations to conduct continuous

monitoring to assess effectiveness and ensure adherence [16], [24]. In the IT context, this would mean involving tools that check for unauthorized changes or vulnerabilities and are able to alert about changes, while in OT, it means monitoring control system integrity and network anomalies. Monitoring provides organizations with early detection of deviations from policy so that they can be corrected proactively. It will create a feedback loop where policy adherence is periodically reviewed and constantly supervised.

In addition to internal reviews and continuous monitoring, third-party assessments play a vital role in governance and compliance. Often, organizations pursue certifications or external audits to validate their security program against standards. For instance, the standards that are utilized here, such as ISO 27001 and IEC 62443 compliance assessments, effectively demonstrate that organizations' policies and control measures meet the required benchmarks. Third-party audits provide an effective and objective evaluation of how well an organization implements and enforces policies. Standards require suppliers and system integrators to confirm their compliance with applicable process requirements as required by the standards [18], [22]. Regulators may also conduct audits under frameworks like NIS2 to supervise critical infrastructure operations. External checks verify policy effectiveness, often uncovering gaps that internal teams overlook, thereby driving continual improvement of the security governance program.

An effective policy framework aligns with well-known security standards to ensure comprehensive coverage. Aligning IT and OT governance with standards like ISO 27001 and IEC 62443 provides a ready-made structure for addressing risks. International security standards can help organizations build a robust governance structure, bridging IT and OT cybersecurity practices. The European NIS2 Directive also encourages organizations to use existing standards; when developing implementation guidelines, the commission recommends member states align with international standards and existing industry best practices in the area of cybersecurity risk management [16]. By mapping internal policies to the controls and requirements outlined in standards and directives, organizations ensure that governance is both up-to-date and widely recognized. The industrial standards also require that organizational policy must align with internationally recognized cybersecurity standards [23]. The alignment also simplifies compliance reporting since meeting a standard’s requirements often satisfies legal or client obligations.

While cybersecurity regulations and standards are a good way of ensuring that organizations' cybersecurity meets requirements, they are not static – they evolve in response to new threats and technologies in the field. For example, the latest renewals are with ISO 27001 and NIS2. Governance policies must be living documents that are regularly reviewed and updated accordingly. The best practice here is that information security policies are reviewed regularly to ensure their continued sustainability and effectiveness [18]. The recommendation is to establish a schedule to revisit and revise these policies, ensuring ongoing compliance with new requirements and adaptation to changes in the organization's IT and OT environment. Maintaining alignment with the latest versions of standards like ISO 27002 and IEC62443 can keep the security program effective and compliant for the organization over time. Maintaining an organization's cybersecurity policies periodically is also mandated by the standards, and they also involve modifying the policies based on the risk assessment outcomes and evolving risks [22], [24].

Finally, policy development and enforcement should be tightly integrated with risk management processes. Security policies are essentially the treatment of risks that have been formalized into rules and procedures for the organization. Risk management frameworks and information risk management frameworks help organizations define risk criteria and appetite, which then inform policy decisions in an organization [32], [34]. As stated previously, industrial standards eventually tie the risk assessment similarly to policy decisions and risk treatment [22]. In practice, this means each policy, whether on access control, network usage, or incident response, should map to identified risks and controls that have been chosen to mitigate. By making these policies a risk management framework, organizations ensure that enforcement is properly prioritized where it matters rather than on feeling decisions, and organizations can, therefore, effectively demonstrate how their policies reduce unacceptable risk to acceptable levels. The risk-aligned approach, recommended by all major standards, ensures that governance is not just about compliance for its own sake but effectively protects the organization's business and critical assets in IT and OT environments.

5.5.5 Auditing, Monitoring, and Continuous Improvement

Auditing begins with the establishment of an audit program, where it is determined how and when we are auditing, what parties are conducting the audits, and whether they are going to align with the regulatory requirements. Starting with an audit program that includes both internal self-assessment and external reviews is essential. Information security management

and industrial control system standards require organizations to perform internal audits at planned intervals to verify that information security management systems meet both organizational requirements and standards requirements while being effectively implemented and well maintained [18], [23]. The internal audits are completed with external audits, such as verification assessments or regular inspections. NIS2 mandates that the regulators have the power to conduct regular audits and even targeted audits based on the risk assessments of essential organizations, which then ensures independent checks on security controls beyond internal reviews [16]. Independent third-party audits and certifications play a vital role in validating compliance with standards and regulations. Often, organizations seek certification for ISO 27001 as an example to demonstrate adherence to best practices. Regulatory frameworks explicitly recommend independent verification, and for instance, NIS2 allows auditors to requires the results of security audits carried out by a qualified auditor as evidence for compliance [16]. Engaging accredited external assessors helps ensure objectivity and lends credibility to the compliance program, often uncovering gaps that internal teams overlook.

Audit programs should be aligned with industry standards and legal requirements. This means that using standards like IEC 62443 for OT security and ISO 27001/22301 for IT and business continuity as benchmarks during audits covers both best practice controls and any specific regulatory mandates. Compliance audits check that policies and controls follow these standards and applicable laws, which might impose stricter oversight for some sectors. In the industrial domain, IEC 62443 emphasized regular auditing as part of the security lifecycle – once controls are implemented, regular audits should be conducted to ensure effectiveness and identify potential improvements, as the standard also recognizes and encourages a continuous improvement approach [23]. Aligning audit criteria with such standards ensures that the organization not only meets the current requirements but also maintains recognized best practices in security governance.

Continuing with continuous security monitoring and threat detection. Implementing centralized log management, security information, and event management solutions to collect security events from IT and OT environments is essential for real-time analysis. Event logging and monitoring are one of the mandates of industrial cybersecurity and information security standards [22], [24]. Security information and event management systems provide continuous monitoring of networks and systems, alerting on suspicious patterns or known indicators of compromise. The proactive capability aligns with regulatory expectations for proactive threat detection, for example, NIS2's risk management measures call for effective detection of

cybersecurity incidents and logging of security and relevant operational events [16]. By collecting and correlating logs, security information and event management systems offer a unified view of security across IT and OT environments, allowing operators to identify threats early and respond quickly. This is essential since prevention mechanisms can't keep pace with the changing cyber threat landscape, and organizations must focus on timely detection and prevention measures.

We must implement OT measures because these devices are unique and often lack support for active monitoring methods. For OT networks, specialized anomaly detection tools monitor traffic patterns and device behavior to spot deviations that could indicate cyber intrusions. Industrial cybersecurity standards mandate such capabilities for industrial systems, as it is stated that control systems should provide the capability to continuously monitor all security mechanisms' performance to help detect and report security breaches in a timely manner [22]. This means that OT environments should employ continuous network monitoring or intrusion detection systems tuned to industrial protocols and device capabilities. Often, industrial tools learn "normal" control system behavior and raise alerts on anomalies, such as unexpected commands or network flows, which provide an early warning of attacks on critical infrastructure. OT anomaly detection should be integrated with IT Security information and event management systems to provide better overall situational awareness across the converged environment. The incident management framework also recommends monitoring to detect information security incidents early and respond promptly to potential threats [31].

Robust logging is fundamental both to monitoring and post-incident analysis. Security logs should record user activities, exceptions, faults, and other events across the systems in IT and OT. According to ISO 27002, logs relevant to post-incident analysis should be produced, stored, protected, and analyzed [24]. Proper log management creates an audit trail that can be used to demonstrate compliance and to investigate incidents in depth. In fact, log data provides the evidence needed to perform forensic analysis after an incident – the standard notes that the purpose of logging is recording events, generating evidence, and supporting investigations, and demands logging and monitoring for these reasons [22]. Organizations should aim to implement centralized log retention that is in line with standards and any NIS2 requirements for record-keeping, and ensure that both logs from IT and OT systems are collected and secured to prevent log tampering [18], [22]. During audits or incident response, these logs enable forensic investigators to reconstruct timelines, identify root causes, and verify whether security controls

operated as intended. This is a function that supports both compliance verification and continuous improvement of the organization's security posture.

Off to continuous improvement in cybersecurity governance. A governance program should have feedback loops to learn from both audits and security incidents. Findings from audit reports, like non-conformities and observations, and post-incident reviews should feed into the updates of policies, procedures, and controls in an organization. Information security standards emphasize continuous improvement from reviews, and audits should be utilized to improve the information security controls, alongside post-incident analysis [24], [33]. Organizations should formally review these lessons learned – for example, through management review meetings or dedicated improvement plans – to decide on corrective actions and enhancements. Industrial standards also find a way to emphasize continuous improvement to help organizations adapt to emerging threats and vulnerabilities [23]. The corrective actions could mean additional training, process changes, technology upgrades, or new controls to address gaps. If an organization aims to treat audits and incidents not as one-off events but as learning opportunities, it continually bolsters the security governance of its IT and OT environments.

Continuous improvement in cybersecurity should be closely tied to ongoing risk management in day-to-day life. Threat landscapes and business processes evolve, so governance must adapt in an iterative plan-do-check-act cycle. Standards like information security, risk management, and business continuity closely prescribe the plan-do-check-act cycle for processes to remain effective [32]. The information security standard specifically describes that organizations should continue to improve the effectiveness and adequacy of the information security management system [18]. In practice, this means regularly reassessing risks, updating risk treatment plans, and modifying controls as needed. OT security standards reinforce this adaptive approach by encouraging periodic risk re-evaluation with threats and vulnerabilities as part of the security programs [17]. New vulnerabilities with, for example, industrial control firmware or emerging threats like ransomware and supply chain attacks may necessitate changes in security architecture or procedures. By implementing continuous monitoring, the threat environment is visible, and the organization can evaluate the effectiveness of existing controls and adjust its defense strategy accordingly. This could involve deploying new detection techniques, revising access controls, or improving network segmentation in plants. The goal is a governance framework that is not static but also evolves through constant refinement, thereby maintaining robust security in the face of change.

Cybersecurity governance must also continuously improve to meet new or changing compliance obligations. Regulations and standards are quite frequently updated to address emerging risks and new technologies – for example, the EU transition from NIS to NIS2 introduced stricter requirements on incident reporting, supply chain risk, and executive accountability, which required organizations to bolster their policies and oversight in cybersecurity [16]. Likewise, industry standards get revised, ISO 27001:2022 added new controls as well as the updates in the IEC 62443 series, organizations should update their governance documentation and practices alongside the standards [18], [23]. Proactivity is the key here, tracking changes in laws and adjusting internal policies and control frameworks to ensure ongoing compliance. Governments and regulators increasingly impose compliance with already existing frameworks to protect critical infrastructure and mandate organizations to have decent cybersecurity measures, including requirements for regular security audits and documentation of controls [16], [23]. A mature governance program will have mechanisms to incorporate these evolving requirements – for example, updating audit checklists, revising incident response plans, and briefing senior management on new obligations. If compliance is properly integrated into governance processes, so will the changes; the organization ensures that its security posture improves continuously and remains aligned with the latest regulatory and industry standards.

5.5.6 Third-party Risk Management and Compliance

Third-party risk management in IT and OT environments refers to the process of identifying, assessing, and controlling risks introduced by external entities that provide products or services to organizations' IT or OT systems. In a factory setting with integrated IT and industrial control systems, third-party compliance is critical to ensure cybersecurity, integrity, supply chain security, and regulatory adherence. External vendors, contractors, and service providers can become weak links if not properly managed. This is seen by NIS2 legislation as an example where third parties are given a specific notation [16]. Third-party risk management helps to protect the organization's digital ecosystem by extending security governance to suppliers and partners. Leading industry standards and frameworks also emphasize this point. Information security standards stress this by addressing the requirements of external parties. In the context of smart factories and critical infrastructure, it can be seen that third-party compliance is not just a best practice but a legal obligation to ensure the security of our operations. An organization is only as strong as its weakest link, meaning that the balance of security has to be considered with third-party vendors. There are several key frameworks and standards that

govern how organizations should manage third-party risks. These standards include information security, industry-specific standards, and regulatory directives.

Before engaging third parties – and throughout the relationship – organizations should aim to conduct a risk assessment and due diligence of third parties. Third-party risk assessment is the process of evaluating the security risk a vendor or supplier poses. This risk assessment is based on factors like the sensitivity of data or systems they will access, the Third party's security posture, and the criticality of the service that they provide. With due diligence, we refer to the investigative steps taken to vet a vendor's security and to classify the vendor's risk level. Methodologies commonly known to perform these assessments are risk assessment, vendor evaluation and tiering, Process for engagement, and sector-specific due diligence.

Starting with Risk Assessment methodology, organizations often leverage standards like ISO 27005 for general guidance on IT risk management or IEC 62443-3-2 for OT-specific risk assessment. Industrial standards provide a risk assessment framework that involves defining zones/conduits and assessing risk for each zone. Although the approach is system-focused, as part of the process, it would identify external dependencies and threats [17]. Similarly, the information security standard encourages assessing risks associated with external parties and treating them within the risk management processes [34]. In practice, many organizations use a vendor risk rating approach, which means evaluating the likelihood and impact of a third-party-related breach. This would include assessing the vendor's controls and the impact on the organization if the vendor were compromised.

Moving on to vendor evaluation and tiering – a practice where we check on the vendor before contracting and onboarding with due diligence, which might include a security questionnaire or assessment, review of certifications or audits, and risk rating and classification. Going through the process could start with a security questionnaire or assessment. In practice, it can be about their security controls, policies, incident history, and anything else. A lot of organizations aim to use standardized questionnaires or frameworks. Then, it can be followed by a review of certifications and audits; if a vendor has ISO certifications, SOC 2 reports, or other third-party audit reports, these could be reviewed to gain assurance that they meet recognized security standards. Following this, there should be risk rating and classification, which in practice means classifying vendor risk tier based on the data from questionnaires, certifications, and audits and classifying vendors based on the engagement of the third party. Commonly, vendors will be categorized as high, medium, or low risk. Criteria should include

the sensitivity of data shared, connectivity, criticality, and the vendor's own maturity. For example, a cloud data center provider for critical OT systems might be rated high risk, whereas an office supplies vendor with no system access is low risk. Vendor evaluation is described in the information security risk management standard and provides assistance in evaluating the likelihood of a third-party breach and the impact it could have [34]. The NIS2 directive clearly mandates conducting due diligence and risk analyses to pinpoint vulnerabilities brought by third parties [16]. This aligns with the concept of risk tiering, ensuring that high-risk vendors are subject to more rigorous assessments.

Next, we'll discuss the engagement process. Before onboarding a new supplier, many organizations establish an internal process called a supplier security assessment or a third-party risk assessment process. The aim of the process is to ensure that the earlier discussed steps are taken. Often, the workflow might include identification, initial screening, due diligence assessment, risk analysis, risk treatment, approval and contracting, and continuous monitoring. The process is fairly simple – Identifying the need for a third-party service and notifying potential security/risk teams - Determining what data/access the vendor will have to scope the risk, Sending the security questionnaire, requesting documentation – Security team reviewing responses, identifying gaps or high residual risks – If risks are found how they are controlled – If vendors meet acceptable risk level the engagement is approved, with risk-based controls written into the contract – once onboarded, the vendor’s risk is re-assessed periodically.

There also needs to be sector-specific due diligence, for example, critical infrastructure sectors might require this. ISO 27019, being an extension of 27002 for energy utility industries, adapts controls for process control systems and emphasizes supplier security in the context of energy OT, building controls equivalent to ISO 27002 [24], [40]. IEC 62443-2-4, which is the standard for service providers, can be used as a checklist to assess an OT service vendor's security program during due diligence, like verifying they have account management procedures, patch management in place, and everything else that is required by the standards [35].

Performing proper third-party risk assessment and due diligence upfront reduces the chance of unpleasant surprises down the line and helps organizations “trust but verify” their partners. If an organization categorizes vendors based on risk and evaluates their security, it can apply appropriate oversight, enabling a focus on high-risk suppliers. Third-party risk assessment is an ongoing process from the initial due diligence forms, building a baseline, but risks must be re-evaluated over time as the system, threats, and the vendor's position or posture evolve. To

manage and mitigate the risks from third parties, organizations should aim to implement a range of security controls. These controls apply both to the third parties and to the organization's own systems to securely accommodate third-party access or data. The key categories for controls include authentication and access control for third parties, network segregation, monitoring of third-party activities, hardening of systems, and continuous oversight.

Beginning with access control and authentication, strict access management is crucial when working with third parties for access to systems or data. Usually, this involves ensuring that third-party users have unique identities and are strongly authenticated. Information security standard provides baseline controls for access management that should also apply to suppliers – Provisioning user accounts with the least privilege principle [24]. In practice, third-party personnel should only be given the minimum access rights necessary, and their accounts should be segregated from internal accounts. Multi-factor authentication is recommended and often required for any remote or privileged access by vendors. Industrial standards set specific system requirements for authentication that require all human users, including externals, to be uniquely identified and authenticated on the industrial control system, and higher levels mandate MFA for untrusted network access [22]. It is also mandated in the industrial standard that account lifecycles are controlled, and credentials are managed securely [22]. These controls should collectively prevent unauthorized or unchecked access through third-party connections.

Moving on to network segmentation and remote access security, third-party connections should be isolated as much as possible. In OT, this means placing vendor connections in demilitarized zones or specific security zones with monitored conduits. The principle of restricted dataflow is a foundational requirement in IEC 62443, which is implemented by segregating networks so that a compromise of a vendor connection does not free roam the entire network [22]. Practical controls would mean using jump servers for vendor remote access, restricting accessible services, and enabling time-bound access only when needed. All remote sessions by third parties should be encrypted and monitored for traceability. Industrial standards also require remote access session termination for inactive sessions, and connections from untrusted networks must be controlled; together, these ensure the secure handling of vendor remote sessions [22]. IEC 62443-4-2, which specializes in component security, provides technical requirements like secure remote administration interfaces on devices, which vendors must implement for secure remote access [29].

The same applies to internal operation-critical systems and software, as well as external systems or software. Any systems or software provided by third parties should be hardened and comply with the organization's security baselines. This would include applying timely patches, disabling unnecessary services, using antivirus/endpoint protection, and configuring secure settings. Many vendor-related breaches occur due to default credentials or unpatched known vulnerabilities in vendor-supplied software. Organizations should require vendors that follow secure development practices and deliver systems that meet standards like IEC 62443-4-2, which brings the technical security requirements for industrial components, which are, for example, authentication, encryption, and audit logging in PLCs or HMIs [29]. On the organization side, any third-party provided systems should go through a security review and hardening before production use. For IT software vendors, this might mean ensuring that the application passes vulnerability scans or possible code analysis; for OT equipment, verifying compliance with industry certifications or performing factory acceptance tests that include cybersecurity checks.

Having already touched on the monitoring of component requirements, once a third-party connection or service is in use, continuous monitoring is vital. The organization should log activities related to third parties; this could mean logging vendor user logins, commands executed, data accessed, and any changes. Information security standards highlight monitoring of supplier service delivery and encourage reviewing reports or alerts relating to third-party services [24]. In OT solutions, if we are using solutions like jump hosts, we can record vendor sessions for later audits. An anomaly detection system may be used to watch for suspicious behavior from third-party accounts as well. Industrial standards have auditing requirements, where auditable event and session control are required to ensure security-relevant event logging and sessions are managed [22]. The organization's security operations team should incorporate third-party access logs into its security information and event management for real-time monitoring. Effective monitoring acts as a detective control to catch any misuse or breach originating from third-party access as quickly as possible.

And finally, endpoint and data security controls – if third parties handle organizations' data, controls must protect that data both at rest and in transit. This would mean including data encryption, strict handling procedures, and data loss prevention measures. For example, if cloud providers store sensitive data, ensure encryption keys are managed properly. Suppose an external maintenance contractor connects a laptop to the OT system. In that case, that laptop has to be verified to have up-to-date anti-malware based on the organization's standards and not

be carrying unapproved software. Additionally, these data security controls mean ensuring that any data shared with suppliers is on a need-to-know basis and via secure channels. Information security standards provide controls on cryptography and the transfer of information to third parties as well [24].

To summarize, the control measures for third-party risk management are about extending the organization's security controls boundary to include vendors or at least buffering your organization from any weaknesses on the vendor side. The combination of preventive controls, detective controls, and corrective controls will significantly reduce third-party risk. Standards like ISO 27002 provide general best practices, while the IEC 62443 series provides more specific technical controls for industrial environments – both standards should be used to inform control selection [23], [24]. If implemented correctly, the organization should be more confident that a third party connects to its environment, that connection is as secure and monitored as any internal access, and that data is handled with relevant protections if a third party processes its data.

Despite putting their best efforts into prevention, security incidents involving third parties can still occur, such as a vendor getting breached, leading to the organization's data being exposed, or a third-party-provided software containing a backdoor. Because of this, incident management processes must explicitly include third-party considerations. This ensures that when something goes wrong involving a supplier, the response is swift, coordinated, and compliant with notification obligations. Beginning with the inclusion of third parties in incident response plans. Organizations should have incident management plans aligned with ISO 27035 that outline how to handle incidents that involve third-party vendors. ISO 27035-2 recommends establishing communication channels and procedures with external parties in advance [33]. This would mean that if an incident is suspected to originate from or affect a vendor, there are already predefined steps: who to contact at the vendor, how to isolate third-party access if needed, and joint investigation procedures. For example, if an intrusion is traced to a contractor's VPN account, the plan would dictate suspending that access and notifying the contractor’s security team immediately. NIS2 directive reinforces this by requiring that third-party incidents are handled with the same seriousness as internal ones, including coordinated response and timely information sharing [16]. A best practice is to conduct periodic joint incident response exercises with key suppliers so that both sides are prepared to collaborate under pressure.

Continuing with breach notification – Clear agreements must be made to stipulate how and when a third party must notify the organizations of an incident and vice versa. If a vendor suffers a breach that potentially affects the organization, the organization should expect notification within a defined timeframe. Contracts should and typically do include breach notification clauses, often requiring notice within 24 or 48 hours of discovering an incident. This allows the organization to take defensive actions. On the other side, if the organization detects an incident that involves a supplier's system, it should promptly inform the supplier so they can contain it on their end. ISO 27002 touches on this in supplier agreements, requiring suppliers to report incidents that may impact the client's information security [24]. Under NIS2, incident reporting to authorities is mandatory for significant incidents, and this includes incidents that stem from supply chain compromises [16]. According to NIS2, Organizations must report within 24 hours for initial notification and 72 hours for a detailed report to the relevant cybersecurity regulators [16]. Ensuring that vendors provide the necessary information quickly is part of this compliance. The third-party incident notification must be both a contractual obligation and a compliance requirement with plans that reflect those obligations.

With third parties, we also need to account for incident handling with third parties. When an incident does occur, organizations should aim to take steps to address third-party involvement. Beginning with containment and access removal, if a vendor's credentials or connection is suspected of being compromised, disabling their access immediately helps to contain damage. For OT, this might sometimes mean physically disconnecting a remote support link. Then there comes the investigation cooperation, working jointly with the third party's security team helps to investigate the root cause. This might involve sharing log data and forensic information under controlled conditions. These environments require NDAs, if not already in place, to facilitate information sharing during the investigations. This leads us to eradication and recovery. If the issue was a third-party component, ensuring the vendor provides a clean update or fix is essential. If the incident is on the vendor's infrastructure, then there needs to be coordination on remediation steps. IEC 62443-2-4 standard-compliant suppliers are expected to handle incidents in line with their own asset requirements, mandating them to be prepared to assist in recovery [35]. Finally, post-incident review, including the third party in the lessons-learned review, helps everyone. Determining if there were failings on the vendor's side and requiring corrective actions, but also assessing if the incident reveals any need to change how the organization manages that third party.

Regulatory and legal considerations also have to be considered, beyond just the notice times. With NIS2 and data protection regulations, organizations might be obligated to report incidents externally and possibly notify customers. If the incident came through a supplier, regulators would expect that the organization had taken appropriate precautions with that supplier. NIS2 specifically calls out supply chain incidents – EU-wide coordination on supply chain cyber threats is encouraged, and entities might be asked to participate in sharing information on such incidents [16]. From a compliance perspective, this would mean being able to show auditors or regulators when you've been notified and what steps were taken to mitigate this, and the organization informed authorities at this time; this is crucial to avoid penalties.

Incident management in the third-party context concerns preparedness and clarity of obligations. If organizations plan ahead with policies and contracts for third-party incidents, they ensure that there won't be scrambling to figure out roles and responsibilities during a crisis. Knownly, ISO standards and NIS2 stress having these plans and agreements in place [16], [24]. A coordinated, timely response can significantly limit the damage of a third-party-related incident and demonstrate due diligence. Creating a cohesive incident response strategy that incorporates third-party collaboration, clearly defined communication pathways, shared investigation methods, and procedures for post-incident evaluation sounds like a best practice for handling incident management promptly and effectively.

Managing third-party risks is not a one-time effort at onboarding. Third parties require ongoing monitoring and periodic re-evaluation throughout the vendor relationship. Cyber threats, along with vendor environments and relationships, evolve, so continuous oversight is necessary to ensure third parties remain in compliance with security requirements over time. Continuous monitoring in a third-party context would involve technical monitoring of third-party-provided services/connections and security performance reviews or audits of the third parties.

Starting with ongoing security monitoring, where organizations should continuously monitor the security of third-party services, which would mean automated tools and processes like service uptime and anomaly monitoring, vulnerability management, periodic access review, and continuous control monitoring [41]. Starting from service uptime and anomaly monitoring, if a third party provides an IT service like a cloud-hosted application, monitoring its service performance for any anomalies or suspicious behaviors that could indicate security issues is recommended [41]. Unexpected downtime or irregular activity might warrant a security check with the vendor. Vulnerability management would mean keeping track of vulnerabilities and

patches related to third-party software or devices in use [23]. If a vendor-supplied system has a new vulnerability disclosed, ensuring the vendor provides a patch and applies it promptly is recommended, alongside maintaining an inventory of third-party assets and their versions [3], [13].

Organizations should aim to review access regularly, especially with third parties, what privileges they have, and what accounts are active. ISO 27001 requires organizations to review user access rights at intervals, which includes external users [18]. Any accounts or accesses that are no longer needed should be removed immediately in cases, for example, where a project with a contractor has ended. With continuous control monitoring, with some critical suppliers, organizations might employ security rating services or tools that monitor the supplier's external security posture, like tracking the vendors ' facing systems if they accidentally leak data, etc. While this is not a foolproof method, these monitoring services can warn early about a decline in vendor security hygiene.

Why this is important—The NIS2 directive explicitly expects organizations to “continuously monitor and evaluate third parties,” adjusting risk assessments based on changes or emerging threats [16]. This would mean that if a vendor introduces a new service or there's news of supply chain attacks in the vendor’s industry, the organization should reassess that vendor’s risk and possibly heighten oversight. Continuous monitoring ensures that security compliance is taken seriously, not just as a snapshot at onboarding.

Regular third-party audits and assessments also support compliance with security requirements, and the acknowledged best practice is to periodically audit third-party compliance. This can range anywhere from informal reviews and discussions with third parties to formal audits. Periodic security questionnaires are one of the ways to handle this. Sending out an updated questionnaire annually to key vendors to capture any changes in their security posture might be the way. It is also the easiest solution of the bunch; organizations might want to gather evidence or documentation as well for critical controls and how they develop over time. Another really good method of verifying third-party environments is on-site or virtual audits. Typically, for high-risk or critical suppliers, the contract may grant the right to audit. Exercising this right, the organization or an independent auditor can audit the vendor’s controls. For example, this could mean reviewing data center security or checking compliance with standards. IEC 62443-2-4 mandates that service providers facilitate audits and security assessments, reflecting this

requirement [35]. Audits should be done regularly, once a year or every two years, for important vendors.

Penetration testing and technical assessments are also a form of audit. If a third-party application or system is in the organization's environment, including it in regular penetration testing cycles is recommended. Any serious findings should be communicated to the vendor for remediation. In an OT environment, this could mean periodically testing remote access pathways or attempting to breach a vendor-maintained segment in a controlled manner to verify its security. Finally, compliance reviews and meetings should be held. Organizations aim to hold regular governance meetings with suppliers, where security should be a standing agenda item. As a topic of discussion, there could be outstanding risks, development in the fields, recent incidents, or changes in organizations, and ensuring that the vendor is addressing previously identified issues. This creates accountability and keeps security relevant throughout the partnership.

From an information security management system perspective, it is mandated to have ongoing monitoring and internal audits for the system as a whole, which extends to controls on suppliers as well. Taken from the standard, the organization should aim to evaluate the performance of supplier-related controls and assess the demand [18]. This could be achieved by auditing a sample of supplier relationships each year as part of the information security management system's internal audit schedule. The result of these audits should feed back into the improvement processes that are also demanded by the standards [18]. But to ensure third parties maintain compliance, organizations should establish clear metrics and follow-up mechanisms. This might include tracking whether all high-risk vendors have up-to-date risk assessments and signed agreements, measuring how quickly critical patches are applied, and monitoring for any exceptions or waivers granted to vendors. Many organizations use vendor risk assessment software to keep track of assessment dates, risk scores, outstanding remediation items, etc. A central register of third-party risks can be maintained and updated as monitoring results come in. If a vendor consistently falls below expected performance, the organization can escalate the issue to vendor management or ultimately consider switching to a more secure provider.

NIS2 will empower authorities to request evidence that supply chain risks are managed on an ongoing basis, not just at a single point [16]. Therefore, documenting organizations' monitoring efforts and activities can help to demonstrate compliance during inspections or audits by authorities. Continuous monitoring and auditing form the “maintenance phase” of third-party

risk management. Our initial due diligence is the front door; ongoing oversight is the camera inside. With standard-driven practices, organizations should be able to catch emerging issues from third parties early and ensure that the relationships remain within acceptable risk bounds [16], [18], [35].

Now, we must continue to address contractual and legal obligations for third-party risk management. Legal agreements and contracts are primary tools for enforcing security compliance on third parties. A well-crafted contract will define the security responsibilities of the vendor and provide the customer with the right to enforce those responsibilities. In many industries, regulators and standards expect certain clauses to be present in third-party contracts as part of due diligence, but some of the contractual and legal obligations might be security requirements, law compliances, right to audit and assess, breach of notification and incident cooperations, service level agreements for security, termination and liability clauses, and confidentiality and data protection.

Let’s start with security requirements; contracts should specify the exact security controls or standards the third party must adhere to. For example, an outsourcing contract may state that the vendor must comply with ISO 27001 or maintain an equivalent information security program [18]. It may also list required controls, such as those used by governmental organizations. For example, contracts might say that the vendor shall implement encryptions for all sensitive data at rest and in transit or that there is a 24-hour patch deployment timeframe for critical vulnerabilities. ISO 27002 also discusses topics including confidentiality clauses, audit rights, incident reporting duties, and compliance with organizations' security policies in supplier agreements [24]. By embedding those clauses, the organization makes its security expectations legally binding.

While staying on the topic of contracts, the contract should require the third party to comply with all applicable cybersecurity and data protection laws. Under NIS2, essential service providers might lay down some obligations to their suppliers. For instance, if the organization is subject to NIS2, it should contractually oblige critical suppliers to meet NIS2-aligned security measures. NIS2 article 21 basically forces this by requiring supply chain security measures, and contracts are the vehicle to implement them [16]. Contracts might also reference industry standards like IEC 62443 for OT suppliers – for example, requiring an automation vendor to comply with IEC 62443-2-4 or achieve a certain security level certification for their products. These references set a clear compliance target for the vendor [35].

A critical clause also reserves the right for the organization or its delegate to audit or inspect the third party's security controls. This legal right underpins the continuous audit practice discussed earlier. Contracts should include audit rights that allow periodic reviews and require the vendor to remediate any deficiencies found [16]. Without an audit clause, a vendor could legally refuse an audit. Often, even if on-site audits are not exercised frequently, the existence of this clause encourages the vendor to maintain compliance, knowing they could be audited. Additionally, the contract can require the vendor to provide copies of any independent audit reports or confirm their certification status annually.

As mentioned earlier, contracts must have clear breach notification requirements. Typically, the wording goes something like this – Vendor shall notify the Customer in writing without undue delay, no later than x hours after discovering any security incident or data breach that affects or may affect customer information. With a similar kind of statement, the contractual obligation would align with ISO 27002, and laws like, for example, data protection laws require data processors to notify controllers [24]. The contract should also oblige the vendor to cooperate in incident investigation and response, which could include preserving evidence, assisting forensic analysis, and taking corrective actions. For example, IEC 62443-2-4 includes incident response as part of service provider requirements, so a vendor conforming to that would naturally meet this obligation [35]. Some contracts also incorporate SLAs related to security, for instance, the maximum allowable time to apply critical patches or uptime for security infrastructure. While most SLAs focus on performance, security SLAs can be useful for critical suppliers.

To enforce compliance, contracts include a right to terminate agreements for material security breaches or non-compliance. This could mean that if a vendor has a serious breach due to negligence, the client can terminate the contract without penalty. With termination clauses, there also might be liability clauses – vendors might be held financially responsible for costs incurred by the client due to the vendor's security failure. While vendors often resist open-ended liability, clients will push for at least some accountability, especially if sensitive data or critical operational parts are at stake. Termination for non-compliance or poor security performance is explicitly suggested as a key contractual element by NIS2 [16]. It is also important to include standard confidentiality clauses to protect the organization's information that the vendor accesses. If personal data is involved, a data processing agreement must be included as it is required by GDPR, specifying how personal data is handled by the vendor,

including security measures. This is another legal layer ensuring that the vendor follows specific technical and organizational measures.

To summarize the contractual and legal obligations, legal agreements translate third-party risk management policies into enforceable commitments. A contract is here to essentially set the ground rules for engagement; it binds the third party to maintain specific security standards, allows organizations to verify and enforce those standards, and defines consequences if expectations are not met. Standards like ISO 27002 emphasize the importance of including security requirements in supplier contracts, and NIS2 requires addressing cybersecurity in supply chain contracts [16], [24]. Contracts address compliance, audits, incident management, and termination, ensuring that third-party governance remains legal and offering recourse if a vendor does not meet their obligations.

Since the Third-party risks in the IT/OT Environment are quite a broad subject in our scheme and there is also a lot that has been missed out, we will summarize the chapter by going over the best practices. The organization should aim to build a robust third-party risk governance program that aligns with the industry's best practices and standards.

Let’s begin by integrating third-party risk into the security governance framework. This begins by treating third-party risk management as an integral part of your overall security program. This would mean ensuring that there is clear executive ownership and policy for third-party security. ISO 27001 requires top management support and a risk management process that covers all information assets, which includes suppliers in that scope [18]. Establish a dedicated third-party risk management or supplier security policy that outlines the process for onboarding, monitoring, and offboarding vendors from a security standpoint. The policy should apply across IT and OT to have a unified approach.

A risk-based approach and tiering are our next best practices. As noted, not all vendors are equal – applying more stringent control and oversight to those that pose higher risk is recommended. For high-criticality suppliers, like access vendors with access to production networks or large volumes of sensitive data, should be conducted with full security assessments, requiring strong contractual terms and reviewing them frequently. Lower-risk vendors can have a lighter process. This prioritization ensures efficient use of resources and that critical third parties get the attention they require for business continuity [16]. Regularly refreshing the risk assessments at least annually or upon significant changes is recommended to capture any new risks.

Organizations should also learn to utilize industry standards and certifications. Aligning third-party requirements with recognized standards is a good practice. For IT vendors, relying on ISO 27001 can provide assurance, but always review the scope and results of audits as well [18]. For OT vendors, the IEC 62443 series is invaluable, requiring OT product suppliers to follow secure development and provide components compliant with technical security requirements, which helps organizations a lot [29], [37]. For service providers, this would mean conforming to IEC 62443-2-4 [35]. Many industry suppliers now advertise compliance or certification against standards or parts of them, which helps to ensure that best practices are met. Standards also provide valuable information so that organizations don't have to reinvent control requirements if standards already cover what is needed.

Establishing strong collaboration between IT and OT for supplier management is also recommended. Risk management cannot be siloed in an IT/OT converged environment. Ensuring the teams responsible for vendor management and OT supplier management share knowledge and processes is critical. For example, an OT support contractor might be evaluated with input from both the enterprise security perspective and the plant engineering team. Standard tooling can be used. This would prevent gaps in understanding how an IT provider might indirectly affect OT operations, and an OT component vendor might have remote support that touches the corporate IT networks. Unified governance avoids blind spots.

Moving onto continuous improvement and adaptation – Following the “plan-do-check-act” cycle of ISO 27001 for the third-party risk domain [18]. This means regularly checking the effectiveness of the third-party controls and making improvements. Organizations should aim to utilize incidents or near-misses as learning opportunities. If the vendor had a minor incident, it's asking, did our process catch it? If not, what can be improved? It’s also about staying updated on emerging threats to supply chains and organizations – if there is a supply chain attack campaign in your sector, it could mean heightened reviews or communication with relevant suppliers. As the threat landscape evolves, so should organizations' third-party risk programs. NIS2 will force organizations to adopt state-of-the-art practices, which might include more detailed supplier risk assessment or cooperation at the sector level for vetting critical suppliers [16].

Training and awareness are critical components as well when counting on the best practices. This means ensuring those involved in procurement and vendor management understand the importance of cybersecurity in third-party dealings. Often, business units may be eager to

onboard a new supplier quickly, training helps them recognize why security due diligence is necessary and how it protects the business. Similarly, providing guidance to third parties about your expectations is as important. Some organizations even offer vendors training or support to meet the required security standards, meaning a collaborative approach to the topic. For instance, sharing your security policy with a third party and giving feedback on the improvement plans of third parties is recommended. A well-informed vendor is more likely to comply with requirements than a less informed one.

And finally, Incident preparedness and resilience – As part of best practices, planning for the worst-case scenario of a third-party compromise is one. This would mean conducting drills or tabletop exercises focusing on a supply chain attack. This would not only test our incident response, which was discussed earlier, but also solidify relationships and communication channels with the third party. Additionally, it is recommended to consider alternatives or backups for critical suppliers, which would increase supply chain resilience. For OT, this will mean having contingency plans if a cyber event incapacitates a key vendor, for example, a control system vendor's system is compromised, so the organization can isolate and rely on having the systems without the vendor's attention while the situation gets resolved. NIS2 stresses continuity plans that include loss of services from critical suppliers [16].

Best practices are strong governance, informed by standards, and proactive management. Using the ISO 27001 framework will give you the management system, IEC 62443 will provide the OT-specific controls, and NIS2 will give the organization with the legal imperative and specific focus areas. Aligning the organization's programs to these will ensure completeness. But document everything and maintain clear records of risk assessments, decisions, and actions for each third party. It not only helps in internal management and tracking progress but also serves as evidence of due diligence for audits, whether internal, external, or by regulators.

5.5.7 Security Awareness and Training

Security awareness and training are essential components of an organization's cybersecurity governance framework. In the context of IT/OT convergence, employees, contractors, and third-party vendors must be equipped with the knowledge and skills to recognize and respond to security threats effectively. Security incidents, whether in the IT or OT domain, often occur due to human errors, such as falling for phishing attacks, misconfiguring systems, or mishandling sensitive data. Therefore, comprehensive security awareness programs and

training are necessary to reduce these risks and strengthen an organization's overall security posture.

Security awareness training programs help ensure that employees understand the importance of security and their role in maintaining it. These programs should be designed not just for IT staff but for all employees, including those who interact with OT systems, such as engineers, operators, and contractors. As IT and OT have different risk profiles and compliance requirements, and training programs must address the unique security challenges present in both environments. Industry standards and regulations emphasize the need for continuous education and training to maintain a secure organizational culture and comply with cybersecurity regulations.

Starting with the role of security awareness in governance and compliance, it is clear that security awareness plays a crucial role in both areas and in risk management by ensuring that everyone within the organization understands their security responsibilities. Without appropriate awareness methods, even the best technical controls can be undermined by employees or contractors who do not follow secure practices. Standards outline specific requirements for establishing security awareness programs within organizations to ensure compliance with regulatory frameworks and internal governance structures.

Beginning with ISO 27001, which requires organizations to implement appropriate security awareness and training programs as part of their information security management system. The clause emphasizes that organizations must ensure that employees and stakeholders are competent to perform their security-related roles and that training or awareness programs should be conducted regularly [18]. This would mean raising awareness of information security threats and vulnerabilities as part of the ongoing education of the workforce. ISO 27002 also provides detailed guidance on how organizations should implement their security awareness programs. There is a clause stating that organizations should ensure that employees are aware of their roles and responsibilities concerning information security [24]. It is also emphasized that training programs should be regularly updated to address evolving threats and that employees should be tested on their understanding of security policies.

Industrial standards, on the other hand, establish the need for an asset owner to implement an ongoing security awareness program. IEC 62443-2-1 mandates that employees involved in the operation and maintenance of industrial systems should be trained both on cybersecurity and physical security, tailored to the specifics of their roles and the security risks they face [23].

The same standard also mandates periodic training for personnel to ensure that they are up to date with the latest security practices and threats [23]. This is coming from the perspective of being an asset owner and should be taken seriously in manufacturing fields. Another industrial standard for security risk assessment and systems design also discusses training, recommending regular security awareness training for individuals involved with industrial systems [17]. They also highlight the importance of educating management about risks in control systems and OT [17]. This aims to ensure all personnel in the domain understand cybersecurity policies and best practices, equipping them to recognize and mitigate risks.

Based on this, the organization should aim to develop a comprehensive security awareness program. This involves several key steps, including the needs assessment, content development, delivery methods, and ongoing evaluation. Organizations should tailor these programs to the specific needs of their workforce, with a focus on IT and OT staff, personnel, and contractors. Security awareness programs should start with a needs assessment that identifies the specific security risks faced by different groups within the organization. The aim is to help identify what each role requires in terms of security knowledge. This may indicate that IT staff concentrate on areas such as technical security, threat detection, vulnerability management, incident response, or secure coding practices. In contrast, OT personnel and operators tend to prioritize the risks associated with control systems, physical security, industrial protocols, and the distinct security challenges that arise in OT environments, while all staff participate in foundational awareness programs. ISO 27001 requires role-specific training tailored for different roles [18].

The content of the security awareness program should cover a broad range of topics, including technical and non-technical aspects of security. This would mean understanding cybersecurity fundamentals and basic concepts such as authentication, encryption, firewalls, and malware. It should also include phishing and social engineering so that attempts to manipulate individuals into sharing confidential information would be recognized and responded to. It should also include how data, especially personal and sensitive data, should be protected in compliance with regulations. Incident reporting should be educated as well, and how users report suspicious activities, incidents, or potential security breaches in the organization should be clear for everyone. ISO 27002 advises that organizations should define clear objectives and topics for their training programs. Employees should be aware of the specific roles' security policies, legal obligations, and security risks [24]. Industrial standards also suggest that OT-specific training should cover both cybersecurity and safety issues, ensuring that personnel with industrial

control systems are equipped to recognize potential security vulnerabilities that could lead to physical safety incidents [23].

Training should be delivered using a variety of methods to ensure that the training is engaging and accessible for different employees. Possible delivery methods could be in-person or virtual workshops, online courses, simulations, or posters. Having a wide variety of solutions for maintaining training is highly recommended to maintain attention. ISO 27002 also emphasizes the need for recurrent training and refreshers, ensuring that staff remain updated on security policies and latest trends [24]. Regular training is, of course, mandated and should be conducted to adapt, but it is also recommended to evaluate the effectiveness of training through tests, audits, and feedback loops [24].

The evaluation and continuous improvement should also be addressed. The success of a security awareness program depends on its effectiveness. To evaluate the effectiveness of training programs, organizations should aim to use assessments, phishing simulation metrics, and incident response metrics. Monitoring and evaluation of the effectiveness of training programs should be a part of the ISMS process, which is required in ISO 27001. It requires that organizations measure the performance of their security management system, which includes training programs. Effectiveness can be monitored in various ways, including incident response data. However, it is advisable to use post-training quizzes or tests to evaluate employees' grasp of essential concepts. Additionally, conducting phishing simulations will help track the number of employees who click on simulated phishing emails and assess improvements over time.

The compliance and legal requirements for security awareness training should also be assessed. Security awareness training is not just a best practice but is often required by regulations and standards. Compliance should be checked to ensure that organizations are adhering to legal and contractual obligations for securing information systems and maintaining operational resilience. The NIS2 directive sets the stage for security awareness and training. It mandates that organizations in critical sectors implement cybersecurity measures that include employee awareness and training. Article 21 of the directive requires that organizations ensure their employees are aware of their roles in managing cyber risks, specifically around data protection and incident reporting. It also notes that training should be an ongoing process to address emerging threats and vulnerabilities [16]. GDPR also requires training by requiring organizations to implement appropriate technical and organizational measures to ensure the security of personal data [42]. This would mean ensuring that staff handling personal data are

properly trained to avoid breaches and that staff recognize and avoid risks related to personal data processing. Standards, as discussed earlier, might also take a stand against the topic, and they often underscore that the training should be tailored to specific security risks; also, in industrial control systems, training should be regular and regularly updated [18], [23], [24].

An often-overlooked aspect of security awareness is its integration with incident response procedures. Training should focus on identifying risks, correct responses, and potential security incidents. This means that employees should know who to contact when they identify suspicious activity, employees should understand the proper procedures for reporting incidents, and training should ensure that employees can react quickly and appropriately to mitigate damage from a breach. The incident management standard provides the best practices for incident management and emphasizes the importance of educating staff on recognizing and responding to security incidents. Incident management standards state that organizations should include staff training as part of their incident response plan, which ensures personnel are ready to support incident response efforts when needed [31].

To summarize security awareness and training in terms of governance, it is important for a robust plan to have some principles. Based on what's covered here, there are five principles that guarantee an organization a good security training and awareness program. Beginning with IT and OT personnel, ensuring that the program covers both IT and OT security challenges and integrates them, if needed, is essential. While IT security focuses on protecting digital data and systems, OT security must consider the physical aspects of cybersecurity, like cyber-physical systems. They have quite different aspects of the security topic that should be covered. The second thing is the training of all personnel – security awareness is a shared responsibility in an organization. Providing training for everyone from executives to contractors and different roles at different levels is essential. Ensure that everyone is receiving security awareness training essential to their roles and responsibilities in an organization. The third is the usage of real-world scenarios – This would mean incorporating real-life examples or simulations into the mix to make training more engaging and relevant. This includes phishing simulations and tabletop exercises for organizations. Number four is continuous reinforcement, which means that security is not a one-off event. Utilizing continuous reinforcement through newsletters, updates, posters, and any fresheners is relevant to maintaining people's interest in security practices. Number five, and finally, measure and adjust, which means regularly assessing the effectiveness of your security awareness programs. This means tracking metrics like simulation results, incident response times, and employee feedback to make data-driven adjustments. The

organization will ensure that security awareness and training are sufficient by following these five practices.

5.5.8 Legal and Regulatory Considerations

Adhering to legal and regulatory requirements is basically the cornerstone of IT/OT governance. Compliance ensures that organizations operate within the law and follow industry best practices, which protects them from sanctions and operational disruptions. In both IT and OT environments, strong governance includes mapping out all applicable laws and regulations and integrating those requirements into security policies and processes. The proactive approach fulfills legal obligations and strengthens cybersecurity and resilience. If not followed, non-compliance with regulations in Europe can lead to severe consequences. Financial penalties are a primary risk – for example, failure to comply with EU cybersecurity laws like NIS2 can incur fines up to 10 million euros or 2% of global turnover, and GDPR violations can reach 4% of annual worldwide revenue or 20 million euros [16], [42]. Beyond the fines, the organizations face reputational damage and operational disruptions if they neglect compliance. A major security breach in an OT environment can halt production, endanger safety, and tarnish an organization's reputation for a long time. European regulations have been increasingly focused on cybersecurity and data protection, introducing many regulations to raise security standards across Europe, including the up-and-coming Radio Equipment Directive update regarding cybersecurity coming later in 2025 [43], [44], [45]. Therefore, Compliance is not just a legal formality but is essential for avoiding costly penalties, maintaining trust, and ensuring uninterrupted operations.

The governance documentation should reference the major regulations and standards that define IT/OT security obligations. For Europe, several key frameworks, such as NIS2, GDPR, RED, and ISO/IEC Standards, set the baseline for compliance.

Beginning with the NIS2 directive, which has been a hot topic for the past couple of years. The EU’s updated network and information security directive imposes strict cybersecurity governance requirements on the operations of essential and important society services. NIS2 expands the score to 18 critical sectors and requires organizations to implement risk management measures and report significant cyber incidents to national authorities [16]. By directive, top management is made accountable for non-compliance, bringing cybersecurity to the boardrooms. Entities must adopt policies for risk analysis, incident handling, business continuity, supply chain security, and so on to ensure a high level of security.

GDPR is another regulation that was a hot topic in 2018 and, for some, still is. The legislation is Europe's foremost data protection law that mandates how personal data is processed and secured. GDPR requires organizations to implement appropriate technical and organizational measures to protect personal data and ensure privacy [42]. It also introduced breach notification obligations for personal data breaches to authorities within 72 hours and punitive fines for non-compliance, which can be up to 4% of global annual turnover for serious violations [42]. The GDPR's influence also extended beyond the EU, setting a high bar for data security and privacy practices worldwide.

The international information security standards also discuss legal and regulatory compliance. ISO 27001 specifically addresses legal and regulatory compliance, requiring that legal, contractual, and general requirements for information security are identified, documented, and kept up to date in organizations [18]. In practice, this would mean that organizations have to maintain a compliance register of all applicable laws/contractual security requirements and incorporate those into the information security management system. The standard also provides a structured framework to align security controls with these obligations and undergo regular audits to verify compliance. The companion guidance standard to ISO 27001, ISO27002, also discusses the best practices in more detail. ISO 27002 helps organizations translate legal requirements into concrete measures. For example, it provides guidance on how to implement control by establishing a legal register and compliance processes [24]. From a wider perspective, ISO 27002 outlines security controls organizationally, regarding people, physically, and technologically, and notes how each control can support compliance with laws and regulations [24]. ISO 27002 is often an organization's way of ensuring that they meet obligations with data protection, access control, incident response, and other areas mandated by the law.

Industrial automation and control system security standards focus on OT security management, as the name states. IEC 62443-2-1 outlines the requirements for establishing an effective security program for industrial automation and control systems, specifically for asset owners [23]. It covers governance policies and procedures tailored to industrial control systems, aligning OT operations with security and regulatory expectations. The regulatory considerations outlined in IEC 62443-2-1 encompass risk assessment, access control, incident response, and system hardening, all of which are specifically tailored for industrial environments [23]. The standard helps organizations in OT-heavy sectors comply with

industry-specific regulations and general cybersecurity laws by following the already recognized best practices for control systems security.

In addition to broad frameworks, many industries have specialized guidelines that should be followed. For example, ISO 27019 provides information security controls tailored to the energy utility industry, extending the guidance of ISO 27002 to power generation and distribution environments [40]. Lately, the financial sector has also been subject to regulations like the EU's Digital Operational Resilience Act (DORA), which was enacted in 2023 to ensure banks and financial entities can withstand and recover from cyber disruptions. Healthcare organizations must follow not only GDPR for patient data but also healthcare-specific cybersecurity frameworks, for example, ISO 27799 [41]. The sector rules complement the general ones, addressing unique risks in the environment and requiring tailored controls. Governance programs should catalog any such specific standards alongside the general EU regulations to ensure full compliance in the relevant industry context.

After covering the regular grounds for compliance. Achieving compliance requires a systematic approach to identify the requirement, implement controls, and prove adherence. It begins with identifying applicable laws and regulations, proceeding to align security policies with legal obligations, and then maintaining the documentation and audit trails. Identifying applicable laws and regulations is the first step. Which laws, regulations, standards, and contractual requirements apply to operations? This depends on the industry, services, data handled, and countries of operation. A best practice is to compile a legal and regulatory register listing all relevant cybersecurity obligations [18]. For example, a company might list GDPR, NIS2, and clients' contractual security clauses in this register. Consulting legal experts and monitoring regulatory updates in the field helps to ensure the list is complete and current as new requirements emerge.

The next step is to align security policies with legal obligations. Each regulatory requirement should be mapped to the organization's internal controls and policies. In practical terms, this means embedding compliance into the information security policy, procedures, and risk management process. For instance, if a law requires data encryption or incident reporting, the organization's security policy should explicitly cover those. ISO 27001 supports this alignment by requiring that controls address identified legal requirements in the organization [18]. By aligning policies and technical measures to the law, the organization ensures it builds in

compliance – reducing the risk of non-compliance by design. The integration helps to avoid gaps as it ties compliance into day-to-day operations rather than treating it as a separate effort.

Proper documentation is also vital for demonstrating compliance. Organizations should document how each requirement is met. For example, maintaining evidence of risk assessments, security configurations, training records, and data processing activities should be documented and clearly displayed to demonstrate compliance. Compliance documentation can include policies mapped to relevant regulatory clauses, meeting minutes that document oversight, and logs of security events. A proper audit trail of changes and decisions provides accountability for the organizations. Regulators and auditors will expect to see records for instance, ISO 27001 states that organizations must be able to show records of internal audits and results as evidence of their compliance efforts [18]. It is also mandated to maintain up-to-date records of applicable requirements and actions taken to meet them in ISO 27001 control points [18]. To summarize, it means that organizations document their actions and adhere to the documented procedures, creating a traceable link between requirements and evidence that those controls are functioning. Thorough documentation and logging significantly ease internal and external audits, reducing legal risk by demonstrating due diligence.

Effective governance extends beyond internal practices to encompass third parties and an ongoing risk management process focused on compliance; this is where legal and contractual compliance management steps in. Organizations must manage security requirements in their supply chain and vendor agreements. GDPR and NIS2 flow down obligations to service providers, as an example to those under GDPR, which require data processors to implement security measures by contract [42]. To ensure compliance, organizations should incorporate specific security and privacy clauses into contracts with vendors, suppliers, and partners. The contract should comply with standards such as ISO 27001 certification, adhere to applicable laws, permit regular audits, and promptly report any incidents. A robust vendor risk management is highlighted in the recent NIS2 directive, as it takes a strong stance on risk management and third parties [16]. Key practices for effective third-party and supplier compliance include conducting due diligence on third parties' security postures, requiring them to sign data protection agreements, and continuously monitoring their compliance. Contractual obligations should cover confidentiality, data protection, incident notification timelines, and compliance with regulations relevant to the service provided. Suppose these expectations are clearly defined and monitoring fulfilled. In that case, an organization mitigates the risk that a

supplier breach or lapse in compliance will, in turn, cause the organization to violate its own legal obligations.

Regulatory compliance should be integrated into the organization's risk management framework as well. This means treating non-compliance or legal penalties as a risk to be assessed and mitigated, just like any other risk. ISO 27001 requires organizations to consider the needs and expectations of stakeholders, including regulators and legal requirements, when evaluating risks and developing their information security management system [18]. This ensures that legal obligations are factored into risk management. ISO 27005 also covers guidance on identifying risks, including compliance risks and analyzing their likelihood and impact [34]. For example, a risk register might include scenarios such as noncompliance with GDPR, leading to fines and data loss, with an assessed impact level. This enables organizations to identify and address these risks effectively, acknowledging them as necessary. Mitigating such risks could be implementing additional controls or training to reduce the chance of a violation. Regular risk assessments should cover changes in the regulatory landscape. Regular risk assessments should cover changes in the regulatory landscape as well. By integrating compliance into risk management, organizations can prioritize resources to areas of high legal exposure and can show regulators a documented, proactive approach to meeting obligations. The process also aligns with ISO 27001, which requires that information security management systems consider legal and regulatory factors in their scope and risk criteria while also satisfying ISO 27005 by systematically managing compliance-related risks [18], [34].

Ongoing auditing and transparent reporting are key components of governance to ensure that compliance is maintained and demonstratable, which starts with internal audits. International standards require organizations to periodically verify their own compliance through internal audits. ISO 27001 mandates that organizations conduct internal audits at planned intervals to determine whether the information security management system conforms to the organizations' requirements as well as the ISO standard [18]. This would mean scheduling regular internal audits to review the effectiveness of security controls and check that legal requirements are being met. Internal auditors should look for evidence that policies are implemented, risks are managed, and controls are functioning as intended. Any non-conformities or compliance gaps discovered should be addressed with corrective actions. The internal audit process, as part of the information security management systems continuous improvement cycle, provides management with assurance that the organization remains in compliance with external audits or regulatory inspections. ISO 27001 also emphasizes the importance of maintaining an audit

program and records. Therefore, organizations should implement and document audit plans, criteria, findings, and follow-up actions as evidence of their compliance oversight [18].

Many regulations involve oversight by external parties or authorities. Organizations certified to ISO 27001 will undergo periodic certification audits by independent auditors [18]. Similarly, in regulated sectors, national authorities may conduct inspections or require compliance reports. The NIS2 directive established tighter supervisory measures, requiring essential entities to be subject to proactive audits or inspections by authorities. Additionally, essential entities may be supervised reactively, for example, following an incident [16]. In any case, organizations must be prepared to demonstrate their cybersecurity governance, risk management, and incident handling processes to regulators. This includes keeping documentation ready for review and staff prepared to answer questions during audits. Reporting obligations are another critical aspect: under NIS2, companies must report significant incidents to their national authority within tight timelines and, in some cases, provide summary compliance reports [16]. For example, the GDPR may require data protection impact assessments and breach reports to be shared with authorities [42]. Best practices for compliance reporting include establishing clear internal procedures for escalating issues to the appropriate compliance team, collecting evidence of security controls in an organized manner, and using standardized report formats.

When security incidents occur, legal obligations come rapidly into play. Governance frameworks must incorporate incident response planning that satisfies regulatory requirements, especially around breach notification and post-incident analysis. Two major European regulations impose strict duties to report security breaches. Under the GDPR, if a personal data breach occurs, the data controller must notify the supervisory authority without delay and not later than 72 hours after being aware of it [42]. This notification must include information on the nature of the breach, affected data, remedial actions, etc. If the breach is serious for individuals with a high risk to their rights and freedoms, the GDPR requires informing the affected data subjects as well [42]. The NIS2 directive defines a tight timeline for reporting network and information system incidents. Organizations under NIS2 must deliver an early incident report within 24 hours of becoming aware of a significant incident, a more detailed notification within 72 hours, and a final report within one month [16]. The phased reporting aims to ensure that authorities are alerted quickly and updated as more details emerge. These legal timelines mean that incident response teams need to detect, assess, and escalate incidents rapidly. Failure to notify within the required window can itself be a compliance violation, leading to fines. This means that a compliance incident response plan should include clear steps

for prompt notification for both internal stakeholders and external regulators. Regular drills and training on incident response can help organizations meet these strict deadlines even under crisis conditions.

Adopting formal incident management frameworks helps organizations effectively meet their legal obligations. ISO 27035 provides a structured approach to incident handling from preparation through to lessons learned [31]. It emphasizes the importance of being ready for an incident, having clear response strategies, and ensuring efficient recovery, all aligned with the organization's policies [31]. If ISO 27035's guidance is followed, the organization will naturally create many elements that regulations expect, such as defined roles and responsibilities for incident handling, procedures for analysis and containment, and communication plans for notifying the appropriate parties. In addition, NIS2 explicitly requires incident response capabilities, discussing incident handling and crisis management as essential security measures for incident scope entities [16]. This means that under EU law, having an incident response plan is not just a best practice but a legal requirement for many organizations. Governance documentation should include an incident response plan that references both ISO 27035 and legislation. Key components include incident detection and reporting processes, a defined incident response team, investigation and containment steps, criteria for when to notify regulators or customers, and finally, post-incident review.

Summarizing the legal and regulatory considerations with a couple of best practices for effective governance. First is keeping up to date with evolving requirements. The regulatory landscape is continually evolving. New laws, such as the EU Cyber Resilience Act, which focuses on product security, and updates to NIS2 and GDPR guidance, can introduce additional obligations [46]. It is crucial to have a process for monitoring and reviewing changes in legislation and standards. Governance should track EU directives, national laws, and updates to international standards. For instance, if the EU introduces new regulations for IoT devices or an existing standard like ISO 27001 is revised, the organization should promptly determine the impact on its compliance programs. Subscribing to regulatory newsletters, participating in industry associations, or consulting legal counsel annually are common practices to stay informed. This way, policies and controls can be adjusted proactively before new rules come into force. Keeping a compliance calendar for upcoming laws and reviews can prevent surprises.

Treating compliance as an ongoing project rather than a one-time task was highlighted quite a few times. Organizations should perform periodic assessments, for example, annual compliance audits or semi-annual gap analyses, to evaluate how well each requirement is met. An internal compliance audit might review GDPR controls in one quarter and NIS2 readiness in the next. These reviews will aim to identify any gaps or areas of partial compliance so that remedial actions can be taken in a timely manner. It is wise for an organization to conduct a formal legal review at least once a year, where experts examine any changes in law or business operations that could introduce new compliance needs. Tools like compliance checklists or frameworks like ISO 27002 can be helpful in structuring assessments. Remember that maintaining compliance is a continuous cycle of evaluating and improving. Documentation from the assessments should be retained as evidence for due diligence.

And finally, people are a critical component of compliance. Even with strong policies, an unaware workforce can lead to accidental breaches of law, like mishandling of personal data. Therefore, the best practice is to include regulatory topics in the organization's security awareness and training programs. Employees should be educated on key obligations relevant to their role – for example, developers should know about secure coding requirements and privacy by design under GDPR, operators in a plant should understand any safety-related cybersecurity regulations, and all staff should grasp the importance of protecting personal data. Training should also cover how to recognize and respond to security incidents in line with the incident response plan. Many frameworks explicitly mandate training. For instance, NIS2 requires organizations to implement “basic cyber hygiene practices and cybersecurity training” [16].

All in all, legal and regulatory compliance with IT/OT governance frameworks is essential for effective and thorough security programs. A governance model that treats compliance as a continuous requirement will ensure that security and privacy are maintained in accordance with the law. Aligning internal policies with international standards and EU regulations provides dual benefits, satisfying regulators while improving the organization's security maturity. Adhering to global frameworks, following legislations, and respecting laws brings credibility to the market but also bolsters operational resilience. Customers, partners, and regulators gain confidence that the organization is managing risks responsibly and can be trusted with sensitive systems and information. Governance documents should, therefore, clearly reflect compliance considerations at every level, from executives to technical controls. With the 500% growth in darknet marketplace credential dumps and the rising use of stealer malware like Redline, the

need for governance to extend to identity protection and third-party access control has become more critical [19].

5.6 Security (Operational Security) Domain: Monitoring, Incident Response, and Enforcement

The security domain focuses on the operational execution of cybersecurity controls within industrial IT/OT systems. While governance defines policies and structures, operational security ensures that protective measures are actively enforced, monitored, and adapted to evolving threats daily.

This section applies technical and procedural controls based on IEC 62443-3-3 for system-level protection, IEC 62443-2-1 for security program management, and ISO 27035 for incident response and event management. It also incorporates insights from industry reports highlighting the need for real-time detection, anomaly monitoring, and proactive handling.

Topics such as network monitoring, vulnerability management, security event logging, access control enforcement, and incident response readiness are addressed. Operational security bridges the gap between policy and practice, ensuring that security objectives are realized within the dynamic realities of industrial environments.

5.6.1 Access Management

Access management is a fundamental security practice that ensures only authorized users, applications, and devices can access IT and OT environments. Effective asset management minimizes the risk of unauthorized access, insider threats, and privilege escalation attacks. Access management regulates and limits entry to systems, networks, applications, and data, adhering to established policies and security guidelines. In contrast, identity and access management is a framework that manages user identities, authentication, and access permissions across an organization. This is important in industrial environments, namely, preventing unauthorized access to critical OT systems like SCADA and industrial controllers while enforcing least privilege access to minimize attack surfaces across the organization.

We should start with role-based access control and the least privilege principle to break down asset management. With role-based access control and the least privilege principle, we aim to restrict access based on user roles and business needs while keeping it to a minimum. In practice, this could mean time-based access controlling, assigning read, write, and full-control

accesses with care in mind, and limiting administrative privileges to only specific personnel. Industrial standards require role-based access controls for industrial environments, but it is recommended to enforce least privilege access across all the IT and OT systems [22], [24]. While limiting access is important, so are the login methods and authentication. Utilizing multi-factor authentication strengthens authentication mechanisms by requiring multiple forms of verification. In OT environments, this could mean utilizing MFA for remote access to OT environments or utilizing one-time passwords for privileged actions within critical applications. For industrial environments, multi-factor authentication is recommended, especially in critical applications and for high-risk applications [24], [35]. Fortinet's threat telemetry shows that 70% of cloud compromises involved suspicious logins from unknown locations, reinforcing the security domain's focus on authentication strength and anomaly detection [19].

Identity and access management are important in access management. Centralized control over user identities and access rights allows for better management across the systems. This could mean integrating the AD of a LDAP for centralized authentication and implementing single sign-on to streamline access control in IT and OT applications. Identity and access management system usage is recommended for managing access across enterprise environments [24]. Identity and access management does not only mean regular accounts that we have, but also privileged accounts. It is essential to secure and monitor privileged accounts with enhanced controls. This could mean using privileged account management solutions to enforce strict control over admin accounts or require session recordings for access to critical systems. Privileged access management solutions are recommended for securing industrial systems, but are also advised to protect privileged credentials [22], [24].

Network segmentation and access control go quite a bit hand in hand. Restricting access between network segments minimizes risk across the organization. This could mean enforcing air-gapping or firewall rules between IT and OT networks or using VLANs to isolate critical assets and reduce unauthorized lateral movement. Implementing Zero Trust Network Access principles to ensure continuous access verification. Network segmentation is one of the core principles for industrial control system security, but access control through network segmentation is generally not supported [23], [24]. While segmentation helps with access control, it also limits, which is why it is essential to have remote access in good hands with suitable security measures. Requiring a VPN with MFA for remote access to industrial environments could be one reasonable way to implement jump hosts to control and log remote connections, limit remote access to maintenance windows, and enforce session recordings.

Defining security requirements for remote access in industrial environments is one step of the way, but it is also advised to secure remote access through strong authentication and encryption [24], [35]. Logging and auditing the access control is one step of the way as well. It is recommended to maintain logs of all access entries for monitoring and compliance; the benefit of this is continuous monitoring, incident response, and forensic investigation [23], [33]. In Practice, this would mean enabling audit logging for all authentication and privilege escalation events, analyzing access logs in security information, and event management with the implementation of real-time alerts for suspicious access patterns.

Implementation of access management is a strategic question and can take quite a bit of effort from the organization. One method of managing this is through zero trust access control, which enforces continuous verification of user identities and the trust levels of devices. This would mean implementing least privilege access for all users, even within trusted zones, and using adaptive authentication that changes security requirements based on user behavior. Zero trust principles are recommended for critical and industrial environments [22]. Access certification and review processes are also implementation methods. Reviewing user access rights to detect and remove unnecessary privileges minimizes the attack surface over time. Practically, it would be conducting quarterly access reviews for IT and OT environments and implementing automated de-provisioning of accounts for departing employees. Regularly reviewing access enables organizations to uphold security compliance and reduce attack surfaces, which is why security standards advocate for this practice [24]. Implementation also means implementing access management into incident response. This would mean automatically disabling accounts associated with security incidents and implementing behavioral analytics to detect compromised accounts and trigger automatic lockouts. Integrating access control with incident response plans is recommended for fast response [31].

Last, alongside the implementation methods, it is also highly important to ensure documentation and compliance. When creating documentation for access management policies, the organization must define and enforce rules regarding users and system access. Organizations should strive to have documented access control policies in place for both systems and users [18]. In practice, this would mean developing a document specifying access levels for different user roles and creating and maintaining an access control matrix to document permissions for critical applications. It is also essential to ensure access management alignment with industry standards and legal requirements while creating the documentation. It is good to enforce NIS2 compliance by maintaining strict access logs and security monitoring; this could

be the same for any industry-specific regulations or laws. Access control compliance is required from industrial suppliers [35]. Access management underlines the security of IT and OT environments and prevents unauthorized access and insider threats. Organizations can enforce secure and compliant access control measures by implementing role-based access controls, multi-factor authentication, zero-trust access, and regular access reviews.

5.6.2 Network Security

Network security is the foundation of protecting IT and OT environments from unauthorized access, cyber threats, and operational disruptions. Network security involves implementing segmentation, encryption, monitoring, and access control to safeguard network infrastructure and connected devices. Network security should be defined as securing network infrastructure, communication paths, and data flows to prevent cyber threats and unauthorized access to end devices. The importance of IT and OT environments lies in preventing unauthorized access and lateral movement between these environments. This ensures the confidentiality, integrity, and availability of critical operational data while mitigating risks from DDoS attacks, man-in-the-middle attacks, malware propagation, and insider threats.

Network segmentation and zoning are core components of network security. Dividing networks into segments reduces attack surfaces and isolates threats. In industrial environments, this would mean implementing the Purdue model, as explained in IEC62443-3-3, to separate IT and OT networks, creating industrial DMZs for secure communication links in IT/OT, and using firewall-based or air-gapped segmentation to limit traffic. Segmentation and zoning are recommended and often required for industrial networks, and segmentation is generally advised to protect critical assets from cyber threats [22], [24]. Establishing defense layers in the network to monitor and control incoming and outgoing traffic is also essential. We will call this perimeter security, and it could mean deploying next-generation firewalls to enforce security policies, implementing intrusion detection and prevention systems to detect anomalies, and whitelisting approaches to restrict unauthorized network connections. Defining perimeter security measures for industrial networks is recommended, as well as using firewalls and threat detection or prevention systems to monitor and control access [22], [24].

Network access control is one of the ways of enforcing security policies to regulate device and user access to networks. This could mean implementing 802.1X authentication for wired and wireless networks, using MAC address filtering to restrict devices, or deploying zero-trust network access to validate users and devices continuously. Restricting access to industrial

networks is always recommended, but strong authentication and access control are also encouraged at the network parameters [24], [35]. While we are limiting access and ensuring continuous authentication, we should also ensure secure remote connections to IT and OT networks for employees and third parties. Remote access security requirements are listed in the industrial standard IEC 62443-2-4, and it is advised to secure remote access through encryption and authentication [24], [35]. Practically, this could require a VPN with multi-factor authentication for remote access, implementing jump hosts to mediate remote connections to industrial environments, and using time-based access controls for vendor maintenance sessions.

Industrial standards require encryption to secure industrial network communications, and it is generally recommended that sensitive network data transmissions be encrypted [22], [24]. Encrypting network traffic is to prevent interception and data manipulation. This could mean using TLS or IPSec for encrypting communication between devices. This could also mean replacing unsecured protocols where applicable with secured protocols and deploying VPN encryption for remote connectivity. Wireless network security is also part of securing traffic while in transmission. Securing wireless communications within IT and OT environments is essential for security. Restricting wireless network exposure in industrial environments is generally advised, but encryption and authentication are recommended for wireless security measures [22], [24]. Practical examples of this would be enforcing newer encryption like WPA3 for wireless networks, implementing RF shielding and wireless intrusion detection to detect rogue APs, restricting Wi-Fi access to OT devices, and preferring wired connections for critical systems.

Monitoring our networks is just ensuring that every security measure is in place, and if it isn’t, then we can have fast-acting solutions to fix it. Network monitoring is recommended to detect suspicious activity in the network, and in industrial environments, it is required to be monitored [23], [24]. Implementing network security monitoring tools to analyze traffic patterns is an example of monitoring with security information and event management tools, as well as deploying anomaly detection to identify anomalies. It all comes down to solid monitoring solutions and knowing when something isn’t expected in our environment. Redundancy and high availability are also key factors in network security. Ensuring network security measures remain operational even during failures is redundancy at best. This means dual firewalls with active/passive failover, redundant VPN gateways to ensure uninterrupted remote access, and implementing load balancers to distribute traffic across multiple security appliances. Redundancy is encouraged for critical security infrastructure, while the network is the backbone

[24]. It should also be required, and high-availability and failover mechanisms should be supported in industrial environments [23].

As network security is quite an extensive topic in security, the implementation doesn't have to be too complicated. Implementation of network security can be as simple as implementing a Zero-Trust Network Architecture. The basic ideology is that an organization assumes that no entity is trusted, enforcing continuous authentication. In practice, this could mean dividing network zones to minimize attack surfaces – it is called micro-segmentation, and implementing least-privilege network access, which would mean restricting users based on business needs. Industrial standards generally support the least privilege ideology and support the implementation of zero-trust network architecture principles for industrial networks [22]. The implementation of network security also means patch management for network devices. Regularly updating network firmware and software to mitigate vulnerabilities is recommended and often required to maintain up-to-date network security controls [22], [24]. In practice, it is implementing automatic firewall firmware updates to prevent exploitation, applying router and switch patches on a controlled schedule, and ensuring that the controlled schedule stays in place.

Network security policies and standards should be set in stone by the organization, and this is done by developing documentation about network security policies outlining firewall rules, segmentation, and monitoring, as well as including an incident response plan specific to network breaches. Documentation of the security policies is recommended, but also, in some cases, defined by the standards [24], [35]. A solid network security policy brings the organization closer to enforcing it in practice. Network security is essential for protecting IT and OT environments from cyber threats and unauthorized access. Organizations can create a resilient and compliant network security architecture by implementing segmentation, encryption, monitoring, access control, and zero-trust principles.

5.6.3 Endpoint Security

In endpoint security, we protect end-user devices, servers, industrial control systems, and networked assets from cyber threats such as malware, unauthorized access, and exploitation. In IT and OT environments, endpoint security is critical for maintaining system integrity, preventing the lateral movement of threats, and ensuring compliance with cybersecurity frameworks. In practice, we aim to prevent malware infections, ransomware attacks, and unauthorized access while keeping integrity and availability in mind for industrial operations.

Endpoint security refers to the process of securing devices such as workstations, servers, industrial devices, IoT devices, and mobile endpoints from cyber threats.

Endpoint detection and response programs, along with endpoint protection platforms, are indeed central to endpoint security in modern environments. Endpoint detection and response programs provide continuous monitoring, real-time threat detection, and automated responses for secure endpoints. In contrast, endpoint protection platforms offer antivirus, anti-malware, and host-based firewall protection for these endpoints. It is generally advisable to employ endpoint monitoring and threat responses, including automated mechanisms, particularly for industrial endpoints [22], [24]. Endpoint detection and response solutions identify suspicious activities at the source and report them, potentially utilizing behavioral analytics to recognize abnormal endpoint behavior. This might also involve automated containment actions. While endpoint protection platforms aim for similar outcomes, they tend to focus more on preventative measures. This includes techniques like whitelisting and blacklisting to manage applications on endpoints or using sandboxing to execute suspicious files in a controlled setting. Industrial standards mandate anti-malware protection for industrial endpoints, and it is generally recommended that endpoint security controls be implemented accordingly [24], [35]. Ensuring all endpoints are updated and patched against vulnerabilities is, again, a good preventative action. Deploying automated IT systems patching solutions while following controlled patching schedules for critical systems ensures endpoint security. Vulnerability scanning can identify missing patches across endpoints, and while all systems can't be patched, organizations can go ahead and implement virtual patching when real-time patching isn’t a feasible option. Timely updates are recommended with vulnerability remediation, and structured patch management practices are often required in industrial environments [23], [24].

Endpoint access control and authentication are one way to handle endpoint protection. This means restricting unauthorized users and devices from accessing critical endpoints. In practice, this would mean implementing multi-factor authentication for all administrative endpoints, using zero-trust network access to verify endpoint access continuously, and restricting endpoint access using role-based access controls. Industrial standards require strict access controls for industrial endpoints, but strong authentication mechanisms are also required [22]. Application and device control would fall under the restriction of endpoint devices. Application and device control would restrict unauthorized applications and devices from running on endpoints. This would mean enforcing application whitelisting to block unauthorized software and implementing USB device control to prevent unauthorized data transfers or malware infections.

Whitelisting and blacklisting is recommended in industrial environments, but also restricting unauthorized software and removable devices in general [22], [24]. Application and device control is also a valid option to force the maintenance and upkeep of asset management.

Industrial control systems are a specific branch for endpoint security – we need to secure human-machine interfaces, programmable logic controllers, remote terminal units, and distributed control system endpoints from cyber threats. Often, the solution is to use air-gapped systems where possible to limit exposure, but it can also mean using host-based firewalls on industrial endpoints to restrict communications and deploying hardening measures to disable unused services. Industrial endpoints are required to have hardened security configurations for industrial systems while also providing security standards advice on securing industrial endpoints from external threats [24], [35]. In industrial environments, we should have data loss prevention methods for endpoints, which ensure that unauthorized data exfiltration or leaks do not happen from endpoints, especially for sensitive data. This could mean utilizing data loss prevention systems to monitor and block sensitive data transfers or implementing endpoint encryption for devices handling critical data with device control policies to block unauthorized file transfers. Encryption and data protection methods are recommended for industrial endpoints, but it is also required to have data loss prevention methods for protecting sensitive information inside the organization [22], [24].

Implementing endpoint security doesn’t have to be too complicated. There are a few straightforward topics – zero trust endpoint security model, endpoint incident detection, and response- that cover a lot of the ground. With the zero-trust endpoint security model, we apply continuous verification and least-privilege access to endpoint security, which means implementing identity-based security policies for endpoints, restricting communications using micro-segmentation, and continuously monitoring endpoint health before granting network access. Zero trust principles are generally supported for industrial security [22]. Endpoint incident detection and response brings the implementation of endpoint security together with preventative methods of zero trust. Enabling rapid identification and response to endpoint security incidents with endpoint security platforms and security information event management systems pushes organizations towards fast mitigation of risks and good analysis of the environment. It also allows the organization to use automated incident containment tools with proper forensic analysis on compromised endpoints. IT security standards require incident response integration with endpoint security, and for industrial environments, forensic analysis and continuous monitoring are supported [23], [33].

Documentation and compliance are as essential to endpoint security as anything else on our list. Ensuring that endpoint security policies are formally listed for endpoint management. The documentation of endpoint security policies is required for ISO 27001 compliance [18]. This would require developing an endpoint security baseline to enforce security controls and maintaining a device inventory to track all endpoints within IT and OT environments. And while documenting the process is essential, so is compliance with industry regulations. Ensuring that endpoint security aligns with legal and regulatory requirements is recommended beforehand. A strong example would be complying with the NIS2 directive, which is essential for securing critical infrastructure endpoints, and another would be deploying GDPR-compliant encryption to safeguard sensitive data. Overall, industrial standards require endpoint protections to comply with the industrial control system security regulations [22]. Endpoint security prevents malware, unauthorized access, and system compromise in IT and OT environments. By implementing the points shown here, organizations can effectively secure their endpoints.

5.6.4 Monitoring and Incident Detection

Monitoring and incident detection are essential for identifying, analyzing, and responding to security threats in IT and OT environments. Effective real-time monitoring and automated threat detection ensure that suspicious activities are identified before they have the possibility to escalate into major security incidents. With monitoring and incident detection, we aim to prevent undetected intrusions that could lead to system disruptions or data breaches and ensure early warning systems for malware, insider threats, and cyberattacks. Through Monitoring, we strive to consistently observe network traffic, user actions, system logs, and endpoint behavior to identify anomalies. Incident detection involves recognizing security breaches, vulnerabilities, and suspicious activities, utilizing both automated tools and manual analysis derived from monitoring efforts.

Security information and event management systems (SIEM) play a critical role in monitoring. They aggregate and analyze security logs from firewalls, endpoints, servers, and OT devices. Implementing security information and event management solutions for centralized log analysis is just the beginning; it is also essential to configure real-time alerts for unusual login attempts and privilege escalation and employ log correlation to identify patterns indicative of advanced persistent threats. It is recommended to use security information and event management for continuous monitoring and compliance, but industrial systems must also be integrated into

security information and event management [22], [24]. Intrusion detection and prevention systems are working alongside security information and event management systems. Intrusion detection systems monitor for suspicious activities, while intrusion prevention systems block malicious traffic. Implementing intrusion detection and prevention systems could mean deploying host-based intrusion detection to monitor logs on individual devices or using network-based intrusion detection for traffic analysis in IT and OT networks. Implementing signature-based detection for known threats and behavioral anomaly detection for zero-day attacks is also recommended. Intrusion detection capabilities are required in industrial networks by standards, but intrusion detection and prevention for network security monitoring are also advised [22], [24].

Endpoint detection and response protect endpoints from malware, ransomware, and unauthorized access. This would mean deploying endpoint detection and response to monitor endpoint activity, implementing automated response mechanisms, and machine learning-based threat detection at endpoints. Similar technologies are Anomaly detection and behavioral analytics, which are often AI-driven analyses to detect unusual user, network, or system behavior. This would mean utilizing user and entity behavior analytics to track deviations from regular activity and utilizing AI-driven anomaly detection in industrial network monitoring. Both methods of endpoint security monitoring in OT environments with automated threat detection support endpoint security [24], [35]. Additionally, it is recommended that anomaly detection for OT security and continuous anomaly detection in IT be utilized with advanced technologies [22], [24].

Using threat intelligence and attack surface monitoring helps an organization detect external threats. Managing attack surface would mean implementing external attack surface monitoring to identify exposed services, and threat intelligence would suggest subscribing to threat intelligence feeds like NIST NVD. It would also mean utilizing honeypots to attract and study attackers targeting industrial environments. Threat intelligence services integration is suggested for incident management and proactive security measures, but it is also supported for industrial cyber risk assessment [23], [33]. The organization should also put additional effort into industrial control system security monitoring. Specialized monitoring tools and industrial network system monitoring are recommended to detect anomalies in SCADA systems, PLCs, and other industrial specialized equipment. This would mean using Industrial-specific threat detection tools, monitoring industrial tools-specific protocols for unusual commands or traffic patterns, and implementing passive monitoring to avoid disrupting critical processes. Industrial

standards require ISC security monitoring as part of OT defence-in-depth and security standards support, utilizing specialized monitoring solutions for operational security [22], [24].

The security operations center is one way of putting continuous monitoring into practice. When needed, a centralized security operations center handles real-time security monitoring, alert triage, and threat response. While talking about IT and OT environments, it would be preferable to establish our own dedicated OT security operations center teams for monitoring industrial networks, implementing automated incident response playbooks to accelerate mitigation, and integrating security orchestration, automation, and response for faster response times. Incident response standards define security operations center best practices for incident detection, but it is also specified in industrial standards to have a dedicated security operations center for critical infrastructure around operational technologies [23], [31]. While it is recommended to have specific OT environment monitoring, it is also recommended to integrate IT and OT security monitoring for unified threat detection. This would mean connecting IT security information and event management systems with OT monitoring tools for cross-domain event correlations. It would also be beneficial to look into IT/OT incident response coordination for rapid containment of threats. IT/OT convergence is recommended for security monitoring [22]. Especially once IT and OT environments have been converged to the same platforms for unified threat detection, it is also important to ensure that logs are stored, analyzed, and protected for forensic investigations. Practically, it is good to retain SIEM logs for at least one year for compliance audits, encrypting security logs to prevent tampering, and implementing log access controls to prevent insider threats. Security standards require log retention and protection policies, but industrial standards also define log security requirements for industrial environments [24], [35].

Incident detection policies and procedures have to be listed as well. Developing a monitoring policy document specifying security information event management system, intrusion detection and prevention system usage, and anomaly detection should be listed. Also, detailed logs for detected incidents should be held for forensic investigation purposes. Security standards require documentation of security monitoring policies and procedures to be held [18]. Monitoring and incident detection are critical defense layers against cyber threats in IT and OT environments. Organizations can enhance their cybersecurity posture and defenses by utilizing the topics discussed in this chapter, bringing together the whole security monitoring and incident detection.

5.6.5 Incident Response and Recovery

Incident response and recovery ensure that organizations can quickly detect, contain, and recover from cybersecurity incidents in IT and OT environments. A well-prepared and structured incident response plan and disaster recovery strategy minimize downtime, prevent data loss, and maintain business continuity. Incident response is the process of detecting, analyzing, containing, and mitigating cybersecurity incidents, while recovery is the restoration of systems, data, and operations to a normal state after a security event. With incident response and recovery, we aim to reduce the impact of ransomware attacks, data breaches, insider threats, and supply chain attacks while ensuring industrial resilience by minimizing operational disruptions.

Incident response starts with a plan – A structured process for responding to security incidents should be formed. Developing an incident response playbook with predefined actions should be done for various scenarios, and assigning incident response roles with escalation protocols to notify key stakeholders. Incident response lifecycles are defined in ISO 27035-1, and industrial standards require documented incident handling procedures for industrial control systems [23], [31]. Incident detection and classification are one step ahead for better incident response planning. Identifying and categorizing incidents based on severity and impact is essential for proper incident response. This could mean classifying incidents as low, medium, or critical based on the business impact, security information, and event management to correlate security events and using threat intelligence feeds to match detected indicators with known cyber threats. Incident detection methodologies are recommended alongside classification, and event logging and anomaly detection are recommended for industrial control systems security [22], [33].

Containment and eradication strategies are essential for incident response. We must define steps to isolate threats and remove malicious artifacts from affected systems. Practically, this would mean network segmentation to isolate infected endpoints from critical systems, blocking malicious IP addresses in firewalls and intrusion prevention systems, and deploying automated containment tools in endpoint detection and response to quarantine infected endpoints, for example. Standards require containment and mitigation strategies for industrial networks, and regarding incident response, it is encouraged to automate response workflows to minimize manual interventions [22], [31]. While containment is the first step in acting on threats, the second should be incident communication and, later on, reporting. Notifying internal teams,

regulatory authorities, and external partners about incidents is essential, which would mean establishing an incident response communication plan with predefined escalation paths. Incident communication procedures are supposed to be defined for enterprises, and industrial standards require suppliers to follow regulated incident disclosure policies [31], [35].

Recovery and restoration processes are essential for incident response. This would mean steps to restore systems, validate integrity, and resume normal operations. During an incident, we need to be able to ensure that restore backups are in a clean, verified state and validate security controls before reintroducing systems to production. Recovery and restoration processes would also include post-incident forensic analysis to determine the root cause. Business continuity standards define disaster recovery processes and their importance to business continuity, while industrial standards require a structured recovery planning for industrial operations [23], [30]. We've already opened the discussion for post-incident forensics, which can be integral for the organization to conduct post-mortem analysis to improve future incident response efforts or resilience. Practically, it would mean finding time to host a post-incident review meeting to discuss lessons learned and how they can be avoided. This would also mean updating incident response playbooks accordingly. In cases of humane errors, employee awareness training should be conducted to prevent similar incidents in the future. Incident response standards advocate for organized post-incident analysis to facilitate continuous improvement, while industrial standards mandate updating security response frameworks based on past incidents [33], [35].

Security Orchestration, automation, and response (SOAR) are key to incident response and recovery. It automates incident triage, containment, and response actions. Deploying SOAR platforms helps organizations automate response workflows as they see fit and implement playbook-driven responses for common incidents. Automation is encouraged for incident containment and response by incident response standards [31]. Bringing incident response to practice - a unified response with IT and OT security response teams helps with coordinated incident handling. Coordination would mean establishing a joint IT/OT incident response team for cross-domain attacks or utilizing OT-aware security tools integrated with security information and event management. The efforts for industrial regulations require joint collaboration for IT and OT teams anyway; therefore, it is recommended to have joint collaboration with security teams for critical infrastructure [22]. Cyber resilience and redundancy planning must also be considered while implementing incident response and recovery. Ensuring that organizations can withstand and recover from cyber disruptions.

Implementing geographically redundant services is key for high availability and for incidents not to happen, and it would also mean deploying redundant control systems to prevent complete OT shutdowns. Resilience strategies play a crucial role in incident response and recovery by averting critical incidents before they occur, making them essential for business continuity [30].

Documentation and compliance with incident response is the final key to the whole process. Establishing formal policies and workflows for responding to security incidents is crucial. This would require developing a cyber incident response plan and maintaining an incident register to document past events and mitigation actions. Documentation of incident response policies is necessary, while industrial standards also support supplier compliance with security response frameworks [18], [35]. With the introduction of new NIS2 regulations, it is now crucial to report incidents within 24 to 72 hours. It is advisable to maintain audit logs for all security incidents to support compliance. Compliance tracking is often recommended and required by other standards [33]. Incident response and recovery play a vital role in ensuring cyber resilience within both IT and OT environments. By adopting structured response plans, automated containment methods, cross-domain collaboration, and forensic analysis, organizations can enhance their cyber resilience and prepare for potential future challenges.

5.6.6 Physical Security

Physical security is a critical aspect of cybersecurity that protects IT and OT assets from unauthorized physical access, tampering, theft, or environmental hazards. A well-designed physical security strategy ensures that sensitive infrastructure, industrial control systems, and endpoints remain secure against physical threats. Physical security is the measures taken to prevent unauthorized physical access, damage, theft, or sabotage of critical IT and OT infrastructure. The aim is to prevent insider threats and unauthorized personnel access to control rooms and industrial facilities while reducing the risk of theft, tampering, and hardware-based cyberattacks like USB malware infections. The latest addition to physical security is that NIS2 regulation in Europe has physical security requirements for critical infrastructure with standards, but standards are not enforced by law.

The core of physical security starts with perimeter security and facility protection. The organization needs to restrict unauthorized access to its offices and industrial plants. It would mean installing fencing, barriers, and reinforced gates around industrial plants, using surveillance cameras with motion detection at entry points, and employing security guards for sites. Standards require organizations to implement physical protection measures for IT

systems, but also recommend facility access control for industrial plants [23], [24]. While we need faculty protection and perimeter security, there is also a clear need for access control and authentication in secure areas. This would mean limiting physical access to critical infrastructure locations. It could be completed with biometric authentication at high-security locations or using proximity-based smart cards for access. Visitor registration and escorted access for third-party contractors are also recommended. Industrial standards mandate physical access controls in industrial settings, and employing multi-factor authentication for such access is advisable [22], [24].

Regardless of the physical security measures, we should still use security cameras and monitoring systems to detect unauthorized physical activities. Deploying 24/7 monitored CCTV cameras for critical locations is one example of handling it and integrating access logs and security footage into security information and event management systems. Continuous monitoring and logging are required for critical facilities, while also industrial systems support monitoring and auditing of physical security events [24], [35]. Surveillance and monitoring are also good for figuring out the cause, and secure equipment and hardware protection are here to prevent theft, unauthorized modifications, and physical tampering with our equipment. It would mean locking server racks with tamper-proof enclosures, anti-theft cable locks for endpoint devices, and secure network cabinets with electronic locking systems. Safeguarding critical hardware and securing it from unauthorized access is required by the standards [23], [24]. Safeguarding is in the same category as preventing data leaks and unauthorized use of removable media and portable devices. Organizations are recommended to limit removable media access, and industrial standards require physical security measures for data-bearing devices [22], [24]. This would practically mean enforcing USB device restrictions on sensitive systems, ensuring that all stored data on portable devices is encrypted, or implementing geofencing policies to restrict device usage.

While physical security can be seen as keeping humans out of critical places, it also ensures that environmental hazards do not damage critical systems. This means installing fire suppression systems, controlling temperature and humidity, and implementing food-resistant enclosures. Security standards require environmental monitoring to protect IT systems, but industrial standards recommend taking environmental controls for OT systems [22], [24]. While we are protecting our physical security measures from everything we can, we should also consider that our security measures can also fail at critical times, so we need to ensure physical security remains in operation in all situations. Redundancy measures for physical security could

mean backup surveillance and alarm systems, and uninterruptible power supplies for security systems. Emergency response teams must also consider physical security measures during disaster recovery. Business continuity planning considers the physical infrastructure and disaster recovery planning, and industrial standards recommend disaster recovery planning and redundancy for industrial facilities [23], [30].

Like with any cybersecurity topic, layered security is the way to implement physical security. The layered model would mean setting different controls for different areas of the facility, such as the outer perimeter, facility access, and endpoint security. Security standards recommend implementing tiered security levels for all IT assets, while industrial standards require multi-layered security for industrial facilities [22], [24]. The example proposed in Table 3 visualizes the layered physical security model that should be utilized.

Table 3: An example of a Layered Physical Security Model

Security Layer	**Controls**	**Examples**
Outer Perimeter	Gates, Fencing, CCTV, security guards	Industrial plant security fences
Facility Access	Smart cards, biometrics, and visitor logs	Data center access control
Server/Equipment Security	Locked server racks, tamper-proof cases	Industrial control cabinets
Endpoint Security	USB restrictions, laptop locks	Workstations and portable devices

While the physical security efforts bring the organization closer to a safer and more secure environment, we still need to ensure that employees recognize and report physical security threats. This would mean conducting drills on unauthorized entry scenarios, training staff to identify social engineering and tailgating threats, and establishing incident reporting hotlines for suspicious activities. Training employees on physical security policies is required, and awareness programs are recommended to mitigate insider threats and unauthorized access [23], [24]. Regularly auditing physical security ensures that the controls set for physical security remain effective. Auditing could mean using penetration testing for physical security and maintaining logs and security footage for compliance. Organizations must conduct audits of their physical security measures according to security standards. Additionally, governmental regulations frequently mandate these audits as well [18], [35].

Defining and enforcing physical security policies for IT and OT environments requires that the requirements for organizational and physical security measures be documented and clearly

listed. This would mean developing a physical security policy document outlining entry restrictions and maintaining access control logs and visitor records for critical locations. Physical security standards demand documentation [18]. Physical security is a critical IT and OT security component that prevents unauthorized access, protects critical assets, and mitigates environmental risks. Organizations enhance their physical security at facilities through perimeter security, access controls, surveillance, environmental safeguards, and redundancy measures.

5.6.7 Training and Awareness

Training and awareness ensure that personnel across IT and OT environments understand cybersecurity risks, policies, and best practices. Practical training reduces human error, strengthens the security culture inside an organization, and improves incident response readiness. Security awareness is often referred to as ongoing activities to build a security-conscious workforce and reinforce the best practices. In contrast, security training is a formal program designed to educate employees, contractors, and stakeholders on cybersecurity policies, attack vectors, and response procedures.

Training and awareness begin with cybersecurity awareness programs. Establishing continuous education initiatives to reinforce security best practices is the first step. This would mean launching monthly security newsletters inside the organization, using gamification techniques to increase engagement, and displaying security awareness posters in offices and industrial control rooms. Organizations are encouraged to conduct ongoing security awareness initiatives, and security training is recommended as a part of the industrial automation and control system cybersecurity framework [23], [24]. How we handle these trainings also matters; tailoring security training for different roles within the organization helps with everyone's development. This would mean general employees receiving training on password hygiene, phishing, and social engineering, IT personnel getting training with hands-on exercises for security monitoring, SIEM usage, and incident response, and executives and management having training for cyber risk management, compliance requirements, and business continuity. Industrial standards require role-based security training for industrial control system product suppliers, but ISO 27002 advises that security training should be aligned with employees' job responsibilities [24], [35].

Phishing and social engineering training are most often the generic cybersecurity training that organizations are handing out. Tracking employees to recognize and respond to phishing attacks

and social engineering tactics helps a lot and reduces human-based risks. In practice, this could mean simulated phishing attacks to test employee awareness and behavior, training employees to verify caller identities before disclosing information, and establishing reporting mechanisms for suspected phishing emails and embracing them. Training on social engineering threats is recommended to reduce human-based risks but also to support sector-specific security training based on risk exposure [23], [24]. On the other hand, as said, we should also focus on specialized training. Utilizing security training for industrial systems and OT networks helps with industrial security while limiting the risks in industrial environments [22], [24]. This could mean training plant operators to identify industrial control system-specific attack vectors, conducting network segmentation drills, and simulating incident response scenarios in industrial environments. Security incident response training is eventually one of the most essential components for IT and OT personnel, but it also helps organizations' employees to know how to behave during a cyberattack or general security incident. Incident response training is recommended to ensure the organization's preparedness so personnel recognize and escalate cybersecurity threats when needed [23], [33]. In practice, this would mean conducting tabletop exercises simulating cyberattacks, training IT and OT teams based on incident response workflows, and using red team vs blue team exercises for cyber resilience drills.

Secure development and coding practices training is essential in educating software developers and IT staff on secure coding techniques. This would mean training on OWASP secure coding practices for web applications, teaching developers to prevent common vulnerabilities like SQL injections or buffer overflows, and implementing secure software development lifecycle training for DevOps and application teams. Secure development lifecycle training is defined by industrial standards for industrial application software engineers, and secure coding awareness is recommended to prevent software vulnerabilities [24], [47]. While we've already highlighted the importance of training, it is also important to understand that training and policies are written down. Ensuring employees understand the organization's security policies and compliance obligations is as vital as training. This would mean conducting annual security policy reviews and quizzes and providing mandatory compliance training for employees who are handling standard, NIS2, or GDPR-regulated systems and data. Modules can help with this learning management system and self-paced security training. Standards require organizations to train personnel on security policies, but industrial standards also require compliance training for third-party vendors and contractors [18], [23].

It's one thing how we implement this security training and awareness. Standards approach the topic by defining structured training frameworks, but also recommend continuous security education programs [23], [24]. The security awareness training framework outlines the training types, target audiences, and training methods. It can also outline how often the training should be kept within the organization. A model could look like a proposed model in Table 4, which covers different training types, audiences, and methods.

Table 4: Example of a Security Awareness Training Framework

Training Type	**Target Audience**	**Training Method**
General Security Awareness	All Employees	E-learning, newsletters, phishing simulations
Role-Based Training	IT, OT, Management, Sales, etc.	Hands-on workshops, case studies
ICS security training	Plant operators, engineers	SCADA security labs, network segmentation training
Secure Coding Training	Developers, DevOps	OWASP coding challenges, SDL training
Incident Response Drills	IT, OT, Automation, and Security teams	Tabletop exercises, Red Team/Blue team simulations

The organization also needs to establish metrics and evaluations to assess the effectiveness of security training programs. This would involve implementing post-training quizzes to evaluate retention rates, tracking phishing simulation failure rates to gauge organizational risk levels, and utilizing employee feedback surveys to enhance training content. Standards recommend evaluating training effectiveness through security assessments [24].

Finally, documentation and compliance. It is essential to formalize an organization-wide security training policy. A cybersecurity training policy outlining annual requirements would move the organization towards enforcing a transparent training policy. It would also be a step toward maintaining a training register documenting employee participation. Standards require organizations to have formal documentation of cybersecurity training programs, and industrial standards support tracking and enforcing mandatory security training [18], [35]. Security training and awareness play a critical role in mitigating human-based security risks. Establishing cybersecurity awareness initiatives, tailored training, phishing simulations, industry-specific education, and incident response drills will assist organizations in creating a setting with reduced human-related risks.

5.6.8 Threat Modelling and Risk Management

Threat modeling and risk management are foundational aspects of managing and securing IT and OT environments. The process aims to help organizations identify vulnerabilities, assess risks, and implement countermeasures to protect critical infrastructure and operations. With threat modeling, we have a structured approach to identifying and analyzing potential threats, attack vectors, and vulnerabilities. Risk management is the process of identifying, analyzing, and mitigating risks to an acceptable level. With threat modeling and risk management, the organization ensures proactive defense against cyber threats and prioritizes security controls based on risk exposure, letting go of feeling-based decision-making.

Risk management principles start with establishing a systematic approach to managing cybersecurity risks. These principles are essential to the continuance and integration of the risk management process, which is suggested in the standard [32]. We start with integrated risk management, which means including risk management in all parts of all organizational activities, ensuring that the process is thorough. Structured and comprehensive risk management ensures that the risk management process is consistent and comparable with previous results. Dynamic risk management aims to recognize the risks that evolve over time. Risks should always be based on the best available information using threat intelligence and historical data. Organizations must consistently integrate these principles into their risk management to achieve optimal long-term outcomes.

Threat identification and analysis are other tasks that require systematic approaches. The process is identifying threat sources, attack vectors, and potential consequences of threats. A practical example can be using attack trees to map cyber-attack paths. There are multiple threat modeling tools like STRIDE, DREAD, and MITRE ATT&CK. Organizations also often use incident-based analysis and learning from the cybersecurity breaches in the past. Industrial standards require identifying threat sources affecting IT/OT assets and providing methodologies for systematic threat identification [17]. A structured approach to evaluating the risk likelihood and impact is recommended, and standards often define risk identification, analysis, and evaluation as key steps in risk management [32]. Risk identification is recognizing risks and vulnerabilities in an environment; risk analysis evaluates the consequences, likelihood, and security gaps; and risk evaluation determines whether the risk is acceptable or requires treatment. Industrial standards provide good guidelines for evaluating risks in Industrial information systems and are advised for use in industrial settings [17].

Cybersecurity threat modeling techniques differ a bit from traditional business risks; therefore, there should be structured methodologies for modeling security threats. This would mean utilizing the STRIDE model, which is known as the Microsoft model or DREAD score that works by assigning scores for damage, reproducibility, exploitability, affected users, and discoverability, or MITRE ATT&CK that maps real-world adversary behaviors and tactics, techniques, and procedures. Incident response standards recommend structured threat modeling techniques, but industrial standards also require evaluating intrusion methods and attack vectors [17], [34].

Risk treatments are essential for risk management, reducing risk exposure, and allowing calculated risks. Treatments basically apply security controls to reduce risk exposure to threats. Risk treatments are generally slotted into four different categories: avoiding the risk, reducing the risk, transferring the risk, and accepting the risk. In practice, this means eliminating exposure to the threat, implementing security controls, using insurance or outsourcing, and preparing for controlled impact. Risk treatment options and implementation plans are essential for proper risk management procedures, and documentation of risk treatment measures is essential for acknowledging the risks taken [17], [32]. Not mitigating all risks is acceptable, but all risks should be acknowledged to the best of knowledge and documented.

Having security controls based on risk is also recommended, and the implementation of that would obviously mean working with risk management processes. Practical examples of mitigating risks based on the risk classification can be segmenting networks based on risk levels, applying zero trust principles to access management, using security information and event management systems, and intrusion detection or prevention systems for real-time monitoring. Mitigating risks based on the classification requires the classification. That is why there should be predefined security level targets, and putting items in that group would mean specific practical mitigation of the risk. Industrial standard requirements define security target levels as one, while generally, for cybersecurity, risk-driven security implementations are highly supported [18], [22].

Risk management should also include risk detection and monitoring platforms. Implementing real-time monitoring and periodic review systems can help organizations stay on track with the current risks and identify new risks as they might arise from evolving threat landscapes. Reviewing risks should be done in a periodic manner, as a lot can be mitigated within the daily operations of the business, and a lot of risk evaluations can gain new knowledge, which might

raise or lower their classification. For continuous risk detection, security information and event management systems and security orchestration, automation, and response systems can help with that. Risk management requires continuous risk monitoring and review to be effective, but industrial standards also require ongoing risk assessment cycles [17], [32]. While we are conducting reviews of risk management, it is also critical to ensure compliance with legal, regulatory, and industry standards. Continuous monitoring would require some risk documentation, but it is also essential for compliance audits and alignment with NIS2. Reporting cyber risks to the organization's executive leadership would also be crucial. If there are risk management requirements for standards, they are often listed out. Still, security standards outline a requirement for formal risk management documentation with compliance obligations for cyber risk reporting in an industrial setting [18], [35].

Implementing threat modeling and risk management doesn’t have to be too complicated. The process can be broken down into five steps: identify threats, analyze Vulnerabilities, assess likelihood and impact, develop risk treatment, and monitor risk changes. Then, that process has to continue with the day-to-day operations. The applicable process for organizations could resemble the one proposed in Table 5.

Table 5: Risk management process

Step	**Action**
1. Identify threats	Define attack vectors and potential risks
2. Analyze vulnerabilities	Use security scans and penetration testing
3. Assess likelihood and impact	Evaluate consequences and risk levels
4. Develop risk treatment	Apply security controls and mitigations
5. Monitor risk changes	Implement continuous risk assessment

Threat modeling and risk management are critical for the security of IT and OT environments. It builds the knowledge of our environment and ensures that all the risks being taken are acknowledged to the best of our ability. When environments become complex, keeping up with all the risks and smaller things is harder. Risks can be minor or significant, but rather than leaving them undocumented, it is good to notice them. By implementing structured methodologies, risk-based security controls, continuous monitoring, and regulatory compliance, organizations can bring risk management closer to reality and reveal hidden risks while aligning with standards.

6 Discussion, Analysis, and Future Works

The six-domain framework (Network, Hardware, Redundancy, Governance and Compliance, Security) was designed with practical adoption in mind. Its modular structure mirrors real operational divisions, acknowledging that each domain has distinct technologies and risk profiles, regardless of working together in IT. This alignment with how industrial operations are actually organized makes the model intuitively accessible to practitioners. In other words, the framework's structure allows organizations to map controls onto existing functions, facilitating implementation across IT and OT teams. Notably, the framework encourages organizations to align internal controls with well-known external benchmarks like the standards, while adapting to their specific technological landscape.

6.1 Practicality and Real-World Applicability

A key advantage for real-world use is the framework's flexibility. Because it breaks cybersecurity into focused domains, organizations can adopt it incrementally. Rather than undertaking a monolithic overhaul, they may begin implementing controls in areas where they already have expertise or where the risk is most urgent. This pragmatic approach allows even less mature organizations to make progress. For example, the model supports starting with whichever domain an organization is strongest in or which mitigates the most critical risk first. This risk-based priorization means that the framework can accommodate the company's current capabilities and grow with them. At the same time, the domain-based approach makes it clear that cybersecurity is a shared responsibility: successful adoption requires collaboration among IT, OT, and management stakeholders. In fact, industry reports emphasize that securing OT is merely a technical challenge but an organizational one requiring cooperation across IT, engineering, and executive leadership. Thus, an organization's culture and cross-disciplinary coordination play a major role in adoption feasibility. Overall, by providing structure yet remaining adaptable, the six-domain framework is positioned to be practical for a range of industrial organizations, from those just beginning IT/OT integration to more advanced industrial organizations.

International standards like ISO 27001 and IEC 62443 series serve as foundational pillars for cybersecurity governance in IT and OT systems, but they should also be applied in converged IT/OT systems. They offer a structured framework of controls and processes that organizations can follow to manage risk systematically. For example, ISO 27001 defines requirements for

establishing an enterprise-wide information security management system. At the same time, IEC 62443 provides detailed guidance for securing industrial automation and control systems down to the component level. Such standards and frameworks bring several benefits. It helps ensure comprehensive coverage of security domains (from asset management and access control to incident response), and it aligns cybersecurity efforts with regulatory and industry expectations. Adopting ISO 27001 and IEC 62443 can also demonstrate due diligence, which is increasingly important as new regulations come into force. For instance, the EU's recent NIS2 directive explicitly mandates board-level accountability for cyber risks in critical infrastructure sectors. Standards compliance provides a measurable way for organizations to meet such obligations and show stakeholders that recognized best practices are in place. Leveraging ISO 27001, IEC 62443, and related frameworks establishes a common language and baseline for governance, supporting consistency and continuous improvement in cybersecurity management.

6.2 Value and Limitations of Standards-Based Governance

Despite their value, standards are not a silver bullet for organizations. Organizations often encounter limitations when applying them in practice. One challenge is that multiple standards may need to be used together, and their scopes can differ, leading to integration difficulties. The alignment between ISO 27001, which focuses on IT, and IEC 62443, which focuses on OT control system security, often remains fragmented in practice. Each standard addresses cybersecurity from a slightly different angle; in this case, it is enterprise IT versus industrial OT control systems, and harmonizing them for a converged environment is non-trivial. In fact, implementing both frameworks side by side often results in overlapping and even conflicting terminologies and control requirements, causing inconsistent interpretations and gaps. For instance, an IT security team may adhere to the controls outlined in ISO 27001. On the other hand, an engineering team follows IEC 62443. Without effective coordination, this could result in specific interfaces, such as the data flow between business IT and plant floor OT, being inadequately addressed. Without a single unified standard, organizations are forced to combine multiple standards and interpret how they fit together, as was done in this thesis framework. This patchwork approach can be resource-intensive and demands significant expertise to implement correctly.

Furthermore, being compliant with a standard does not automatically equate to being secure. If an organization treats compliance as a checkbox exercise, it might meet the letter of ISO 27001

or IEC 62443 but still lack practical security depth. Complexity is another limitation: The IEC 62443 series, for instance, consists of numerous parts covering different roles (operators, component suppliers, service providers) and can be overwhelming for small to medium-sized companies to fully adopt. Similarly, ISO 27001 requires an organizational commitment to maintain an information security management system over time, which can be challenging if cybersecurity is not yet integrated into the company's governance culture.

The IEC 62443 family is a comprehensive standard for industrial control system security, but several critiques emerge in practice. It's a multi-part structure (spanning policies for asset owners, integrators, component suppliers, etc.) that introduces complexity that can overwhelm organizations, especially small and medium enterprises [48]. Implementing the full suite of IEC 62443 often demands significant expertise and resources, and in converged IT/OT environments, it may need to be combined with IT-focused standards (like ISO 27001), which can lead to overlapping or even conflicting requirements from different standards. A notable analysis by Dragos found that the IEC 62443 standards exhibit a "prevention bias"; about 75% of controls focus on preventative measures, with only ~25% addressing detection, response, and recovery [49]. This imbalance means that organizations relying solely on IEC 62443 might underdevelop their incident detection and response capabilities, a gap that has been reflected in real-world ICS incidents [49]. In short, IEC 62443 provides a solid base of controls, but its breadth and prevention-heavy focus are seen as limitations when not complemented by equally robust monitoring and response measures.

ISO 27001 is a widely adopted information security management system standard, but in industrial contexts, it has been criticized for being too generic and IT-centric. Case studies indicate that 27001 can be challenging for industrial organizations without dedicated security staff; the standard's terminology and requirements may be hard for plant engineers to interpret, and maintaining the ISMS is resource-intensive [48]. One study of the oil & gas sector found that 27001's scope is somewhat narrow, not explicitly covering areas like operational safety, physical process security, or control system reliability [48]. ISO 27005, which guides risk assessment, follows ISO 31000 principles and similarly lacks ICS-specific guidance, meaning critical cyber-physical risks (e.g. threats to process safety or equipment uptime) might be underestimated if one uses 27005 "out of the box". It is pointed out that traditional IT security standards need updates to reflect the unique requirements of SCADA/ICS environments [50]. In other words, the risk profiles in industrial systems (where attacks can cause physical damage) demand tailoring and therefore resources; simply applying ISO 27001/27005 controls can leave

blind spots in areas like safety-integrity or real-time response [51]. Indeed, a survey of ICS security management highlighted a “dearth of ICS-specific security metrics” as a barrier, necessitating additional domain-specific risk assessment techniques beyond what ISO standards provide [51]. Overall, ISO 27001/27005 provides a valuable baseline, but it may prove insufficient for granular ICS threat scenarios and OT operational constraints without augmentation.

ISO 31000 is an overarching risk management framework that is not specific to cybersecurity, therefore being more abstract when applied to industrial cybersecurity. Its strength is in providing a high-level process for risk governance, but critics note its limitations in ICS settings. Because it is industry-agnostic, ISO 31000 does not address how to quantify cyber-physical risks or how to prioritize safety vs security, challenges that are central in ICS risk management. Practitioners often must develop custom methodologies on top of ISO 31000 to handle, for example, the cascading effects of an OT system failure or the likelihood of advanced persistent threats targeting control devices. It is observed that even well-established security standards need to be updated to capture the modern and unique requirements of modern SCADA environments [50]. By extension, a general risk framework like ISO 31000 provides a structured process but not specific controls or threat models for ICS, which is expected, meaning its practical effectiveness hinges on how it is supplemented. ISO 31000 can ensure that industrial organizations have a risk process, but on its own, it may be too high-level, lacking guidance on industry scenarios, incident impact on physical processes, and technical mitigation strategies.

The Network and Information Security Directive 2 (NIS2) represents a regulatory push to raise cybersecurity baselines across European critical infrastructure, including industrial sectors. NIS2’s strengths lie in mandates for governance, like board-level accountability and incident reporting, and its alignment with standards like ISO 27001 and IEC 62443 in areas of risk management and continuity. However, early analyses and industry observations point out certain limitations. Because NIS2 is broadly scoped to many sectors, its requirements remain fairly general; organizations are instructed on what to achieve, like risk management, but not how, often deferring to existing standards for implementation. This can lead to the same challenges as discussed above; companies may check the compliance boxes of NIS2 by adopting ISO/IEC controls, yet still lack effective security depth. Another concern is the uneven maturity and resources across organizations. NIS2 expands obligations to medium-sized and more OT-intensive companies, which might struggle with compliance due to limited

cybersecurity capabilities, echoing the SME challenges noted for ISO 27001 [48]. The original NIS directive in 2016 saw patchy implementation across EU member states, and those gaps are partly what NIS2 tries to address, but it remains to be seen how consistently organisations can meet the new, stricter measures in practice. In an industrial context, NIS2's impact may be constrained if organizations treat it as a minimal compliance exercise. Being compliant does not equate to being secure, a point often echoed by experts. Therefore, while NIS2 raises the cybersecurity floor, its effectiveness for ICS protection will depend on how thoroughly companies exceed the baseline, for example, by incorporating ICS-specific safeguards beyond the directive's broad requirements.

Numerous incidents and studies underline that standards-based compliance alone can prove insufficient. For instance, an analysis of ICS cyber incidents over recent years showed that many organizations had invested heavily in preventative controls to meet standards, yet were caught unprepared to detect or respond to attacks [49]. The 2015 Ukrainian power grid attack and the 2017 Triton malware attack are often cited in discussions; in both cases, simply adhering to existing security guidelines was not enough to prevent or quickly mitigate the attack. Investigations suggest those environments lacked certain ICS-specific monitoring and incident response capabilities that were not explicitly required by regulation at the time. This reinforces a critical view, frameworks like ISO 27001 or IEC 62443 set important minimums, but organizations that stopped at mere compliance suffered when novel threats emerged [49]. Experts, therefore, argue that a culture of continuous risk assessment and threat intelligence must complement standards [50]. The need to integrate lessons from real attacks, like attackers' TTPs from events like Stuxnet or NotPetya, often outpaces the updates to formal standards. Case studies show that without adaptation and proactive measures, even a fully "compliant" ICS may remain vulnerable, a sobering reminder of the gap between paperwork and actual security.

These limitations underscore that while standards-based governance provides a solid foundation, it must be complemented by precise tailoring and integration efforts. Organizations need to interpret how generic controls apply to their specific mixed IT/OT environment and ensure the standards are implemented in a unified, operationally workable manner. The six-domain framework proposed in this thesis is one attempt to create such a unifying structure, mapping controls from various standards into a coherent model. As there is no universal harmonizing standard for IT/OT security, leveraging multiple global standards within a

common framework is the closest practical approach available, where this won't be the first nor the last attempt across organizations.

6.3 Fragmentation of Reference Architectures

Just as there are many standards, the industrial realm also hosts numerous reference architectures aimed at IT/OT systems – yet no single model has achieved universal adoption. The Purdue Enterprise Reference Architecture (PERA), introduced in the 1990s, became a de facto guideline for segmenting industrial networks into levels from enterprise IT down to control devices. In recent years, newer models have emerged to address the connected, data-driven requirements of Industry 4.0. Notably, the Reference Architecture Model Industrie 4.0 (RAMI 4.0) and the Industrial Internet Reference Architecture (IIRA) were developed to provide layered frameworks that incorporate modern concepts, such as IIoT devices, cloud services, and lifecycle integration, beyond Purdue's scope. Each architectures offer functional perspectives – for example, RAMI 4.0 organizes concerns across a three-dimensional grid (hierarchy levels, life cycle/value stream, and layers) to ensure interoperability. IIRA defines functional domains and use-case viewpoints to guide industrial IoT system design. However, the coexistence of multiple reference models has led to a fragmented landscape. Different companies and sectors pick different models (or pieces of them), resulting in a lack of uniformity in how IT/OT convergence is architected and secured. Modern surveys of Industry 4.0 initiatives point out a wide range of platforms, architectures, and frameworks in use, reflecting a lack of standardization across the industry [11]. Hundreds of industrial IoT platforms and frameworks exist, and new ones continue to be introduced [11]. This vast array of options underscores the absence of a universally accepted common framework for converged architectures.

The fragmentation in reference architectures is not merely an academic concern – it has real, practical consequences. When each vendor or organization follows a different architecture model (or a customized hybrid), interoperability suffers, and security becomes inconsistent. Industrial systems end up with incompatibilities and inconsistent implementation of security measures across different layers or sites. For example, one plant might strictly adhere to the Purdue model's network zones, while another (even within the same company) experiments with the flatter network using IIoT gateways per IIRA guidelines. If those two plants are connected or share data, the lack of common architecture can create blind spots and integration headaches. It was emphasized in the review 2019 that solving such interoperability challenges

requires addressing them not just locally but on a global scale, where the World Economic Forum has called for internationally harmonized standards to enable true Industry 4.0 integration [11]. In the current state, organizations face confusion in deciding which reference architecture to follow, sometimes leading to “framework fatigue”. Many still lean on Purdue (PERA) because of the lack of a better universal option, even though Purdue was not originally designed for modern cloud-connected OT. Meanwhile, applying newer models like RAMI 4.0 in practice can be daunting without clear migration paths. The conclusion is that no single architecture has emerged as the comprehensive solution for IT/OT convergence, while it has been going on. This thesis's six-domain architecture is an attempt to bridge this gap by focusing on security control domains rather than prescribing a detailed architecture. It draws from multiple architectures and standards to create a security-centric overlay that could, in theory, sit on top of any of these reference models. Still, a broadly accepted harmonized framework remains an open need in the industry. Achieving that will likely require collaboration between standards bodies (ISO, IEC, ISA), industry consortia, and academia to integrate the best of PERA, RAMI, IIRA, and others into a unified model that is adaptive and future-proof. Until then, companies must navigate the patchwork by combining global standards with a harmonizing model as a pragmatic solution.

6.4 Alternative Frameworks

The NIST CSF is frequently highlighted as a more adaptable and practical model for ICS security management. Unlike one-size-fits-all standards, the CSF is a framework organized into five core functions: Identify, Protect, Detect, Respond, and Recover, which are meant to be balanced [49]. This balance is particularly valuable for industrial environments, as it encourages equal attention to operational visibility, incident response, and recovery, not just preventive protection. Many organizations have found the CSF’s risk-based approach easier to tailor to their specific context. In fact, in 2023, 72% of organizations used recognized frameworks like NIST CSF and IEC 62443 to map their control system security programs, underscoring the CSF’s popularity [4]. Its flexibility allows companies to start with a maturity level that suits them and improve over time, which is crucial in an OT setting where one cannot simply apply a rigid control checklist without considering process impact. Another advantage is that NIST CSF provides a common language that can bridge IT and OT teams, for example, both can agree on high-level outcomes (e.g, “detect anomalies in control network traffic”) and then implement controls appropriate to their domains. While the CSF itself is not a prescriptive standard, it integrates well with other standards, as it includes mappings to ISO 27001, IEC

62443, NIST 800-53, etc., so organizations in regulated industries can use it as an overarching governance layer. In essence, NIST CSF's adaptability and clarity have led many to view it as more practical for ICS: it focuses on outcomes and continuous improvement, which helps organizations navigate the rapidly evolving landscape better than a static compliance checklist [49]. That said, CSF is voluntary; its effectiveness depends on management's commitment to actually implement the identified improvements.

One prominent modern tool addressing some gaps of traditional standards is the MITRE ATT&CK for ICS knowledge base. This framework, introduced around 2020, provides a detailed matrix of adversary tactics and techniques specifically observed in industrial control system environments [52]. The value of ATT&CK for ICS is that it catalogs how real-world attackers operate, from initial access methods in OT networks, to techniques for compromising PLCs or HMIs, to steps for causing physical process disruptions. Mapping known threat behaviors or TTPs gives asset owners and defenders a practical lens to evaluate their security. For example, an organization can cross-reference which ATT&CK techniques they have detection or mitigation for, and which are blind spots. This approach is highly adaptable: it is not a compliance document at all, but rather a living library that can inform many security activities, like threat modelling, monitoring use-case development, incident response playbooks, etc. In industrial settings, where new attack vectors are continually discovered, like firmware manipulation of safety controllers or novel OT malware, ATT&CK for ICS helps ensure defence strategies stay current with the latest adversary tradecraft [52]. In the context of our discussion, ATT&CK is often seen as complementary to the traditional standards, whereas ISO/IEC or NIST standards tell you what controls to have, ATT&CK maps out what you need to be able to detect or respond to. This makes it a practical tool for operators to validate that their IEC 62443 or NIS2-based controls are actually effective against known threats. ATT&CK for ICS is relatively new and not a silver bullet, as it doesn't prescribe mitigations or account for every possible attack [52]. Early adoption in industry has shown it to be a powerful, adaptable model for improving security monitoring and incident preparedness in ICS environments.

In addition to NIST CSF and ATT&CK, there are further models and frameworks that experts propose for more effective industrial cybersecurity. The NIST SP 800-82 guide, for instance, provides detailed security recommendations for ICS and is often used alongside the CSF or ISO standards to get more operational detail [53]. Sector-specific regulations like NERC CIP offer mandatory baselines, though they, too, have faced criticism for being compliance-driven [54].

Some organizations are adopting zero-trust architecture principles in OT or sexperimenting with consequence-driven cyber-informed engineering, an approach that starts by identifying worst-case physical consequences and working backwards to mitigate them. These newer methodologies share a common theme: they strive to be more dynamic and scenario-driven than traditional checklists. They acknowledge that industrial cybersecurity is not just about documentation or periodic audits, but about continuously adapting to threats that can have safety and reliability impacts.

The thesis framework, which unifies multiple standards into a tailored model, can be enriched by considering these perspectives. The discussed standards each contribute valuable elements but also have clear limitations in an ICS context, as evidenced by both academic analyses and industry case studies. A combined approach can mitigate some weaknesses, for example, using IEC 62443 for OT specific controls and ISO 27001 for governance. However, as our discussion shows, no single standard is sufficient on its own for the complex cybersecurity challenges of industrial environments. Alternative frameworks like NIST CSF and MITRE ATT&CK for ICS offer more adaptable and focused lenses, whether it be a broader balance of security functions or a granular mapping of adversary behaviors, that can greatly enhance an industrial cybersecurity program. These insights provide a basis to compare and contrast the thesis's proposed framework with the wider landscape, highlighting how this approach aligns with the best practices, where it addresses known shortcomings of existing standards, and how it could integrate the strengths of other models to achieve a more resilient ICS security posture.

6.5 Visibility and Awareness Challenges in IT/OT Environments

A recurring challenge in converged environments is maintaining adequate visibility over assets and activities across both IT and OT. Historically, OT systems were isolated and managed by engineering teams, often without the sophisticated monitoring tools common in IT. As integration has increased, many organizations struggle to obtain a unified real-time view of all their critical components. Studies reveal an alarming lack of visibility into OT networks. One survey found that only about 5% of organizations claim to have full visibility into their OT activities, a percentage that had even decreased from prior years [9]. Another industry report noted that over half of organizations have limited situational awareness of their industrial control system environments [4]. This means that the majority of companies cannot confidently inventory all of their OT devices or detect malicious activity promptly in those environments. The consequence of limited visibility is that threats or failures in OT may go unnoticed until

they escalate into major incidents. For example, malware could infiltrate a production network and remain undetected for a long period, as intrusions can embed without detection when ICS monitoring is weak [55]. The complexity and proprietary nature of many OT devices, along with insufficient deployment of monitoring tools, contribute to this gap.

Compounding the technical visibility issue is often a lack of management awareness regarding OT assets and risks. In many enterprises, upper management and even IT security leadership may not fully understand the critical components on the plant floor or the network dependencies that could lead to an outage. OT systems sometimes fall outside of the traditional IT risk management and thus escape executive attention until a failure occurs. This is starting to change as high-profile incidents make headlines (For instance, when production is halted by a cyber attack, executives quickly take notice). However, surveys still indicate that bridging the communication gap between plant operations and business leadership is an ongoing struggle[4]. One market study stressed that addressing OT security requires collaboration across departments, implying that leadership must be involved and informed. Without management visibility into what the critical OT devices are – and what their failure or compromise would mean in business terms – organizations cannot effectively prioritize investments or emergency responses. A key lesson identified in this thesis is the importance of a robust asset management function to tackle these issues. Maintaining an accurate, continuously updated inventory of all IT and OT assets is essential for visibility and is emphasized by standards like ISO 27001 and IEC 62443-2-1. Such an asset repository, if leveraged well, gives both engineers and managers a common reference for what needs to be protected and monitored. It enables mapping of criticality so that management knows which systems are mission-critical and helps in tracking security requirements or incidents by asset. In practice, instituting centralized asset management and network monitoring in OT environments can be difficult – it may require retrofitting legacy equipment with sensors or deploying new network taps in sensitive production networks. Yet, improving OT visibility is paramount; without it, even the best framework or policy will have blind spots. Therefore, organizations should invest in tools and processes such as OT network monitoring solutions, centralized asset databases, and cross-functional risk reviews that increase transparency in an organization. Leadership should be regularly briefed on the state of OT security, including which critical components exist and how they are protected. Enhancing visibility and awareness in this way complements the six-domain framework proposed, as it provides the necessary factual basis for knowing what's out there to apply the appropriate controls in each domain effectively.

6.6 Criticality and Acceptable Risk Levels from a Business Perspective

One fundamental aspect of risk management underscored by this work is the need to clearly define the criticality of assets and processes and the acceptable level of risk for each. Industrial organizations must recognize that not all assets are equally important – a cyber incident on a non-critical support system might be tolerable, but an incident on a safety-critical control system or a production-critical network could be catastrophic. Therefore, a structured approach to classifying systems by their criticality to operations is crucial. Frameworks like IEC 62443-3-2 support this by recommending that one segment the environments into zones based on the risk and criticality of assets. Similarly, the classic Purdue model and its derivatives implicitly rank systems by criticality to production. By identifying which systems, data, or processes are "crown jewels" (e.g, those that could cause major safety incidents, environmental harm, or multi-million-dollar losses if compromised), organizations can prioritize defensive resources and tailor controls to the needed level of rigor.

Defining acceptable risk levels goes hand-in-hand with determining criticality. IT involves business-driven decisions on how much risk (in terms of potential impact or downtime) can be tolerated for each asset or domain. This essentially sets a risk appetite for different parts of the operation. For example, a company might decide that for critical OT systems controlling production, it will accept almost no cyber risk, driving requirements for redundant systems, strict network isolation, and continuous monitoring. On the other hand, for less critical systems, a moderate risk might be acceptable if mitigating it would be too costly or impractical. The important point is that these decisions should be made explicitly and in advance, not ad hoc after an incident. Aligning security measures with the business impact of an asset ensures that protection efforts are commensurate with potential losses. Neglecting to do so can lead to misallocating resources, where trivial assets get over-protected while vital ones remain vulnerable. A vivid illustration of why this matters is the potential cost of incidents: a recent industry survey found that the average cost of a security incident affecting ICS/OT systems is roughly 3 million dollars, with some events exceeding 100 million dollars in losses [56]. These figures include the technical recovery costs, production downtime, safety liabilities, and reputational damage. Such statistics underscore that for truly critical operations, even a small likelihood of compromise might pose an unacceptable risk to the business.

Defining criticality and acceptable risk should be a collaborative exercise between operational managers, engineers, and business leaders. Techniques like conducting business impact

analyses for industrial processes and risk assessments aligned with ISO 31000 or ISO 27005 methodologies can help quantify impacts regarding financial loss or safety consequences. While standards such as ISO 31000 and IEC 62443-3-2 offer structured mechanisms for identifying risk and assigning criticality, their practical application within industrial environments, particularly in converged IT/OT contexts, remains uneven. Defining what is "critical" often depends not just on technical attributes, but also on business impact, interdependencies, and recovery complexity. Recent academic and industry literature emphasizes that many organizations struggle to assess these factors holistically. For example, one study points out that most industrial enterprises do not adequately account for cross-domain dependencies or socio-technical factors in their risk evaluations [6]. This leads to an underestimation of systemic vulnerabilities, such as shared infrastructure or identity services that may act as single points of failure across multiple layers.

Further complicating the issue, it is observed that industrial organizations often fail to adopt structured reference architectures like RAMI 4.0 or IIRA that could help visualize layered risk [57]. A recent study reveals that decision-makers frequently delegate risk evaluations to technical teams, resulting in fragmented ownership and limited alignment between technical risk assessment and business-level understanding [57]. Moreover, it is also argued that risk management practices in many industrial contexts remain primarily compliance-driven, producing risk registers that satisfy auditors but are disconnected from business continuity strategies or real-time operational visibility [58]. This disconnect is framed as a cultural challenge: cybersecurity and risk remain siloed technical disciplines, rarely integrated into broader decision-making processes [58].

The framework developed in this thesis responds to these shortcomings by proposing a structured, domain-based breakdown that facilitates traceability and priorization. While it does not dictate a universal model for critical analysis, it provides a foundation that organizations can adapt to their own risk appetites. Standards like IEC 62443-3-2 support this by encouraging the creation of risk-based zones and conduits that reflect both technical and operational importance. By applying such segmentation, organizations can begin to better identify their "crown jewels" and align their security controls accordingly. Importantly, this process should not be static. As operational priorities evolve and new technologies are introduced, the classification of systems and corresponding risk tolerance levels must be continuously reassessed. Without such adaptive mechanisms and business-level engagement, even well-structured frameworks risk becoming outdated or ineffective in practice.

Many organizations adopt a tiered risk level classification for their assets. This thesis's framework inherently supports this by encouraging an understanding of how each domain contributes to operations. For instance, in the Redundancy domain, one lesson is to decide which systems absolutely require redundancy because they cannot fail without a significant impact, versus those that can tolerate downtime. Once critical assets are identified, the acceptable risk level informs what controls are needed. If zero compromise is the goal for a safety system, one might implement the highest security level from the IEC 62443 standard, alongside fail-safes and continuous diagnostics. Basic measures and periodic review might suffice for a less critical asset if that risk is deemed acceptable. Documenting these decisions is essential, and it provides a rationale for why certain controls are in place or why certain risks are being accepted by management. It also ties cybersecurity strategy back to business objectives, ensuring that security is technically sound and aligned with operational priorities. The outcome of this approach is a more risk-aware culture, where everyone from engineers to executives understands which systems matter most and how much risk can be tolerated, enabling more informed and faster decision-making during both planning and incident response. In summary, defining criticality and risk appetite is a foundational step that strengthens the effectiveness of any structured security framework by focusing efforts where they matter most.

6.7 Evolving Threat Landscapes

The threat landscape for industrial cybersecurity continues to evolve rapidly, reinforcing the relevance of a robust, structured approach like the six-domain framework. As IT and OT networks become more interconnected, attackers have increasingly turned their attention to industrial targets, knowing that disruption of physical processes can have a high payoff or strategic impact. Organizations are not only facing a growing attack surface but also interconnected system dependencies that are hard to model using traditional cybersecurity frameworks [59]. Complex systems such as ICS are designed as collections of highly connected units involving multiple stakeholders, and identifying risks across these domains requires a system-wide approach beyond standard methods. Cyber-physical interdependencies mean that compromising IT infrastructure may lead to safety issues, downtime, or even physical damage to equipment, making the need for dual-focus risk models increasingly urgent [59].

Recent trends and incidents bear this out. According to the SANS 2024 survey, the number of reported intrusions into industrial control systems has risen significantly, with nearly one-third

of organizations experiencing six or more intrusions in the past year and almost two-thirds experiencing at least three incidents [4]. Notably, the most common attack vector has become the IT-to-OT lateral movement, where adversaries breach traditional IT systems and then pivot into OT environments. This trend highlights the dangers of inadequate network segmentation between IT and OT – a gap that the proposed framework's network controls seek to address. It also exemplifies why converged governance is needed; a breach in IT can no longer be viewed in isolation if it can cascade into plant operations.

Beyond statistics, specific cyber incidents in recent years have underscored the stakes in industrial cybersecurity. In 2021, for example, a ransomware attack on Colonial Pipeline forced a shutdown of fuel distribution on the U.S. East Coast, grabbing worldwide attention [60]. Although the ransomware primarily affected business IT systems, the company pre-emptively halted OT operations to contain the threat, demonstrating how even IT-side attacks on industrial infrastructure can have broad economic and societal consequences [60]. It has spurred greater investment in securing critical energy pipelines and closer government-industry collaboration in the U.S. and elsewhere. Another concerning development was the 2017 Triton/Trisis malware attack on the Saudi Petrochemical plant's safety instrumented systems [61]. That attack, which attempted to disable safety controls, illustrated that threat actors are willing to target human safety by compromising OT [61]. This scenario elevates cybersecurity to a life-and-death matter. While Triton was a wake-up call, even more advanced toolsets have emerged since. In 2022, researchers discovered a modular ICS malware toolkit dubbed PIPEDREAM, also known as INCONTROLLER, before it could be deployed in the wild. PIPEDREAM is noteworthy because it is a cross-industry framework, "a Swiss army knife" of ICS attack capabilities, that can target a wide range of industrial controllers and protocols out of the box. IT was built by a highly skilled adversary group with the apparent intention to attack industrial infrastructure in the United States and Europe [62]. According to analysts, this malware could potentially impact tens of thousands of devices across different manufacturers, making it one of the most universal and dangerous ICS cyber weapons seen to date [62]. Fortunately, it was discovered through proactive threat hunting before causing damage, but its existence confirms that the threat landscape is escalating with more sophisticated, ICS-specific malware. The framework remains relevant in this context, as layered defences are emphasized that would collectively make it harder for such malware to succeed.

Another ongoing trend is the rise of ransomware and other financially motivated attacks against manufacturing and critical infrastructure. Initially, many ransomware groups avoided OT for

fear of triggering dangerous process disruptions, but that stance has eroded. By 2022, 70% of the ransomware attacks tracked by one industrial cybersecurity firm targeted manufacturing firms [62]. We have seen ransomware incidents halt automobile factories, food processing plants, and even cause outages in utility companies. In these cases, even if the OT network isn't directly encrypted by the malware, the business often must stop production out of caution or due to loss of a supporting IT system, like with Colonial Pipeline. The financial impact of such downtime can be immense. For instance, the 2019 ransomware attack on Norsk Hydro, a global aluminum producer, cost the company an estimated 50-70 million dollars due to lost output and recovery expenses [63]. Attacks aren't limited to ransomware either; nation-state actors have continued to probe critical infrastructure. During the Russia-Ukraine conflict, cyberattacks on the Ukrainian power grid in 2015, 2016, and 2022 demonstrated that state-sponsored groups are capable of causing blackouts via cyber means [64]. All these examples drive home that the threat to the industrial system is very real and continuously growing. They also validate many of the control objectives in the six-domain framework; network isolation can contain IT intrusions, redundancy and backups can help recover, strict software allowlisting and monitoring can catch novel malware behavior, and so on. In essence, the evolving threat landscape underscores why a comprehensive and up-to-date security framework is needed. Attackers will continue to find new ways to infiltrate or disrupt converged IT/OT systems; therefore, organizations must continuously strengthen their defenses across all domains. The framework provides a structured way to ensure no major area is neglected as threats advance. It also highlights the need for continuous vigilance and adaptation; what is effective security today may not be sufficient tomorrow, so organizations should regularly reassess their risks and controls in light of the latest threat intelligence. The recent incidents cited serve as lessons, reminding practitioners that cybersecurity in industrial environments is a moving target and reinforcing the relevance of efforts like this thesis to create structured, resilient approaches.

6.8 Key Findings/Outcomes

This thesis set out to develop a standards-based cybersecurity framework tailored for converged IT/OT industrial environments. By analyzing a range of international cybersecurity and risk management standards, architectural reference models, and recent academic research, the thesis produced a modular framework structure around six interrelated control domains: Network, Hardware, Software, Redundancy, Governance and Compliance, and Security. These domains allow for a structured and traceable approach to cybersecurity management that is responsive to the needs of modern industrial operations.

One key outcome of the work is the demonstration that existing standards, notably the IEC 62443 series, ISO 27001, and the NIS2 Directive, can be effectively interpreted and integrated to support a unified governance and control approach in industrial contexts. Although originally developed for different scopes and audiences, these standards contain overlapping and complementary guidance that, when organized systematically, offer strong support for managing cybersecurity across converged systems. The thesis illustrates how the IEC 62443 series supports technical and role-based segmentation, ISO 27001 structures strategic governance, and the NIS2 Directive reinforces regulatory alignment.

Despite the availability of international standards, the practical execution of cybersecurity governance in OT-heavy environments remains inconsistent [58]. It has been pointed out that ICS cybersecurity programs often fail not due to technical limitations, but because of poorly aligned governance structures, especially when leadership is fragmented or driven primarily by IT or legal departments with limited OT insights [58]. Traditional Governance, Risk, and Compliance frameworks frequently lack the domain-specific industrial control environments, leaving asset owners with minimal guidance for implementing role-specific controls or responding to incident scenarios unique to OT [58].

The six-domain framework proposed in this work offers a logical structure for dividing complex IT/OT security responsibilities into manageable areas. While not intended as a comprehensive or all-encompassing model covering every control aspect from all referenced standards, it facilitates clarity, cross-disciplinary communication, and modular implementation. The framework focuses on the most practically relevant domains identified through the analysis of standards, prioritizing areas of convergence and operational applicability, while acknowledging that some niche or sector-specific controls fall outside the scope of this thesis, such as cryptographic key lifecycle management or specific data privacy extensions. Its structure draws on principles embedded in industrial security standards, such as the zone-conduit model from IEC 62443-3-2, and mirrors the layered defense strategies commonly promoted in OT security design.

This framework is also informed by industrial reference architectures such as PERA, RAMI 4.0, and IIRA. These models were reviewed to ensure architectural alignment, and their layered views on lifecycle management, functional segmentation, and connectivity informed the layout of the proposed domains. Although the reference architectures themselves are not directly integrated into the framework, they serve as valuable conceptual support and highlight the

importance of aligning cybersecurity strategy with system lifecycle and asset taxonomy. The thesis, at the same time, discusses concerns identified in both academic and industry literature, such as the fragmentation of guidance in IT/OT security and the challenges organizations face in adapting generic security standards to the specific constraints of industry operations. While this work does not provide empirical validation, the framework it proposes addresses many of these recurring concerns by offering a structured way to interpret and implement controls based on industrial use cases.

Moreover, the work reflects on visibility challenges in industrial environments. Studies and incident analyses have repeatedly shown that a lack of asset visibility and poor documentation of cross-domain dependencies have led to misconfigured access points, unnoticed vulnerabilities, and recovery delays. For example, shared database infrastructure such as SQL clusters or centralized authentication services often go undocumented in OT contexts, despite serving as foundational components. While this thesis does not include empirical field data, it addresses these concerns by incorporating practices such as asset inventory development, risk-based segmentation, and cross-domain traceability. These are derived from established practices outlined in IEC 62443 and ISO 27005 and aim to raise management awareness and operational clarity around shared infrastructure.

A further consideration addressed in the thesis is the difficulty organizations face in defining criticality and determining acceptable risk levels. In many organizations, risk classification is either too generic to guide operational decisions or not updated frequently enough to reflect evolving dependencies and system roles. This is especially problematic for IT components that support multiple OT functions, where failure may not be immediately visible but can cause cascading disruption, such as remote access platforms, historians, or edge processing nodes. The standards reviewed in this thesis, particularly ISO 31000's risk appetite framework and IEC 62443-3-2's Security Level Targeting, emphasize structured risk evaluation methodologies. By adopting these approaches, the proposed framework encourages organizations to not only formalize criticality assessments but also to periodically re-evaluate risk in light of operational changes. This is particularly relevant for organizations with fragmented governance processes or distributed asset ownership.

Lastly, the framework reflects the need for adaptability in the face of evolving cyber threats. Industry analysis, such as the SANS 2024 State of ICS/OT Cybersecurity report, identifies a shift in attack vectors toward IT-originated intrusion, exploitation of remote access, and supply

chain attacks. The modular nature of the framework allows organizations to adapt controls as the threat landscape changes, supporting continuous improvement in line with established risk principles.

In summary, the findings of the thesis indicate that a domain-based, standards-aligned framework can serve as a practical foundation for improving cybersecurity posture in industrial IT/OT environments. While not prescriptive, the structure encourages strategic alignment, layered defense, and operational clarity. The findings also align with broader research, which emphasizes that IT/OT convergence introduces fundamentally different attacker motivations and system characteristics compared to traditional IT systems [6]. While IT security emphasizes confidentiality and integrity, OT security prioritizes availability and safety, requiring organizations to asses both cyber and physical impacts when designing protections [57]. Future research may explore the empirical application of the model, including its use in audits, maturity assessments, or as part of continuous evaluation platforms.

6.9 Limitations of This Research and Future Work

While the six-domain framework and the accompanying analysis provide a structured approach to IT/OT cybersecurity, it is important to acknowledge the limitations of the current work. First, this framework, at this stage, is largely conceptual and has not been implemented or tested in a live industrial environment as part of the thesis. This means that there is limited evidence of its effectiveness or the practical challenges that might arise during real deployment. For instance, the framework assumes organizations have the resources and willingness to assign responsibilities and perform continuous management in each domain. In practice, smaller organizations or those with lower security maturity might struggle to dedicate efforts to all six domains simultaneously. This touches on the second limitation: the model's adoption requires a certain baseline of organizational capability, which may not exist in every case. If those fundamentals are not in place, the framework could be overwhelming or applied superficially. Another clear limitation is the potential overlap between domains. While attempting to delineate them clearly, some security controls, in reality, span multiple domains. This could lead to confusion unless governance is carefully coordinated. Additionally, the framework doesn't explicitly address certain specialized areas like security and safety engineering, assuming those are handled separately. In highly integrated cyber-physical security programs, one might need to extend or interface the framework with safety risk management processes.

It was also observed that aligning the six-domain model with every existing standard and architecture can be complex. The framework draws from many sources, but different organizations might prefer one standard over another, and the framework might need some adaptation in those contexts to fit the organization's language. This could be seen as a limitation in universal applicability, as some tailoring is required per context. Furthermore, the framework aims to harmonize IT and OT security practices; it might face resistance to change in an organization where IT and OT teams are accustomed to working independently. Therefore, cultural resistance can limit the framework's immediate impact, a factor beyond the framework's design. In summary, the main limitations are the lack of real-world validation, the need for a certain level of organizational maturity, potential domain overlaps, and customization for specific corporate environments.

Recognizing these limitations points to future work directions to enhance and build upon the thesis results. Two key areas for improvement are the development of a lightweight audit and control verification platform and the design of a continuous cybersecurity assessment process. Initially, the thesis aimed to include these two future works; however, they had to be removed due to the extensive workload.

A practical step would be to create a tool or platform to help organizations easily assess and verify the controls in each of the six domains. Conducting a comprehensive IT/OT security audit can be labor-intensive and require significant expertise. Many organizations rely on periodic manual audits or checklists, which are time-consuming and may not be repeatable frequently [65]. A lightweight audit platform could automate portions of this process, tailored to the six-domain framework. For example, the platform could periodically collect data from network, hardware, and software components and then check compliance with the recommended controls of each domain. This would provide an internal control verification mechanism quicker and more continuously than annual audits. Given that even though 70% of organizations perform OT security assessments, only 23% do so continuously due to resource constraints [65].

An automated or semi-automated tool could significantly improve security posture by enabling more frequent checks. The platform should be lightweight in the sense that it does not require huge deployments or expert-only operations. Ideally, it would represent a dashboard of domain-wise compliance, flagging gaps in different domains or control points. By providing this actionable feedback per domain, this tool would help maintain the framework's implementation

over time and offer management a clear view of control effectiveness. Developing and pilot-testing such a platform in a real industrial setting would be invaluable future work to validate the framework's practicality and help organizations self-improve. This would align with industry calls for technology-enabled assessment methods that move beyond purely manual approaches [65].

Alongside tool development, there is a need for a well-defined assessment process that organizations can adopt to evaluate their cybersecurity posture across IT and OT continuously. This goes beyond one-time gap analysis or project-based improvements, as it means embedding cybersecurity risk management into ongoing operations. Future works could develop a process model, potentially inspired by existing maturity models or the PDCA cycle from ISO 27001, that ties into the six domains. For example, the process might entail quarterly domain-specific reviews, management scorecards for each domain, and integration of security metrics into operational key performance indicators. It should also incorporate threat intelligence updates and lessons learned from incidents; when new vulnerabilities or attack techniques emerge, the continuous assessment process would trigger a re-evaluation of controls in the relevant domain. Many organizations conduct cybersecurity assessments infrequently, and even those that increase frequency struggle to maintain momentum [65].

A structured, continuous assessment process would help address the drop-off in commitment by assigning cadence and ownership to regularly review each domain’s status. This might involve developing mechanisms for continuous monitoring as part of the framework, freeing time from the assessments. Over time, the continuous assessment yields data that can show the organization's trends and direction. Incorporating that feedback loop would make the cybersecurity program more adaptive and proactive for the organization, rather than reactive. Many frameworks emphasize that cybersecurity risk management should be a continuous process of improvement, which would therefore align with our ideology. Ultimately, the goal is to enable continuous cybersecurity assessments so that security posture keeps pace with changes in the environment and threat landscape, thereby sustaining the efficacy of the six-domain framework over time. This is also recognised in the market with Fortinet calling this evolution Continuous Threat Exposure Management (CTEM) recommending organizations to adopt iterative, automated threat identification to stay ahead [19].

While this thesis lays the foundation by proposing and discussing a structured IT/OT cybersecurity framework, it also opens several avenues for future refinement. Addressing the

limitations through real-world pilots, tool development, and process integration will be crucial. By pursuing the future work highlighted, we will be closer to a sustainable, self-correcting cybersecurity management system for industrial environments. The advancements would validate the framework's concepts and provide practical means for organizations to improve their resilience against evolving cyber threats. The journey of securing IT/OT convergence is ongoing. Still, a structured, continuous, and verifiable approach, as envisioned, will significantly enhance an organization's ability to manage risk in this complex domain.

7 Conclusions

This thesis sets out to explore how a comprehensive, standards-based cybersecurity environment model can support IT/OT convergence in industrial environments. The convergence of information technology and operational technology systems has introduced both significant opportunities and cybersecurity challenges. A successful environment model must navigate the complexity of securing critical infrastructure, ensuring operational continuity, and meet growing regulatory demands while enabling innovation.

To this end, a detailed analysis of globally recognized cybersecurity standards was undertaken, focusing on the IEC 62443 series, ISO 27001, ISO 31000, ISO 27005, and the NIS2 directive. These documents provided a foundation for defining a structured approach that is modular, scalable, and applicable across diverse industrial contexts. Additionally, reference architectures such as PERA, RAMI 4.0, and the IIRA were examined to ensure that the proposed model aligns with modern industrial systems and their functional layers.

Having outlined the primary regulatory and industry frameworks, showing how each contributes to an integrated security posture. IEC 62443, in particular, informed the domain-based structure and mapped effectively across IT and OT control boundaries. The NIS2 directive introduced an imperative to manage cybersecurity risks in supply chains and critical sectors, reinforcing the need for governance at both organizational and system levels. There was also the introduction of the six-domain structure of the framework. This structure reflects how cybersecurity responsibilities and risks are distributed in an industrial setting. It supports a clear delineation between foundational components, platform-level requirements, operational procedures, and strategic oversight.

The thesis also shows the applicability of the framework and aims to demonstrate it. Technical sections provide real-world implementation strategies and aim to map them to relevant controls. While the issues of the environment model are also discussed, alongside the practicality of standard adoption, visibility of shared infrastructure, and the lack of harmonized reference architectures for IT/OT convergence.

As a reminder, the research questions are highlighted below.

1. How can industrial organizations develop a comprehensive IT/OT cybersecurity framework that balances security, operational efficiency, and regulatory compliance?

2. What are the main challenges and best practices for standardizing IT/OT infrastructure across diverse industrial facilities, and how can these be addressed using existing standards and models?

3. How does IT/OT integration impact cybersecurity postures in industrial environments, and what strategies can organizations adopt to mitigate emerging risks while enhancing interoperability and resilience?

The thesis showed that industrial organizations can achieve the balance of security, operational efficiency, and regulatory compliance by building a modular framework based on existing cybersecurity standards, while tailoring implementation to organizational context and maturity. Standards like IEC 62443 provide technical requirements across system and component levels, while ISO 27001 and ISO 31000 introduce governance and risk-based principles. The six-domain model proposed in the thesis enables organizations to deploy security practices in logical layers while maintaining interoperability and traceability.

Key challenges within IT and OT environments include legacy infrastructure, varied system architecture across sites, and misalignment between IT and OT teams. These are compounded by regulatory complexity and vendor diversity. Best practices include aligning all sites to a common security maturity model, applying zoning and segmentation per IEC 62443 3-2, and using control baselines like those in ISO 27001. PERA, RAMI 4.0, and IIRA frameworks guide the structural integration of business, functional, and technical perspectives.

IT/OT integration exposes systems to broader attack surfaces, increases the risk of lateral movement across domains, and introduces third-party vulnerabilities through supply chain interdependencies. Mitigation strategies include implementing zero-trust architectures, network segmentation, real-time monitoring with anomaly detection, and secure software development practices. Integration also demands new operational policies, such as secure remote maintenance and third-party onboarding, which are supported by the standards IEC 62443-2-4 and ISO 27035.

The framework presented is based on interpretive synthesis of standards and academic literature, and while generalizable, it has several limitations. The proposed model is designed for broad industrial relevance. However, sector-specific requirements may need tailored extensions to the framework. There is also a lack of empirical validations, as the framework has not been field-tested in a live environment. Effectiveness is based on theoretical alignment

with standards. The framework also emphasizes convergence principles, but does not address in detail the migration paths from legacy systems or the integration of emerging technologies.

This thesis has demonstrated the potential of a standards-based, domain-structured cybersecurity framework to address the growing challenges of IT/OT integration in industrial environments. A flexible and practical approach has been created by combining foundational guidance from internationally accepted standards with structural insight from reference models. The environment model emphasizes modularity, traceability, and resilience, ensuring that organizations can adapt to evolving threats and regulatory landscapes. Furthermore, it provides a basis for organizations to align their technical controls with governance policies, thereby improving visibility, accountability, and strategic planning.

While industrial cybersecurity continues to evolve rapidly, driven by digitalization, automation, and geopolitical risks, the foundational principles established here remain highly relevant. Organizations that adopt structured, standards-aligned strategies are better positioned to not only defend against emerging threats but also to foster operational innovation in secure and compliant ways.

The future work of this can explore empirical validation, maturity model development, and continuous assessment tooling to support dynamic cybersecurity lifecycle management in converged IT/OT environments.

References

[1] V. K. Khatri, A. J. Ghangro, J. Kumar and S. J. U. Haque, “Industrial Data Acquisition and Control System Using Two PLCs Networked over MPI Network,” Kuala Lumpur, Malaysia: IEEE, Oct. 2009, pp. 399–402. doi: 10.1109/ISIEA.2009.5356437.

[2] L. Hu, H. Li, Z. Wei, S. Dong and Z. Zhang, “Summary of Research on IT Network and Industrial Control Network Security Assessment,” in *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, Xi’an, China: IEEE, 2019, pp. 1203–1210. doi: 10.1109/ITNEC.2019.8729052.

[3] M. Wiboonrat, “Cybersecurity in Industrial Control Systems: An integration of information technology and operational technology,” in *IECON Proceedings (Industrial Electronics Conference)*, Brussels, Belgium: IEEE Computer Society, 2022. doi: 10.1109/IECON49645.2022.9968468.

[4] Jason D. Christopher, “SANS 2024 State of ICS/OT Cybersecurity,” Bethesda, Maryland, USA, Oct. 2024. Accessed: Oct. 16, 2024. [Online]. Available: https://www.sans.org/white-papers/sans-2024-state-ics-ot-cybersecurity/

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

[6] H. Kanamaru, “The Extended Risk Assessment Form for IT/OT Convergence in IACS Security,” in *2021 60th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*, Tokyo, Japan, 2021, pp. 1365–1370.

[7] K. Zhang, Y. Shi, S. Karnouskos, T. Sauter, H. Fang and A. W. Colombo, “Advancements in Industrial Cyber-Physical Systems: An Overview and Perspectives,” Jan. 01, 2023, *IEEE Computer Society*. doi: 10.1109/TII.2022.3199481.

[8] M. W. Santiago Soler Perez Olaya, “The Role of Comprehensive Function Models in the Management of Heterogeneous Industrial Networks,” Institute of Electrical and Electronics Engineers, Dresden, Germany, May 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8758047

[9] Inc. Fortinet, “2024 State of Operational Technology and Cybersecurity Report,” Sunnyvale, California, USA, Mar. 2024. Accessed: Nov. 01, 2024. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-ot-cybersecurity.pdf

[10] H. Boyes, B. Hallaq, J. Cunningham and T. Watson, “The industrial internet of things (IIoT): An analysis framework,” *Computers in Industry*, vol. 101, pp. 1–12, Oct. 2018, doi: 10.1016/j.compind.2018.04.015.

[11] T. Burns, J. Cosgrove and F. Doyle, “A review of interoperability standards for industry 4.0.,” *Procedia Manufacturing*, vol. 38, pp. 646–653, 2019, doi: 10.1016/j.promfg.2020.01.083.

[12] M. Salah and L. M. Elshenawy, “Attacks Detection in Industrial Cyber-Physical Systems Using Convolutional Neural Networks,” in *ICEEM 2023 - 3rd IEEE International Conference on Electronic Engineering*, Menouf, Egypt: Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ICEEM58740.2023.10319541.

[13] S. Li, F. Meng, D. Zhang, Q. Liu, L. Lu and Y. Ye, “Research on Security Defense System of Industrial Control Network,” in *Proceedings of 2021 IEEE 2nd International Conference on Information Technology, Big Data and Artificial Intelligence, ICIBA 2021*, Chongqing, China: Institute of Electrical and Electronics Engineers Inc., 2021, pp. 631–635. doi: 10.1109/ICIBA52610.2021.9687994.

[14] Zsolt Szabó, “Cybersecurity Issues in Industrial Control Systems,” in *2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY)*, IEEE, 2018. doi: 10.1109/SISY.2018.8524613.

[15] A. B. Berhe, K.-H. Kim and G. A. Tizazu, “Industrial Control System Security Framework for Ethiopia,” IEEE, Addis Ababa, Ethiopia and Suwon, South Korea, Jul. 2017. doi: 10.1109/ICUFN.2017.7993912.

[16] European Parliament and Council, “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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive),” Brussels, Belgium, Dec. 2022. [Online]. Available: http://data.europa.eu/eli/dir/2022/2555/oj

[17] International Society of Automation, “Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design (ANSI/ISA-62443-3-2:2020),” Research Triangle Park, NC, USA, 2020. [Online]. Available: https://www.isa.org

[18] International Organization for Standardization and International Electrotechnical Commission, “Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC 27001:2022),” Geneva, Switzerland, 2022. [Online]. Available: https://www.iso.org

[19] Fortinet, “GLOBAL THREAT LANDSCAPE REPORT 2025,” Sunnyvale, California, USA, May 2025. Accessed: May 27, 2025. [Online]. Available: https://www.fortiguard.com/ThreatLandscapeReport

[20] M. Negi and M. Karimi, “IT/OT challenges and opportunities to improve cyber resiliency for utilities: A review paper,” in *IEEE PES Innovative Smart Grid Technologies Europe, ISGT EUROPE 2024*, Dubrovnik, Croatia: Institute of Electrical and Electronics Engineers Inc., 2024, pp. 1–5. doi: 10.1109/ISGTEUROPE62998.2024.10863572.

[21] A. Atieh, P. Nanda and M. Mohanty, “A Zero-Trust Framework for Industrial Internet of Things,” in *2023 International Conference on Computing, Networking and Communications, ICNC 2023*, Honolulu, HI, USA: Institute of Electrical and Electronics Engineers Inc., 2023, pp. 331–335. doi: 10.1109/ICNC57223.2023.10074295.

[22] International Electrotechnical Commission, “Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels (IEC 62443-3-3:2013),” International Electrotechnical Commission, Geneva, Switzerland, 2013. [Online]. Available: https://www.iec.ch

[23] International Electrotechnical Commission, “Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program (IEC 62443-2-1:2010),” International Electrotechnical Commission, Geneva, Switzerland, 2010. [Online]. Available: https://www.iec.ch

[24] International Organization for Standardization and International Electrotechnical Commission, “Information security, cybersecurity and privacy protection – Information security controls (ISO/IEC 27002:2022),” Geneva, Switzerland, 2022. [Online]. Available: https://www.iso.org

[25] A. Apostlov, *IEC 61850: Digitizing the Electric Power Grid*. Norwood, MA, USA, 2022.

[26] Z. Wang, S. Ma, T. Wang and W. Tao, “Research on Industrial System Operation Pattern Recognition Based on Deep Generative Model,” in *ICEIEC 2024 - Proceedings of 2024 IEEE 14th International Conference on Electronics Information and Emergency Communication*, Beijing, China: Institute of Electrical and Electronics Engineers Inc., 2024, pp. 217–220. doi: 10.1109/ICEIEC61773.2024.10561874.

[27] D. Zhang, P. Zhang, W. Wang, M. Jin and F. Xiao, “Evaluation of Network Security State of Industrial Control System Based on BP Neural Network,” in *2022 4th World Symposium on Artificial Intelligence, WSAI 2022*, Jilin, China: Institute of Electrical and Electronics Engineers Inc., 2022, pp. 1–8. doi: 10.1109/WSAI55384.2022.9836386.

[28] M. Li, W. Li, P. Yu and F. Zhou, “Risk Prediction of the SCADA Communication Network Based on Entropy-Gray Model,” IEEE, Tokyo, Japan, Nov. 2017. doi: 10.23919/CNSM.2017.8256004.

[29] International Society of Automation, “Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components (ANSI/ISA-62443-4-2-2018),” ISA, Research Triangle Park, NC, USA, 2018. [Online]. Available: https://www.isa.org

[30] International Organization for Standardization, “Security and resilience – Business continuity management systems – Requirements (ISO 22301:2019),” Geneva, Switzerland, 2019. [Online]. Available: https://www.iso.org

[31] International Organization for Standardization and International Electrotechnical Commission, “Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management (ISO/IEC 27035-1:2016),” British Standards Institution, Geneva, Switzerland, 2016. [Online]. Available: https://www.iso.org

[32] International Organization for Standardization, “Risk management – Guidelines (ISO 31000:2018),” Geneva, Switzerland, 2018. [Online]. Available: https://www.iso.org

[33] International Organization for Standardization and International Electrotechnical Commission, “Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response (ISO/IEC 27035-2:2016),” British Standards Institution, Geneva, Switzerland, 2016. [Online]. Available: https://www.iso.org

[34] International Organization for Standardization and International Electrotechnical Commission, “Information security, cybersecurity and privacy protection – Guidance on managing information security risks (ISO/IEC 27005:2022),” Geneva, Switzerland, 2022. [Online]. Available: https://www.iso.org

[35] International Electrotechnical Commission, “Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers (IEC 62443-2-4:2015),” International Electrotechnical Commission, Geneva, Switzerland, 2015. [Online]. Available: https://www.iec.ch

[36] Anderson Ross, *Security Engineering: A Guide to Building Dependable Distributed Systems (3rd Edition)*, 3rd ed. Indianapolis, Indiana, USA: John Wiley & Sons, Inc., 2020. [Online]. Available: https://www.wiley.com/en-us/Security+Engineering%3A+A+Guide+to+Building+Dependable+Distributed+Systems%2C+3rd+Edition-p-9781119642787

[37] International Electrotechnical Commission, “Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements (IEC 62443-4-1:2018),” Geneva, Switzerland, 2018. [Online]. Available: https://www.iec.ch

[38] OWASP Foundation, “OWASP Secure Coding Practices – Quick Reference Guide (Version 2.0),” Online, Nov. 2010. [Online]. Available: https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/

[39] OWASP Foundation, “OWASP Top Ten,” https://owasp.org/www-project-top-ten/. [Online]. Available: https://owasp.org/www-project-top-ten/

[40] International Organization for Standardization and International Electrotechnical Commission, “Information technology – Security techniques – Information security controls for the energy utility industry (ISO/IEC 27019:2017),” Geneva, Switzerland, 2017. [Online]. Available: www.iso.org

[41] International Organization for Standardization, “Health informatics – Information security management in health using ISO/IEC 27002 (ISO 27799:2016),” Geneva, Switzerland, 2016. [Online]. Available: https://www.iso.org/

[42] THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, “REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016,” 2016.

[43] European Parliament and Council, “Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC,” Brussels, Belgium, May 2014. [Online]. Available: http://data.europa.eu/eli/dir/2014/53/oj

[44] European Commission, “Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f),” Brussels, Belgium, Jan. 2022. [Online]. Available: https://eur-lex.europa.eu/eli/reg_del/2022/30/oj

[45] European Commission, “Commission Delegated Regulation (EU) 2023/2444 of 20 July 2023,” Brussels, Belgium, Oct. 2023. [Online]. Available: https://eur-lex.europa.eu/eli/reg_del/2023/2444/oj

[46] European Commission, “Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act),” Brussels, Belgium, Oct. 2024. Accessed: Apr. 01, 2025. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847

[47] International Electrotechnical Commission, “Security for Industrial Automation and Control Systems – Part 4-1: Secure Product Development Lifecycle Requirements (IEC

62443-4-1:2018),” Geneva, Switzerland, Jan. 2018. [Online]. Available: https://www.isa.org/

[48] M. Shohoud, “Study the Effectiveness of ISO 27001 to Mitigate the Cyber Security Threats in the Egyptian Downstream Oil and Gas Industry,” *Journal of Information Security*, vol. 14, no. 02, pp. 152–180, 2023, doi: 10.4236/jis.2023.142010.

[49] J. Benjamin, “Correcting Prevention Bias in Your OT Cyber Incident Response,” Dragos Blog. Accessed: Apr. 26, 2025. [Online]. Available: https://www.dragos.com/blog/correcting-prevention-bias-in-your-ot-cyber-incident-response/

[50] Y. Cherdantseva *et al.*, “A review of cyber security risk assessment methods for SCADA systems,” *Computers and Security*, vol. 56, pp. 1–27, Feb. 2016, doi: 10.1016/j.cose.2015.09.009.

[51] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso and K. Jones, “A survey of cyber security management in industrial control systems,” *International Journal of Critical Infrastructure Protection*, vol. 9, pp. 52–80, Jun. 2015, doi: 10.1016/j.ijcip.2015.02.002.

[52] The MITRE Corporation, “MITRE ATT&CK® for Industrial Control Systems (ICS),” McLean, Virginia, USA, Mar. 2020. Accessed: Apr. 05, 2025. [Online]. Available: https://attack.mitre.org/techniques/ics/

[53] K. Stouffer *et al.*, “Guide to Operational Technology (OT) Security (NIST SP 800-82 Rev. 3),” Gaithersburg, Maryland, USA, 2023. Accessed: Apr. 26, 2025. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

[54] North American Electric Reliability Corporation (NERC), “NERC Critical Infrastructure Protection (CIP) Reliability Standards,” 2024. Accessed: Apr. 27, 2025. [Online]. Available: https://www.nerc.com/pa/Stand/Pages/Default.aspx

[55] Krishnan Ashwin, “Top 10 ICS Cybersecurity Threats and Challenges,” Newton, Massachusetts, USA, Jan. 2023. Accessed: Apr. 01, 2025. [Online]. Available: https://www.techtarget.com/searchsecurity/tip/Top-10-ICS-cybersecurity-threats-and-challenges

[56] Kovacs Eduard, “ICS, OT Cybersecurity Incidents Cost Some U.S. Firms Over $100 Million: Survey,” Sarasota, Florida, USA, Nov. 2021. Accessed: Apr. 01, 2025. [Online]. Available: https://www.securityweek.com/ics-ot-cybersecurity-incidents-cost-some-us-firms-over-100-million-survey/

[57] A. Amiri, G. Steindl and S. Hollerer, “Integrated Safety and Security by Design in the IT/OT Convergence of Industrial Cyber-Physical Systems,” in *2024 IEEE 7th International Conference on Industrial Cyber-Physical Systems, ICPS 2024*, St. Louis, MO, USA: Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/ICPS59941.2024.10640023.

[58] R. S. H. Piggin, “Governance, risk and compliance: impediments and opportunities for managing operational technology risk in industrial cyber security and safety,” United Kingdom, Oct. 2014. [Online]. Available: https://doi.org/10.1049/cp.2014.0982

[59] A. O. Rotibi, N. Saxena, P. Burnap and A. Tarter, “Extended Dependency Modeling Technique for Cyber Risk Identification in ICS,” *IEEE Access*, vol. 11, pp. 37229–37242, Apr. 2023, doi: 10.1109/ACCESS.2023.3263671.

[60] J. Easterly and Fanning Tom, “The Attack on Colonial Pipeline: What We’ve Learned & What We’ve Done Over the Past Two Years,” Washington, D.C., USA, May 2023. Accessed: Apr. 01, 2025. [Online]. Available: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

[61] Giles Martin, “Triton is the World’s Most Murderous Malware, and It’s Spreading,” Cambridge, Massachusetts, USA, Mar. 2019. Accessed: Apr. 01, 2025. [Online]. Available: https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/

[62] Gates Megan, “ICS 2022 in Review: The Rise of PIPEDREAM and Ransomware,” Alexandria, Virginia, USA, Feb. 2023. Accessed: Apr. 01, 2025. [Online]. Available: https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2023/february/ICS-2022-in-Review/

[63] Briggs Bill, “Hackers Hit Norsk Hydro with Ransomware. The Company Responded with Transparency,” Microsoft News. Accessed: Apr. 01, 2025. [Online]. Available: https://news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

[64] Cerf Emily, “Ukraine Blackouts Caused by Malware Attacks Warn Against Evolving Cybersecurity Threats to the Physical World,” Santa Cruz, California, USA, May 2024. Accessed: Apr. 01, 2025. [Online]. Available: https://news.ucsc.edu/2024/05/ukraine-cybersecurity/

[65] Verve Industrial Protection, “OT Security Assessments: Beyond Manual Methods,” Downers Grove, Illinois, USA, Feb. 2024. Accessed: Apr. 01, 2025. [Online]. Available: https://verveindustrial.com/resources/blog/ot-security-assessments-traditional-to-technology-enabled/