Università degli studi di Verona
Dipartimento di Informatica
Laurea in Ingegneria e scienze informatiche

A methodology for the risk analysis of industrial control systems

Relatore:
Prof.ssa
Federica Maria Francesca Paci

Correlatore:
Dott. Marco Rocchetto

Candidato:
Emanuel Cirabisi
VR472646

ANNO ACCADEMICO 2022/2023

Contents

Chapter 1

Introduction

1.1 Motivation

Industry 4.0, known as the "fourth industrial revolution", represents the era of interconnected and automated systems that exploit advanced digital technologies to improve industrial processes. Through real-time data exchange and automation, companies can optimise production, improve supply chain management and develop smarter products and services, increasing productivity and innovation. Today's industrial processes have reached a high level of complexity and automation, thanks to the implementation of advanced "Operating Technology" (OT). It is a set of hardware and software devices that allow the control and monitoring of industrial processes. Moreover, it is particularly used within critical infrastructures where continuous, real-time monitoring of industrial processes is required. A main component of OT systems are "Industrial Control Systems" (ICS) that ensure the security and reliability of industrial processes. The use of these systems allow the control and management of devices used in the industrial environment such as "Programmable Logic Controller" (PLC) and "Human Machine Interface" (HMI). These systems make it possible to automate the management of production and the critical infrastructure to which the devices are connected. These systems have good reliability and a high response time in the management of industrial processes. OT systems exploit technologies to improve the efficiency of industrial processes. Another example of ICS are the "Distributed Control Systems" (DCS) used to monitor and control complex industrial processes. An attack on these devices can compromise the security of the industrial infrastructure and for this reason the security of OT systems is essential to guarantee the integrity, availability, and confidentiality of industrial processes. These systems are the essential infrastructure for monitoring and controlling industrial processes. In this regard, it is necessary to emphasise the

increasing convergence with information systems (IT). They are oriented towards managing digital information and supporting business activities while OT systems are oriented towards the control of physical processes. From a security perspective, the two systems have different priorities. Indeed, OT systems allow to avoid physical damage and production interruptions, while IT systems focus on corporate privacy. Instead, from a networking perspective, IT and OT networks are separated by a clear segmentation of the network to facilitate monitoring, but this division is not always effective because a direct link between the data cannot always be found. Therefore, in recent years, companies have been trying to find ways to improve the interconnection between IT and OT networks [1] to optimise processes. Within industrial processes, *IoT* [2] systems play a crucial role in industry today, thanks to the possibility of creating a network of interconnected devices in which, through the use of different technologies such as actuators and sensors, data can be sent to a control system that monitors and prevents malfunctions. These developments have led to greater efficiency, accuracy, and production but have also introduced new challenges related to **cybersecurity**. These processes over time have undergone significant transformation through technological innovation. The increase of digitization and automation have provided the possibility to increase efficiency, reduce costs and achieve better product quality. However, this evolution has brought a series of challenges, including cybersecurity, which has become a critical issue in modern industrial processes [3]. The term cybersecurity today is strictly related to the definition of industrial infrastructure; the goal of cybersecurity is to ensure that information systems and what is part of them are protected from cyber-attacks. The basic principles on which it is based are confidentiality, availability and integrity, and these are the basic principles that make it possible to protect the system from unwanted *threats*. Due to the high interconnection of the various networked devices, it is not always easy to ensure that these principles are respected, which is why it is important for every company to adopt strategies to minimise its *vulnerabilities*. The difference between threat and vulnerability is not obvious and there is often confusion between the two terminologies. The two terms are consequences of each other: the *threat* is the weakness of the system caused by a failure to implement a security requirement, while the *vulnerability* is the way in which a given threat can be exploited and which corresponds to its consequence. Protecting industrial processes has become a crucial priority, as cyber threats can have devastating consequences for production, the environment and human security. From the statistics of 2023 [4], each passing month, attacks on the industrial sector are increasing considerably. From the data provided, even the countries considered to be the most secure have shown vulnerabilities to

this series of cyber-attacks, while countries such as Africa show a very high percentage of attacks. A considerable figure relates to the high number of malware families that have been detected and blocked in this calendar year, which clearly exceeds that of previous years. Among the most prevalent malware families in this area, malicious scripts and fake HTML pages stand out, as they can be spread either via phishing e-mails or via the network. The importance of keeping industrial processes at the forefront of security is crucial. Manufacturing, energy, logistics and many other sectors depend on these processes. A cyber-attack can cause serious damage, from disruption of production to loss of sensitive data, environmental pollution or, in extreme cases, endangering human life. There are several examples of real attacks on industrial infrastructures that affected different control systems. Since the most notable attack in 2010 via Stuxnet, a worm realised to attack PLCs used to control uranium facilities in Iran, the number of attacks has increased dramatically over the years. For example, Triton is a malware discovered in 2017 designed to tamper with control systems used to protect critical industrial processes at a petrochemical plant in the Middle East. Among the most recent, in 2021 in Oldsmar, Florida, an attack was carried out on the water treatment plant in which attackers managed to remotely access the control systems. Also in the same year, vulnerabilities such as "Ripple20" and "Amnesia:33" were discovered within IoT devices which caused serious dangers to companies that had adopted these devices. These are just some of the examples of countless cyber-attacks carried out over the years and for this reason it is necessary to find a solution that allows identifying possible threats and the corresponding vulnerabilities so that they can be mitigated. Due to these repeated cyber-attacks, in recent years the need has arisen to create processes and methodologies that allow companies to identify and mitigate cybersecurity threats relating to their internal infrastructure and the devices used in industrial processes. For this reason, different methodologies have been created for risk analysis and some of them can be applied for industrial control processes.
Some examples of these methodologies are:

- *CORAS*: It is a model-based framework realised for risk assessment, consisting of eight steps, and applicable across various sectors. It has the main advantage of using a graphical representation in order to involve the main stakeholders in the risk assessment, but its development can be time-consuming and require specific expertise, and for complex systems the model-based representation may not be very efficient.

- *NIST 800-30*: It is a guide for risk analysis and provides a 4-step process for identifying and prioritising information security risks. It

is an approach that can be applied to different information systems and allows great flexibility so that it can be adapted to the company using it by implementing only the relevant parts of the guideline. A complete implementation of the process may require significant resources in terms of time and technical expertise.

- *OCTAVE*: It is a methodology that allows to identify and manage IT risks in 3 different phases. It is designed to be adapted to medium-sized and large companies. Due to its flexibility, it can be applied in several contexts and allows the participation of employees from different organisational areas. It is not suitable for smaller companies because it is a complex methodology and, in addition, specific training may be required to apply it. It allows for a general evaluation by moving away from a holistic approach.

The analysis of these methodologies has revealed that their main disadvantage is related to the complexity or size of the company. In particular, some methodologies necessitate employee training for effective use, whereas others, due to their complexity and management requirements, are more suited to larger companies and may not be practical for smaller companies, where their complexity could result in unclear analysis. For this reason the objective in this thesis is to create a methodology that can respect the following characteristics:

- It can be applied to several companies of different sizes through a simple and flexible approach.
- It is possible for the company to choose the level of complexity that can bring to the risk assessment process according to the level of detail with which it decides to analyse the threats.
- It can be useful for companies that have to apply risk analysis on several products and need to carry out periodic reviews through a simple and quick assessment.
- It is useful for companies where no special technical knowledge is required so that interested stakeholders can also be involved.
- It can be applied to several industrial control systems and can be integrated with other frameworks or standards such as the IEC 62443 - 4 -1 [5].

The methodology proposed in this thesis was applied on a particular industrial control system, an HMI which is one of the main elements within an industrial process. The choice to use this device comes from the collaboration between the University of Verona and a local company,

V-Research, which allowed me to carry out the risk analysis on a real HMI device, designed by a customer company. From this collaboration, the objective was to create a method that is both simple and flexible, and that complies with the IEC 62443-4-1 standard, which provides guidelines on how processes related to the security of industrial control systems should be implemented. For this reason, the aim of this thesis was to develop a risk assessment methodology with two distinct phases:

- Examine the state of the art of methodologies in the field of cyber-physical systems (CPS) and OT (Operational Technology) with the aim of understanding the methodologies that currently exist and the advantages and disadvantages of each.
- Define a methodology applicable to the devices used in the CPS environment and, in this specific case, an HMI was chosen as the main element to apply this methodology. In particular, through successive steps, the internal structure of the device is identified (by analyzing the hardware and software architectures), and then the threats that could affect it. Further, the risk, associated with each individual threat, is assessed, estimating its severity and how it may impact the system. Finally, possible mitigation solutions to each threat are provided and a new risk assessment is carried out to understand how the mitigation solutions may change the assessment.

Moreover, this thesis is structured as follows:

- **Chapter 1**: This first introductory chapter provides a general overview of issues related to the industrial environment and the objective of the thesis.
- **Chapter 2**: The second chapter provides an overview of the main background concepts needed to better understand the proposed methodology.
- **Chapter 3**: The third chapter presents the state of the art in which a comparison is made between the proposed methodology and existing ones.
- **Chapter 4**: The fourth chapter outlines the proposed methodology.
- **Chapter 5**: The fifth chapter provides a comparison of the methodology proposed in this thesis with the "OWASP Risk Rating Methodology".
- **Chapter 6**: The sixth chapter proposes the conclusions deduced from the work done by highlighting the problems encountered at

various stages. Finally, ideas are proposed on how to continue the present work.

Chapter 2

Background knowledge

This chapter provides an overview of the main basic concepts of the methodology proposed in this thesis. In particular, standards and methodologies used in the development of this thesis are described and examples are provided for a better understanding of the concepts.

2.1 Industrial control systems

Industrial control systems are devices that allow the control and monitoring of industrial processes and aim to ensure the security and efficiency of the operations performed. These systems include several devices, including:

- **SCADA systems**: Systems that allow the collection and transfer of information to a central computer that controls and supervises the data collected.
- **PLC**: A device used in an industrial environment that is programmed to manage and control the devices to which it is connected.
- **HMI**: A device that allows control and monitoring of the industrial devices to which it is connected to prevent failures and malfunctions.
- **DCS**: Distributed control systems are a subset of ICS systems and aim to manage large-scale industrial plants by distributing functions among the various connected devices through decentralised management.

To maintain the interconnection between devices within an industrial process, different protocols can be used for different purposes. the main protocols used are:

- *Modbus*: Serial communication protocol that allows the exchange of information between a master device and one or more slave devices responding to the master's requests.
- *OPC UA*: a communication protocol designed for secure and reliable data exchange between control systems. It supports encryption, authentication and data integrity and it is designed to be used on different systems and hardware architectures.
- *Profinet*: Ethernet-based protocol supporting real-time data transmission to interconnect devices between control systems.
- *DNP3*: Distributed Network Protocol 3 is a communication protocol for controlling and monitoring industrial operations. It is based on a master-slave architecture, supports several levels of physical communication, and allows proper data transmission.

2.2 IEC 62443 – 4 – 1

The "Security for industrial automation and control systems, Part 4-1: Secure product development lifecycle requirements" [5] is a standard that covers the security of control systems in the industrial environment and provides general guidelines for the design, implementation, and maintenance of security within industrial processes focusing on product development requirements. The standard provides a description of the terminology that are used in the various sections. The standard is also divided into *eight main practices*, with subsections providing guidelines on how to implement a particular feature. A general description of each practice is given here:

1. **Practice 1 - Security management**: The standard begins by defining Practice 1 for the realisation of a process capable of producing a secure product at every stage of its life cycle. The standard states that it is important to ensure from the earliest stages of development that there must be no ambiguity in the realisation of the documentation; furthermore, it is important that the objectives are well defined so that there are no contradictions in the subsequent phases. The last paragraphs of this practice focus on the cyber-security aspect of business processes; in particular, the product during the development phase must be protected from unauthorised modifications and the documentation created must be constantly updated. In addition, special attention must be paid to hardware and software components that are implemented within the product that could lead to unwanted vulnerabilities.

2. **Practice 2 - Specification of security requirements**: This practice plays a crucial role in the product development process. At this stage, it is necessary to define a process for gathering security requirements for the product, defining in which context it must be used. It is important to understand the context in which the device will be used in order to define the next steps in the development process. Indeed, the level of physical security and the threats that could affect the device could change considerably. For example, section 2 of this practice concerns the realisation of the threat model for a given product. The threat model is a graphical and textual representation of the cyber threats that may affect a hardware or software device. It allows the identification and mitigation of threats that can be detected in a product to be defined through successive steps.

3. **Practice 3 - Secure by design**: This practice provides a general view of how the product design phase should be structured, considering guidelines or, rather, "best practices" to be followed to implement a secure design. Defining security layers, considering "defence in depth design", allows a series of security levels to be defined that make the system secure in a way that makes it difficult to attack and bypass.

4. **Practice 4 - Secure implementation**: This practice provides guidelines on how to ensure that features are implemented correctly. In particular, the focus is on the importance of a periodic review of what has been implemented, from the security requirements to the analysis of threats that may affect the assets. This makes it possible to find deprecated libraries or new vulnerabilities that have not previously been considered.

5. **Practice 5 - Security verification and validation testing**: This practice focuses on the importance of testing at various stages of the product development cycle. In particular, the practice focuses on the importance of testing starting with the implemented security requirements and then concentrating on how the detected threats can be mitigated. In addition, it provides guidelines to follow on how to detect internal system vulnerabilities like graphical diagrams or an analysis of known vulnerabilities. The last part of this section focuses on the importance of having tests carried out by product developers in order to make the process more efficient.

6. **Practice 6 - Management of security - related issues**: This practice focuses on how to manage security issues that may occur and affect company assets. For example, having a system that

quickly notifies any problems could avoid further malfunctions. In particular, it is important that the problem does not increase the risk and that it is contained when it occurs. Furthermore, it is essential to understand how far the problem extends in order to outline which assets are at risk. At the end of this section guidelines are provided on how to prevent these problems in order to reduce the risk of them occurring or being repeat such as the ability to disable or remove features or change harmful elements in the system design.

7. **Practice 7 - Security update management**: This section provides guidelines on how to ensure good management of security updates. In particular, it focuses on the importance of verifying that released updates provide the features for which they were made without creating regression. Furthermore, it is important that each update is documented and approved before it is authorised for installation.

8. **Practice 8 - Security guidelines**: Finally, Practice 8 focuses on several aspects, such as the safe disposal of the product, to be followed if a company wants to keep its data confidential, or on the responsibilities that users must have to use the product correctly, defining precise privileges. The practice concludes by affirming that it is important to carry out a periodic review of the documentation because, over time, new features are added and new industrial processes are implemented that may lead to a significant change in the requirements to be adopted.

This standard helps companies realise a complete process and allows them to control the complete product life cycle.

2.3 Threat modelling

Threat modelling is a process that allows the identification and assessment of threats [6] that could compromise a system. Through this process, vulnerabilities and attack scenarios in the system can be identified, allowing companies to implement a prevention plan to reduce the risk of cyber attacks. Performing this process is one of the steps to be followed for compliance with IEC 62443-4-1 [5]. Over time, several methodologies [7] have been developed to optimise the threat modelling process. Some of the main reasons that justify the existence of these threat modelling methodologies include:

- *Context of application*: The realisation of threat modelling depends on the context in which the system is used. For example, the need

of this process in critical infrastructures may differ significantly from those in the financial or healthcare context.

- *System complexity*: Each threat modelling methodology uses distinct approaches to identify threats that could compromise a system. In instances where the system is particularly complex, it may be appropriate to adopt a hybrid approach incorporating several methodologies, in order to conduct a more accurate analysis.

- *Improvements in Methodologies*: Over time, methodologies are improved and refined to make the threat modelling process more efficient. It is important that companies keep updated on developments in new methodologies.

Over the years, several methodologies have been developed to satisfy each different approach. Some of the most commonly methodologies of threat modeling are STRIDE [8], DREAD [7], PASTA [9] and LINDDUN[10]:

- **STRIDE**: This is a methodology, introduced in 1999 by Microsoft, based on different steps to identify and categorise threats detected in a software application. Today, it is the most widely used methodology.

- **DREAD**: This is a methodology for prioritising threats detected within a software application. DREAD is an acronym and each letter is a risk analysis category. Indeed, it is possible to define a numerical value for each category to assess the risk associated with a specific threat.

- **PASTA**: PASTA is an acronym for "Process for Attack Simulation and Threat Analysis". It is a methodology that consists of seven distinct phases, and allows to identify and mitigate security risks in software applications. This is a flexible methodology that can be adapted to each corporate project in order to detect specific threats.

- **LINDDUN**: It is a methodology for maintaining data security and detecting privacy threats within software or hardware applications. Like STRIDE and DREAD, LINDDUN is an acronym and each letter refers to a precise privacy feature. In particular, it is possible to create a table in which it is possible to mark which privacy feature is violated.

2.3.1 Microsoft STRIDE

The *STRIDE methodology* [8] has been introduced in 1999 by Microsoft to help developers to identify and mitigate security vulnerabilities in the software design phase. It is a methodology that allows to categorise threats that may damage a system and allows associating a risk value with each identified threat.
STRIDE is an acronym, and each letter refers to a specific threat:

- **S (Spoofing)**: Spoofing is a threat related to activity in which an attacker falsifies his identity by pretending to be a legitimate user to gain unauthorised access to the system. Spoofing can be associated with several activities such as the activity of sending fake e-mails in which an attacker pretends to be a trusted user. Moreover, it is the activity of the web spoofing in which an attacker uses a fake sites to steal sensitive data from website visitors.

- **T (Tampering)**: Tampering is a threat related to the activity in which an attacker performs an unauthorised modification of data to tamper with the system attached.

- **R (Repudiation)**: Repudiation is the action in which a user denies having performed actions. This threat occurs when a user denies having carried out an operation.

- **I (Information disclosure)**: Information disclosure is related to the activity in which an attacker performs an unauthorised disclosure of sensitive information.This threat occurs when a user accesses information for which he does not have authorisation.

- **D (Daniel of Service)**: Daniel of Service is an attack in which the attackers' goal is to alter the proper functioning of the system. These attacks are conducted with the aim of overloading the server of the system in use so that users cannot use the service.

- **E (Elevation of Privilege)**: Elevation of privileges is relating to the activity in which an unauthorised user obtains elevated privileges with the goal to alter the system.

Microsoft STRIDE loops through four phases (as depicted in Figure 2.1):

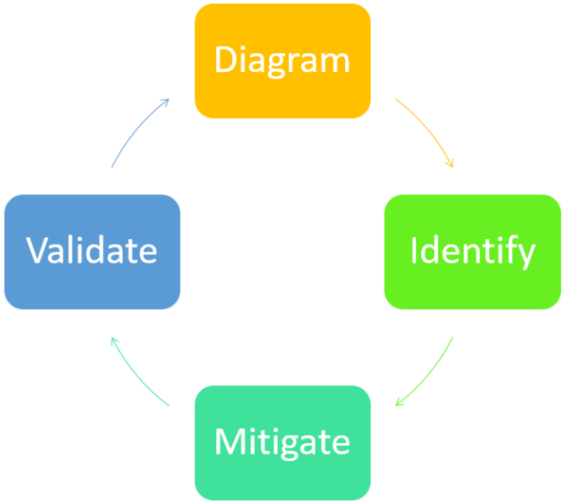

Figure 2.1: Stages of STRIDE Threat Modeling.

- *Diagram*: In this first phase, it is important to create several diagrams that can represent the internal structure of the system. Microsoft suggests using different diagrams depending on the system to be analysed. For example, the most common diagrams used in this phase are "deployment diagram" and "data flow diagram" (DFD):
  - *Deployment diagram*: It is a diagram that allows to represent the physical and logical disposition of elements within a system. It makes possible to define the internal components of a system, to group them, and to show the relationships between the entities that communicate with the system.

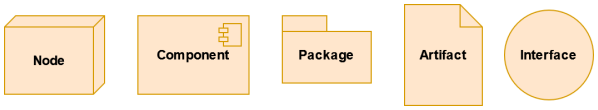

Figure 2.2: Deployment diagram elements

The notation of the deployment diagram consists of a set of symbols with specific features. The main symbols (as shown in Figure 2.2) are divided into:

* *Node*: It is a physical element and represents the physical execution units of the system. This element is represented by a three-dimensional cube, which can be associated a stereotype, a term that describes its functionality. Within

a node, it is possible to include other nodes and components. An example of a node can be a mobile device, a server or any hardware platform.

  * *Component*: It is a part of the system and can be used to define hardware or software elements within the system. It is advantageous to define dependencies between the various components in order to provide a more detailed representation of the system. An example of a component can be a physical interface or software supported by the system.
  * *Artifact*: It is identifiable as an executable file or data on a node. Artifacts can be used within nodes and components, depending on the level of detail considered. An example of an artefact may be a database, libraries or execution files.
  * *Interface*: An interface is used to define a service or functionality that a component possesses. This concept is used to establish a separation between functionality and its implementation, and interfaces are implemented by components. An example of functionality may be related to a listening or reading activity of a component.
  * *Package*: It is an element that is used when making complex diagrams. In particular, it allows elements to be grouped in order to improve the representation of the diagram.

- *Data flow diagram*: The DFD is a diagram that allows the graphical representation of how information flows within the system considering the several activities performed by an external entity such as a user. The potential advantage of realising a DFD is to identify the system's functionalities and the relationships between the elements in order to detect possible problems and ambiguities in the realisation of the system. For the realisation of a DFD, it is important to follow a precise notation in order not to create ambiguity about the temrinology to be used. Like the deployment diagram, the DFD also has a precise symbolism and among the main elements (visible in Figure 2.3), there are:

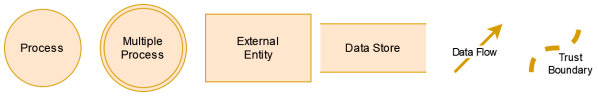

Figure 2.3: DFD elements

  - *External Entity*: The external entity is an element external to the system identified as the source or destination of the data flow. It is typically represented by a geometric shape such as a rectangle with a unique name identifying it. An example of an external entity may be a user or a hardware device that exchanges data with the system.
  - *Process*: A process is represented by a geometric shape similar to a circle in which an identifying name can be entered. In addition, it makes it possible to identify the activities and functions performed within the system. Each process must have at least one data input and one data output.
  - *Multiple process*: A multiple process is an element of the DFD similar to a process but with the purpose of defining the presence of multiple processes within it. It is represented by two concentric circles.
  - *Data store*: Typically, the data store is an entity in which system information is stored. Typically it is directly connected to a process in which information exchange occurs. Each data store should have at least one data flow in and one data flow out.
  - *Data flow*: The data flow is a line that defines the connection between external entities, processes and data stores and defines the flow of information from one element to another.
  - *Trust boundary*: The trust boundary is an element of the DFD that allows defining the points in which the trust level changes within the system. The trust boundary is represented by a dotted straight line where the type of boundary can be specified.

- *Identify*: In this phase, it is essential to identify potential threats that could compromise the system. After creating the Data Flow Diagram (DFD), it is necessary to proceed through a series of steps:

  1. Develop a table assigning the relevant STRIDE threats to each element of the DFD, in order to obtain a preliminary overview of the general threats identified in each part of the system.
  2. It is possible to use tables created in the previous step to develop "attack trees", diagrams that graphically represent the threats in order to obtain specific threats.
  3. Once the threats have been identified, a risk value can be assigned considering the likelihood and impact factors. The

value obtained could correspond to four possible levels: Low, Medium, High and Critical.

- *Mitigate*: In this phase, it is important to mitigate the threats and respective vulnerabilities found in the previous phase by defining appropriate countermeasures.

- *Validate*: In this last phase, it is important to verify that the requirements defined in the previous phase are implemented correctly.

2.3.2 OWASP Threat Modeling

The "OWASP Threat Modelling" is a methodology developed by OWASP with the aim of identifying and evaluating security risks for an application. This methodology allows to analyse the system by considering the point of view of an attacker and how he might exploit vulnerabilities to attack the system. This methodology can be divided into three main steps that allow the realisation of the OWASP threat modelling:

1. The first step allows to decompose the system in order to understand the application and interactions between the elements within the system. To do this, OWASP uses tables to identify the main elements of the system:

    - *External dependencies*: The external dependencies table allows to define the elements that are external to the system but depend directly on it. An example of an external dependency could be software developed by a third-party company.
    - *Entry points*: The table of entry points is useful to identify all possible points in the system where the exchange of information with the external environment takes place. An example of entry points could be I/O interfaces or certain functionalities such as the possibility of connecting the device in a network.
    - *Assets*: An asset is an element that has value for a company that owns it. Anything that has an impact on the security of the system can also be identified as an asset. For this reason, all the functionality within the system that have an impact on security can be considered as assets. The creation of this table makes it possible to identify the assets internal to the system.
    - *Trust levels*: The table of trust levels is useful for identifying users who can access the system. It allows a distinction to be made between the types of privileges a user must have in order to access the different functionalities of the system.

This methodology uses these tables for the realisation of data flow diagrams, inspired by the STRIDE methodology.

2. The second step is related to the identification and classification of threats. In this case, a threat list is defined using the STRIDE methodology so that a threat analysis can be carried out. This analysis evaluates threats by considering factors relating to likelihood (the probability of a threat occurring) and impact (relating to the dangerousness of a cyber attack). Specifically, the risk value is calculated through the product of likelihood and impact. To make this risk assessment, OWASP uses "Threat Tree Diagrams", diagrams in which, starting from a threat, it is possible to identify the associated vulnerabilities and to indicate what can be implemented to mitigate vulnerability. In addition, OWASP recommends "Use and Abuse cases", diagrams that allow to identify vulnerabilities within the system by considering how a legitimate user can use the system or an attacker can exploit vulnerabilities to attack the system. OWASP uses the DREAD methodology in combination with STRIDE to assess the risk of each threat. In particular, DREAD provides risk factors that can be considered as metrics to which a useful score can be associated.

3. The third and final step allows the determination of countermeasures related to the threats detected in the previous step and, for each type of threat, it associates mitigation techniques.

2.4 Risk Assessment

Risk assessment is a process that allows the evaluation of threats that may attack a system. This process allows companies to make decisions on how to manage the identified threats by evaluating the associated risk. Risk is the main element in this process and it is defined [11] via the following relationship:

$$R = f(P, G) \tag{2.1}$$

where:

- **P** represents the likelihood of a harmful event occurring.
- **G** represents the severity of the damage and it is called "impact". It also defines the severity of the consequences if a damaging event occurs.
- **R** represents the risk of a threat occurring in relation to the two factors P and G.

The combination of likelihood and impact provides a mathematical function for risk assessment. Several methodologies for risk assessment exist [11] and are generally divided into:

- **Inductive method**: The inductive method assumes the presence of a malfunction of the hardware or software component within the system to identify potential consequences.
- **Deductive method**: The deductive method hypothesises a final event with the aim of tracing the events that caused it.

Risk analysis methods can also be classified according to different approaches such as:

- **Qualitative method**: This method is not based on mathematical expressions but uses a descriptive method to estimate the risk. The result of the assessment is not a numerical value but is often associated with a string that can take the qualitative value of "Low", "Medium" or "High", depending on the severity of the threat.
- **Quantitative method**: This method is based on mathematical expressions and considers several metrics to which scores are assigned. The result is a numerical value that defines the value associated with a given threat. This methodology is usually adopted to carry out a detailed assessment.
- **Semi-quantitative method**: This method is a hybrid approach of the previous ones. Risk is calculated using a mathematical expression but in a simplified manner. It is possible to consider general metrics to which scores are assigned.
- **Multi-criteria method**: In this method, the risk is calculated by considering different metrics according to the threat being considered. In addition, an approximate view of risk assessment is maintained by considering quantitative aspects. This is a flexible methodology in which subsequent corrective actions can be implemented.

The several methods mentioned are characterised by different purposes, but all follow the same steps for carrying out risk assessment. These can be summarised in three main steps:

1. *Threat identification*: In this phase, all threats that could affect the system to analyse are identified. It is possible to use historical data or checklists.

2. *Risk evaluation*: This step changes according to the type of method is possible to use. For example, it is possible to choose a qualitative or quantitative method.

3. *Risk prioritisation*: At this stage, it is possible to order the risk values obtained in order to prioritise the most urgent cases or those requiring the most attention.

Depending on the method chosen for risk assessment, there are several different techniques, and the choice depends on the purpose to be achieved. Following the literature, the most common qualitative techniques are:

- *Historical analysis*: An analysis of data is carried out considering different sources and is useful to prevent damaging events that have already occurred.

- *Checklists*: Danger or error checklists are created in order to quickly respond to design specifications and understand which features are implemented.

- *HAZOP analysis*: This analysis makes it possible to identify the risks associated with an activity within the company by comparing the opinions of different employees.

- *SWIFT*: This is a study that allows risks to be identified from the definition of hypotheses in order to cover anomalous cases where a threat could arise.

  Instead, the most common quantitative techniques are:

- *FMEA (Failure Modes and Effects Analysis)*: This analysis makes it possible to identify the causes and effects of possible anomalies that may affect a system.

- *Security audit*: It consists of collecting information on company security through interviews and questionnaires.

2.4.1 OWASP Risk Rating Methodology

There are several methodologies with different approaches to carry out a risk assessment, and the "OWASP Risk Rating Methodology" [12] is an example of these. It is developed by OWASP and allows through successive steps the risk assessment on threats and vulnerabilities that could alter a system. As OWASP states, the choice to carry out threat modelling is only the initial step to ensure the persistence of the product's life cycle, but it is also important to estimate which risks could alter the proper functioning of the system and to understand which risks it

is important to prioritise. This approach performs the risk assessment by considering impact and likelihood factors. Moreover, it is based on a quantitative approach in which risk values are mapped onto a risk matrix in which each value is associated with a string like "Known", "Low", "Medium", "High" and "Critical". In this matrix, the product of the values obtained from the likelihood and impact factors is calculated. This methodology is based on 6 different steps:

1. *Risk identification*: The first step is to identify the risk related to a given threat that could compromise the target system. It is preferable to consider the worst case so that the company can have an overview of the risk for each threat in order to prioritise and begin threat mitigation.

2. *Likelihood estimation*: The likelihood estimate is calculated by considering several metrics. Each metric has an associated set of scores describing how likely a given event is to occur.

3. *Impact estimation*: Impact estimation is calculated by considering several metrics. Each metric has an associated set of scores describing how likely a given event is to occur.

4. *Risk Severity*: In this step, risk is calculated using the scores provided in the previous steps. Specifically, for likelihood and impact, the score is calculated through the arithmetic mean of the scores provided previously where each score can be assigned three different levels, as can be seen in Table 2.1.

Likelihood and Impact levels	
0 to <3	Low
3 to <6	Medium
6 to <9	High

Table 2.1: Likelihood and impact levels

Once the two scores are obtained, a new average is calculated to obtain an overall value. This value is compared with a matrix (Table 2.2) that provides the severity of the associated risk.

Overall risk severity				
Impact	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Known	Low	Medium
		Low	Medium	High
	Likelihood			

Table 2.2: OWASP risk matrix

5. *Deciding what to fix*: Once the various scores have been obtained, it is important to decide what to fix. A company may decide to proceed by considering problems that have a high risk value. Sometimes the company may decide not to follow this order and prefer to solve problems that it considers more important than others.

6. *Customising the model*: It is possible that some scores may not reflect the actual risk of a threat, and for this reason you may decide to customise the scores according to other factors or metrics to get a more accurate assessment.

Chapter 3

Related works

In [13] the authors analysed the different threat modelling techniques that can be applied within the software development process. The aim of the work is to demonstrate the importance of integrating threat identification and assessment into a single process considering the different levels of risk associated with each threat. Threat modelling is used today in different applications such as online and mobile services, or within more complex processes where there is the interconnection of multiple devices such as the automation and automotive sectors. In this regard, a collection of academic articles has been compiled in Table 3.1, which shows a division of the articles according to the field of application. In particular, each author has been associated with the title of their article and the application of the proposed methodology in order to have a general overview of the different threat modelling methodologies that exist today.

Titles	Applications
Threat modeling of a mobile device management system for secure smart work. [14] Security for Mobile Operators in Practice. [15]	Mobile device
Introducing OSSF: A Framework for Online Service Cybersecurity Risk Management. [16] Threat modeling approaches and tools for securing architectural designs of an e-banking application. [17]	Online service
Energy-Theft Detection Issues for Advanced Metering Infrastructure in Smart Grid. [18]	Smart grid
Modular analysis and modelling of risk scenarios with dependencies. [19]	Power supply system
Towards a Security Architecture for IP-Based Optical Transmission Systems. [20]	Telecommunication systems
A STRIDE-Based Threat Model for Telehealth Systems. [21]	Telehealth system
Threat Modelling and Risk Assessment Within Vehicular Systems. [22]	Automotive industry
A methodology for the risk analysis of industrial control systems	Industry 4.0

Table 3.1: Threat modelling applications

The table shows that there are different areas of application of threat modelling and different methodologies have been developed in each of these cases. In some cases, more than one study has been conducted for the same area of application in order to cover specific cases. In [23] the authors collected a set of academic articles on different types of threat modelling and carried out an analysis of the existing methodologies and approaches used. Their aim was to gather as much information as possible on the various existing methodologies by categorising the various approaches used. From the results obtained, there is a tendency to use graphical representations to allow the reader to understand the proposed methodology, and there is also evidence of a greater realisation of manual methodologies than automated ones. NIST (National Institute of Standards and Technology) [24] has published a guideline on carrying out risk assessment consisting of several steps that can be applied in different application contexts. In this guideline, possible approaches to assessment are presented, identifying the main advantages and disadvantages of each approach. It can be seen that a quantitative approach is used for cost-benefit analyses, but the scoring of the different factors is not always clear and explanations may be unclear. Furthermore, it may be accurate and consistent in results, but can have negative effects such as cost in terms of time and the need for employee training. Instead, as NIST states,

a qualitative approach uses a category-based assessment by associating a descriptive expression with a range of values. This approach does not allow for an accurate assessment due to the small ranges. In fact, if a category of values is not associated with a description, it can lead to misunderstandings. One of the sectors most affected by cyber attacks in recent years is industry. The objective of this thesis is to propose a new methodology for the risk assessment of threats that may affect devices used in this area. In February 2020, in [25] the author provided a general overview of the importance of conducting a risk assessment within the industry 4.0 ecosystem. This article analyses possible threats and vulnerabilities that can cause damage to companies and their control systems. By using different tools, it was possible to group a set of cyber-attacks and classify them following precise metrics. Suzen analysed the main threats that could compromise company security, such as a lack of staff training or a weak network infrastructure. Then, measures to prevent these vulnerabilities were provided. This work has led to the conclusion that one of the possible solutions to minimise the damage caused by cyber attacks is the adoption of one or more risk assessment methodologies in relation to the application and system to be protected. From the conclusions provided by [25], an analysis of the different risk assessment processes was carried out in this chapter, considering the different methodologies that can be applied in order to understand which methodologies are applied within the industrial scenario and in which context. Several studies [22] [26] [13] [27] have been carried out on different domains of industrial application. In [26] the authors published a paper proposing a risk assessment methodology for calculating the financial losses caused by cyber attacks performing a cost-benefit analysis on the adoption of hardware or software devices. In [27], an automated risk assessment methodology was proposed for evaluating possible risks to critical devices related to the Industrial Control System (ICS) but still the methodology is not precise and accurate enough on the scores and needs to be extended to the attack models analysed. In [22] the authors analysed some threat modelling and risk assessment methodologies and applied them to the automotive sector. They provided an overview of the most popular methodologies considering threat modelling and risk assessment. Moreover, they carried out a risk assessment by applying all the different proposed methodologies to understand which of them is the most appropriate for the automotive domain. The result of this study showed that STRIDE is a valid choice for automotive threat modelling. This study concluded that the "OWASP Risk Rating Methodology" is not appropriate for this domain as it does not emphasise asset information on each specific threat. The OWASP methodology is also analysed in this thesis to make a comparison with the proposed methodology. The

result is the same as that of [22] and shows that OWASP does not use precise metrics for each type of threat causing an inaccurate assessment. In [22], [26] [13], and [27] is evident the importance of integrating the processes of threat identification and threat assessment within a process in order to achieve a comprehensive analysis of the system from a threat perspective. In [13] authors analysed traditional risk assessment and threat modelling techniques such as STRIDE, PASTA and TRIKE and came to the conclusion that STRIDE, individually, is not sufficient to carry out a risk assessment because it does not allows the quantification of the cost of identified threats and does not allows the generation of a list of threats. For this reason, to be able to carry out threat modelling that also includes a detailed risk assessment phase, it is possible to use a hybrid approach that allows several threat modelling methodologies to be combined. In 2022 [28], the authors realised a threat modelling that allows the STRIDE methodology to be combined with the DREAD methodology. Indeed, while the STRIDE methodology allows threats to be identified and classified, the DREAD methodology allows vulnerabilities detected in the previous phases to be evaluated. DREAD allows scores to be assigned to metrics divided into categories to subsequently calculate their average. Similar work was carried out in 2016 by [29] in which a quantitative risk assessment methodology was proposed by combining the two methodologies STRIDE and CVSS. This process allowed for an accurate assessment of the vulnerabilities detected. The STRIDE methodology was used to build an attack tree to obtain the vulnerabilities for each threat and then the CVSS methodology was used to assign a risk value to the vulnerabilities. The work of this thesis aims to provide a new methodology that makes the risk assessment process flexible and efficient. This methodology takes inspiration from STRIDE for the analysis of the system and then by means of a qualitative approach the system analysis is carried out from a set of specific threats.

Chapter 4

Methodology

In this chapter, a new methodology for the threat analysis and risk assessment of industrial devices is proposed.

4.1 Proposed methodology

This thesis is the result of a collaboration between the University of Verona and V-Research with the aim of realising a flexible and efficient methodology for risk assessment that is compliant with IEC 62443-4-1 standard (see 2.2). The proposed methodology is divided into six different steps:

1. **Device identification**: The first step allows to identify the device to apply this methodology.
2. **Device analysis**: This step allows a complete analysis of the device considering its internal structure and the external entities with which it communicates.
3. **Threat identification**: The third step of this methodology allows the identification of threats that may compromise the device.
4. **Risk evaluation**: The risk assessment allows a score to be associated with each threat detected.
5. **Mitigation**: The mitigation phase makes it possible to define a set of solutions to mitigate the risk associated with each threat and to understand how the solutions adopted can change the risk assessment.

The next subsections will present each of the steps of the methodology.

4.1.1 Step 1: Device identification

The device chosen to implement this methodology is an HMI (Human Machine Interface) produced by a V-Research customer company, designed for monitoring and controlling industrial operations. This step is based on the first two sections of "Practice Two" (see 2) of the IEC 62443-4-1 standard:

1. The initial section defines the "Product security context", a guideline to assist employees in identifying the application context of the product.

2. The second section introduces the concept of "Threat Modeling" and provides a list of features for applying this process.

Product security context

Practice 2 (see 2 for further details) of the IEC 62443-4-1 standard defines a section titled "Product security context", offering guidance on recognizing the operational environment of a device within an industrial process. The core of the risk assessment process in this methodology is to identify the security context of the product. This makes it possible to identify the environment in which the device operates and facilitates the identification of potential threats in subsequent steps.

This section of the standard defines four key points for identifying the context in which the device is used. These points are categorised into:

1. **Location in the network**: The aim is to gather useful information about the network used by the device within the industrial environment, such as whether it has a network connection or the network topology.

2. **Physical or cyber security**: The standard recommends documenting both the physical and cyber security aspects implemented within the environment where the device is used.

3. **Isolation**: It is necessary to determine whether the device is connected to the network. A device without network connectivity has a reduced risk of potential cyber-attacks.

4. **Potential impact to the environment**: It proposes the assessment of environmental damage resulting from the misuse or potential violation of the device.

    - *Defence in depth strategy*: The concept of "deep defence" is based on defining a set of security layers to safeguard the system and reduce the likelihood of successful cyber attacks.

The implementation of security levels depends on the specific environment in which the device is located. The goal in this point is to identify the different security levels implemented in the environment in which the device is used.

The methodology includes a template designed to illustrate the four points defined in the standard section. For each point, a series of questions was formulated to acquire information on the environment in which the device is used by the company. In this regard, the template created is illustrated below, and for each of the questions there are the answers provided by the company producing the device adopted for this methodology. The first set of questions concerns "Location in the network" where six questions were defined to understand how the device is connected to the network. In particular, several information can be obtained through these answers, such as whether the device is used in an industrial environment, whether it is connected in a private network and whether it can be accessed remotely:

1. Does the device have internet access?
   - ☒ Yes.
   - ☐ No.
2. Which types of networks are involved with the device?
   - The device supports different types of network configurations such as LAN, intranet and VPN connections.
3. Is the device installed on a private network?
   - ☒ Yes.
   - ☐ No.
4. Is the device accessible from a corporate network or even from a remote location?
   - Yes, the device is accessible from a corporate network and a remote location.
5. In what types of networks is the device used? Select your choice:
   - ☒ Industrial networks.
   - ☐ Clinical networks.
   - ☐ Military networks.
6. Does the device have a central or peripheral role in the topology of the network?

- The device is part of a group of devices inside the network with the objective to monitor the industrial process.

For "Physical and cyber security", two general questions were formulated to understand the types of physical and IT security implemented in the environment in which the device is located:

1. Does the device require physical access control to ensure security?
   - Yes, access control is required when it is necessary.
2. Does the device require specific controls regarding network and information security?
   - The device must be checked periodically, and access control must be documented.

The answers show that the environment ensures a controlled access policy, and each access to the environment is carefully monitored and documented. For the point concerning the "Isolation" of the device, a single question was defined in to understand whether the device is networked:

1. Is isolation from the mains required for the product?
   - No, the product is connected to the network to send operational data.

For this application, the device requires a network connection to receive data on the operations of other connected devices and to manage control operations. The "Potential impact to the environment" was divided into two groups of questions to include the "Defence in depth strategy". The initial set of questions were included to understand whether improper use of the device could cause damage within the environment in which it is located:

1. Is the device installed in a safety-critical environment?
   - The device is installed in a controlled industrial environment with different security levels.
2. Can a violation of the device cause economic and/or reputation damage to the company?
   - Yes, a violation of the device can cause economic and repudiation damage.

3. Is the device located in a network where other devices can be reached?

    - Yes, the device is in a network where other devices are present.

From the answers provided, it can be seen that the device is interconnected with other industrial devices and a violation of the device could lead to repudiation and financial damage. The "Defence in depth strategy" is an approach based on several principles, which allows the identification and diversification of security levels to increase the resilience of the system against attacks. In these questions, the goal is to understand how many security levels were implemented or could be implemented to make the device secure:

1. Does the product allow you to implement a policy that defines the use of secure passwords?

    - Yes, the device has many features that allow you to implement secure password policy.

2. Does the product provide a backup and restore mechanism?

    - Yes, the device has a factory reset functionality that allow you to restore the system; moreover, the device is connected to the network where data are stored in a secure database.

3. Is it possible to define a mechanism for managing user privileges?

    - Yes, Inside the company each employee has a precise role and precise privileges and only the authorized employee can use the device.

4. Is remote access to the device possible?

    - Yes, there is a functionality that allow you to manage the device through remote access.

The responses to these questions offer information about the characteristics of the device's usage environment, taking into account different security aspects across various levels. This information helps to assess the overall safety of the environment for the device, facilitating potential improvements during the design phase.

4.1.2 Step 2: Device analysis

The second step of the methodology aims at identifying the internal and external elements of the HMI device and understanding their communication dynamics. The execution of this step is based on the "OWASP

Threat Modeling Methodology" (2.3.2), that supports a similar process. However, in this thesis, a distinct approach is employed, compliant with the guidelines provided in the IEC 62443-4-1 standard. Specifically, the second section of Practice 2 of the standard, known as "Threat model", provides guidelines on executing the threat modeling process. This section defines the elements to be identified within the threat modeling process such as external entities and internal processes defining data flow and security boundaries. Three types of graphical representations were selected to illustrate these characteristics:

- **Deployment diagram**: This diagram provides an overview of the HMI device, helping to identify the main entities, components, and communication protocols implemented.
- **Data tables**: A series of data tables were realised to represent the main system assets, entry points, and external dependencies of the system.
- **Data Flow Diagram**: This diagram allows the identification of the main processes associated with the use of the HMI device. Specifically, it helps identify data stores, trust boundaries, and the data flow between different processes.

Deployment diagram

From the initial stages of the risk assessment process, it is important to obtain a lot of information about the device to be analyzed. This phase allows us to understand the elements with which the device communicates within its usage environment and allows us to identify its internal components. To respect these requirements, a deployment diagram was adopted in this thesis (as can be seen in Figure 4.1).

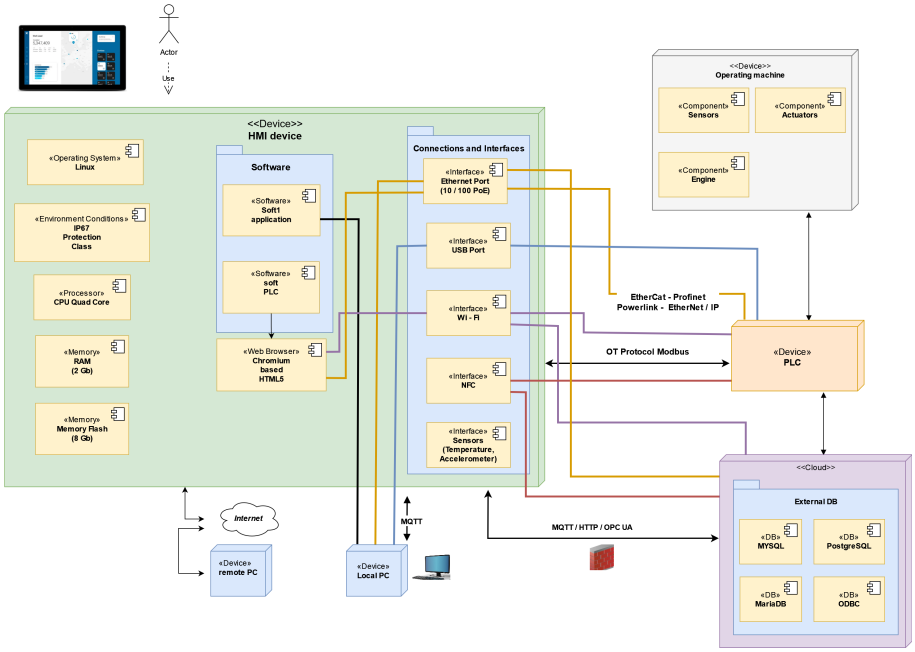

Figure 4.1: HMI device deployment diagram

Within the diagram, some of the fundamental components of the deployment diagram (see 2.2 for further details), such as nodes, components, and packages were adopted. Each node and component is assigned a stereotype to provide a descriptive name for that element. Specifically:

- *Nodes*: This scheme contains six nodes, with the primary node associated with the HMI device acting as the central component of the system. These nodes represent the foundational elements of the system. Notably, the HMI node establishes direct connections to the PLC, Cloud, and two PC nodes, facilitating data exchange among them. This connection allows the identification of devices involved in data interactions. The operating machine node is directly linked to a PLC, allowing various machine components to transmit operational information to the PLC, while the PLC sends commands to change machinery operations. Additionally, two PC nodes are present, indicating the capability to communicate and transfer data through a local PC or a PC located remotely, using an appropriate communication protocol.

- *Components*: The components are distributed among various nodes, with specific organisation within the main node, structured into packages for more clarity. Within the HMI node, it is possible to distinguish software and hardware components integrated in the device. Among the software components, there is the Soft1

software that is a key element that enables the management and customisation of the main interface of the HMI device, optimising the monitoring of industrial operations. I/O components include an Ethernet port, a USB port and a Wi-Fi interface, which facilitate the connection with the external environment and other devices. Consideration of these components makes it possible to identify possible access points that could be exploited by potential attackers in order to compromise the system.

- *Connectors*: Within the deployment diagram, connectors allow communications between the various components and with external nodes to be delineated. In particular, two types of connectors were used for this diagram:
  - The *association connector* is used to generically define the relationship between two components or nodes through a link where information is exchanged in both directions.
  - The *communication path* provides a more detailed definition of how information flows between components or nodes. In the context of the diagram, certain connectors include a description of the type of protocol supported for communication between elements.

The creation of this diagram offers an overview of the device under consideration. Moreover, from a cyber security perspective, this diagram provides information about potential access points and devices that could be exploited by attackers to compromise the device or steal sensitive data.

Data tables

In this section, the analysis process continues considering the hardware system. During this phase, tables containing various aspects of the system were realised individually. The deployment diagram created in the previous phase facilitates the realisation of these tables by offering an initial representation of the system elements. In this context, the components and functionalities of the device are described and analysed using tables. Four tables were realised:

- *External dependencies table*: Table containing a description of the devices that interact externally with the system and the supported hardware and software components.
- *Entry points table*: Table containing a list of device components that can be exploited as entry points for information exchange.

- *Assets table*: This table contains elements (data or functionalities) that have value to the company and are of interest to potential attackers.

- *Trust levels table*: This table defines the levels of security guaranteed by the system in order to distinguish the users and their respective roles that have access to the system.

The purpose of the external dependencies table is to identify external elements of the device that interact with it. Usually, these dependencies are selected elements of the organisation and are monitored to prevent potential threats.

External dependence		
Components	**ID**	**Description**
Physical devices	ED - 1	The device can be connected to a **PLC** for the purpose of exchanging machinery information.
	ED - 2	The device can be connected to a **personal computer** to exchange sensitive data or update software within the system.
Cloud	ED - 3	The device has the ability to exchange sensitive information through an **external database** with other devices
Software	ED - 4	**Soft1** is a project management application for monitoring industrial processes.
	ED - 5	**Soft PLC** is the development environment installed in the device that allows centralised programming of the control system

Table 4.1: Table of external dependencies

The Table 4.1 was organised in three distinctive columns:

- *Components*: A unique name is associated with each component external to the device.

- *ID*: Each component is associated with a unique identifier (ID).

- *Description*: A detailed description is given to each component.

Components external to the device were categorised in the table as follows:

- *Physical Devices*: Physical devices represent the external elements with which the HMI device interacts, such as PLCs or PCs, to facilitate data exchange.

- *Cloud*: The cloud manages and stores the information flowing within the system and between the various external components.
- *Software*: External software integrated in the device is classified as an external dependency because it can be developed by third-party companies.
- *Security requirements*: The security requirements define the protocols and cryptographic algorithms supported within the device.
- *Architecture*: From the initial design stages, the company must choose the architecture of the device. For example, the choice between a Linux distribution or a Windows system may have different consequences in terms of resources and security.
- *Web*: The decision to connect the device to the Internet and use a web browser can have significant security implications, depending on the type of application used for the web connection.

For a detailed analysis of the device, in addition to considering its constituent elements, it is important to understand which users can access the device and what operations they can perform. For this reason, Table "Trust level" (4.2) has been realised to answer these needs.

Trust level		
ID	**Name**	**Description**
TL - 1	Employee	An ordinary employee within the company
TL - 1.1	Employee with valid login credentials	An employee who want to use the HMI and is logged in using valid credentials
TL - 1.2	Employee with not valid login credentials	An employee who want to use the HMI and is no logged because he is using invalid credentials
TL - 1.1.1	Employee with high privileges (Admin)	An employee with valid credentials that has the ability to change system settings. He can create guest user inside the system and send commands to change machinary settings.
TL - 1.1.2	Employee with low privileges	An employee with valid credentials that hasn't the ability to change system settings but has the possibility to monitor operations

Table 4.2: Table of trust levels

The table consists of three columns in which users are distinguished according to their privileges. The columns are subdivided as follows:

- *Name*: Each specific type of privilege available to a user is associated with a unique name.

- *Id*: Each user privilege is associated with a unique identifier (ID).
- *Description*: A detailed description of the relative privilege levels for each user is provided.

The table distinguishes three categories of users who may have access to the device:

- *Employee*: An employee is a user affiliated with the company. Within the table, various types of access privileges were differentiated according to the role an employee may have:
  1. *Level 1*: Generic employee who is not granted access to the system.
  2. *Level 2*: Employee with valid credentials for access to the system.
  3. *Level 3*: Employee with access to the system, valid credentials, and who may have limited or high privileges. In addition, a distinction is made between employees with valid credentials who have the ability to insert external software or hardware.
- *System technician*: System technician with special privileges who has access to functions not available to other employees.
- *Guest user*: The guest user is a user from outside the company using the device. The guest user can be registered from the control panel of the HMI device and it is possible to specify the type of privileges that the user may possess. In this case it was decided to use a second layer distinguishing users with high or low privileges in relation to the type of user using the system.

This table is useful for the subsequent tables to associate the trust levels with each component and functionality of the system. In fact, the distinct privileges in the table above were mapped within the Table "Entry Points" (4.3). Identifying entry points to the system helps to understand which elements allow the exchange of information with the external environments. These are often considered the main elements that attackers exploit to perform malicious actions.

Entry point				
Category	**ID**	**Name**	**Description**	**Trust levels**
I/O Interfaces	EP - 1	Ethernet port	The ethernet port is used by the employee to communicate with other devices and to install the Soft1 application into the HMI	(TL – 1) Employee (TL – 2) System technician (TL – 3) Guest user
	EP - 2	USB port	The USB port is used by the employee to install or update software application into the device	(TL – 1) Employee (TL – 2) System technician (TL – 3) Guest user
	EP - 3	Debug port	Debug ports are special I/O ports within the device that allow the authorised user, during maintenance, to access sensitive data to perform diagnostic operations.	(TL – 2) System technician
Software	EP - 4	Soft1	Soft1 is an application developed by the company for the purpose of monitoring and sending commands to other connected devices.	(TL - 1.1) Employee with valid login credentials (TL - 3.1) Guest user with high privileges
	EP - 5	Web browser	The web browser enables the employee to browse the Internet.	(TL - 1.1.1) Employee with high privileges (Admin) (TL - 3.1) Guest user with high privileges

Table 4.3: Table of entry points

This table is composed by five columns:

- *Category*: Each entry point was divided into a group of categories.
- *Name*: A unique name is associated with each specific type of entry point.
- *Id*: Each entry point is associated with a unique identifier (ID).
- *Description*: A description is provided for each trust level.
- *Trust level*: The trust levels obtained in the previous table are mapped for each entry point.

This table contains the components that allow the exchange of data with the external environment. The table considered the software and hardware components that allow users to use the device and permit the exchange of information. In addition, there are some system functionalities that allow the device to connect with the external environment and exchange data.

The last table was realised to identify the assets within the company. It considers the value that the company attributes to each element and its potential impact on the security of the device. In particular, if an element has a significant impact on security, it could arouse the interest of an

attacker by becoming an element to be protected and therefore an asset. Following this logic, the main asset covered by this study is the HMI device. In order to conduct a more in-depth analysis, functionalities that could cause security damage, if used improperly, were also considered as assets.

Asset				
Category	**ID**	**Name**	**Description**	**Trust levels**
Employee	A - 1	Employee login credentials details	The login credentials that an employee will uses to log into the HMI	(TL - 1.1.1) Employee with high privileges (Admin)
System	A - 2	Execution of external code	It is possible to execute external code to update or enhance existing software; only valid software must be executed on the HMI.	(TL - 1.1.1) Employee with high privileges (Admin) (TL - 1.3) Employee with valid external software / hardware
	A - 3	Ability to connect the HMI to other devices	Connecting the HMI device to other devices enables fast data exchange for better monitoring	(TL - 1.1.1) Employee with high privileges (Admin)
	A - 4	Ability to send commands to connected devices	The HMI device via its interface provides the ability to send commands to manage machineries and their production	(TL - 1.1.1) Employee with high privileges (Admin)
	A - 5	Access session to the web service	The HMI supports Chromium and allows access to web services offered	(TL - 1.1.1) Employee with high privileges (Admin)
	A - 6	Details about machinaries informations (Monitoring)	The HMI device displays the data of the machinery to which they are connected for continuous monitoring	(TL - 1.1.1) Employee with high privileges (Admin) (TL - 1.1.2) Employee with low privileges (TL - 1.4) Guest user with high privileges (TL - 1.5) Guest user with low privileges

Table 4.4: Table of assets

The Table 4.4 is composed by five distinctive columns as follows:

- *Category*: Each asset was divided into a group of categories.
- *Id*: Each asset is associated with a unique identifier (ID).
- *Name*: A unique name is associated with each specific asset.
- *Description*: A description is provided for each asset.
- *Trust level*: The trust levels obtained in the previous table are mapped for each asset.

In this case, assets were divided into three distinct categories:

1. *Employee*: The decision to include the employee category is motivated by the possible interest of an attacker in employee access credentials and associated personal data.

2. *System*: Within this category were aggregated the several functionalities considered assets, which can significantly affect business operations and dynamics.

3. *Company*: In the "Company" category, assets that include sensitive information of the company and their devices were categorised.

Data flow diagram

The DFD (data flow diagrams) (see 2.3.1 for further details) is a diagram that allows the graphical representation of the information flow and internal processes of the HMI device. The potential advantage of realising a DFD is to detect potential inconsistencies in the realised system and possible vulnerabilities in order to improve process development. In this thesis, in order to gain a detailed understanding of the HMI device, four DFDs diagrams were realised. The "context diagram" (or "level 0" diagram) is the first diagram that represents (Figure 4.2) the device. The purpose of this diagram is to identify the external entities with which the device communicates.

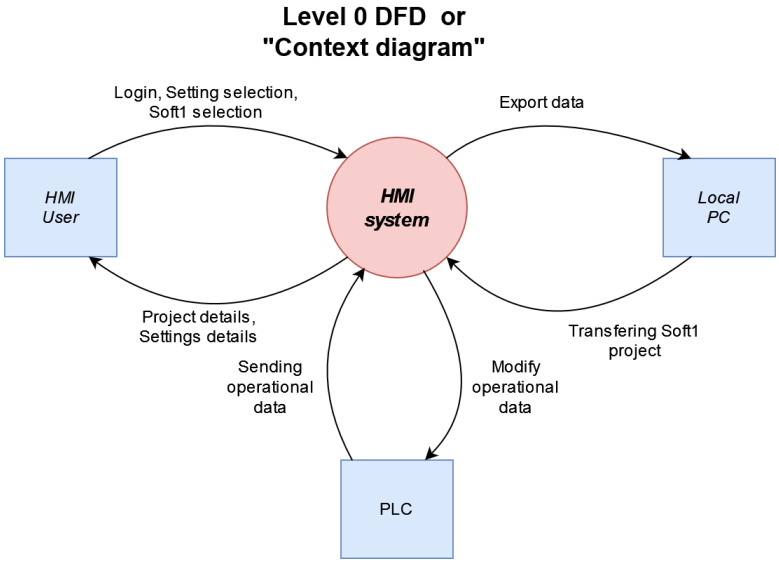

Figure 4.2: DFD level 0

In particular, three main external entities were identified:

- *HMI user*: The HMI device user is the entity that uses and performs operations on the device. This entity is connected to the HMI system, via data flows in which it receives information about the operations performed.

- *PLC*: This entity is represented by a PLC and communicates with the HMI system. Through this connection, the PLC sends commands on the operations of the machinery involved in the industrial process. In this case, the HMI sends requests on changing the operations involved and receives the result of the operation from the PLC.

- *Local PC*: This entity is a personal computer and is used for the transfer of the HMI device's control panel software. The connection between the HMI device and the PC allows data to be exported from the HMI device.

Then, it was realised the DFD diagram of "level 1", shown in the Figure 4.3, in which the main process was decomposed into other, more detailed processes.

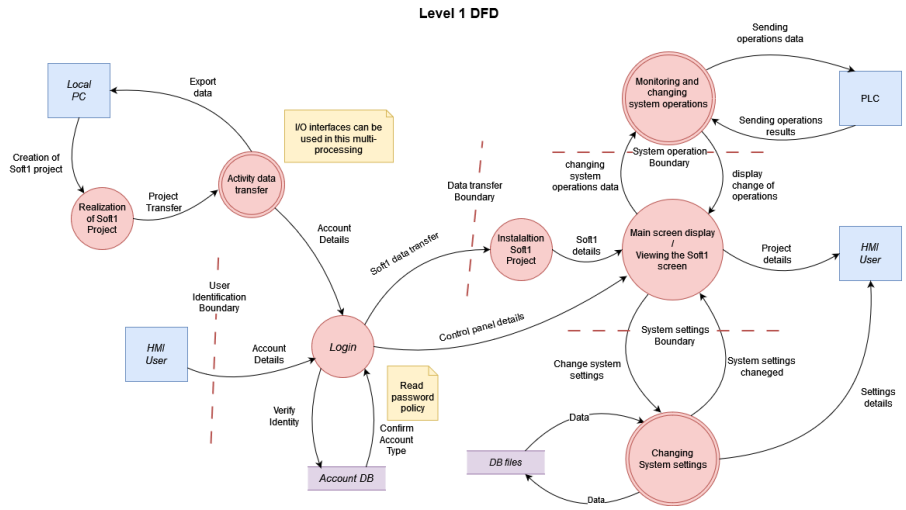

Figure 4.3: DFD level 1

Within the diagram, the process of using the HMI device by an authorised employee is depicted. In this case, the symbolism is detailed. In fact, there are:

- *External entities*: The external entities are the same as in the previous diagram, but in this diagram the main subjects are the processes.

- *Processes and Multi-Processes*: Processes and multi-processes are the elements in the diagram that are represented in red and are the activities carried out by the user using the device.
- *Data Store*: There are two data stores in this diagram, which allow data to be stored and verified.
- *Trust boundary*: Trust boundary are represented by dotted red lines and indicate the points at which the type of privilege to perform operations changes.
- *Notes*: For better understanding, there are notes in yellow that provide explanations of the process.

The reading of this diagram starts from the left and in particular from the local PC entity. From the local PC, a user has the possibility of realising a project, via the Soft1 software, with the aim to obtaining the graphics of the main control panel of the HMI device. Once the project has been created, it can be transferred to the HMI device via its I/O interfaces. The user must log in with valid login credentials to transfer the project within the HMI device. At this point, it can be seen that the login process also receives an input data flow from a second entity, namely the HMI user. This entity is inserted at this point in case the project is already present within the device and the user needs to log in to the device. For the login phase, the login credentials are compared with a database containing employee credentials. If the credentials are valid, the process can continue and the user can perform other operations, otherwise the user cannot log in. After logging in, if the Soft1 project needs to be installed, the installation proceeds, otherwise the user starts using the device and the main screen is displayed. Once on the main screen, the user can perform two distinct operations:

- The user can change the system settings of the device.
- The user can change parameters and send operations to PLCs with which it communicates.

In this diagram, for a better comprehension, the entity of the HMI user was duplicated and has the same role in both cases. Furthermore, at the points where trust boundaries are present, it means that a different type of privilege is required to continue operations. Indeed, each user within the company has different roles and privileges and only authorised users can perform certain operations. In order to have a higher level of detail of the device's operation, two DFD of "level 2" diagrams have been realised relating to two of the multi-processes present in the level 1 diagram. The first level 2 diagram is an extension of the multi-process related to the

data transfer activity. This representation was chosen because there are different ways of transferring software within the device. Furthermore, the transfer activity within the device allows to understand the operation of the I/O interfaces.

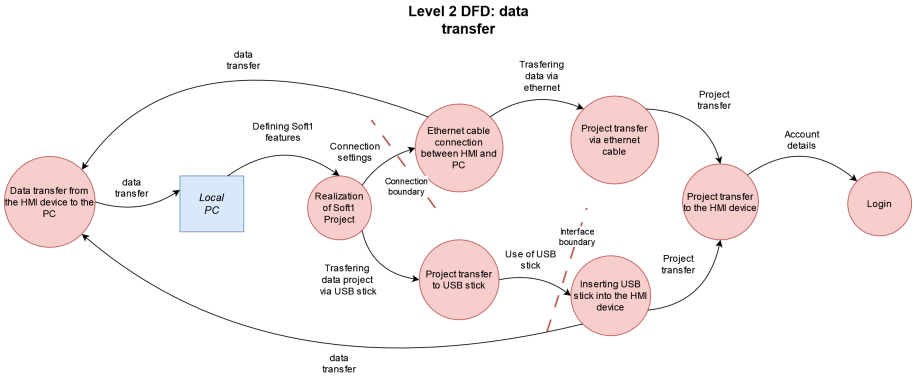

Figure 4.4: DFD level 2: data transfer

As Figure 4.4 shows, the software transfer process was expanded by considering the two main possibilities. In fact, once the Soft1 project is realised, it is possible to transfer it within the device using a USB stick or to connect the HMI and the PC via an Ethernet cable. Two trust boundary have been defined because the transfer of this software can take place via authorised users. Furthermore, it was decided to represent a second level 2 diagram relating to system settings.

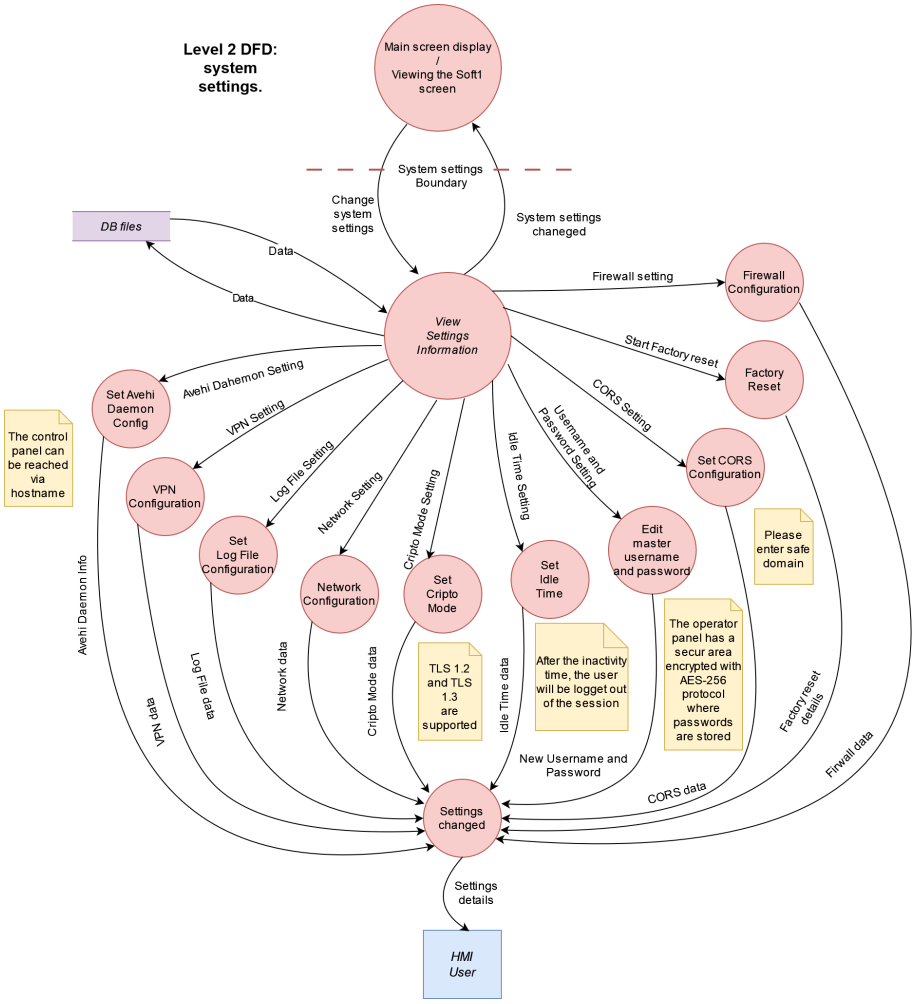

Figure 4.5: DFD level 2: system settings

Figure 4.5 shows the process of setting a functionality within the device. In this case, it has been decided to consider within the representation the possible functionalities that the user can enable from the control panel, and the user can enable one functionality at a time. In this case, notes have been used to inform the user of the features of that particular functionality. The decision to detail the functionalities of the device, is due to the fact that these are considered assets because they have value within the device. In fact, enabling or disabling certain security functionalities can lead to consequences in the production system and therefore represent assets to be considered.

4.1.3 Step 3: Threat identification

This is the step where the contribution of my thesis lies: a new approach for threat analysis and risk assessment. The goal of this step is to identify threats that may target an HMI device. For the realisation of this step, a threat list provided by the V-Research was used, and 31 different threats were identified. An example of a threat in this list can be seen in Table 4.5.

ID	Threat	Category	Description
1	Employee error (accidental or negligence)	Accidental	Accidental errors made by an authorised user (internal or external) when using or maintaining information systems. *Assessment guidance*: At **lower levels** of threat strength (i.e. individuals with limited or no access privileges) errors will generally result in greatly reduced or minimal impact to information systems. At **higher levels** of threat strength (i.e. individuals that were assigned privileged access such as administrators), errors have the ability to cause greater impact to information systems.

Table 4.5: Example of threat list

The purpose of adopting a threat list is to take into account threats that are not only intentional but are linked to cyber attacks by malicious users. The list also includes threats that are caused by environmental and accidental factors. For this reason, each threat was classified into:

- *Accidental*: A threat is accidental if not caused intentionally.
- *Adversarial*: A threat is adversarial if the attacker has the motivation to compromise the device
- *Environmental*: A threat is classified as environmental if it is caused by environmental and atmospheric phenomena.

In addition, each threat is defined by a *description* and an *assessment guide*. In particular, the assessment guide considers two aspects:

- *Lower levels*: These levels define the least significant consequences that a threat could cause. In this case, it may occur but does not have a serious impact on the system.
- *Higher levels*: These levels define the most significant consequences that a threat could cause. In particular, they identify the greatest impact that a threat could have if exploited by an attacker.

In the Table 4.5, the "Employee error" was taken as an example of a threat and was classified as accidental, since an authorised user should not cause damage to the device voluntarily. Guideline describes what can happen if the device is accessed by users with different privileges. In fact, if the user has limited access privileges, there is minimal impact on the device, while if the user is an administrator with several privileges, the impact of this threat is greater. The threat list has the advantage of considering the greatest number of scenarios that can compromise the HMI device thanks to the high level of abstraction at which each threat is described. After defining the list of threats, the next step is to associate each threat with a scenario by identifying in which part of the system that particular threat may occur.

ID	**Asset**	**System or Subsystem Potentially Affected**	**Threat**	**Scenario**
TID-1	HMI		Employee error (accidental or negligence)	**Threat Scenarios**: 1. Technical mistakes, made during the design or development of the software and hardware architectures of the product, that result in security issues. 2. Technical mistakes made during the configuration or installation of the product at the customer site or during operations/provisioning, that result in security issues. **Consequences** (Attack Scenarios - Examples): (A) Disabling a security control or security configuration to perform some maintenance operations that threaten the security of the asset. (B) Logging of sensitive information. (C) Insecure communication due to a mistake in the configuration of the wireless or wired communication. (D) Debug ports/functionalities remain in production. (E) Weak security protocols in use.

Table 4.6: Threat scenario

Table 4.6 was divided into the following columns:

- *ID*: The ID is a unique identifier for each threat analysed.
- *Asset*: The asset is the element that has value for the company.
- *System or subsystem potentially affected*: This column identifies all elements within the device that may be tampered by the threat.
- *Threat*: This column contains the name of the threat taken from the list of threats.
- *Scenario*: A description is given of how the threat may be exploited within the system.

The purpose of this table is to map the threats on the components potentially involved and to define the scenario in which these threats

could occur. The scenario makes it possible to identify the causes and consequences in which a threat may manifest itself. In fact, the scenario is divided into two main parts:

- *Threat scenario*: All possible scenarios in which a threat may alter the device are identified.
- *Consequences*: The consequences of threats are identified within the scenario according to what has previously been described as the threat scenario.

Considering the employee error case, an example of how a scenario can be realised is presented in Table 4.6. In this case, the ways in which this threat may occur, such as during the design or development phase of the device architecture, or the installation of the device, are considered as scenarios. Once the scenarios have been defined, it is necessary to identify the potential consequences of the scenarios considered in the previous step. In fact, if an employee makes a mistake during production, a possible consequence could be that the device does not respond correctly to user requests. As can be seen, scenario realisation is particularly advantageous as it allows multiple aspects of a single threat to be identified.

4.1.4 Step 4: Risk evaluation

Risk assessment is the phase that allows to understand how a threat manifests itself within the system by evaluating the potential effects on security. After the creation of specific scenarios for each threat, it is necessary to calculate its risk value considering two factors: **likelihood** and **impact**.

Likelihood

Likelihood is the first factor analysed to calculate the risk value of a threat. Within this methodology, a qualitative approach was chosen, with the aim of associating descriptive indicators with each threat for the assessment of likelihood. Indicators are defined by considering the consequences of attack scenarios. This approach makes it possible to develop a bulleted list of indicators specific to each threat. In the specific case of the "employee error" threat, three main indicators were identified that can influence the likelihood calculation, as follows:

- *Number of employees*: The participation of a larger number of employees in the system may increase the likelihood of making mistakes, especially if they are not properly trained or aware of security practices.

- *Lack of training*: Lack of employee training can increase the likelihood of making mistakes. Employees who do not know how to do their job correctly may be more prone to make mistakes.

- *Lack of verification of security requirements*: Failure to check security requirements can lead to accidental damage.

The list of indicators can be integrated within the scenario to increase the compactness and improve the reading of the assessment. A larger number of indicators associated with a threat helps to provide a more detailed assessment. In addition, it is essential to assign a likelihood score in relation to the previously defined indicators. As shown in Table 4.7, likelihood is calculated by considering 3 different values in which a string is associated with each value.

Likelihood	
Levels	Points
Low	1
Medium	2
High	3

Table 4.7: Likelihood values.

In this methodology, no specific weights or scores are assigned to the indicators. It is normal that each indicator could have a low or high individual weight influencing the final score. In order to understand how to manage the weighting of indicators, it is important to have a clear understanding of the system and good documentation of previous steps, so that decisions can be made without the need to score them. This choice is intended to ensure greater flexibility in the evaluation, allowing a more dynamic and adaptable evaluation for each individual scenario. For a better evaluation, a reference table for calculating likelihood was developed. This table provides precise scores that can be used as a guide to assess the probability associated with each indicator. The use of this table simplifies the decision-making process and provides support in risk analysis.

	Attacker profile				
Likelihood indicators	System Knowledge	Physical distance from the System needed to concretize the threat	Financial support (inversely proportional to likelihood) or necessary manpower	Likelihood based on probability of Interest based on attacker's objective (motivations and aim)	Offensive Knowlege (Tools and resources needed to concretize the threat)
Low	Specific knowledge of private infromation (only available from within the company)	Physical access	Team of attacker above 3 ppl and budget above 50K	Industrial espionage (or nation-state)	Complex toolchain, ad-hoc tools or technique needed (e.g. new malware for zero-day) or specific resources (e.g. cloud based tech)
Medium	Basic knowledge of private information (only available from within the company)	Both physical and virtual proximity (e.g. same building and same subnet) is required	Hacking team <= 3 OR budget <= 50K	Insider (e.g. disgruntled employees or external contractors)	Mainstream hacking tools needed (e.g. sqlmap, nessus) and basic resources (e.g. alpha0 antenna, rubber ducky)
High	Publicly available information of the system	Internet	Lone attacker and budget below 10K	Multiple threat agents	No specialized hacking tool or technique needed (e.g. input or 1=1 as sqli) and no specific resources needed (e.g. a laptop may suffice)

Table 4.8: Likelihood table: attacker profile.

	System status		
Likelihood indicators	Today Exploitability	Historic Data on Exploitation of the Threat on the System	Mitigation
Low	Not Exploitable / Limited Time Window	Never in historic data / Once in historic data	Fixed / Partial mitigation
Medium	Unknown or not yet tested	Multiple occurrences in historic data	Mitigation planned
High	Exploitable	Currently applicable	No mitigation in place / No mitigation possible

Table 4.9: Likelihood table: system status.

Tables 4.8 and 4.9 differentiates the indicators by taking into consideration two fundamental aspects:

- *Attacker Profile*: This aspect considers five main factors from the attacker's point of view, and for each factor three different indicators are identified in relation to the likelihood value. For example, if information about the system becomes public, the attacker gains complete knowledge of the system, resulting in a likelihood value categorised as "High".

- *System Status*: This aspect takes into consideration three factors relating to the status of the system, and for each factor a rating indicator is associated. For example, if a threat is exploitable within the system, it is classified as "Exploitable", thus generating a risk value classified as "High".

No scores were given to each factor in the table. However, it provides a useful reference for the evaluation of likelihood. From the information provided, the threat "employee error" was assigned the value "2" categorised as "Medium" in relation to the indicators previously provided.

Impact

Impact is the second element considered in the risk assessment. STRIDE was used as a reference point for the assessment. Each letter of the

STRIDE acronym (see 2.3.1 for further details) is associated with a specific threat, and each of these is associated with a *security property* (Table 4.10).

STRIDE			
	Description	**Impacting to**	**Risk Score**
S	**Spoofing**: falsification of a legitimate user identity.	Authenticity	1
T	**Tampering**: unauthorized modification of data.	Integrity	2
R	**Repudiation**: an user denies their actions.	Non-repudiation	1
I	**Information disclosure**: unauthorized disclosure of sensitive information.	Confidentiality	1
D	**DoS**: service unavailable.	Availability	2
E	**Elevation of privilege**: unauthorized escalation of privileges.	Authorization	2

Table 4.10: Reference STRIDE table.

STRIDE was chosen as a reference because it allows threats to be categorised according to their security properties. Within this methodology, a score was given to each letter of the acronym in relation to the impact of the corresponding threat on the system. Table 4.10 presents the mapping of each STRIDE element to its respective threat category. In particular, for each element:

- A value of "1" was assigned in the case of no serious impact on the system.
- A value of "2" was assigned for elements that have a significant impact on the system and whose presence may compromise the correct functioning of the device,

After assigning scores to each category, the total sum of points was set at 9. To ensure a consistent mathematical correspondence in the risk calculation, the initial score, varying from 1 to 9, was mapped onto a new range between 1 and 3. This transformation was performed using the **linear normalisation** formula:

$$X_{\text{norm}} = \frac{X_{\max} - X_{\min}}{X - X_{\min}} \cdot (NewMax - NewMin) + NewMin \quad (4.1)$$

In this formula:

- X-norm = Represents the new normalised value in the new range.

- X-min = Initial value of the old range.
- X-max = Final value of the old range.
- NewMin = Initial value of the new range.
- NewMax = Final value of the new range.
- X = Value of the old range which is mapped into the new range.

The application of this formula allowed the impact values to be mapped into a new range, thus ensuring consistency between the likelihood and impact ranges. The scores resulting from this transformation are visualised in Table 4.11.

Mapping impact to 1-3 range	
Total points	**New range**
1	1
2	1.25
3	1.5
4	1.75
5	2
6	2.25
7	2.5
8	2.75
9	3

Table 4.11: Mapping impact in new range.

After the realisation of the new range, a checklist containing the threat categories was created, as depicted in Table 4.12.

Qualitative approach						
S	**T**	**R**	**I**	**D**	**E**	**Impact value**
Authenticity	Integrity	Non-Repudiation	Confidentiality	Availability	Authorisation	
☐	☐	☐	☒	☒	☐	**Low [1.5]**

Table 4.12: Impact checklist.

This checklist provides an opportunity to assess the impact of each threat considered. Within the Table 4.12 , an example of the "employee error" threat is provided, in which the properties "Confidentiality" and "Availability" were selected. The decision to choose these two factors was made in relation to the consequences described within the scenario. In particular:

- *Confidentiality*: This category was selected because in this case an employee could mistakenly access sensitive information.
- *Availability*: This category was selected because an employee could cause an error in the production phase of the device, creating potential malfunctions.

The elements of the checklist produce a value whose sum is mapped within the Table 4.11 by deriving the value in the new range. The value obtained represents the sum of the elements selected in the checklist to which is associated a descriptive string of the range in which the value belongs, as shown in Table 4.13.

Impact scale	**Impact value**
1 to <1.75	Low
1.75 to <2.5	Medium
2.5 to 3	High

Table 4.13: Impact table.

Considering the "employee error" example, the selection of the two security properties impacted by the threat gave a result of "1.5" categorised as "Low".

Evaluation

Once the respective Impact and Likelihood values have been calculated, it is possible to proceed with the risk assessment. The risk value is calculated by considering the product of the two values obtained from Likelihood and Impact, respectively:

$$\text{Risk} = \text{Likelihood} \cdot \text{Impact} \tag{4.2}$$

The formula produces as output a value that is mapped into a string, as can be seen in Table 4.14.

Likelihood and Impact levels	
1 to <3	Low
3 to <6	Medium
6 to 9	High

Table 4.14: Risk mapping.

This can be seen in the Table 4.15 showing the risk assessment for the "employee error" threat. It shows the product of the values obtained from

the likelihood and impact factors, resulting in a value of "3" categorised as "Medium".

Likelihood	Impact	Risk evaluation (L / M / H)
Medium [2]	**Low [1.5]**	**Medium [3]**

Table 4.15: Employee error assessment.

4.1.5 Step 5: Mitigation

The mitigation step identifies which solutions are implemented by the company to prevent the occurrence of a given threat. In this methodology, this step is divided into two main phases:

- The first stage of this step identifies which solutions are implemented at the time the threat is assessed.
- In the second phase of this step, the aim is to re-assess the risk of the threat just assessed in relation to the mitigation solutions adopted by the company.

After assessing the threat, the mitigation phase began with the realisation of a list of solutions used by the company to reduce the risk associated with a threat. Considering the example of the "employee error" threat, three specific solutions can be identified, which are detailed in Table 4.16.

Mitigation
• Employee training on security protocols. • Adopt testing and validation procedures. • Clearly define security guidelines.

Table 4.16: Mitigation plan.

After identifying the solutions adopted by the company to mitigate the threat, the objective now is to verify how the risk analysis changes. In particular, the threat "employee error" categorised as accidental was

taken as an example. In particular, it was seen that the risk analysis for this threat provided a risk value corresponding to “3” categorised as “Medium”. After implementing the provided mitigation, the risk value changed. Indeed, the value calculated for likelihood idetified previously as “Medium [2]” and after mitigation was calculated as “Low [1]”. From this first result, it can be seen that the likelihood of the threat occurring has decreased considering the same factors as previously defined. Instead, the calculation of the impact has not changed because the security categories involved in the occurrence of the threat are the same. Doing the product between likelihood and impact again, the result obtained gives a risk value of “Low [1.5]”. This result shows how, after applying the mitigation for this threat, the risk value decreased. This last phase allowed us to understand how the mitigation process is carried out in this methodology by identifying the solutions adopted by the company, and then it was possible to carry out a new assessment to understand how the risk of a threat may change in relation to the solutions adopted.

Chapter 5

Comparison with the OWASP risk rating methodology

The purpose of this chapter is to compare the methodology proposed in this thesis with the "OWASP Risk Rating Methodology" considering in both cases an HMI device as the target of analysis.

5.1 Comparative Evaluation

The two methodologies considered use different approaches:

- The methodology proposed in this thesis is based on a qualitative approach to gain an in-depth understanding of how threats can compromise the system.
- The OWASP methodology is based on a quantitative approach in which risk analysis is performed by considering a set of factors to which a score is associated.

The OWASP methodology makes it possible to customise the factors for risk assessment and this is advantageous because it is adaptable in several contexts. In particular, it assesses risk through the product of likelihood and impact factors. The calculation of these factors is done by considering a set of factors in which a score can be selected from possible choices. In this case, the factors were taken from [12]; in particular, the factors of the Table 5.1 and 5.2, represent the "threat agent factors" and "vulnerability factors" respectively that can be selected for the likelihood calculation.

Threat agent factors							
Skill level		**Motivate**		**Opportunity**		**Size**	
No Technical skills	1	Low or no reward	1	Full access or expensive resources required	1	Developers	2
Some technical skills	3	Possible reward	4	Special access or resources required	4	System administrators	2
Advanced computer user	5	High reward	9	Some access or resources required	7	Intranet users	4
Network and programming skills	6			No access or resources required	9	Partners	5
Security penetration skills	9					Authenticated users	6
						Anonymous Internet users	9

Table 5.1: Threat agent factors table

Vulnerability factors							
Ease of discovery		**Ease of exploit**		**Awareness**		**Intrusion detection**	
Practically impossible	1	Theoretical	1	Unknown	1	Active detection in application	1
Difficult	3	Difficult	3	Hidden	4	Logged and reviewed	3
Easy	7	Easy	5	Obvious	6	Logged without review	8
Automated tools available	9	Automated tools	9	Public knowledge	9	Not logged	9

Table 5.2: Vulnerability factors table

In particular:

- *Threat agent factors*: The choice of scoring depends on the information a company has on the attacker or threat, such as the number of attackers involved and their skills.
- *Vulnerability factors*: The scoring in this case depends on how vulnerable the asset in question is. In particular, some security aspects relating to the asset are analysed.

The likelihood in this case is calculated by considering eight distinct factors and for each of them there are choices with an associated score and description. For example, the "skill level" factor defines the level of knowledge an attacker has to exploit the threat. If the attacker has no particular technical skill, "No technical skill" is selected for this factor and the lowest score is associated with it. Instead, if the attacker has advanced knowledge, the highest score is chosen as "Security penetration skills". If no information is available on the attacker, a score can be assigned in relation to the knowledge required to exploit a threat.
Impact is instead calculated using the factors in Table 5.3 and 5.4.

Technical Impact Factors							
Loss of Confidentiality		**Loss of Integrity**		**Loss of Availability**		**Loss of Accountability**	
Minimal non-sensitive data disclosed	2	Minimal slightly corrupt data	1	Minimal secondary services interrupted	1	Fully traceable	1
Minimal critical data disclosed	6	Minimal seriously corrupt data	3	Minimal primary services interrupted	5	Possibly traceable	7
Extensive non-sensitive data disclosed	6	Extensive slightly corrupt data	5	Extensive secondary services interrupted	5	Completely anonymous	9
Extensive critical data disclosed	7	Extensive seriously corrupt data	7	Extensive primary services interrupted	7		
All data disclosed	9	All data totally corrupt	9	All services completely lost	9		

Table 5.3: Technical impact factors table.

Business Impact Factors							
Financial damage		**Repudiation damage**		**Non-compliance**		**Privacy violation**	
Less than the cost to fix the vulnerability	1	Minimal damage	1	Minor violation	2	One individual	3
Minor effect on annual profit	3	Loss of major accounts	4	Clear violation	5	Hundreds of people	5
Significant effect on annual profit	7	Loss of goodwill	5	High profile violation	7	Thousands of people	7
Bankruptcy	9	Brand damage	9			Millions of people	9

Table 5.4: Business impact factors table.

Impact factors are divided into:

- *Technical impact factors*: Scoring these factors requires knowledge of the consequences caused by a threat.
- *Business impact factors*: Scoring is done on the knowledge of financial and sensitive company information.

Again, eight different factors were considered with the possibility of selecting a score in relation to the threat and system information. For example, considering the factor "Loss of availability", a low score is associated if the damage caused by a threat is not significant, while a high score is associated if the threat causes damage that compromises the proper functioning of the system. This methodology is customisable according to the selected threats and, for this study, it is possible to select factors for evaluation based on the documentation provided and the type of threat to be analysed. Factors that are not scored are automatically assigned the value 0. This is done for two reasons:

- Motivate the user using this approach to obtain a lot of information about the system to make the risk calculation more accurate.

- It is inconvenient to consider only one factor and not consider the others. This could lead to assigning a high weight to a factor that is actually not significant in the final calculation and falsify the final risk calculation.

Information on risk calculation for this methodology was defined in Chapter 2 (see 4 for further details). From this premise, it is possible to say that:

- The OWASP methodology analyses each threat individually but considers the same factors showing the characteristics of the attacker and the system.
- The methodology proposed in this thesis analyses each threat individually but the factors are defined in relation to the characteristics of the threat analysed and its consequences.

Some of the threats used for the methodology proposed in this thesis will now be analysed and used for comparison with the OWASP methodology, identifying the strengths and weaknesses of each methodology. The first threat chosen for comparison is "employee error": it occurs when an employee within the company makes an error in an accidental manner that can cause anomalies in the system. Tables 5.5, 5.6 and 5.7 show how the risk assessment of this threat was carried out using the methodology proposed in this thesis.

Proposed methodology	
Likelihood factors	**Likelihood evaluation**
• The greater the number of employees involved in the development process, the greater the likelihood of making a mistake. • Poor cybersecurity skills/training/awareness on the part of employees can increase the likelihood of this threat. • The lack of an automated process for testing/verifying security requirements.	**Medium [2]**

Table 5.5: Employee error likelihood.

Proposed methodology						
S	**T**	**R**	**I**	**D**	**E**	**Impact value**
Authenticity	Integrity	Non-Repudiation	Confidentiality	Availability	Authorisation	
☐	☐	☐	☒	☒	☐	**Low [1.5]**

Table 5.6: Employee error impact.

Proposed methodology		
Likelihood	Impact	Risk evaluation (L / M / H)
Medium [2]	**Low [1.5]**	**Medium [3]**

Table 5.7: Employee error assessment.

The calculation of likelihood and impact for this threat was described in the previous chapter. Considering Table 5.5, a value of "2" was associated with the likelihood in relation to the three indicators described because the employee's error leads to consequences whose probability is not high. On the other hand, for the impact calculation (see Table 5.6), *availability* and *confidentiality* were selected in relation to the consequences described within the attack scenario. The value obtained in this case is "1.5", given by the sum of the values assigned to the two security properties. The risk value obtained in this case is calculated from the product of the values obtained from the two impact and likelihood factors and is defined as "Low".

The same threat was analysed using the OWASP methodology through the factors defined earlier in this chapter. Table 5.8 shows the values that were assigned for the likelihood calculation.

OWASP methodology			
Threat agent factors			
Skill level	**Motivate**	**Opportunity**	**Size**
No Technical skills [1]	Low or no reward[1]	Special access or resources required [4]	Authenticated users [6]
Vulnerability			
Ease of discovery	**Ease of exploit**	**Awareness**	**Intrusion detection**
Not selected [0]	Not selected [0]	Unknown[1]	Logged and reviewed [3]
Overall likelihood			
Low [2]			

Table 5.8: Likelihood value of the employee error threat according to the OWASP methodology.

In this case, the attacker is an authorised employee within the company. Following these factors, it becomes clear that these are not appropriate for an accidental threat, but for an adversarial threat carried out by an attacker with a malicious purpose. This is evident because a contradiction is created by considering the factor "Skill level" which corresponds to the attacker's level of knowledge. In particular, in this case, the value has been set to the minimum because an employee who makes a mistake does not have any valid skills, but this is absurd because this threat is less probable to occur when it should be more probable. The calculated likelihood value is "Low" and some of the factors were not selected because they are not suitable for this threat. An example of this, is the "Easy of exploit" factor that is unsuitable for the evaluation of this threat and could give a rating that negatively compromises the final score. This factor makes it possible to identify the facility with which an attacker can exploit a vulnerability in the system, but in this case the vulnerability is not directly linked to the device but depends on the error committed by the employee. Table 5.9 shows the values assigned for the impact calculation.

OWASP methodology			
Technical impact			
Loss of confidentiality	**Loss of integrity**	**Loss of availability**	**Loss of accountability**
Minimal critical data disclosed [6]	Minimal seriously corrupt data [3]	Minimal primary services interrupted [5]	Possibly traceable [7]
Business impact			
Financial damage	**Reputation damage**	**Non-compliance**	**Privacy violation**
Less than the cost to fix the vulnerability [1]	Loss of major accounts [4]	Clear violation [5]	One individual [3]
Overall impact			
Medium [4.25]			

Table 5.9: Impact value of the employee error threat according to the OWASP methodology.

OWASP methodology		
Likelihood	Impact	Risk evaluation (L / M / H)
Low [2]	**Medium [4.25]**	**Low**

Table 5.10: Employee error assessment using the OWASP methodology.

In this case, different factors have been considered and it can be seen that in this threat, high scores have been associated with *confidentiality*, *availability* and *accountability*, obtaining an overall value (Table 5.10) of "Medium". Table 5.11 shows the scores obtained from both methodologies in order to understand in which situations the scores are similar or different.

Proposed methodology			**OWASP methodology**		
Likelihood	Impact	Risk evaluation	Likelihood	Impact	Risk evaluation
Medium [2]	**Low [1.5]**	**Medium [3]**	**Low [2]**	**Medium [4.25]**	**Low**

Table 5.11: Comparison of employee error threat.

Using the proposed methodology, likelihood in the first case has a value of "Medium" , while it is "Low" using the OWASP methodology. The difference between the two values is caused by the factors considered for the threat assessment. In contrast, the scores and values differ significantly in the calculation of impact. In fact, in the first case the value obtained is "1.5" corresponding to "Low", while in the second case a score of "4.25" is obtained corresponding to "Medium". This distance between the scores is caused by the values that are assigned to the different security categories. In the proposed methodology, the categories affected by the threat are selected using a checklist, while in the second methodology, a different score can be selected for each category according to the severity of the threat. The possibility of assigning different weights to the factors allows for an accurate evaluation. Another example of a threat used for comparison is "social engineering". It is not accidental, but adversarial and it is usually carried out with the aim of causing damage to a company asset.

Table 5.12, 5.13 and 5.14 show the analysis of this threat by applying the methodology proposed in this thesis.

Proposed methodology	
Likelihood factors	**Likelihood evaluation**
• Company doesn't block suspicious email. • The company doesn't follow steps before making a system change. • The company does not have alert systems. • The company does not carry out access controls.	**High [3]**

Table 5.12: Social engineering likelihood.

Proposed methodology						
S	**T**	**R**	**I**	**D**	**E**	**Impact value**
Authenticity	Integrity	Non-Repudiation	Confidentiality	Availability	Authorisation	
☒	☒	☒	☒	☒	☒	**High [3]**

Table 5.13: Social engineering impact.

Proposed methodology		
Likelihood	Impact	Risk evaluation (L / M / H)
High [3]	**High [3]**	**High [9]**

Table 5.14: Risk assessment of social engineering threat according to the proposed methodology.

The worst case was considered for the threat analysis. The reason is that the threats were defined in a general manner with the aim of identifying the greatest number of consequences for each threat. In the proposed example, a social engineering attack potentially has a high probability of occurring if no security strategies are in place within the company to prevent this threat. Moreover, it can have an impact on all the security categories mentioned because there are different types of attacks related to this threat and the consequences can be multiple. For this reason, the risk value in this case is classified as "High" because in both cases, likelihood and impact were rated as "High". Using the OWASP methodology, Table 5.15 shows the likelihood assessment for the same threat.

OWASP methodology			
Threat agent factors			
Skill level	**Motivate**	**Opportunity**	**Size**
Network and programming skills [6]	Possible reward [4]	Some access or resources required [7]	Anonymous Internet users [9]
Vulnerability			
Ease of discovery	**Ease of exploit**	**Awareness**	**Intrusion detection**
Difficult [3]	Difficult [3]	Hidden [4]	Logged and reviewed [3]
Overall likelihood			
Medium [4.875]			

Table 5.15: Likelihood value of the social engineering threat according to the OWASP methodology.

The result obtained considering the OWASP methodology for the calculation of likelihood is classified as "Medium" with a value of "4.875". Table 5.16 shows the impact assessment.

OWASP methodology			
Technical impact			
Loss of confidentiality	**Loss of integrity**	**Loss of availability**	**Loss of accountability**
Extensive non-sensitive data disclosed [6]	Extensive slightly corrupt data [5]	Minimal primary services interrupted [5]	Possibly traceable [7]
Business impact			
Financial damage	**Reputation damage**	**Non-compliance**	**Privacy violation**
Significant effect on annual profit [7]	Brand damage [9]	High profile violation [7]	Thousands of people [7]
Overall impact			
High [6.625]			

Table 5.16: Impact value of the social engineering threat according to the OWASP methodology.

OWASP methodology		
Likelihood	Impact	Risk evaluation (L / M / H)
Medium [4.875]	**High [6.625]**	**High**

Table 5.17: Social engineering assessment using the OWASP methodology.

From the results obtained, in this case, the impact value is "6.625" and is classified as "High" providing an overall risk value (Table 5.17) of "High".

Table 5.18 shows the comparison of the two methodologies for the "social engineering" threat.

Proposed methodology			**OWASP methodology**		
Likelihood	Impact	Risk evaluation	Likelihood	Impact	Risk evaluation
High [3]	**High [3]**	**High [9]**	**Medium [4.875]**	**High [6.625]**	**High**

Table 5.18: Comparison of social engineering threat using the two methodologies.

5.1.1 Discussion of results

The result obtained using both methodologies is the same in both risk and impact calculations. Instead, there is a difference on the likelihood assessment since the metrics considered for both methodologies are different. The results obtained show that, with the proposed methodology:

- Using a descriptive approach for each factor to calculate likelihood can lead to a precise threat assessment.
- It may be advantageous to make an analysis using threats belonging to different categories.
- Using a checklist for impact calculation can lead to a quick and easy evaluation.

In contrast, the OWASP Risk Rating Methodology shows that:

- This methodology allows weights to be assigned to each evaluated factor, providing an accurate assessment.
- Assigning the same factors to calculate all threats may not always lead to an accurate assessment.
- This methodology is very accurate but becomes inefficient when considering a large number of threats because scoring each individual factor can be time-consuming.

From the points described, it is clear that the two methodologies use different approaches to risk assessment and may lead to a different evaluation. From the comparison, it can be seen that:

- The proposed methodology is particularly advantageous if a simple and precise analysis is to be carried out for each individual threat assessment. In particular, as has been described, the likelihood calculation allows a very precise assessment because it is carried out for each threat.
- The OWASP methodology, factors defined at the beginning are used, and the same ones are used for all threats, resulting in an approximate assessment.

Furthermore, it is evident that:

- It is not possible to adopt the OWASP methodology for different threat categories because this could create contradictions in the assessment and lead to an invalid result.

- The proposed methodology offers great flexibility because it evaluates any type of threat regardless of its category. This is because no predefined factors are used, but these are defined for each threat.

Finally, from this comparison, the most important point to focus on is the efficiency and speed with which to carry out the risk assessment:

- One of the advantages of the proposed methodology is its efficiency and simplicity in risk assessment. In particular, the ability to select only a range of values for the likelihood and the use of a checklist for impact assessment leads to a simple and fast methodology that allows for the evaluation of a large set of threats. This is particularly advantageous for companies that need to perform risk assessments on multiple products and must conduct periodic reviews on all products.

- The OWASP methodology is not particularly efficient when considering a large number of threats because, for each threat, it is necessary to select, as shown in the example in this chapter, a large number of factors. The selection of all these factors for so many threats is not advantageous, especially for companies that need to perform risk assessments on multiple products and must conduct periodic reviews.

The two methodologies chosen in this chapter make it possible to carry out a valid risk analysis. The choice of which methodology to adopt depends on the needs of each company and the resources it possesses; moreover, the results may differ depending on various aspects such as the type of application chosen to be analysed.

Chapter 6

Conclusions

This chapter presents the objectives and results obtained during the implementation of this methodology for the risk assessment of industrial control systems. The proposed methodology is developed with the aim of realising a template for risk assessment in accordance with the IEC 62443-4-1 standard. From the initial stages, the primary objective has been to develop a methodology aimed at conducting an in-depth analysis of the system and its structure. The device selected for this methodology is an HMI, and through the three different graphical representations, along with the definition of the "product security context", it was possible to identify the main characteristics of the device and its uses. An approach to threat assessment was proposed, starting with threat identification. Indeed, a threat list was realised with the aim of grouping the main threats that may occur within an HMI device. Each threat was categorised, and a precise description was provided for better understanding. The formulation of scenarios made it possible to identify how a threat could manifest itself within the system, identifying the possible components that could be altered. The peculiarity of this methodology manifests itself in the risk assessment and calculation of the "likelihood" and "impact" factors through a qualitative approach. In particular, the calculation of "likelihood" was carried out by creating a bulleted list of factors relating to the threat under analysis. This approach allowed a flexible evaluation, taking into different aspects of a specific threat. Moreover, it provides an assessment in relation to the documentation developed in the previous stages. Instead, the impact assessment was conducted through the use of a checklist in which security properties impacted by the threat can be selected. The last stage of the proposed methodology identified the solutions adopted by the company to mitigate the threat and, from these, it was possible to carry out a new assessment to understand how the risk could change. The comparison with the OWASP methodology allowed the identification of the strengths and weaknesses of this methodology,

highlighting that the assignment of individual factors for each threat is effective in the assessment of likelihood. However, a potential limitation was identified in the impact assessment where it is not possible to choose from a set of values for the security factors, as is the case with the OWASP methodology. On the basis of these considerations, it is possible to improve the present methodology by introducing a more precise assessment of impact by assigning different weights to each factor considered. This would allow a more accurate estimation and give a more significant value to each of the factors taken into consideration.

Integration with the 62443 - 4 - 2 The standard IEC 62443-4-2 entitled "Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components" defines a set of guidelines on the adoption of technical requirements for systems used in an industrial environment. One way of extending this methodology would be to derive threats from the requirements provided by the standard. In particular, from the denial of each requirement, it is possible to derive threats that can be used to extend the threat list presented for this methodology in order to add technical threats to cover specific aspects of the system components analysed. Extending this list with technical threats would provide a greater level of detail to the risk assessment and increase its efficiency.

Bibliography

[1] R. Paes, D. C. Mazur, B. K. Venne, and J. Ostrzenski, "A guide to securing industrial control networks: Integrating it and ot systems," *IEEE Industry Applications Magazine*, vol. 26, no. 2, pp. 47–53, 2020.

[2] M. T. Okano, "Iot and industry 4.0: the industrial new revolution," in *International Conference on Management and Information Systems*, vol. 25, 2017, p. 26.

[3] I. Jamai, L. Ben Azzouz, and L. A. Saïdane, "Security issues in industry 4.0," in *2020 International Wireless Communications and Mobile Computing (IWCMC)*, 2020, pp. 481–488.

[4] Kaspersky. (2023, 09) Attacks on industrial sector hit record in second quarter of 2023. [Online]. Available: https://www.kaspersky.com/about/press-releases/2023_attacks-on-industrial-sector-hit-record-in-second-quarter-of-2023

[5] I. E. Commission, "Security for industrial automation and control systems, part 4-1: Secure product development lifecycle requirements," *International Standard*, 2018.

[6] J. Ingalsbe, D. Shoemaker, and N. Mead, "Threat modeling the cloud computing, mobile device toting, consumerized enterprise - an overview of considerations." 01 2011.

[7] N. Shevchenko, T. A. Chick, P. O'Riordan, T. P. Scanlon, and C. Woody, "Threat modeling: a summary of available methods," Carnegie Mellon University Software Engineering Institute Pittsburgh United . . . , Tech. Rep., 2018.

[8] Microsoft. (2023, 02) Minacce di microsoft threat modeling tool. [Online]. Available: https://learn.microsoft.com/it-it/azure/security/develop/threat-modeling-tool-threats

[9] T. UcedaVelez and M. M. Morana, *Intro to Pasta*, 2015, pp. 317–342.

[10] K. Wuyts and W. Joosen, "Linddun privacy threat modeling: a tutorial," *CW Reports*, 2015.

[11] I. N. Distefano. Risk management e metodi di risk assessment. [Online]. Available: https://www.dicar.unict.it/sites/default/files/files/Lezione3.pdf

[12] OWASP. (2017) Owasp risk rating methodology. [Online]. Available: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

[13] V. Maheshwari and M. Prasanna, "Integrating risk assessment and threat modeling within sdlc process," in *2016 international conference on inventive computation technologies (ICICT)*, vol. 1. IEEE, 2016, pp. 1–5.

[14] K. Rhee, D. Won, S.-W. Jang, S. Chae, and S. Park, "Threat modeling of a mobile device management system for secure smart work," *Electronic Commerce Research*, vol. 13, pp. 243–256, 2013.

[15] C. K. Dimitriadis, "Security for mobile operators in practice." *Int. J. Netw. Secur.*, vol. 15, no. 5, pp. 397–404, 2013.

[16] J. Meszaros and A. Buchalcevova, "Introducing ossf: A framework for online service cybersecurity risk management," *computers & security*, vol. 65, pp. 300–313, 2017.

[17] C. Möckel and A. E. Abdallah, "Threat modeling approaches and tools for securing architectural designs of an e-banking application," in *2010 Sixth International Conference on Information Assurance and Security*. IEEE, 2010, pp. 149–154.

[18] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. Shen, "Energy-theft detection issues for advanced metering infrastructure in smart grid," *Tsinghua Science and Technology*, vol. 19, no. 2, pp. 105–120, 2014.

[19] G. Brændeland, A. Refsdal, and K. Stølen, "Modular analysis and modelling of risk scenarios with dependencies," *Journal of Systems and Software*, vol. 83, no. 10, pp. 1995–2013, 2010.

[20] S. Hofmann and R. Kasseckert, "Towards a security architecture for ip-based optical transmission systems," *Bell Labs Technical Journal*, vol. 16, no. 1, pp. 133–153, 2011.

[21] M. Abomhara, M. Gerdes, and G. M. Køien, "A stride-based threat model for telehealth systems," *Norsk informasjonssikkerhetskonferanse (NISK)*, vol. 8, no. 1, pp. 82–96, 2015.

[22] S. P. Kadhirvelan and A. Söderberg-Rivkin, "Threat modelling and risk assessment within vehicular systems," 2014.

[23] W. Xiong and R. Lagerström, "Threat modeling–a systematic literature review," *Computers & security*, vol. 84, pp. 53–69, 2019.

[24] NIST. (2012) Guida per la conduzione delle valutazioni dei rischi. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/30/r1/final

[25] A. A. Süzen, "A risk-assessment of cyber attacks and defense strategies in industry 4.0 ecosystem," *International Journal of Computer Network and Information Security*, vol. 12, no. 1, p. 1, 2020.

[26] S. Patel and J. Zaveri, "A risk-assessment model for cyber attacks on information systems." *J. Comput.*, vol. 5, no. 3, pp. 352–359, 2010.

[27] M. Fujimoto, W. Matsuda, T. Mitsunaga, and Y. Hashimoto, "Efficient industrial control systems risk assessment using the attack path to the critical device," in *2021 3rd International Conference on Management Science and Industrial Engineering*, 2021, pp. 104–110.

[28] L. Zhang, A. Taal, R. Cushing, C. de Laat, and P. Grosso, "A risk-level assessment system based on the stride/dread model for digital data marketplaces," *International Journal of Information Security*, pp. 1–17, 2021.

[29] B. Potteiger, G. Martins, and X. Koutsoukos, "Software and attack centric integrated threat modeling for quantitative risk assessment," in *Proceedings of the Symposium and Bootcamp on the Science of Security*, 2016, pp. 99–108.

Appendix

Table 6.1: Table of external dependencies

External dependence		
Components	**ID**	**Description**
Physical devices	ED - 1	The device can be connected to a **PLC** for the purpose of exchanging machinery information.
	ED - 2	The device can be connected to a **personal computer** to exchange sensitive data or update software within the system.
Cloud	ED - 3	The device has the ability to exchange sensitive information through an **external database** with other devices
Software	ED - 4	**Soft1** is a project management application for monitoring industrial processes.
	ED - 5	**Soft PLC** is the development environment installed in the device that allows centralised programming of the control system
Security requirements	ED - 6	The device offers the possibility to configure a **firewall** to protect himself against malicious attack
	ED - 7	The device supports the **TLS 1.2 and TLS 1.3** cryptographic algorithms
	ED - 8	The operator panel has a secure area encrypted with **AES-256** protocol where passwords are stored
Architecture	ED - 9	The BSP contains a Linux distribution based on the Yocto project; the Yocto environment provides a tool called CVE-check that uses official CVE databases to check whether selected modules used by the BSP are affected by vulnerabilities
Web	ED - 10	The web browser is a stand-alone application based on the open source Chronium project

Table 6.2: Table of trust levels

Trust level		
ID	**Name**	**Description**
TL - 1	Employee	An ordinary employee within the company
TL - 1.1	Employee with valid login credentials	An employee who want to use the HMI and is logged in using valid credentials
TL - 1.2	Employee with not valid login credentials	An employee who want to use the HMI and is no logged because he is using invalid credentials
TL - 1.1.1	Employee with high privileges (Admin)	An employee with valid credentials that has the ability to change system settings. He can create guest user inside the system and send commands to change machinary settings.
TL - 1.1.2	Employee with low privileges	An employee with valid credentials that hasn't the ability to change system settings but has the possibility to monitor operations
TL 1.3	Employee with valid external software / hardware	An employee who want to insert a valid software / hardware on the HMI through the I/O ports
TL - 1.4	Employee with not valid external software / hardware	An authorized employee who want to insert an invalid software / hardware on the HMI through the I/O ports but the system rejects it.
TL - 2	System technician	The system technician is a special user that can use the debug ports to debug the system and carry out system test.
TL - 3	Guest user	The guest user is an external user of the company or an unauthorized user that temporarly use the system after receiving legitimate permits.
TL - 3.1	Guest user with high privileges	Guest user that is temporarily created by an authorized user that has the ability to change system settings and send commands to system machinary
TL - 3.2	Guest user with low privileges	Guest user that is temporarily created by an authorized user that has the ability to monitor the system.

Table 6.3: Table of entry points

Entry point				
Category	**ID**	**Name**	**Description**	**Trust levels**
I/O Interfaces	EP - 1	Ethernet port	The ethernet port is used by the employee to communicate with other devices and to install the Soft1 application into the HMI	(TL – 1) Employee (TL – 2) System technician (TL – 3) Guest user
	EP - 2	USB port	The USB port is used by the employee to install or update software application into the device	(TL – 1) Employee (TL – 2) System technician (TL – 3) Guest user
	EP - 3	Debug port	Debug ports are special I/O ports within the device that allow the authorised user, during maintenance, to access sensitive data to perform diagnostic operations.	(TL – 2) System technician
Software	EP - 4	Soft1	Soft1 is an application developed by the company for the purpose of monitoring and sending commands to other connected devices.	(TL - 1.1) Employee with valid login credentials (TL - 3.1) Guest user with high privileges
	EP - 5	Web browser	The web browser enables the employee to browse the Internet.	(TL - 1.1.1) Employee with high privileges (Admin) (TL - 3.1) Guest user with high privileges
System settings	EP - 6	Wi-Fi connection	The Wi-Fi connection allows you to access the web browser and send industrial information to other devices.	(TL - 1.1.1) Employee with high privileges (Admin) (TL - 3.1) Guest user with high privileges
	EP - 7	Login interface	When an employee uses turns on the HMI, the first page is the login interface that allows him to access to the device.	(TL - 1.1) Employee with valid login credentials (TL - 1.2) Employee with not valid login credentials (TL – 2) System technician (TL – 3) Guest user
	EP - 8	Interface for managing settings	The settings management interface allows you to enable or disable some features	(TL - 1.1.1) Employee with high privileges (Admin) (TL - 3.1) Guest user with high privileges

Asset				
Category	**ID**	**Name**	**Description**	**Trust levels**
Employee	A - 1	Employee login credentials details	The login credentials that an employee will use to log into the HMI	(TL - 1.1.1) Employee with high privileges (Admin)
System	A - 2	Execution of external code	It is possible to execute external code to update or enhance existing software; only valid software must be executed on the HMI.	(TL - 1.1.1) Employee with high privileges (Admin)
	A - 3	Ability to connect the HMI to other devices	Connecting the HMI device to other devices enables fast data exchange for better monitoring	(TL - 1.1.1) Employee with high privileges (Admin)
	A - 4	Ability to send commands to connected devices	The HMI device via its interface provides the ability to send commands to manage machineries and their production	(TL - 1.1.1) Employee with high privileges (Admin)
	A - 5	Access session to the web service	The HMI supports Chromium and allows access to web services offered	(TL - 1.1.1) Employee with high privileges (Admin)
	A - 6	Details about machinery information (Monitoring)	The HMI device displays the data of the machinery to which they are connected for continuous monitoring	(TL - 1.1.1) Employee with high privileges (Admin) (TL - 1.1.2) Employee with low privileges (TL - 1.4) Guest user with high privileges (TL - 1.5) Guest user with low privileges
	A - 7	Ability to access or modify Audit files	Using the HMI device, it is possible to access or modify audit files containing information on the operations performed by each user	(TL - 1.1.1) Employee with high privileges (Admin)
	A - 8	Details of supported certificates	Using the HMI device, information on supported certificates can be accessed and there is a function to update devices	(TL - 1.1.1) Employee with high privileges (Admin)
Continue on the next page				

Table 6.4: Asset table

Asset				
Category	**ID**	**Name**	**Description**	**Trust levels**
System	A - 9	Connectivity of the device	The device has the functionality of being able to connect to the network to facilitate the information exchange	(TL - 1.1.1) Employee with high privileges (Admin)
	A - 10	Ability to create users	Using the device, it is possible to create users who can be given limited privileges	(TL - 1.1.1) Employee with high privileges (Admin)
	A - 11	Ability to edit username and password	Using the device, it is possible to modify the employee username and password, if he is logged in.	(TL - 1.1.1) Employee with high privileges (Admin)
	A - 12	Ability to do a factory reset	Using the device, it is possible to reset the system if the system has been compromised.	(TL - 1.1.1) Employee with high privileges (Admin)
	A - 13	Ability to modify network / VPN configuration	Using the device, it is possible to modify the network / VPN configuration when necessary	(TL - 1.1.1) Employee with high privileges (Admin)
	A - 14	Ability to modify the firewall configuration	Using the device, it is possible to enable the firewall configuration to make the system more secure.	(TL - 1.1.1) Employee with high privileges (Admin)
Company	A - 15	Infrastructure details of the company	The company provides information about its infrastructure on its site.	(TL- 1) Employee
	A - 16	Information about the produced devices.	The company provides information on its site about the devices they produce.	(TL- 1) Employee
	A - 17	Information about employees	The company has information related to its employees in its databases	(TL - 1.1.1) Employee with high privileges (Admin)

Threat list			
ID	**Threat**	**Category**	**Description**
1	Employee error (accidental or negligence)	Accidental	Accidental errors made by an authorised user (internal or external) when using or maintaining information systems. *Assessment guidance*: At **lower levels** of threat strength (i.e. individuals with limited or no access privileges) errors will generally result in greatly reduced or minimal impact to information systems. At **higher levels** of threat strength (i.e. individuals that have been assigned privileged access such as administrators), errors have the ability to cause greater impact to information systems.
2	Software bugs (integration or use of externally acquired software)	Accidental	Incorrect execution or failure of software acquired from an external party (e.g. enterprise applications and commercial-off-the-shelf (COTS) software (such as ERP, CRM), office productivity software, communications software and security software). Assessment guidance: Software malfunctions are typically caused as a result of an application flaw, a software bug or equivalent.
3	Mishandling of critical and/or sensitive information by authorised users	Accidental	An authorised user unintentionally discloses sensitive/critical information. Assessment guidance: At lower levels of threat strength (i.e. individuals with limited or no access privileges), the threat is likely to have access to less sensitive/critical information, resulting in reduced impact from disclosure. At higher levels of threat strength (i.e. individuals that have been assigned privileged access such as administrators), the threat will have access to more sensitive/critical information, resulting in greater impact from disclosure.
4	Software bugs (internally produced software)	Accidental	The threat exploits coding bugs or design flaws (e.g. buffer overflows, improper validation of input) in an organisation's information systems in order to gain unauthorised access. *Assessment guidance*: Vulnerabilities that threats will attempt to exploit can exist in: • Applications (e.g. end-user applications) • Services (e.g. web servers, database management systems) • Operating systems (e.g. Microsoft Windows, Linux, Apple OS X, IBM z/OS) • Virtual systems (e.g. virtual servers and virtual desktops) • Networking equipment (e.g. routers, wireless access points and firewalls) • Mobile devices (e.g. tablets and smartphones). At **lower levels** of threat strength the threat is likely to target mainstream software and exploit publically-available, commonly-known vulnerabilities (i.e. those that have been known for a long period of time and are likely to have corresponding patches available). At **higher levels** of threat strength the threat is more likely to exploit recent vulnerabilities (that may only recently have been patched) or unpublicised vulnerabilities (often referred to as 'zero-day' vulnerabilities), for which there are unlikely to be patches available. Additionally, these threats may target less common information systems (i.e. custom SCADA controllers) in use by specific organisations.
Continue on the next page			

Table 6.5: Threat list table

Threat list			
ID	**Threat**	**Category**	**Description**
5	Resource depletion (e.g. lack of physical maintenance)	Accidental	Excessive system activity or demand for services causing performance degradation or failure (often as a result of inadequate capacity planning).
6	Maintenance error	Accidental	An authorised user neglects to perform, or inadequately performs, system maintenance, resulting in performance or security issues with information systems.
7	Accidental physical damage	Accidental	Accidental material damage to information systems, network equipment or the physical environment in which they are located, which affects their normal function.
8	Structural event (e.g. short circuit)	Accidental	Accidental material damage to information systems, network equipment or the physical environment in which they are located, which affects their normal function. Fire or Flooding may cause structural events.
9	Undesirable effects of business change	Accidental	Unforeseen or unintended adverse impacts upon information and/or information systems from significant changes within the organisation, including: • organisational/environmental changes. • updates to business processes or business information. • newly implemented or recently changed software or network hardware.
10	Exploit misconfiguration such as misconfigured information systems	Adversarial	The threat exploits misconfigured information systems (i.e. those not configured in accordance with security standards, or organisational build requirements) in order to gain unauthorised access. Assessment guidance: This threat event can affect all types of organisational information systems, including: • Applications (e.g. end-user applications, database servers) • Services (e.g. web servers and database management systems) • Operating systems (e.g. Microsoft Windows, Linux, Apple OS X and IBM z/OS) • Virtual systems (e.g. virtual servers and virtual desktops) • Networking equipment (e.g. routers, wireless access points and firewalls) • Mobile devices (e.g. laptops, tablets and smartphones).
11	Introducing unauthorised code into applications or software	Adversarial	The threat inserts code that masquerades as an authorised programme or conceals its existence while carrying out one or more unauthorised actions (e.g. transmitting business information to unauthorised individuals).
12	Exploit insecure disposal (physical or virtual) of an organisation's information assets.	Adversarial	The threat obtains organisational information assets due to insecure disposal. Assessment guidance: This threat event could include exploiting: • Insecure or incomplete data deletion in the target environment, or an environment supporting the target environment (e.g. development or testing environments). • Insecure disposal of information assets related to the environment, such as mobile devices, portable storage devices and office equipment.
Continue on the next page			

Threat list			
ID	**Threat**	**Category**	**Description**
13	Introduce malware to information systems	Adversarial	The threat introduces malware to an organisation's information systems. Assessment guidance: At lower levels of threat strength the threat is likely to use relatively unsophisticated techniques to develop malware (e.g. using publicly available malware development kits or existing malware, along with common vulnerabilities)and deliver malware (e.g. through the use of email and social networks). At higher levels of threat strength the threat is more likely to use a range of sophisticated techniques to: • Develop malware (e.g. producing custom-written malware using unpublicised, or 'zero-day' vulnerabilities). • Deliver malware (e.g. targeting specific key individuals via their personal mobile devices, enticing them to visit infected websites or infecting portable storage devices that they may use). • Conceal malware (e.g. using rootkits or anti-forensics techniques).
14	Social Engineering (potentially in connection with phishing or other attacks)	Adversarial	The threat manipulates individuals within an organisation performing actions that could harm the organisation (e.g. disclosing sensitive information or granting unauthorised physical access). Assessment guidance: A threat can use a variety of social engineering techniques, including: • Impersonating a valid user, especially one of privilege. • Persuading an employee or valid user. • Bribery. • Extortion or blackmail.
15	Conduct a denial of service (DoS) attack	Adversarial	The threat deliberately impairs the availability or performance of an organisation's information system(s). Assessment guidance: At lower levels of threat strength, the threat is likely to use relatively unsophisticated techniques, involving the use of publically-available tools, a single source/host and limited network bandwidth. At higher levels of threat strength, the threat could employ more sophisticated techniques, involving: • The development and/or use of use of custom tools. • A large number of information systems in different locations. • A large amount of network bandwidth. • Interfering with wireless communications (e.g. Wi-Fi or GSM/CDMA) so as to impede or prevent communications from reaching intended recipients.
16	HTTP(S) session hijacking (customer<->website)	Adversarial	The threat obtains unauthorised control of (hijacks) a pre-existing, legitimate network session between information systems, or between information systems and end users.
17	Exploit design or configuration issues in an organisation's remote access service (e.g. VPNs)	Adversarial	The threat takes advantage of design or configuration issues in how remote access is handled for an organisation. Assessment guidance: This threat event can include exploiting: • 'Split tunnelling' to gain access to organisational networks. • Vulnerabilities in the way authentication is handled. • Weak encryption.
Continue on the next page			

Threat list			
ID	**Threat**	**Category**	**Description**
18	Exploit poorly-designed network/cloud architecture	Adversarial	The threat takes advantage of poorly-designed network architecture to identify potential target systems for further threat events. Assessment guidance: This threat event can include exploiting: • Unnecessary or unprotected Internet connections. • Weak filtering on Internet or internal network connections. • A lack of segregation of critical systems or business functions (e.g. no DMZ in place).
19	Unauthorised physical access to information systems potentially leading to physical damage to, thefth of, or tampering with information systems	Adversarial	The threat obtains physical access to an organisation's information systems (e.g. by misusing access or bypassing physical security checks) and uses this access to gain unauthorised access to organisational information systems and information assets.
20	Unauthorised network scanning and/or probing	Adversarial	The threat performs unauthorised scanning or probing of an organisation's information systems to gather information that could be used to initiate subsequent threat events.
21	Conduct physical attacks on organisational facilities or their supporting infrastructure	Adversarial	The threat conducts a physical attack on an organisation's facilities or supporting infrastructure (e.g. telecommunications, power, water or gas).
22	Gathering of publicly-available information about an organisation	Adversarial	The threat obtains and analyses publically-available information about an organisation (e.g. information systems, business processes, personnel or external relationships) that could be used to initiate subsequent threat events.
23	Gathering information about the physical details of the organisations premises	Adversarial	The threat obtains and analyses information about the physical details of an organisation (e.g. office and building diagrams, infrastructure details of a data centre) that could be used to initiate subsequent threat events.
24	Loss of information systems	Adversarial	Staff or external individuals (e.g. consultants, contractors or employees of external parties) lose or misplace information systems or equipment containing the organisation's information assets such as laptops, tablets, smartphones, portable storage devices and physical authentication devices, such as tokens and smartcards. Assessment guidance: Information systems or equipment that can be lost or misplaced typically includes laptops, tablets, smartphones, portable storage devices and physical authentication devices, such as tokens and smartcards. At lower levels of threat strength (i.e. individuals with limited or no access privileges), it is assumed that such individuals would have access to limited sensitive/critical information on their devices, and as a result the loss of such a device would be of lesser impact to the organisation. At higher levels of threat strength (i.e. individuals that have been assigned privileged access such as executives or administrators), it is assumed that such individuals would have greater access to sensitive/critical information on their devices, and as a result the loss of such a device would be of greater impact to the organisation.
Continue on the next page			

Threat list			
ID	**Threat**	**Category**	**Description**
25	Exploit vulnerable authorisation mechanisms	Adversarial	The threat exploits vulnerabilities in the authorisation mechanisms of an organisation's information systems in order to gain access to sensitive functions and information assets. Assessment guidance: This threat event can manifest in a number of ways, including: • Bypassing authorisation checks • Privilege escalation attacks • Forced browsing/navigation.
26	Compromise supplier or business partner of target organisation	Adversarial	The threat compromises information systems at a key supplier or business partner of an organisation in order to gain access to the organisation's information systems and information assets. Assessment guidance: At lower levels of threat strength the threat is likely to use relatively unsophisticated techniques, involving other, lower-level threat events to compromise a vendor or business partner's information systems and gain access to the targeted organisation's information assets stored there. At higher levels of threat strength, the threat could employ more sophisticated techniques, involving: • Using other, higher-level threat events to compromise a vendor or business partner's information systems and gaining access to the targeted organisation's information assets stored there. • 'Pivoting' off a foothold in a vendor or business partner's information systems to gain access to the targeted organisation's environment. • Compromising the design, manufacture and/or distribution of critical information system components at selected suppliers. This can be used to replace critical information system components the targeted organisation requires, with modified or corrupted components.
27	Unauthorised monitoring and/or modification of communications, i.e. passive (information gathering) or active attackers models	Adversarial	The threat gains unauthorised access to information assets in transit (i.e. 'sniffing')and potentially alters information while it is being transmitted. Assessment guidance: Depending on the environment, this threat event can involve one or more of the following: At lower levels of threat strength, the threat is likely to use relatively unsophisticated techniques, limited to interception of traffic only and involve: • DNS hijacking, or man-in-the-middle attacks • Exploiting unencrypted or weakly-encrypted communications (at different layers of the network stack, such as either wireless at media layer, or at transport/session/application layers). At higher levels of threat strength, the threat could employ more sophisticated techniques, involving interception and real-time modification of traffic using freely-available or custom tools, or other more advanced techniques (e.g. crypt analysis of strongly-encrypted sessions).
Continue on the next page			

Threat list			
ID	**Threat**	**Category**	**Description**
28	Phishing	Adversarial	The threat counterfeits communications from a legitimate/trustworthy source to mislead recipients into revealing sensitive information such as usernames, passwords or personally identifiable information (PII). Assessment guidance: At lower levels of threat strength the threat is likely to use relatively unsophisticated techniques, involving: • The use of generic, publically-available phishing tools, • Basic delivery mechanisms (e.g. spam emails). • Targeting a large number of individuals or organisations indiscriminately. At higher levels of threat strength the threat could employ more sophisticated techniques, involving: • The use of customised phishing tools. • The use of more advanced delivery mechanisms (e.g. counterfeit websites with forged TLS certificates). • 'Spear phishing', or targeting specific individuals (e.g. executives or individuals with privileged access).
29	Unauthorised access	Adversarial	The threat obtains unauthorised access to authentication credentials and uses these to gain access to an organisation's information systems. Assessment guidance: Authentication information can be obtained in numerous ways, including: • A leak of authentication information. • Insecure storage of authentication information. • Conducting brute force login attempts/password guessing attacks. Which the threat may combine with exploits, including: • Exploiting unencrypted or poorly-encrypted information. • Determining 'weak' passwords by valid system users.
30	Environmental event (Fire, Flooding, etc)	Environmental	Pathogen (e.g. disease outbreak) Storm (hail, thunder, blizzard), Hurricane, Tornado, Earthquake, Volcanic eruption, Flooding (wild), Tsunami, Fire (wild), Power failure or fluctuation, Damage to or loss of external communications, Failure of environmental control systems, Hardware malfunction or failure.

Acknowledgements

Desidero ringraziare la mia famiglia, che è stata sempre presente nel corso di questi anni. Ringrazio mia madre per il sostegno e i consigli forniti e mio padre che mi ha indirizzato verso questo speciale percorso universitario ricco di grandi opportunità. Inoltre, un ringraziamento speciale va a mia zia Dorotea che, come una seconda madre, ha preso parte al raggiungimento degli obiettivi accademici.

Ringrazio la prof.ssa Federica Maria Francesca Paci, mia relatrice, la cui guida esperta ha reso possibile la realizzazione di questa tesi. Desidero ringraziare il mio tutor aziendale e correlatore, Marco Rocchetto, che con pazienza e disponibilità mi ha guidato nella stesura di questa tesi. Grazie alla sua formazione e ai suoi consigli, ho avuto modo di appassionarmi a questo vasto ambito di ricerca.

Un ringraziamento speciale va anche a Giuseppe e Gaspare, miei cari amici, che mi sono stati vicini nel corso di questi anni lontano da casa, e sicuramente ai miei amici e colleghi universitari, per questi anni passati nella collaborazione e nel divertimento. In particolare, ringrazio Massimo, che è stato al mio fianco nei momenti più difficili, come anche Alessandro, Gabriele e Giulio, con i quali ho condiviso un rapporto di vera amicizia e fratellanza.