UNIVERSITY OF TARTU
Faculty of Science and Technology
Institute of Computer Science

Analysis of Cyber Security Risks and Mitigation Options for Automated Systems and Technologies

Tartu 2024

Kaasrahastanud Euroopa Liit

ECCC

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

Abstract

Automated systems and technologies is a network of interconnected actuators, such as industrial robots and computational devices, forming an integrated web of systems that span design, planning, logistics, manufacturing, warehousing, and sales in the manufacturing sector.

These systems automate functions traditionally performed by humans, enhancing efficiency and productivity across various stages of the manufacturing process. Automated systems and technologies can be of different levels, from entirely manual to fully automated systems. They depend on the vendor's maintenance and trouble-shooting handling policies and may require remote access mechanisms to ensure proper functioning. This complex environment uses data and information that must be confidential, integral, and available for the organisation to stay competitive. With the pressing need for digitisation, increased need for on-demand production, and increasing labour costs, securing these systems is no longer just an option but a critical investment.

However, using automated systems and technology and awareness of their security risks and countermeasures are rather limited. The operational and security aspects are communicated orally without established security policies, and the security aspects get more attention only after security events. The companies need to be made aware of the security standards and regulations. The response to the security events includes the data and system restoration from the local backups.

This report presents the results of the interviews, systematic literature study and survey performed in the organisation using automated systems and technologies. It discusses the context and valuable assets that must be protected against security risks. More specifically, it considers the domain model for security risk management to describe the automated system vulnerabilities, their security threats, and their impact on data and information confidentiality, integrity, and availability. The report also suggests security risk treatment decisions and countermeasures to mitigate the identified risks.

Keywords: Automated systems and technology, protected assets, security risks, STRIDE, security countermeasures, security requirements and control, security standards, ISSRM, and manufacturing organisations.

Contents

List of Figures

List of Tables

1 Introduction

Nowadays, digitization and intelligent infrastructure change human activities and industrial systems. Disruptive technologies, such as cloud computing, blockchain, AI/ML systems, automated systems and technologies and others, have become applicable in various domains of manufacturing. The intensive use of these technologies also generates and manages a lot of data and information, which should be used for the intended purposes, made available when needed, and integral to making correct decisions. It means that security should be treated as the first-level citizen in the digitalized processes and automated systems and technology.

The annual report on Cyber Security in Estonia [17] highlights a surge in security threats and risks, specifically targeting institutions and service sectors. As digitalization continues to be a focus for the business sector, it has become imperative for organizations to enhance their security measures. This involves preparing for potential threats and proactively implementing strategies to mitigate risks, thereby preventing unwanted outcomes in worst-case scenarios.

This report presents an analysis of the context, assets, risks and countermeasures in the automated manufacturing systems. The aim is to gain a preliminary explanation of the information security measures employed by manufacturing entities. Special attention is given to Small and Medium-sized Enterprises (SMEs) that have integrated automation into their production processes to various extents. This focus is driven by the recognition of SMEs as pivotal contributors to the economic fabric [40], yet often under-resourced in terms of advanced security infrastructures.

The report is structured as follows: in Chapter 2, the research approach is explained. The report follows the principles of the domain model for information system security (a.k.a., ISSRM). It is applied to collect data using interviews, systematic literature reviews, and surveys on the security concerns in automated systems and technologies. In Chapter 3 we define the context. here we also discuss a reference architecture model industries 4.0 framework, which highlights key components of the automated system and technology. In Chapter 4 we overview the standards. Chapter 5 presents the assets, Chapter 6 – security risks, and Chapter 7 – security countermeasures to mitigate these risks in automated systems and technology. Chapter 8 and 9 present two use cases – analysis of the insider risks in the manufacturing order processing and analysis of security threats in the manufacturing processes. Chapter 10 highlights some concluding remarks.

2 Research Approach

In this chapter, we define the research questions and discuss the research method applied to collect and analyse the data on the security of automated systems and technology. This work is driven by the information systems security risk management approach, which is a systematic method to define system context and assets, analyse security risks and reason for the countermeasures to mitigate these risks. The data are collected using three empirical research methods:

- interviews with the representatives from the manufacturing organisations,
- systematic literature review,
- survey performed in Estonian manufacturing organisations.

In this chapter, the steps of the research are defined and collected data are presented.

2.1 Security Risk Management

Security engineering is a process of lowering the risk of intentional unauthorized harm to valuable assets to a level that is acceptable to the system's stakeholders by preventing and reacting to malicious harm, misuse, threats, and security risks [14].

This activity includes security risk management tasks. In this work, we will apply the domain model of information systems security risk management (a.k.a. ISSRM domain model, see Fig. 1) [11] [29] consists of three major groups of concepts: asset-related concepts, risk-related concepts, and risk treatment-related concepts. According to the survey results [16], ISSRM was assessed as one of the most proficient concepts that implement ISO/IEC 27001 standard requirements.

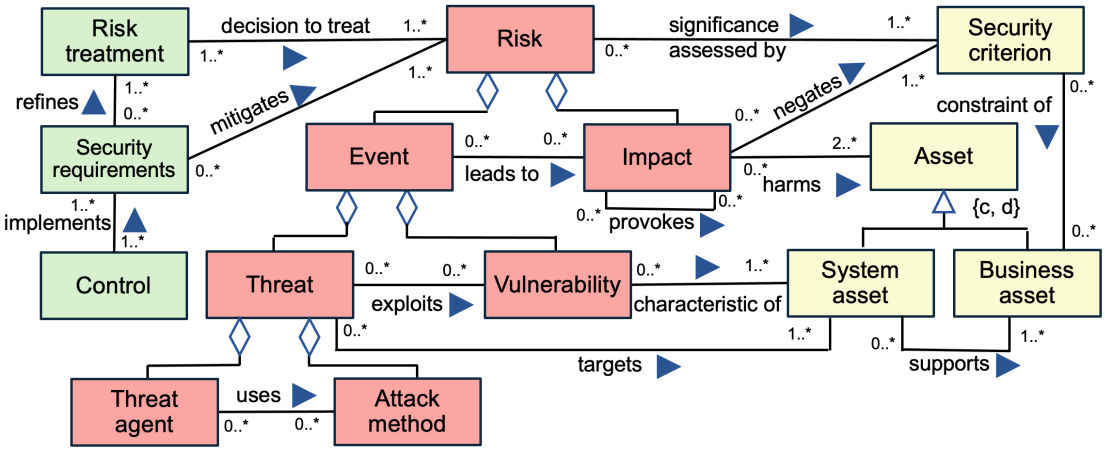

Figure 1. The ISSRM domain model, adapted from [11] [29]

Asset-related concepts describe which of an organisation's assets are important to protect and what criteria guarantee a certain level of asset security [11] [29]. An asset is anything that is

valuable and plays a role in accomplishing the organisation's objectives. Assets can be classified as business assets or organisational assets. A business asset describes the information, processes, capabilities and skills essential to the business and its core mission. Typically, business assets are immaterial.

A **security criterion** (also called security property) characterises a security need and is a property or constraint on business assets. The security objectives are defined using security criteria on business assets. Thus, the security criteria describe the security needs, which are, typically, expressed as confidentiality, integrity and availability of business assets:

- **Confidentiality** describes the property not being made available or disclosed to unauthorised individuals, entities, or processes[11] [29]. It deals with preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **Availability** describes the property of being accessible and usable upon demand by an authorised entity [11] [29]. It means ensuring timely and reliable access to and use of information.
- **Integrity** is the property of guarding the accuracy and completeness of business assets [11] [29]. Accuracy could be threatened by unauthorized or undesirable updates or tampering. Completeness could be threatened by alteration or deletion. In other words, integrity protects against improper information modification or destruction and ensures information's non-repudiation and authenticity.

A **system asset** is a component or part of an information system, valuable to the organisation since it supports business assets. A system asset can be a component of the information technology system (e.g., hardware, software or network), but also a person or a facility that plays a role in the system and, therefore, in its security. The IS assets (except software) are material. System assets are identified as assets that facilitate the functioning of business assets [29]. This encompasses the elements required for transactions, information collection, storage, maintenance, and other functions related to business assets. In [2], information processing functions are derived. These are:

- **Capturing information**, for example using a keyboard, bar code reader, digital camera etc.). Information can be collected in several different ways, depending on the type of information being collected and the device or method used to collect it.
- **Transmitting information**, for example, wired or wireless phones, internet etc. The transmission of information may take place through different means of communication, depending on the type of information being transmitted.
- **Storing information**, for example, hard disk, memory card, databases etc. Information can be stored in many different ways, depending on the type of information being stored and the storage medium or method used.

- **Retrieving information**, for example, from any physical device, data store, etc. This function may request or collect information from any device or system capable of generating or storing data. Retrieval can be done from different types of devices, be it computers, smart devices, machines or other physical devices.
- **Manipulating information** for example, calculations, combinations, statistics, etc. This function may include calculating, combining, using statistical methods and other processing of information. Manipulation of information can be done using software applications, algorithms or other means, depending on the type of manipulation or analysis desired.
- **Displaying information**, for example, monitor, printer, etc. This function allows users or systems to view or access processed or stored information.

All six functions – capturing, transmitting, storing, retrieving, manipulating, and displaying information – are essential to the functioning of the system. These functions contribute to the support of business assets, which may be represented as data, information, or operations and processes.

Risk-related concepts introduce definitions of risk itself and its immediate components [11] [29]. A risk is a combination of a threat with one or more vulnerabilities leading to a negative impact on two or more assets by harming them. The combination of threat and vulnerabilities represents a risk event and impact is the consequence of this risk. An impact is the potential negative consequence of a risk that negates the security criterion defined for business assets and harms these assets when a threat (or an event) is accomplished. The impact can also be described at the level of IS assets (e.g., data destruction, failure of a component, etc.) or at the level of business assets, where it negates security criteria (e.g., loss of information confidentiality, loss of process integrity, loss of data availability). In addition, one impact can provoke a chain reaction of impacts (or indirect impacts), for example, a loss of confidentiality of sensitive information leads to a loss of customer confidence.

A **risk event** is an aggregation of a threat and one or more vulnerabilities. A vulnerability is the characteristic of an IS asset or group of IS assets that exposes a weakness or flaw in terms of security. A threat is an incident initiated by a threat agent using an attack method to target one or more IS assets by exploiting their vulnerabilities. A threat agent is an agent that has the means to intentionally harm IS assets. A threat agent triggers a threat and, thus, is the source of a risk. The threat agent is characterised by expertise, available resources, and motivation. An attack method describes a standard means by which a threat agent executes a threat.

Security risk analysis includes consideration of security threats. In this work, we apply the STRIDE approach [39], which allows the categorisation of identified threats under each part of its mnemonic. The threat taxonomy identifies security threat types within represented elements. STRIDE stands for:

- **Spoofing** – pretending to be something you are not or someone you are not,
- **Tampering** – modifying something that you are not supposed to modify,
- **Repudiation** – claiming you didn't do something (regardless of if this is true or not),

- **Information disclosure** – exposing information to those who are not authorised to view it,
- **Denial of service** – attacks that are designed to prevent a system from providing its intended service,
- **Elevation of privilege** – when a program or user can do things (technically) that they're not supposed to be able to do.

These are designed to help software builders identify software attacks. Each of the aforementioned threat-specific sections provides a deeper explanation of threats including its violated security requirement:

- **Spoofing** - Authentication
- **Tampering** - Integrity
- **Repudiation** - Non-repudiation
- **Information Disclosure** - Confidentiality
- **Denial of Service** - Availability
- **Elevation of privilege** - Authorisation

Risk treatment-related concepts describe the concepts to treat risk [11] [29]. A risk treatment decision is a decision to treat the identified risk. A treatment satisfies a security need, expressed in generic and functional terms and refined to security requirements. There are four categories of risk treatment decisions possible:

- **Risk avoidance** is a decision not to become involved with or to withdraw from a risk. The system's functionality is modified or discarded to avoid the risk;
- **Risk reduction** includes actions to lessen the probability, negative consequence, or both associated with risk. Security requirements are, typically, selected for reducing the risks;
- **Risk transfer** defines how risk parties could share the burden of loss from a risk. A third party is related to the (or part of the) system. This also means that some security requirements could be defined regarding the third party;
- **Risk retention** constitutes acceptance of the burden of loss from a risk. No design decision is necessary in this case.

A security requirement is a condition on the phenomena of the environment that we wish to make true by installing the information system, to mitigate risks [11] [29]. A security requirement is the refinement of a risk treatment decision to mitigate the risks. On the one hand risk reduction decisions lead to security requirements. But sometimes, risk transfer decisions must improve some security requirements on third parties. Avoiding risk and retaining risk do not need any security requirements. On the other hand, each security requirement contributes to covering

one or more risk treatments for the target system. A control (countermeasure or safeguard) is a designed means to improve security by implementing the security requirements. Security controls can be processes, policies, devices, practices or other actions or components of the IS and its organisation that act to reduce risks.

The ISSRM process [11] [29] (see Fig. 2) begins with (a) a study of the organisation's **context and the identification of its assets**. In this step, the organisation, its environment and the system(s) used in this organisation are described. Then, based on the level of protection required for the assets, (b) one needs to **determine the security objectives**. Security objectives are defined in terms of confidentiality, integrity and availability of the business assets. The next step of the process is (c) **risk analysis**, where security risks which harm assets and threaten security objectives are elicited and assessed. Once the risk assessment is finished, (d) **decisions about risk treatment are taken** (e.g., avoiding, reducing, transferring or accepting the risk). The next step (e)) is the **elicitation of security requirements** to mitigate the identified risks. Finally, security requirements are (f) **implemented as security controls**, i.e., system-specific countermeasures that are implemented within the organisation.

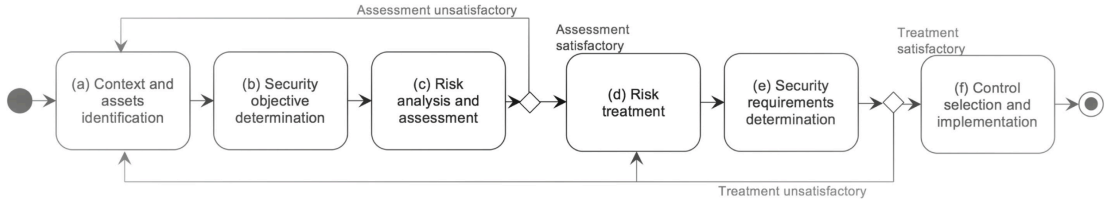

Figure 2. The ISSRM process, adapted from [11] [29]

In this work, we will use the ISSRM approach to define the context, risks, security requirements and countermeasures of the automated system and technology. In the next section, we will consider the research questions and method.

2.2 Research Questions

To guide the analysis of the automated systems and technology, here, we introduce six research questions:

1. What is the context of automated systems and technology?
2. What are the challenges of automated systems and technology
3. What are the protected assets of information systems and technology?
4. What are the security risks to the automated systems and technology?
5. What are security requirements and controls to mitigate risks of the automated systems and technology?
6. What standards should be followed while using automated systems and technology?

To answer these questions, firstly, we conducted interviews with the selected experts from Estonian manufacturing companies. Next, we did a systematic literature analysis. Finally, we executed a survey, where using the the online questionnaire, and we collected data from Estonian manufacturing organisations. All three empirical studies are guided by the application of the ISSRM process and domain model.

2.3 Interviews

The purpose of the interviews was to explore the context of the automated systems and technologies in Estonia and to learn about the current landscape of information security practices within the domain of automated manufacturing. The results of this study were also used as the input to the other two empirical studies (i.e., literature review and survey).

The face-to-face interviews were conducted in the participants' native languages. It allowed the interviewer to establish a comfortable and familiar environment for the interviewee, facilitating a more natural and responsive dialogue that could be dynamically based on the participant's responses.

The primary objective of this survey was to garner an understanding of existing practices. Hence, predefined, structured questions were defined to avoid inadvertently steering the conversation away from organic insights into the practices under scrutiny. Furthermore, conducting interviews orally, as opposed to written questionnaires, was strategically chosen to prevent the interviewees from excessively refining their responses. This measure was intended to ensure authenticity and minimize the potential for the reactions to be artificially tailored or distorted.

To achieve a diversity of insights, the study set a minimum objective of conducting three interviews. Ultimately, a total of five interviews were successfully executed. The focus of these interviews was explicitly directed towards Small and Medium-sized Enterprises (SMEs), as specified in [12]. To clarify and ensure comprehension across diverse linguistic backgrounds, the definition of SMEs was translated into Estonian. The translation was integral to ensuring that the interviewees understood the scope and context of the study.

To ensure consistency across all interviewees, the interviews were unstructured but had predefined themes and sub-questions to guide the discussion. This approach not only preserved the structural integrity of the interviews but also afforded the interviewees the latitude to articulate their experiences and perspectives naturally and spontaneously. Each interview session was recorded using a smartphone, following the acquisition of consent from the participants. This approach facilitated precise data collection, obviating the need for concurrent note-taking and allowing the interviewer to focus entirely on the interviewee. After each interview, the audio recordings were transcribed verbatim. These transcriptions were categorized according to the established thematic framework, ensuring the responses were arranged for the analysis. The analysis of the transcribed data was conducted using thematic analysis techniques. By allocating the responses to their respective thematic categories, recurring patterns were identified.

Table 1 presents the characteristics of the interviewed companies.

Table 1. Interviewed companies

	Number of employees as of 2022	Interviewee role	Part of a larger group
Interviewee 1	101 - 200	CEO	no
Interviewee 2	101 - 200	IT Manager	no
Interviewee 3	201 - 400	IT specialist	yes
Interviewee 4	201 - 400	IT Manager	yes
Interviewee 5	1 - 100	CEO	no

2.3.1 Interview Topics and Questions

- Automated Systems and Machinery Handling
  - What automated systems are used in your manufacturing processes, and how are they secured against unauthorized access or manipulation?
  - Can you describe the procedures for handling and maintaining machinery, including software updates, physical security, and network isolation?
  - How are access rights coordinated within your company, especially regarding remote access or third-party vendors interacting with critical systems?
- General Security Strategy
  - Can you provide an overview of your company's cybersecurity strategy and how it aligns with your business objectives?
  - How do you assess and prioritize the cyber risks specific to the manufacturing sector, and what frameworks are you using for risk management?
  - What regular security assessments or audits are conducted within your organization to ensure compliance with the latest standards and regulations?
- Threat Awareness and Incident Response
  - Have you experienced any cyber threats or security incidents? If so, how were they handled, and what lessons were learned?
  - Can you describe your incident response plan and how it is tailored to address the unique challenges within the manufacturing environment?
  - How do you collaborate with external parties, such as government or industry organizations, for sharing threat intelligence and best practices?
- Data Exchange and Integrity
  - What kind of data is exchanged between the systems within your organization, and how is it encrypted or otherwise protected during transmission?

  - Is there any possibility of data being stolen or manipulated within your system, and what controls are in place to detect and prevent such incidents?
  - How do you ensure data integrity and availability, especially in system failure or targeted attacks?

- Employee Education and Training
  - What continuous training and awareness programs are in place to educate personnel about the latest cyber threats and security measures?
  - How do you ensure that security awareness is integrated into the company culture, especially among non-technical staff who may interact with automated systems?

- Compliance and Legal Awareness
  - Are you aware of any specific legislation, standards, or regulations that apply to your industry regarding cyber security? How do you ensure compliance?
  - What processes are in place for engaging with regulators, law enforcement, or legal counsel in case of a cyber incident, and how are responsibilities delineated within the organisation?
  - How do you balance the need for security with other business considerations, such as operational efficiency, innovation, and customer trust?

- Technology and Innovation
  - How do you stay abreast of emerging technologies and threats in the manufacturing domain, and how do they influence your cyber security strategy?
  - Can you discuss any innovative approaches or technologies you've adapted to enhance security within your manufacturing processes, such as AI, blockchain, or IoT security measures?
  - What are your plans for cyber security investments and developments, especially considering the manufacturing industry's evolving landscape of automation and interconnectivity?

2.4 Literature Review

We performed a systematic literature review based on the guidelines by Kitchenham *et al.* [24]. The review goal is to survey primary literature covering security risks in automated systems and technology. The objectives of the literature review were to explore the context of automated manufacturing systems. We aimed to define the nature and components of automated manufacturing systems, their security needs, systems' security risks, strategies and methods (requirements and controls) employed to mitigate these risks.

Search Process: We used SCOPUS[1] and Web of Science[2] digital libraries. The search queries include "automated manufacturing system, cyber security, cybersecurity". These search queries are connected using Boolean operators tailored to each digital library. Table 2 shows the results of the search results from the sources. We identified 125 results (see Table 2) from which we selected 10 for analysis based on the inclusion/ exclusion criteria (see Table 3).

Table 2. Selected sources and corresponding results for literature review

Sources	SCOPUS	Web of Science	Total
Returned	70	55	125
Filter 1	29	23	52
Filter 2 (Final selection)	6	4	10

Paper Selection: We subjected the identified papers to an initial screening which covered the title, keywords, abstract, results, and conclusion. To select relevant papers, we applied the following two filters based on our research questions:

1. Filter 1: Applying inclusion/exclusion criteria in Table 3 on the selected papers. Table 2 presents the results of applying the inclusion/exclusion criteria resulting in 52 results.
2. Filter 2: Quality assessment of the papers that passed Filter 1 following the Kitchenham quality guidelines [24], with the questions:
    - Does the study cover the scope of work?
    - Does the study describe security risks in automated manufacturing systems?
    - Does the study provide the countermeasures to mitigate security risks?

Table 3. Inclusion/exclusion criteria on the selected papers

Inclusion criteria	Exclusion criteria
Papers in the area of industrial automation.	Papers that focus on security in limited aspects of automated manufacturing systems.
Papers that explicitly carry out security risk assessment or analysis.	Papers that focus on automated manufacturing systems safety features - unintentional harm to stakeholders.
Papers that present security risk solutions.	Non-English papers.
Academic papers that are accessible in full text from the university.	Duplicate works.

[1]https://www.scopus.com/home.uri

[2]https://www-webofscience-com/wos/woscc/basic-search

Selected Papers: Out of the 125 articles initially considered, 115 were excluded based on the filtering criteria. The remaining ten articles were thoroughly examined to address the research questions. Below, we provide an overview of the selected articles, highlighting their respective contexts. Subsequently, we catalogue the standards referenced in each article. Lastly, we offer a consolidated perspective of the specific assets targeted in each article, aligning them with the context of the automated systems and technology.

1. **Khalid et al.** "Understanding vulnerabilities in cyber physical production systems" [23]
   The paper aims to systematically identify risk sources and highlight hazards in cyber-physical production systems (CPPS), focusing on integrating safety and security aspects. It seeks to contribute to developing future Human-Robot Collaboration (HRC) capable of integration in manufacturing systems, particularly in the context of Industry 4.0. The research revolves around a use case in the automobile industry, where a heavy payload robot, a key component of the CPPS, is installed for active HRC. The study explores the CPPS model for this use case, detailing the technology requirements and framework design. The simulation aims to reveal system vulnerabilities, particularly in cyber-attacks leading to safety and failure issues.

   The paper identifies various risks and hazards associated with CPPS, particularly when integrated with heavy payload robots in manufacturing environments. The results highlight the vulnerabilities of these systems to cyber-attacks and their potential impact on safety and operational failure. By utilising the simulation benchmark, the study demonstrates how cyber-attacks can compromise safety and disrupt the functioning of the CPPS. The findings underscore the necessity for robust safety and security integration in CPPS to safeguard against cyber threats and ensure the effective functioning of HRC in industrial settings.

2. **Urooj et al.** "Risk Assessment of SCADA Cyber Attack Methods: A Technical Review on Securing Automated Real-Time SCADA Systems" [41]
   The paper aims to comprehensively review cybersecurity risk assessment methods for Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS). It seeks to identify potential future research areas and available methods focusing on specific aspects of risk assessment in automated SCADA systems. The study reviews the state-of-the-art techniques in cybersecurity risk assessment for SCADA systems, comparing multiple contemporary approaches. It outlines key points of these approaches and analyses them in terms of conventional risk assessment procedures, analytical methods, and research challenges.

   The key risks identified in SCADA systems include network security vulnerabilities, weak cryptographic issues, SCADA system configuration vulnerabilities, and imperfect credential management. The paper emphasises the need for regular security enhancement and updated maintenance to protect against these risks. It suggests that the network architecture of SCADA systems should be carefully designed to ensure remote users have access to information monitoring and analysis as per corporate needs, focusing on the segregation of control systems from external traffic. The paper concludes that

despite numerous risk assessment methodologies for SCADA systems, further research and improvements are needed in areas like credentials encryption, attack/failure awareness, human factors, assessment and verification, and tool support. A comprehensive technique covering all stages of the risk management process is deemed necessary.

3. **Thames et al.** "Distributed, Collaborative and Automated Cybersecurity Infrastructures for Cloud-Based Design and Manufacturing Systems" [27]
   The research aims to enhance cybersecurity in Cloud-Based Design and Manufacturing (CBDM) systems. These systems, integral to modern product development and manufacturing, require robust cybersecurity measures due to their diverse and internet-enabled cyber-physical nature. The study proposes a reference architecture that utilises global cyber information exchange frameworks for dynamic cybersecurity in CBDM systems. The research particularly focuses on global-scale cybersecurity information exchanges, highlighting initiatives like TAXII (Trusted Automated eXchange of Indicator Information) for sharing security event information across organisations.

   The study introduces the Distributed Firewall and Active Response (DFAR) architecture, a cybersecurity reference framework for CBDM systems. DFAR operates within a Trusted Domain of Administration (TDA), where each cyber entity is a producer and consumer of cybersecurity information. This architecture aims to dynamically protect networks by leveraging security event information shared across organisations via TAXII messages. The research showcases how DFAR can offer practical, distributed, collaborative, and automated cybersecurity protection for CBDM systems in conjunction with global cyber exchanges.

4. **Clark et al.** "Cybersecurity Issues in Robotics" [8]
   The paper addresses the overlooked aspect of cybersecurity in robot design and manufacturing. The paper aims to identify current and potential cybersecurity threats to robots at hardware, firmware/OS, and application levels. It discusses economic impacts and human safety concerns related to cyberattacks on robots. Various robot types, including eldercare robots, drones, automated vehicles, and manufacturing robots, are examined for vulnerabilities.

   To counter these threats, the paper suggests various countermeasures targeted at different layers of robot systems. It recommends security processes for hardware attacks in production and validation of suppliers. For firmware/OS, it suggests standardising on a standard operating system and creating a consortium for overseeing platform security. Application-level countermeasures include emphasising secure coding practices and using tools to prevent or detect cyberattacks during application execution.

5. **Kutzler et al.** "Boosting Cyber-Physical System Security" [25]
   The paper examines the challenges and risks associated with the increasing automation in businesses and infrastructure, particularly in the context of cybersecurity. The paper notes that current cybersecurity measures in critical infrastructures, such as network or intrusion detection systems, are inadequate for fully addressing the security needs of these

automated systems. There is a lack of comprehensive tools and approaches for assessing potential threats in designing automated solutions.

The AUTOSEC project developed an advanced Cybersecurity Risk Management Process Model to address these gaps. Based on the NIST Framework for Improving Critical Infrastructure Cybersecurity, this model incorporates core and supporting management functions for cybersecurity risk management. It aims to be user-friendly, compatible with existing standards, and adaptable to various industrial applications. The model also considers the unique characteristics of cyber-physical systems, such as context awareness, dynamic topology, and distributed organizational structure, vital for security.

6. **Quarta et al.** "An Experimental Security Analysis of an Industrial Robot Controller" [35]
This study focuses on the security of industrial robot controllers, which is crucial in automated manufacturing and logistics processes. With these systems' increasing complexity and interconnection, the paper aims to systematically analyse and evaluate their vulnerabilities to cyber-attacks, a relatively unexplored area despite the significant reliance on robots in various sectors. The paper presents a domain-specific attacker model to explore how exploitation of software vulnerabilities in robots can lead to physical consequences. This approach involves examining the standard architecture of industrial robots and identifying potential attack vectors. To assess their impact on robot functionality, the study encompasses various attacks, such as compromising safety measures and impairing movement precision.

   The research highlights the increasing risk of cyber-attacks on industrial robots due to their connectivity for programming, maintenance, and integration into broader ICT ecosystems. The study identifies vulnerabilities that can lead to significant safety and operational disruptions, including weak encryption, inadequate integrity checks, and lack of access control systems. It emphasises the necessity of securing robot networks and communication systems against manipulation and proposes a set of countermeasures to mitigate these risks. The paper concludes that despite existing security measures, further research and improvements are needed in areas like credentials encryption, attack/failure awareness, and human factors in robot programming and control.

7. **Jablonski et al.** "A Case Study in the Formal Modeling of Safe and Secure Manufacturing Automation" [21]
This paper presents a case study applying formal methods to assess safety and security risks in automated manufacturing systems (AMS). The focus is on exploring and evaluating the effectiveness of various methodologies for identifying, prioritising, and mitigating risks associated with AMSs. The study utilises a range of formal methods, including Unified Modeling Language (UML), linear-time propositional temporal logic (LTL), Architecture Analysis and Design Language (AADL), and fault and attack trees. These methods are applied to model and analyse the behaviours and properties of AMSs, providing a foundation for formal verification of end-to-end production facilities. The paper also incorporates an aluminium can AMS case study, dissecting its operations and risk factors.

   The analysis includes a detailed description of the AMS, consisting of 12 interconnected

stations designed for processing materials and producing subcomponents of a final product. The study highlights the complexity of orchestrating logical flows between these stations and the associated safety and security risks. The researchers identified potential safety and security issues within the AMS using formal methods, mainly focusing on the body maker and its subcomponents. The application of AADL enabled the creation of state-based behaviour specifications to define data flows within the system, identify errors, and analyse faults and potential attacks. This comprehensive approach allowed for a structured analysis of system vulnerabilities, offering insights into fault and attack probabilities and their impact on the overall safety and security of the AMS.

8. **Chundhoo et al.** "Cybersecurity Risks in Meat Processing Plant and Impacts on Total Productive Maintenance" [7]
   This study aims to identify cybersecurity threats in the Australian meat manufacturing industry, particularly those affecting IoT-based meat processing systems. It focuses on understanding how these threats impact the overall quality and safety of meat products and the efficiency of the production processes. The research involves a case study approach, focusing on various levels of threats identified through threat modelling processes in an IoT-based meat processing system. The study examines the impact of potential cyberattacks on the system's controls, particularly on processes like small goods tempering (SGT), which are crucial for maintaining product quality and safety.

   Cyberattacks on IoT systems adversely affected Overall Equipment Effectiveness (OEE), a key performance indicator in Total Productive Maintenance (TPM). Variabilities in process sequences or parameters, such as product temperature due to cyber threats, can lead to significant product quality issues. To mitigate these risks, the paper proposes integrating cybersecurity as a new pillar in the existing TPM framework. This addition aims to enhance the resilience and security of IoT systems in meat processing plants against cyberattacks. The study also discusses barriers to implementing TPM and the success factors for effective deployment, emphasising the integration of vulnerability prediction for IoT systems with monitoring OEE.

9. **Shah et al.** "A survey on Classification of Cyber-attacks on IoT and IIoT devices" [38]
   This paper addresses the concerns around the security of Internet of Things (IoT) and Industrial Internet of Things (IIoT) devices, which have become integral to modern life and industry. With the integration of these devices in various sectors, particularly in automated manufacturing under Industry 4.0, they become potential targets for cyber-attacks.

   The paper outlines the layered architecture of IIoT systems, detailing the components and potential attacks at each layer. It highlights how the integration of Information Technology (IT) and Operational Technology (OT) in IIoT introduces complex security vulnerabilities, emphasising the need for robust security measures against a range of cyber-attacks, including malware, authentication attacks, phishing, SQL injection, DNS spoofing, web application attacks, and reverse engineering.

   To mitigate these threats, the paper suggests using stronger passwords, updating software, creating separate networks, employing more robust encryption, changing default

settings, enabling multi-factor authentication, generating backups, and utilising virtual private networks (VPNs). Additionally, it points out the necessity for ongoing research in standardisation and significant data security to cope with the evolving nature of IoT/IIoT and their associated cyber threats.

10. **Pu et al.** "Security of Industrial Robots: Vulnerabilities, Attacks and Mitigations" [34]
    This paper focuses on assessing the security vulnerabilities of industrial robots, which are critical components in intelligent and automated manufacturing systems. The study aims to explore and summarise the vulnerabilities, potential cyber-attacks, and existing security solutions for industrial robots, considering the challenges and difficulties in enhancing robot security. The research involves a detailed analysis of the vulnerabilities in industrial robots' control cabinets and firmware modules, comparing their security with traditional IT systems. It assesses various aspects, including task program vulnerabilities, communication network weaknesses, and access control system flaws. The study also reviews current security checks and encryption methods in robot communication networks and control systems.

    The study identifies several vulnerabilities in industrial robots, such as weak encryption, inadequate integrity checks, and lack of access control systems. These vulnerabilities open up possibilities for various cyber-attacks, including malicious programming, data manipulation, and unauthorised control. The paper highlights the consequences of such attacks, like compromising sensitive data and disrupting robot operations, potentially leading to physical damage due to the cyber-physical nature of these robots.

2.5 Survey

Questionnaire: The purpose of the survey is to learn about the existing state of automated systems and technologies and their security in Estonia. We have designed an online questionnaireconsisting of 19 questions. Its context is provided in Appendix II.

After inquiring about the demographic information on the organisation size (questions 1 and 2), manufacturing field (question 3), the respondent's role in the represented organisation (question 4), and information on the organisation's automation level (question 5), the questionnaire focuses on the automated manufacturing and security concerns.

Automated manufacturing is considered in seven questions. Hence, we are interested in learning what perspectives are for managing automated manufacturing systems (question 6), how these systems evolved during the last five years (question 7), what the main challenges are in using them (question 8), what information is managed (question 9), for which purpose the organisations utilise information technology in the automated manufacturing processes (questions 10 and 11), and whether the organisation align to any architecture framework for the automated systems and technology (question 12).

The security concerns are considered in five questions. The questionnaire inquires about how security-related topics are handled in organisations (question 13), what regulations and standards are used (question 14), whether the organisation encounter any security risks or threats (question 15), what countermeasures are applied (question 16), and what personnel training on security is

conducted in the organisation (question 16).

The last two questions are open-ended. Question 18 encourages the respondents to share related issues on automated systems and their security, that were not captured in the previous questions. The final question inquiries about the possibility of contacting the respondent later for a potential collaboration.

Survey: The survey was conducted between February 12 and March 31, 2024 in Estonia. It was promoted through the newsletter and social media platform of the University of Tartu, Institute of Computer Science, as well as through the AIRE[3] newsletter, social media channels, and personal social media accounts. The study targeted manufacturing Small and medium-sized enterprises (SMEs) undergoing digitisation.

The survey saw 90 attempts to participate, with 20 completed submissions. Among these 20, two companies were classified as micro-sized, seven as small, nine as medium-sized enterprises, and two as other categories (see Fig. 3). Eight out of the 20 participating companies were part of a larger group or conglomerate.

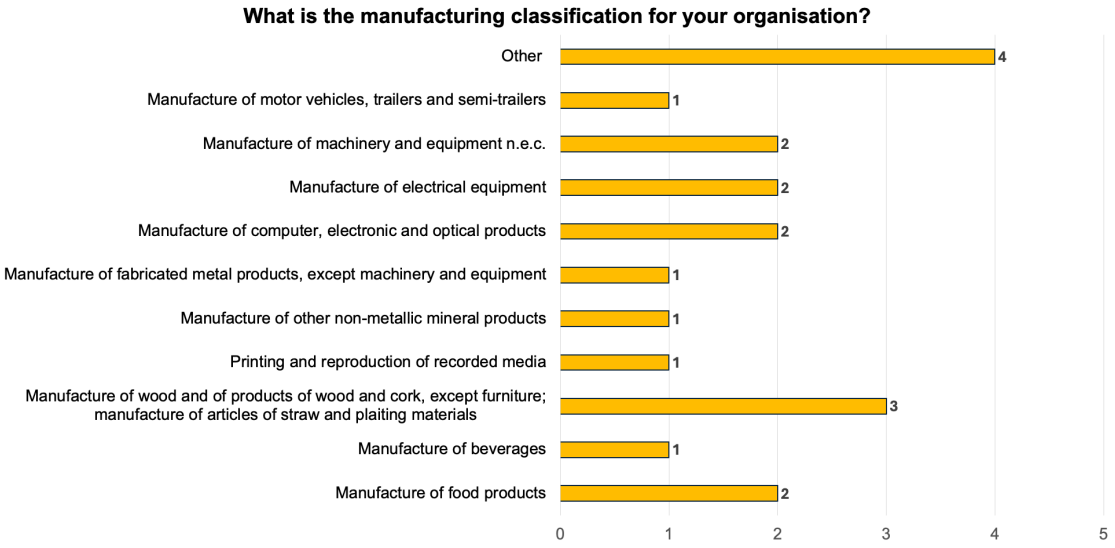

Figure 3. Organisations' Manufacturing Category

The survey results did not show a clear dominance in the manufacturing sector background of the respondents. Fig. 3 illustrates that the responses were diverse across different manufacturing categories. A similar diversity was observed in the respondents' roles, as shown in Fig. 4.

2.6 Threats to Validity

Several threats to the validity of this study have been identified.

Instrument validity: There is a risk that the tools (e.g., questionnaires and data extraction/summary forms) used in interviews, the systematic literature review and the survey are not

[3]https://aire-edih.eu/en/

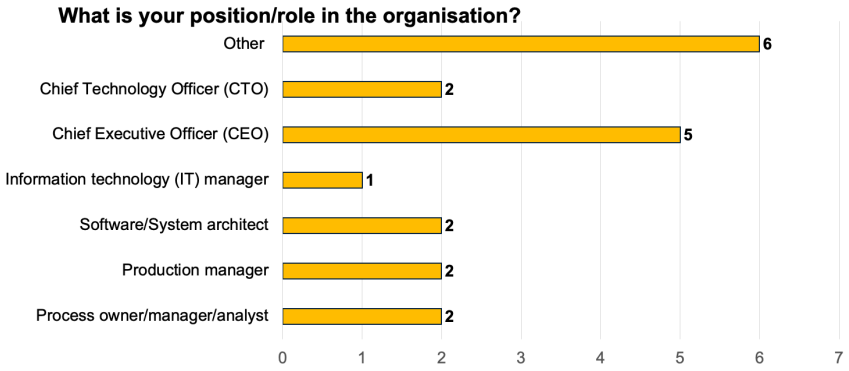

Figure 4. Responder Roles

accurate. It raises questions about whether the received results contribute to the accurate data and information needed to conclude. The risk here is that any limitations in these instruments could lead to incomplete or biased data collection, thereby affecting the overall findings. To mitigate this risk, we have reviewed the developed instruments within the research team and collected some feedback from outside contributors. We have done some minor piloting analysis of the questionnaire used in the survey.

Conclusion validity concerns the reliability of the conclusions drawn from the research data. This involves inspecting the methods used for data analysis, particularly in interpreting interview responses and synthesising findings from the literature. The main threat lies in the subjective interpretation and accuracy of qualitative data gathered in all three empirical steps. To mitigate this risk we review and align the collected data from all three empirical steps. Such an alignment allows for validation and conclusion taking into account different perspectives (interviewees, literature sources and survey respondents).

Internal validity addresses the causal relationships established within the study. The systematic literature review examines the linkages between the findings of different studies. The interviews pertain to the connections drawn between the interview data and the overarching research questions. Internal validity is threatened if these linkages are not explicit or empirically sound. This can lead to incorrect assumptions about cause-and-effect relationships. We mitigate this risk by reviewing the steps of the empirical research methods and their relationships to the targeted research methods.

External validity relates to the generalizability of the research findings. It questions whether the results from the interviews, the literature review and the survey can be applied to other contexts or populations. The primary threat is the possibility that the specificity of the chosen literature and the characteristics of the interviewed companies may limit the applicability of the conclusions to broader settings or different organisational environments. We consider this threat rather limited since the sources for the data collection are reviewed carefully and the received results and findings will be generalisable to the other contexts.

3 Context of Automated Systems and Technology

Automated systems and technology can be understood from different perspectives ranging from industrial robots to automated manufacturing systems. In this section, we define automated systems and technology and recapture different automation levels. The purpose is to explain what the context of the automated systems and technology is, therefore we present RAMI 4.0 - reference architecture model for Industry 4.0. Next in the chapter we briefly recall a few challenges that manufacturing organisations could potentially encounter.

3.1 Definition of Automated Systems and Technologies

Historical overview: A comprehensive overview of the evolution of automated system technologies is presented in [1]. Automation emerged as a concept in April 1947, coined within the context of Ford's automotive assembly lines [1]. The aim was to leverage technology to enhance production rates and improve overall productivity in manufacturing. In 1997, automation was conceptualised as executing functions by machines (e.g., computers) that humans traditionally performed. This shift in process automation transformed working conditions and the human role within the industrial sector. Humans transitioned from being direct operators to assuming roles such as designers, maintenance personnel, or supervisors. In 2016, automation was described as a system programmed to perform specific tasks without the capacity for autonomous decision-making or action modification. Such systems operate based on pre-established actions, lacking the ability to adapt or alter these actions in future contexts. The current technological endeavour in manufacturing aims to develop production lines that could be adapted to varying products and production volumes [1].

Definition: After an overview of the historical background of automated systems and technologies, in Table 4 we present a compilation of definitions, ranging from industrial robots to automated manufacturing systems. However, in this report, we adjust the following definition:

> **Automated systems and technologies** is a network of interconnected actuators, such as industrial robots and computational devices, forming an integrated web of systems that span design, planning, logistics, manufacturing, warehousing, and sales in the manufacturing sector. These systems automate functions traditionally performed by humans, enhancing efficiency and productivity across various stages of the manufacturing process.

Automated systems and technology can be at different automation levels as defined in [15]. The automation levels are:

- **Completely manual** - manual work, no tools are used, only the users' muscle power.
- **Static hand tool** - manual work with the support of the static tool(s).
- **Flexible hand tool** - manual work with the support of flexible tool.
- **Automated hand tool** - Manual work with the support of automated tool.

Table 4. Related definitions

Term	Description	Source
Industrial robots	They are utilized in intelligent and automated manufacturing environments. They execute physical tasks (e.g., picking and placing objects, which are determined through their interactions with other devices within the manufacturing systems, facilitated by the manufacturing network).	[34]
Cyber-physical systems (CPSs)	These systems encompass a range of hardware and software components, including mechanical actuators, controllers, sensors, devices for human interaction, control logic, firmware, and operating systems.	[35]
Embedded computing systems	They are integrated within a larger structure, tailored explicitly for dedicated functions. A single system comprises a blend of hardware and software components and mechanical elements. The robots consist of mechanical structures, sensors, actuators, and computer software that oversee and control these components.	[8]
Cyber-infrastructure elements (in Cyber-physical systems)	Examples are computational processes, control algorithms, decision systems, and databases, along with physical infrastructure components (i.e., including physical processes and elements). These components are interconnected through sensors and actuators. These systems can connect physical and virtual processes within an intelligent network and possess the functionality to self-monitor their status and that of other cyber-physical systems.	[25]
Automated Manufacturing System	They comprise a series of interconnected stations, each structured to process materials and create subcomponents or partially completed final product components. These components are transferred to subsequent areas for additional processing. The orchestration of logical flows between these stations necessitates control. This control mechanism coordinates the functions of the various stations within the manufacturing chain via a communication network.	[21]

- **Static machine/workstation** - automatic work by a machine that is designed for a specific task.
- **Flexible machine/workstation** - automatic work by a machine that can be reconfigured for different tasks.
- **Completely automatic** - Automatic work, the machine solves all deviations or problems that occur by itself.

3.2 Reference Architectural Model Industrie 4.0

Reference Architectural Model Industrie 4.0 (RAMI 4.0) is a strategic framework developed as a part of the Industrie 4.0 initiative [10]. It is a guiding architecture for the digital transformation of manufacturing and industrial sectors, pivotal in the fourth industrial revolution era.

Industrie 4.0, originating from a German government initiative, represents a paradigm shift in the industry, emphasizing integrating digital technologies into manufacturing processes [33]. The advent of RAMI 4.0 emerged as a necessity to standardize and structure this integration. It was developed collaboratively by the German Electrical and Electronic Manufacturers' Association (ZVEI), the German Institute for Standardization (DIN), and the VDI/VDE Society for Measurement and Automatic Control. RAMI 4.0's primary goal is to create a unified framework encompassing all aspects of the industrial value chain, ensuring consistency, interoperability, and efficient communication within digitalized industrial environments. RAMI 4.0 is depicted as a three-dimensional map, which includes axes representing different layers of an industrial system [22][42][31]. These layers range from physical assets and their integration into networks to the application of data analytics and business models.

The intent of RAMI 4.0 is to be resilient and easy to expand or link with other manufacturing architectures. As per [42], any level of a manufacturing enterprise can find a location in this three-level architecture. Several vital standards in the context of RAMI 4.0 include:

- **IEC 62890** for life-cycle status,
- **ISO/IEC 62264** for enterprise-control system integration,
- **IEC 61512** for batch control.

Other related standards include IEC 62541, IEC 61784, VDMA 24582, IEC 61987, and ISO/IEC 20140 [42]. Moreover, RAMI 4.0 is considered an underlying standard through previous research on reference manufacturing architectures [42], [31]. Authors [22] also define RAMI 4.0 as a standardized, layer-based enterprise architecture.

Hierarchy Levels Axis of RAMI 4.0 is derived from the International Electrotechnical Commission's (IEC) reference architecture for factory design. It categorizes elements of industrial processes into seven levels:

- **Product**: The product is the outcome of the manufacturing in the industry
- **Field Device**: These are the hardware components, such as sensors and actuators, that collect the environment values.
- **Control Device**: Controlling devices such as PLCs and DCs take the readings from sensors and send the controlling commands to operate the system.
- **Station**: This is where the user with administrative rights monitors the industrial activity and takes care of processes and events, e.g., SCADA.
- **Work Centers**: This provides the data storage, information, and analysis (MES) based on historical insights.

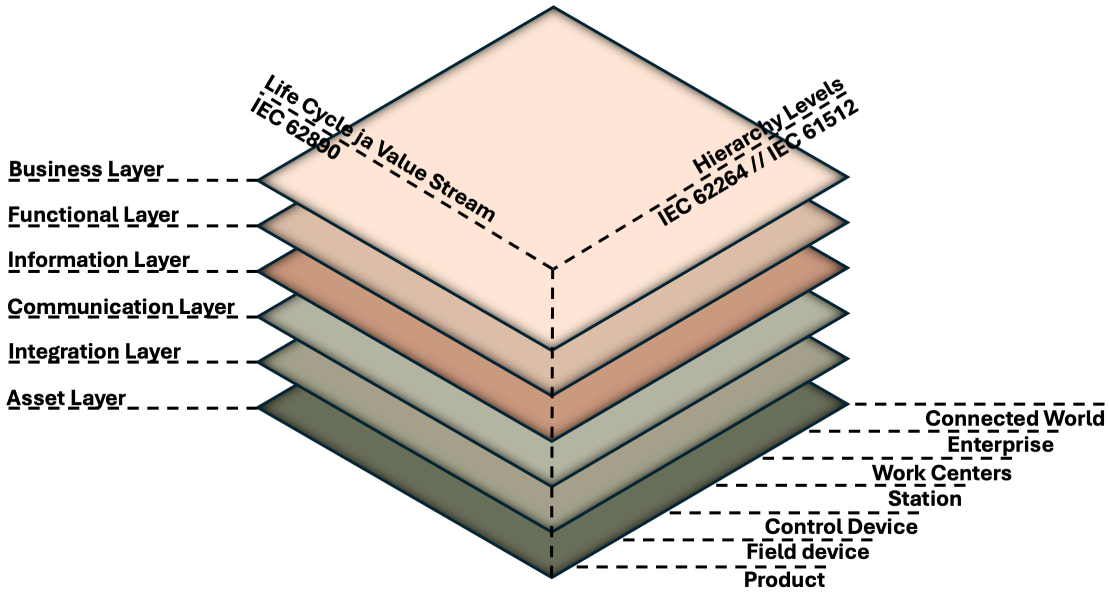

Figure 5. RAMI 4.0 Architecture model, adapted from [10]

- **Enterprise**: The enterprise level (ERP) is followed to manage all information and make profitable business decisions. It keeps track of production vs. orders and expenses vs. revenue and manages the manufacturing planning.
- **Connected World**: The system is connected to the internet to remain connected with the supply-chain process with external industries.

Life Cycle Value Stream dimension of RAMI 4.0 addresses the product life cycle from its inception to its disposal, incorporating the idea of a "Type" and "Instance" at every stage. This aspect emphasizes the importance of considering products and assets in their operational phase and throughout their existence, including development, manufacturing, use, and decommissioning. This perspective explains the changing requirements of products and systems as they progress through their life cycles.

Architecture Layers. RAMI 4.0 comprises six layers designed to provide a comprehensive view of the industrial system. Each layer serves a specific function, from the physical elements of the system (i.e., Asset Layer) to the overarching business objectives and models (i.e., Business Layer). This layered approach supports the analysis and design of industrial systems, ensuring that aspects, from hardware to data analytics, are integrated. The layers are:

- **Asset Layer**: This is the lowest layer, which contains all the physical components, including the devices and peripherals.
- **Integration Layer**: This layer provides the information generated from assets to the upper layers, enables the command and control of assets to the application and functional layer and contains the IT elements such as RFID, HMI, and actuators.

- **Communication Layer**: This layer is responsible for maintaining the communication between networks using the standards and protocols and enables the interaction of asset and Integration layers with the upper layers.
- **Information Layer**: This layer provides the pre-processing of information for different events, ensures the integrity and quality of data received from the lower layers and then presents the structured data to the Functional and Business layers.
- **Functional Layer**: The functional layer receives the data from the Assets layer and makes decisions based on data analytics.
- **Business Layer**: This layer covers the enterprise business models, legal frameworks, and industrial real-time monitoring services using dashboards and user interaction applications.

The RAMI 4.0 levels facilitate the mapping of traditional industrial setups into the digitized Industry 4.0 paradigm, ensuring each component's role is defined and integrated within the overall system.

In the context of this report, we focus on the Asset architecture layer. We extract data from selected papers (see Section 2.4) as per Hierarchy levels presented in the Asset architecture layer. After extracting physical assets related to the manufacturing process, we can provide context regarding information value to other architecture layers.

3.3 Challenges

Organisations, to stay competitive in the market have to deal with numerous challenges. In [20], a few major challenges are briefly reviewed. For instance, **digital transformation** or in other words integration of technology into the business and manufacturing processes could lead to an inconsistent experience for users of the organization's applications. Taking a more systematic approach to digital transformation that considers how each piece of technology is integrated into the whole process is a challenge for the IT advisory service.

Cloud solutions could contribute to information security and access [20]. However, they are created differently and could become a challenging task to integrate the cloud with processes Wrong implementation could potentially lead to data breaches. **Compliance requirements** differ depending on the organisation's size, location, industry vertical, business model, and customers served. Failure to comply with specific technology regulations results in fines and penalties that can cancel manufacturing processes.

Integrations and upgrades are unavoidable in digital transformation [20]. Upgrading and integrating systems into new technology infrastructure may not always be successful because application programming interfaces may fail to be compatible with new/old software systems or take longer to upgrade. The manufacturing industry leverages **automation** tools to accelerate processes, reduce production costs, and increase employee safety. New automation tools affect operations; employees may take time to learn how to use the latest technology. **Artificial intelligence and machine learning** (AI/ML) support the functionality of automation tools. However, finding suitable AI/ML methods for the targeted tasks is challenging.

Organisations need **data management** strategies to protect their data from unauthorized access and manipulation [20]. In the event of a data breach, organisations can find it challenging to keep the systems running. Implementation of new solutions and technologies **changes the infrastructure** and can have a disruptive effect. These disruptions can cost time and money as employees struggle to learn how to work with (or around) big changes. Also, managing infrastructure changes can be a costly and time-consuming process.

Organisations lack **experienced professionals** [20]. Thus, they either use the outsourced services or train employees to be competent in managing automation tools, processes, applications, etc. **Managing** (i.e., planning, organizing, and implementing) automation initiatives is challenging. Ineffective project execution may result in budget overruns and extensive delays.

A data breach is a primary threat to **data security** [20]. It affects the financial health and competitive advantage of the organisation. Security threat agents are constantly creating new strategies to cause harm to businesses. Since different companies follow different information security requirements, data and information security remains challenging.

3.4 Interview Results

This section provides an overview of the results of the interviews. Interviewees discussed challenges challenges which are experienced by their organisations with the automated system and machinery handling, general security strategy, threat awareness and incident response, data exchange and integrity, employee education and training, compliance and legal awareness, and technology and innovation. Below we summarise the interview results outcomes.

Automated Systems and Machinery Handling: Organisations exhibit varying degrees of automation in their processes ranging from completely automated to manual processes. Notably, newer machinery often requires vendor-specific remote access for troubleshooting, while older machines frequently operate on outdated software or firmware, acknowledged as a risk due to investment rationales.

General Security Strategy: There exists a correlation between an organisation's size and its security preparedness. Larger organisations tend to have established security policies and strategies, whereas smaller or startup companies lack such formal procedures. Security measures, including software updates, user access rights, and data backups, are established, either managed in-house or outsourced.

Threat Awareness and Incident Response: Security incidents have been experienced in the respondents' organisations. Respondents reported that these led to updated security measures. However, the focus on security has diminished over time since the incident. The organisation's size appears to influence the likelihood of conducting security tests and the level of subsequent response.

Data Exchange and Integrity: Organisations employ a mix of in-house and cloud-based data storage solutions, reflecting varied levels of trust in external storage providers. Incidents have shown that combining in-house and cloud-based storage methods offers recovery options. Established processes and behaviour patterns hinder plans for cloud migration among larger companies.

Employee Education and Training: The extent and regularity of security training vary

across organisations. Larger companies have structured training programs in place. However, all respondents identified a gap in security training, emphasising it as a drawback.

Compliance and Legal Awareness: Awareness of GDPR and other specific security regulations is present but it varies in depth and detail (especially in smaller companies and startups). This indicates a need to explain compliance with security legislation.

Technology and Innovation: Cost considerations and the goal of profitability influence decision-making regarding technology adaption. Preferences for established European vendors are noted, particularly for local or semi-local support. Negotiations with vendors for best practices, especially regarding remote access, are common, reflecting an awareness of the importance of cybersecurity in new technologies.

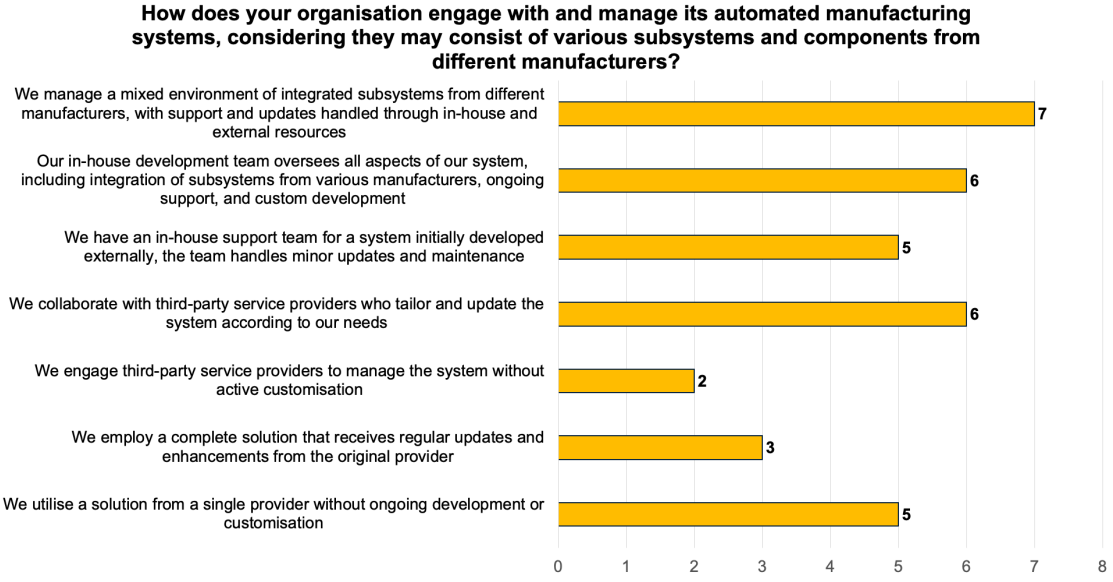

Figure 6. Automated manufacturing systems' implementation variations

3.5 Survey Results

The findings from the questionnaire underscore a trend towards integrating various technological approaches within the manufacturing sector, exhibiting a preference for sourcing solutions from a single provider. As depicted in Fig. 6, a predominant inclination exists towards the consolidation of various solution types under the umbrella of a singular corporate entity. This tendency not only highlights the multifaceted and segmented nature of the manufacturing ecosystem but also reflects the strategic move towards simplification and streamlining of technological infrastructures within companies. Such a strategy facilitates smoother operations, enhances interoperability among different technological components, and potentially lowers the complexity and cost of managing multiple vendors.

Fig. 7 illustrates how respondents see the automation levels in their organisations. It is worth noting that all responses were between levels 3 and 6, confirming that automation is

indeed happening across the industry. The majority (7 answers) report that they use static machines/workstations, which are designed for specific tasks (Level 5). Automated hand tools which support manual work (Level 4) are reported by 6 respondents, and 4 respondents indicate that they use machines that can be reconfigured for different tasks (Level 6).

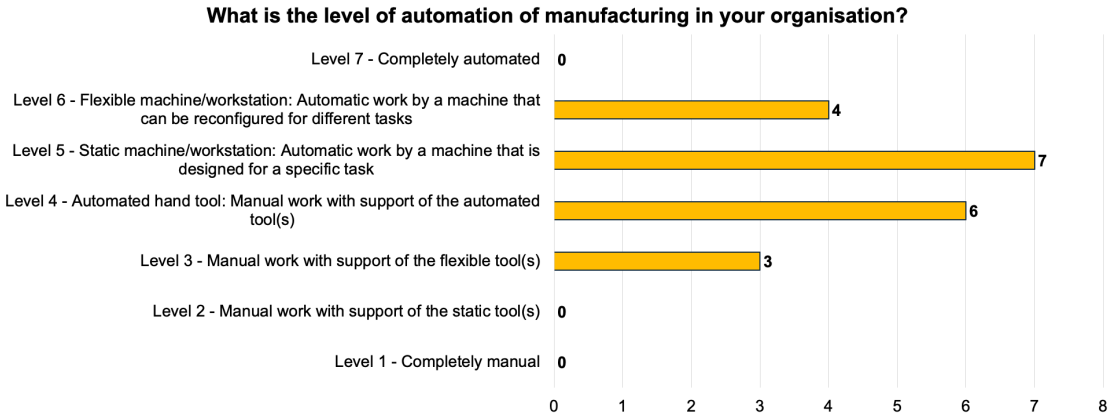

Figure 7. Levels of automation

In parallel, an overwhelming consensus among participants acknowledges the significant transformations within the last five years (see Fig. 8).

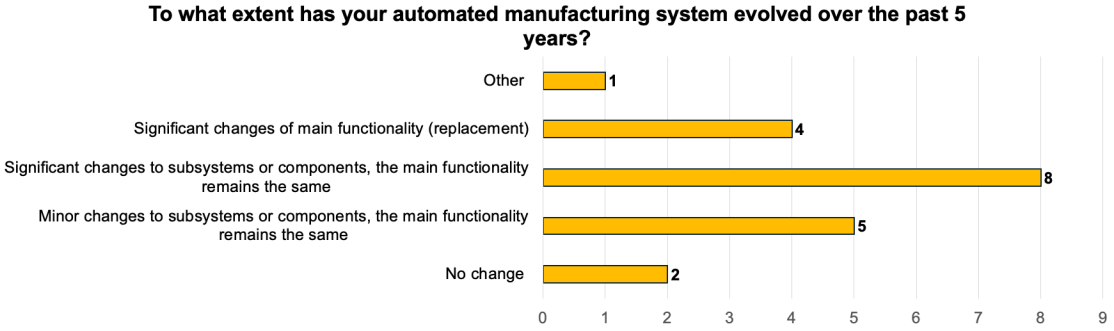

Figure 8. Automated manufacturing systems' alterations over last 5 years

Manufacturing process optimisation across multiple different subsystems is reported as the most challenging (11 answers) during integration, development and support of the automated systems and technology (see Fig. 9). This challenge is followed by the need to achieve high-quality characteristics, manage system security and reliability, balance system efficiency with privacy concerns, and ensure data privacy and security during the integration of diverse subsystems and manufacturers (every 8 answers).

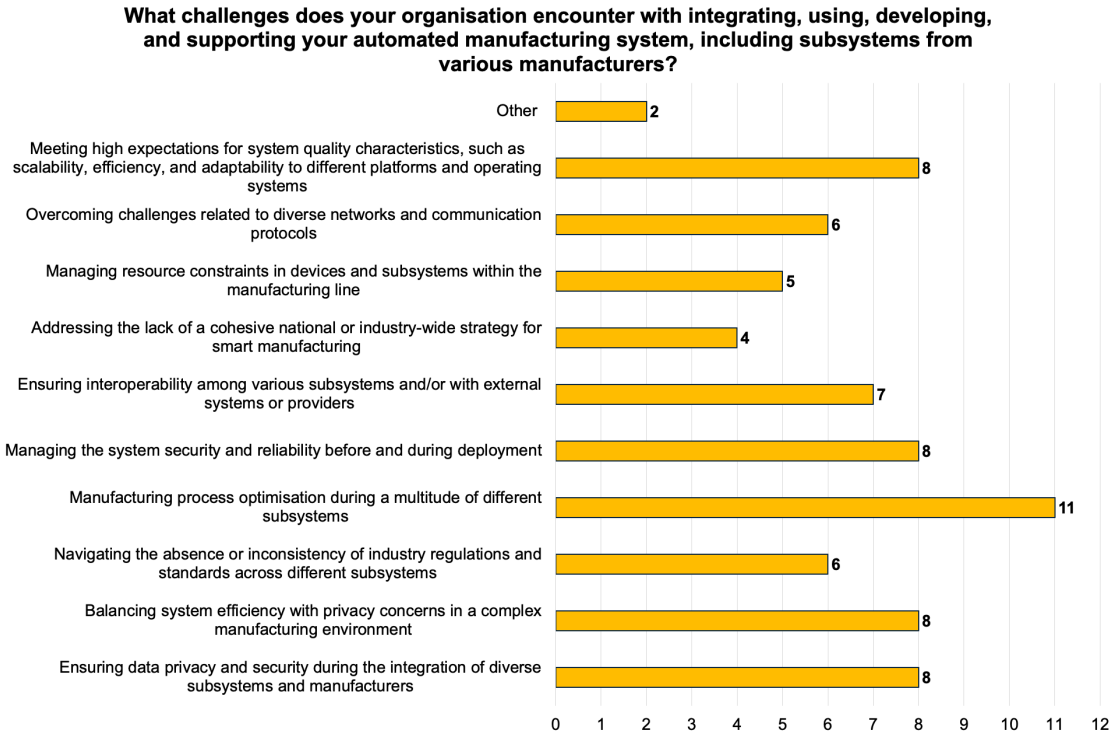

Figure 9. Challenges of Implementation of Automated Manufacturing Systems

3.6 Discussion

The findings indicate that manufacturing organisations are keen on transforming their work practices to automated ones. This transformation results in an evolution and adoption of advanced solutions, spotlighting the escalating imperative for digitalisation within the sector. This shift is not merely a response to the demands for increased efficiency and productivity but also a proactive approach to embracing the future of manufacturing, marked by a degree of automation, data integration, and smart manufacturing practices.

The integration of novel solutions brings to the forefront the difficulties associated with merging diverse technological systems under a unified operational framework. These challenges often pertain to compatibility issues, data silos, and the complexity of managing integrated systems. The benefits of such technological integration – ranging from enhanced operational efficiency and data analytics capabilities to improved product quality – outweigh the initial obstacles. This positive outlook reinforces the value proposition of digital transformation in manufacturing, underscoring the industry's readiness to tackle the challenges for long-term innovation and competitiveness.

4 Standards

In this section, we'll explore the range of standards referenced in the reviewed articles, which shows their complexities and underscores their applicability to the varied use cases of automation presented. This exploration covers a spectrum from safety protocols in industrial robotics to cybersecurity frameworks in cloud-based manufacturing systems. Each standard plays a distinct and critical role in enhancing the robustness and dependability of contemporary automated systems. The aim of this review is twofold: to provide insightful information and to offer guidance for future practical applications and research within the field of industrial automation. Specifically, we consider what standards should be followed while using automated systems and technology.

4.1 Safety and Security Standards for Industrial Robotics and Automation

In industrial automation and safety, many standards and frameworks play a pivotal role in shaping automated systems' design, implementation, and operation. These standards, ranging from safety protocols in industrial robotics to cybersecurity measures in cloud-based manufacturing systems, are instrumental in ensuring the robustness and reliability of these systems. They provide structured guidelines and methodologies for maintaining operational efficiency, safety, and security in various automation scenarios.

4.1.1 Standards for Industrial Robotics and Automation

The scientific articles related to safety standards for industrial robotics and automation [35, 23, 21, 41, 7] encompass a broad spectrum of automation scenarios, ranging from industrial robotics to cyber-physical production systems, each relying on distinct standards and frameworks. This diversity reflects the multifaceted nature of automation in various sectors and underscores the necessity for a comprehensive understanding of these governing principles.

Safety And Security Standards for Industrial Robotics and Automation were mentioned by Quarta et. al. [35] and Khalid et.al.[23]. **ISO TS 15066** specifically addresses collaborative robot systems, **ISO 12100** deals with general safety principles, and **ISO 10218 parts 1 and 2** focus on safety requirements specific to industrial robots. These standards collectively provide guidelines for the safe design, implementation, and operation of industrial robots. **ISO 8373** defines what constitutes an industrial robot, emphasising its programmable, multi-purpose nature and applicability in industrial automation.

Jablonski et al. [21] suggest standards for system architecture and safety in complex systems. AADL (**SAE AS5506C**) offers a framework for modelling and analysing complex systems, particularly focusing on aspects like timing and safety. The others, AADL Behavior Model Annex (**SAE AS5506/2**) and AADL Error Model Annex v2 (**SAE AS5506/1A**), annexes provide additional tools for specifying system behaviours and error handling mechanisms, crucial for ensuring the reliability and safety of automated systems.

Urooj et al. [41] and Chundhoo et al. [7] directing to general risk management standards (**ISO 31000**), which offers principles, guidelines, and a process for managing risks effectively.

While the standards discussed thus far lay a solid foundation for safety and system architecture in industrial automation, an examination reveals a gap in the cybersecurity coverage within these frameworks. This gap becomes increasingly significant in the context of the rapid evolution of cyber threats and the deeper integration of automation systems with information and communication technologies. Despite the robust frameworks for physical safety and operational efficiency, the current standards landscape exhibits limitations in adequately addressing the multifaceted challenges posed by cybersecurity threats to automated manufacturing systems.

This realisation underscores the necessity of augmenting our understanding of cybersecurity by drawing on established knowledge and practices from IT systems. The ensuing chapter aims to bridge this gap, introducing standards and regulations from the IT sector that can be effectively applied to enhance the cybersecurity posture of automated manufacturing systems. By integrating these insights, we aim to provide a more holistic approach to securing automated environments against emerging cyber risks, ensuring the resilience and reliability of these critical systems in the face of evolving threats.

4.1.2 Cybersecurity Convergence: From IT Infrastructure to Industrial Automation

In addressing cybersecurity within automated manufacturing systems, it is imperative to acknowledge the foundational principle that security cannot be definitively guaranteed; rather, the focus must be on identifying vulnerabilities and the absence of security measures. This sets the stage for the critical role of security controls, which encompass an array of managerial, operational, and technical strategies designed to protect the system's confidentiality, integrity, and availability. These controls are implemented through a combination of policies, procedures, and technical measures, both manual and automated, to reduce potential risks.

Central to the cybersecurity framework are standards that aim to ensure interoperability, compliance with national and international regulations, and a set of minimum requirements to ensure the security of systems in terms of availability, confidentiality and integrity. Also, cybersecurity baselines (*de facto* standards), formulated from best practices, provide organisations with guidelines for implementing security measures and conducting risk analysis. Examples such as:

- **ISO/IEC 27000 Family** - Information security, cybersecurity and privacy protection [19]
- **NIST Cybersecurity Framework** [32]
- **CIS Critical Security Controls** [6]
- **E-ITS, Estonian Information Security Standard** [37] in which one of the ten modules, the IND module, deals separately with industrial automation
- **Microsoft Security Baselines** [30] main focus is on Microsoft products and services.

Standards establish a common language and practices for effectively managing cybersecurity risks. Ensuring compliance with established standards and regulations involves a multifaceted approach, including audits, certifications, and self-evaluations.

Kutzler et al. [25] suggest additionally the **Framework for Improving Critical Infrastructure Cybersecurity** by NIST, which guides the development of robust cybersecurity strategies, particularly relevant for protecting critical infrastructure systems, including manufacturing ones.

But also, the standards and frameworks **TAXII** (Trusted Automated eXchange of Indicator Information), **STIX** (structured threat information expression) and **CyBEX** (Cybersecurity information EXchange framework) referenced by Schaefer et al. [27] are vital for cybersecurity information sharing and collaboration, helping organisations to better defend against and respond to cyber threats.

Among the pivotal standards critical to fortifying cybersecurity in industrial automation systems, the **ISA/IEC 62443** [18] series stands out for its focus on Industrial Control Systems security. Developed to address the unique challenges faced by sectors such as energy, manufacturing, and transportation, IEC 62443 provides a framework for securing industrial automation and control systems. It outlines a structured approach to cybersecurity, covering aspects from risk assessment and system design to implementation and maintenance, thereby ensuring the resilience of these systems against cyber threats.

In addition to the technical and operational standards essential for securing industrial automation systems, regulatory frameworks play a crucial role in shaping cybersecurity practices. Among these, the **General Data Protection Regulation (GDPR)** [13] of the European Union stands as a paramount legal framework, emphasising the importance of personal data protection. GDPR imposes requirements on data processing activities, ensuring the privacy and security of personal data across various sectors, including manufacturing.

For automated manufacturing systems that collect, process, or store personal data, compliance with GDPR is not just a legal obligation but also a component of cybersecurity hygiene. It underscores the necessity for data protection measures, such as data minimisation, encryption, and timely breach notification, aligning with the broader objectives of cybersecurity to protect system integrity and confidentiality. The intersection of GDPR with industrial cybersecurity standards like IEC 62443 demonstrates the multifaceted nature of securing modern automated systems, where ensuring data privacy becomes integral to the overarching cybersecurity framework.

4.2 Survey Results

Fig. 10 presents what security, privacy or safety-related legislation, regulations and/or standards affect the automated manufacturing systems used in the respondents' organisations. The most frequently indicated are the General Data Protection Regulation, GDPR (9 answers) recognised across Europe and Estonia's *Isikuandmete kaitse seadus* (Estonia's Personal Data Protection Act), IKS (10 answers). *Küberturvalisuse seadus* (Cyber Security Act) KüTS and Estonian Information Security Standard (E-ITS) take the third place (both with 4 answers).

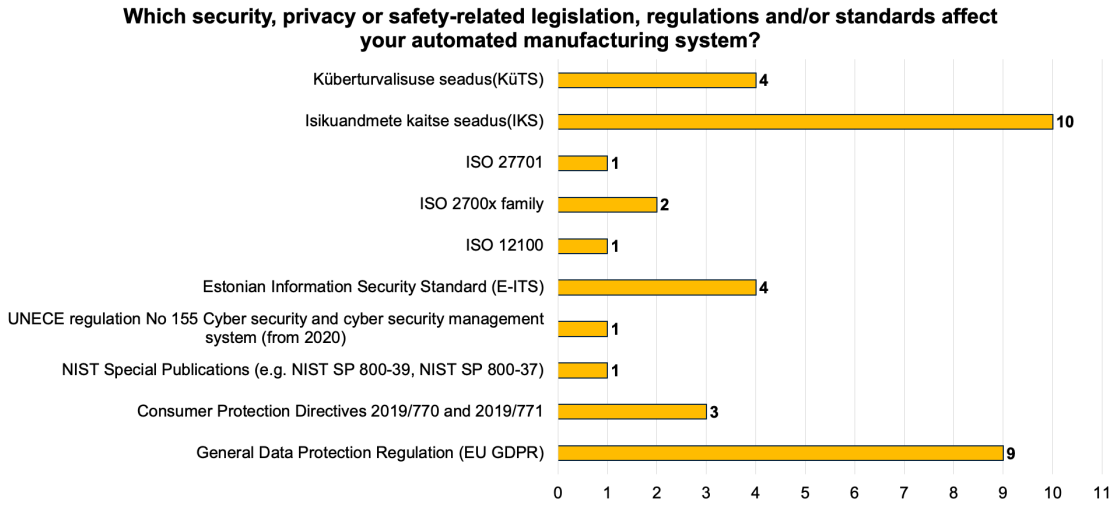

Figure 10. Security, Privacy or Safety-Related Legislation, Regulations and/or Standards that Affected Automated Manufacturing System

4.3 Discussion

Security, privacy or safety-related legislation, regulations and/or standards potentially can introduce organisations to the best practices for automated systems and technology engineering, management and maintenance. The standards can guide organisations with security policies, risk management approaches and mitigation strategies. However, the survey results regarding the respondents' legal awareness revealed a concentrated focus on personal data protection norms, such as the General Data Protection Regulation (GDPR) recognised across Europe and Estonia's *Isikuandmete kaitse seadus* (IKS). This narrow scope of legislative familiarity underscores a knowledge gap, a lack of understanding and experience with broader legal frameworks that govern the digital and cybersecurity landscapes.

This finding is particularly concerning in an era where digital operations are tied to various regulatory requirements beyond personal data protection. Such regulations range from industry-specific compliance standards to international cybersecurity protocols, which play critical roles in safeguarding the interests of businesses and their stakeholders.

5 Asset of Automated Systems and Technology

In this chapter, we present the results of interviews, a literature review and a survey regarding the assets of automated systems and technology. We recall that assets can be grouped into business assets (e.g., data, information and services) and system assets (system components or their combinations supporting business assets). Security objective is defined using security criteria (i.e., confidentiality, integrity and availability) as a constraint on the business assets. In this chapter, we consider what protected assets are in automated systems and technology.

5.1 Interviews Results

In this section, we present the interviewees' perspectives on how the automated systems and technology used in their organisations could be explained with the dimensions of the RAMI 4.0 framework. The results are summarised in Table 5, where the assets are linked to the RAMI 4.0 Asset architecture layer. It is worth noting that interviews were conducted before the structured literature review and, therefore, do not have a specific granularity of detail. But they present a high-level overview of assets per interviewees' organisations in the manufacturing process.

It should be noted that the fifth interviewee represents a start-up company with outsourced production capabilities. The Enterprise and Connected World assets are of primary importance for this entity, as they are integral to daily operations. Regarding the other interviewees, a similar emphasis was placed on the Enterprise and Connected World levels, but attention was also given to lower-level assets. In all instances, the device manufacturers typically managed protection at the Field Device and Control Device levels due to vendor lock-in, which included specified access rights or requirements for on-site equipment troubleshooting.

Table 5. Mapping of interview results to RAMI 4.0 Asset dimension; "+" refers to mentioning assets

	Product	Field device	Control device	Station	Control centers	Enterprise	Connected world
Interviewee 1	-	+	+	+	+	+	+
Interviewee 2	-	+	+	+	+	+	+
Interviewee 3	-	+	+	+	+	+	+
Interviewee 4	-	+	+	+	+	+	+
Interviewee 5	-	-	-	-	-	+	+

5.2 Literature Review Findings

In this section, we summarise the findings of the literature review regarding the system and business assets. Similar to the previous section, firstly, Table 6 illustrates the mapping of system assets identified in the literature to the Asset dimension of the RAMI 4.0 framework.

Table 6. Mapping of system assets from literature to RAMI 4.0 Asset dimension. ”+“ refers to mentioning assets

Publication	Product	Field device	Control device	Station	Control Centers	Enterprise	Connected World
Khalid *et al.* (2021) [23]	-	+	+	+	-	-	-
Urooj *et al.* (2022) [41]	-	+	+	+	+	-	+
Thames *et al.* (2014) [27]	-	+	-	-	+	+	-
Clark *et al.* (2017) [8]	-	+	-	+	-	-	-
Kutzler *et al.* (2021) [25]	-	+	-	+	+	-	-
Quarta *et al.* (2017) [35]	-	+	+	+	-	+	+
Jablonski *et al.* (2021) [21]	-	+	-	+	-	-	-
Chundhoo *et al.* (2021) [7]	-	+	-	-	-	+	-
Shah *et al.* (2020) [38]	-	+	+	+	+	+	-
Pu *et al.* (2023) [34]	-	+	+	+	-	-	-

Product encompasses the final output of manufacturing processes, such as consumer goods or industrial products, central to the company’s revenue and market positioning. These products define the brand identity and are key to customer satisfaction.

Field device includes essential tools like robots, sensors, and actuators, crucial for precision and efficiency in manufacturing operations. These devices impact product quality, production speed, and adaptability to manufacturing tasks.

Control devices (e.g., programmable logic controllers (PLCs), remoter terminal units (RTUs), and distributed control systems (DCS)) are fundamental for automating manufacturing processes, ensuring consistency, and managing real-time data for operational decision-making.

Stations oversee and control specific manufacturing processes using workstations and operator interfaces ensuring the execution and monitoring of production activities.

Work centers comprises the technological backbone of an organization, including computers, servers, and collaboration software, which support activities like design, planning, and administrative tasks.

Enterprise: (e.g., ERP systems, cloud computing solutions, and business analytics tools) support strategic decision-making and resource allocation.

Table 7. RAMI 4.0 Asset layer assets

Hierarchy levels	**System assets**	**Business assets**
Product	–	–
Field devices	Robots, Actuators, Sensors, Motors, Transmitters, Embedded devices, Physical manufacturing machines, Cameras, 3D Printers.	Production data, operational conditions data, environmental factor data, quality control data, operational data, visual data.
Control device	Programmable Logic Controller(PLC), Remote Terminal Unit(RTU), Distributed Control System(DCS), Gateways.	Production data, operational conditions data, quality control data, automated decision-making process.
Station	Workstation (Digital Control Unit), SCADA/SCADA Masters, Operators, Operator Stations.	Operational data, operational processes, operational services.
Work Centers	Office Products, Collaboration software, IT Hosts, Computers, Servers, Data centres, Mail and Web services.	Application data, the application process, application services.
Enterprise	Enterprise resource planning systems (ERP), Total productive maintenance systems (TPM), Vendors, Partners, Business applications, Data analytics, Cloud computing.	Business process, operational resource planning, supply chain process, business application data.
Connected world	Internal network, Robot Network, Industrial demilitarized zone (DMZ), public internet.	Business application data, operational data, services and processes.

Connected world involves the network infrastructure, including internal and external communication networks. It helps integrate various business processes.

Mapping system assets to business assets in the context of RAMI 4.0 involves understanding the intrinsic business value these assets bring to an organisation. The considered papers do not explicitly highlight the security need (in terms of confidentiality, integrity or availability of the business assets). Hence we assume that all three criteria are important and depend on the specific security risks (we will consider several examples in Chapters 8 and 9). Table 7 summarises AST assets (system and business assets), classifies these assets, and illustrates the basic functional areas of each layer.

5.3 Survey Results

Survey results underscore a shift towards data-driven decision-making within manufacturing processes. Fig. 11 presents a spectrum of responses, illustrating that most enterprises now actively gather various data from their production operations. Moreover, Fig. 12 highlights the primary applications of IT systems in manufacturing, with data storage emerging as the predominant use (17 answers). This is followed by the management of the sales process (11 answers) and enterprise resource planning (ERP) (12 answers).

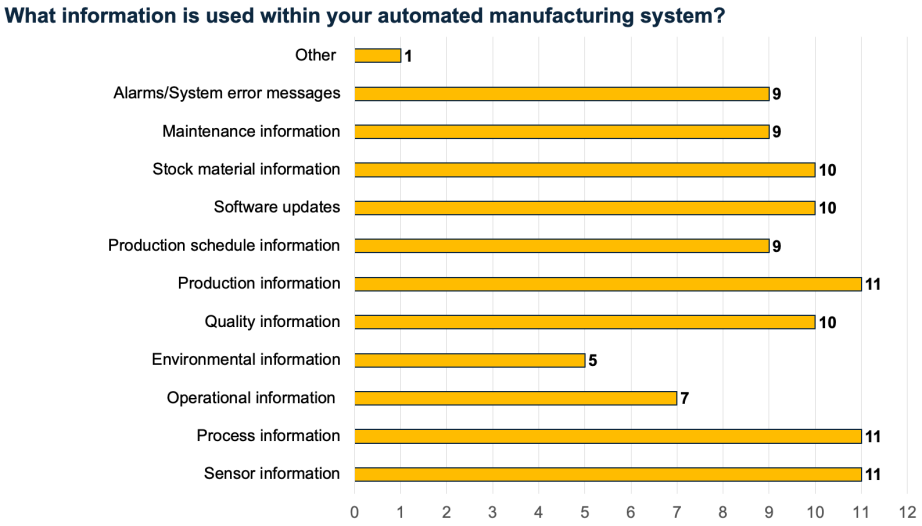

Figure 11. Data utilised in Automated manufacturing systems

5.4 Discussion

Adapting data-driven strategies yields main benefits, **extending process optimisation and reduced operational costs**. The prioritisation of data storage underscores the role of **data as a foundational asset** in the digital transformation. Data storage solutions enable enterprises to securely store, manage, and retrieve vast amounts of data, serving as the backbone for other data-driven activities. The role of sales process management reflects the **importance of integrating customer data and interactions into the manufacturing strategy**, ensuring that production aligns with market demand and customer expectations. Utilising ERP systems signifies the **comprehensive approach to integrating core business processes**, facilitating real-time data flow across departments, enhancing operational visibility, and improving decision-making efficiency.

The advantages include enhanced product quality, predictive maintenance, which minimises downtime by anticipating equipment failures before they occur, contribute to supply chain management through forecasting and inventory control and customer satisfaction by tailoring products to specific needs and preferences. Data utilisation underlines the strategic shift in manufacturing towards intelligent, efficient, and customer-centric operations.

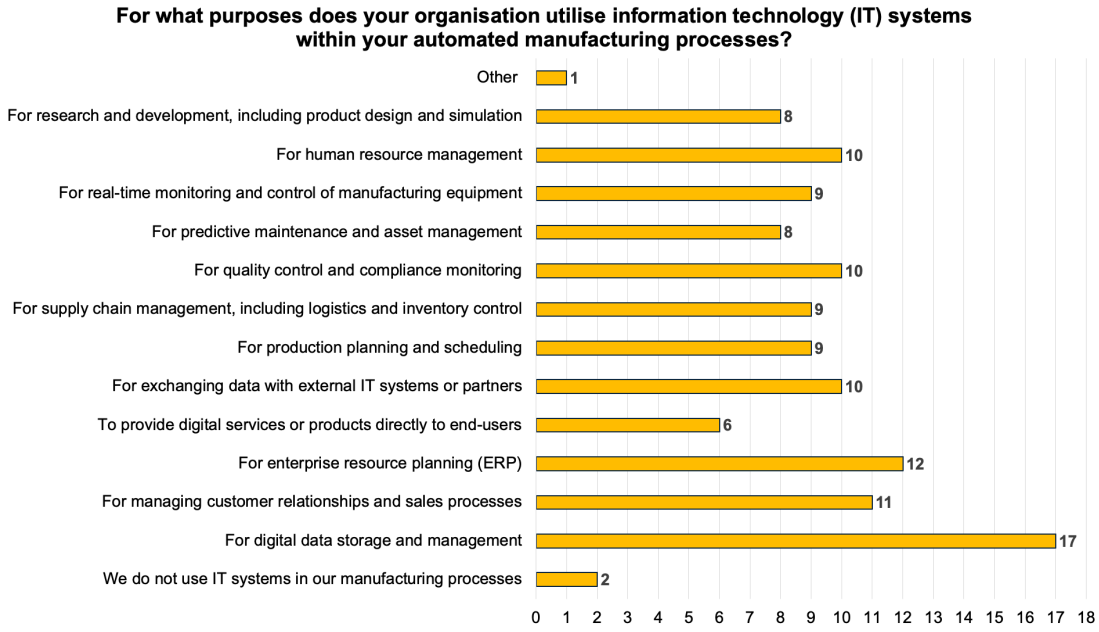

Figure 12. IT System usage purposes in Automated manufacturing systems

The findings show the evolving landscape of manufacturing, where **data-driven decisions** and **IT integration** are becoming central to operational strategies. By harnessing data, manufacturers are not only optimising their immediate processes, they also position themselves for sustained innovation, competitiveness, and growth in an digital and customer-focused market environment.

6 Security Risks to Automated Systems and Technology

In this chapter, we report on the security threats and risks observed in the literature review and the survey. We recall that a security risk is a combination of the threat exploiting one or more vulnerabilities, leading to a negative impact on the system and business assets. In this chapter, we analyse the security risks of automated systems and technology.

6.1 Situation in Estonian Cyberspace

Throughout 2023, geopolitical tensions significantly impacted Estonian cyberspace, as stated in the annual Cyber Security assessment [36]. In November, the conflict between Israel and Hamas extended its effects to Estonia with cyberattacks targeting the district heating network.

A notable cyberattack in late November 2023 disrupted a district heating company, affecting the control systems of eight boiler units. Although these units were switched to manual operation to maintain heat generation and distribution, the damage to the equipment was severe enough to necessitate replacements. Similar cyberattacks targeted at least two Estonian entities, one in the water supply and the other in the construction industry. The attacks aimed not at Estonian companies or institutions but at programmable logic controllers (PLCs) manufactured in Israel, regardless of their geographic location. This pattern was also observed in the United States, particularly affecting water utilities. The attackers, claiming to have an Iranian background, stated that these actions were in retaliation to the Israel-Hamas conflict. This series of events highlights how global geopolitical tensions and military conflicts can precipitate cyberattacks in distant countries like Estonia.

The cyber landscape in Estonia saw increased activity due to the ongoing conflict in Ukraine, with Denial of Service (DDoS) attacks quadrupling. This surge in cyber aggression peaked the already high levels of activity observed in 2022, setting a new record with 484 denial-of-service attacks recorded last year—60% more than the previous year. In just one month, the frequency of DDoS attacks surpassed the annual total observed before the escalation of hostilities in Ukraine. Of these, 139 attacks, constituting less than a third, were deemed impactful, typically causing brief downtime or reduced responsiveness for websites and services. However, in September, some instances, such as the attacks on Ridango a company managing ticket sales for the stateowned train service Elron had more severe consequences, disrupting online and onboard ticket purchases for nearly a day.

These cyberattacks became increasingly sophisticated and focused throughout the 2023, with attackers spending more time preparing and concentrating on specific targets to ensure noticeable disruption. The pattern often involved two stages: an initial short attack to gauge the target's defences and a more prolonged and intense attack if the first was successful. These DDoS attacks were frequently correlated with Estonia's support for Ukraine or the announcement of new sanctions against Russia, indicating a political motive behind the cyber aggression. This trend of politically motivated attacks continues to be a concern.

6.2 Literature Review Findings

Literature analysis results in 43 security threats. The extracted results are presented in Tables 8 and 9 and summarised in Fig. 13. The majority (19) of the threats are identified as tampering threats, 15 threats – the elevation of privilege, 4 threats – information disclosure, 4 – denial of service, and 1 – spoofing. We did not identify any repudiation threat in the considered literature.

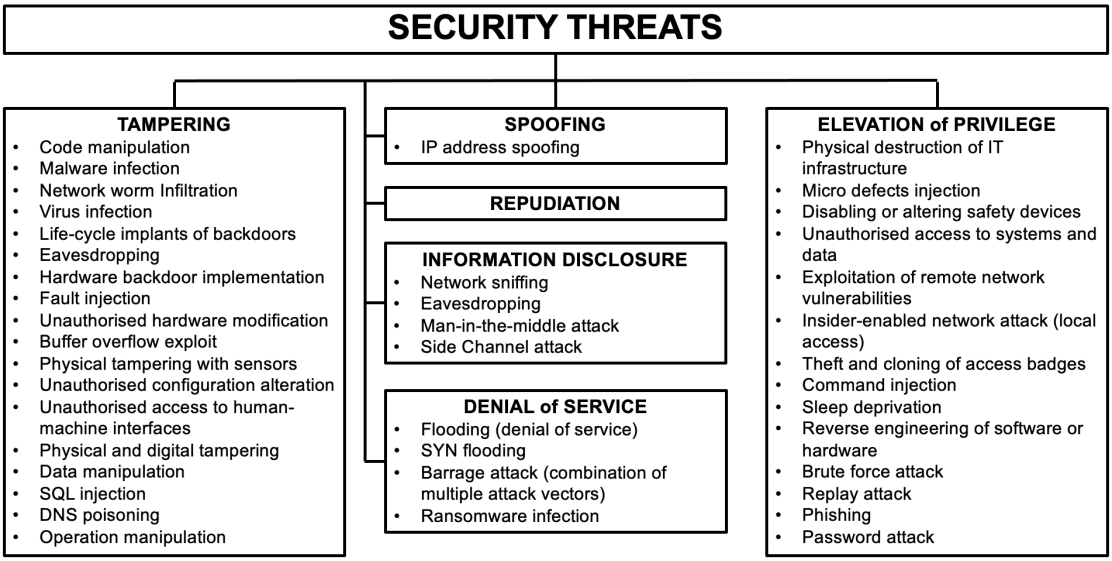

Figure 13. Security Threats Identified in Literature Review

Each security threat is elaborated to security risks (see Appendix III). Hence, the appendix presents the attack method, threat, vulnerability, and impact. As defined in [11] [29], the combination of these components defines the security risk to the system and business assets. Below, we present a few examples of the security scenarios.

Spoofing: IP Address Spoofing [38]: In this scenario, the threat comes from the ability to disguise malicious traffic as legitimate by altering the source IP address in data packets. This can bypass security measures relying on IP addresses for authentication or launch attacks against other targets, making it appear that the traffic originates from a trusted source. The key vulnerability lies in the network's inability to authenticate and validate the true origin of a packet. The impact of IP spoofing can be significant, ranging from unauthorised network access and data breaches to being implicated in attacks against third parties. Mitigating this risk involves implementing strong network security measures like packet filtering and intrusion detection systems, employing anti-spoofing techniques at the network perimeter, and consistently monitoring network traffic for suspicious activities.

Tampering: Code Manipulation [23][8][38]: In this scenario, the attacker's goal is to manipulate the code to create a backdoor for future access, disrupt critical systems' functionality, or ex-filtrate sensitive data. The lack of robust security practices in the software development lifecycle, such as thorough code reviews and automated security testing, creates a vulnerability the attacker can exploit. The impact of such an attack can be far-reaching, affecting not just

Table 8. Security threat classification to STRIDE Taxonomy (1)

Article	Spoofing	Tampering	Repudiation
Khalid *et al.* (2021) [23]	–	Code Manipulation, Malware infection, Network Worm Infiltration, Virus Infection, Life-cycle Implants of Backdoors, Eavesdropping, Hardware Backdoor Implementation.	–
Clark *et al.* (2017) [8]	–	Code Manipulation, Malware infection, Virus Infection, Life-cycle Implants of Backdoors, Eavesdropping, Hardware Backdoor Implementation, Fault Injection, Unauthorized Hardware Modification, Buffer Overflow Exploit.	–
Kutzler *et al.* (2021) [25]	–	Code Manipulation.	–
Quarta *et al.* (2017) [35]	–	Fault Injection.	–
Jablonski *et al.* (2021) [21]	–	Physical Tampering with Sensors, Unauthorized Configuration Alteration, Unauthorized Access to Human Machine Interfaces.	–
Chundhoo *et al.* (2021) [7]	–	Physical and Digital Tampering.	–
Shah *et al.* (2020) [38]	IP Address Spoofing.	Malware infection, Eavesdropping, Data Manipulation, SQL Injection, DNS Poisoning.	–
Pu *et al.* (2023) [34]	–	Malware infection, Data Manipulation, Operation manipulation.	–

the integrity of the software but also significant operational and reputation damages to the organisation.

Information disclosure: Network Sniffing [38]): In this scenario, the threat involves the unauthorised capture and analysis of network traffic. This is particularly effective against networks that transmit data in unencrypted formats or have weak security configurations. The key vulnerability lies in not securing the data in transit and the lack of robust network surveillance mechanisms. The impact of network sniffing can be significant as it may lead to the compromise of sensitive information, which can be used for further malicious activities.

Denial of service: Flooding(Denial of Service) [23][38] [34]: In this scenario, the attack aims to compromise the availability aspect of cybersecurity. Unlike other attacks that steal or corrupt data, flooding attacks are primarily about overwhelming system resources to cause service disruptions. Vulnerabilities in this context often involve inadequate preparedness for

Table 9. Security threat classification to STRIDE Taxonomy (2)

Article	Information disclosure	Denial of service	Elevation of privilege
Khalid *et al.* (2021) [23]	Eavesdropping.	Flooding (Denial of Service).	Physical destruction of IT Infrastructure.
Clark *et al.* (2017) [8]	Eavesdropping.	–	–
Quarta *et al.* (2017) [35]	–	–	Physical destruction of IT Infrastructure, Micro Defects Injection, Disabling or Altering Safety Devices, Unauthorized access to Systems and Data, Exploitation of Remote Network Vulnerabilities, Insider-Enabled Network Attack (Local access).
Jablonski *et al.* (2021) [21]	–	–	Physical destruction of IT Infrastructure, Theft and Cloning of Access Badges, Command Injection.
Chundhoo *et al.* (2021) [7]	Man-in-the-Middle Attack.	SYN Flooding, Barrage attack (combination of multiple attack vectors).	Sleep deprivation.
Shah *et al.* (2020) [38]	Network Sniffing, Eavesdropping, Man-in-the-Middle Attack, Side Channel attack.	Flooding (Denial of Service).	Reverse Engineering of Software or Hardware, Brute force attack, Replay attack, Phishing, Password attack.
Pu *et al.* (2023) [34]	–	Flooding (Denial of Service), Ransomware infection.	–

sudden spikes in network traffic, such as not having the scalable infrastructure or advanced threat detection and mitigation tools. The impact is significant, especially for businesses that rely heavily on online presence and services, as it directly affects their ability to operate and maintain customer trust. Addressing these risks requires a strategic combination of robust network architecture, real-time monitoring tools, and contingency planning for traffic overload scenarios.

Elevation of privilege: Physical destruction of IT Infrastructure [23][35][21]): In this scenario, the attack is characterised by physical actions that directly damage or destroy IT assets. This type of threat is often overlooked in cybersecurity planning, which tends to focus

more on digital threats. However, physical security is a critical aspect of overall IT security. Vulnerabilities typically stem from inadequate protective measures, such as insufficient physical barriers, surveillance, or access restrictions to sensitive areas. The impact of such an attack can be severe and immediate, affecting not only the hardware but also the data and services that rely on that hardware. Effective management of this risk involves robust physical security measures and comprehensive disaster recovery and business continuity planning to minimise the impact and ensure quick recovery in the event of such incidents.

6.3 Survey Results

In the survey, we considered whether there are any security risks that organisations experienced. It reports on 32 cases (see Fig. 14), where the most frequent is the Phishing attack followed by the virus and other threats.

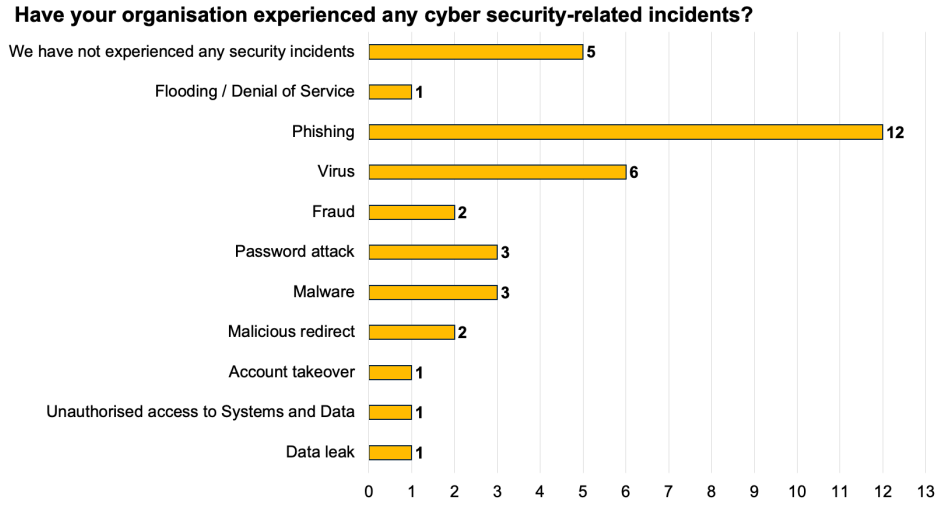

Figure 14. Security Threats as Indicated by Respondents

6.4 Discussion

In this chapter, we illustrate that security threats can be observed in different components of automated systems and technology. A good tool to guide such an analysis is the reference or architecture framework (e.g., RAMI 4.0), which suggests the potential system asset components and functional units. Another guidance can be provided by the information processing functions (i.e., capturing, transmitting, storing, retrieving, manipulating and displaying information). These functions represent the data and information processing perimeter, where the business assets (i.e., data and information) potentially change their form and state, and thus, are vulnerable and can be exploited by security threats.

It is important not only to identify the symptoms of the security threats. The organisations have to explore why the threat was possible (what the system vulnerabilities are), how the risk

constituted itself (what the attack method steps) and how it impacts the system (how it harms the system, business assets and negates security criteria).

The Study highlights an increasing trend among companies experiencing various cyber incidents, with most respondents identifying phishing attacks as a prevalent issue. Instances of virus or malware infections closely follow this. As organisations rely on IT systems and manufacturing processes become interconnected, the likelihood of facing a security event escalates.

The reliance on digital technologies and networked operations introduces vulnerabilities that cyber attackers exploit, emphasising the critical need for security countermeasures. The prevalence of phishing attacks underscores the importance of continuous employee training and awareness programs, as these threats target individuals through deceptive emails or messages[4].

[4]Find out more https://cyberphish.eu/learn

7 Security Countermeasures in Automated Systems and Technology

In this chapter, we present the security countermeasures found in the considered literature and survey. We recall that security risk treatment decisions include risk retention (i.e., the decision not to become involved with or to withdraw from a risk), risk transfer (i.e., the decision to share the burden of loss from a risk), risk avoidance (i.e., the decision not to become involved with or to withdraw from a risk), and risk reductions (i.e., actions to lessen the probability, negative consequence, or both associated with a risk). The latter decision results in the elicitation of security requirements and the implementation of security controls to mitigate the identified risks. In this chapter, we present security requirements and controls to mitigate the security risks of automated systems and technology.

7.1 Literature Review Findings

Building on the foundation laid by the STRIDE framework for threat identification and classification, we further employ STRIDE to guide the development of targeted countermeasures. These countermeasures are designed to address and neutralise the identified threats, ensuring a defence mechanism tailored to the specific security requirements. The strategies of risk reduction may vary depending on the type, specifics, complexity and domain of the automated systems and technology.

The threat-driven requirements elicitation approach supports security requirements categorisation into three groups – preventive (**P**), detective (**D**) and corrective (**C**). We annotate the elicited security requirements with P, D and C attributes. In the security requirements, the term "system" refers to the automated systems and technology (and their components).

In Table 10, the requirement and control to mitigate spoofing attack is presented. In considered literature, we observe one control, but potentially we acknowledge that other countermeasures (e.g., biometric authentication, credentials management policy, etc.) could potentially be alternatives for the multi-factor authentication. Fig. 18 presents a dependency among the information processing functions (i.e., information transmission), IP address spoofing and its countermeasure.

Table 10. Security Requirements [3] [4] and Controls to Mitigate Spoofing Risks

Security Requirements	**Security Controls**
SS1.R1: The system should authenticate user (P)	Multi-factor authentication [34]

Table 11 presents security countermeasures to mitigate tampering risks. The majority of security requirements requirement suggests the preventive security strategies (except for requirement ST3.R1 which implies the corrective security strategy). The identified security controls are encryption protocols for communication, hardware inspection, command whitelisting, utilisation of private networks and secure coding practices.

Countermeasures for mitigating information disclosure risks are listed in Table 12. Here, the majority of the strategies (except for the requirement SID2.R.2) focus on detective strategies.

Table 11. Security Requirements [3] [4] and Controls to Mitigate Tampering Risks

Security Requirements	Security Controls
ST1.R1: The system should use secure protocols for the provisioning of credentials (P). **ST1.R2**: The system should communicate with data storage via a channel protected by encryption protocol (P).	Encryption protocols for communication [8], [34]
ST2.R1: The system components should follow quality policy (P). **ST2.R2**: The organization should control physical access to transmission channels within organizational facilities (P).	Hardware Inspection [8]
ST3.R1: The system should conduct input data validation (C). **ST3.R2**: The system should define limitations to the user-provided data input (P). **ST3.R3**: The system interfaces should hide sensitive data during external communications (P). **ST3.R4**: The system should allow income traffic communications from the authorized sources (P).	Command whitelisting [41]
ST4.R1: The system should authenticate the device before establishing the connection (P). **ST4.R2**: The system should ensure the confidentiality of transmitted information (P). **ST4.R3**: The system should follow the wireless capabilities policies (P).	Utilisation of virtual private networks [34]
ST5.R1: The organization security personnel should conduct static code analysis before the system launch (P). **ST5.R2**: The organization security personnel should conduct dynamic program analysis for the launched system (P).	Secure coding practices [8]

Literature suggests applying payload detection solutions, anomaly detection alarms, and protocol health monitoring.

Table 12. Security Requirements [3] [4] and Controls to Mitigate Information Disclosure Risks

Security Requirements	Security Controls
SID1.R1: The security personnel should analyse system logs according to the log management policy (D).	Payload Detection Solutions [8]
SID2.R1: The system should identify unauthorised connections to the network (D).	Anomaly detection alarm [41]
SID3.R1: The system should verify the integrity of the transmitted data (D). **SID3.R2**: The system should protect the entire web sessions (P).	Protocol health monitoring [41]

To mitigate denial of service risk, preventive, detective and corrective security strategies can be applied as illustrated by the security requirements in Table 13. Hence the literature suggests the application of intrusion detection systems, numbering of the data packages over a short time, regular updates and patches, comparison of initiated and established TCP connections, traffic management and limitations, and regular backup generations.

Table 13. Security Requirements [3] [4] and Controls to Mitigate Denial of Service Risks

Security Requirements	**Security Controls**
SDS1.R1: The system should detect compromising the system boundaries (D).	Intrusion detection system [38]
SDS2.R1: The system should follow data management policy (C).	Number of data packets over short time scale [38]
SDS3.R1: The system should follow the policy of external systems quality (P). **SDS3.R2**: The system should remain integral after software updates (P). **SDS3.R3**: The system should execute only authorized programs (P).	Regular updates/patching [41], [38], [34]
SDS4.R1: The system should have a backup channel for communication (C).	Compare initiated and established TCP connections [38]
SDS5.R1: The system should use a channel protected by encryption protocol for remote managing (P). **SDS5.R2**: The system should balance incoming network traffic (C).	Traffic management and limitations [41], [38]
SDS6.R1: The system should use backups for recovering organizational information (P). **SDS6.R2**: The organisation should ensure data backups protection (P). **SDS6.R3**: The system should have central log management control (D). **SDS6.R4**: The system should conduct action logging on the system components (D). **SDS6.R5**: The system should maintain timestamps consistency of logs on system components (P).	Regular backups generation [34]

Table 14 lists the countermeasures to mitigate the elevation of privilege risks. The literature recommends two security controls: user screening and user access management. These security controls are achieved by implementing security requirements that mostly include preventive security strategies, except for requirements SEP1.R2 (corrective strategy) and SEP2.R4 (detective strategy).

The identified security countermeasures, after their implementations, became a part of the autonomous systems and technology. This means they become the system assets that support the

Table 14. Security Requirements [3] [4] and Controls to Mitigate Elevation of Privilege Risks

Security Requirements	Security Controls
SEP1.R1: The organization should follow user management policy (P). **SEP1.R2**: The system should separate different user roles (C). **SEP1.R3**: The system should authenticate data storage users (P). **SEP1.R4**: The system should protect displayed on the mobile device sensitive data (P). **SEP1.R5**: The system shall guide users to set particular configuration settings on the mobile devices used for interaction with the system (P).	User screening [38]
SEP2.R1: The system should implement an access control mechanism (P). **SEP2.R2**: The system should authorize access for data storage users (P). **SEP2.R3**: The system should store user credentials securely (P). **SEP2.R4**: The system should log access attempts to its interfaces (D).	User access management [38]

corresponding business assets. The organisation should continuously monitor their security level, and thus potentially identify and assess security risks of the added countermeasures.

7.2 Survey Results

The survey insights on countermeasures against security threats highlight a blend of strategies companies employ to secure their assets. As illustrated in Fig. 15, organisations use automated security solutions (10 answers), and cybersecurity is a responsibility of the IT department (10 answers). Employees participate in training and awareness programs (12 answers). The latter is also confirmed in Fig. 16, where online training courses and resources (8 answers) are used, regular cybersecurity training sessions for the employees (7 answers) are organised, and specialised training for IT and security staff (6 answers) are arranged. However, results also show that formal cybersecurity training is not provided in some organisations (8 answers).

The most popular controls to mitigate security incidents include regular software updates and patch management (15 answers), firewalls and intrusion detection/ prevention systems (14 answers), limitation of user privileges and access control (13 answers), and antivirus and anti-malware solutions (13 answers).

7.3 Discussion

Security risk treatment activities contribute to the prevention, detection and correction strategies to mitigate security risks. The first step, the organisation need to take, is the security treatment

Figure 15. Security-related Topics Handled Within Organisations

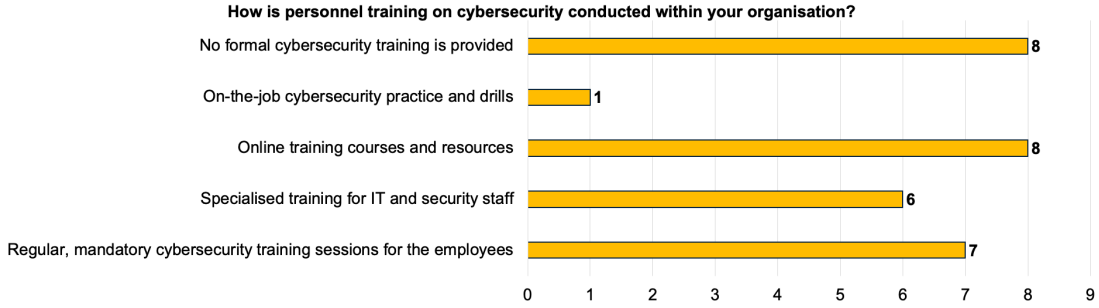

Figure 16. Training on Security in Organisations

decision. This includes risk retention, risk transfer, risk avoidance or risk reduction. The later decision contributes to the refinement of the security strategies to the security requirements and implementation of the security risks. In this chapter we highlighter security requirements and what security controls implement these requirements. In Figures 18–22 we explicit the dependency among the information processing function (system assets), security risks and threats and security countermeasures. These examples could potentially be considered as the checklist for defining security risk mitigation strategies.

The survey insights into countermeasures against security threats highlight a blend of strategies companies employ to safeguard their assets. An array of security measures has been integrated into the routine policies of organisations, underscoring the multifaceted approach necessary to combat cyber risks. Practices such as ensuring that IT systems are consistently updated to the latest versions and the implementation of user access controls are foundational actions mandatory across all sectors. These measures are pivotal for improving an organisation's security and mitigating vulnerabilities that cyber threats could exploit. In addition to these technical safeguards, the survey results emphasise the role of ongoing cybersecurity education for employees.

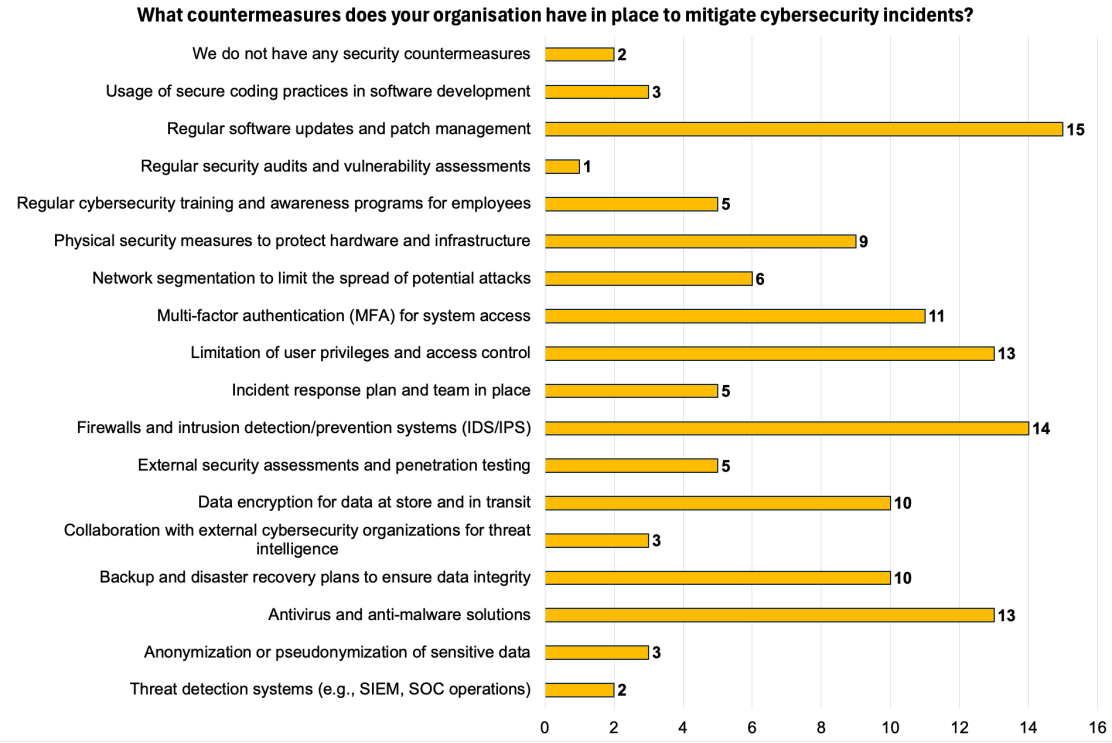

Figure 17. Countermeasures to Mitigate Security Events

Given the dynamic nature of the digital landscape, where technological advancements and threats evolve hand in hand, the importance of keeping the workforce informed and alert cannot be overstated. Regular training sessions create a culture of awareness, equipping employees with the knowledge to recognise and respond to potential security incidents effectively. This proactive approach to cybersecurity education is vital in addressing the increasing sophistication of targeted attacks, which often exploit human factors.

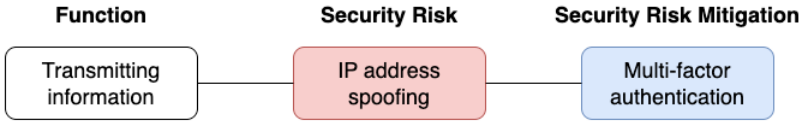

Figure 18. Dependency Among the Information Processing Function (System Assets), Spoofing Threat and Security Countermeasure

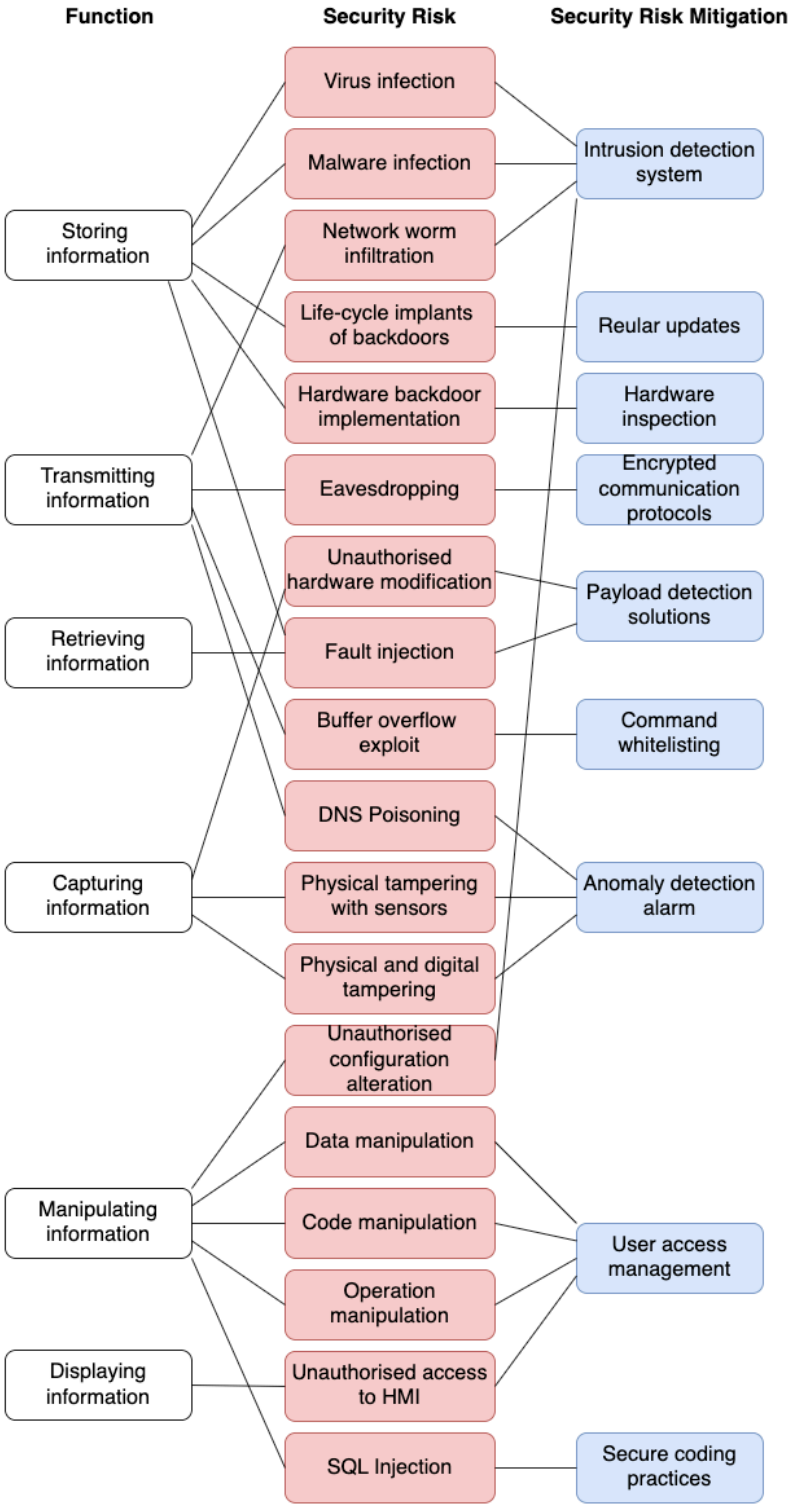

Figure 19. Dependency Among the Information Processing Functions (System Assets), Tampering Threats and Security Countermeasure

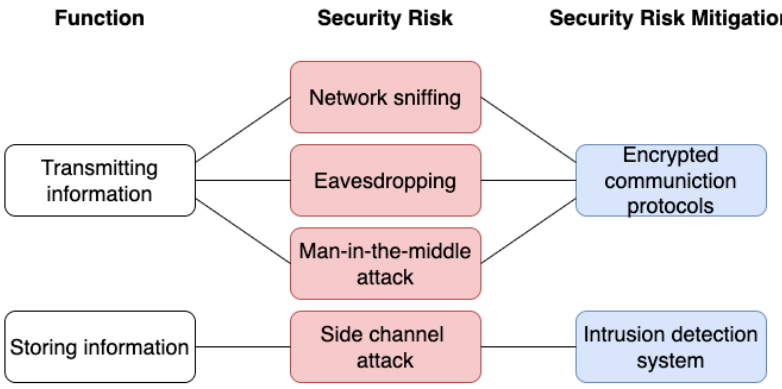

Figure 20. Dependency Among the Information Processing Functions (System Assets), Information Disclosure Threats and Security Countermeasure

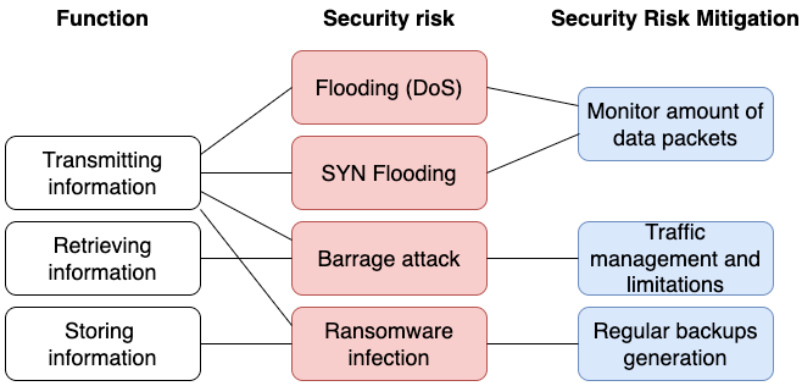

Figure 21. Dependency Among the Information Processing Functions (System Assets), Denial of Service Threats and Security Countermeasure

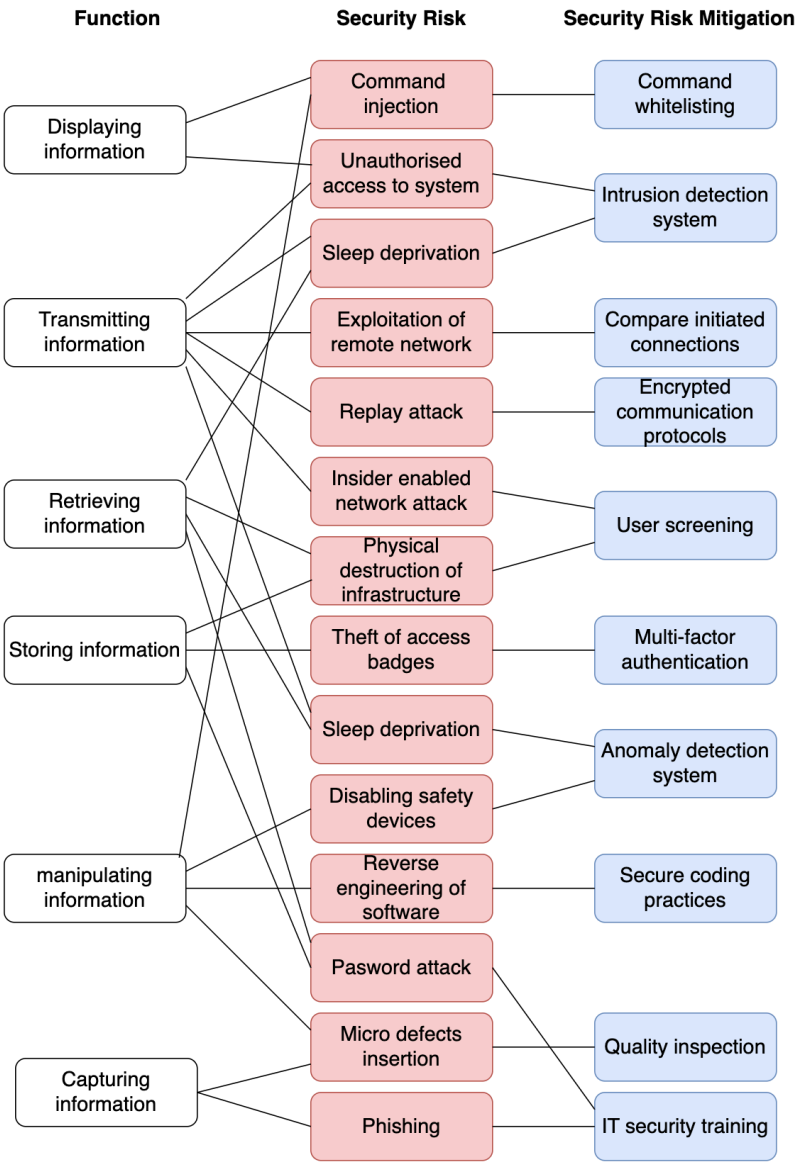

Figure 22. Dependency Among the Information Processing Functions (System Assets), Elevation of Privilege Threats and Security Countermeasure

8 Insider Security Risks in the Manufacturing Order Processing

This chapter recaptures a case study [28] from a medium-sized manufacturing enterprise employing approximately 80 people. The enterprise specialises in the precision CNC-machining (computer numerical control; i.e., highly automated machining tool, using programs generated in CAD – computer-aided design – or CAM – computer-aided manufacturing – tools) of complex metallic components for electric and motor devices. In this section, we illustrate how the ISSRM approach, presented in Chapter 2.1, could potentially carried out. Specifically, we focus on processes related to insider security threats. To support the analysis, the case scenarios are expressed using the business process model and notation (BPMN)[5].

8.1 Context Analysis

A scenario highlights the processes associated with receiving and fulfilling orders, with a particular emphasis on enhancing security measures. The main process of CNC machining order execution is presented in Fig. 23, and the production execution subprocess is illustrated in Fig. 24. The organisation utilises an enterprise resource planning (ERP) system to manage the lifecycle of orders, handling incoming, ongoing, and completed orders. Personnel (e.g., managerial staff and factory workers) across various levels perform data entry into the system. The manufacturing process data is stored on local servers. The storage system is devoid of any form of monitoring for reasons that remain unidentified.

The company has implemented a chip-based system for monitoring employee attendance to augment managerial oversight. This system furnishes management with insights regarding employee attendance patterns. The company also keeps track of incoming material. However, wasted material and failed products are not monitored once disposed of.

8.2 Industrial Espionage

Table 15 illustrates an analysis of assets, industrial espionage risk and the potential risk reduction solution.

Asset identification: In this scenario, data related to order processing (e.g., product designs and models) is kept on a storage server split into two main areas:

- The **management area** stores details about current orders, backups, and archives. Only the company's top management can access this area and its folders.
- The **manufacturing area** holds information for ongoing production orders, including product IDs, technical drawings, models, and quantities. This part is open to all company users.

[5]http://www.omg.org/spec/BPMN/2.0/

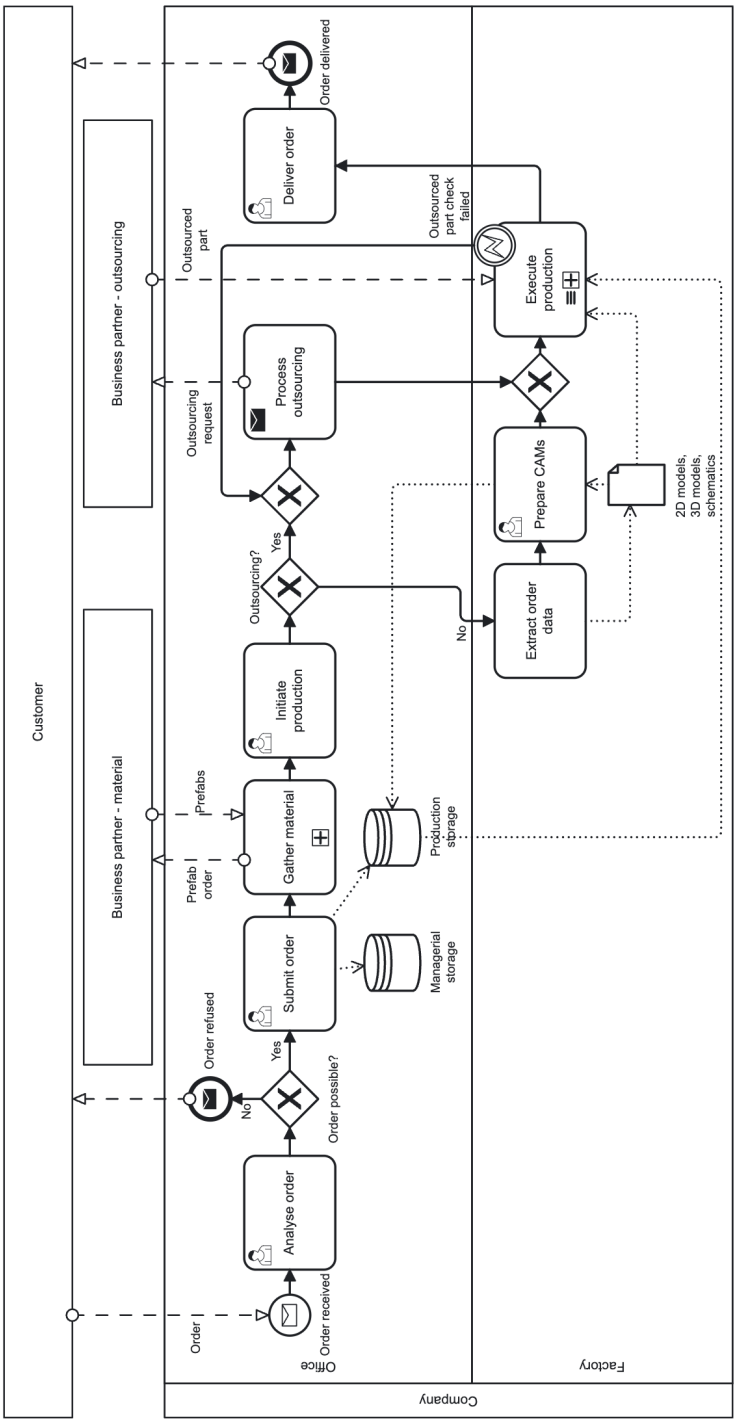

Figure 23. Order Processing Scenario, adapted from [28]

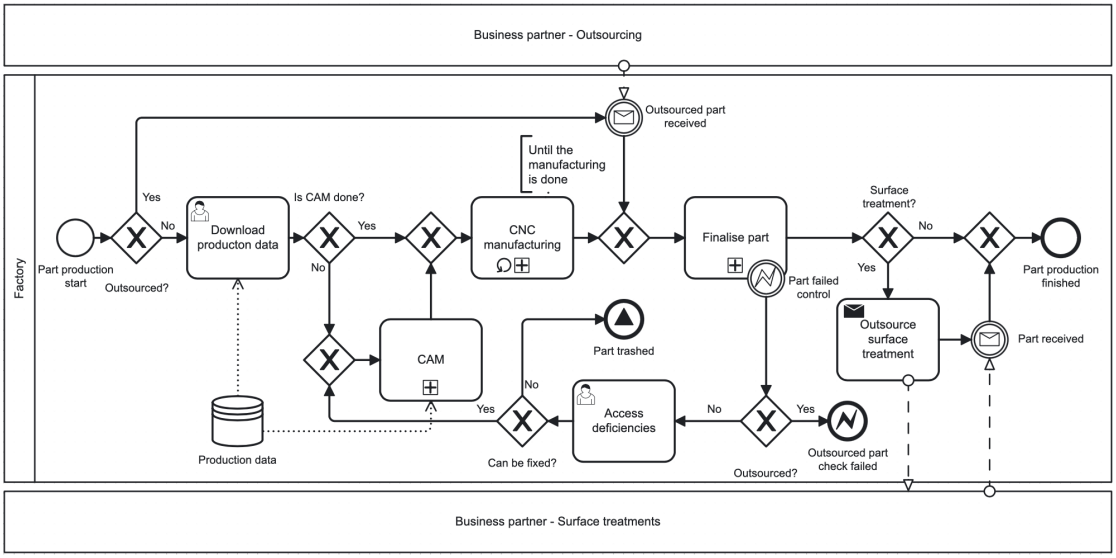

Figure 24. Production Execution Scenario, adapted from [28]

Table 15. Industrial espionage risk management, adapted from [28]

Business Asset	Schematics of products.
IS Asset	Production storage.
Risk	An insider with access to the company's production storage locates schematics of products in the company's storage and copies them to the insider's storage to exploit that access to the company's production storage is not properly monitored and analysed. This leads to the loss of data, its confidentiality and loss of storage server reliability.
Impact	Loss of data confidentiality, stolen data, loss of storage server reliability.
Vulnerability	Access to the company's data storage is not properly monitored and analysed.
Threat Agent	An insider with access to the company's production storage.
Attack method	An insider locates schematics of yet unreleased products in the company's production storage and copies them into the insider's storage.
Security Requirement	The security system shall generate a response to suspected industrial espionage.
Controls	Proper data storage monitoring setup, employee activity logging and process mining utilisation on the generated data.

Risk analysis: These settings result in sensitive information being available to anyone in the company or any outsider pretending to be an employee. As illustrated in Fig. 25 employees (i.e.,

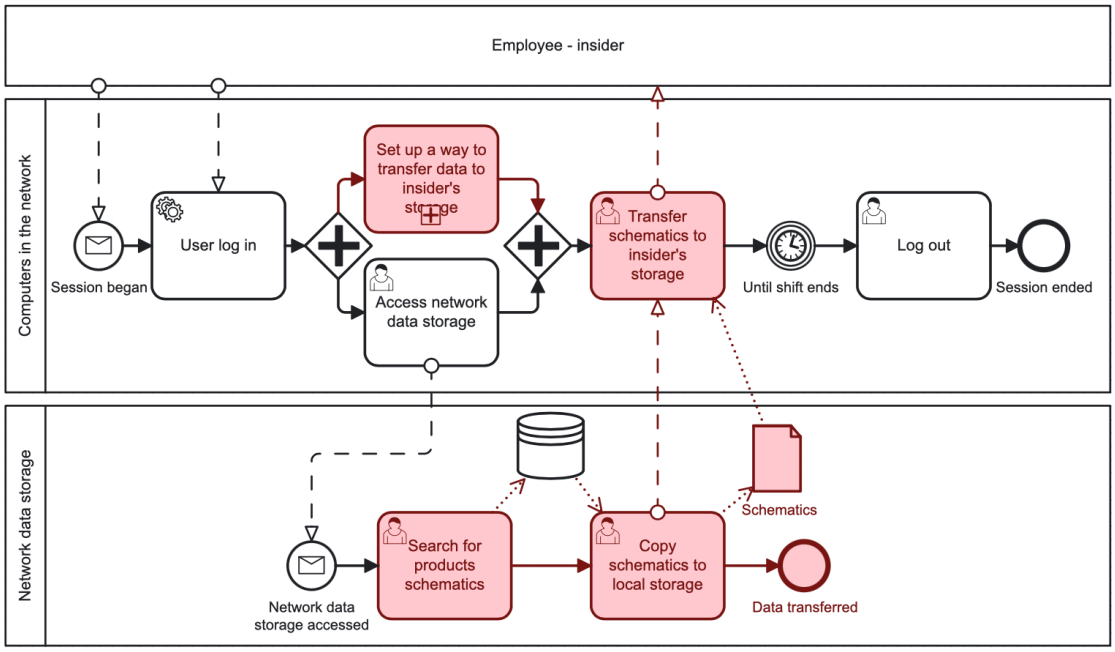

Figure 25. Industrial espionage risk model, adapted from [28]

insiders) could connect their device to the company's network or use a computer already on it, like one controlling manufacturing. From there, they might get into at least the manufacturing area and look for and take any valuable data they find.

Risk reduction: To mitigate industrial espionage, one should monitor storage storage, (especially the management and manufacturing areas). The system would track who accesses or changes files. By watching how files are used over time, we can learn the normal behaviour of employees and managers who use these directories. This information allows us to create profiles or models of typical user behaviour. Then, we can apply techniques that check if current activities match these expected patterns. This checking system would run on our company's servers, continuously watching for actions that don't fit the norm. If it finds anything unusual, it could decide on the best course of action, considering how risky the activity is and what harm it could cause.

8.3 Fraudulent Work

Table 16 illustrates assets, the fraudulent work risk and the potential risk reduction solution.

Asset identification: High-quality manufacturing typically adds a lot of value but comes at a high cost, including the machinery and the skilled workforce required. Employees, aware of the resources at their disposal, may take risks by bringing in external materials to use the company's time and equipment for personal projects or work for competitors, often without the knowledge of their employer or regulatory authorities. This practice undermines the company's interests and could be illegal.

Table 16. Fraudulent work risk management, adapted from [28]

Business Asset	Product process.
IS Asset	CNC machine, CNC machine storage, manufacturing control computer.
Risk	An insider responsible for the CNC production uploads custom production data into the CNC machine storage. Subsequently, they insert material they brought from the outside and create a product unrelated to the company's business interest. Using this approach, the insider takes advantage of the fact that the manufacturing control computer cannot obtain relevant information about active orders and the integrity of data uploaded to the CNC machine, resulting in the decreased overall accessibility and integrity of product manufacturing.
Impact	Overall accessibility and integrity of product manufacturing is decreased.
Vulnerability	Manufacturing control computer cannot obtain relevant information about active orders and whether the data uploaded to the CNC machine is valid.
Threat Agent	Insider responsible for the CNC production.
Attack method	An insider uploads custom production data into the CNC machine storage. The insider then inserts material they brought from the outside, and finally, the insider creates a product that is unrelated to the company's business.
Security Requirement	The security system shall detect unauthorised usage of the company's machinery.
Controls	Employee activity logging, monitoring of data transfers into the company's machinery, analysing the CNC machine native logs and process mining utilisation on the collected data.

Risk analysis: To carry out unauthorised work, as presented in Figure 26, someone looking to exploit the company's resources must bring in external materials to the production area. Next, they need to find a method to transfer their data into the company's system, aiming to get it directly onto a computer that controls manufacturing. Once they gain control over this computer, they can upload their specific production instructions, such as custom Computer-Aided Manufacturing (CAM) files, to the equipment, typically a CNC machine. After setting everything up, they use the machine as usual but with their data and materials, producing items that have nothing to do with the company's official products.

Risk reduction: Tracking how data is altered and noting information on active orders is crucial for in-depth analysis. By pairing this data with records from the company's equipment, it's possible to spot cases where employees might be working on projects that don't match any current orders, or at least trying to. However, this method isn't foolproof, as collecting activity data from all machinery can be challenging. The common issue is dealing with manual machinery

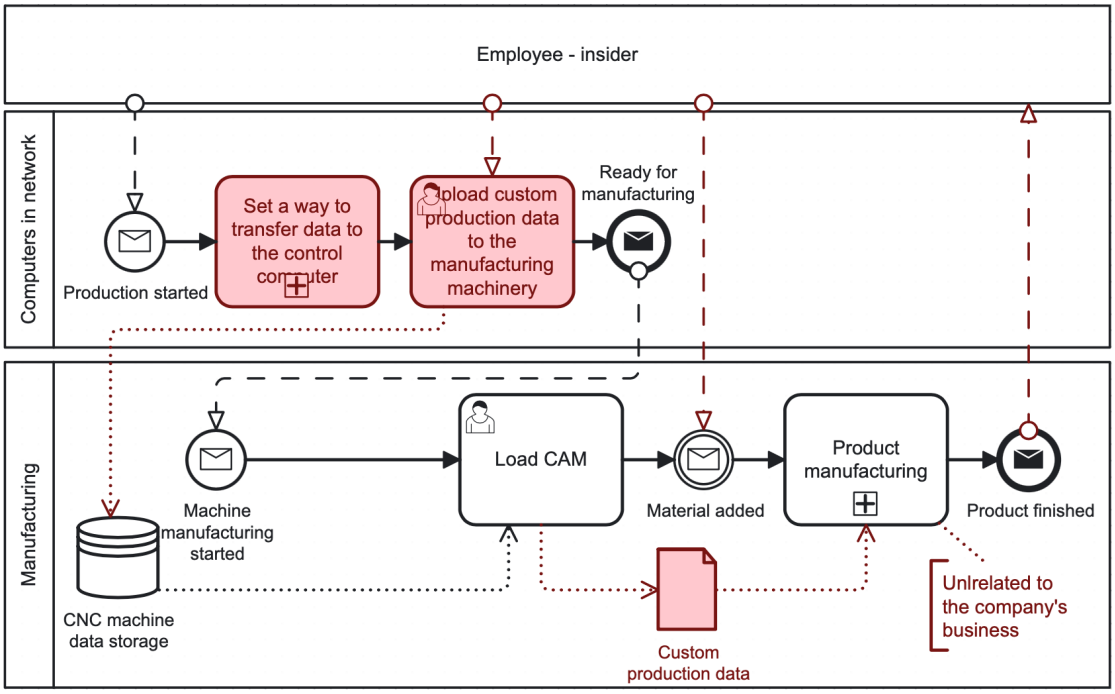

Figure 26. Fraudulent work risk model, adapted from [28]

that only automatically logs activity data.

We suggest using information from the attendance and ERP (Enterprise Resource Planning) systems to address these gaps. This includes details on product processing, the sequence of operations, and the time workers spend on each step, as reported by them and the production specialists. Although this data might be flawed due to how it's collected, it's still feasible to use process discovery techniques to outline a typical manufacturing workflow, including the average duration for each stage. Through conformance checking, we can pinpoint any significant discrepancies from this standard model, alerting managers to potentially suspicious activities that may warrant a closer look.

8.4 Intentional Sabotage

Table 17 illustrates an analysis of assets, intentional sabotage risk and the potential risk reduction solution.

Asset identification: As manufacturing becomes increasingly automated, the precision of production processes improves. Yet, this precision is accompanied by a rise in complexity and the delicate nature of these processes. If security measures are not robust, various components within the manufacturing environment could become targets for sabotage. Such sabotage could be the work of a disgruntled current employee, a competitor's insider, or a former employee seeking revenge.

Risk analysis: The consequences of such actions might include the corruption or deletion

Table 17. Intentional sabotage risk management, adapted from [28]

Business Asset	Prepared CAMs.
IS Asset	Production storage.
Risk	A disgruntled employee locates prepared CAMs and damages them to exploit that production storage is not properly monitored and analysed which results in a violation of the integrity of prepared CAMs.
Impact	The integrity of prepared CAMs is violated.
Vulnerability	Production storage is not properly monitored and analysed.
Threat Agent	A disgruntled employee.
Attack method	An insider locates prepared CAMs and damages them.
Security Requirement	The security system shall prevent unauthorised damage to prepared CAMs.
Controls	Proper data storage monitoring setup, employee activity logging and process mining utilisation on the generated data.

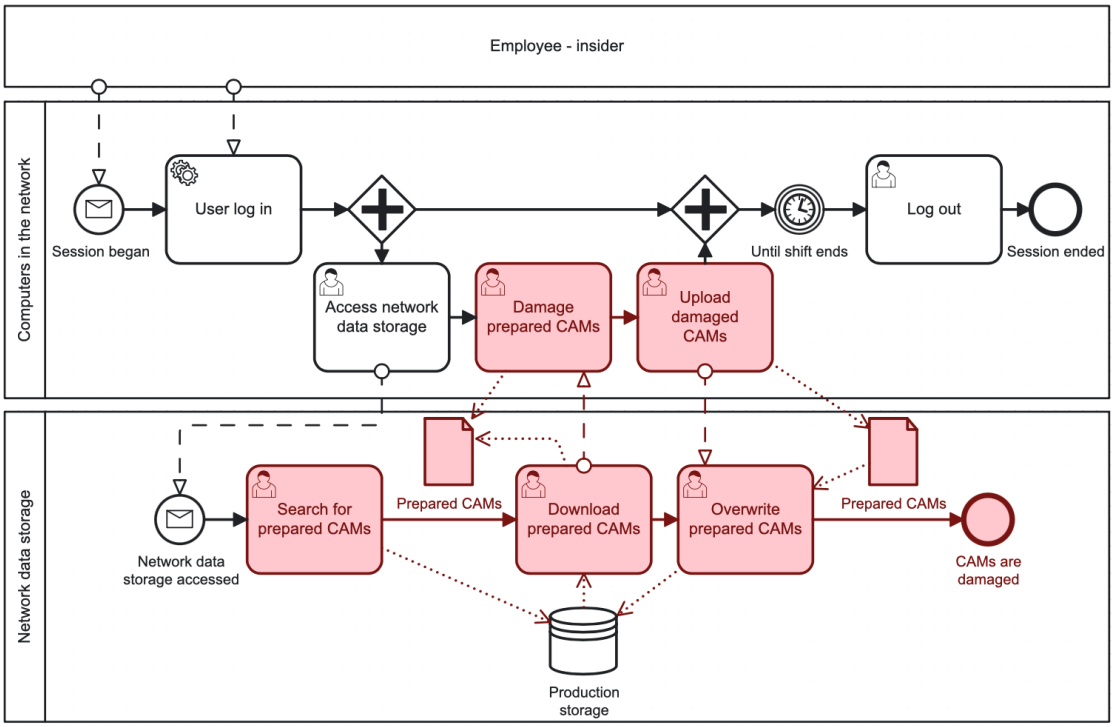

Figure 27. Intentional sabotage risk model, adapted from [28]

of critical data like CAM programs for CNC machines, details of active orders, or essential production software. It could also lead to physical damage to expensive machinery or the wastage of significant amounts of materials. These incidents cause direct damage and can lead to delays

in fulfilling orders. This, in turn, erodes customer trust and goodwill, potentially resulting in a substantial loss of revenue over time.

Sabotage exploits weaknesses in a company's IT infrastructure, much like those vulnerabilities highlighted in industrial espionage scenarios. However, sabotage attempts can be more wide-ranging, targeting a broader array of the company's systems. Once an attacker gains entry to any part of the IT network, they can proceed to sabotage.

For example, as presented in Figure 27, they might download CAM files intended for manufacturing from the company's data storage onto a compromised computer, tamper with or damage them, and then upload them back, replacing the original files in the production storage.

Risk Reduction: Just like in the industrial espionage scenario, keeping an eye on how data within the manufacturing and management sections is handled—this time focusing on additions, changes, and deletions—is crucial. This step would help us build or generate models of how employees interact with this data using process mining. We could then apply conformance checking to keep track of any new interactions with the data. Additionally, we could enhance our analysis by comparing the data storage activity logs with other information from the production process, such as details from the ERP software, attendance records, or logs from the production machines. This would not only aid in detection through process mining but also allow us to spot possible suspicious activities through signs like:

- Unusual patterns in employee check-ins regarding time and location,
- Unauthorised or unnecessary use of machinery,
- Starting production of items that aren't listed in the current orders on the ERP system,
- An unusually high rate of production failures that can't be fixed and
- Excessive amounts of wasted material.

By integrating and analysing this variety of data sources, we can more effectively identify and respond to potential security risks within our operations.

8.5 Unintentional Damage

Asset identification: While the effects of unintentional damage by an employee may look like those from industrial espionage or intentional sabotage, the behaviours leading up to such incidents often differ, given the high demand for skilled workers in manufacturing, firing an employee is generally seen as a last resort. It's crucial to figure out if the damage was intentional or resulted from an employee falling prey to social engineering, carelessness, or lack of familiarity with certain equipment or software, even though the outcomes might be hard to tell apart.

Risk analysis: The risk of unintentional damage can manifest in several ways, with the common factor being a well-meaning employee with legitimate access to the company's systems who either:

- Makes a spontaneous error while using the company's systems, such as shutting down machinery in a panic, leaving it in an unpredictable state. This can lead to damage to data, software, or the machinery itself.
- Gets deceived by someone outside the company into unwittingly helping them, for example, by following instructions over the phone that result in giving remote access to the company's systems or by responding to a phishing email, which hands over sensitive information to the adversary.

Risk reduction: Given the distinct outcomes of intentional versus unintentional damage, focusing on process analysis emerges as a natural approach to addressing this issue. Models representing unintentional mishaps are likely to appear more complex and erratic than those depicting intentional sabotage, which typically have clear, defined objectives from the start. Nonetheless, due to the relatively rare occurrence of unintentional damage events in manufacturing settings, accumulating sufficient data to construct models capable of distinguishing between these two types of incidents might require months or even years.

As an alternative strategy, we suggest gathering as much data as possible from the system's environment and storing it for a predetermined period. If the system designed to detect intentional sabotage flags any activity as suspicious, it could employ process discovery to create a one-off "enriched" model using all available data. This model could then be presented to management to decide whether the behaviour was deliberate. Over time, as the system accumulates data from past incidents, it could begin assigning confidence levels to whether an activity is likely to be intentional sabotage, refining its ability to discern between the two.

8.6 Lessons Learnt

In this chapter, we illustrated how a security risk management approach can be applied to elicit security risks in the manufacturing domain. Specifically, in this example, we targeted one particular type of security risk, namely insider risks. We stress that the organisation must estimate different security attack scenarios, including the security threats by the organisation's employees.

In this example, we consider four security risks - industrial espionage, fraudulent work, intentional sabotage, and unintentional damage. Potentially we can explicitly link these attacks to the protected assets, security risks and risk countermeasures discussed in the previous chapter. For instance, in the example, we discuss the application of the ERP system, which plays an important role at the Enterprise level of the RAMI 4.0 Hierarchy Level Axis. Industrial espionage risk targets the production storage, which potentially could be protected by implementing requirements for the user screening and/or user access management controls (see Table 14).

The presented case also illustrates that in the manufacturing processes, different business assets may exist and they could have different security needs. For instance, the confidentiality of information (i.e., the confidentiality of schematics of products) should be protected against industrial espionage risk; the integrity of the process (i.e., the integrity of the product process) should be protected against fraudulent work risk; and integrity of the production instrument (i.e., integrity of CAM) should be protected against the intentional sabotage risks. The example

illustrates that threat agents potentially may target different assets in the architectural hierarchy of the automated system and technology.

9 Analysis of STRIDE Security Threats in Manufacturing Company

As described in [26], Company X is a wood manufacturing enterprise based in Estonia, with a 20-year presence in the European market. Its product range expands with the annual introduction of new items. Operating within the furniture industry, Company X primarily serves large retail corporations, positioning its activities within the business-to-business (B2B) sector. Beyond its existing product lineup, Company X also provides design and development services, complemented by its production capabilities. Orders drive its production model—no inventory is produced in advance, and approved orders trigger production planning. In this chapter, we follow the STRIDE taxonomy (see Chapters 2 and 6) and analyse assets, risks, and their treatment in company X's processes.

9.1 Company Description

Company X oversees the operation of each supply chain unit, predominantly managing in-house processes. However, it occasionally resorts to outsourcing production efforts to accommodate demand fluctuations. Major trends impacting company X are

- **European Union's Green Growth Objectives:** These goals emphasise environmental sustainability, resource utilisation, and alignment with green economy principles.
- **Geopolitical Challenges:** The war crisis has compelled Estonian firms to seek alternative suppliers, impacting the import of roundwood and inflating costs.
- **Technological Advancements and Automation:** To stay competitive, the wood industry, including Company X, embraces automation and robotisation, aiming to enhance production efficiency.
- **Digital Transformation:** The adoption of digital tools, including AI, machine learning, and cyber-physical systems, revolutionises data processing and overall enterprise management.
- **Labour Shortage:** This ongoing issue is partially addressed by automation and digitalisation, yet the demand for skilled professionals persists. Promoting the industry's significance and the ecological benefits of wood is seen as a strategic move to attract talent.

Company X's business objectives are offering competitive pricing, ensuring that product quality meets established standards, guaranteeing on-time product delivery, maintaining short delivery periods, and facilitating rapid development of new products.

9.2 System Context

Company X uses the following software solutions:

- ERP system for resource planning,
- SolidWorks for design and engineering tasks,
- Internal software for product planning, and
- MS Office software for various operational tasks.

The value chain is depicted through key processes, as illustrated in Fig. 28, here each process is overseen by an assigned process owner responsible for its management and control. The interconnection between these processes is facilitated by exchanging inputs and outputs, ensuring a seamless flow of information for progressing to subsequent stages. Information systems such as ERP and production planning software are employed to bolster these main processes. Additionally, auxiliary tools like Excel and SolidWorks support these operations; Excel functions as a data transfer and processing tool. SolidWorks is primarily utilised for creating product models, assembly drawings, instructions, and packaging diagrams.

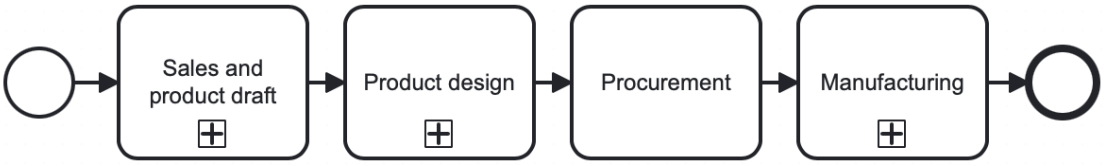

Figure 28. Company X main processes, adapted from [26]

Sales and Product Draft: Sales performs several functions (see Fig. 29): product development management, customer base management, master planning (long-term), and order management. When the company gets a request from a customer, the sales manager starts by examining the project to decide if it can be met with the existing product line or if new production elements need to be developed. Following this initial assessment, the sales manager negotiates pricing with the customer and drafts a manufacturing plan. The process only moves forward to begin manufacturing after the customer has made a prepayment, as indicated by the payment of a prepayment invoice.

Product design The product design process, depicted in Fig. 30, starts by analysing requests from the sales team. Once it is confirmed that the request can be made, necessary sub-folders and project file allocation may commence. during this process, it is wise to reuse as many already constructed details as possible, thereby minimising development costs and complexity. Nonetheless, there might still be occurrences of situations where new details need to be developed. In these cases, a sub-request is made to the product development team, where all the necessary schematics, manuals, and product descriptions are created and sent back. Once the necessary information is gathered, production baseline prices will be calculated and sent back to sales. In some cases, when a new product is being developed, a sample product may be produced, but due to this being rather an exception, this case is not depicted as a separate process.

Manufacturing: The manufacturing process can be divided into three sub-categories: (*i*) creation of manufacturing process for a new product, (*ii*) detailed planning, and (*iii*) production execution. Here, we focus on the production execution process (see Fig. 31)

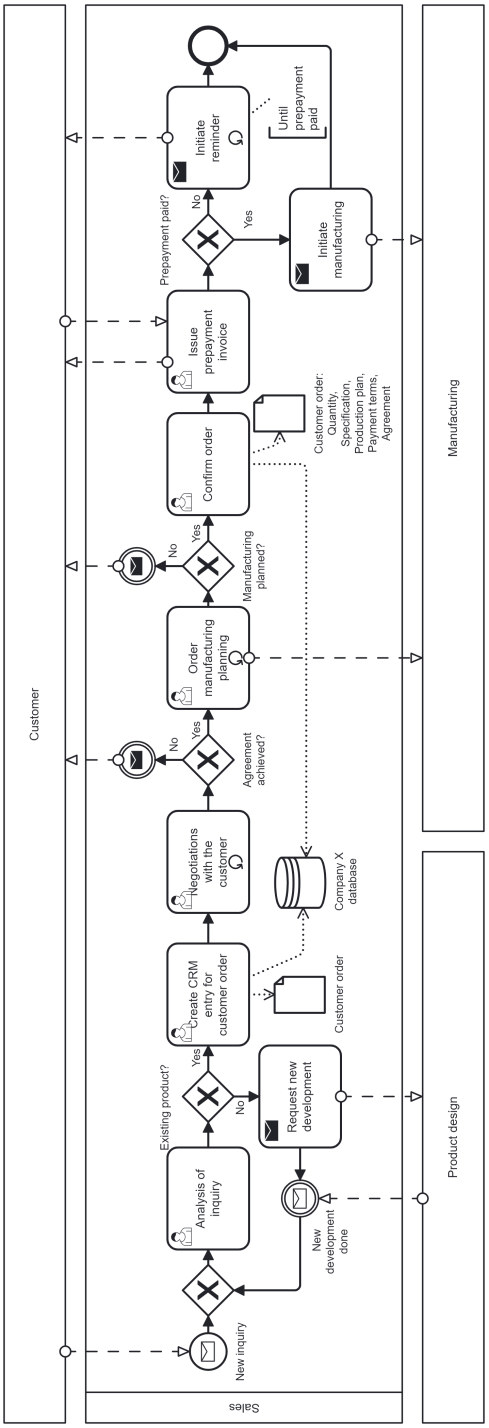

Figure 29. Sales process, adapted from [26]

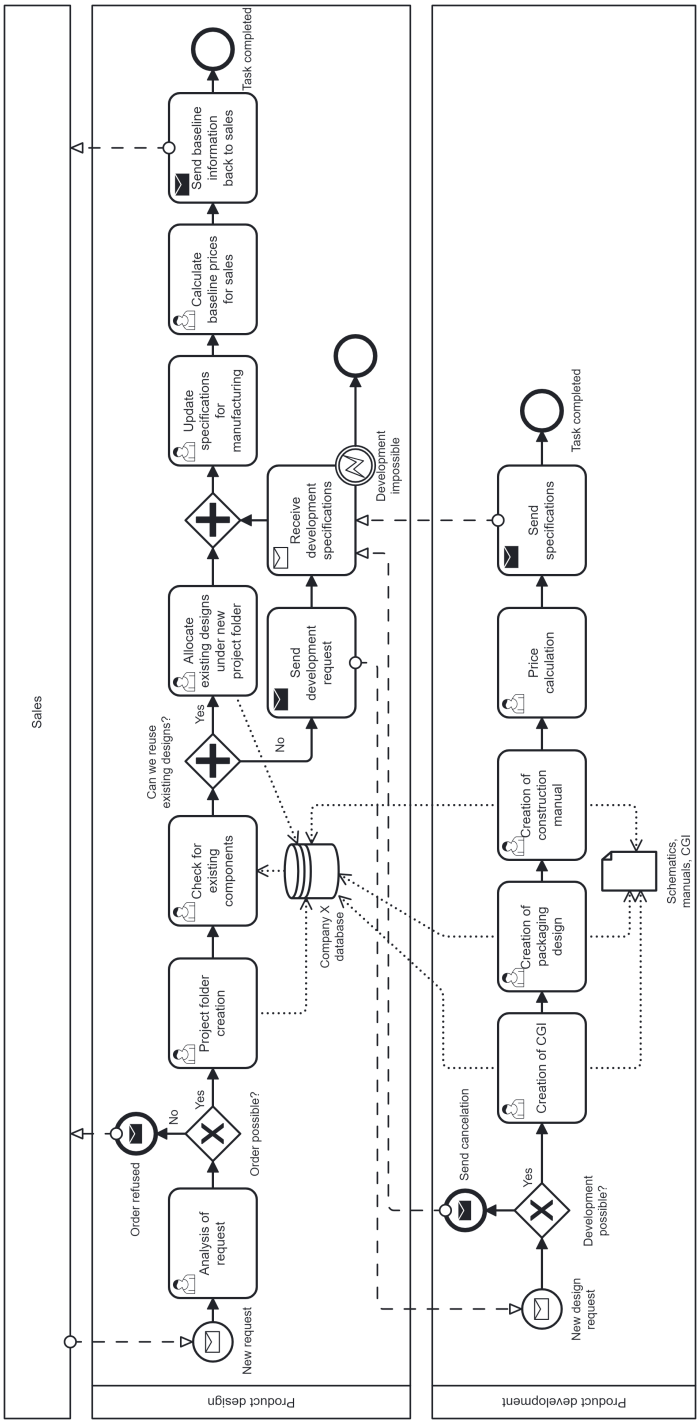

Figure 30. Product design process, adapted from [26]

A prerequisite for the start of manufacturing is the existence of metadata for the product. Manufacturing consists of various woodworking activities and starts with choosing a product profile. All products pass through Sawwing, Machine processing, CNC Machine cutting, Finishing works, and packaging. Some products require assembly. The process is finished with the dispatch request for delivery.

9.3 Security Risk Management

9.3.1 Spoofing

As defined in Section 2, spoofing means pretending to be something or someone other than yourself. For example, IP address spoofing represents a challenge, where an attacker masquerades as a trusted device by falsifying the IP address in packet headers. This technique is often employed to bypass IP address-based security measures, facilitating unauthorised access to networks or launching denial-of-service (DoS) attacks, often overwhelming the target with traffic from multiple spoofed sources.

In an enterprise network, the risk of IP address spoofing could stem from insufficient network perimeter defences or a lack of internal security practices, such as not employing packet filtering or validation mechanisms. Attackers could exploit these vulnerabilities to mimic internal devices, thereby gaining the ability to intercept, modify, or inject malicious data into the network's traffic. This could lead to data breaches, unauthorised data modification, and disruption of services, severely impacting the organisation's operations and credibility.

Table 18. Instance of IP Address Spoofing attack

Business Asset	Data sent using communication network.
IS Asset	Network infrastructure (Router, Switch, Wireless access points).
Risk	An attacker masquerades as a legitimate user or device by falsifying IP address information in their network packets, aiming to bypass IP-based security measures, impersonate other devices, or conduct a reflected attack.
Impact	Unauthorised access to network resources.
Vulnerability	Lack of network authentication protocols.
Threat Agent	An attacker with corresponding means.
Attack method	An attacker bypasses network security rules.
Security Requirement	The system must detect unauthorised remote connections.
Controls	Addresses insufficient remote connection rules by monitoring and analysing TCP connections to identify discrepancies between initiated and established connections, helping detect unauthorised access attempts.

Risk reduction: efforts against IP address spoofing must be multi-faceted. Implementing ingress and egress filtering on routers and switches can significantly reduce the risk of spoofed packets entering or exiting the network. Similarly, deploying network intrusion detection systems

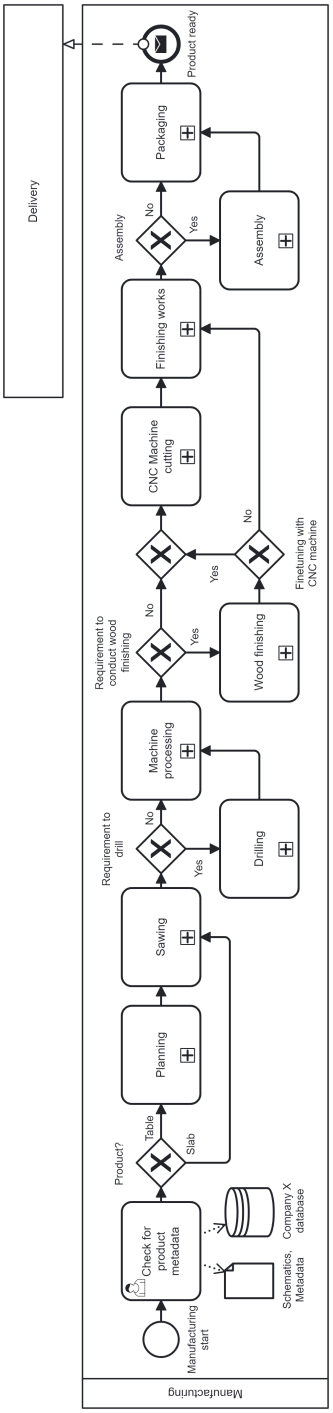

Figure 31. Manufacturing process, adapted from [26]

(NIDS) and intrusion prevention systems (NIPS) can help identify and block suspicious traffic patterns associated with spoofing. Additionally, embracing encryption protocols for sensitive data transmission and adopting secure authentication mechanisms can mitigate the impact of intercepted communications, ensuring that even if data is captured, it remains unintelligible to unauthorised parties.

Furthermore, educating employees about the risks associated with phishing emails or malicious websites, which could be part of a spoofing attack to install malware on internal devices, is crucial. Regularly updating and patching network devices and software to fix vulnerabilities is also key to protecting against this threat.

To conclude, IP address spoofing poses a risk to network security, requiring a strategy that includes technical defences, employee awareness, and security policies to detect, prevent, and respond to these threats.

9.3.2 Tampering

Tampering means modifying something on a disk, network, memory, or any device. In Chapter 6, we have identified 18 tampering threats. In the case of Company X, multiple threats could be considered. Since the company heavily relies on pre-created product schematics, the **Data Manipulation** threat becomes the most influential threat and should be taken more seriously. The scenario in Fig. 32 highlights the threat posed by data manipulation, ranging from minor tweaks to complete fabrications of product designs. An attacker, for instance, can use phishing to get access to companies' systems. This way, the attacker is capable of altering data, which is confirmed for production and will not be double-checked. The manufacturing process is directly damaged as the first realisation that something is going wrong will come only during or even after everything is manufactured.

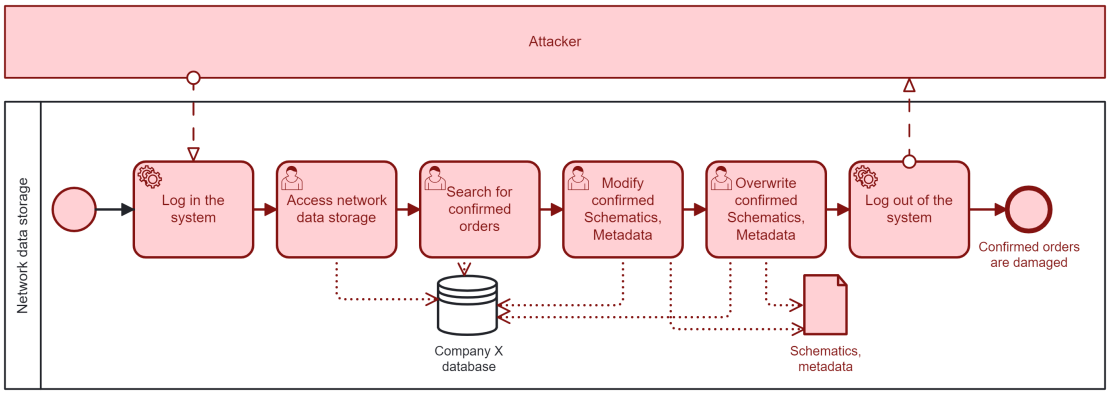

Figure 32. Data Tampering Scenario

Such unauthorised changes can lead to problems, including production errors, financial losses, and a loss of customer trust. The organisation's current approach, allowing all employees access to these schematics, increases the risk of accidental and deliberate data manipulation. Malicious individuals, whether they are insiders with harmful intentions or outsiders who've

gained access through security weaknesses, could modify these designs. Their motives might vary from disrupting the company's operations to giving competitors an edge or stealing intellectual property.

Table 19. Instance of Data Manipulation attack

Business Asset	Data stored in the database.
IS Asset	Database.
Risk	An attacker subtly alters critical data within a system or in transit to corrupt information, undermine decision-making processes, or achieve financial gain.
Impact	Data integrity is corrupted.
Vulnerability	Lack of access controls.
Threat Agent	An attacker with corresponding means.
Attack method	An attacker gets access to product schematics and alters them.
Security Requirement	User access policies must be established and enforced, regulating user access rights.
Controls	Counteract inadequate access controls to software, systems and data by implementing policies and systems that manage and monitor user permissions, ensuring only authorised personnel can access.

Risk reduction: to mitigate these threats, a defensive strategy is needed. Implementing access controls and assigning permissions based on roles can significantly reduce risks, ensuring that only employees who need access to their work can make changes. Moreover, deploying monitoring technologies can help identify unauthorised or unusual activities with the data. These systems would monitor how data is accessed and changed, alerting to any unusual patterns.

Additionally, using digital watermarking for product schematics can help trace and authenticate files, making it easier to spot any manipulations. Regular audits of data access and changes, combined with training programs to educate employees about the importance of data security and the risks associated with manipulation, will strengthen the company's defence against these threats.

9.3.3 Information Disclosure

Information Disclosure means providing information to someone not authorised to access it. Considering Company X's digitisation, the risk of Man-in-the-Middle (MitM) attacks is rather high. In such attacks, a hacker intercepts and may alter the communication between two unknowing parties. This threatens Company X, especially during data transfer within its supply chain and in dealings with major retail partners. Uninterrupted information flow is crucial, from analysing customer requests to dispatching final deliveries. A MitM attack could disrupt communication, for example, during negotiations between sales managers and clients, where altered terms or fraudulent payment instructions could be injected, as depicted in Fig. 33. Likewise, exchanges between sales, product development teams, and external partners during design phases are at risk,

with the potential for altered specifications or stolen proprietary designs, leading to financial loss or production sabotage.

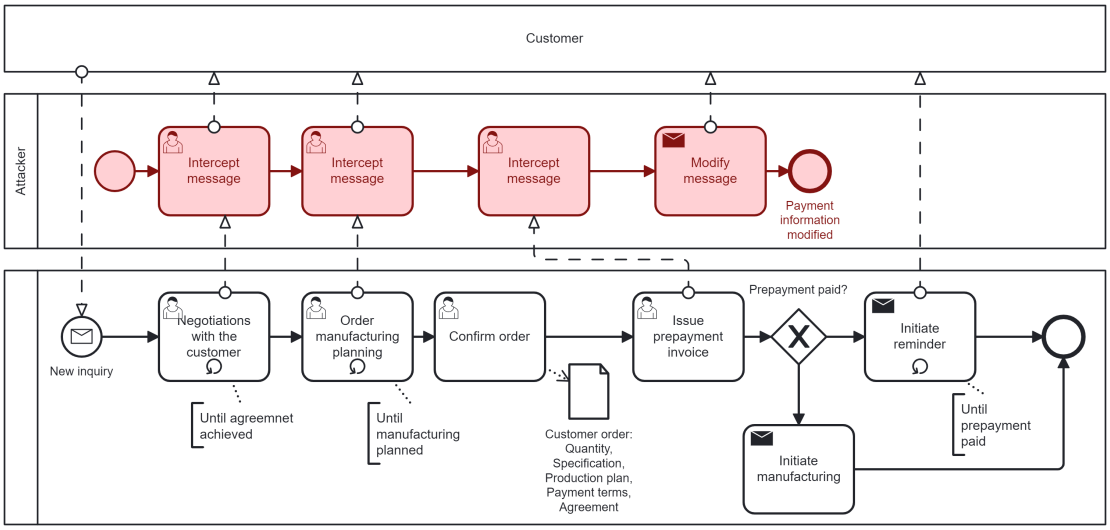

Figure 33. Man-in-the-Middle attack scenario

The process of issuing and paying prepayment invoices is another vulnerable area. Hackers could redirect payments to fake accounts by intercepting invoice communications. In Company X's B2B context, such fraud could gravely impact financial health and business relations.

Risk reduction: can be done by encrypting data in transit, authenticating users, and continuously monitoring for unusual network activity. Training staff on cybersecurity awareness and securing communication channels are also vital. These actions will protect Company X's digital interactions, ensuring trust and operational reliability.

Table 20. Instance of Man-in-the-middle attack

Business Asset	Data in transit.
IS Asset	Communication Network.
Risk	An attacker intercepts and potentially alters the communication between two parties without their knowledge.
Impact	Data confidentiality and integrity is corrupted.
Vulnerability	Unsecured and/or unencrypted communication channels.
Threat Agent	An attacker with corresponding means.
Attack method	An attacker intercepts communication channels.
Security Requirement	All digital data transmissions must be encrypted.
Controls	Ensure any communication in transit is secure and encrypted, preventing unauthorised access and data breaches.

9.3.4 Denial of Service

Denial of Service means exhausting resources needed to provide service. For example, the Flooding attack poses a threat to operations. This attack strategy floods the company's network or systems with excessive traffic, rendering it unable to process legitimate requests. Such disruptions could impede Company X's supply chain, delay production, and disrupt communications with retail partners, harming its business operations.

Company X's reliance on a digital framework for its B2B activities, from receiving orders to planning and delivering production, makes it vulnerable. Critical systems like ERP for resource planning and SolidWorks for product design are essential for daily operations. An attack on these systems could cause substantial operational delays, affecting everything from order processing to dispatching finished products. With Company X's manufacturing model based on confirmed orders, any production delays could lead to contract violations, financial penalties, or lost business.

The threat isn't just external; it could also stem from compromised internal systems or IoT devices within the company's network. For instance, if a device in the production line were hacked to join a Flooding attack, it could affect operational efficiency.

Table 21. Instance of Flooding (Denial of Service) attack

Business Asset	Availability of operational services.
IS Asset	Network infrastructure.
Risk	An attacker overwhelms the organisation's network resources or services with excessive traffic.
Impact	Loss of service availability.
Vulnerability	Insufficient network bandwidth; Lack of filtering mechanisms.
Threat Agent	An attacker with corresponding means.
Attack method	An attacker overflows the organisation's resources with excessive traffic.
Security Requirement	The system must implement real-time intrusion detection mechanisms for monitoring the flow of data packets.
Controls	Address lack of rate limiting or request filtering on devices by monitoring the flow of data packets in short time frames to quickly identify and respond to potential DDoS attacks or other malicious activities.

Risk reduction: to counter such risks, Company X needs to adapt intrusion detection systems to regulate incoming traffic. Utilising traffic analysis tools and implementing rate limiting can aid in spotting and addressing abnormal traffic patterns early. Establishing backup systems and network pathways can help keep the company operational during an attack.

9.3.5 Elevation of Privilege

Elevation of Privilege means allowing someone to do something they are not authorised to do. In Chapter 6 we identified 14 elevation of privilege threats. Considering the general scale of

manufacturing companies, the risk of **Micro Defects Injection** presents a complex challenge. This threat involves intentionally introducing subtle flaws into product designs or manufacturing processes. Such tampering could drastically undermine the integrity and longevity of the finished products, resulting in reputation harm, financial setbacks, and safety concerns.

Company X's success relies on an integrated supply chain and the use of digital solutions like ERP for resource planning and SolidWorks for product design. The company's practice of initiating production exclusively based on confirmed orders underscores the need for precision and dependability in every unit produced. In this context, Micro Defects Injection could be realised through tampered digital files or malevolent modifications to design schematics on the company's data server. The digital-centric nature of design and development makes such alterations particularly subtle, as they could be introduced and propagated through the production cycle without immediate detection.

Potential points for the injection of micro defects include:

- **Design Phase:** Tampering with SolidWorks files to embed flaws in the product designs.
- **Production Planning:** Altering ERP data to change manufacturing parameters or material specifications.
- **Manufacturing Execution:** Tweaking CNC machine programming to deviate from the original designs.

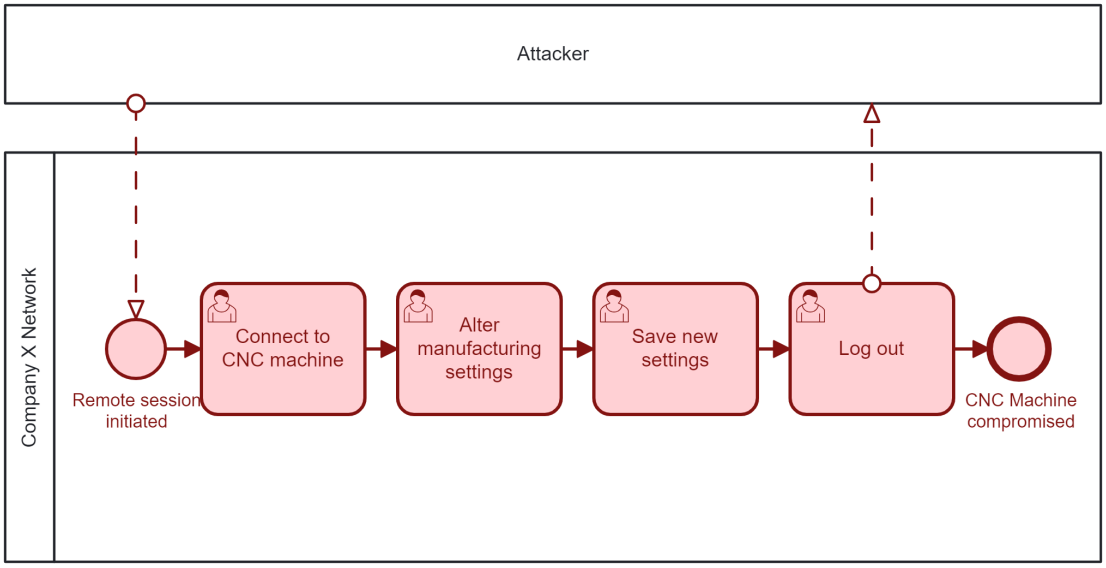

Figure 34. Micro Defects Injection attack scenario

Computer Numerical Control (CNC) machining is a manufacturing method where computer software that has been pre-programmed controls the movement of factory equipment and tools. This technique allows for the operation of various complex machines, including grinders, lathes,

mills, and CNC routers. CNC machining enables the execution of three-dimensional cutting tasks through a single sequence of commands. Configuration changes can be subtle yet bring along long-lasting quality defects, which are unseen by the eye and only come forth after quality checks or through a certain amount of use. As depicted in Figure 34, an attacker could remotely connect to a CNC machine and alter quality metrics or, even worse, safety settings. As stated in [5] "*A user (or a process) is often given full access to any system's resource, including its file-system or memory locations. For example, an application written on top of THINC-API will have full access permission to any system's resource including the internal controller configurations; with Ethernet Q, a remote user can write to memory locations mapped outside of the running process.*"

Risk reduction: includes implementing digital security to prevent unauthorised access and manipulation of design and manufacturing data. This includes access control mechanisms, audit checks of digital files, data encryption and quality checks of produced deliverables. Moreover, quality assurance measures can identify and correct deviations from product standards early on. Detailed reviews of design and production processes and analytical methods can spot anomalies suggestive of micro defects.

Promoting a culture of awareness and openness encourages staff to be alert to potential security issues or suspicious behaviour. At the same time, ongoing cybersecurity education emphasises everyone's role in maintaining the company's operational and reputational integrity.

Table 22. Instance of Micro Defects Injection attack

Business Asset	Deliverables.
IS Asset	Production machinery.
Risk	An attacker introduces microscopic defects into components during manufacturing or maintenance.
Impact	Loss of integrity for producible deliverable.
Vulnerability	Lack of inspection and testing protocols for components.
Threat Agent	An attacker with corresponding means.
Attack method	An attacker injects micro defects through CNC machine operations.
Security Requirement	The organisation must establish quality inspection and testing protocols.
Controls	Examination of components for any deviations in quality that could compromise the product, ensuring integrity.

9.4 Lessons Learnt

In this Chapter, we presented the manufacturing company, its sales and product draft, product design and manufacturing activities. Firstly, we illustrate that this company faces similar challenges as discussed in Chapter 3, including geopolitical, technological and digital transformation and labour shortage. Secondly, we illustrate the utility of the STRIDE taxonomy to guide security risk management. Although in the example we illustrate five security risks, the STRIDE classification can draw analysts' attention to different security concerns in the organisation.

10 Concluding Remarks

In manufacturing, automated systems and technologies have evolved into complex, field-specific systems containing interconnected frameworks of Industry 4.0. This development underscores the critical need for contemporary security measures to ensure secure and reliable workflows.

In this report, the information systems security risk management (ISSRM) approach is used to explain the context, assets, security risks and their countermeasures in the automated systems and technology. The ISSRM domain model guides a systematic identification of the supporting and protected assets and security needs. It also defines a security risk as a combination of the threat agent, attack method, vulnerabilities and impact. The domain model is used in the interviews, systematic literature review and survey performed in the Estonian organisations.

The collected data is used to identify challenges in manufacturing organisations that use automated systems and technology. The main challenge is defined as data and information security. Empirical validation of these findings was achieved through interviews with manufacturing companies, which revealed that despite well-defined security measures for systems and machinery, human personnel often represent a vulnerability in the security chain. This report emphasises the use RAMI 4.0 as a domain-agnostic reference architecture, which is applicable across various manufacturing domains. Through the lens of RAMI 4.0, it is possible to identify business assets and supporting system assets that might be vulnerable to security threats.

The STRIDE taxonomy is used to explore what the security threats are in automated systems and technology. The analysis of the literature identifies 43 security threats that are systematically elaborated using the ISSRM risk definition. The majority of the risk is related to tampering and elevation of privileges. The study did not result in any risk of repudiation. The security countermeasures, including the security requirements and controls, are elaborated to mitigate the identified security risks. Survey results also suggest that organisations apply not only technical countermeasures but also organise or participate in security training, and onsite and online courses.

The literature review highlighted a gap in existing security standards, which predominantly focus on system safety rather than comprehensive security protocols.

The discussed use cases illustrate how security risk management could be performed in manufacturing organisations. It is important to explain that security events can happen not only from outside the organisation. Companies need to explore insider threats, too.

The conducted research paves the way for more detailed follow-up analyses. Delving deeper into the specific data types and processes governing manufacturing operations is vital to identifying potential attack vectors and developing effective mitigation strategies accurately. While RAMI 4.0 provides a standardised framework, its practical implementation within the industry warrants further exploration. Thus, a follow-up research is necessary to ascertain if security measures tailored to RAMI 4.0 exist how they are applied in practical scenarios and what the other security risks of the modern manufacturing processes are.

References

[1] Hasnaa Ait Malek, Alain Etienne, Ali Siadat, and Thierry Allavena. A Literature Review on the Level of Automation and New Approach Proposal. In Bojan Lalic, Vidosav Majstorovic, Ugljesa Marjanovic, Gregor Von Cieminski, and David Romero, editors, *Advances in Production Management Systems. The Path to Digital Transformation and Innovation of Production Management Systems*, volume 591, pages 408–417. Springer International Publishing, Cham, 2020. Series Title: IFIP Advances in Information and Communication Technology.

[2] Steven Alter. *The Work System Method: Connecting People, Processes, and IT for Business Results*. Work System Method, 2006.

[3] Mariia Bakhtina. Securing Passenger's Data in Autonomous Vehicles. Master's thesis, University of Tartu, 2021.

[4] Mariia Bakhtina and Raimundas Matulevičius. Information Security Risks Analysis and Assessment in the Passenger-Autonomous Vehicle Interaction. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 13(1):87–111, 2023.

[5] Marco Balduzzi, Francesco Sortino, Fabio Castello, and Leandro Pierguidi. A Security Analysis of CNC Machines in Industry 4.0. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 132–152. Springer, 2023.

[6] Center for Internet Security. CIS Critical Security Controls.URL: *https://www.cisecurity.org/controls* (last checked: 15.04.2024), 2024.

[7] Vickram Chundhoo, Gopinath Chattopadhyay, Gour Karmakar, and Gayan Kahandawa Appuhamillage. Cybersecurity Risks in Meat Processing Plant and Impacts on Total Productive Maintenance. In *2021 International Conference on Maintenance and Intelligent Asset Management (ICMIAM)*, pages 1–5, Ballarat, Australia, December 2021. IEEE.

[8] George W. Clark, Michael V. Doran, and Todd R. Andel. Cybersecurity Issues in Robotics. In *2017 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)*, pages 1–5, Savannah, GA, USA, March 2017. IEEE.

[9] Cybernetica AS. AKIT: Andmekaitse ja Infoturbe portaal, URL: *https://akit.cyber.ee/* (viimati kontrollitud: 30.04.2024), 2023.

[10] Dr. Karsten Schweichhart. Reference Architectural Model Industrie 4.0 (RAMI 4.0), 2016.

[11] Éric Dubois, Patrick Heymans, Nicolas Mayer, and Raimundas Matulevičius. *A Systematic Approach to Define the Domain of Information System Security Risk Management*, pages 289–306. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[12] EAS, Enterpise Estonia. Väike- ja keskmise suurusega ettevõtja (vke) definitsiooni selgitus vastavalt euroopa komisjoni määruse 800/2008/eÜ lisa 1-le, 2009.

[13] Europian Union. General Data Protection Regulation. URL: *https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04* (last checked: 15.04.2024), 2016.

[14] Donald Firesmith. Engineering Safety and Security Related Requirements for Software Intensive Systems. In *ICSE Companion*, page 169, 2007.

[15] J. Frohm, V. Lindström, and M. Winroth. Levels of Automation in Manufacturing. *Int. J. Ergon. Hum. Factors*, 30(19), 2008.

[16] Ganji, D. and Mouratidis, H. and Gheytassi, S.M. Towards a Modelling Language for Managing the Requirements of ISO/IEC 27001 Standard. In *In Proc. of the 5th International Conference on Advances and Trends in Software Engineering (SOFTENG'19)*, pages 17–23, 2019.

[17] Information System Authority. Cyber Security in Estonia 2023, URL: *https://www.ria.ee/en/media/2702/download* (last checked: 15.04.2024), 2023.

[18] ISA Standards and Publications. ISA/IEC 62443 Series of Standards. URL: *https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards* (last checked: 15.04.2024), 2024.

[19] ISO, Organization for Standardization. ISO/IEC 27000 Family, Information Security Management. URL: *https://www.iso.org/standard/iso-iec-27000-family* (last checked: 15.04.2024), 2024.

[20] Ugalde J. 15 Technology Challenges Businesses May Face in 2023. URL: *https://www.systems-x.com/blog/technology-challenges-businesses-face* (last checked: 15.04.2024).

[21] Matthew Jablonski, Bo Yu, Gabriela Felicia Ciocarlie, and Paulo Costa. A Case Study in the Formal Modeling of Safe and Secure Manufacturing Automation. *Computer*, 54(9):59–71, September 2021.

[22] Jan Kaiser, Duncan McFarlane, Gregory Hawkridge, Pascal André, and Paulo Leitão. A Review of Reference Architectures for Digital Manufacturing: Classification, Applicability and Open Issues. *Computers in Industry*, 149:103923, August 2023.

[23] Azfar Khalid, Zeashan Hameed Khan, Muhammad Idrees, Pierre Kirisci, Zied Ghrairi, Klaus-Dieter Thoben, and Jürgen Pannek. Understanding Vulnerabilities in Cyber Physical Production Systems. *International Journal of Computer Integrated Manufacturing*, 35(6):569–582, June 2022.

[24] Barbara Kitchenham, O. Pearl Brereton, David Budgen, Mark Turner, John Bailey, and Stephen Linkman. Systematic Literature Reviews in Software Engineering – A Systematic Literature Review. *Information and Software Technology*, 51(1):7–15, January 2009.

[25] Tobias Kutzler, Alexandra Wolter, Andy Kenner, and Stephan Dassow. Boosting Cyber-Physical System Security. *IFAC-PapersOnLine*, 54(1):976–981, 2021.

[26] Laanemets, Hendrik. Normeerimise ja marsruudi loomise kontseptsioon ettevõtte x näitel, 2023.

[27] J. Lane Thames. Distributed, Collaborative and Automated Cybersecurity Infrastructures for Cloud-Based Design and Manufacturing Systems. In Dirk Schaefer, editor, *Cloud-Based Design and Manufacturing (CBDM)*, pages 207–229. Springer International Publishing, Cham, 2014.

[28] Martin Macak, Radek Vaclavek, Dasa Kusnirakova, Raimundas Matulevičius, and Barbora Buhnova. Scenarios for Process-Aware Insider Attack Detection in Manufacturing. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ARES '22, New York, NY, USA, 2022. Association for Computing Machinery.

[29] Raimundas Matulevičius. *Fundamentals of secure system modelling*. Springer, 2017.

[30] Microsoft. Microsoft Security Baselines. URL: *https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines* (last checked: 15.04.2024) , 2024.

[31] Akseer Ali Mirani, Gustavo Velasco-Hernandez, Anshul Awasthi, and Joseph Walsh. Key Challenges and Emerging Technologies in Industrial IoT Architectures: A Review. *Sensors*, 22(15):5836, August 2022.

[32] NIST, National Institute of Standards and Technology. NIST Cybersecurity Framework. URL: *https://www.nist.gov/cyberframework* (last checked: 15.04.2024), 2024.

[33] Plattform Industrie 4.0. The background to Plattform Industrie 4.0. url: *https://www.plattform-i40.de/IP/Navigation/EN/ThePlatform/Background/background.html* (last checked: 15.04.2024), 2022.

[34] Hongyi Pu, Liang He, Peng Cheng, Mingyang Sun, and Jiming Chen. Security of Industrial Robots: Vulnerabilities, Attacks, and Mitigations. *IEEE Network*, 37(1):111–117, January 2023.

[35] Davide Quarta, Marcello Pogliani, Mario Polino, Federico Maggi, Andrea Maria Zanchettin, and Stefano Zanero. An Experimental Security Analysis of an Industrial Robot Controller. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 268–286, San Jose, CA, USA, May 2017. IEEE.

[36] Riigi Infosüsteemi Amet. Cyber Security in Estonia. URL: *https://www.ria.ee/kuberturvalisus/kuberruumi-analuus-ja-ennetus/olukord-kuberruumis* (last checked: 15.04.2024), 2024.

[37] Riigi Infosüsteemi Amet. Eesti Infoturbestandard. URL: *https://eits.ria.ee/* (last checked: 15.04.2024), 2024.

[38] Yash Shah and Shamik Sengupta. A survey on Classification of Cyber-attacks on IoT and IIoT devices. In *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pages 0406–0413, New York, NY, USA, October 2020. IEEE.

[39] Adam Shostack. *Threat Modeling: Designing for Security*. John Wiley & Sons, 2014.

[40] Statistikaamet. Eesti Tööstus. URL: *https://www.stat.ee/et/avasta-statistikat/valdkonnad/majandus/toostus* (last checked: 15.04.2024), 2023.

[41] Beenish Urooj, Ubaid Ullah, Munam Ali Shah, Hira Shahzadi Sikandar, and Abdul Qarib Stanikzai. Risk Assessment of SCADA Cyber Attack Methods: A Technical Review on Securing Automated Real-time SCADA Systems. In *2022 27th International Conference on Automation and Computing (ICAC)*, pages 1–6, Bristol, United Kingdom, September 2022. IEEE.

[42] Baicun Wang, Fei Tao, Xudong Fang, Chao Liu, Yufei Liu, and Theodor Freiheit. Smart Manufacturing and Intelligent Manufacturing: A Comparative Review. *Engineering*, 7(6):738–757, June 2021.

Appendix

I. Glossary

- **AI** - Artificial Intelligence.
  Interdisciplinary field, usually regarded as a branch of computer science, dealing with models and systems for the performance of functions generally associated with human intelligence, such as reasoning and learning [9].
- **B2B** - Business-2-Business.
  A business model in which the companies involved create products and services for other businesses [9].
- **BPMN** - Business Process Model and Notation.
  A graphical representation for specifying business processes in a business process model [9].
- **CAD** - Computer-Aided Design.
  Design activities, including drafting and illustrating, in which data processing systems are used to carry out functions such as designing, simulating, or improving a part or a product. Computer-aided design programs may provide precise dimensioning and positioning of each graphic element for engineering and manufacturing purposes [9].
- **CAM** - Computer-Aided Manufacturing.
  Using software and computer-controlled equipment to automate the manufacturing process.
- **CNC** - Computer numerical control.
  The control of devices, particularly machine tools, by direct input of data from a computer program [9].
- **DCS** - Distributed control system.
  System for process control purposes which, while being functionally integrated, consists of sub-systems which may be physically separated and located remotely from one another [9].
- **DDoS** - Distributed Denial-of-Service attack.
  A denial-of-service attack based on multiple sources of flooding traffic [9].
- **ERP** - Enterprise Resource Planning.
  Software supporting enterprise resource planning.
- **GDPR** - General Data Protection Regulation.
  A regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA) [9]. This regulation lays down the legal norms governing the protection of natural persons in the processing of personal data and the free movement of personal data, and its purpose is to protect the fundamental rights and freedoms of natural persons, especially their right to the protection of personal data.

- **IEC** - International Electrotechnical Commission.
  A global independent, nongovernmental membership organization that prepares and publishes international standards for all electrical, electronic, and related technologies [9].

- **IIoT** - Industrial Internet of Things.
  Global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies [9].

- **IKT** - information and communication technology.
  Resources for capturing, processing, storing and distributing information; the term also includes communications technology.

- **ISO** - International Organisation for Standardization.
  A nongovernmental organization that comprises standards bodies from more than 160 countries, with one standards body representing each member country [9].

- **ISSRM** - Information Systems Security Risk Management.
  A model of the field of information security, which includes the systematic identification, assessment and management of security risks in the context of information systems.

- **IoT** - Internet of Things.
  Infrastructure of interconnected entities, people, systems and information resources together with services that process and react to information from the physical world and virtual world [9].

- **NIST** - National Institute of Standards and Technology.
  A non-regulatory agency of the United States Department of Commerce developing and promoting standards [9].

- **PLC** - Programmable Logic Controller.
  A programmable electronic device used in industrial automation to provide logic and sequencing controls for machinery [9].

- **RAMI 4.0** - Reference Architectural Model Industrie 4.0.
  A three-dimensional model that shows how to approach Industry 4.0 in a structured way. RAMI 4.0 unites all elements and IT components in a single layer and life cycle model.

- **RTU** - Remote Terminal Unit.
  A microprocessor-controlled electronic device that collects data and controls processes in, for example, industrial facilities or parts of infrastructure distribution networks. These devices can collect data from sensors, forward it to a central control system, and receive commands and control functions from the central system.

- **SCADA** - Supervisory Control and Data Acquisition.
  A type of industrial control systems [9].

- **STRIDE** - Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege.
  A security risk assessment framework consisting of different categories of security risks.
- **SYN flood**.
  Malicious client-to-server jamming attack: based on mass repetition of SYN packet, generating mass incomplete TCP handshakes; the handshake is invalidated by the lack of receipt or forgery of the address [9].
- **Industry 4.0**.
  The 4th industrial revolution, which is characterized by the digitalization of industry, the emergence and use of big data and data analytics, the introduction of object networks and machine learning.
- **VoIP** - Voice over IP.
  A method and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet [9].

II. Questionnaire Questions and Answer Options

1. What is the size of your organisation?
    - Medium-sized
    - Small
    - Micro
    - Other
2. Is your organisation part of a bigger group, concern or conglomerate?
    - Yes
    - No
3. What is the manufacturing classification for your organisation?
    - Manufacture of food products.
    - Manufacture of beverages.
    - Manufacture of textiles.
    - Manufacture of wearing apparel.
    - Manufacture of leather and related products.
    - Manufacture of wood and of products of wood and cork, except furniture; manufacture of articles of straw and plaiting materials.
    - Manufacture of paper and paper products.
    - Printing and reproduction of recorded media.
    - Manufacture of coke and refined petroleum products.
    - Manufacture of chemicals and chemical products.
    - Manufacture of basic pharmaceutical products and pharmaceutical preparations.
    - Manufacture of rubber and plastic products.
    - Manufacture of other non-metallic mineral products.
    - Manufacture of basic metals.
    - Manufacture of fabricated metal products, except machinery and equipment.
    - Manufacture of computer, electronic and optical products.
    - Manufacture of electrical equipment.
    - Manufacture of machinery and equipment n.e.c.
    - Manufacture of motor vehicles, trailers and semi-trailers.
    - Manufacture of other transport equipment.

- Manufacture of furniture.
- Other

4. What is your position/role in the organisation?

    - Project manager
    - Process owner/manager/analyst
    - Production manager
    - System Analyst
    - Software/System architect
    - Information technology (IT) manager
    - Information Security Officer(ISO)
    - Chief Executive Officer (CEO)
    - Chief Technology Officer (CTO)
    - Other

5. What is the level of automation of manufacturing in your organisation?

    - Level 1 - Completely manual.
    - Level 2 - Manual work with support of the static tool(s).
    - Level 3 - Manual work with support of the flexible tool(s).
    - Level 4 - Automated hand tool: Manual work with support of the automated tool(s).
    - Level 5 - Static machine/workstation: Automatic work by a machine that is designed for a specific task.
    - Level 6 - Flexible machine/workstation: Automatic work by a machine that can be reconfigured for different tasks.
    - Level 7 - Completely automated.

6. How does your organisation engage with and manage its automated manufacturing systems, considering they may consist of various subsystems and components from different manufacturers?

    - We utilise a solution from a single provider without ongoing development or customisation.
    - We employ a complete solution that receives regular updates and enhancements from the original provider.
    - We engage third-party service providers to manage the system without active customisation.

- We collaborate with third-party service providers who tailor and update the system according to our needs.
- We have an in-house support team for a system initially developed externally, the team handles minor updates and maintenance.
- Our in-house development team oversees all aspects of our system, including integration of subsystems from various manufacturers, ongoing support, and custom development.
- We manage a mixed environment of integrated subsystems from different manufacturers, with support and updates handled through in-house and external resources.
- Other

7. To what extent has your automated manufacturing system evolved over the past 5 years?

    - No change.
    - Minor changes to subsystems or components, the main functionality remains the same.
    - Significant changes to subsystems or components, the main functionality remains the same.
    - Significant changes of main functionality (replacement).
    - Other.

8. What challenges does your organisation encounter with integrating, using, developing, and supporting your automated manufacturing system, including subsystems from various manufacturers?

    - Ensuring data privacy and security during the integration of diverse subsystems and manufacturers.
    - Balancing system efficiency with privacy concerns in a complex manufacturing environment.
    - Navigating the absence or inconsistency of industry regulations and standards across different subsystems.
    - Manufacturing process optimisation during a multitude of different subsystems.
    - Managing the system security and reliability before and during deployment.
    - Ensuring interoperability among various subsystems and/or with external systems or providers.
    - Addressing the lack of a cohesive national or industry-wide strategy for smart manufacturing.
    - Managing resource constraints in devices and subsystems within the manufacturing line.

- Overcoming challenges related to diverse networks and communication protocols.
- Meeting high expectations for system quality characteristics, such as scalability, efficiency, and adaptability to different platforms and operating systems.
- Other.

9. What information is used within your automated manufacturing system?
    - Sensor information.
    - Process information.
    - Operational information.
    - Environmental information.
    - Quality information.
    - Production information.
    - Production schedule information.
    - Software updates.
    - Stock material information.
    - Maintenance information.
    - Alarms/System error messages.
    - Other.
10. What automated systems do you use?
    - Open answer.
11. For what purposes does your organisation utilise information technology (IT) systems within your automated manufacturing processes?
    - We do not use IT systems in our manufacturing processes.
    - For digital data storage and management.
    - For managing customer relationships and sales processes.
    - For enterprise resource planning (ERP).
    - To provide digital services or products directly to end-users.
    - For exchanging data with external IT systems or partners.
    - For production planning and scheduling.
    - For supply chain management, including logistics and inventory control.
    - For quality control and compliance monitoring.
    - For predictive maintenance and asset management.

- For real-time monitoring and control of manufacturing equipment.
- For human resource management.
- For research and development, including product design and simulation.
- Other

12. Does your organisation's automated manufacturing process architecture align with RAMI 4.0 (Reference Architecture Model Industrie 4.0)? If not, please specify the model or architecture framework you adhere to or describe the structure of your manufacturing process architecture.

    - It is not aligned to any architecture or framework.
    - Yes, it aligns with RAMI 4.0.
    - Other.

13. How are security-related topics handled within your organisation?

    - Cyber security is managed entirely In-House. Our dedicated in-house cyber security team develops and implements security policies, conducts regular security assessments, and responds to incidents.
    - Collaboration with External Cyber Security organisations. We partner with external cyber security organisations for audits, threat intelligence, and incident response to complement our in-house capabilities.
    - Cyber Security as a Part of IT Department. Cyber security responsibilities are integrated into our IT department's roles, covering everything from routine security updates to employee training.
    - Use of Automated Security Solutions. We rely on automated security solutions (e.g., firewalls, intrusion detection systems) for continuous monitoring and threat detection, with periodic oversight by IT staff.
    - Outsourced Cyber Security Management. Cyber security management is entirely outsourced to a specialised organisation that handles all aspects of our security, from policy development to incident response.
    - Ad Hoc Cyber Security Practices. Cyber security measures are implemented ad hoc, with no dedicated team or consistent strategy, often in reaction to specific threats or incidents.
    - Employee Training and Awareness Programs. We prioritise employee training and awareness programs to ensure all staff understand cyber security risks and best practices.
    - Compliance with Industry Regulations and Standards. Our cyber security practices are guided by compliance with industry regulations and standards, ensuring that we meet specific security benchmarks.

- Other.

14. Which security, privacy or safety-related legislation, regulations and/or standards affect your automated manufacturing system?

    - General Data Protection Regulation (EU GDPR)
    - Consumer Protection Directives 2019/770 and 2019/771
    - NIST Special Publications (e.g. NIST SP 800-39, NIST SP 800-37)
    - UNECE regulation No 155 Cyber security and cyber security management system (from 2020)
    - Estonian Information Security Standard (E-ITS)
    - NIS2 directive
    - ISO 10218
    - ISO 12100
    - ISO TS 15066
    - ISO 2700x family
    - ISO 27701
    - ISO 31000
    - Isikuandmete kaitse seadus(IKS)
    - Küberturvalisuse seadus(KüTS)
    - I don't know
    - Other

15. Have your organisation experienced any cyber security-related incidents?

    - Data leak
    - Data manipulation(e.g. intentional modification of data)
    - Unauthorised access to Systems and Data
    - Exploitation of Remote Connection Vulnerabilities
    - Account takeover
    - Ransomware
    - Malicious redirect
    - Malware
    - Password attack
    - Fraud
    - Virus

- Phishing
- Flooding / Denial of Service
- We have not experienced any security incidents
- Other

16. What countermeasures does your organisation have in place to mitigate cybersecurity incidents?

    - Threat detection systems (e.g., SIEM, SOC operations).
    - Anonymization or pseudonymization of sensitive data.
    - Antivirus and anti-malware solutions.
    - Backup and disaster recovery plans to ensure data integrity.
    - Collaboration with external cybersecurity organizations for threat intelligence.
    - Data encryption for data at store and in transit.
    - External security assessments and penetration testing.
    - Firewalls and intrusion detection/prevention systems (IDS/IPS).
    - Incident response plan and team in place.
    - Limitation of user privileges and access control.
    - Multi-factor authentication (MFA) for system access.
    - Network segmentation to limit the spread of potential attacks.
    - Physical security measures to protect hardware and infrastructure.
    - Regular cybersecurity training and awareness programs for employees.
    - Regular security audits and vulnerability assessments.
    - Regular software updates and patch management.
    - Usage of secure coding practices in software development.
    - Use of blockchain or other advanced technologies to enhance security.
    - We do not have any security countermeasures.
    - Other

17. How is personnel training on cybersecurity conducted within your organisation?

    - Regular, mandatory cybersecurity training sessions for the employees.
    - Specialised training for IT and security staff.
    - Online training courses and resources.
    - External workshops and seminars.
    - On-the-job cybersecurity practice and drills.

- No formal cybersecurity training is provided.
- Other.

18. In case you want to share anything related to security, feel free to do so. Expand or provide context on any specific topic that you feel needs more attention.
    - Open answer.
19. May we contact you in the future for a potential collaboration? If yes, please provide your e-mail.
    - Open answer.

III. Risk Scenarios

Risk ID	Attack	Threat	Vulnerability	System Asset	Business Asset	Impact
001	Insider Attack [23], [35], [34], wittingly or unwittingly	Insider manipulates the operational commands	Lack of security background check of personnel	**RAMI 4.0**: Field device, Station, Work centre, Enterprise; **Target**: Personnel [23]	Operational data, Production parameters	Negates integrity of the business asset, Negates reliability of system asset
002	Data and policy corruption [23]	An external or internal actor corrupts data and alters security policies	Inadequate data validation and integrity checks; Weak policy management and oversight	**RAMI 4.0**: Work centre, Enterprise; **Target**: Server, Datacenter	Policy management system, Security policies, Security protocols	Compromises the confidentiality and integrity of business assets; Disrupts the effectiveness and reliability of security measures and system assets; Disruption of operators behaviour [23]
003	Code Manipulation [23], [8], [38]	An external or internal actor inject malicious code or alters existing code within the organisations software systems	Insufficient code review processes; Lack of automated security testing; Inadequate access controls to source code repositories [38], [34]	**RAMI 4.0**: Field device, Control device, Work Center, Enterprise; **Target**: Field device firmware, Application servers, Source code repositories	Application software and Device firmware [23]	Compromised application functionality [23], [38], [34], Potential data breaches, Unauthorised access to systems [34]

004	Malware infection [23], [8], [34]	An attacker deploys malware into the organisations' network, which could be in the form of a virus, worm, Trojan horse, ransomware or spyware	Inadequate endpoint security; Lack of regular system updates and patches [34]; Insufficient network segmentation and security [34]; Weak e-mail and web filtering policies	**RAMI 4.0**: Work Center(Servers), Enterprise(Servers), Connected world(end-user devices); **Target**: Servers, End-user devices	System and application availability and performance; Organizational and Customer data	Disruption of operations due to system compromise or failure, data theft or loss, financial loss, legal and compliance implications, damage to reputation
005	Network Worm Infiltration [23]	A self-replicating worm infiltrates the network, rapidly spreading across devices and systems without user intervention	Unpatched software or operating systems, open network shares, insufficient network segmentation [34], and lack of advanced threat detection mechanisms	**RAMI 4.0**: Work Center(Servers), Enterprise(Servers); **Target**: Routers, Switches, Servers	Network infrastructure, data stored on networked devices	Degradation of network performance, system failures [21], [38], unauthorised access to data [23], [34], disruption of business operations
006	Virus Infection [23], [8]	An attacker introduces a computer virus into the organisation's systems, which attaches itself to a program or file	Lack of up-to-date antivirus software, insufficient employee training [41], weak email and download security policies, and inadequate system patching protocols	**RAMI 4.0**: all; **Target**: Any asset with software	Integrity and availability of data and software	Disruption of individual and organisational productivity [23], [21], [38], loss or compromise of sensitive data [34], financial losses due to system recovery and repair efforts and damage to the organisation's reputation [8], [35], [38]

007	Flooding (Denial of Service) [23], [34]	An attacker overwhelms the organization's network resources or services with excessive traffic	Insufficient network bandwidth, lack of rate limiting or traffic filtering mechanisms [34], inadequate DDoS (Distributed Denial of Service) protection strategies [34]	**RAMI 4.0**: Network Infrastructure; **Target**: Routers, Switches, Servers [23]	Online services [34], customer access to digital platforms, operational efficiency	Loss of service availability leading to operational disruptions [38], [34], damage to customer trust and satisfaction [35], [38], revenue loss during downtime [35], and increased costs for network remediation and bolstering defences
008	Life-cycle Implants of Backdoors [23], [8]	An attacker implants backdoors during the software or hardware development life-cycle, allowing unauthorized access or control at a later stage	Inadequate security measures in the development and supply chain process, lack of thorough vetting of third-party vendors, insufficient code audits, and weak access controls over development environments	**RAMI 4.0**: Development Tools and Environments; **Target**: Production Software/Hardware, Supply Chain Infrastructure	Integrity and security of the product, trust in the organization's products and services, intellectual property	Unauthorised access to systems and data [34], potential for widespread compromise of the product and associated systems, erosion of customer and stakeholder trust [35], [38], legal and regulatory consequences, and significant financial and reputation damage

009	Physical destruction of IT Infrastructure [23], [35], [21]	Deliberate physical destruction of critical IT hardware and infrastructure by internal or external actors, such as employees, contractors, or intruders	Inadequate physical security measures at IT infrastructure locations (data centers, server rooms), lack of surveillance and access control systems, insufficient disaster recovery and business continuity planning	**RAMI 4.0**: Asset, Integration, Communication and Functional Layers; **Target**: Physical IT hardware [23], [35], [21], Server, Router, Switch	Operational data, Continuity of Business operations, Integrity and availability of products and services	Immediate loss of critical IT services and data, significant downtime and disruption to business operations, potential loss of sensitive data, high recovery and replacement costs, and potential damage to the organisation's reputation
010	Eavesdropping [23], [8], [34]	Unauthorized interception and listening to private digital communications, such as email, voice calls, or data transfers, by external or internal actors	Unencrypted communication channels [34], weak network security, inadequate use of secure communication protocols [41], and insufficient endpoint security	**RAMI 4.0**: Communication Layer and Asset layer devices; **Target**: Router, Switch, Wi-Fi access point, Communication systems(e-mail, Voip systems)	Confidentiality of information, sensitive business communications, intellectual property	Compromise of sensitive information leading to data breaches, loss of competitive advantage, potential legal and compliance violations, erosion of customer and stakeholder trust, and reputation damage [35], [38]

011	Hardware Backdoor Implementation [23], [8]	An attacker, potentially through a compromised supply chain or during manufacturing, embeds a backdoor within the hardware components, allowing for unauthorised access or control	Inadequate security vetting of hardware suppliers, lack of thorough security testing of hardware before deployment, insufficient oversight of the manufacturing process, and weak supply chain security	**RAMI 4.0**: Asset layer; **Target**: Physical components of any sort	Integrity and security of the physical technology infrastructure	Unauthorized access to and control over critical systems [34], widespread compromise of the organisation's network [23], damage to customer trust and business reputation, legal and compliance issues, and significant financial losses [35], [38]
012	Fault Injection [8], [35]	An attacker deliberately induces faults in a system's hardware or software to cause it to malfunction	Susceptibility of hardware and software to external manipulation, inadequate testing for fault tolerance, lack of robust error handling and validation mechanisms	**RAMI 4.0**: Asset layer; **Target**: embedded systems	System reliability and security, data integrity	Compromise of system functionality, data corruption, undermining of security measures, damage to the organisation's credibility and customer trust
013	Unauthorized Hardware Modification [8]	An attacker physically alters or tampers with hardware components	Inadequate physical security of hardware [34], [34], lack of tamper-detection mechanisms, insufficient monitoring of hardware integrity, and poor control over hardware maintenance [38]	**RAMI 4.0**: Asset layer; **Target**: embedded systems	System reliability and security, data integrity	Unauthorized system access [34] leading to data breaches or system damage, disruption of operations, potential espionage, and reputational damage [35], [38]

014	Buffer Overflow Exploit [8]	An attacker exploits a buffer overflow vulnerability in a software program to execute arbitrary code	Software that does not properly manage memory allocation, lack of bounds checking in code, use of insecure programming languages or libraries prone to buffer overflows	**RAMI 4.0**: Functional layer; **Target**: Software applications, Operating Systems, Firmware	Integrity, availability and confidentiality of software systems, data confidentiality and integrity	Unauthorised access [34], potential system crashes, data breaches, compromise of network security, and significant harm to the organization's reputation and trust [35], [38]
015	Micro Defects Injection [35]	An attacker introduces microscopic defects into hardware components during manufacturing or maintenance	Lack of inspection and testing protocols, insufficient oversight of manufacturing and maintenance processes, reliance on unvetted third-party components or services	**RAMI 4.0**: Integration layer; **Target**: Embedded devices, Integrated Circuits, Microprocessors, Printed Circuit boards(PCBs)	Integrity of hardware system components	Compromise of hardware functionality, damage to the organisation's reputation for quality and reliability, increased costs [35], [38] for recalls and repairs, and potential safety hazards
016	Disabling or Altering Safety Devices [35]	An attacker physically disable or alters safety devices to create hazardous conditions or to remove barriers to unauthorised physical access	Inadequate physical security [34] and surveillance of safety devices, insufficient tamper-proof mechanisms, lack of regular inspections and testing of safety equipment	**RAMI 4.0**: Asset layer; **Target**: Physical access control rooms(stations), Safety/Emergency Shutdown systems	Operational safety, personnel well-being	Increased risk of accidents and physical harm, potential for operational disruptions, damage to critical infrastructure, legal liabilities [35], [38]

017	Unauthorized access to Systems and Data [35]	An attacker gains access to the organisation's systems or data without permission	Weak authentication mechanisms, insufficient access controls [41], [38], [34], lack of multi-factor authentication, poor password management, and unsecured network services [34]	**RAMI 4.0**: Functional layer; **Target**: Databases, File Servers, User management systems, Administrative tools	Data confidentiality	Data breaches, unauthorised changes to system configurations or business data, legal and regulatory compliance breaches, reputational damage, and financial losses [35], [38]
018	Exploitation of Remote Network Vulnerabilities [35]	An attacker remotely exploits vulnerabilities within the organisation's network	Insufficient network segmentation, outdated or unpatched network software [34], insecure remote access protocols [41], inadequate firewall rules, and lack of intrusion detection/prevention systems [34]	**RAMI 4.0**: Communication Layer; **Target**: Firewalls, Routers, Switches, Remote Access Servers, Gateways	Network Integrity and security, confidentiality and integrity of transmitted data	Unauthorised access to internal networks [34], disruption of network services, potential data interception and theft, compromise of sensitive information, and the subsequent financial and reputational damage to the organisation [35], [38]

019	Insider-Enabled Network Attack (Local access) [35]	An insider or an attacker with physical access to the organisation's premises connects to the network locally	Inadequate physical access controls to network ports and devices, poor network segmentation, insufficient monitoring of local network traffic, lack of robust authentication [41], [38], [34] mechanisms	**RAMI 4.0**: Asset layer; **Target**: Physical network equipment	Integrity of networked systems, confidentiality of internal communications	Compromise of network security, introduction of malware, unauthorised surveillance, disruption of IT services, and subsequent operational, financial, and reputation damages [35], [38]
020	Physical Tampering with Sensors [21]	An individual physically obstructs, disrupts, or damages sensors	Lack of physical safeguards around sensitive sensors [38], insufficient detection of tampering, failure to implement redundancy, and weak incident response protocols	**RAMI 4.0**: Asset Layer(Field device); **Target**: Sensors, cameras, actuators	Real+time data integrity, operational awareness	Loss of situational awareness, incorrect data, potential for physical harm or process failures, and compromise of the organisation's ability to maintain operational continuity [38]
021	Theft and Cloning of Access Badges [21]	An attacker steals physical access badges from authorised personnel or clones them to gain unauthorised entry to secure locations	Insufficient physical security measures, lack of badge access monitoring, weak authentication processes, and failure to promptly deactivate lost or stolen badges	**RAMI 4.0**: Asset layer; **Target**: Identification badges	Security of physical premises, the safety of employees	Unauthorized access leading to potential theft or sabotage [34], compromised security of facilities, the risk to employee safety

022	Command Injection [21]	An attacker exploits insecure input validation in software to inject unauthorised commands	Insufficient input validation and sanitation, over-privileged process execution, lack of effective application layer security controls, and insecure coding practices	**RAMI 4.0**: Functional layer; **Target**: Application software, Operating systems, Execution environments(Web servers, databases)	Integrity and availability of software applications	Unauthorized system activities leading to data breaches, system compromise, and disruption of services; damage to the organisation's reputation and trust [35], [38]
023	Unauthorized Configuration Alteration [21]	An attacker gains access to configuration interfaces or files and makes unauthorised changes	Insufficient access controls on configuration settings, lack of change management and monitoring, over-privileged user accounts, and inadequate auditing of configuration changes	**RAMI 4.0**: Functional layer; **Target**: Application software, Operating systems, Execution environments(Web servers, databases)	Integrity and security of IT systems	Operational disruption due to misconfigured systems, regulatory non-compliance issues, potential data breaches, and loss of trust among stakeholders [35], [38]
024	Unauthorized Access to Human Machine Interfaces (HMI) [21]	An attacker exploits vulnerabilities in HMI systems to gain unauthorised access, leading to control over physical processes	Weak authentication mechanisms [41], [38], [34], unpatched HMI software, insufficient network segmentation, and lack of monitoring and alerting on HMI activities	**RAMI 4.0**: Asset layer(Control device/Station); **Target**: Control systems, HMI Panels, SCADA Systems	Integrity and availability of operational processes	Potential safety hazards due to loss of control over industrial processes [21], [38], [34], unauthorised changes to operational setpoints, data falsification, and physical damage to industrial assets

025	Physical and Digital Tampering [38]	An attacker physically alters or digitally manipulates devices, software, or data	Insufficient physical security controls, inadequate integrity checks for data and software, lack of tamper-detection and prevention mechanisms, weak access management	**RAMI 4.0**: Asset and Functional layer; **Target**: Application software, Physical devices	Integrity of data and operational systems	Unauthorised changes leading to system malfunctions [21], [38], [34], data corruption or loss, the introduction of vulnerabilities
026	Sleep deprivation [38]	An attacker continuously sends requests to a system, device, or component, preventing it from entering a low-power state (sleep mode)	Lack of rate limiting or request filtering on devices, insufficient energy management protocols, and inadequate monitoring of system performance and health	**RAMI 4.0**: Asset layer; **Target**: IoT devices, Servers, Networking equipment	Availability and integrity of the hardware, operational efficiency	Increased power consumption leading to higher operational costs [35], [38], reduced lifespan of devices due to constant operation, potential system failures or malfunctions, and decreased overall system performance
027	SYN Flooding [38]	An attacker sends a rapid succession of SYN requests to a target server but does not respond to the server's SYN-ACK responses	Insufficient SYN flood protection on servers, lack of rate limiting, inadequate network infrastructure to handle high volumes of traffic, poor SYN packet filtering	**RAMI 4.0**: Asset and Communication Layers; **Target**: Web servers, Application Servers, Network Infrastructure	Availability of online services, operational efficiency	Server downtime or reduced performance, denial of service to legitimate users, potential revenue loss during periods of inaccessibility, increased operational costs [35], [38] for traffic management and mitigation

028	Man-in-the-Middle Attack [38], [34]	An attacker intercepts and potentially alters the communication between two parties without their knowledge	Unsecured or poorly encrypted communication channels [41], [34], weak authentication protocols [41], [34], lack of endpoint security [34], and susceptibility to DNS or ARP spoofing	**RAMI 4.0**: Asset and Communication Layers; **Target**: Web and Application Servers, Network Communication equipment	Confidentiality and integrity of Transmitted data	Data breach involving sensitive information, unauthorised access to system credentials, potential manipulation of data leading to incorrect decisions or actions, loss of trust among users, and reputation damage [35], [38]
029	Sinkhole attack [38]	An attacker redirects network traffic through a malicious node (the sinkhole), allowing them to intercept, analyse, or manipulate the data flowing through the network	Compromised network routing information, weak authentication for network updates [34], susceptibility to routing protocol attacks, and inadequate network monitoring	**RAMI 4.0**: Asset layer; **Target**: Routers, Switches, Network infrastructure	Integrity and confidentiality of network traffic	Interception and compromise of sensitive data [34], disruption or degradation of network services, unauthorised access to networked systems, and overall compromise of network security

030	Barrage attack (combination of multiple attack vectors) [38]	An attacker launches a coordinated assault using a variety of attack methods simultaneously or in rapid succession, aiming to overwhelm defences	Insufficiently layered defence mechanisms, lack of real-time threat detection and response capabilities, inadequate training [41] and preparedness for complex attack scenarios, and weak inter-system communication and control	**RAMI 4.0**: Functional, Communication and Asset Layers; **Target**: Anything	Availability and integrity of business operations	Rapid compromise of multiple systems, increased difficulty in identifying and mitigating threats, significant operational disruptions, potential data breaches, and substantial damage to the organisation's reputation and trust [35], [38]
031	Reverse Engineering of Software or Hardware [34]	An attacker analyses software or hardware to understand its design, functionality, and potential vulnerabilities	Lack of robust protections against reverse engineering, such as obfuscation techniques for software [34], and physical security measures for hardware	**RAMI 4.0**: Functional and Asset layers; **Target**: Software applications, Firmware, Hardware devices	Intellectual property	Unauthorized replication or modification of products, undermining of competitive advantage, potential security breaches based on discovered vulnerabilities, and erosion of market share and brand integrity

032	Brute force attack [34]	An attacker uses automated methods to systematically try all possible combinations of passwords or encryption keys until the correct one is found, granting unauthorised access	Weak password policies [41], lack of account lockout mechanisms after multiple failed attempts, insufficient encryption strength [41], [34], and inadequate monitoring of authentication attempts	**RAMI 4.0**: Functional and Business Layers; **Target**: Authentication Systems, User account database	Data confidentiality, system integrity	Unauthorized access to sensitive systems and data, the potential for further malicious activities within the network
033	Network Sniffing [34]	An attacker uses packet-sniffing tools to intercept and analyse network traffic, aiming to capture sensitive information such as passwords, session tokens, or confidential data being transmitted over the network	Unencrypted network traffic [41], weak network security configurations [34], lack of network monitoring and intrusion detection systems, and unsecured wireless network connections	**RAMI 4.0**: Communication Layer; **Target**: Network infrastructure(Routers, Switches, wireless access points)	Data confidentiality, the integrity of communication network	Exposure of sensitive information, potential for subsequent targeted attacks, undermining of network security, and damage to the organisation's reputation and trust [35], [38]

034	Replay attack [34]	An attacker intercepts valid data transmission (like authentication tokens) and retransmits it, potentially to gain unauthorised access or perform a transaction fraudulently	Lack of or inadequate implementation of sequence numbers or timestamps in communication protocols [41], [34], insufficient encryption mechanisms, and weak session management	**RAMI 4.0**: Communication Layer; **Target**: Network infrastructure (Routers, Switches, wireless access points)	Data confidentiality, the integrity of communication network	Unauthorized access to systems or data, fraudulent transactions, compromise of secure communication channels, and erosion of trust among users and stakeholders [35], [38]
035	IP Address Spoofing [34]	An attacker masquerades as a legitimate user or device by falsifying IP address information in their network packets, aiming to bypass IP-based security measures, impersonate other devices, or conduct a reflected attack	Lack of network authentication protocols [41], [34], insufficient packet filtering, weak network configuration, and inadequate monitoring of network traffic for anomalies	**RAMI 4.0**: Communication Layer; **Target**: Network infrastructure(Routers, Switches, wireless access points)	Data confidentiality, the integrity of communication network	Unauthorized access to network resources, disruption of services, potential for further network-based attacks, compromised data integrity, and damage to the organisation's reputation [35], [38]

036	Data Manipulation [34]	An attacker subtly alters critical data within a system or in transit, aiming to corrupt information, undermine decision-making processes, or achieve financial gain	Insufficient data integrity checks, lack of robust access controls, weak encryption of data in transit [41], [34], inadequate auditing and monitoring of data changes	**RAMI 4.0**: Asset layer; **Target**: Databases, File storage systems	Data integrity and availability	Incorrect decisions made based on altered data, erosion of trust in data reliability, financial losses due to manipulated data (e.g., in financial transactions), potential legal and regulatory consequences
037	Phishing [34]	Attackers deceive users into revealing sensitive information, such as login credentials or personal information, by masquerading as a trustworthy entity in digital communication	Lack of user awareness and training [41], inadequate email filtering and security measures, insufficient verification processes for digital communications [34]	**RAMI 4.0**: Business and Communication Layers; **Target**: E-mail systems, User devices, Web browsers	Data confidentiality	Unauthorized access to accounts and sensitive data, the potential for further security breaches, financial losses due to fraud or data theft, damage to the organisation's reputation [35], [38], and erosion of trust in communication channels
038	SQL Injection [34]	An attacker exploits vulnerabilities in a web application's database query software by injecting malicious SQL code	Inadequate input validation, lack of prepared statements or parameterised queries in database interactions, insufficient user input sanitisation, and weak database configuration	**RAMI 4.0**: Information Layer; **Target**: Web application Servers, Databases	Integrity, confidentiality and availability of data	Unauthorized access to sensitive data, potential database corruption or loss, disclosure of private information, loss of data integrity, legal and compliance issues, and damage to the organisation's reputation

039	DNS Poisoning [34]	An attacker corrupts the DNS (Domain Name System) cache with false information, redirecting users to malicious websites or servers without their knowledge	Weak security measures in DNS servers, lack of DNS request validation, outdated or unpatched DNS software, and insufficient network security protocols [34]	**RAMI 4.0**: Communication layer; **Target**: Network infrastructure	Integrity of web traffic	Users unknowingly directed to fraudulent sites leading to phishing attacks or malware infection, compromise of sensitive information, disruption of legitimate web traffic, and potential damage to the organization's credibility
040	Side Channel attack [34]	An attacker exploits the physical implementation of a cryptosystem, such as timing information, power consumption, electromagnetic leaks, or even sound, to gain insights about the underlying data or cryptographic keys	Cryptosystems not designed to be resistant to physical leakage, insufficient shielding of hardware, lack of noise in data operations, and inadequate monitoring of physical access to critical systems	**RAMI 4.0**: Asset layer; **Target**: Cryptographic devices, Servers	Data confidentiality	Compromise of cryptographic information leading to data breaches, undermining of data encryption practices, potential exposure of sensitive information, and loss of trust in security measures

041	Password attack [34]	An attacker attempts to gain unauthorised access to systems or data by cracking or guessing user passwords	Weak user password policies [41]), [38], [34], lack of multi-factor authentication, insufficient user education [41] on secure password practices and inadequate account lockout mechanisms after multiple failed login attempts	**RAMI 4.0**: Functional and Asset layers; **Target**: User accounts	Data confidentiality and integrity	Unauthorized access to critical systems and data, the potential for further malicious activities within the network, compromise of user credentials, operational disruptions, and damage to the organisation's reputation
042	Operation manipulation [34]	An attacker gains control of operational systems or alters their configurations, leading to incorrect operations, disruption of processes, or causing physical damage to equipment	Inadequate access controls on operational systems, lack of monitoring and alerting on system activities, insufficient segregation between IT and operational technology (OT) networks, and weak authentication mechanisms [41]), [38], [34]	**RAMI 4.0**: Asset layer; **Target**: Industrial Control Systems(ICS), Programmable Logic Controllers(PLC), SCADA Systems	Integrity of operational processes, personnel safety	Disrupted operational processes, potential physical damage to machinery or infrastructure, safety hazards for employees, operational downtime, and financial losses [35], [38]

043	Ransomware infection [34]	An attacker encrypts the organisation's data or systems and demands payment for the decryption key, hindering access to critical data and disrupting operations	Inadequate endpoint security [34] lack of regular data backups, insufficient employee training [41] on malware threats, weak email and web security policies, and unpatched systems	**RAMI 4.0**: Asset and Information layers; **Target**: Data storage systems, End-user devices, Servers	Integrity and availability of data	Loss of access to critical data and systems, operational downtime, potential data breaches if data is ex-filtrated, financial losses due to ransom payments and recovery efforts, and reputation damage