Software und Digitalisierung

Applied Risk Management for Plant Operators & Asset Owners: Quick Start

VDMA Experts' Circle Security Solutions for Industry

22.05.2025

Preface

Due to changing regulatory requirements (CRA, NIS2, amongst others), the machinery and plant building industry is mandated to establish cybersecure production environments and produce cybersecure products.

Effective security may necessitate action in various organizational units of a company, even though the total security budget may be limited.

This is why the VDMA's Expert Circle Security Solutions for Industry chooses a risk-based approach. The measures described within this guide are of intrinsic motivation, as they prioritize maximizing a company's security with regulatory compliance as a secondary effect – regardless of this, whenever a measure also fulfills any regulatory requirements, this is clearly mapped.

This guideline is applicable to businesses with different levels of security, but aims to also support companies that just start out with their security concept.

Created by the VDMA's Expert Circle Security Solutions for Industry. We aim to support the productive industry branches with guidelines and best practices that enable companies to secure their business. The Circle consists of security experts from various VDMA-Members that have Cybersecurity as their core business.

Contents

Executive Summary

This document, Applied Risk Management for Plant Operators and Asset Owners: Quick Start, serves as a practical guide for implementing cybersecurity risk management practices in industrial environments. Developed by the VDMA Experts' Circle Security Solutions for Industry, it aims to help plant operators and asset owners prioritize cybersecurity efforts, especially when working within constrained resources.

The guide begins by recognizing the evolving regulatory landscape and the need for action across different organizational units to achieve secure operations. It underscores a risk-based approach to cybersecurity, focusing on practical and strategic investments rather than broad, generic compliance efforts.

The main chapters present a structured methodology for risk management in operational technology (OT) environments. Starting with an overview of a typical reference architecture, the document describes the distinct network zones (Enterprise Network, IDMZ, and Industrial Network) and identifies the unique security challenges associated with each.

Subsequent sections introduce a comprehensive process for threat analysis and risk assessment. The approach leverages recognized frameworks like IEC 62443-3-2, STRIDE, and MITRE ATT&CK®, enriched with practical examples to bridge the gap between theoretical standards and real-world implementation. The assessment process involves identifying assets, analyzing threats, assigning impact levels, and calculating residual risks. The goal is to develop a clear picture of the current security posture and guide targeted risk mitigation efforts.

The document places strong emphasis on control selection and prioritization. Rather than recommending exhaustive control lists, it proposes a phased implementation strategy based on control maturity and risk impact. This approach encourages organizations to focus first on a core set of foundational controls that provide the highest return on security investment. Enhanced and comprehensive security coverage is achieved progressively as resources and organizational maturity grow.

An epilogue highlights the collaborative effort of the VDMA Experts' Circle in creating this practical guide and encourages feedback and contributions for future improvements. Supplementary sections include references, literature resources, legal disclaimers, details about the working group, and publication information.

1. Introduction

The introduction of the Network and Information Systems Directive 2 (NIS2) [1] marks a transformative milestone in the European Union's approach to cybersecurity, particularly for manufacturing companies. With a broadened scope and stricter requirements, NIS2 mandates organizations, including those in the operational technology (OT) domain, to adopt robust cybersecurity measures. For manufacturing plants — often the backbone of industrial operations — this directive underscores the necessity to protect production environments against ever-evolving cyber threats. Yet, for many organizations, especially those with minimal cybersecurity measures in place, achieving compliance may seem overwhelming, particularly under tight budgetary and personnel constraints.

1.1 The Challenge for OT Manufacturers

Historically, OT networks have prioritized safety, reliability, and availability over cybersecurity. Unlike information technology (IT) environments, OT systems often consist of legacy devices, devices using proprietary protocols, and safety-critical real-time operations that were usually not designed with cybersecurity in mind. This makes them particularly vulnerable to cyberattacks, ranging from ransomware targeting industrial control systems (ICS) to nation-state actors seeking to disrupt critical infrastructure.

Under NIS2, manufacturers must demonstrate that they have implemented "appropriate and proportionate technical, operational, and organizational measures" to mitigate these risks. However, for organizations starting from scratch, understanding where to focus their efforts is crucial. The question then arises:

If I am a manufacturing company with only basic and/or unmanaged cybersecurity controls, which measures should I prioritize to achieve the greatest risk reduction?

1.2 A Risk-Based Approach to Cybersecurity

At its core, cybersecurity is a discipline of risk management. Every security measure we implement — whether deploying a firewall in our home or organization, encrypting sensitive passwords, or adopting advanced cybersecurity countermeasures — is driven by the intention to reduce or, ideally, eliminate specific risks.

Recognizing this fundamental principle, regulatory frameworks such as NIS2 (cf. Art. 21 in [1]), the Cyber Resilience Act (CRA) (cf. Part I (1), Annex I in [2]), and the EU Machinery Regulation (cf. Part B (1), Annex III in [3]) all place risk management at the core of their requirements. These regulations emphasize a structured approach to identifying, assessing, and mitigating risks as a fundamental aspect of cybersecurity compliance.

In this document, we focus on addressing cybersecurity risks for manufacturers and OT operators with technical rigor. While various risk management frameworks exist, we adhere to the principles outlined in IEC 62443-3-2 [4], a widely recognized standard in industrial automation and control system (IACS)[1] security. IEC 62443 provides a systematic approach to risk assessment and mitigation, enabling organizations to prioritize resources effectively and implement security measures proportionate to the identified threats.

Where the IEC 62443 standard does not provide sufficient technical depth, particularly regarding threat modeling and likelihood estimation, we complement it with elements from other well-established risk assessment methodologies, especially Threat Analysis and Risk Assessment (TARA), to ensure a more complete and technically sound evaluation.

1 The terms "ICS", "IACS", "OT environment" are used interchangeably in this document

For the sake of this document and to keep the character of a "quick start guide", we've made some simplifications when applying IEC 62443-3-2:

- Using a generic System Under Consideration – yours will look different
- Limited to 3 to 4 possible threats per asset – your threat landscape will differ
- Focus on the assets – as per IEC 62443-3-2, conduits need to be assessed as well

At its core, the risk-based approach of this document involves:

1. **Understanding the Reference Architecture:** Using a typical OT network reference architecture to visualize the current state of the network and its components. In this document, we propose a reference architecture for typical industrial deployments based on the consensus of all participants in the Experts' Circle.
2. **Identifying Risks:** Conducting a thorough risk assessment to identify vulnerabilities, threats, and potential consequences across the OT environment. This step is particularly important for environments that lack existing controls, as the risk surface is often broad and diverse.
3. **Prioritizing Risks:** Evaluating risks based on their likelihood and impact to focus on the most critical areas first.
4. **Note:** This is a simplification. It can be helpful to also consider the perspective from threat to impact, or to prioritize based on business-relevant flows such as material flow or cash flow, which may offer additional insight.
5. **Implementing Targeted Controls:** Recommending specific controls to mitigate identified risks.
6. **Balancing Costs and Benefits:** Considering the financial constraints of manufacturers, the proposed controls are selected for their ability to maximize risk reduction while minimizing implementation complexity and cost.

1.3 Goal of this Document: Strategic Cybersecurity Investment

The implementation of appropriate cybersecurity measures in the initial stage can achieve a significant reduction in risks with a relatively small investment. By prioritizing controls with the greatest impact on cybersecurity, organizations can establish a strong baseline of protection without requiring large budgets or extensive resources [5].

Accordingly, this document aims to help OT manufacturers answer a central question:

> **How can I strategically allocate limited budget and resources to implement the most effective cybersecurity controls in my production environment?**

It is essential to acknowledge that the recommendations provided in this document are based on our experience with typical OT setups and are intended to serve as a general guide. However, every manufacturing company is unique, and each OT network has its own distinct characteristics and vulnerabilities. While the controls outlined here are designed to address many common risks in OT environments, we cannot guarantee their effectiveness in mitigating the specific risks of the reader's particular setup. As required by NIS2, each organization must conduct its own comprehensive risk assessment with full scope, i.e., including its production environment. Only through this individualized approach can companies ensure they are addressing the specific cybersecurity challenges they face.

By focusing on a small number of foundational controls, manufacturers can achieve several key objectives: rapidly reducing risks by addressing the most significant threats to their operations, strengthening their overall cybersecurity posture in line with NIS2 requirements, and safeguarding the continuity of their production processes by minimizing downtime caused by cyber incidents. While this document offers a starting point, it is ultimately the responsibility of each company to adapt these recommendations to their unique circumstances, ensuring their approach to cybersecurity aligns with both regulatory obligations and operational needs.

1.4 Structure of this Document

This document aims to guide plant operators and asset owners through a pragmatic approach to cybersecurity risk management. It begins with a detailed Introduction that contextualizes the cybersecurity challenges faced by OT manufacturers, describes the risk-based approach adopted in the document, and defines the goal of the guide as a tool for strategic cybersecurity investment.

Following the introduction, the Reference Architecture chapter outlines a representative OT architecture. It includes descriptions of key network zones: the Enterprise Network, the Industrial Demilitarized Zone (IDMZ), and the Industrial Network. These sections highlight the unique components, interactions, and security concerns of each zone.

The next main chapter, Threat Analysis and Risk Assessment, details the process for identifying assets, analyzing potential threats, and evaluating the associated risks. This section incorporates methodologies and standards like IEC 62443-3-2 and enriches them with practical techniques (e.g., STRIDE and MITRE ATT&CK frameworks). It also covers the assignment of impact levels and the evaluation of residual risks after applying mitigating controls.

The document continues with a Discussion on Control Selection and Prioritization, which emphasizes the importance of focusing on a small set of foundational controls. It discusses control selection based on maturity and impact, proposing a phased implementation plan that aligns with real-world resource constraints.

Finally, the document includes an Epilogue that highlights the collaborative effort of the VDMA Experts' Circle Security Solutions for Industry in creating this guideline. It stresses the critical need for OT security and encourages ongoing improvements in risk management practices.

To support further reading and application, the document concludes with a References section listing all cited sources, a Literature section for supplementary resources, and Legal Notices to clarify the document's non-binding nature. The final sections include details about the Working Group and an Imprint providing publication and contact information.

2. Reference Architecture

In this document, we have chosen a reference architecture that we believe best represents the real-world operational technology architectures commonly observed within the manufacturing environments of our members. This reference architecture is designed to illustrate the complex interactions between various components and the hierarchical nature of OT networks. It spans an entire production facility, encompassing everything from the foundational production processes to the enterprise-level management systems.

At the core of this architecture is a supervisory controller, often referred to as a control server, which manages subordinate devices through a dedicated control network. The supervisory controller communicates critical instructions, such as operational setpoints, to field-level controllers while simultaneously collecting data from these devices. The distributed field controllers—such as programmable logic controllers (PLC), machine controllers, and process controllers—play a pivotal role. They translate the high-level commands from the supervisory controller into precise actions by engaging with process actuators and interpreting real-time feedback from various sensors within the system.

This architecture also highlights the diverse communication methodologies that exist within OT environments. For instance, some controllers rely on traditional point-to-point wiring to interface with sensors and actuators. Others, however, utilize fieldbus networks, which simplify infrastructure by eliminating the need for extensive wiring. These fieldbus systems not only streamline communication but also enhance functionality. They support device diagnostics, allow for decentralized control logic execution directly within the network, and minimize the need for constant signal routing back to central controllers like PLCs. Standardized industrial communication protocols, such as Modbus and Fieldbus, are frequently employed across control networks and fieldbus systems to ensure seamless integration and interoperability among devices.

Please note: The following figure represents an "unsecure" configuration – Security controls are needed here. This serves as our starting point for the following risk assessment. Once we have determined necessary security controls, we will show them in our concluding network architecture at the end of this guideline.

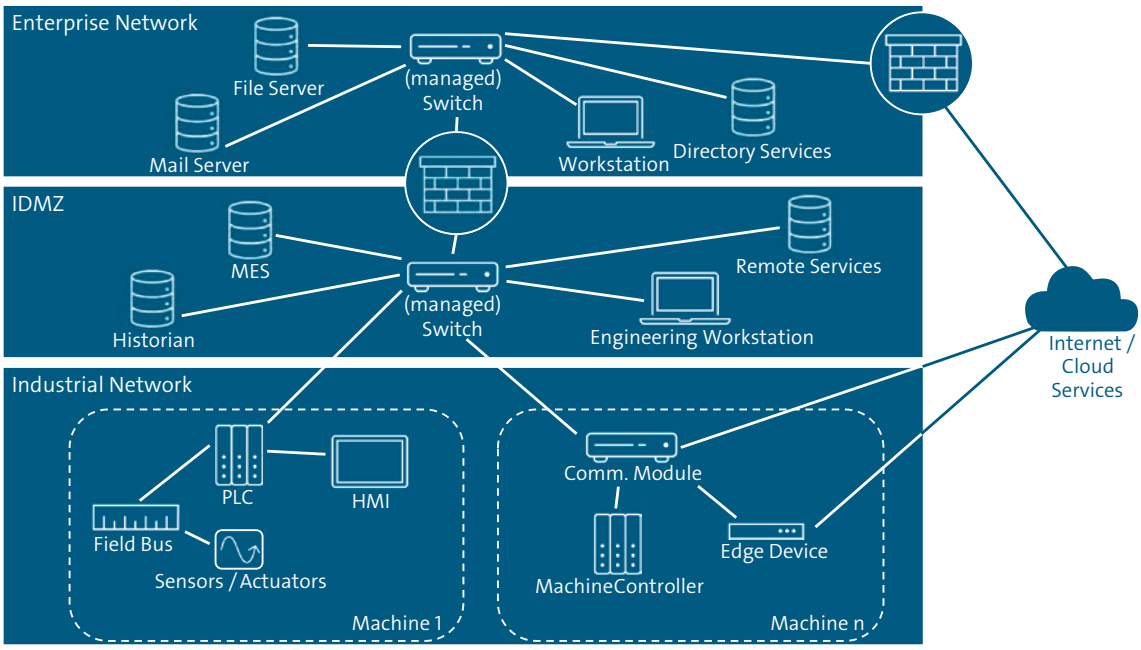
2.1 Description of the System under Consideration (SUC)

The impact levels of the zones shown in Figure 1 and described here is only a high-level approach to give a first impression of exposure and impact. Later in Table 1, we assign impact levels according to the assessment categories described in IEC 62443-3-2:2020 for each asset of the zones. The impact level for the whole zone is given by the highest impact level for the assets contained within the zone. Different assets within one zone will have different exposure and therefore different impacts and risks associated with them.

Note on Safety Instrumented Systems (SIS): This document focuses on the practical application of OT cybersecurity risk management for small to mid-sized industrial organizations. As such, SIS are not considered within the scope of the presented reference architecture or risk management approach. In many small to mid-sized operations, SIS are either not deployed or are governed by separate safety regulations and lifecycle processes that are outside the core cybersecurity domain addressed here. While cybersecurity considerations for SIS are critical in high-risk industries (e.g., oil & gas, chemical), our aim is to provide a pragmatic and accessible framework aligned with the typical OT environments of our target audience. Organizations with integrated SIS should complement this guidance with industry-specific standards such as IEC 61511 and consider dedicated risk assessments that address the intersection of safety and security.

Figure 1:

System under consideration



2.1.1 Enterprise Network

Description:

The Enterprise Network represents the highest-level systems in the OT environment that interface with business operations. This zone typically includes IT-systems used for decision-making, planning, and overall management of the production facility. Typically Mail Servers, Web Servers, ERP and CRM Systems and others are contained within this network. The Enterprise Network usually connects to the Internet and other external (Cloud-)Services.

Especially because of the numerous connections to remote clients and external networks, the Enterprise Network faces IT-related threats. The Enterprise Network should be separated from networks containing critical assets, to ensure proper defense-in-depth and limit the impact of IT-related incidents on the OT-Infrastructure. While attacks here might not immediately disrupt production, they can compromise sensitive business data or provide an entry point to lower zones.

Impact Level:

Medium—Compromise may lead to data breaches, loss of intellectual property, or enable further attacks on critical production zones.

-or-

High – It should be assessed, if critical business processes depend on IT Infrastructure. If so, Incidents in the Enterprise Network can also disrupt OT-Systems.

For the purpose of this document, we classify the Impact Level of the Enterprise Network as **medium.** Please consider IEC 62443-3-2:2020 Table B.3 for assessing the impact associated with the Enterprise Network when conducting a risk assessment.

Examples of Assets:

- File Server
- Mail Server
- Workstation
- Managed Switch
- Web Server

2.1.2 Industrial Demilitarized Zone (IDMZ)

Description:

This zone serves as the intermediary between the enterprise and the production processes. It is responsible for monitoring and controlling the operations in real-time. The systems here act as the "brains" of the production facility, making it critical for maintaining operational continuity. Communications between networks should be set up via conduits with firewalls to reduce the risk of unauthorized access and other outside threats to critical OT Systems and Processes. With these conduits and the DMZ Infrastructure, an organization can effectively separate networks and monitor traffic while simultaneously enabling controlled communication and enforcement of security policies. Only explicitly allowed connections and protocols should pass through the DMZ.

Impact Level:

High—Attacks can disrupt coordination between higher-level management systems and low-level production, leading to operational inefficiencies or stoppages.

Examples of Assets:

- Manufacturing Execution System (MES)
- Engineering Workstations
- Historian
- Managed Switch

2.1.3 Industrial Network

Description:

The Industrial Network encompasses the low-level field devices that directly control and monitor physical processes. These systems are the most critical to production, as they interact directly with machinery, sensors, and actuators. Any disruption here can lead to immediate production stops, equipment damage, or safety risks. Safety and Availability are a major concern for these networks. Downtime of these networks, caused by incidents or system maintenance, should be reduced to a minimum, to ensure productivity. Additional challenges also stem from the widespread use of legacy technology in these networks: in contrast to IT-systems, OT-systems often use legacy devices and protocols, as industrial automation systems are too specialized and expensive to be updated/upgraded as regularly as IT-systems.

Impact Level:

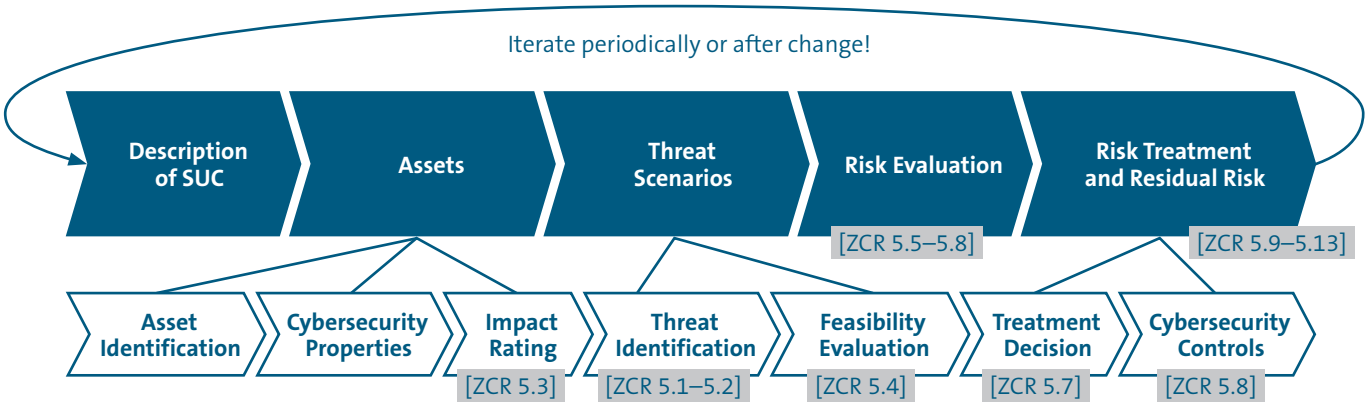
High—A compromise can halt production, damage physical assets, or endanger human safety and/or the environment.

Examples of Assets:

- Programmable Logic Controllers
- Human-Machine Interface (HMI)
- Sensors (e.g., temperature, pressure, and flow sensors)
- Actuators (e.g., valves, motors, and pumps)
- Fieldbus Systems and Associated Controllers
- Communication Devices (e.g. Remote access routers)
- Edge Devices

3. Threat Analysis and Risk Assessment

Figure 2:
Overall threat anlaysis and risk assessment process



Legend: Work package from IEC 62443-3-2

In this chapter, we address the modelling of threats and the execution of the risk assessment. We follow the methodology of the IEC 62443-3-2 standard [4], which provides a generic, yet structured approach specifically designed for OT environments. This makes it suitable as a foundational framework for risk-oriented security assessments in industrial systems.

However, while IEC 62443-3-2 offers a solid base, certain aspects, such as the evaluation of threat likelihood, remain described in rather abstract terms. Therefore, this document goes beyond the standard and serves as a practical guide for performing threat analysis and risk assessment in real-world industrial settings. Our aim is to increase the usability of the framework by providing concrete instructions, examples, and decision-making criteria that are immediately applicable.

Where the guidance in IEC 62443-3-2 proves too generic or high-level, we enrich the methodology by incorporating proven techniques from other domains. For example, we use STRIDE and the MITRE ATT&CK framework to support structured and comprehensive threat identification. These models allow for a more precise mapping of threats to components and functions, enabling improved traceability and completeness. Furthermore, for the estimation of likelihood, we adopt a tailored approach inspired by the TARA methodology from the automotive cybersecurity domain. TARA provides a systematic means to evaluate the feasibility of attacks based on attacker capabilities, required resources, and potential entry points. This allows us to overcome the limitations of generic probability scales and instead ground our analysis in realistic threat scenarios and attacker models.

Accordingly, we perform a detailed risk assessment aligned with IEC 62443-3-2 while integrating enhancements where necessary to increase the practicality and applicability of the process (see chapter ZCR 5: Performing a detailed cyber security risk assessment). The overall process is depicted in Figure 2.

3.1 The Assets

The assets utilized in our evaluation were previously introduced in Section 2.1. Table 1 provides a detailed description of the relevant cybersecurity objectives associated with each asset and includes the corresponding impact assessment.

The use of cybersecurity objectives, confidentiality (C), integrity (I), and availability (A), serves as a structured way to evaluate and model the potential impact of cyberattacks on assets. These three objectives, known as CIA triad[2], represent the core properties that define the security profile of an asset and help to assess the consequences if the asset is compromised:

- **Confidentiality** ensures that sensitive data is only accessible to authorized individuals and systems. A breach of confidentiality could lead to unauthorized disclosure of sensitive business information or operational data, which may result in competitive disadvantages, reputational damage, or regulatory penalties.
- **Integrity** ensures that data and system configurations remain accurate and unaltered. If integrity is compromised, manipulated data or system behavior could lead to incorrect decisions, faulty production processes, or safety hazards.
- **Availability** ensures that assets remain accessible and operational when needed. Loss of availability could lead to production downtimes, operational failures, or safety incidents. In industrial environments, availability has usually higher priority than other cybersecurity objectives.

2 Other cybersecurity objectives, such as authenticity and non-repudiation, exist in the literature. We follow the CIA triad as defined in IEC 62443, but other objectives can and should be used if relevant.

It is important to note that not all cybersecurity objectives are relevant for every asset. The relevance of confidentiality, integrity, and availability depends on the specific function and purpose of the asset within the system. For example, a file server that stores sensitive business data requires strong confidentiality protections, whereas a PLC used in a production line may prioritize availability and integrity over confidentiality. If a particular cybersecurity property is not relevant to an asset, it does not need to be modeled or evaluated. This approach helps focus the risk assessment on meaningful threats and avoids inflating the analysis with irrelevant scenarios.

3.1.1 Impact Evaluation

In the context of IEC 62443-3-2, the consequence or severity of an incident can be categorized into three impact levels: **A (High), B (Medium), and C (Low).** These categories help assess the potential outcomes of a security breach or failure across various domains such as operations, finances, legal impact, public confidence, and health, safety, and environment (HSE).

Category A (High impact) refers to severe consequences such as prolonged outages, major disruption to national infrastructure, very high financial losses, significant legal implications (e.g., felony), and critical HSE effects like fatalities or widespread environmental damage.

Category B (Medium impact) includes moderate disruptions that may extend beyond the company level, noticeable financial loss, legal concerns (e.g., misdemeanors), and health and safety effects that cause lost work time or local community concern.

Category C (Low impact) represents limited or localized consequences, minimal financial and legal repercussions, and minor or no HSE effects.

For detailed definitions and criteria associated with each impact level, please refer to Table B.3 of the IEC 62443-3-2:2020 standard [4].

Discussion on the correct impact evaluation

The impact evaluation presented in this section provides a structured overview of the potential consequences associated with the compromise of each identified asset. The specific impact values assigned (high, medium, low) reflect a combination of operational, financial, and health, safety, and environmental (HSE) considerations, as defined in IEC 62443-3-2 ZCR 5.3. While we followed an accurate evaluation of the presented assets based on the authors' experience, the document still reflects an exemplary architecture. For this reason, it is important to emphasize that the impact assessment should be carefully reviewed and adjusted based on the unique characteristics and operational context of each OT system. Variations in system architecture, process dependencies, and business requirements may lead to different outcomes in real-world scenarios. Therefore, while the table provides a consistent and standardized framework for initial impact evaluation, the actual impact for each system must be assessed in detail.

Please note: We've omitted confidentiality as a relevant security objective for some of the assets in the Industrial Network. Please carefully evaluate, if confidentiality is necessary for any data held by every asset when conducting your own impact assessment! Furthermore, we also did not consider, if assets communicate wirelessly or hard-wired. Wireless communication faces additional threats, like jamming, that could impact their availability.

Table 1:

Summary of the identified assets and their impact assessment

Asset	Relevant cybersecurity objectives[3]	Impact [IEC 62443-3-2 ZCR 5.3]		
		Operational	Financial	HSE
	Enterprise Network			
File Server	C: relevant for protecting sensitive business data. I: data stored or transmitted is relevant for production and, therefore, it shall not be manipulated. A: the file server must be accessible for ICS operations, log analysis, and process continuity.	B (medium)	C (low)	C (low)
Mail Server	C: it might contain sensitive communications such as ICS alerts, process status updates, vendor details. I: attackers may alter email content or sender addresses. A: the availability of the mail server is important for security operations including warnings and emergency response coordination.	C (low)	C (low)	C (low)
User Workstations with Access to Machinery	C: at least some critical data such as user access credentials have to be protected against unauthorized access. I: software and production-relevant data (such as configuration files, BOM, SBOM) shall not be manipulated. A: ensure operators can access the workstations to avoid delays in production or maintenance tasks.	A (high)	B (medium)	B (medium)
Managed switch	I: attackers can modify VLAN configurations, reroute traffic, or disable security policies to allow unauthorized access. A: if the switch is unavailable, communication between ICS devices may fail, causing process disruptions.	B (medium)	C (low)	C (low)
Firewall	C: If the firewall is misconfigured or compromised, attackers may gain unauthorized access to confidential internal systems and data. I: Manipulation of firewall rules can lead to unauthorized traffic flows, allowing malicious activity or blocking legitimate communication. A: A failure or targeted attack on the firewall can disrupt network availability, resulting in downtime of business-critical services.	A (high)	B (medium)	C (low)

3 Cybersecurity objectives: Confidentiality, Integrity, Availability. Only relevant objectives are described.

Asset	Relevant cybersecurity objectives[3]	Impact [IEC 62443-3-2 ZCR 5.3]		
		Operational	Financial	HSE
Directory Services (Active Directory)	C: unauthorized access to Active Directory can expose sensitive information such as user identities, group memberships, and authentication data. I: if attackers manipulate directory data, they can escalate privileges, alter access rights, or create persistence in the environment. A: an unavailable directory service can prevent user authentication and disrupt access to essential systems and applications across the organization.	A (high)	B (medium)	C (low)
Update Server	C: if compromised, an update server could leak sensitive configuration or system information to unauthorized parties. I: manipulated updates may deliver malicious code or unauthorized changes to connected systems, compromising their integrity. A: if the update server is unavailable, critical patches or software updates may be delayed, increasing exposure to vulnerabilities.	C (low)	C (low)	C (low)
	IDMZ			
Manufacturing Execution Systems (MES)	C: relevant for protecting sensitive business data. I: production data, such as schedules, workflow instructions, and quality control data, shall not be manipulated. A: system is relevant for uninterrupted business operations.	B (medium)	C (low)	C (low)
Engineering Workstations	C: at least some critical data such as user access credentials have to be protected against unauthorized access. I: software and production-relevant data shall not be manipulated. A: ensure operators can access the workstations to avoid delays in production or maintenance tasks.	A (high)	B (medium)	B (medium)
Historian	C: relevant for protecting sensitive business data. I: it should not be possible to manipulate data stored. A: these data is production-relevant and therefore shall be available without interruptions.	B (medium)	C (low)	C (low)
Remote Access / Services	C: unauthorized access to credentials could lead to control over critical systems. I: manipulated remote sessions could change system behavior or data. A: downtime of remote access may delay troubleshooting or halt operations.	A (high)	B (medium)	B (medium)

Asset	Relevant cybersecurity objectives[3]	Impact [IEC 62443-3-2 ZCR 5.3]		
		Operational	Financial	HSE
	Industrial Network			
PLC (Machine 1)	C: at least some critical data such as user access credentials have to be protected against unauthorized access. I: these devices are essential for operation and therefore data integrity must be guaranteed. A: uninterrupted availability is essential for operation.	A (high)	B (medium)	B (medium)
HMI (Machine 1)	C: unauthorized physical access to the HMI could lead to unwanted information disclosure to an adversary. I: manipulation of data could lead to wrong operator decisions, system malfunctions, and even safety issues. A: a failure can cause production downtime or dangerous situations, especially for process that are not operated autonomously.	A (high)	B (medium)	B (medium)
Sensors / Actuators (Machine 1)	I: these devices are essential for operation and therefore data integrity must be guaranteed. A: uninterrupted availability is essential for operation.	B (medium)	C (low)	B (medium)
Fieldbus network (Machine 1)	I: it shall be ensured that operational data is accurate and not tampered with. A: uninterrupted availability is essential for operation.	A (high)	B (medium)	C (low)
Communication Module (Machine n)	I: attackers can alter communication parameters, affecting how devices interact and execute commands. A: if unavailable, PLCs, SCADA, and field devices cannot communicate, disrupting process automation.	A (high)	B (medium)	C (low)
Machine controller (Machine n)	I: if the controller logic is altered, machines may operate outside safe parameters, causing physical damage or production failures. A: if a machine controller is disabled or overloaded, production may halt, leading to financial losses.	A (high)	B (medium)	C (low)
Edge device (Machine n)	C: edge devices store and process sensitive ICS data, making them valuable for industrial espionage. I: if an edge device is tampered with, it can send manipulated data to SCADA and control systems, leading to faulty decision-making. A: if an edge device is taken offline, real-time industrial data processing is disrupted, affecting predictive maintenance and anomaly detection.	A (high)	B (medium)	C (low)

3.2 Threat Identification

Threat modeling is a structured process used to identify and assess potential security threats to a system. The mitigation of threats is usually also part of threat modeling. There is no single, universally accepted method for threat modeling. In a generic way, threat modeling is the answer to these four questions [7]:

1. What are we working on?
2. What can go wrong?
3. What are we going to do about it?
4. Did we do a good enough job?

Different approaches and frameworks exist, each with their own strengths and focus areas. Combining multiple methods often provides a more comprehensive understanding of the threat landscape, as different techniques highlight different aspects of security risks.

Detailing the full process of threat modeling would require significant time and space, which is beyond the intended scope of this document. Therefore, we focus only on presenting the results of our threat modeling efforts. Comprehensive resources on threat modeling, such as [8], are readily available for readers seeking further guidance.

Our approach involves structured brainstorming, supported by the STRIDE [9] methodology and relevant threat catalogs. STRIDE (which stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) is a widely used model for identifying security threats based on potential attack types. However, STRIDE relies heavily on the experience of the analyst performing the assessment, which increases the risk of overlooking certain threats. To reduce this risk and enhance completeness, it is beneficial to combine STRIDE with a framework or catalog, such as the MITRE ATT&CK® framework for ICS. Therefore, we supplemented our analysis with techniques from the MITRE ATT&CK® [10] framework[4] for ICS and Enterprise systems. For the purposes of this document, we identified and prioritized the most critical threats associated with each asset. A Combination of threat assessment frameworks and threat catalogues is always possible, if done in a structured manner.

3.3 Who is the Attacker?

Operational technology systems face a wide range of threat actors, each with distinct capabilities and motivations. It is important that the thread source is well understood to implement adequate measures. While it can be hard to keep track of the current threat landscape and the thread groups either disappearing, reformatting under different name or newly evolving. The following image shows an overview of threat actor archetypes that can help to model the risk posed by these archetypes instead of a concrete threat group that is currently operating. A detailed taxonomy of these threat actors can be found in the NIST SP 800-82 [6] and ENISA Threat Landscape 2014 [11]. We shortly describe relevant threat sources from these taxonomies.

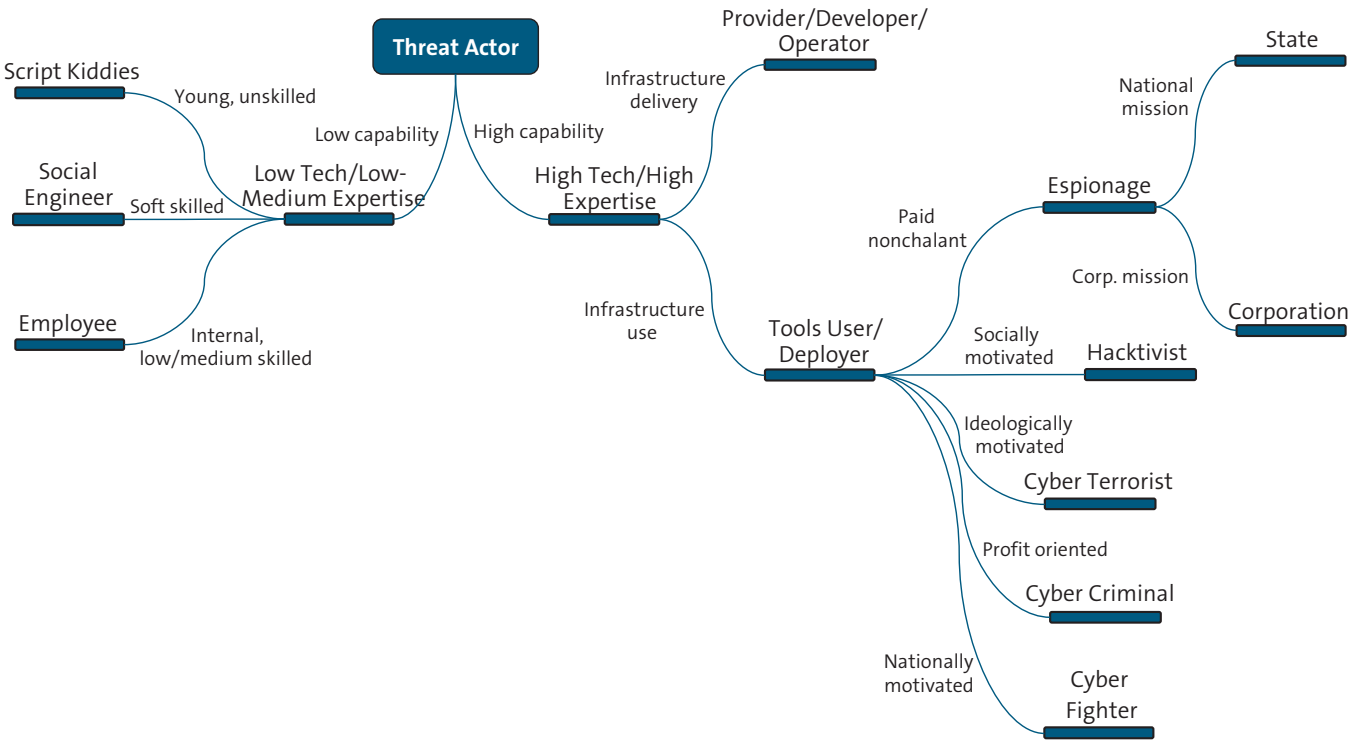
Script Kiddies:

Script Kiddies are typically young, inexperienced users who use pre-made hacking tools to perform cyber-attacks, often seeking recognition or thrill. Despite limited skills, they can cause unintended damage due to poor judgment and overconfidence.

4 The MITRE ATT&CK® framework contains a database of techniques that describe, in principle, how threats are executed. They are not threat scenarios themselves. However, for the sake of simplicity, we use them to directly describe threat scenarios.

Figure 3:

Hostile Threat Actor



Social Engineers:

These actors exploit social engineering techniques to manipulate or deceive individuals, often without relying on sophisticated technology. Their primary resources include profiling, data breaches, and social media to steal identities, credentials, and personal data.

Employees (Insiders):

Insiders, including current or former staff and contractors, pose threats through both intentional acts (e.g., sabotage) and unintentional mistakes (e.g., human error). Their access to internal systems makes them especially dangerous, contributing significantly to data breaches and outages. An example was the Tesla insider sabotage attempt (2020) [14], where an employee was offered $1 million to introduce malware into the company's network.

Nation States / Advanced Persistent Threats:

Nation-state actors conduct cyber espionage and intelligence operations, targeting sensitive governmental, military, and corporate data to gain strategic advantages. Equipped with vast resources and advanced capabilities, these actors pose a severe and often covert threat.

Adversarial threats, such as bot network operators, pose significant risks by launching large-scale DDoS attacks against industrial control systems, as seen in the 2015 Ukrainian power grid attack [11], where the BlackEnergy malware facilitated widespread outages.

Nation-state actors conduct espionage and cyber warfare, with groups like Sandworm (Russia) being linked to the Industroyer attack (2016) [15] against Ukraine's energy grid, while China-linked Volt Typhoon [16] has infiltrated U.S. critical infrastructure.

Corporations:

Corporations engage in cyber-espionage to steal trade secrets, intellectual property, or sabotage competitors, often mirroring the tactics of nation-states. They may collaborate with states or employ individuals from other threat groups to carry out attacks. Well-funded and knowledgeable, their actions can result in high economic losses for targeted organizations.

Hacktivists:

Hacktivists are politically or ideologically motivated attackers aiming to influence public opinion or decision-making through cyber means like DDoS attacks, defacement, and data leaks. They typically form loosely organized groups and mobilize during politically sensitive events. Their visibility-focused targets and unpredictable alliances make them challenging to profile and defend against. For example, CYBERAV3NGERS [13], an Iran-affiliated group, has targeted Israeli water treatment facilities with disruptive cyberattacks.

Cyber Terrorists:

Terrorist organizations, though historically less active in OT cyber warfare, pose an emerging threat as cyber capabilities become more accessible, with concerns about potential attacks on nuclear facilities or transportation networks.

Cyber terrorists aim to cause large-scale societal disruption or harm national security, often by targeting critical infrastructure. Their hallmark is the indiscriminate use of cyber violence to pursue political or ideological goals.

Cybercriminals:

Cybercriminals pursue financial gain through illegal cyber activities, often operating within highly organized and well-funded networks using advanced tools and infrastructure. Their operations span numerous sectors and include fraud, ransomware, and cybercrime-as-a-service, with specialized roles facilitating the underground market. An example of such attacks was the Colonial Pipeline ransomware attack (2021) [12], which led to fuel shortages across the U.S. due to operational disruptions.

Cyber Fighters:

Cyber fighters are politically or nationally motivated individuals or groups that perform sabotage and publicize attacks to gain attention or promote national interests. They often act in support of governments or ideological causes and exhibit increasing sophistication. Their actions resemble hacktivism but are usually more coordinated and aggressive.

Accidental Threats:

Beyond intentional attacks, accidental threats also present significant risks. Everyday users and operators may inadvertently cause disruptions by misconfiguring industrial control systems or falling victim to phishing campaigns, as seen in the Triton malware attack (2017) [17], where compromised engineering workstations were exploited to attempt sabotage of a Saudi petrochemical plant's safety systems.

Privileged users and administrators, despite their expertise, can introduce security gaps through misconfigurations, such as the 2019 Norsk Hydro ransomware attack [18], where inadequate segmentation allowed the malware to spread across industrial networks.

Structural Threats:

Structural threats stem from inherent system weaknesses, including outdated or unpatched OT assets, supply chain risks, and environmental failures. Legacy systems, common in industrial settings, often lack modern security controls, making them vulnerable to exploits like those leveraged by the EKANS ransomware (2019) [19], which specifically targeted industrial processes.

Supply chain attacks represent another significant challenge, exemplified by the SolarWinds compromise (2019) [20], where adversaries infiltrated thousands of organizations through a trusted software update.

Environmental and infrastructure failures, such as power outages and natural disasters, can also exacerbate cybersecurity risks by disrupting security monitoring systems and leaving industrial sites vulnerable to cyber and physical threats.

3.3.1 Evaluation of Threat Scenarios

The IEC 62443-3-2 standard allows the use of both qualitative and quantitative methods to determine the likelihood of a threat (cf. Section 4.6.5.2 in [4]). However, the standard does not provide in-depth guidance on how to assess likelihood. Instead, it offers a simplified approach in Annex B (see Table B.2 in [4]), which estimates likelihood based on the frequency of occurrence of events.

The relevance of threat scenarios is also highly dependent on the individual company conducting the evaluation. For example, an organization operating in critical infrastructure sectors, such as energy, healthcare, or defense, must consider different threat scenarios than companies with less critical operations.

To enhance the technical rigor of our risk management approach, we decided to assess threat likelihood using the attack potential evaluation methodology from ISO/IEC 18045:2022 [21]. This methodology is widely recognized and has been successfully applied in various risk management frameworks, including TARA in the automotive industry [22]. Each organization must define and justify its own suitable approach.

The evaluation of the attack potential follows the ISO/IEC 18045:2022 (see Section B.6.2 in [21]) and it is based on the factors **elapsed time, specialist expertise, knowledge of the TOE[5], window of opportunity, and equipment required for the exploitation.**

Each factor contributes to an overall score, which reflects the effort required by an attacker to exploit a given vulnerability or execute a specific threat scenario.

The final likelihood is derived by mapping the total attack potential score to qualitative likelihood levels using Table 2, which has been adapted from Table B.3 of ISO/IEC 18045:2022 [21].

5 TOE: Target of Evaluation. TOE, as defined in ISO/IEC 18045 and the Common Criteria, refers to the specific product or system component being assessed for security properties. While conceptually similar to the “System under Consideration” (SUC) in IEC 62443-3-2, the TOE typically focuses on individual components, whereas the SUC encompasses a broader operational context, including network zones, conduits, and industrial processes.

Table 2:

Mapping attack potential to likelihood

Likelihood	Attack potential values
Very high	0–9
High	10–13
Medium	14–19
Low	20–24
Very low	≥ 25

Table 3:

Summary of the most relevant threats for the identified vulnerabilities of the assets

Asset	Threat Description [IEC 62443-3-2 ZCR 5.1]	Unmitigated likelihood based on attack potential [IEC 62443-3-2 ZCR 5.4]					
		Elapsed Time	Specialist Expertise	Knowledge of the TOE	Window of Opportunity	Equipment	Likelihood
Enterprise Network							
File Server	**Threat scenario:** An attacker gains access to the file server and deletes or corrupts critical files (e.g., configuration files, logs, engineering data). **Related MITRE ATT&CK® technique:** Data Destruction (T1485) **Attack vector (CVSS):** Network **STRIDE:** Tampering	≤ 3 months	Proficient	Critical	Difficult	Standard	Very low
	Threat scenario: The file server may expose SMB, RDP, or other network services, which attackers exploit via vulnerabilities. **Related MITRE ATT&CK® technique:** Exploitation of Remote Services (T0866) **Attack vector (CVSS):** Network **STRIDE:** Elevation of privilege	≤ 2 weeks	Expert	Public	Unnecessary / unlimited access	Standard	Very high

Asset	Threat Description [IEC 62443-3-2 ZCR 5.1]	Unmitigated likelihood based on attack potential [IEC 62443-3-2 ZCR 5.4]					
		Elapsed Time	Specialist Expertise	Knowledge of the TOE	Window of Opportunity	Equipment	Likelihood
File Server	**Threat scenario:** Once inside the network, attackers query the file server to discover stored files, user accounts, or mapped drives. Gaining access to configurations, backups, or ICS schematics can help attackers launch targeted attacks against industrial control systems. **Related MITRE ATT&CK® technique:** Loss of Availability (T0826) **Attack vector (CVSS):** Network **STRIDE:** Denial of service	≤ 2 weeks	Expert	Public	Unnecessary / unlimited access	Standard	Very high
	Threat scenario: Once inside the network, attackers deploy ransomware to encrypt data stored on the file server. This renders critical files, backups, or shared directories inaccessible to users and systems. The resulting disruption can halt business operations or production processes, especially if ICS documentation, configuration files, or operational data are affected. In some cases, attackers also demand ransom payments in exchange for decryption keys. **Related MITRE ATT&CK® technique:** Data Encrypted for Impact (T1486) **Attack vector (CVSS):** Network **STRIDE:** Denial of service	≤ 1 day	Expert	Public	Unnecessary / unlimited access	Standard	Very high
Mail Server	**Threat scenario:** Attackers send malicious emails to employees, tricking them into opening weaponized attachments or clicking on phishing links. **Related MITRE ATT&CK® technique:** Phishing (T1566) **Attack vector (CVSS):** Network **STRIDE:** Elevation of privilege	≤ 1 day	Expert	Public	Easy	Standard	Very high
	Threat scenario: If the mail server allows SSH access, attackers may use stolen credentials (from phishing) to log in remotely. **Related MITRE ATT&CK® technique:** Remote Services: SSH (T1021.004) **Attack vector (CVSS):** Network **STRIDE:** Elevation of privilege	≤ 3 months	Expert	Critical	Unnecessary / unlimited access	Standard	Very low

Asset	Threat Description [IEC 62443-3-2 ZCR 5.1]	Unmitigated likelihood based on attack potential [IEC 62443-3-2 ZCR 5.4]					
		Elapsed Time	Specialist Expertise	Knowledge of the TOE	Window of Opportunity	Equipment	Likelihood
Mail Server	**Threat scenario:** Once access is gained, adversaries query the mail server to gather intelligence on email accounts, mail flows, and stored messages. **Related MITRE ATT&CK® technique:** Loss of Availability (T0826) **Attack vector (CVSS):** Network **STRIDE:** Denial of service	≤ 2 weeks	Expert	Public	Unnecessary / unlimited access	Standard	Very high
	Threat scenario: Attackers exploit a vulnerability in a public-facing application of the mail server, such as Outlook Web Access or Exchange Web Services, to gain unauthorized access. Once the vulnerability is exploited, attackers may execute arbitrary code, create new accounts, or move laterally within the network. From there, they can access mailboxes, internal communication, and even escalate privileges to compromise other critical systems in the infrastructure. Related MITRE ATT&CK® technique: Exploit Public-Facing Application (T1190) **Attack vector (CVSS):** Network **STRIDE:** Elevation of privilege / Spoofing / Information disclosure	≤ 3 months	Expert	Public	Unnecessary / unlimited access	Standard	Medium
User Workstations with Access to Machinery	**Threat scenario:** Attackers alter or forge reporting messages sent from the workstation to engineers, operators, or SCADA systems. **Related MITRE ATT&CK® technique:** Spearphishing Attachment (T0865) **Attack vector (CVSS):** Network **STRIDE:** Tampering	≤ 1 month	Expert	Public	Moderate	Standard	Medium
	Threat scenario: The attacker tricks a user (e.g., an ICS engineer) into opening a malicious file, script, or application. **Related MITRE ATT&CK® technique:** User Execution (T1204) **Attack vector (CVSS):** Network **STRIDE:** Elevation of privilege	≤ 3 months	Expert	Public	Difficult	Standard	Very low

Asset	Threat Description [IEC 62443-3-2 ZCR 5.1]	Unmitigated likelihood based on attack potential [IEC 62443-3-2 ZCR 5.4]					
		Elapsed Time	Specialist Expertise	Knowledge of the TOE	Window of Opportunity	Equipment	Likelihood
User Workstations with Access to Machinery	**Threat scenario:** If the attacker gains access to the workstation, they may use PowerShell, Python, or Bash scripts to run malicious payloads, modify configuration files to weaken security Settings, or disable monitoring tools to evade detection. **Related MITRE ATT&CK® technique:** Command and Scripting Interpreter (T1059) **Attack vector (CVSS):** Network **STRIDE:** Elevation of privilege	≤ 3 months	Expert	Restricted	Unnecessary / unlimited access	Standard	Medium
	Threat scenario: Attackers establish access to ICS workstations or servers by abusing remote services such as RDP, VNC, or SSH. Through these remote connections, they can interact directly with critical systems, modify configurations, or transfer malicious tools into the environment. This remote access not only enables lateral movement across the ICS network but also provides a platform for launching targeted attacks, potentially impacting availability, integrity, or safety of industrial processes. **Related MITRE ATT&CK® technique:** Remote Services (T1021) **Attack vector (CVSS):** Network **STRIDE:** Elevation of Privilege / Denial of service	≤ 1 month	Expert	Public	Moderate	Standard	Medium
Managed switch	**Threat scenario:** Attackers intercept or block network commands sent to/from the switch, disrupting control signals between SCADA systems, PLCs, or field devices. **Related MITRE ATT&CK® technique:** Default Credentials (T0812) **Attack vector (CVSS):** Network **STRIDE:** Elevation of privilege	≤ 1 month	Expert	Public	Moderate	Standard	Medium
	Threat scenario: If the switch allows remote SSH access, attackers can use stolen credentials or exploit weak authentication to gain control. **Related MITRE ATT&CK® technique:** Remote Services: SSH (T1021.004) **Attack vector (CVSS):** Network **STRIDE:** Elevation of privilege	≤ 3 months	Expert	Critical	Unnecessary / unlimited access	Standard	Very low

Asset	Threat Description [IEC 62443-3-2 ZCR 5.1]	Unmitigated likelihood based on attack potential [IEC 62443-3-2 ZCR 5.4]					
		Elapsed Time	Specialist Expertise	Knowledge of the TOE	Window of Opportunity	Equipment	Likelihood
Managed switch	**Threat scenario:** If the attacker gains access to the workstation, they may use PowerShell, Python, or Bash scripts to run malicious payloads, modify configuration files to weaken security Settings, or disable monitoring tools to evade detection. **Related MITRE ATT&CK® technique:** Command and Scripting Interpreter (T1059) **Attack vector (CVSS):** Network **STRIDE:** Elevation of privilege	≤ 3 months	Expert	Restricted	Unnecessary / unlimited access	Standard	Medium
	Threat scenario: By compromising a managed switch or exploiting network protocols, attackers position themselves between communicating devices using techniques such as ARP spoofing or MAC flooding. This enables them to intercept, manipulate, or block communication between critical ICS components. Sensitive data such as credentials, control commands, or configuration files can be captured or altered, potentially leading to system disruptions or enabling further targeted attacks on industrial processes. **Related MITRE ATT&CK® technique:** Man-in-the-Middle (T1557) **Attack vector (CVSS):** Network **STRIDE:** Information Disclosure / Tampering / Denial of service	≤ 3 months	Expert	Public	Moderate	Standard	Low
Firewall	**Threat scenario:** if adversaries got access to the firewall and exploit an unknown (zero-day) vulnerability in the firewall software to gain unauthorized access or execute malicious code. **Related MITRE ATT&CK® technique:** Exploit Public-Facing Application (T1190) **Attack vector (CVSS):** Network **STRIDE:** Elevation of Privilege	≤ 3 months	Expert	Critical	Unnecessary / unlimited access	Standard	Medium
	Threat scenario: Adversaries has access to the firewall and perform brute-force attacks against the firewall's management interface to gain administrative access. **Related MITRE ATT&CK® technique:** Brute Force (T1110) **Attack vector (CVSS):** Network **STRIDE:** Elevation of Privilege	≤ 1 month	Expert	Restricted	Moderate	Standard	Medium

Asset	Threat Description [IEC 62443-3-2 ZCR 5.1]	Unmitigated likelihood based on attack potential [IEC 62443-3-2 ZCR 5.4]					
		Elapsed Time	Specialist Expertise	Knowledge of the TOE	Window of Opportunity	Equipment	Likelihood
Firewall	**Threat scenario:** Adversaries got access to the firewall and upload and execute web shells on the web interfaces to maintain access and perform malicious actions. **Related MITRE ATT&CK® technique:** Server Software Component: Web Shell (T1505.003) **Attack vector (CVSS):** Network **STRIDE:** Elevation of Privilege, Tampering	≤ 3 months	Expert	Restricted	Moderate	Standard	Low
Directory Services (Active Directory)	**Threat scenario:** Adversaries got access to the internal network and performs SQL injection through a vulnerable web application to exfiltrate, modify, or delete backend database data. **Related MITRE ATT&CK® technique:** Input Capture: SQL Injection (T1505.001) **Attack vector (CVSS):** Network **STRIDE:** Information Disclosure, Tampering	≤ 1 week	Expert	Restricted	Moderate	Standard	Medium
	Threat scenario: Adversaries got access to the internal network and exploit misconfigurations in directory services to escalate privileges or bypass access controls. **Related MITRE ATT&CK® technique:** Abuse Elevation Control Mechanism (T1548) **Attack vector (CVSS):** Local **STRIDE:** Elevation of Privilege, Tampering	≤ 1 week	Expert	Restricted	Moderate	Standard	Medium
	Threat scenario: Adversaries got access to the internal network and extract sensitive information (e.g., users, groups, trusts) from Active Directory for further attacks or lateral movement. **Related MITRE ATT&CK® technique:** Account Discovery (T1087) **Attack vector (CVSS):** Local **STRIDE:** Information Disclosure	≤ 1 week	Expert	Restricted	Moderate	Standard	Medium
Update Server	**Threat scenario:** Adversaries got access to the internal network and spoof or redirect update requests to deliver rogue updates from a malicious server. **Related MITRE ATT&CK® technique:** Software Deployment Tools (T1072) **Attack vector (CVSS):** Network **STRIDE:** Spoofing, Tampering	≤ 3 months	Expert	Restricted	Moderate	Standard	Low

Asset	Threat Description [IEC 62443-3-2 ZCR 5.1]	Unmitigated likelihood based on attack potential [IEC 62443-3-2 ZCR 5.4]					
		Elapsed Time	Specialist Expertise	Knowledge of the TOE	Window of Opportunity	Equipment	Likelihood
Update Server	**Threat scenario:** Adversaries got access to the internal network and compromise the update server to distribute malicious software during routine update processes. **Related MITRE ATT&CK® technique:** Supply Chain Compromise (T1195) **Attack vector (CVSS):** Network **STRIDE:** Tampering	≤ 3 months	Expert	Restricted	Moderate	Standard	Low
	Threat scenario: Adversaries got access to the internal network and exploit vulnerabilities or misconfigurations in the update server to gain unauthorized access or control. **Related MITRE ATT&CK® technique:** Exploit Public-Facing Application (T1190) **Attack vector (CVSS):** Network **STRIDE:** Elevation of Privilege	≤ 1 week	Expert	Restricted	Moderate	Standard	Medium
	IDMZ						
Manufacturing Execution System (MES)	**Threat scenario:** Attackers compromise the MES, causing operators to lose visibility and control over manufacturing processes. **Related MITRE ATT&CK® technique:** Loss of Control (T0827) **Attack vector (CVSS):** Network **STRIDE:** Denial of service	≤ 2 months	Proficient	Restricted	Unnecessary / unlimited access	Standard	High
	Threat scenario: Once inside the MES, attackers use it as a pivot point to deploy malicious tools to other ICS assets (e.g., SCADA, PLCs, Historians). **Related MITRE ATT&CK® technique:** Lateral Tool Transfer (T0867) **Attack vector (CVSS):** Network **STRIDE:** Elevation of privilege	≤ 1 month	Expert	Restricted	Difficult	Standard	Low
	Threat scenario: Attackers alter what operators see in the MES dashboard, tricking them into believing processes are running normally when they are actually compromised. **Related MITRE ATT&CK® technique:** Manipulation of View (T0832) **Attack vector (CVSS):** Network **STRIDE:** Tampering	≤ 2 months	Expert	Restricted	Unnecessary / unlimited access	Standard	Medium

Asset	Threat Description [IEC 62443-3-2 ZCR 5.1]	Unmitigated likelihood based on attack potential [IEC 62443-3-2 ZCR 5.4]					
		Elapsed Time	Specialist Expertise	Knowledge of the TOE	Window of Opportunity	Equipment	Likelihood
Manufacturing Execution System (MES)	**Threat scenario:** By targeting the MES, attackers manipulate or disable automated response functions such as alarms, alerts, or escalation procedures. As a result, critical production anomalies, quality deviations, or system faults may go unnoticed or unresolved. This can lead to undetected process failures, production defects, or safety risks, especially in highly automated environments, and ultimately supports broader attacks on industrial operations. **Related MITRE ATT&CK® technique:** Alarm Suppression (T0878) **Attack vector (CVSS):** Network **STRIDE:** Denial of service / Tampering	≤ 2 months	Expert	Restricted	Unnecessary / unlimited access	Standard	Medium
Engineering Workstations	**Threat scenario:** Attackers alter or forge reporting messages sent from the workstation to engineers, operators, or SCADA systems. **Related MITRE ATT&CK® technique:** Spearphishing Attachment (T0865) **Attack vector (CVSS):** Network **STRIDE:** Tampering	≤ 1 month	Expert	Public	Moderate	Standard	Medium
	Threat scenario: Adversaries exploit vulnerabilities in RDP, SSH, or proprietary industrial protocols to take control of the system. **Related MITRE ATT&CK® technique:** Remote Services (T0886) **Attack vector (CVSS):** Network **STRIDE:** Elevation of privilege	≤ 2 months	Expert	Public	Moderate	Standard	Medium
	Threat scenario: Engineers may unknowingly run malware through weaponized engineering software or phishing. **Related MITRE ATT&CK® technique:** User Execution (T1204) **Attack vector (CVSS):** Network **STRIDE:** Elevation of privilege	≤ 3 months	Expert	Public	Difficult	Standard	Very low

Asset	Threat Description [IEC 62443-3-2 ZCR 5.1]	Unmitigated likelihood based on attack potential [IEC 62443-3-2 ZCR 5.4]					
		Elapsed Time	Specialist Expertise	Knowledge of the TOE	Window of Opportunity	Equipment	Likelihood
Engineering Workstations	**Threat scenario:** Attackers target the engineering workstation to disrupt its availability, either by deploying ransomware, deleting critical configuration files, or overloading system resources. As a result, operators and engineers lose access to essential tools for configuring, maintaining, or troubleshooting control systems. This can delay incident response, prevent deployment of control logic updates, and significantly impact production continuity or system safety. **Related MITRE ATT&CK® technique:** Loss of Availability (T0826) **Attack vector (CVSS):** Network **STRIDE:** Denial of service	≤ 2 weeks	Expert	Public	Unnecessary / unlimited access	Standard	Very high
Historian	**Threat scenario:** Attackers target historians to exfiltrate sensitive process data, logs, and trends for industrial espionage or reconnaissance. **Related MITRE ATT&CK® technique:** Theft of Operational Information (T0882) **Attack vector (CVSS):** Adjacent **STRIDE:** Information disclosure	≤ 2 weeks	Proficient	Restricted	Easy	Standard	Very high
	Threat scenario: Attackers passively monitor network traffic to and from the Historian, capturing sensitive industrial data. **Related MITRE ATT&CK® technique:** Network Sniffing (T0842) **Attack vector (CVSS):** Adjacent **STRIDE:** Information disclosure	≤ 2 weeks	Proficient	Restricted	Unnecessary / unlimited access	Standard	Very high
	Threat scenario: Attackers use stolen, weak, or default credentials to gain unauthorized access to the Historian. **Related MITRE ATT&CK® technique:** Valid Accounts (T1078) **Attack vector (CVSS):** Adjacent **STRIDE:** Elevation of privilege	≤ 1 day	Proficient	Restricted	Unnecessary / unlimited access	Standard	Very high
Remote Access / Services	**Threat scenario:** Adversaries gain unauthorized access to systems by exploiting exposed or weakly secured remote access services (e.g., RDP, VPN). **Related MITRE ATT&CK® technique:** Remote Services (T1021) **Attack vector (CVSS):** Network **STRIDE:** Elevation of Privilege	≤ 1 weeks	Proficient	Public	Unnecessary / unlimited access	Standard	Very high

Asset	Threat Description [IEC 62443-3-2 ZCR 5.1]	Unmitigated likelihood based on attack potential [IEC 62443-3-2 ZCR 5.4]					
		Elapsed Time	Specialist Expertise	Knowledge of the TOE	Window of Opportunity	Equipment	Likelihood
Remote Access / Services	**Threat scenario:** Adversaries use stolen or brute-forced credentials to log in via legitimate remote access services. **Related MITRE ATT&CK® technique:** Valid Accounts (T1078) **Attack vector (CVSS):** Network **STRIDE:** Repudiation, Elevation of Privilege	≤ 1 day	Proficient	Public	Unnecessary / unlimited access	Standard	Very high
	Threat scenario: Adversaries deploy remote access tools (RATs) to maintain persistent access to compromised systems. **Related MITRE ATT&CK® technique:** Remote Access Software (T1219) **Attack vector (CVSS):** Network **STRIDE:** Spoofing, Tampering	≤ 1 month	Expert	Public	Unnecessary / unlimited access	Standard	High
	Industrial Network						
PLC (Machine 1)	**Threat scenario:** Attackers exploit hard-coded, vendor-supplied, or unchanged default credentials to gain unauthorized access to the PLC. **Related MITRE ATT&CK® technique:** Default Credentials (T0812) **Attack vector (CVSS):** Local **STRIDE:** Elevation of privilege	≤ 1 month	Expert	Public	Moderate	Standard	Medium
	Threat scenario: Attackers launch a DoS attack on the PLC, causing it to crash, freeze, or reboot continuously. Common attack methods include sending malformed packets that exploit protocol vulnerabilities (e.g., Modbus, PROFINET), flooding the PLC with excessive traffic to overwhelm processing capabilities, and exploiting firmware vulnerabilities to cause repeated failures. **Related MITRE ATT&CK® technique:** Denial of Service (T0814) **Attack vector (CVSS):** Adjacent **STRIDE:** Denial of service	≤ 2 weeks	Proficient	Restricted	Unnecessary / unlimited access	Standard	Very high
	Threat scenario: Once inside the PLC, attackers alter its logic or programming, leading to dangerous process manipulation. **Related MITRE ATT&CK® technique:** Modify Program (T0889) **Attack vector (CVSS):** Adjacent **STRIDE:** Tampering	≤ 1 week	Expert	Restricted	Unnecessary / unlimited access	Standard	High

Asset	Threat Description [IEC 62443-3-2 ZCR 5.1]	Unmitigated likelihood based on attack potential [IEC 62443-3-2 ZCR 5.4]					
		Elapsed Time	Specialist Expertise	Knowledge of the TOE	Window of Opportunity	Equipment	Likelihood
HMI (Machine 1)	**Threat scenario:** Adversaries perform unauthorized observation or data collection through the HMI to understand processes and prepare follow-up attacks. **Related MITRE ATT&CK® technique:** Monitor Process State (T0801) **Attack vector (CVSS):** Local **STRIDE:** Information Disclosure	≤ 1 week	Expert	Restricted	Moderate	Standard	Medium
	Threat scenario: Adversaries exploit vulnerabilities in HMI software to execute code or escalate privileges within the control environment. **Related MITRE ATT&CK® technique:** Exploit Public-Facing Application (T1190) **Attack vector (CVSS):** Network **STRIDE:** Elevation of Privilege	≤ 3 months	Expert	Restricted	Moderate	Standard	Low
	Threat scenario: Adversaries gain access to the HMI to manipulate control settings, disrupt operations, or cause physical damage. **Related MITRE ATT&CK® technique:** Unauthorized Command Message (T0855) **Attack vector (CVSS):** Network **STRIDE:** Tampering, Denial of Service	≤ 3 months	Expert	Restricted	Moderate	Standard	Medium
Sensors / Actuators (Machine 1)	**Threat scenario:** Attackers can alter sensor readings or actuator responses to disrupt processes. **Related MITRE ATT&CK® technique:** Graphical User Interface (T0823) **Attack vector (CVSS):** Local **STRIDE:** Tampering	≤ 2 weeks	Proficient	Public	Moderate	Standard	Very high
	Threat scenario: Fake or altered sensor data can be sent to mislead operators and automation systems. **Related MITRE ATT&CK® technique:** Spearphishing Attachment (T0865) **Attack vector (CVSS):** Network **STRIDE:** Tampering	≤ 1 month	Expert	Public	Moderate	Standard	Medium
	Threat scenario: Attackers may corrupt sensor firmware or delete calibration data, causing failures. **Related MITRE ATT&CK® technique:** Commonly Used Port (T0885) **Attack vector (CVSS):** Network **STRIDE:** Tampering	≤ 2 weeks	Expert	Restricted	Moderate	Standard	Medium

Asset	Threat Description [IEC 62443-3-2 ZCR 5.1]	Unmitigated likelihood based on attack potential [IEC 62443-3-2 ZCR 5.4]					
		Elapsed Time	Specialist Expertise	Knowledge of the TOE	Window of Opportunity	Equipment	Likelihood
Fieldbus network (Machine 1)	**Threat scenario:** Adversaries send rogue commands to manipulate actuators or control processes. **Related MITRE ATT&CK® technique:** Unauthorized Command Message (T0855) **Attack vector (CVSS):** Adjacent **STRIDE:** Tampering	≤ 2 weeks	Expert	Restricted	Moderate	Standard	Medium
	Threat scenario: Attackers disrupt Fieldbus network communications, preventing devices from receiving control signals. **Related MITRE ATT&CK® technique:** Denial of Control (T0813) **Attack vector (CVSS):** Adjacent **STRIDE:** Denial of service	≤ 1 week	Layman	Restricted	Moderate	Standard	Very high
	Threat scenario: Attackers position themselves between industrial devices by hijacking the Fieldbus network, allowing them to intercept, alter, or block data packets. **Related MITRE ATT&CK® technique:** Adversary-in-the-Middle (T0830) **Attack vector (CVSS):** Adjacent **STRIDE:** Tampering	≤ 1 week	Proficient	Restricted	Moderate	Standard	High
Communication Module (Machine n)	**Threat scenario:** Attackers exploit remote management interfaces (e.g., SSH, Telnet, VNC, proprietary ICS protocols) to gain unauthorized access to the communication module. **Related MITRE ATT&CK® technique:** Exploitation of Remote Services (T0866) **Attack vector (CVSS):** Network **STRIDE:** Elevation of privilege	≤ 2 weeks	Expert	Public	Unnecessary / unlimited access	Standard	Very high
	Threat scenario: Attackers overload, crash, or disrupt the communication module to prevent industrial devices from exchanging data. **Related MITRE ATT&CK® technique:** Denial of Control (T0813) **Attack vector (CVSS):** Network **STRIDE:** Denial of service	≤ 1 week	Layman	Restricted	Moderate	Standard	Very high

Asset	Threat Description [IEC 62443-3-2 ZCR 5.1]	Unmitigated likelihood based on attack potential [IEC 62443-3-2 ZCR 5.4]					
		Elapsed Time	Specialist Expertise	Knowledge of the TOE	Window of Opportunity	Equipment	Likelihood
Communication Module (Machine n)	**Threat scenario:** Attackers position themselves between industrial devices by hijacking the communication module, allowing them to intercept, alter, or block data packets. **Related MITRE ATT&CK® technique:** Adversary-in-the-Middle (T0830) **Attack vector (CVSS):** Adjacent **STRIDE:** Tampering	≤ 1 week	Proficient	Restricted	Moderate	Standard	High
Machine controller (Machine n)	**Threat scenario:** Attackers use vendor-supplied or unchanged default credentials to gain access to the machine controller. **Related MITRE ATT&CK® technique:** Default Credentials (T0812) **Attack vector (CVSS):** Adjacent **STRIDE:** Elevation of privilege	≤ 1 month	Expert	Public	Moderate	Standard	Medium
	Threat scenario: Attackers modify the machine controller's logic to alter or disrupt industrial processes. **Related MITRE ATT&CK® technique:** Modify Program (T0889) **Attack vector (CVSS):** Adjacent **STRIDE:** Tampering	≤ 1 week	Expert	Restricted	Unnecessary / unlimited access	Standard	High
	Threat scenario: Attackers launch a DoS attack on the machine controller, preventing it from functioning. **Related MITRE ATT&CK® technique:** Denial of Service (T0814) **Attack vector (CVSS):** Adjacent **STRIDE:** Denial of service	≤ 2 weeks	Proficient	Restricted	Unnecessary / unlimited access	Standard	Very high
Edge device (Machine n)	**Threat scenario:** Attackers exploit exposed remote access services (e.g., SSH, RDP, VPN, HTTP APIs) on the edge device to gain control. **Related MITRE ATT&CK® technique:** Exploitation of Remote Services (T0866) **Attack vector (CVSS):** Network **STRIDE:** Elevation of privilege	≤ 2 weeks	Expert	Public	Unnecessary / unlimited access	Standard	Very high
	Threat scenario: Attackers overload or crash the edge device, disrupting industrial communications. **Related MITRE ATT&CK® technique:** Denial of Service (T0814) **Attack vector (CVSS):** Network **STRIDE:** Denial of service	≤ 2 weeks	Proficient	Restricted	Unnecessary / unlimited access	Standard	Very high

Asset	Threat Description [IEC 62443-3-2 ZCR 5.1]	Unmitigated likelihood based on attack potential [IEC 62443-3-2 ZCR 5.4]					
		Elapsed Time	Specialist Expertise	Knowledge of the TOE	Window of Opportunity	Equipment	Likelihood
Edge device (Machine n)	**Threat scenario:** Attackers use the edge device to map the ICS network, identifying high-value targets. **Related MITRE ATT&CK® technique:** Internet Accessible Device (T0883) **Attack vector (CVSS):** Network **STRIDE:** Information disclosure	≤ 1 week	Layman	Public	Unnecessary / unlimited access	Standard	Very high

3.5 Risk Evaluation and Risk Treatment

In this section, we evaluate and mitigate risks by following a structured risk management process. First, we determine the unmitigated risk by assessing the likelihood and impact of each identified threat in the absence of security controls. Next, we propose risk treatment measures, which consist of technical and organizational controls aimed at reducing the likelihood and/or impact of the threat. Finally, we calculate the residual risk, reflecting the level of risk that remains after the implementation of these controls.

To systematically calculate the unmitigated risk, we rely on a risk matrix (Table 4), which has been adapted from Table B.1 of the IEC 62443-3-2 [4] standard. This matrix provides a visual representation of risk levels based on the combination of two key factors:

- **Impact (A, B, C):** This refers to the severity of the consequences if the threat were to occur. Impact is categorized as A (high), B (medium), or C (low), and is derived from the criticality of the asset and the potential consequences (e.g., operational disruption, financial loss, HSE).

  Important: For the sake of simplicity and to save space, we have chosen to solely calculate the risk based on the maximum impact value across the three categories operational, financial, and HSE. Organizations are free to extend the analysis to consider each category individually if desired. By focusing on the highest impact value, the security team can still trace back to the original asset impact assessment to understand which category was critical and make informed decisions, e.g., a high financial impact might be acceptable through risk sharing, whereas the same level of impact in operational or HSE terms may require mitigation.

- **Likelihood:** This denotes the probability or frequency of the threat scenario occurring, and is rated as Very Low, Low, Medium, or High.

Since the IEC 62443 standard does not mandate a specific risk evaluation method, each company must define its own tailored approach, considering its operational context, **risk appetite** (i.e., the level of risk it is willing to accept in pursuit of its objectives), and applicable **safety requirements.** The structure and thresholds of the risk matrix should reflect not only the organization's tolerance for business disruption or financial loss but also its obligations in terms of functional and process safety, particularly in environments where cybersecurity incidents could pose risks to human life or critical operations.

By cross-referencing the impact category of the asset with the estimated likelihood of the threat scenario, we can determine the unmitigated risk value using the color-coded matrix in Table 4. This matrix yields qualitative risk levels ranging from Low to High, which are then used to prioritize mitigation efforts.

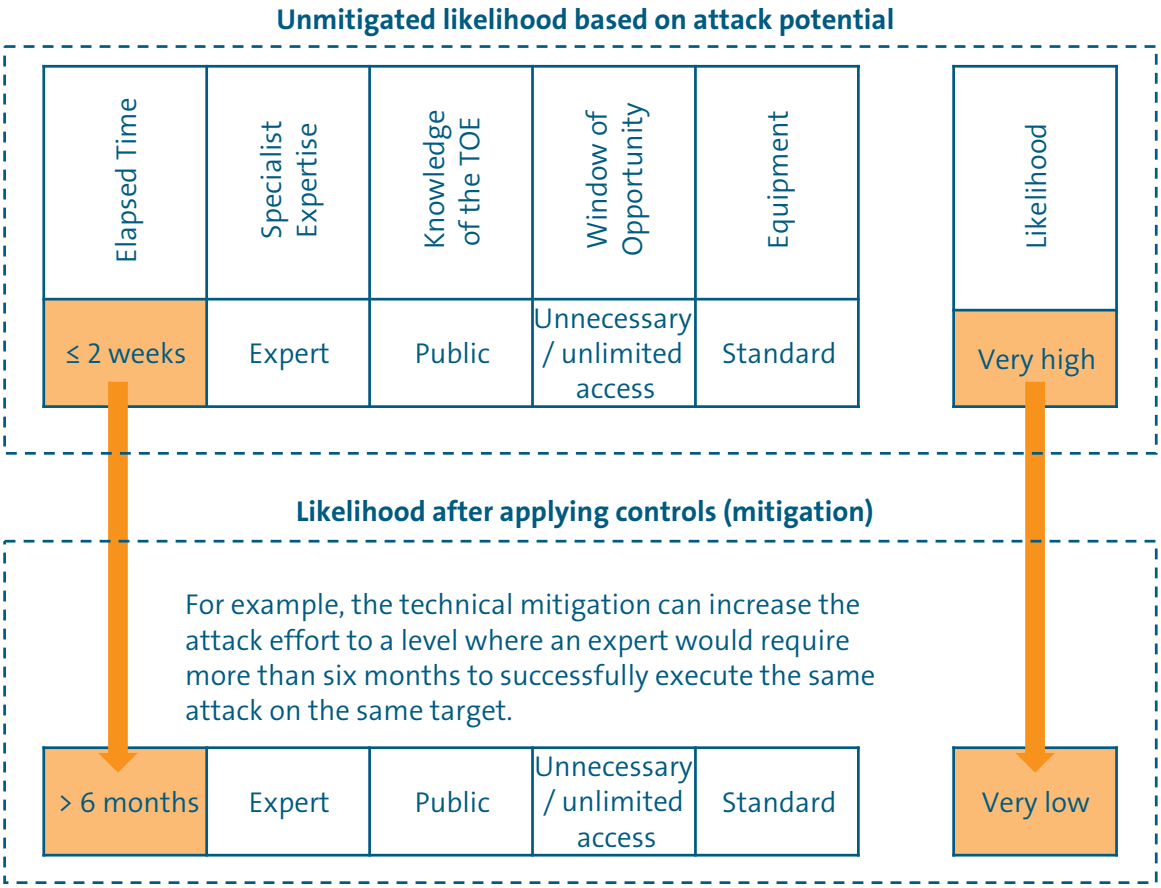
For example, if a threat has a medium likelihood and affects an asset with high impact (A), the unmitigated risk is categorized as Med-high. This categorization guides the selection of suitable controls and the evaluation of residual risk once those controls are applied.

Figure 4 shows how the likelihood of a successful attack can change after applying technical mitigation measures. In the upper part, the unmitigated likelihood is assessed based on various attacker capabilities and conditions leading to a **Very high** likelihood when no controls are in place. The lower part shows the same scenario after mitigation, where improvements (e.g., increasing the required attack time to over six months) significantly reduce the likelihood to **Very low.**

Note: While the example focuses on increased elapsed time, a realistic mitigation scenario may also impact other factors such as window of

Figure 4:

Representation of how the new likelihood is calculated



opportunity, required knowledge, or available equipment. A comprehensive assessment should consider the overall change in attack feasibility.

In a real-world risk assessment project, this process (evaluating the impact of controls on each likelihood factor) must be repeated for every identified risk that is intended to be mitigated. Each risk requires a detailed before-and-after analysis to determine how specific controls affect the attack potential and resulting likelihood. To maintain readability and conserve space, this document does not include all intermediate steps for each risk. Instead, we present only the final, mitigated risk ratings in Table 5, where the impact of the applied countermeasures is already reflected in the updated risk levels.

3.5.1 Source of Controls and Assignment Criteria

To ensure consistency throughout our risk management and mitigation approach, we base the selection and assignment of controls on the same framework used for threat modeling: the MITRE ATT&CK® framework. This decision maintains a coherent methodology across all phases of the analysis and ensures that identified threats are addressed using a recognized and structured set of defensive measures.

For assigning controls, we defined the following criteria based on the assessed risk level:

- **Low Risk:** No countermeasures are assigned. The residual risk is considered acceptable without the need for additional mitigating actions.
- **Medium-Low and Medium Risk:** A reduced package of countermeasures derived from the MITRE ATT&CK® framework is assigned. The reduced package focuses on essential controls that provide a reasonable level of protection without introducing excessive cost or complexity.
- **Medium-High and High Risk:** A full package of countermeasures from the MITRE ATT&CK® framework is assigned. In these cases, a comprehensive set of mitigations is necessary to sufficiently reduce the risk to an acceptable level.

Table 4:

Risk matrix (cf. Table B.1 in [4])

		Impact		
		A (high)	B (medium)	C (low)
Likelihood	Very high	High	High	Med-high
	High	High	Med-high	Medium
	Medium	Med-high	Medium	Med-low
	Low	Medium	Med-low	Low
	Very low	Med-low	Low	Low

Table 5:

Summary of the risk value for each asset and threat scenario, including the recommended controls and residual risk obtained

Asset	Impact (Combined maximum impact value from Table 1)	Threat Description [IEC 62443-3-2 ZCR 5.1]	Likelihood	Risk Value (Unmitigated risk) [IEC 62443-3-2 ZCR 5.5]	Recommended Controls [IEC 62443-3-2 ZCR 5.8]	Residual risk [IEC 62443-3-2 ZCR 5.10]
Enterprise Network						
File Server	B (medium)	**Threat scenario:** An attacker gains access to the file server and deletes or corrupts critical files (e.g., configuration files, logs, engineering data).	Very low	Low	No control needed	Low
		Threat scenario: The file server may expose SMB, RDP, or other network services, which attackers exploit via vulnerabilities.	Very high	High	Application Isolation and Sandboxing (M0948) Disable or Remove Feature or Program (M0942) Exploit Protection (M0950) Network Segmentation (M0930) Privileged Account Management (M0926) Threat Intelligence Program (M0919) Update Software (M0951) Vulnerability Scanning (M0916)	Low
		Threat scenario: Once inside the network, attackers query the file server to discover stored files, user accounts, or mapped drives. Gaining access to configurations, backups, or ICS schematics can help attackers launch targeted attacks against industrial control systems.	Very high	High	Data Backup (M0953) Out-of-Band Communications Channel (M0810) Redundancy of Service (M0811)	Low

Asset	Impact (Combined maximum impact value from Table 1)	Threat Description [IEC 62443-3-2 ZCR 5.1]	Likelihood	Risk Value (Unmitigated risk) [IEC 62443-3-2 ZCR 5.5]	Recommended Controls [IEC 62443-3-2 ZCR 5.8]	Residual risk [IEC 62443-3-2 ZCR 5.10]
File Server		**Threat scenario:** Once inside the network, attackers deploy ransomware to encrypt data stored on the file server. This renders critical files, backups, or shared directories inaccessible to users and systems. The resulting disruption can halt business operations or production processes, especially if ICS documentation, configuration files, or operational data are affected. In some cases, attackers also demand ransom payments in exchange for decryption keys.	Very high	High	Behavior Prevention on Endpoint (M1040) Data Backup (M1053)	Low
Mail Server	C (low)	**Threat scenario:** Attackers send malicious emails to employees, tricking them into opening weaponized attachments or clicking on phishing links.	Very high	Med-high	Antivirus/Antimalware (M1049) Audit (M1047) Network Intrusion Prevention (M1031) Restrict Web-Based Content (M1021) Software Configuration (M1054) User Training (M1017)	Low
		Threat scenario: If the mail server allows SSH access, attackers may use stolen credentials (from phishing) to log in remotely.	Very low	Low	No control needed	Low
		Threat scenario: Once access is gained, adversaries query the mail server to gather intelligence on email accounts, mail flows, and stored messages.	Very high	Med-high	Data Backup (M0953) Out-of-Band Communications Channel (M0810) Redundancy of Service (M0811)	Low

Asset	Impact (Combined maximum impact value from Table 1)	Threat Description [IEC 62443-3-2 ZCR 5.1]	Likelihood	Risk Value (Unmitigated risk) [IEC 62443-3-2 ZCR 5.5]	Recommended Controls [IEC 62443-3-2 ZCR 5.8]	Residual risk [IEC 62443-3-2 ZCR 5.10]
Mail Server		Threat scenario: Attackers exploit a vulnerability in a public-facing application of the mail server, such as Outlook Web Access or Exchange Web Services, to gain unauthorized access. Once the vulnerability is exploited, attackers may execute arbitrary code, create new accounts, or move laterally within the network. From there, they can access mailboxes, internal communication, and even escalate privileges to compromise other critical systems in the infrastructure.	Medium	Med-low	Limit Access to Resource Over Network (M1035) Network Segmentation (M1030) Privileged Account Management (M1026) Update Software (M1051)	Low
User Workstations with Access to Machinery	A (high)	**Threat scenario:** Attackers alter or forge reporting messages sent from the workstation to engineers, operators, or SCADA systems.	Medium	Med-high	Antivirus/Antimalware (M0949) Network Intrusion Prevention (M0931) Restrict Web-Based Content (M0921) User Training (M0917)	Med-low
		Threat scenario: The attacker tricks a user (e.g., an ICS engineer) into opening a malicious file, script, or application.	Very low	Med-low	Execution Prevention (M1038) User Training (M1017)	Med-low
		Threat scenario: If the attacker gains access to the workstation, they may use PowerShell, Python, or Bash scripts to run malicious payloads, modify configuration files to weaken security Settings, or disable monitoring tools to evade detection.	Medium	Med-high	Antivirus/Antimalware (M1049) Audit (M1047) Behavior Prevention on Endpoint (M1040) Code Signing (M1045) Disable or Remove Feature or Program (M1042) Execution Prevention (M1038) Limit Software Installation (M1033) Privileged Account Management (M1026) Restrict Web-Based Content (M1021)	Med-low

Asset	Impact (Combined maximum impact value from Table 1)	Threat Description [IEC 62443-3-2 ZCR 5.1]	Likelihood	Risk Value (Unmitigated risk) [IEC 62443-3-2 ZCR 5.5]	Recommended Controls [IEC 62443-3-2 ZCR 5.8]	Residual risk [IEC 62443-3-2 ZCR 5.10]
User Workstations with Access to Machinery		**Threat scenario:** Attackers establish access to ICS workstations or servers by abusing remote services such as RDP, VNC, or SSH. Through these remote connections, they can interact directly with critical systems, modify configurations, or transfer malicious tools into the environment. This remote access not only enables lateral movement across the ICS network but also provides a platform for launching targeted attacks, potentially impacting availability, integrity, or safety of industrial processes.	Medium	Med-high	Audit (M1047) Disable or Remove Feature or Program (M1042) Limit Access to Resource Over Network (M1035) Multi-factor Authentication (M1032) Password Policies (M1027) User Account Management (M1018)	Med-low
Managed switch	B (medium)	**Threat scenario:** Attackers intercept or block network commands sent to/from the switch, disrupting control signals between SCADA systems, PLCs, or field devices.	Medium	Medium	Access Management (M0801) Password Policies (M0927)	Low
		Threat scenario: If the switch allows remote SSH access, attackers can use stolen credentials or exploit weak authentication to gain control.	Very low	Low	No control needed	Low
		Threat scenario: If the attacker gains access to the workstation, they may use PowerShell, Python, or Bash scripts to run malicious payloads, modify configuration files to weaken security Settings, or disable monitoring tools to evade detection.	Medium	Medium	Antivirus/Antimalware (M1049) Behavior Prevention on Endpoint (M1040) Execution Prevention (M1038) Limit Software Installation (M1033) Privileged Account Management (M1026)	Low

Asset	Impact (Combined maximum impact value from Table 1)	Threat Description [IEC 62443-3-2 ZCR 5.1]	Likelihood	Risk Value (Unmitigated risk) [IEC 62443-3-2 ZCR 5.5]	Recommended Controls [IEC 62443-3-2 ZCR 5.8]	Residual risk [IEC 62443-3-2 ZCR 5.10]
Managed switch		**Threat scenario:** By compromising a managed switch or exploiting network protocols, attackers position themselves between communicating devices using techniques such as ARP spoofing or MAC flooding. This enables them to intercept, manipulate, or block communication between critical ICS components. Sensitive data such as credentials, control commands, or configuration files can be captured or altered, potentially leading to system disruptions or enabling further targeted attacks on industrial processes.	Low	Med-low	Encrypt Sensitive Information (M1041) Filter Network Traffic (M1037) Limit Access to Resource Over Network (M1035) Network Segmentation (M1030)	Low
Firewall	A (high)	**Threat scenario:** if adversaries got access to the firewall and exploit an unknown (zero-day) vulnerability in the firewall software to gain unauthorized access or execute malicious code.	Medium	Med-high	Application Isolation and Sandboxing (M1048) Exploit Protection (M1050) Limit Access to Resource Over Network (M1035) Network Segmentation (M1030) Privileged Account Management (M1026) Update Software (M1051) Vulnerability Scanning (M1016)	Med-low
		Threat scenario: Adversaries has access to the firewall and perform brute-force attacks against the firewall's management interface to gain administrative access.	Medium	Med-high	Account Use Policies (M1036) Multi-factor Authentication (M1032) Password Policies (M1027) User Account Management (M1018)	Med-low
		Threat scenario: Adversaries got access to the firewall and upload and execute web shells on the web interfaces to maintain access and perform malicious actions.	Low	Medium	Disable or Remove Feature or Program (M1042) User Account Management (M1018)	Med-low

Asset	Impact (Combined maximum impact value from Table 1)	Threat Description [IEC 62443-3-2 ZCR 5.1]	Likelihood	Risk Value (Unmitigated risk) [IEC 62443-3-2 ZCR 5.5]	Recommended Controls [IEC 62443-3-2 ZCR 5.8]	Residual risk [IEC 62443-3-2 ZCR 5.10]
Directory Services (Active Directory)	A (high)	**Threat scenario:** Adversaries perform SQL injection through a vulnerable web application to exfiltrate, modify, or delete backend database data.	Medium	Med-high	Audit (M1047) Code Signing (M1045) Privileged Account Management (M1026)	Med-low
		Threat scenario: Adversaries got access to the internal network and exploit misconfigurations in directory services to escalate privileges or bypass access controls.	Medium	Med-high	Audit (M1047) Execution Prevention (M1038) Operating System Configuration (M1028) Privileged Account Management (M1026) Restrict File and Directory Permissions (M1022) Update Software (M1051) User Account Control (M1052) User Account Management (M1018)	Med-low
		Threat scenario: Adversaries got access to the internal network and extract sensitive information (e.g., users, groups, trusts) from Active Directory for further attacks or lateral movement.	Medium	Med-high	Operating System Configuration (M1028) User Account Management (M1018)	Med-low
Update Server	C (low)	**Threat scenario:** Adversaries got access to the internal network and spoof or redirect update requests to deliver rogue updates from a malicious server.	Low	Low	No control needed	Low
		Threat scenario: Adversaries got access to the internal network and compromise the update server to distribute malicious software during routine update processes.	Low	Low	No control needed	Low

Asset	Impact (Combined maximum impact value from Table 1)	Threat Description [IEC 62443-3-2 ZCR 5.1]	Likelihood	Risk Value (Unmitigated risk) [IEC 62443-3-2 ZCR 5.5]	Recommended Controls [IEC 62443-3-2 ZCR 5.8]	Residual risk [IEC 62443-3-2 ZCR 5.10]
Update Server		**Threat scenario:** Adversaries got access to the internal network and exploit vulnerabilities or misconfigurations in the update server to gain unauthorized access or control.	Medium	Med-low	Application Isolation and Sandboxing (M1048) Exploit Protection (M1050) Privileged Account Management (M1026)	Low
			IDMZ			
Manufacturing Execution System (MES)	B (medium)	**Threat scenario:** Attackers compromise the MES, causing operators to lose visibility and control over manufacturing processes.	High	Med-high	Data Backup (M0953) Out-of-Band Communications Channel (M0810) Redundancy of Service (M0811)	Low
		Threat scenario: Once inside the MES, attackers use it as a pivot point to deploy malicious tools to other ICS assets (e.g., SCADA, PLCs, Historians).	Low	Med-low	Network Intrusion Prevention (M0931)	Low
		Threat scenario: Attackers alter what operators see in the MES dashboard, tricking them into believing processes are running normally when they are actually compromised.	Medium	Medium	Communication Authenticity (M0802) Out-of-Band Communications Channel (M0810)	Low
		Threat scenario: By targeting the MES, attackers manipulate or disable automated response functions such as alarms, alerts, or escalation procedures. As a result, critical production anomalies, quality deviations, or system faults may go unnoticed or unresolved. This can lead to undetected process failures, production defects, or safety risks, especially in highly automated environments, and ultimately supports broader attacks on industrial operations.	Medium	Medium	Network Allowlists (M0807) Network Segmentation (M0930)	Low

Asset	Impact (Combined maximum impact value from Table 1)	Threat Description [IEC 62443-3-2 ZCR 5.1]	Likelihood	Risk Value (Unmitigated risk) [IEC 62443-3-2 ZCR 5.5]	Recommended Controls [IEC 62443-3-2 ZCR 5.8]	Residual risk [IEC 62443-3-2 ZCR 5.10]
Engineering Workstations	A (high)	**Threat scenario:** Attackers alter or forge reporting messages sent from the workstation to engineers, operators, or SCADA systems.	Medium	Med-high	Antivirus/Antimalware (M0949) Network Intrusion Prevention (M0931) Restrict Web-Based Content (M0921) User Training (M0917)	Med-low
		Threat scenario: Adversaries exploit vulnerabilities in RDP, SSH, or proprietary industrial protocols to take control of the system.	Medium	Med-high	Access Management (M0801) Authorization Enforcement (M0800) Filter Network Traffic (M0937) Human User Authentication (M0804) Network Allowlists (M0807) Network Segmentation (M0930) Password Policies (M0927) Software Process and Device Authentication (M0813) User Account Management (M0918)	Med-low
		Threat scenario: Engineers may unknowingly run malware through weaponized engineering software or phishing.	Very low	Med-low	Execution Prevention (M1038) User Training (M1017)	Med-low
		Threat scenario: Attackers target the engineering workstation to disrupt its availability, either by deploying ransomware, deleting critical configuration files, or overloading system resources. As a result, operators and engineers lose access to essential tools for configuring, maintaining, or troubleshooting control systems. This can delay incident response, prevent deployment of control logic updates, and significantly impact production continuity or system safety.	Very high	High	Data Backup (M0953) Out-of-Band Communications Channel (M0810) Redundancy of Service (M0811)	Med-low

Asset	Impact (Combined maximum impact value from Table 1)	Threat Description [IEC 62443-3-2 ZCR 5.1]	Likelihood	Risk Value (Unmitigated risk) [IEC 62443-3-2 ZCR 5.5]	Recommended Controls [IEC 62443-3-2 ZCR 5.8]	Residual risk [IEC 62443-3-2 ZCR 5.10]
Historian	B (medium)	**Threat scenario:** Attackers target historians to exfiltrate sensitive process data, logs, and trends for industrial espionage or reconnaissance.	Very high	High	Data Loss Prevention (M0803) Encrypt Sensitive Information (M0941) Operational Information Confidentiality (M0809) Restrict File and Directory Permissions (M0922)	Low
		Threat scenario: Attackers passively monitor network traffic to and from the Historian, capturing sensitive industrial data.	Very high	High	Encrypt Network Traffic (M0808) Multi-factor Authentication (M0932) Network Segmentation (M0930) Privileged Account Management (M0926) Static Network Configuration (M0814)	Low
		Threat scenario: Attackers use stolen, weak, or default credentials to gain unauthorized access to the Historian.	Very high	High	Account Use Policies (M1036) Active Directory Configuration (M1015) Application Developer Guidance (M1013) Multi-factor Authentication (M1032) Password Policies (M1027) Privileged Account Management (M1026) User Account Management (M1018) User Training (M1017)	Low
Remote Access / Services	A (high)	**Threat scenario:** Adversaries gain unauthorized access to systems by exploiting exposed or weakly secured remote access services (e.g., RDP, VPN).	Very high	High	Audit (M1047) Disable or Remove Feature or Program (M1042) Limit Access to Resource Over Network (M1035) Multi-factor Authentication (M1032) Password Policies (M1027) User Account Management (M1018)	Med-low

Asset	Impact (Combined maximum impact value from Table 1)	Threat Description [IEC 62443-3-2 ZCR 5.1]	Likelihood	Risk Value (Unmitigated risk) [IEC 62443-3-2 ZCR 5.5]	Recommended Controls [IEC 62443-3-2 ZCR 5.8]	Residual risk [IEC 62443-3-2 ZCR 5.10]
Remote Access / Services		**Threat scenario:** Adversaries use stolen or brute-forced credentials to log in via legitimate remote access services.	Very high	High	Account Use Policies (M1036) Active Directory Configuration (M1015) Application Developer Guidance (M1013) Multi-factor Authentication (M1032) Password Policies (M1027) Privileged Account Management (M1026) User Account Management (M1018) User Training (M1017)	Med-low
		Threat scenario: Adversaries deploy remote access tools (RATs) to maintain persistent access to compromised systems.	High	High	Disable or Remove Feature or Program (M1042) Execution Prevention (M1038) Filter Network Traffic (M1037) Limit Hardware Installation (M1034) Network Intrusion Prevention (M1031)	Med-low
		Industrial Network				
PLC (Machine 1)	A (high)	**Threat scenario:** Attackers exploit hardcoded, vendor-supplied, or unchanged default credentials to gain unauthorized access to the PLC.	Medium	Med-high	Access Management (M0801) Password Policies (M0927)	Med-low
		Threat scenario: Attackers launch a DoS attack on the PLC, causing it to crash, freeze, or reboot continuously. Common attack methods include sending malformed packets that exploit protocol vulnerabilities (e.g., Modbus, PROFINET), flooding the PLC with excessive traffic to overwhelm processing capabilities, and exploiting firmware vulnerabilities to cause repeated failures.	Very high	High	Watchdog Timers (M0815)	Med-low

Asset	Impact (Combined maximum impact value from Table 1)	Threat Description [IEC 62443-3-2 ZCR 5.1]	Likelihood	Risk Value (Unmitigated risk) [IEC 62443-3-2 ZCR 5.5]	Recommended Controls [IEC 62443-3-2 ZCR 5.8]	Residual risk [IEC 62443-3-2 ZCR 5.10]
PLC (Machine 1)		**Threat scenario:** Once inside the PLC, attackers alter its logic or programming, leading to dangerous process manipulation.	High	High	Audit (M0947) Authorization Enforcement (M0800) Code Signing (M0945) Human User Authentication (M0804)	Med-low
HMI (Machine 1)	A (high)	**Threat scenario:** Adversaries perform unauthorized observation or data collection through the HMI to understand processes and prepare follow-up attacks	Medium	Med-high	Mitigation Limited or Not Effective (M0816): This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.	Med-high
		Threat scenario: Adversaries exploit vulnerabilities in HMI software to execute code or escalate privileges within the control environment.	Low	High	Application Isolation and Sandboxing (M1048) Exploit Protection (M1050) Privileged Account Management (M1026)	Med-low
		Threat scenario: Adversaries gain access to the HMI to manipulate control settings, disrupt operations, or cause physical damage.	Medium	High	Filter Network Traffic (M0937) Network Allowlists (M0807) Network Segmentation (M0930)	Med-low
Sensors / Actuators (Machine 1)	B (medium)	**Threat scenario:** Attackers can alter sensor readings or actuator responses to disrupt processes.	Very high	High	Mitigation Limited or Not Effective (M0816): This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.	High
		Threat scenario: Fake or altered sensor data can be sent to mislead operators and automation systems.	Medium	Medium	Network Intrusion Prevention (M0931) Restrict Web-Based Content (M0921)	Low
		Threat scenario: Attackers may corrupt sensor firmware or delete calibration data, causing failures.	Medium	Medium	Network Intrusion Prevention (M0931) Network Segmentation (M0930)	Low

Asset	Impact (Combined maximum impact value from Table 1)	Threat Description [IEC 62443-3-2 ZCR 5.1]	Likelihood	Risk Value (Unmitigated risk) [IEC 62443-3-2 ZCR 5.5]	Recommended Controls [IEC 62443-3-2 ZCR 5.8]	Residual risk [IEC 62443-3-2 ZCR 5.10]
Fieldbus network (Machine 1)	A (high)	**Threat scenario:** Adversaries send rogue commands to manipulate actuators or control processes.	Medium	Med-high	Communication Authenticity (M0802) Filter Network Traffic (M0937) Network Allowlists (M0807) Network Segmentation (M0930) Software Process and Device Authentication (M0813) Validate Program Inputs (M0818)	Med-low
		Threat scenario: Attackers disrupt Fieldbus network communications, preventing devices from receiving control signals.	Very high	High	Data Backup (M0953) Out-of-Band Communications Channel (M0810) Redundancy of Service (M0811)	Med-low
		Threat scenario: Attackers position themselves between industrial devices by hijacking the Fieldbus network, allowing them to intercept, alter, or block data packets.	High	High	Audit (M0947) Communication Authenticity (M0802) Disable or Remove Feature or Program (M0942) Network Intrusion Prevention (M0931) Network Segmentation (M0930) Out-of-Band Communications Channel (M0810) Software Process and Device Authentication (M0813) Static Network Configuration (M0814)	Med-low
Communication Module (Machine n)	A (high)	**Threat scenario:** Attackers exploit remote management interfaces (e.g., SSH, Telnet, VNC, proprietary ICS protocols) to gain unauthorized access to the communication module.	Very high	High	Application Isolation and Sandboxing (M0948) Disable or Remove Feature or Program (M0942) Exploit Protection (M0950) Network Segmentation (M0930) Privileged Account Management (M0926) Threat Intelligence Program (M0919) Update Software (M0951) Vulnerability Scanning (M0916)	Med-low

Asset	Impact (Combined maximum impact value from Table 1)	Threat Description [IEC 62443-3-2 ZCR 5.1]	Likelihood	Risk Value (Unmitigated risk) [IEC 62443-3-2 ZCR 5.5]	Recommended Controls [IEC 62443-3-2 ZCR 5.8]	Residual risk [IEC 62443-3-2 ZCR 5.10]
Communication Module (Machine n)		**Threat scenario:** Attackers overload, crash, or disrupt the communication module to prevent industrial devices from exchanging data.	Very high	High	Data Backup (M0953) Out-of-Band Communications Channel (M0810) Redundancy of Service (M0811)	Med-low
		Threat scenario: Attackers position themselves between industrial devices by hijacking the communication module, allowing them to intercept, alter, or block data packets.	High	High	Audit (M0947) Communication Authenticity (M0802) Disable or Remove Feature or Program (M0942) Network Intrusion Prevention (M0931) Network Segmentation (M0930) Out-of-Band Communications Channel (M0810) Software Process and Device Authentication (M0813) Static Network Configuration (M0814)	Med-low
Machine controller (Machine n)	A (high)	**Threat scenario:** Attackers use vendor-supplied or unchanged default credentials to gain access to the machine controller.	Medium	Med-high	Access Management (M0801) Password Policies (M0927)	Med-low
		Threat scenario: Attackers modify the machine controller's logic to alter or disrupt industrial processes.	High	High	Audit (M0947) Authorization Enforcement (M0800) Code Signing (M0945) Human User Authentication (M0804)	Med-low
		Threat scenario: Attackers launch a DoS attack on the machine controller, preventing it from functioning.	Very high	High	Watchdog Timers (M0815)	Med-low

Asset	Impact (Combined maximum impact value from Table 1)	Threat Description [IEC 62443-3-2 ZCR 5.1]	Likelihood	Risk Value (Unmitigated risk) [IEC 62443-3-2 ZCR 5.5]	Recommended Controls [IEC 62443-3-2 ZCR 5.8]	Residual risk [IEC 62443-3-2 ZCR 5.10]
Edge device (Machine n)	A (high)	**Threat scenario:** Attackers exploit exposed remote access services (e.g., SSH, RDP, VPN, HTTP APIs) on the edge device to gain control.	Very high	High	Application Isolation and Sandboxing (M0948) Disable or Remove Feature or Program (M0942) Exploit Protection (M0950) Network Segmentation (M0930) Privileged Account Management (M0926) Threat Intelligence Program (M0919) Update Software (M0951) Vulnerability Scanning (M0916)	Med-low
		Threat scenario: Attackers overload or crash the edge device, disrupting industrial communications.	Very high	High	Watchdog Timers (M0815)	Med-low
		Threat scenario: Attackers use the edge device to map the ICS network, identifying high-value targets.	Very high	High	Network Segmentation (M0930)	Med-low

3.5.2 About the Residual Risk

In this type of risk assessment approach, where risk levels are determined using a likelihood-impact matrix, it is possible that some risks remain at a medium or high level even after the application of technical mitigations. This typically occurs when the impact of a potential attack remains high, despite a significant reduction in the likelihood. It is important to note that this is a **limitation of the calculation model** and should not be misinterpreted. In reality, by substantially lowering the likelihood, e.g., by making an attack infeasible within a realistic timeframe, we effectively reduce the probability of the attack occurring in the first place.

In cases where residual risk remains above acceptable thresholds, organizations may also consider alternative risk treatment decisions such as **accepting the risk** (when justified), **sharing or transferring the risk** (e.g., through insurance), **removing the risk** (by changing the design of the TOE, like removing an interface originating the risk) or implementing additional organizational or procedural safeguards.

Furthermore, in certain cases, no direct mitigations are provided by the MITRE ATT&CK® framework. For instance, MITRE classifies some techniques under the category **Mitigation Limited or Not Effective** (M0816), indicating that these techniques exploit inherent system features and cannot be effectively countered through traditional preventive controls. In such situations, the evaluator or security expert must assess the case individually. Alternative measures, such as physical access restrictions, process redesign, or compensating controls, may be considered when justified by the risk context.

For this reason, we say that after the risk analysis is before the risk analysis. A risk assessment is a living document that must be regularly reviewed and updated. It should be repeated whenever there are significant changes to the system design, the threat landscape, or after the discovery of new vulnerabilities. This iterative nature ensures that the security posture remains aligned with evolving risks and system realities.

4. Discussion on Control Selection and Prioritization

This document began with a central question:

If I am a manufacturing company with only basic or unmanaged cybersecurity controls, which measures should I prioritize to achieve the greatest reduction in cyber risk?

The risk assessment results and control mapping provide a clear answer: not all controls offer equal value, especially in the early stages of building an OT security program. Some controls appear repeatedly across threat scenarios and are linked to the mitigation of high or medium-high risks. These controls are the "low-hanging fruit", the most effective starting points for reducing risk with limited resources.

Table 4 provides a consolidated overview of the controls applied to mitigate the risks identified in Table 3. To improve clarity and readability, we have intentionally removed the MITRE ATT&CK® IDs. This is because certain mitigations share the same name but differ in their identifier depending on whether they apply to Enterprise or ICS domains. For the purpose of this discussion, control names alone are sufficient to illustrate the coverage and frequency.

By analyzing the table, we observe that some controls, such as Network Segmentation, Privileged Account Management, and Audit, appear frequently and are associated with a high number of risks, particularly at the High and Medium-High levels. These controls represent high-leverage mitigations that offer broad coverage across multiple threats and should therefore be prioritized in any mitigation strategy.

However, implementing all identified controls at once is often unrealistic. While it may be desirable to apply all listed mitigations, resource constraints, existing system maturity, and operational feasibility often make this impractical in the short term. Therefore, a phased, **maturity-based approach** can be a pragmatic solution.

We do not explain each control in detail due to space constraints and because they are well documented in existing literature. The controls referenced here are based on established sources, such as the MITRE ATT&CK® for ICS framework. However, for the sake of example, we highlight the importance of network segmentation:

Network segmentation: Hardware and network-level segmentation is a fundamental measure to protect control systems in OT environments. By isolating safety-critical systems from less trusted zones, organizations can significantly reduce the risk of cyber incidents affecting production or safety.

Internet connectivity, if needed, should only be permitted during defined maintenance windows and strictly limited to the duration of the task. This ensures minimal exposure and helps prevent unauthorized access or malware propagation.

Hardware separation can be implemented in very practical ways, for example, by physically disconnecting an Ethernet cable when external access is no longer required. Simple measures like these play a crucial role in maintaining the integrity and safety of industrial operations.

4.1 Maturity-based Implementation Plan

To support practical implementation, the identified controls can be grouped and applied in a phased manner. The following three-step strategy proposes a maturity-based rollout, prioritizing controls by their frequency of occurrence and the severity of the risks they mitigate. This approach enables organizations to focus first on high-impact areas while progressively expanding their security posture over time:

- **Step 1 - Foundational Controls:** Focus on the top 10 most frequently occurring controls, which collectively address a large share of High and Med-high risks. This includes, for example, Network Segmentation, Disable or Remove Features or Programs, and Network Intrusion Prevention.
- **Step 2 - Enhanced Coverage:** Extend the control set by implementing the next 20 controls, which continue to reduce residual risks and provide more comprehensive protection across the attack surface.
- **Step 3 - Full Coverage:** Integrate the remaining controls to achieve a mature and well-rounded security posture, particularly in areas with less common but still relevant threats.

Table 6:

Summary of the applied controls

Control	Control occurrences								
	Control Count	Occurrences per risk level					Control Count Percentage	Control Count Cumulative
		High	Med-high	Medium	Med-low	Low		
Network Segmentation	15	7	3	3	2	0	6,85%	6,85%
Privileged Account Management	14	6	4	2	2	0	6,39%	13,24%
Disable or Remove Feature or Program	10	7	2	1	0	0	4,57%	17,81%
Audit	10	5	5	0	0	0	4,57%	22,37%
Network Intrusion Prevention	9	3	3	2	1	0	4,11%	26,48%
Out-of-Band Communications Channel	9	6	2	1	0	0	4,11%	30,59%
User Account Management	9	3	5	1	0	0	4,11%	34,70%
Password Policies	9	3	5	1	0	0	4,11%	38,81%
User Training	7	2	3	0	2	0	3,20%	42,01%
Data Backup	7	5	2	0	0	0	3,20%	45,21%
Update Software	6	3	2	0	1	0	2,74%	47,95%
Application Isolation and Sandboxing	6	3	1	1	1	0	2,74%	50,68%
Exploit Protection	6	3	1	1	1	0	2,74%	53,42%
Redundancy of Service	6	4	2	0	0	0	2,74%	56,16%
Execution Prevention	6	1	2	1	2	0	2,74%	58,90%
Multi-factor Authentication	6	4	2	0	0	0	2,74%	61,64%
Restrict Web-Based Content	5	0	4	1	0	0	2,28%	63,93%
Limit Access to Resource Over Network	5	1	2	0	2	0	2,28%	66,21%
Antivirus/Antimalware	5	0	4	1	0	0	2,28%	68,49%
Filter Network Traffic	5	1	2	1	1	0	2,28%	70,78%
Vulnerability Scanning	4	3	1	0	0	0	1,83%	72,60%
Communication Authenticity	4	2	1	1	0	0	1,83%	74,43%
Software Process and Device Authentication	4	2	2	0	0	0	1,83%	76,26%
Code Signing	4	2	2	0	0	0	1,83%	78,08%
Access Management	4	0	3	1	0	0	1,83%	79,91%
Network Allowlists	4	0	2	2	0	0	1,83%	81,74%
Behavior Prevention on Endpoint	3	1	1	1	0	0	1,37%	83,11%
Static Network Configuration	3	3	0	0	0	0	1,37%	84,47%
Human User Authentication	3	2	1	0	0	0	1,37%	85,84%
Threat Intelligence Program	3	3	0	0	0	0	1,37%	87,21%
Account Use Policies	3	2	1	0	0	0	1,37%	88,58%
Authorization Enforcement	3	2	1	0	0	0	1,37%	89,95%
Watchdog Timers	3	3	0	0	0	0	1,37%	91,32%
Limit Software Installation	2	0	1	1	0	0	0,91%	92,24%
Operation System Configuration	2	0	2	0	0	0	0,91%	93,15%
Active Directory Configuration	2	2	0	0	0	0	0,91%	94,06%
Application Developer Guidance	2	2	0	0	0	0	0,91%	94,98%
Encrypt Sensitive Information	2	1	0	0	1	0	0,91%	95,89%
Restrict File and Directory Permissions	2	1	1	0	0	0	0,91%	96,80%
Validate Program Inputs	1	0	1	0	0	0	0,46%	97,26%
Software Configuration	1	0	1	0	0	0	0,46%	97,72%
User Account Control	1	0	1	0	0	0	0,46%	98,17%
Data Loss Prevention	1	1	0	0	0	0	0,46%	98,63%
Operational Information Confidentiality	1	1	0	0	0	0	0,46%	99,09%
Encrypt Network Traffic	1	1	0	0	0	0	0,46%	99,54%
Limit Hardware Installation	1	1	0	0	0	0	0,46%	100,00%

Disclaimer: This summarizes the controls from this risk assessment and should not be understood as a ranking of generally applicable controls – the controls at the bottom of this list may be as important as the ones at the top! Prioritization of controls should be done individually by the engineer conducting the risk assessment.

5. Epilogue

The VDMA Experts' Circle Security Solutions for Industry concentrates security expertise from various security-focused VDMA-Members. This expertise was poured into this guideline. Many more should follow this first one – the Experts' Circle is just getting started.

The participating companies generated their security expertise by offering services and products related to methods and controls detailed in this document. Therefore, this guideline only contains proven and practical advice. We aim to support the whole machinery and plant building industry with this expertise – feel free to contact the Experts' Circle in case you have any questions about this guideline or specific controls or methods that we advise in this document. We also welcome feedback on this document and constructive suggestions for future revisions.

Especially the smaller plant operators can benefit from the Experts' Circle's output. Usually, when there's limited expertise or resources that can be allocated to security, advice from trade associations like the VDMA or expertise within the VDMA's network can be the deciding advantage when tackling security issues.

OT security is not an option, it is a must. Therefore, it is important to start securing the OT properly. One of the first steps should be to implement and perform such a TARA.

6. References

[1] European Union, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union," 27 12 2022. [Online]. Available: **http://data.europa.eu/eli/dir/2022/2555/oj**.

[2] European Union, "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," 20 11 2024. [Online]. Available: **http://data.europa.eu/eli/reg/2024/2847/oj**.

[3] European Union, "Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC," 29 06 2023. [Online]. Available: **http://data.europa.eu/eli/reg/2023/1230/oj**.

[4] International Electrotechnical Commission, "IEC 62443-3-2:2020 - Security for industrial automation and control systems—Part 3-2: Security risk assessment for system design," 2020. [Online]. Available: **https://webstore.iec.ch/publication/30727**.

[5] N. Pohlmann, Cyber-Sicherheit - Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung, Springer Vieweg Wiesbaden, 2019.

[6] "Threat Modeling Manifesto," [Online]. Available: **https://www.threatmodeling-manifesto.org/**. [Accessed 2025 3 17].

[7] A. Shostack, Threat Modeling: Designing for Security, Wiley, 2014.

[8] L. Kohnfelder and P. Garg, "The threats to our products," Microsoft Interface, Microsoft Corporation, vol. 33, 1999.

[9] The MITRE Corporation, "MITRE ATT&CK®," [Online]. Available: **https://attack.mitre.org/**.

[10] NIST, NIST SP 800-82 Rev. 3, 2022.

[11] ENISA, ENISA Threat Landscape 2014, **https://www.enisa.europa.eu/publications/enisa-threat-landscape-2014**, January 27, 2015.

[12] WIRED, "A Tesla Employee Thwarted an Alleged Ransomware Plot," 27 August 2020. [Online]. Available: **https://www.wired.com/story/tesla-ransomware-insider-hack-attempt/**.

[13] MITRE ATT&CK®, "2015 Ukraine Electric Power Attack," 27 September 2023. [Online]. Available: **https://attack.mitre.org/campaigns/C0028/**.

[14] MITRE ATT&CK®, "Industroyer," 04 Januar 2021. [Online]. Available: **https://attack.mitre.org/software/S0604/**.

[15] MITRE ATT&CK®, "Volt Typhoon," 27 Juli 2023. [Online]. Available: **https://attack.mitre.org/groups/G1017/**.

[16] MITRE ATT&CK®, "CyberAv3ngers," 25 März 2024. [Online]. Available: **https://attack.mitre.org/groups/G1027/**.

[17] CISA, "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years," 07 Mai 2023. [Online]. Available: **https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years**.

[18] MITRE ATT&CK®, “Triton Safety Instrumented System Attack,” 25 März 2024. [Online]. Available: **https://attack.mitre.org/campaigns/C0030/**.

[19] Hydro, “Cyber-attack on Hydro,” 15 Mai 2024. [Online]. Available: **https://www.hydro.com/en/global/media/on-the-agenda/cyber-attack/**.

[20] MITRE ATT&CK®, “EKANS,” 12 Februar 2021. [Online]. Available: **https://attack.mitre.org/software/S0605/**.

[21] MITRE ATT&CK®, “SolarWinds Compromise,” 24 März 2023. [Online]. Available: **https://attack.mitre.org/campaigns/C0024/**.

[22] International Organization for Standardization/International Electrotechnical Commission, “ISO/IEC 18045:2022 - Information technology—Security techniques—Methodology for IT security evaluation,” 2022. [Online]. Available: **https://www.iso.org/standard/72889.html**.

[23] R. do Carmo and A. Schlensog, Automotive Threat Analysis and Risk Assessment in Practice – A practical guide to TARA following the ISO/SAE 21434 standard for automotive embedded and IT/OT systems, Springer, 2024.

7. Literature

VDMA minimum recommendations on Supply Chain Security
Language: German
Price: free

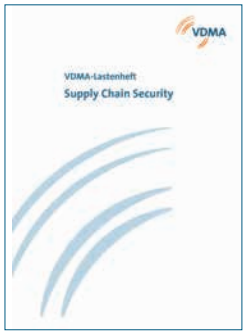
Minimum recommendations for machine and plant manufacturers regarding technical, organizational, and procedural requirements for implementing security for products and processes. Part of the Supply Chain Security document series.

https://www.vdma.org/viewer/-/v2article/render/92030451

VDMA supplier self-disclosure (Excel)
Language: German, English
Price: free

Generally applicable questionnaire for suppliers without specific procurement reference. Reference to machine regulation and Cyber Resilience Act. Developed jointly with the BSI. Part of the Supply Chain Security document series.

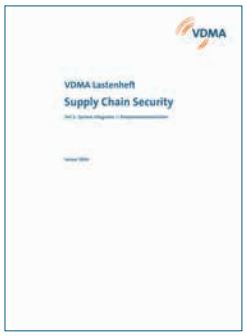
https://www.vdma.org/viewer/-/v2article/render/92030451



VDMA requirement specification "Asset Owner <>Integrator"
Language: German
Price: free

Specification sheet with cybersecurity requirements based on IEC 62443. Target audience: purchasers who want to set generally accepted requirements for the cybersecurity of machines and systems, from design to cyber-secure operation. Part of the Supply Chain Security document series.

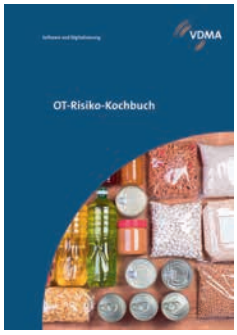
https://www.vdma.org/viewer/-/v2article/render/92030451



VDMA requirement specification "Integrator<>Component Manufacturer"
Language: German, English
Price: free

Specification sheet with cybersecurity requirements based on IEC 62443. The target audience is integrator purchasers who want to set generally accepted security requirements for their component suppliers, from design to cyber-secure operation. Part of the Supply Chain Security document series.

https://www.vdma.org/viewer/-/v2article/render/92030451



VDMA OT-Risk cookbook
Language: German
Price: free

Practical guide to conducting OT risk assessments with a focus on processes and methods. Enables targeted transfer of IT security expertise to the OT environment. Aimed at managers in production and security/IT.

https://www.vdma.org/viewer/-/v2article/render/93887232

VDMA Specification 24774:2023-03
"IT-Security in building automation"
Language: German
Price: free for VDMA-Members

Revised edition from March 2023, which reflects the requirements of the basic protection modules Infrastructure for Technical Building Management (INF.13) and Building Automation (INF.14) of the BSI IT-Grundschutz Compendium.

https://www.vdma.org/viewer/-/v2article/render/55742079

VDMA Publication
"Secure remote maintenance in the machinery and plant building industry"
Language: German
Price: free for VDMA-Members

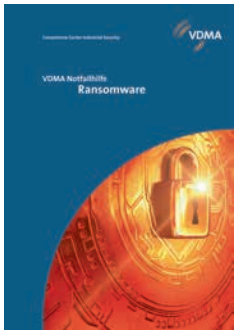
Examples of remote maintenance architectures demonstrate how machine and plant manufacturers can ensure reliable remote service.

https://www.vdma.org/viewer/-/v2article/render/45231112

VDMA Guideline IEC 62443 for machinery and plant builders
Language: German, English
Price: 50 Euro for non-members, free for VDMA-Members

Description of a path through IEC 62443 as an integrator of a machine according to security level 2, including examples according to 62443-3-3.

https://www.vdmashop.de/executive-briefings/informatik-und-technik/482/leitfaden-iec-62443-fuer-den-maschinen-und-anlagenbau?number=&c=23



VDMA emergency help ransomware
Language: German, English
Price: free

Support, recommended actions in the event of a ransomware infection, contact points for authorities and service providers. List of indicators for infection and measures to be taken.

https://www.vdma.org/viewer/-/v2article/render/1295961

VDMA Position
"Cybersecurity: Operator and employer obligations in terms of joint efforts"
Language: German
Price: free

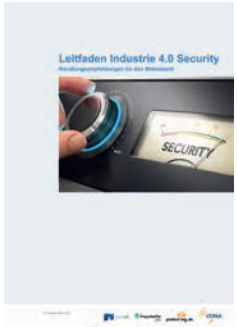
Formulation of the VDMA position on cybersecurity obligations in daily plant operations.

https://vdma.org/viewer/-/v2article/render/4769363

VSMA sample IT-emergency plan
Language: German
Price: free of charge upon request from VSMA

The sample IT emergency plan is designed to help you get back to normal IT operations as quickly as possible after a major disruption to business operations caused by IT infrastructure failure.

https://unternehmen-cybersicherheit.de



VDMA Guideline "Industry 4.0 Security"
Language: German, English
Price: free

83 recommendations for action in 17 areas for the secure and permanently reliable networking of machines and systems.

https://www.vdma.org/viewer/-/v2article/render/1141526

VDMA Questionnaire
“Industrial Security – Just get started.”
Language: German
Price: free for VDMA-Members

Introduction to the selection and evaluation of security measures for production environments. Initial assessment using 33 questions.

Available on request from Biljana Gabric: biljana.gabric@vdma.org

VDMA Guide:
“Information Security, Part 1: Employee Awareness”
Price: Euro 44,00
VDMA-Members: Euro 22,00
ISBN: 978-3-8163-0575-0

https://www.vdmashop.de/executive-briefings/unternehmensfuehrung/132/leitfaden-zur-informationssicherheit/teil-1-sensibilisierung

VDMA Guide
“Information Security, Part 2: ISMS, Documents, and Templates”
Price: Euro 50,00
VDMA-Members: kostenfrei
EAN: 4250697518395

https://www.vdmashop.de/executive-briefings/informatik-und-technik/711/leitfaden-zur-informationssicherheit-teil-2-isms-dokumente-und-vorlagen

VDMA Guideline
“Information Security, Part 3: Electronic exchange of information with external parties and their connection”
Price: Euro 44,00
VDMA-Members: 22,00
ISBN: 978-3-8163-0686-3

https://www.vdmashop.de/executive-briefings/unternehmensfuehrung/138/leitfaden-zur-informationssicherheit/teil-3-elektronischer-informationsaustausch-mit-externen-und

8. Legal notice

We recommend that you regularly review your own procedures to ensure that they comply with the law. The VDMA Legal Department will be happy to provide you with the names of appropriate attorneys.

The findings and recommendations in the present “Component Requirements Specification” and “Component Requirements Specification Guide” documents have been formulated in part on the basis of available drafts. In no case can a claim to completeness and correctness be derived. This document is therefore in no way to be understood as legal advice.

The authors assume no liability for errors and offer no guarantee that the content complies with the applicable legal provisions.

9. About the Authors

The following members from the VDMA Experts' Circle "Security Solutions for Industry" and other external experts were involved in the creation of the table and this application guide.

EC Member	Company
Maximilian Moser	VDMA e. V.
Dr.-Ing. Rodrigo do Carmo Martin Rohnke Alexander Schlensog secunet	**secunet Security Networks AG** secunet - protecting digital infrastructures secunet is Germany's leading cybersecurity company. In an increasingly networked world, the company uses a combination of products and consulting to ensure resilient digital infrastructures and the highest possible level of protection for data, applications and digital identities. secunet specializes in areas where there are special security requirements - such as cloud, IIoT, eGovernment and eHealth. With secunet's security solutions, companies can comply with the highest security standards in digitalization projects and thus drive their digital transformation forward. Over 1,000 experts strengthen the digital sovereignty of governments, companies and society. Its customers include federal ministries, more than 20 DAX-listed companies and other national and international organizations. The company was founded in 1997. It is listed on the German stock exchange and generated sales of 407 million euros in 2024 secunet is an IT security partner of the Federal Republic of Germany and a partner of the Alliance for Cyber Security. www.secunet.com
Ralf King M&M software	**M&M Software GmbH is an international software and digitalization partner.** We accompany companies in the digital transformation of their organizations, products and business models. We identify potential, generate ideas, derive strategies and develop tailor-made software solutions for the digital world. The results of our trusting and cooperative collaboration are digital products or systems that are successful on the market and that we accompany throughout their entire life cycle. We consult and implement at eye level and in close coordination with our customers. In this way, we create new business opportunities and secure competitive advantages. Our global teams work closely with partners in research, academia, and industry.
Sebastian Schneider ONEKEY	**ONEKEY GmbH** ONEKEY is Europe's specialist in automated Product Cybersecurity & Compliance, with expertise in binary firmware analysis, IoT & OT security.

EC Member	Company
Timo Bednarek	**MB connect line GmbH**
	MB connect line is an independent medium-sized company and a pioneer in secure industrial communication via the Internet. Our core competencies include Secure Remote Access, Industrial IoT (IIoT) and Industrial Security. We enable the digital transformation of our customers by connecting machines and systems worldwide and protecting their data from unauthorized access and manipulation. We focus on reliability, innovation and IT-security in everything we do. Our goal: to make industrial digitalization more secure. OUR DNA: 100% IT-SECURITY **www.mbconnectline.com**
Mirco Kloss	**TXOne Networks**
	TXOne Networks is the Leader of OT Zero Trust. TXOne Networks offers cybersecurity solutions that ensure the reliability and safety of ICS and OT environments through the OT zero trust methodology. At TXOne Networks, we work together with both leading manufacturers and critical infrastructure operators to develop practical, operations-friendly approaches to cyber defense. The OT zero trust-based technologies we've developed go beyond the limitations of traditional cyber defense to streamline management, reduce security overhead, and resolve challenges faster. We offer both network- and end-point-based solutions that integrate with the layered arrangements and varied assets common to work sites, providing real-time, defense-in-depth cybersecurity to both mission critical devices and the OT network. **www.txone.com**
Thomas Freund	**Adesso SE**
	Our expertise will be the foundation for digital transformation in Europe. Because we are the company that brings people and technology together like no other business. We stand for digital excellence and offer services and products that enable our customers to grow securely and successfully. Our claim: technologically leading solutions that secure long-term competitive advantages. We measure ourselves by the success of our customers. Despite our passion for technology, the needs and goals of people are at the centre of everything we do. We design systems and applications that create value and open up new perspectives. With a team of more than 10,300 employees on over 60 sites within the adesso Group, we are one of the leading IT service providers in the German-speaking area. We work every day to successfully implement our customers' projects.

Imprint

Imprint

VDMA
Lyoner Str. 18
60528 Frankfurt am Main
Germany
E-Mail: informatik@vdma.org
Internet www.vdma.org

Contact
Maximilian Moser
Competence Center Industrial Security
Phone +49 69 6603-1909
E-Mail maximilian.moser@vdma.org

Status
June 2025

Design
DesignStudio

Production
Druck- und Verlagshaus
Zarbock GmbH & Co. KG
Frankfurt am Main

VDMA
Informatics

Lyoner Str. 18
60528 Frankfurt am Main
Germany

Phone +49 69 6603-0
E-Mail informatik@vdma.org
Internet www.vdma.org

www.vdma.org/cybersecurity

VDMA DesignStudio