International Journal of Information Security manuscript No.
(will be inserted by the editor)

A Cybersecurity Risk Assessment Methodology for Industrial Automation Control Systems

Francesco Brancati[a,1], **Diamantea Mongelli**[b,1], **Francesco Mariotti**[c,2,3], **Paolo Lollini**[d,2,3]

[1]ResilTech s.r.l., Piazza Nilde Iotti 25, Pontedera (Pisa), Italy
[2]University of Florence, Dipartimento di Matematica e Informatica 'U. Dini', Viale Morgagni 65, Firenze, Italy
[3]Consorzio Interuniversitario Nazionale per l'Informatica (CINI), Via Ariosto 25, Roma, Italy

Received: date / Accepted: date

Abstract Industrial Automation Control Systems (IACS) are employed in current critical infrastructures and industrial plants spanning very different domains, and the transformation process towards Industry 4.0 is further increasing the dependencies on such systems. Since IACS can be exposed to malicious threats that could lead to catastrophic consequences, it is extremely important to assess the cybersecurity risk of these systems, to identify the possible threats, their impact, likelihood, and possible countermeasures. The ISA/IEC 62443 series of standards is suited for the design and security risk analysis of IACS, and has been submitted to the International Standards on Auditing and International Electrotechnical Commission for global adoption as international standards.

In this paper, we focus on the Zone and Conduit Requirement 5 (ZCR 5) of the 62443-3-2 part of the standard, which provides the steps for detailed cybersecurity risk assessment of IACS. These steps are fundamental to identify threats related to the system, determine the risk associated with them, and derive appropriate countermeasures.

We provide a methodology for conducting a detailed risk assessment of IACS that is compliant with all the steps of the ZCR 5 and integrates the following features: i) capability to manage the complexity of the assessment process, ii) capability to select tailored countermeasures for critical assets through the identification of attack paths, iii) explicit involvement of the asset owner in the key steps of the assessment process, and iv) tool-supported.

We illustrate the methodology by applying it to a case study of a power plant using gas turbines.

Keywords security · IACS · IEC 62443 · power plant · risk · STRIDE

1 Introduction

Cybersecurity is becoming increasingly important in every field: from the software applications that we use in everyday life to complex industrial systems. These last kinds of systems, in the past, used to work in an isolated way, relying on components, e.g., PLCs, that were not communicating with the external world. Due to an increasing interest in automation, nowadays such kinds of systems, known as Industrial Automation Control Systems (IACS) [17], are highly connected, can be remotely accessed for control actions and monitoring, and as a consequence they can potentially be exposed to external threats.

Cybersecurity risk assessment is meant to identify the possible threats that can menace the system under consideration (SUC), their impact, and their likelihood. Several security standards have been proposed to support organizations in the management of cybersecurity aspects [5]. The ISA/IEC 62443 [17] is a widely adopted series of guidelines suited for the design and cybersecurity risk analysis of embedded systems and IACS. They are submitted to the International Standards on Auditing (ISA) and International Electrotechnical Commission (IEC) for global adoption as international standards and are endorsed by the United Nations.

The guidelines provided in Zone and Conduit Requirement 5 (ZCR 5) of the 62443-3-2 part of the standard indicate which are the fundamental steps of a detailed cybersecurity risk assessment process. Among them: the identification of the threats that can menace the system, the evaluation of their impact and likelihood, the determination of the risk, and the derivation of countermeasures. These steps can

[a]francesco.brancati@resiltech.com
[b]diamantea.mongelli@resiltech.com
[c]francesco.mariotti@unifi.it, Corresponding Author
[d]paolo.lollini@unifi.it, Corresponding Author

help security experts in conducting a standardized risk assessment process over IACS, even if not specifying how to accomplish them.

From an industry point of view, there are several corporate needs that a risk assessment methodology for IACS should take into account. Certifications of compliance are often required by regulations to operate in this domain. Hence, the methodology should be *compliant with all the steps of the ZCR 5*, which defines the detailed risk assessment process. The majority of the works in the literature, instead, focus on some specific part of ZCR 5. Second, the methodology should *manage the complexity of the risk assessment process*. Cost and time are fundamental aspects for companies, thus it is important to have a methodology as efficient as possible. Still concerning time and cost, there should be *support for guiding the selection of the possible security countermeasures* to be implemented in the system, considering the actual threats that could menace the system and showing their benefit in achieving the desired target security level. Another important aspect is to *actively involve the asset owner or the system integrator* during some key steps of the methodology where their presence is essential, e.g. for estimating the business impact of the identified threats. Finally, the methodology should be *supported by tools* to facilitate its application and to speed up the assessment process.

In this paper, we present a methodology that can be used to implement the risk assessment process of industrial control systems in compliance with the ZCR 5 of ISA/IEC 62443-3-2. The methodology has been built, applied, and refined in several interactions with different companies and IACS owners in the smart grid domain. Starting from an architectural description of the system, the methodology allows to identify the threats which can menace the system's assets, to derive the risk associated with them, and to select and apply the appropriate countermeasures until the obtained risk is under a tolerable threshold.

The key features of the proposed methodology are the following:

1. Coverage of all the ZCR 5 steps. The methodology is compliant with 62443-3-2 part of the standard, implementing step by step the ZCR 5 detailed cybersecurity risk assessment. In this paper, we focus on the analysis of the zones of the SUC, while the analysis of the conduits is out of scope but may follow a similar process.
2. Management of complexity. The direct usage of extensive catalogs of threats and attacks, e.g., CAPEC[1] or MITRE ATT&CK[2], would lead to very complex, time-consuming, and costly analysis. The proposed methodology analyses the assets of the SUC using categories of threats as in a threat and operability analysis (THROP). Each threat category associated with the asset is systematically examined by the analyst together with the asset owner/system integrator, and the related impact and likelihood are identified and combined to derive the risk.
3. Identification of tailored countermeasures for each asset. During the risk determination process, the methodology identifies and evaluates the critical attack paths that could be exploited by an attacker to reach and threaten a specific asset. Threats are identified according to categories, and each threat category is associated with the possible countermeasures derived from the ISA/IEC 62443-3-3 part, which lists the security requirements grouped by Foundational Requirements (FR). This allows the asset owner to invest in specific solutions, rather than apply the entire set of countermeasures to the whole zone.
4. Involvement of the asset owner or system integrator. These figures participate directly in several steps of the methodology, e.g., during the evaluation of impact and likelihood of threats.
5. Tool support. The methodology is supported by a toolchain of spreadsheets and scripts, which provide the analyst with a semi-automated approach.

To the best of our knowledge, this is the only existing methodology integrating all these key features (a detailed discussion is given in section 5).

The rest of the paper is organized as follows. In section 2 we give the basics on risk assessment and ISA/IEC 62443 standard. In section 3 we present a case study in the power production domain, which will be used along the paper to show the application of the methodology. In section 4 we illustrate the proposed methodology step by step, in accordance with ZCR 5, also showing its application to the case study. In section 5 we discuss the related works and compare them with key aspects of the proposed methodology. Possible limitations of the methodology are then discussed in section 6, while section 7 concludes the paper.

2 Background

2.1 ISA/IEC 62443

The ISA/IEC 62443 [17] is a series of standards that define requirements and processes for the project, development, and maintenance of electronically secure industrial automation and control systems (IACS).

Each of the individual standards and reports in the ISA 62443 series addresses a specific aspect of the process. The elements of the series are organized into four groups. The first group, the general group, includes elements that address topics common to the whole series (62443-1-1, 62443-1-2, 62443-1-3, and 62443-1-4). Elements of the second group

[1] https://capec.mitre.org/

[2] https://attack.mitre.org/

focus on policies and procedures associated with IACS security (62443-2-1, 62443-2-2, 62443-2-3, 62443-2-4, and 62443-2-5). The elements of the third group (62443-3-1, 62443-3-2, and 62443-3-3) relate to system-level security technologies, risk assessment, and requirements. Finally, items in the fourth group include information on the more specific and detailed requirements associated with the development of IACS (62443-4-1 and 62443-4-2). Each of the standards and technical reports in the series is specifically intended for application at one or more stages of an IACS' life cycle.

A key concept of the standard is the definition of IACS zones and conduits, introduced in IEC 62443-1-1. Zones are a grouping of logical or physical assets based upon risk or other criteria, such as criticality of assets, operational function, physical or logical location, required access (e.g., least privilege principles), or responsible organization. Conduits, instead, are a logical grouping of communication channels that share common security requirements connecting two or more zones.

Another concept of the standard is the security level (SL), which is the measure of confidence that the SUC, security zone, or conduit is free from vulnerabilities and behaves in the intended manner. The target security level (SL-T) is the desired level of security for a particular IACS, zone, or conduit. The achieved security level (SL-A) is instead the actual level of security, attained with the current configurations and security countermeasures. The possible values of an SL are the following:

- SL 0: No specific requirements or security protection necessary.
- SL 1: Protection against casual or coincidental violations.
- SL 2: Protection against intentional violation using simple means with low resources, generic skills, and low motivation.
- SL 3: Protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation.
- SL 4: Protection against intentional violation using sophisticated means with extended resources, IACS-specific skills, and high motivation.

2.1.1 ISA/IEC 62443-3-2

There is no simple procedure that can be followed to easily understand how secure an IACS is. Each IACS has different levels of risk, depending on its vulnerabilities, the threats to which it is exposed, the likelihood of those threats occurring, and the consequences if the system is compromised. In addition, every application domain that works and operates with IACS has its own risk tolerance. The IEC 62443-3-2 part of the standard aims to define a set of engineering measures to guide the process of risk assessment of a particular IACS and identify and apply countermeasures to reduce the risk to tolerable levels.

The IEC 62443-3-2 document describes the guidelines for dividing the SUC into zones and conduits for assessing cybersecurity risk and determining the SL-T for each defined zone and conduit. The steps of the process are the following:

- ZCR 1: Identify the SUC. The SUC shall be identified by the organization, including a demarcation of the security perimeter and an identification of all access points to the SUC.
- ZCR 2: Initial cybersecurity risk assessment. A cyber security risk assessment of the SUC shall be performed by the organization to identify the initial cyber security risk related to the IACS operations.
- ZCR 3: Partition the SUC into zones and conduits. The SUC shall be divided into zones and conduits, separating business from IACS/safety assets, and wireless and external networks.
- ZCR 4: Risk comparison. The initial risk determined in ZCR 2 shall be compared to the organization's tolerable risk. If the initial risk exceeds the tolerable risk, the organization shall perform a detailed cybersecurity risk assessment.
- ZCR 5: Perform a detailed cybersecurity risk assessment. The detailed risk assessment process includes, among others the identification of threats, the derivation of their impact, likelihood and risk, and the determination of countermeasures.
- ZCR 6: Document cyber security requirements, assumptions and constraints. A cybersecurity requirements specification (CRS) shall be created to document mandatory security countermeasures of the SUC based on the outcome of the detailed risk assessment as well as general security requirements based upon company policies, and other standards/regulations.
- ZCR 7: Asset owner approval. The asset owner shall review and approve the results of the cybersecurity risk assessment.

The focus of the methodology proposed in this work is on the ZCR 5, i.e., the detailed risk assessment phase, which will be discussed in section 4.

3 IACS case study: a power generation plant using gas turbines

In this section we present a specific IACS in the power production domain, depicted in Figure 1, which will be used in the rest of the paper as a case study for the application of the methodology. We present here a sanitized version of a real system that was analyzed with the proposed methodology.

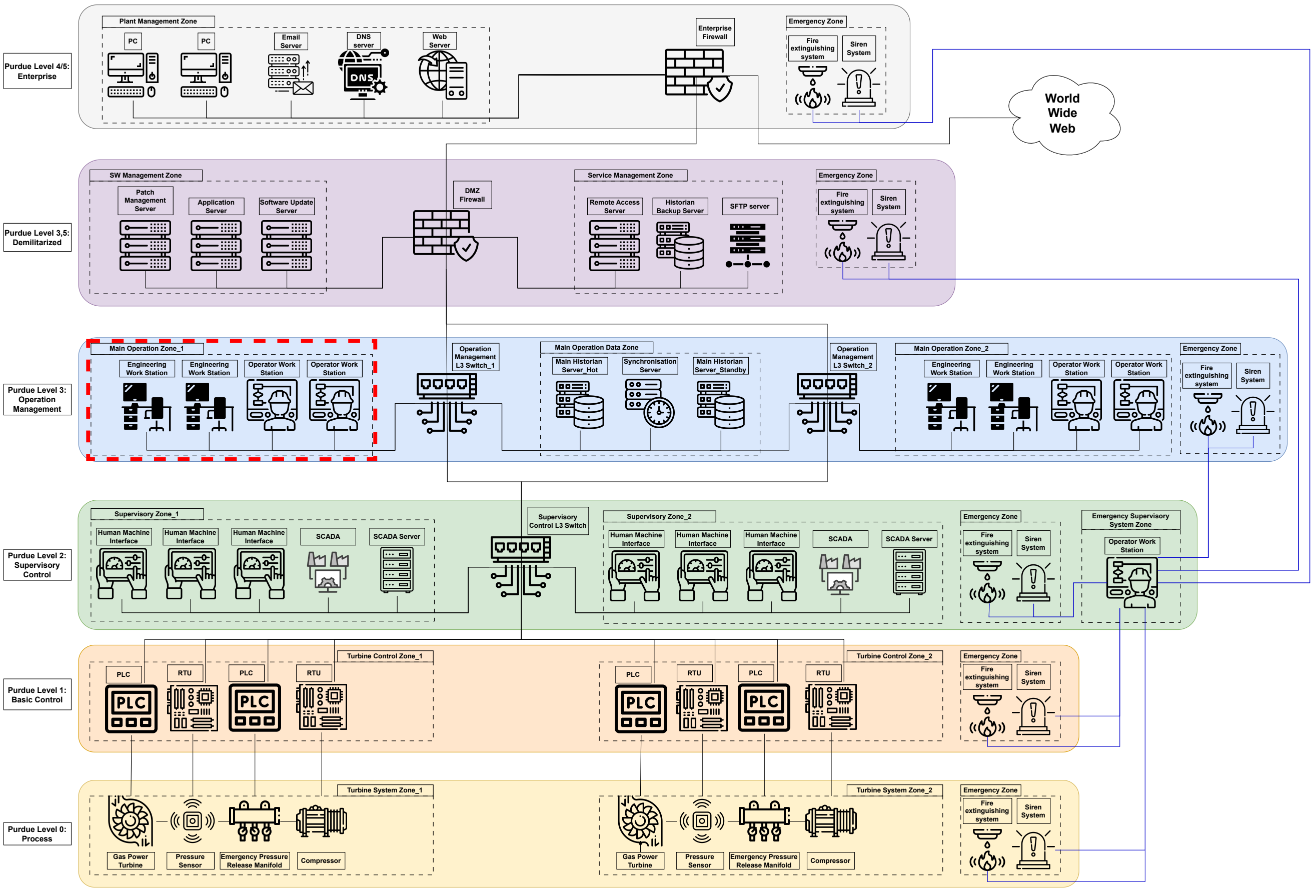


Fig. 1 Architectural view of the power generation plant SUC according to the Purdue Model. The focus of the exemplification of the methodology is the Main Operation Zone 1, which is here highlighted by a thick dotted line.

The reported system architecture refers to an IACS of a power generation plant using gas turbines. The system architecture, represented in Figure 1 with the Purdue Model [27], consists of six levels:

- Level 0 (Process): This level consists of all the operational (physical) components of the system (turbines, pressure sensors, compressors, etc.). All the physical processes of power production take place in this level.
- Level 1 (Basic Control): This level is composed of different electronic control devices, such as Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs), which deal with the management of physical devices of level 0, and interact with level 2 for data exchange and for the process of configuring work parameters.
- Level 2 (Supervisory Control): This level includes all the control components of the devices of the underlying levels, such as the Human Machine Interfaces (HMI) and the Supervisory Control and Data Acquisition (SCADA) systems. HMIs allow to view the parameters of devices in the lower tiers and provide the interface through which these devices are programmed, starting from workstations located at the upper level. SCADA systems, on the other hand, allow the acquisition of plant data from the lower levels.
- Level 3 (Operation Management): This level consists of the operating stations of engineers and operators, also including the communications distribution equipment, i.e., two L3 Switches that are used to connect the workstations with the respective turbine control areas and with the historical databases, which contain all the operational data of the plant.
- Level 3.5 (Demilitarized): This level contains all the devices, servers and databases necessary to make an adequate separation between the OT zone (represented by levels 0, 1, 2 and 3) and the IT zone (represented by level 4/5). This level allows to "filter" communications between these two zones, to disallow unauthorized traffic to the operational areas. This separation is achieved through a firewall configured with specific rules, which manages incoming and outgoing communication between the IT and OT zones.

- Level 4/5 (Enterprise): This level consists of management employee workstations, servers and PCs that allow them to monitor the status of the system (such as performance parameters, or system operating parameters). From that level, it is possible to reach even the lowest levels of control, if necessary, first going through the level 4/5 firewall and then through the level 3.5 firewall.

To exemplify the application of the methodology, in the following section we will consider a subset of the whole architecture focusing on the Main Operation Zone 1 at level 3 (highlighted in Figure 1 by a thick dotted line). Here we have two Operator Workstations, that are used for monitoring all system operations, e.g., accessing the data of the RTUs and PLCs (level 2) and of the Historian Server (level 3) responsible for collecting and storing the plant's operational data. In this zone, they are also located two Engineering Workstations that consist of a mobile laptop used for device maintenance in facilities, i.e., database configuration, and generation and modification of reports. Both Operator Workstation and Engineering Workstation are responsible for managing the configuration parameters of the lower-level machines (RTUs, PLCs, and SCADA).

For the sake of clarity, we limit the explanation of the methodology to a small portion of the system (one zone). Given that the SUC is partitioned into zones and conduits (as required by the standard), the time and effort required to apply the methodology to the whole system will scale linearly with the number of zones. In general, the most time-demanding steps are those that require an interaction with the asset owner, like ZCR 5.3: Determine consequences and impact, ZCR 5.4: Determine unmitigated likelihood, and ZCR 5.8: Identify and evaluate existing countermeasures.

4 Methodology

This section focuses on the proposed risk assessment methodology and on its application to the selected case study (presented in section 3). An overview of the methodology is depicted in Figure 2, which emphasizes the expected input and output for each step of the whole detailed cybersecurity risk assessment process following the steps of ZCR 5.

4.1 ZCR 5.1: Identify threats

Guidelines from ISA/IEC 62443. *The standard requires to define a list of the threats that could affect the assets contained within the zone or conduit. For each threat, the standard suggests to provide a description of the threat source, a description of the capability or skill level of the threat source, a description of possible threat vectors, and an identification of the potentially affected asset(s).*

Challenge: how to identify the threat vectors.

To identify the threat vectors it is necessary to explicitly represent the communication channels that connect the assets of the zones, taking into account both logical data flows and network connections. For this purpose, this step takes as input a sequence diagram of the use cases and the detailed architecture description/diagram of the SUC, depicted according to the Purdue Model [27]. The Purdue Model representation is suggested by the standard, but different models could be used as well.

For each zone of the SUC, that has been already identified and is provided as input to the methodology, a Data Flow Diagram (DFD) is also provided. DFD uses the element shapes from the Microsoft SDL methodology [14], i.e., process, data store, external entity, data flow, and trust boundary, and it can be created using Draw.io[3]. Each asset inside the zone is represented as a process or as a data store (depending on its kind). Data flow elements are used to connect the assets within and outside the zone and trust boundary elements are used to delimit the zones. All the other assets outside the zone (even those at the same Purdue level) are represented as external entities. The external entities to be represented depend on the physical and logical connections and on the considered use case. According to the Purdue Model, a level can directly communicate only to the levels close to it, i.e., the upper and/or the lower level. Hence, for a zone located at a certain level of the Purdue Model, the other zones to be represented in the DFD are those located at the same level and/or at the upper/lower level that are directly linked to the considered zone. Data flow elements are used to connect the assets of the zone with other internal or external assets, reflecting the physical connections and logical data flows. Network components like firewalls or L3 switches are conduits and will be evaluated during the conduits analysis, together with the communication protocols used.

Challenge: how to identify the threats associated with the assets of the SUC, managing the complexity of the process.

The second important output of this step of the methodology is the identification of the threats associated with each asset, which might be a very complex task. In fact, using extensive catalogs of threats would quickly lead to an unmanageable number of threats to be considered, which would impair the applicability of this strategy to real complex systems. The proposed methodology attacks this problem relying on threats categories rather than on specific threats, based on the six threats categories defined by the STRIDE methodology [14]: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. In Table 1 we provide a synthetic description of these categories, and the identification of the specific CIA-

[3] https://app.diagrams.net/

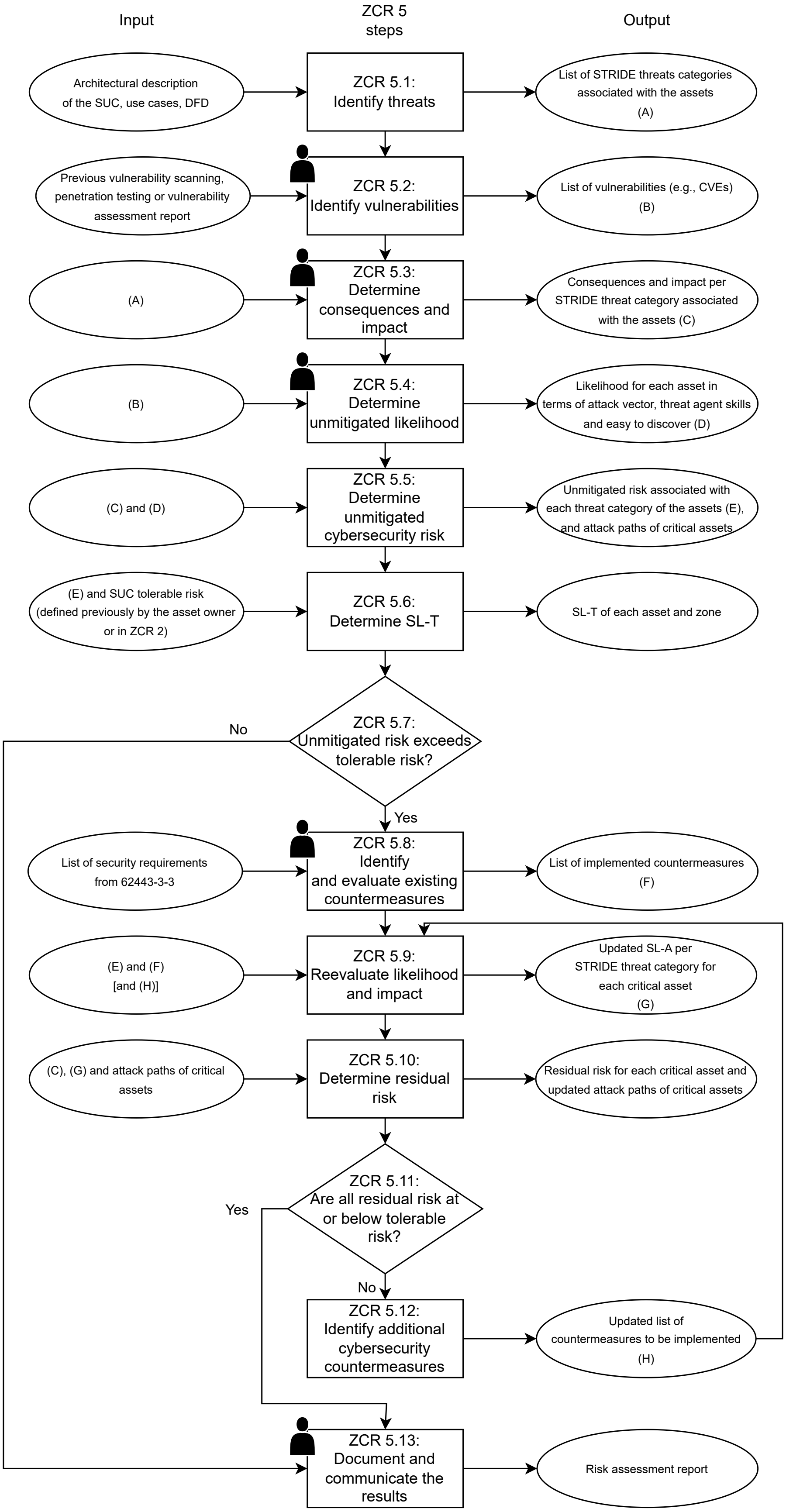

Input
ZCR 5 steps
Output
Architectural description of the SUC, use cases, DFD
ZCR 5.1: Identify threats
List of STRIDE threats categories associated with the assets (A)
Previous vulnerability scanning, penetration testing or vulnerability assessment report
ZCR 5.2: Identify vulnerabilities
List of vulnerabilities (e.g., CVEs) (B)
(A)
ZCR 5.3: Determine consequences and impact
Consequences and impact per STRIDE threat category associated with the assets (C)
(B)
ZCR 5.4: Determine unmitigated likelihood
Likelihood for each asset in terms of attack vector, threat agent skills and easy to discover (D)
(C) and (D)
ZCR 5.5: Determine unmitigated cybersecurity risk
Unmitigated risk associated with each threat category of the assets (E), and attack paths of critical assets
(E) and SUC tolerable risk (defined previously by the asset owner or in ZCR 2)
ZCR 5.6: Determine SL-T
SL-T of each asset and zone
ZCR 5.7: Unmitigated risk exceeds tolerable risk?
No
Yes
List of security requirements from 62443-3-3
ZCR 5.8: Identify and evaluate existing countermeasures
List of implemented countermeasures (F)
(E) and (F) [and (H)]
ZCR 5.9: Reevaluate likelihood and impact
Updated SL-A per STRIDE threat category for each critical asset (G)
(C), (G) and attack paths of critical assets
ZCR 5.10: Determine residual risk
Residual risk for each critical asset and updated attack paths of critical assets
ZCR 5.11: Are all residual risk at or below tolerable risk?
Yes
No
ZCR 5.12: Identify additional cybersecurity countermeasures
Updated list of countermeasures to be implemented (H)
ZCR 5.13: Document and communicate the results
Risk assessment report

Fig. 2 Overview of the methodology. In the central part of the diagram there are the steps of the methodology. In the left part the inputs to the steps are represented, while in the right part, the outputs are shown. The steps where the asset owner is directly involved are marked with a human-like symbol.

Threat Category	CIA-AAA Property
Spoofing: breaching the user's authentication information	**Authentication**: verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources
Tampering: modifying system or user data with or without detection	**Integrity**: guarding against improper information modification or destruction
Repudiation: denying a wrongdoing without any way to prove otherwise	**Auditing (Accountability)**: ensuring that the actions of an entity may be traced uniquely to that entity
Information disclosure: exposing information to individuals who are not supposed to see it	**Confidentiality**: preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
Denial of service: making the system temporarily unavailable or unusable	**Availability**: ensuring timely and reliable access to and use of information
Elevation of privilege: an unprivileged user gains privileged access and thereby has sufficient access to potentially compromise or destroy the entire system	**Authorization**: the right or permission that is granted to a system entity to access a system resource

Table 1 Mapping between STRIDE threats and CIA and AAA properties [22].

AAA (Confidentiality, Integrity, Availability - Authentication, Authorization, Auditing) security property affected/targeted by such threats, as proposed by [22].

For applying the methodology we consider each asset of the zone represented as a Process or Data Store in the DFD, and we associate to each of them the STRIDE threat categories applicable to the specific asset. External entities are not considered during this phase, since they will be evaluated when their zone is analyzed.

Application to the case study. Concerning the application of the methodology to the case study described in section 3, the zones and conduits of the SUC presented in Figure 1 are used as input to this step. The produced DFD of the Main Operation Zone 1 is depicted in Figure 3.

Note that, following the methodology, when we focus on a specific zone, all the assets inside the zone are represented as processes, while assets of the other zones are represented as External Entities. In each DFD we represent as External Entities only the assets that are contained in zones at the same/upper/lower level of the considered zone. For example, in Figure 3, we represent as external entities the assets of Main Operation Data Zone and Main Operation Zone 2, which are at the same level as Main Operation Zone 1, and SW Management Zone and Service Management Zone, which are at the upper level. We do not represent the assets of the Plant Management Zone as they are located at level 4/5 and they are not directly communicating with level 3. In the selected zone all the communications between assets are bidirectional.

Concerning the threats, we apply all the STRIDE threat categories to the assets contained within the zones.

4.2 ZCR 5.2: Identify vulnerabilities

Guidelines from ISA/IEC 62443. *The standard requires to define a list of known vulnerabilities associated with the assets contained within the zone or conduit.*

Challenge: how to identify the SUC's vulnerabilities and how to consider them in the risk assessment process.

At this point of the methodology, with the help of the asset owner, the vulnerabilities related to the assets of the SUC are identified and enumerated. One could rely on prior vulnerability assessment reports, penetration testing activities, SUC security probes, or vulnerability scanning enumerations provided by the asset owner. Hence, the output of this activity is a list of vulnerabilities, e.g., a list of scanned Common Vulnerabilities and Exposures[4] (CVE). If not provided by the asset owner, the vulnerabilities can be retrieved from the CVEs catalog based on the model and manufacturer brand of the asset. CVE vulnerabilities can then be mapped to STRIDE threats categories using CWE[5] and NVD[6] catalogs.

The list of vulnerabilities is identified here for compliance with ISA/IEC 62443. The actual management of the vulnerabilities is then delegated to the security management process, which will address the most severe vulnerabilities. In fact, the final CSR document produced during ZCR 6 will specify that, to reach a zone SL-T and therefore for each asset, it will be necessary to resolve the identified CVEs that exceed a specific severity threshold.

4.3 ZCR 5.3: Determine consequence and impact

Guidelines from ISA/IEC 62443. *In this step, the standard asks for an evaluation of each threat scenario to determine the consequence and the impact in case of threat exploitation. Consequences should be documented in terms of the worst-case impact on risk areas such as personnel safety, financial loss, business interruption, and environment.*

Challenge: how to identify the consequences and impact of each threat category on the assets.

In our approach, each asset of the SUC is analyzed in a Threat and Operability (THROP) manner, where the STRIDE threat categories are applied to the assets. In this step, the asset owner plays a major role in assessing the real value of the assets and the impact/consequences in case of attacks.

[4] https://cve.mitre.org/
[5] https://cwe.mitre.org/
[6] https://nvd.nist.gov/

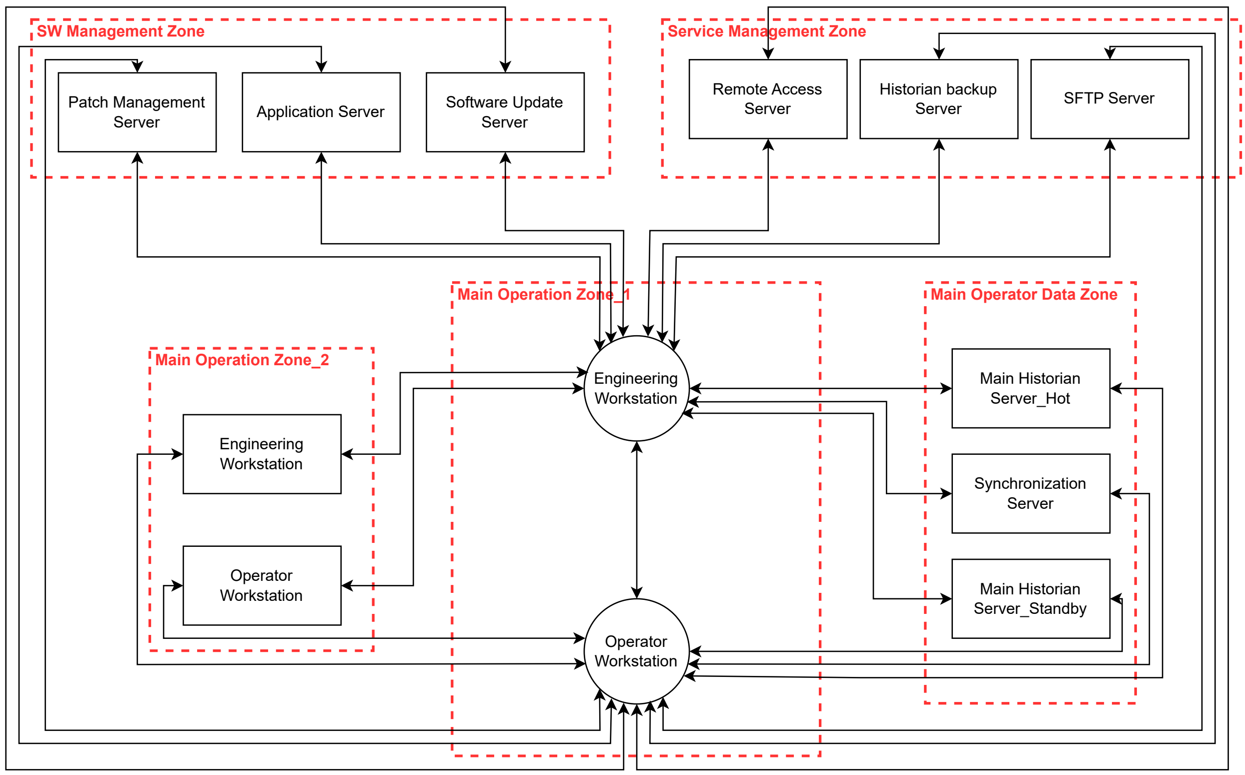


Fig. 3 DFD of the Main Operation Zone 1.

First, for each asset, data exchanged between the considered asset and other assets or external entities are identified. In particular, when analysing a specific asset, only outgoing communications from the asset under consideration to the other assets are taken into account. Incoming communications will be considered when the other assets are analysed. For each asset we need to perform a consequence analysis and an impact analysis.

Consequence analysis. We have to analyse what are the consequences of the exploitation of each different STRIDE threat category on the asset, and on its connected assets. To accomplish this task we rely on the knowledge of the SUC (also with the help of the asset owner) and on the consequences that are commonly associated with STRIDE threats. The combination of the knowledge of the owner and the expertise of the analyst plays a fundamental part in this activity. As already mentioned, some of the STRIDE threat categories might not be applicable due to the nature of the asset. For example, Spoofing, Repudiation, and Elevation of Privilege are generally not applicable to those assets that do not distinguish between different users (e.g., actuators). In these cases, the impact analysis will be limited to a subset of the STRIDE threat categories.

Worst-case scenarios are built on the functions and data type of the assets, considering the STRIDE threats. The functions of the various assets are described in the use case diagrams that are built together with the asset owner. The worst cases will correspond to the assets that are marked as critical, i.e., those whose risk is greater than the tolerable risk (see subsection 4.5).

Impact analysis. Then, the impact on each threat category is assigned together with the asset owner in terms of Business and Operational, Financial (Cost, Legal and Public Confidence), and Human, Safety, and Environmental (HSE) impacts (from Table B.3 of the annex B of 62443-3-2 [17]), assigning to each impact factor a qualitative score ranging from Low to High (for a total of five levels). Note that the qualitative levels can be adjusted according to the asset owner's needs and/or the level of abstraction of the information that the asset owner is able to provide. The final impact score of the threats over an asset is given by the maximum value among the impacts assigned to the STRIDE threat categories over the asset, thus adopting a conservative worst-case impact estimation.

Application to the case study. Concerning the consequences and impact analysis applied to the case study, we focused on the Operator Workstation in the Main Operation Zone 1 and on two specific data communications: the historian server access data that are sent to the Historian Server (external entity), and the PLCs status data that are sent to the Engineering Workstation. In Figure 4 we show the consequences and impact analysis of the Operator Workstation in the Main Operation Zone 1.

For example, focusing on the PLCs status sent by the Operator Workstation to the Engineering Workstation, the consequences identified for the Denial of Service (DoS) threat category are that the data will not be sent to the Engineering Workstation, which may lead to the loss of functional operations relying on these data. The impact of such consequences are then assessed with the owner that assigns a qualitative score to Business and Operational, Financial, and HSE impacts. For Business and Operational impact a Med-Low score is assigned since the asset owner estimates a little impact on sectors beyond the individual company and on the community in the case of DoS on the PLCs status data. Also for the Financial impact, a Med-Low score is assigned since a moderate financial loss is estimated, with minor impact in terms of extraordinary legal actions or fines, related to contractual or legal requirements and minor loss of brand image, third-party relationships, and customers. Finally, for the HSE impact, a Medium score is assigned since the DoS of the PLCs data might hinder the prompt intervention in case of emergencies in the plant, which might cause minor injuries to the personnel.

The final impacts of the threats grouped by threat category are shown in Figure 5, taking the maximum value of the impact assigned to the threat categories.

4.4 ZCR 5.4: Determine unmitigated likelihood

Guidelines from ISA/IEC 62443. *In this step, the standard requires to determine the unmitigated likelihood associated with each threat.*

Challenge: how to identify the likelihood of an attack to each asset of the SUC.

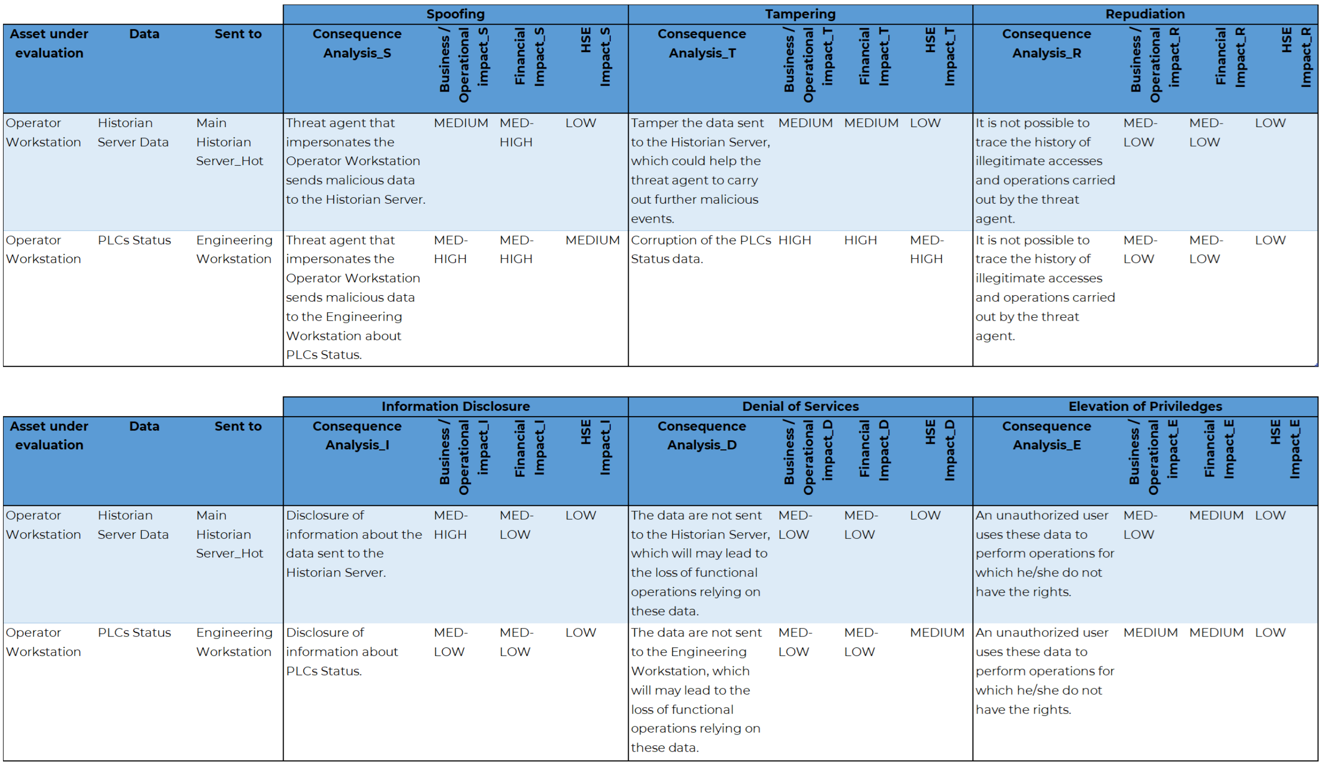
At this point of the ZCR 5, security countermeasures of the system are not considered since it is asked to derive the unmitigated risk. Assigning a likelihood to every single threat would be unfeasible since it would be difficult to reasonably explain how probable an attacker could successfully exploit a specific threat over the asset. For this reason, in the methodology, rather than assigning a likelihood to each single threat category, we adopt the *Attack Feasibility Rating* (AFR) metric defined as the ease with which a threat agent can successfully attack the asset, which is related to the intrinsic nature of the asset, i.e., on how the asset has been developed. The AFR is therefore estimated according to the following factors, which are partially inspired by the guidelines of ZCR 5.1 (identify threats, subsection 4.1):

- *Attack Vector*: it is inspired by the metric with the same name from the CVSS 4.0[7] and reflects the context by which threat exploitation is possible. The qualitative values adopted are Physical, Local, Adjacent, and Network, in ascending level of likelihood. For example, an asset directly connected to a network will be more probably attacked than an asset that can be only accessed physically.
- *Threat Agent Skills*: it is adopted from CLC/TS 50701 (Table 4, Likelihood assessment matrix) [9]. It indicates the typical attacker that can threaten the asset. For critical systems, this factor is set to High, while for other kinds of systems, it is set to Low.
- *Easy to Discover*: it is derived from CLC/TS 50701 (Table 4, Likelihood assessment matrix) [9]. It estimates the effort demanded by an attacker to identify the asset's vulnerabilities that might exploit the threats. This is related to the development process of the asset. For example, if the asset is a COTS, it will very likely contain well-known vulnerabilities, while if the asset's development follows a highly recognized security life cycle, it will very unlikely contain well-known vulnerabilities. Five levels are adopted, ranging from Low to High.

As for the impact, a qualitative score is assigned to each likelihood factor (ranging from Low to High). For each asset, the *Attack Feasibility Rating* is then derived using a 3-dimensional array that combines the three qualitative factors. The qualitative levels can be customized according to the owner's needs.

Application to the case study. In the lower part of the spreadsheet in Figure 5 (*AFR* field) we show the *Attack Feasibility Rating* estimation for the assets of the Main Operation Zone 1. A "Network" Attack Vector is assigned to the Operator Workstation, since the asset can be compromised directly from the Internet. Then a High score is assigned to the Threat Agent Skills since the power plant is a critical system that can be the potential target of advanced threat agents, e.g., terrorists organizations. The asset is developed with a quality-management software-development life cycle, so an attacker might be able to discover the weakness, but would possibly require to access the source code or have some reverse engineering knowledge. Therefore, a Medium score is assigned to the Easy to Discover. Combining these three factors through the 3-dimensional array, a Med-High score is assigned to the Attack Feasibility Rating.

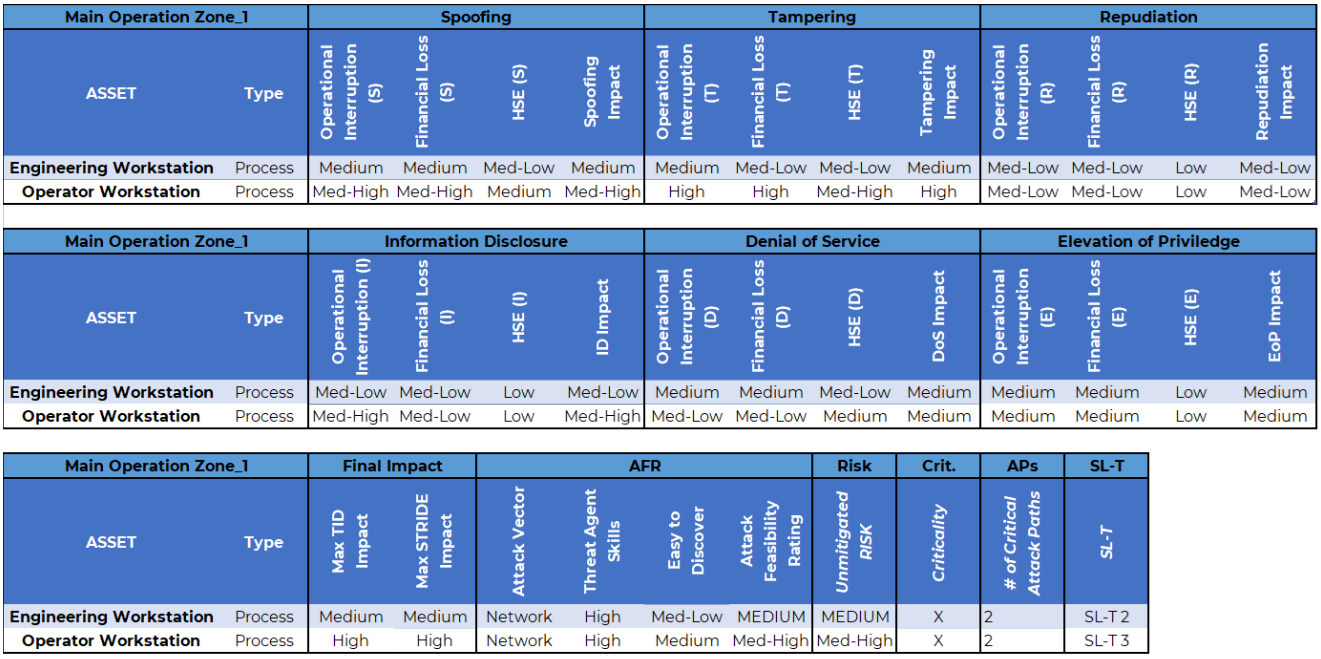
[7] https://www.first.org/cvss/v4.0/specification-document



Asset under evaluation	Data	Sent to	Spoofing Consequence Analysis_S	Business / Operational impact_S	Financial Impact_S	HSE Impact_S	Tampering Consequence Analysis_T	Business / Operational impact_T	Financial Impact_T	HSE Impact_T	Repudiation Consequence Analysis_R	Business / Operational impact_R	Financial Impact_R	HSE Impact_R
Operator Workstation	Historian Server Data	Main Historian Server_Hot	Threat agent that impersonates the Operator Workstation sends malicious data to the Historian Server.	MEDIUM	MED-HIGH	LOW	Tamper the data sent to the Historian Server, which could help the threat agent to carry out further malicious events.	MEDIUM	MEDIUM	LOW	It is not possible to trace the history of illegitimate accesses and operations carried out by the threat agent.	MED-LOW	MED-LOW	LOW
Operator Workstation	PLCs Status	Engineering Workstation	Threat agent that impersonates the Operator Workstation sends malicious data to the Engineering Workstation about PLCs Status.	MED-HIGH	MED-HIGH	MEDIUM	Corruption of the PLCs Status data.	HIGH	HIGH	MED-HIGH	It is not possible to trace the history of illegitimate accesses and operations carried out by the threat agent.	MED-LOW	MED-LOW	LOW

Asset under evaluation	Data	Sent to	Information Disclosure Consequence Analysis_I	Business / Operational impact_I	Financial Impact_I	HSE Impact_I	Denial of Services Consequence Analysis_D	Business / Operational impact_D	Financial Impact_D	HSE Impact_D	Elevation of Priviledges Consequence Analysis_E	Business / Operational impact_E	Financial Impact_E	HSE Impact_E
Operator Workstation	Historian Server Data	Main Historian Server_Hot	Disclosure of information about the data sent to the Historian Server.	MED-HIGH	MED-LOW	LOW	The data are not sent to the Historian Server, which will may lead to the loss of functional operations relying on these data.	MED-LOW	MED-LOW	LOW	An unauthorized user uses these data to perform operations for which he/she do not have the rights.	MED-LOW	MEDIUM	LOW
Operator Workstation	PLCs Status	Engineering Workstation	Disclosure of information about PLCs Status.	MED-LOW	MED-LOW	LOW	The data are not sent to the Engineering Workstation, which will may lead to the loss of functional operations relying on these data.	MED-LOW	MED-LOW	MEDIUM	An unauthorized user uses these data to perform operations for which he/she do not have the rights.	MEDIUM	MEDIUM	LOW

Fig. 4 Consequences and impact analysis of the Main Operation Zone 1. The *asset under evaluation* field identifies the considered asset. The *data* field specifies the type of exchanged data to analyse. The *sent to* field contains the destination of the data coming from the asset under evaluation. Then, for each STRIDE threat categories, the consequences for the specified data exchange are reported, along with the corresponding Business and Operational, Financial, and Human, Safety, and Environmental (HSE) impact scores.

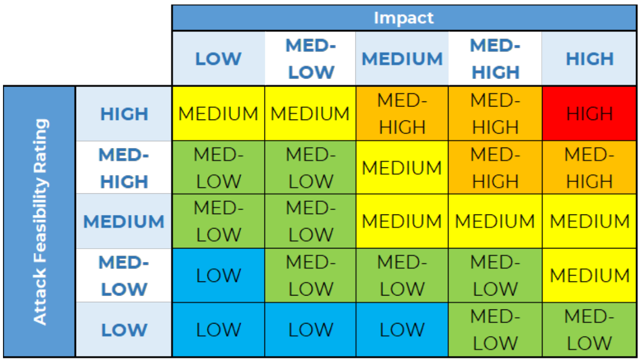


Main Operation Zone_1		Spoofing				Tampering				Repudiation			
ASSET	Type	Operational Interruption (S)	Financial Loss (S)	HSE (S)	Spoofing Impact	Operational Interruption (T)	Financial Loss (T)	HSE (T)	Tampering Impact	Operational Interruption (R)	Financial Loss (R)	HSE (R)	Repudiation Impact
Engineering Workstation	Process	Medium	Medium	Med-Low	Medium	Medium	Med-Low	Med-Low	Medium	Med-Low	Med-Low	Low	Med-Low
Operator Workstation	Process	Med-High	Med-High	Medium	Med-High	High	High	Med-High	High	Med-Low	Med-Low	Low	Med-Low

Main Operation Zone_1		Information Disclosure				Denial of Service				Elevation of Priviledge			
ASSET	Type	Operational Interruption (I)	Financial Loss (I)	HSE (I)	ID Impact	Operational Interruption (D)	Financial Loss (D)	HSE (D)	DoS Impact	Operational Interruption (E)	Financial Loss (E)	HSE (E)	EoP Impact
Engineering Workstation	Process	Med-Low	Med-Low	Low	Med-Low	Medium	Medium	Med-Low	Medium	Medium	Medium	Low	Medium
Operator Workstation	Process	Med-High	Med-Low	Low	Med-High	Med-Low	Med-Low	Medium	Medium	Medium	Medium	Low	Medium

Main Operation Zone_1		Final Impact		AFR				Risk	Crit.	APs	SL-T
ASSET	Type	Max TID Impact	Max STRIDE Impact	Attack Vector	Threat Agent Skills	Easy to Discover	Attack Feasibility Rating	*Unmitigated RISK*	*Criticality*	*# of Critical Attack Paths*	*SL-T*
Engineering Workstation	Process	Medium	Medium	Network	High	Med-Low	MEDIUM	MEDIUM	X	2	SL-T 2
Operator Workstation	Process	High	High	Network	High	Medium	Med-High	Med-High	X	2	SL-T 3

Fig. 5 Asset evaluation of the Main Operation Zone 1. For each asset, the spreadsheet provides the following elements: the maximum Business and Operational, Financial, and Human, Safety, and Environmental (HSE) impacts are reported for each STRIDE threat category; the final TID and STRIDE impacts associated with the asset, given by the maximum score among the impact over the TID and STRIDE threat categories; the AFR score and the factors that are combined to obtain it (*Attack Vector*, *Threat Agent Skills*, and *Easy to Discover*); the *Unmitigated Risk*, obtained as a combination of final STRIDE impact and AFR; the *criticality* of the asset and the *number of critical attack paths*; the *SL-T*.



		Impact				
		LOW	MED-LOW	MEDIUM	MED-HIGH	HIGH
Attack Feasibility Rating	HIGH	MEDIUM	MEDIUM	MED-HIGH	MED-HIGH	HIGH
	MED-HIGH	MED-LOW	MED-LOW	MEDIUM	MED-HIGH	MED-HIGH
	MEDIUM	MED-LOW	MED-LOW	MEDIUM	MEDIUM	MEDIUM
	MED-LOW	LOW	MED-LOW	MED-LOW	MED-LOW	MEDIUM
	LOW	LOW	LOW	LOW	MED-LOW	MED-LOW

Fig. 6 Example of risk matrix combining attack feasibility rating and impact.

4.5 ZCR 5.5: Determine unmitigated cybersecurity risk

Guidelines from ISA/IEC 62443. *Following the standard, the unmitigated cybersecurity risk for each threat shall be determined combining the impact and the unmitigated likelihood identified in ZCR 5.3 and ZCR 5.4, respectively.*

Challenge: how to assign a risk score to each asset.

In our approach, the unmitigated risk for each asset is computed using a risk matrix as the one shown in Figure 6, which combines impact and AFR scores. Such a matrix can be customized according to the company's needs. An asset is marked as critical if its risk level is greater than the tolerable risk. The tolerable risk should have been defined previously by the asset owner and/or in ZCR 2. It is worthwhile emphasizing that this type of risk assessment is based on the likelihood that attacks/threats will directly target each asset, so it is not considering the possible attack paths targeting the same assets but started from other assets of the zone.

Challenge: how to analyze the propagation of an attack within the zone.

Besides considering the threats directly targeting a critical asset, we need to consider all the possible attack paths targeting each asset but started from other assets within the zone. An attack path represents the path, with the corresponding steps, that the attacker can follow and exploit to reach the final goal. The attack paths are derived starting from external entities, while the entity targeted by the attacker, called objective target, is chosen among the assets within the considered zone.

The attack paths can be derived from the DFD produced during ZCR 5.1 (subsection 4.1). The derivation of the attack paths associated with a zone is done following the steps shown in Listing 1.

The risk of an attack path is calculated combining the attack path AFR and the attack path impact, still using the risk matrix in Figure 6. The attack path AFR is given by the minimum AFR of the assets involved in the attack path, which constitutes the most difficult attack step to be performed by an attacker (it is less ease that a threat agent can successfully complete this attack step). This means that, for each attack path, we are considering the asset that is more difficult to be attacked, hence, the asset having more probabilities to cut off the attack chain. The attack path impact, instead is the impact score of the TID (a subset of STRIDE) assigned to the objective target asset, i.e., considering the maximum impact score related to Tampering, Information Disclosure, and Denial of Service. Only TID threat categories are considered as possible threats for the objective target asset, since Spoofing, Repudiation, and Elevation of Privilege are not final objectives but are typically used by an attacker as intermediate steps to reach the final goal. The attack paths whose risk is greater than the tolerable risk are marked as critical.

From an implementation point of view, following the Model-Driven Engineering (MDE) approach [24], the XML file related to the DFD is first exported from Draw.io and then it is parsed using a Python script for deriving all the possible attack paths targeting each critical asset, which are described in terms of nodes, edges, sources, and destinations. The attack paths are then reported into a spreadsheet that will be used in a next step to derive the risk associated with each attack path.

Application to the case study. Both Engineering Workstation and Operator Workstation are marked as critical (see Figure 5), having, respectively, a Medium and Med-High unmitigated risk which are both greater than the SUC tolerable risk (Low).

The derived attack paths are shown in Figure 7. Each attack path is described by the IDs of the assets that compose it. The external entity from which the attack starts is not explicitly represented in the attack path. We take as an example the last attack path (the one with ID 4), which starts from one of the external entities, passes through the Engineering Workstation (ID 3), and ends on the Operator Workstation (ID 4, the objective target). The attack path AFR is set to Medium, which is the AFR score of the attack step with minimum AFR (the one associated with the Engineering Workstation). The attack path impact is High, which is the TID impact score of the objective target, i.e., the Operator Workstation. The derived risk is then Medium, which is greater than the tolerable risk, therefore the attack path is marked as critical. Following this approach we identified 4 critical attack paths in the Main Operation Zone 1.

4.6 ZCR 5.6: Determine SL-T

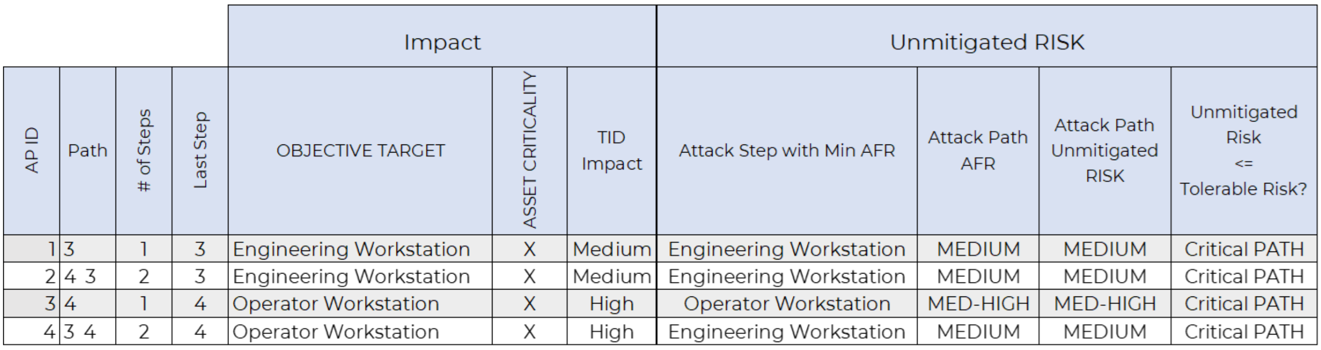
Guidelines from ISA/IEC 62443. *A target security level (SL-T) shall be established for each security zone or conduit.*

Challenge: how to assign a SL-T to each zone.

In our approach, we first assign a SL-T to each asset that is contained in a zone. The SL-T of an asset is calculated

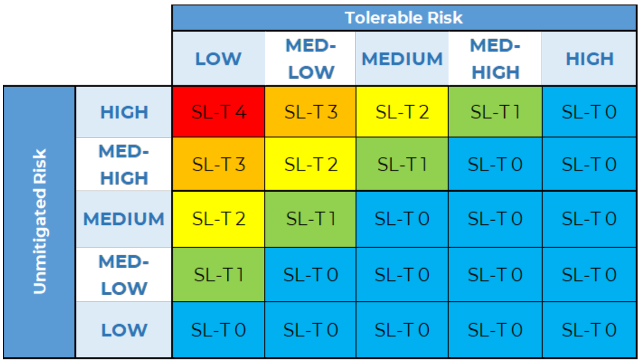
```
for each critical asset inside the zone
    fix an asset as objective target
    for each attack path from external entities to objective target
        attack path risk = min AFR among assets of the path ∗ TID impact of objective target
        if attack path risk > tolerable risk
            then mark the attack path as critical
```

Listing 1 Pseudo-code algorithm for the generation of the attack paths within a zone.



				Impact			Unmitigated RISK			
AP ID	Path	# of Steps	Last Step	OBJECTIVE TARGET	ASSET CRITICALITY	TID Impact	Attack Step with Min AFR	Attack Path AFR	Attack Path Unmitigated RISK	Unmitigated Risk <= Tolerable Risk?
1	3	1	3	Engineering Workstation	X	Medium	Engineering Workstation	MEDIUM	MEDIUM	Critical PATH
2	4 3	2	3	Engineering Workstation	X	Medium	Engineering Workstation	MEDIUM	MEDIUM	Critical PATH
3	4	1	4	Operator Workstation	X	High	Operator Workstation	MED-HIGH	MED-HIGH	Critical PATH
4	3 4	2	4	Operator Workstation	X	High	Engineering Workstation	MEDIUM	MEDIUM	Critical PATH

Fig. 7 Attack paths analysis for the the Main Operation Zone 1. The spreadsheet specifies, among others, the following information: the attack path, represented using the IDs of the assets that compose it; the *Objective Target*; the *TID impact*; the *attack path AFR*; the *attack path unmitigated risk*.



		Tolerable Risk				
		LOW	MED-LOW	MEDIUM	MED-HIGH	HIGH
Unmitigated Risk	HIGH	SL-T 4	SL-T 3	SL-T 2	SL-T 1	SL-T 0
	MED-HIGH	SL-T 3	SL-T 2	SL-T 1	SL-T 0	SL-T 0
	MEDIUM	SL-T 2	SL-T 1	SL-T 0	SL-T 0	SL-T 0
	MED-LOW	SL-T 1	SL-T 0	SL-T 0	SL-T 0	SL-T 0
	LOW	SL-T 0	SL-T 0	SL-T 0	SL-T 0	SL-T 0

Fig. 8 Example of SL-T matrix combining unmitigated risk and tolerable risk.

using the risk associated with the asset and the tolerable risk of the SUC according to the (customizable) matrix shown in Figure 8. Therefore, the SL-T of the zone is assigned using the maximum SL-T associated with the assets of the zone, following a conservative (worst-case) approach.

The SL-T identified here is temporary, and will be possibly updated when evaluating the existing (and additional) countermeasures.

Application to the case study. A SL-T 3 is assigned to the Operator Workstation since the maximum risk is Med-High and the SUC tolerable risk is Low. The SL-T of the Main Operation Zone 1 is SL-T 3, which is the maximum SL-T among its assets: SL-T 2 for the Engineering Workstation and SL-T 3 for the Operator Workstation.

4.7 ZCR 5.7: Compare unmitigated risk with tolerable risk

Guidelines from ISA/IEC 62443. *For this step, the standard asks for a comparison of the unmitigated risk for each threat (identified in ZCR 5.5) to the organization's tolerable risk. If the unmitigated risk exceeds the tolerable risk, the organization shall determine whether to accept or mitigate the risk. To mitigate the risk, it is required to further evaluate the threat by completing ZCR 5.8 through ZCR 5.12. Otherwise, the organization may document the results in ZCR 5.13 and proceed to the next threat.*

The attack paths having an associated risk greater than the tolerable risk are considered critical, so the risk associated to those attack paths has to be mitigated in the next steps of the methodology. If there are no critical attack paths, it is possible to skip to ZCR 5.13 (subsection 4.13).

Application to the case study. Four critical attack paths are associated with the Main Operation Zone 1 (see Figure 7), so the process must continue in order to mitigate the risk.

4.8 ZCR 5.8: Identify and evaluate existing countermeasures

Guidelines from ISA/IEC 62443. *The standard points out that already implemented countermeasures in the SUC shall be identified and evaluated to determine their effectiveness in reducing the likelihood or impact.*

Challenge: how to identify and classify already existing countermeasures.

The ISA/IEC 62443-3-3 part of the standard provides a list of security requirements grouped according to seven Foundational Requirements (FR). Since the STRIDE threat categories can be mapped to the foundational requirements [22] (see Table 2), except for the Restricted Data Flow, they can be used to evaluate how the existing countermeasures can leverage the likelihood of the threat categories and, therefore, the risk (see subsection 4.9). The list of security requirements is provided to the asset owner, who indicates which of them are already implemented in the SUC.

Application to the case study. An excerpt of the existing countermeasures identified for the assets of the Main Operation Zone 1, specifically those related to the Resource Availability (FR 7), are shown in Figure 9. For example, the asset owner reported the presence of a control system backup for the Operator Workstation, hence the SR 7.3 is marked as an existing countermeasure.

4.9 ZCR 5.9: Reevaluate likelihood and impact

Guidelines from ISA/IEC 62443. *At this point of the ZCR 5, impact and likelihood shall be re-evaluated considering the countermeasures already implemented in the SUC.*

Challenge: how to re-evaluate the assets considering the already implemented countermeasures.

The impact and likelihood (or AFR) associated with the asset are left unchanged when considering the already implemented countermeasures since they depend on the intrinsic characteristics of the system. According to 62443-3-3, what changes when considering the implemented countermeasures is the Security Level Achieved (SL-A). In particular, the guidelines provide, for a given FR, the list of required system requirements to meet a specific SL. In this way, for each threat category mapped to the FRs, it is possible to assign an SL-A associated with the asset on the basis of the already implemented security requirements (countermeasures).

Application to the case study. In Figure 10 we show the derivation of the SL-A for the Main Operation Zone 1 considering the existing countermeasures. Concerning the Denial of Service threat category, which corresponds to the Resource Availability (RA) FR, the security level achieved by the Operator Workstation is SL-A 0 ("RA" column of Figure 10), since not all the countermeasures required to reach SL 1 are implemented (in particular SR 7.2, SR 7.4 and SR 7.5 are not implemented on the Operator Workstation - as shown in the "Existing" column of Figure 9).

4.10 ZCR 5.10: Determine residual risk

Guidelines from ISA/IEC 62443. *The residual risk for each threat identified in ZCR 5.1, shall be determined by combining the mitigated likelihood and impact determined in ZCR 5.9.*

Challenge: how to re-evaluate the risk considering the already implemented countermeasures.

The risk is re-evaluated according to the SL-A derived through the list of implemented security countermeasures (subsection 4.9) and the unmitigated risk previously identified (subsection 4.5). Figure 11 reports the matrix used for the residual risk estimation. The total re-evaluated risk associated with an asset is the maximum re-evaluated risk among the STRIDE threat categories, following a conservative (worst-case) approach.

For the re-evaluation of the attack paths associated with critical assets, we adopt a method similar to the one used during ZCR 5.5 (subsection 4.5). In this case to compute the risk related to an attack path we consider, besides the TID impact and the AFR which are left unchanged, the already implemented countermeasures, i.e., the SL-A. Therefore the re-evaluated risk of an attack path is given by the minimum among the risks of the assets that compose the attack path.

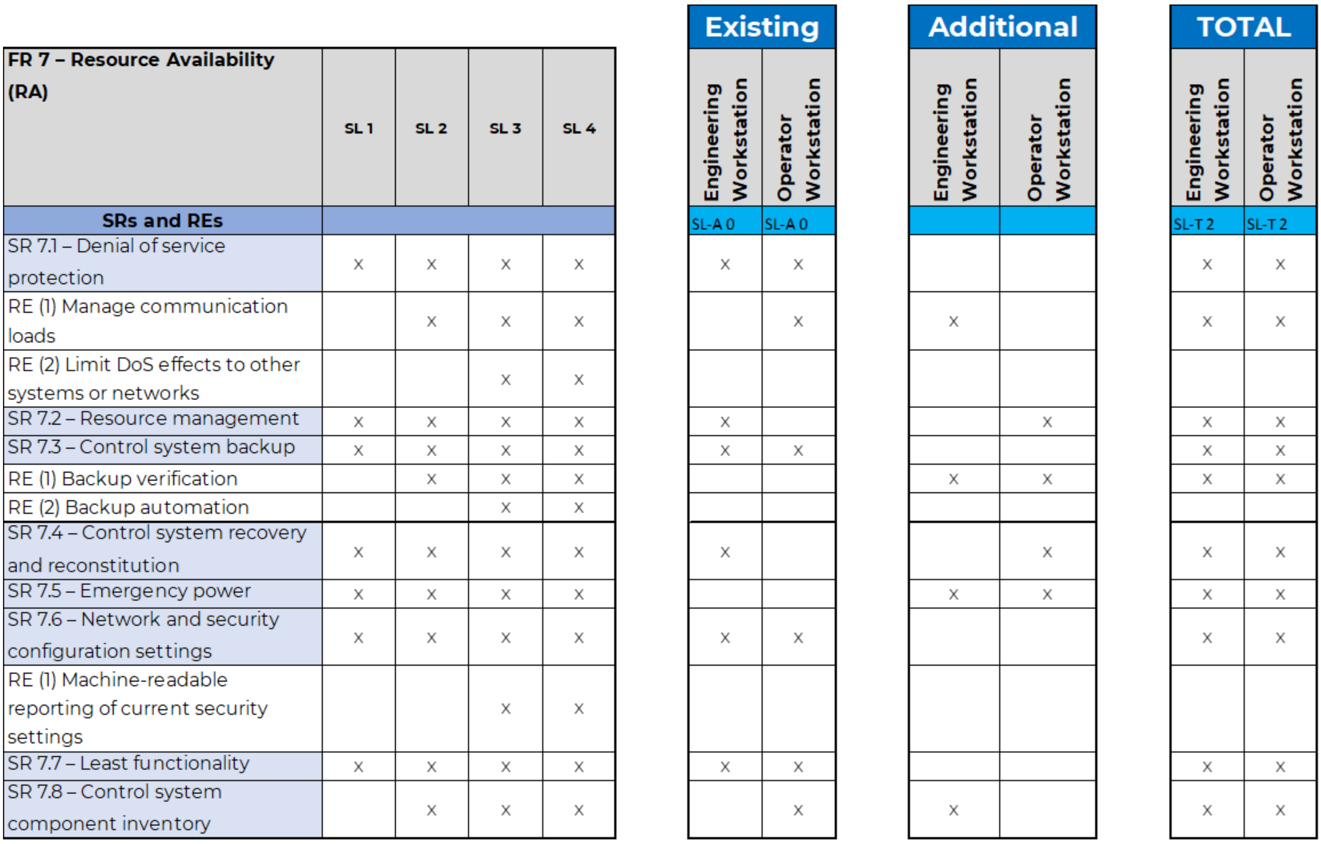
Application to the case study. The risk re-evaluation of the Main Operation Zone 1 is shown in Figure 10. For example, if we consider the Operator Workstation and we focus on the Denial of Service threat category, the combination of the SL-A 0 with the unmitigated risk (Medium) leads to a re-evaluated risk equal to Medium (see the matrix of Figure 11). Deriving again the attack paths for the Main Operation Zone 1 using the re-evaluated risk, the criticality of the attack paths does not change with respect to what is reported in Figure 7, and the re-evaluated risk of the Operator Workstation is still Med-High.

4.11 ZCR 5.11: Compare residual risk with tolerable risk

Guidelines from ISA/IEC 62443. *The 62443-3-2 standard asks for a comparison of the residual risk for each threat (identified in ZCR 5.1) to the organization’s tolerable risk. If the residual risk exceeds the tolerable risk, the organization shall determine if the residual risk will be accepted, transferred, or mitigated based on the organization’s policy.*

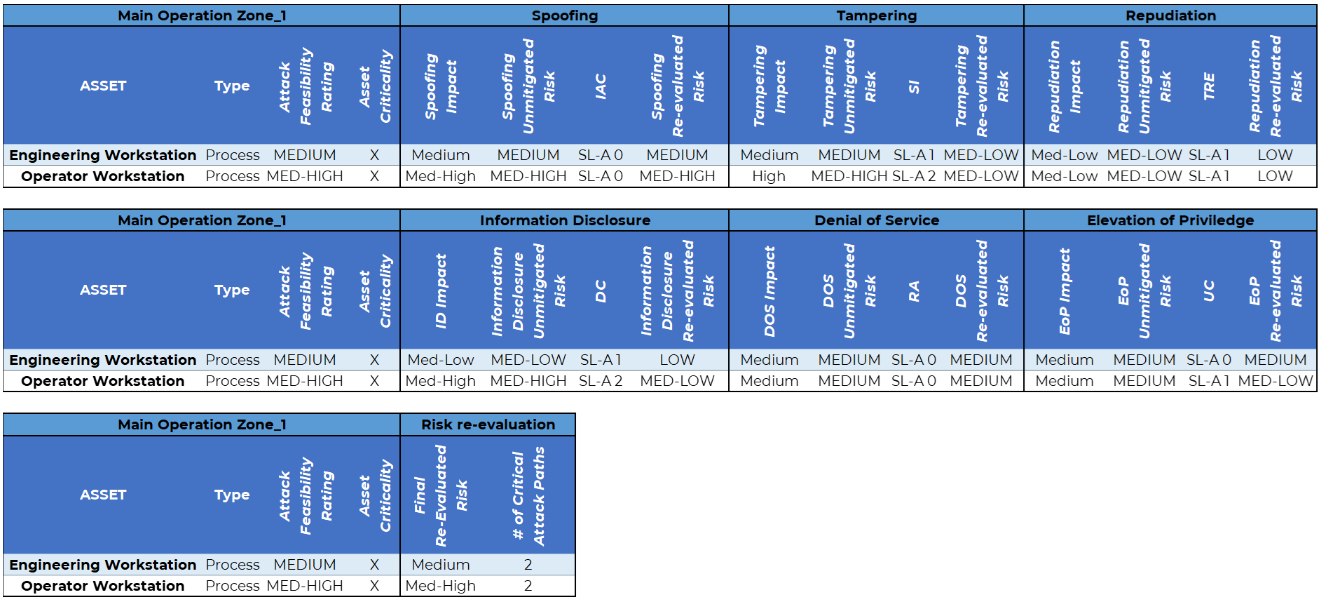
In the methodology, if there are still critical attack paths, i.e., attack paths with re-evaluated risk greater than the tolerable risk. Therefore additional countermeasures must be identified.

Application to the case study. In the Main Operation Zone 1, even after the re-evaluation, there are still four critical attack paths to mitigate.



FR 7 – Resource Availability (RA)					Existing		Additional		TOTAL	
	SL 1	SL 2	SL 3	SL 4	Engineering Workstation	Operator Workstation	Engineering Workstation	Operator Workstation	Engineering Workstation	Operator Workstation
SRs and REs					SL-A 0	SL-A 0			SL-T 2	SL-T 2
SR 7.1 – Denial of service protection	x	x	x	x	x	x			x	x
RE (1) Manage communication loads		x	x	x		x	x		x	x
RE (2) Limit DoS effects to other systems or networks			x	x						
SR 7.2 – Resource management	x	x	x	x	x			x	x	x
SR 7.3 – Control system backup	x	x	x	x	x	x			x	x
RE (1) Backup verification		x	x	x			x	x	x	x
RE (2) Backup automation			x	x						
SR 7.4 – Control system recovery and reconstitution	x	x	x	x	x			x	x	x
SR 7.5 – Emergency power	x	x	x	x			x	x	x	x
SR 7.6 – Network and security configuration settings	x	x	x	x	x	x			x	x
RE (1) Machine-readable reporting of current security settings			x	x						
SR 7.7 – Least functionality	x	x	x	x	x	x			x	x
SR 7.8 – Control system component inventory		x	x	x		x	x		x	x

Fig. 9 Existing and additional countermeasures of the Main Operation Zone 1 for the FR 7 Resource Availability. The left part of the figure is derived from ISA/IEC 62443-3-3 and describes which are the Security Requirements needed in order to achieve a specific SL. The right part is used to mark which are the existing and additional countermeasures identified for the assets of the Main Operation Zone 1.



Main Operation Zone_1				Spoofing				Tampering				Repudiation			
ASSET	Type	Attack Feasibility Rating	Asset Criticality	Spoofing Impact	Spoofing Unmitigated Risk	IAC	Spoofing Re-evaluated Risk	Tampering Impact	Tampering Unmitigated Risk	SI	Tampering Re-evaluated Risk	Repudiation Impact	Repudiation Unmitigated Risk	TRE	Repudiation Re-evaluated Risk
Engineering Workstation	Process	MEDIUM	X	Medium	MEDIUM	SL-A 0	MEDIUM	Medium	MEDIUM	SL-A 1	MED-LOW	Med-Low	MED-LOW	SL-A 1	LOW
Operator Workstation	Process	MED-HIGH	X	Med-High	MED-HIGH	SL-A 0	MED-HIGH	High	MED-HIGH	SL-A 2	MED-LOW	Med-Low	MED-LOW	SL-A 1	LOW

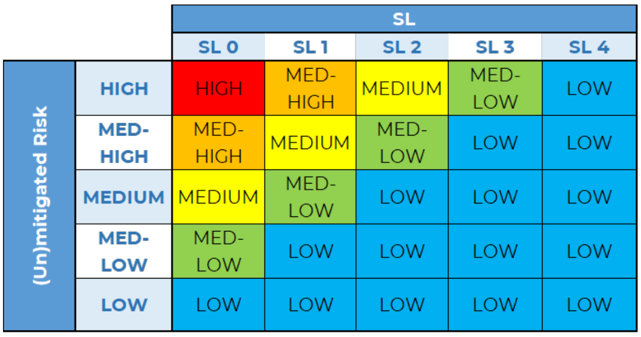
Main Operation Zone_1				Information Disclosure				Denial of Service				Elevation of Priviledge			
ASSET	Type	Attack Feasibility Rating	Asset Criticality	ID Impact	Information Disclosure Unmitigated Risk	DC	Information Disclosure Re-evaluated Risk	DOS Impact	DOS Unmitigated Risk	RA	DOS Re-evaluated Risk	EoP Impact	EoP Unmitigated Risk	UC	EoP Re-evaluated Risk
Engineering Workstation	Process	MEDIUM	X	Med-Low	MED-LOW	SL-A 1	LOW	Medium	MEDIUM	SL-A 0	MEDIUM	Medium	MEDIUM	SL-A 0	MEDIUM
Operator Workstation	Process	MED-HIGH	X	Med-High	MED-HIGH	SL-A 2	MED-LOW	Medium	MEDIUM	SL-A 0	MEDIUM	Medium	MEDIUM	SL-A 1	MED-LOW

Main Operation Zone_1				Risk re-evaluation	
ASSET	Type	Attack Feasibility Rating	Asset Criticality	Final Re-Evaluated Risk	# of Critical Attack Paths
Engineering Workstation	Process	MEDIUM	X	Medium	2
Operator Workstation	Process	MED-HIGH	X	Med-High	2

Fig. 10 Risk re-evaluation of the Main Operation Zone 1 taking into account the existing countermeasures. For each STRIDE threat category (and FR), besides the *impact* and the *unmitigated risk* which are reported from the previous asset evaluation, the SL-A and the *re-evaluated risk* considering the existing countermeasures are specified. The *final re-evaluated risk* and the *number of critical attack paths* after the re-evaluation are reported as well.

ISA/IEC 62443-3-3 Foundational Requirement	CIA-AAA Property	Threat Category
Identification and authentication control (IAC)	Authentication	Spoofing
System integrity (SI)	Integrity	Tampering
Timely response to events (TRE)	Auditing (Accountability)	Repudiation
Data confidentiality (DC)	Confidentiality	Information Disclosure
Resource availability (RA)	Availability	Denial of Service
Use control (UC)	Authorization	Elevation of Privilege
Restricted Data Flow (RDF)	System Segmentation	

Table 2 Mapping between ISA/IEC 62443-3-3 Foundational Requirements, CIA-AAA security properties and STRIDE threat categories. Table adapted from [22].



		SL				
		SL 0	SL 1	SL 2	SL 3	SL 4
(Un)mitigated Risk	HIGH	HIGH	MED-HIGH	MEDIUM	MED-LOW	LOW
	MED-HIGH	MED-HIGH	MEDIUM	MED-LOW	LOW	LOW
	MEDIUM	MEDIUM	MED-LOW	LOW	LOW	LOW
	MED-LOW	MED-LOW	LOW	LOW	LOW	LOW
	LOW	LOW	LOW	LOW	LOW	LOW

Fig. 11 Example of a matrix for the re-evaluation of the risk after the countermeasures' identification, combining (un)mitigated risk and SL.

4.12 ZCR 5.12: Identify additional cybersecurity countermeasures

Guidelines from ISA/IEC 62443. *The standard indicates that additional cybersecurity countermeasures shall be identified to mitigate the intolerable risk related to threats.*

Challenge: how to identify additional countermeasures to lower the risk.

At this step of the methodology, we need to identify additional countermeasures for the attack paths that are still critical. In particular, the additional countermeasures will be implemented over the assets of the attack path which have the minimum risk, that is computed as specified in subsection 4.10. The rationale is that these assets already constitute the hardest obstacles to be passed by a threat agent due to the already implemented countermeasures, and if they will be further protected the attack chain will be more likely cut off. For these assets, and for each threat category, the methodology aims at identifying the minimum set of countermeasures associated with the SL, to have a residual risk equal to the tolerable risk. For doing this it is possible to rely on the matrix shown in Figure 11: starting from the mitigated risk of a given asset, it is possible to derive the SL-T required to achieve the tolerable risk (Low). All the countermeasures associated with the identified SL-T for the specific FR have to be implemented.

Application to the case study. The final risk re-evaluation of the Main Operation Zone 1 taking into account the additional countermeasures to be implemented is shown in Figure 12. Let us again consider the Denial of Service threat category for the Operator Workstation. If we take the risk matrix in Figure 11, and we consider the mitigated risk of the Denial of Service for the Operator Workstation (Medium), we see that the minimum SL-T that allows to achieve the tolerable risk (Low) is SL-T 2 (third row, third column). Hence, to accomplish this we have to implement all the countermeasures that are associated with the FR 7 Resource Availability for the SL-T 2 (see Figure 9).

The same procedure is applied to all the other threat categories (see Figure 12). Note that different SL-T are associated with the threat categories, meaning that the asset owner has to implement countermeasures tailored to the specific threats. Without this approach, the asset owner would have to implement the whole set of countermeasures associated with the SL-T of the zone, which would be SL-T 3 for the Main Operation Zone 1.

Analysing again the attack paths it is possible to observe that there are no more critical paths.

4.13 ZCR 5.13: Document and communicate results

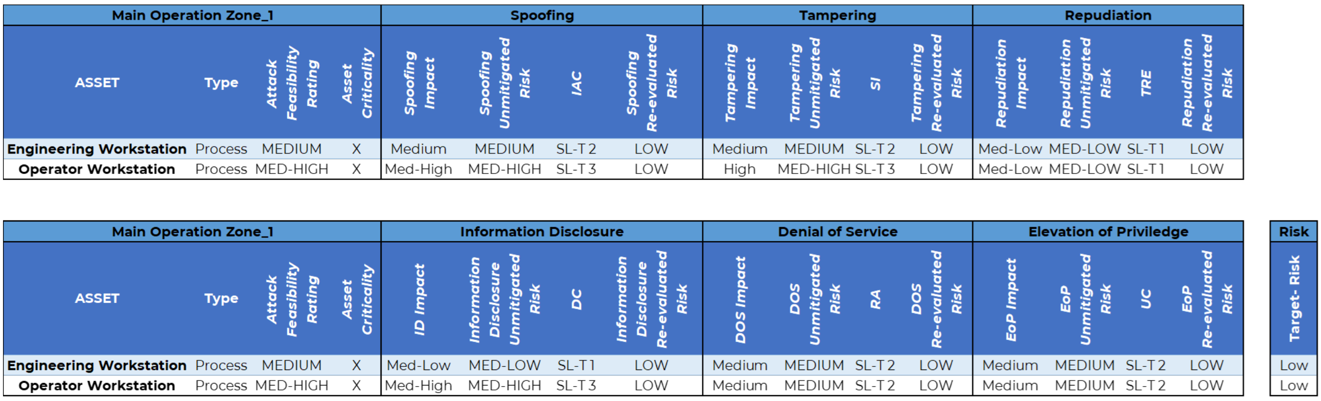
Guidelines from ISA/IEC 62443. *The results of the detailed cyber risk assessment shall be documented, reported, and made available to the organization.*

A technical report is produced, containing all the relevant results of the whole risk assessment process.

5 Related work

ISA/IEC 62443 [17] is a standard that is capturing the interest of industry and research, due to the growth in importance and diffusion of IACS. In the literature, some works propose approaches that deal, even only partially, with risk assessment in compliance with this standard. In the following, we compare such approaches with the methodology proposed in this paper. The results of the comparison are synthetically reported in Table 3). The aspects that we have considered for this comparison are the following:

- The level of coverage of ZCR 5 steps;



Main Operation Zone_1				Spoofing				Tampering				Repudiation			
ASSET	Type	Attack Feasibility Rating	Asset Criticality	Spoofing Impact	Spoofing Unmitigated Risk	IAC	Spoofing Re-evaluated Risk	Tampering Impact	Tampering Unmitigated Risk	SI	Tampering Re-evaluated Risk	Repudiation Impact	Repudiation Unmitigated Risk	TRE	Repudiation Re-evaluated Risk
Engineering Workstation	Process	MEDIUM	X	Medium	MEDIUM	SL-T 2	LOW	Medium	MEDIUM	SL-T 2	LOW	Med-Low	MED-LOW	SL-T 1	LOW
Operator Workstation	Process	MED-HIGH	X	Med-High	MED-HIGH	SL-T 3	LOW	High	MED-HIGH	SL-T 3	LOW	Med-Low	MED-LOW	SL-T 1	LOW

Main Operation Zone_1				Information Disclosure				Denial of Service				Elevation of Priviledge				Risk
ASSET	Type	Attack Feasibility Rating	Asset Criticality	ID Impact	Information Disclosure Unmitigated Risk	DC	Information Disclosure Re-evaluated Risk	DOS Impact	DOS Unmitigated Risk	RA	DOS Re-evaluated Risk	EoP Impact	EoP Unmitigated Risk	UC	EoP Re-evaluated Risk	Target- Risk
Engineering Workstation	Process	MEDIUM	X	Med-Low	MED-LOW	SL-T 1	LOW	Medium	MEDIUM	SL-T 2	LOW	Medium	MEDIUM	SL-T 2	LOW	Low
Operator Workstation	Process	MED-HIGH	X	Med-High	MED-HIGH	SL-T 3	LOW	Medium	MEDIUM	SL-T 2	LOW	Medium	MEDIUM	SL-T 2	LOW	Low

Fig. 12 Risk re-evaluation of the Main Operation Zone 1 taking into account the additional countermeasures to be implemented. For each STRIDE threat category (and FR), besides the *impact* and the *unmitigated risk* which are reported from the previous asset evaluation, the SL-T and the *re-evaluated risk* considering the additional countermeasures are specified. The final *target risk* is reported as well.

- How the complexity of the methodology is managed, i.e., what is the level of control over the number of possible threats/situations to consider in the analysis;
- Identification of tailored countermeasures;
- Level of involvement of the asset owner (or system integrator) in the risk assessment process;
- Development/usage of tools to support the risk assessment (e.g., a newly developed tool or a toolchain of custom and/or commercial tools).

The work in [26] investigates the design process of a security service architecture based on the 62443-2-4 part of the standard. The approach is not directly compliant with ZCR 5, even if a risk assessment activity is mentioned. This part is done through vulnerability scanning tools and CVSS Assessment Handling, to identify the vulnerabilities of each asset and to lower the risk. The detailed analysis of the vulnerabilities could lead to a very complex assessment process. The asset owner is involved during the process, e.g., for installation, maintenance, and operation requirements or to decide on the scanning tool to be used. No supporting tools are mentioned.

The authors of [2] focus on availability property, asserting that it is the most important one for IACS. Following this idea, in the cybersecurity risk assessment process, assets are replaced with functions, and just the availability property is considered. A quantitative metric for availability evaluation is provided. Since the focus of the work is only on the availability property, the ZCR 5 risk assessment is covered in a very partial way. The asset owner is not involved in the approach and no supporting tools are provided.

Some works in the literature aim at automating the risk assessment process through Model Driven Engineering techniques and through approaches based on ontologies [6–8, 20, 23]. In [20] a meta-model is proposed for the partitioning and the representation of zones and conduits of the SUC. A security level is assigned to each data flow between components through an initial cybersecurity risk assessment, which is not described. Then the security level of the zones and conduits is derived according to the relationships defined by the meta-model. The assignment of security levels based on the meta-model is then automatically derived from an architectural description of the SUC. The asset owner is not explicitly involved during the process.

In [8] the authors propose a method for automated risk assessment which consists of the following steps: information collection based on process analysis, information formalization with a semiformal model, information usage applying first-order logic to extract expert knowledge, and information access using a digital twin. Moreover, in [7], they extend the work by relating the SL-T vector of a threat to the skills and resources level of attackers' profiles from the Threat Agent Library (TAL) [3]. The identification of countermeasures for the specific threat is based on those provided by the MITRE ATT&CK, which are then mapped to the IEC 62443-3-3 Security Requirements. However, even if the automated approach can support the process, relying on extensive catalogs like the MITRE ATT&CK can lead to complex analyses. Moreover, in these works the authors do not cover all the steps of ZCR 5, focusing on ZCR 5.1, ZCR 5.2, and ZCR 5.6. Some fundamental steps like the determination of impact and likelihood of threats are not explored. Lastly, the asset owner is only consulted for the approval of the results.

The work in [6] proposes an ontology-based method that automatically identifies sources of security risks and the corresponding attack consequences based on engineering data described in Automation Markup Language (AML), a standardized format widely used in the engineering domain for data exchange. The approach covers some steps of ZCR 5, such as the identification of threats, vulnerabilities, and their consequences and impact. The tool can derive the attack paths that an attacker can follow to exploit an asset. However, no likelihood estimation, SL assignment, and countermeasures identification are considered. The proposed ap-

Work	Coverage of ZCR 5	Management of complexity	Identification of tailored countermeasures	Involvement of the asset owner	Tool support
[26]	None	Low	No	Medium	No
[2]	Low	Low	No	None	No
[20]	None	Medium	No	None	Yes, not specified if open-source
[8], [7]	Medium	Medium	Yes	Low	Yes, open-source
[6]	Medium	Medium	No	None	Yes, open-source
[23]	Medium	Medium	No	Low	Yes, not open-source
[4], [13]	Medium	Medium	Yes	None	No
[15], [16]	High	Medium	Yes	None	No
[10]	Medium	Medium	Yes	None	Yes, not specified if open-source
[12]	Medium	Medium	Yes	None	No
[11]	Medium	Low	Yes	None	Yes, not specified
[25]	High	Low	No	Low	No
This work	High	High	Yes	High	Partial, not open-source

Table 3 Related works: coverage of the proposed key methodological aspects. For the "identification of tailored countermeasures" and "tool support" aspects, "Yes" and "No" values are used, while for all the other aspects the values "None", "Low", "Medium", and "High" are used.

proach consists of a full-fledged automated framework. The asset owner is not taken into account.

In [23], a MDE tool called ResilBlockly was introduced to model the system using some built-in blocks and to conduct a cybersecurity risk assessment. Even if the approach does not directly refer to the steps of ZCR 5, several of them, e.g., threats identification, impact and likelihood estimation, risk determination, and countermeasures identification are partially covered by the modeling framework. However, the tool relies on catalogs like CWE, CVE, and CAPEC for the identification and evaluation of threats, vulnerabilities, and attacks, which may lead to a very complex assessment process. Concerning likelihood estimation, the methodology relies on existing assessment reports, historical data of attacks on similar systems, manufacturer vulnerability reports, and the user's experience. In this way, the asset owner can be somehow involved during the risk assessment process.

Several works make use of HAZOP-like or THROP-like approaches for the identification and evaluation of threats [4, 10, 12, 15, 16]. The work in [4] focuses on the interplay between safety and security, allowing the identification of both hazards and threats using HAZOP and STRIDE, respectively. The authors extend this work in [13], where they first derive the attack sequences related to the identified threats using MITRE ATT&CK. In doing this, they also consider the threat actor with the minimum skills and resources required to perform the attack. Then, they compute the CVSS score associated with the threat, and finally, they derive the SL-T using a CVSS/SL mapping. Even if the steps of ZCR 5 are not explicitly mentioned, the work covers the identification of threats, the determination of consequences and impacts, and the derivation of SL-T. Countermeasures are identified for the specific considered threats. No support tool is provided together with this approach and the asset owner is not directly involved in the process.

The authors of [15] and [16] propose a risk assessment methodology for chemical and process plants. They rely on a database of past incidents in the domain to elicit possible threats, and, taking as input the detailed scheme of the plant, they proceed with an HAZOP-like analysis. In this way, they try to find possible mishaps in the plant (mainly safety hazards) that can be triggered by remote actions. The mishap probability, described as attack credibility, is derived in terms of how much knowledge about the plant the attacker has and of cyber complexity, i.e., the complexity of the attack. Countermeasures are identified among procedural or physical safeguards to specific security events. Several steps of ZCR 5 are covered. The HAZOP-like approach can be used to conduct a guided analysis. However, the works mainly focus on physical interactions between components, without considering IT components. Also, they do not provide any support tool, and collaboration with the asset owner is not considered.

In [10], an approach is proposed that uses HAZOP combined with bow-tie analysis, for the identification and visualization of threats and barriers, i.e., countermeasures against specific threats. The risk is determined in terms of the overall number of threats and their likelihood, barriers and their effectiveness, consequence and their severity. Even if the approach does not explicitly mention the ZCR 5, the identification of threats, the determination of consequences and impact, and the identification of countermeasures (or barriers) are taken into account. The likelihood of threats is also considered. The combination of HAZOP and bow-tie analysis can help in reducing the complexity of the problem. The work makes use of a tool for the creation of the bow-tie diagram. The asset owner is not involved in the process.

The authors of [12] transform existing HAZOP risk analysis into cybersecurity risk analysis, called cyber-HAZOP. The steps of ZCR 5 are not explicitly covered, but the consequences/impact (severity) and likelihood of threats are derived and the identification of countermeasures (mainly recommendations) to specific threats is elicited during the process. However, how severity and likelihood are associated with threats is not specified. No support tool is provided by the approach nor direct involvement of the asset owner is present.

In [11], a risk assessment approach based on penetration testing is proposed. The likelihood of the identified threats is determined by the occurrence of such threats during the penetration testing campaign, while the impact is assigned according to the consequences on confidentiality, integrity, and availability. Very low-level countermeasures are proposed to cover the threats identified during the process. We believe that a penetration testing activity instead of being part of the risk assessment process could be an input to it, e.g., for the identification of vulnerabilities during ZCR 5.2. During this process, the asset owner is not involved. Classic penetration testing tools are used during this activity.

The authors of [25] focus on the application of 62443 in the Unmanned Offshore Facilities domain. They provide some pointers which cover all the steps of the 62443-3-2, including ZCR 5, and which could be used to address some open points of the standard but lack details on how to practically apply them. For the identification of threats, they suggest relying on institutionalized threat intelligence sources, e.g., MITRE ATT&CK. The asset owner is considered only at the beginning of the process and for the final approval. No support tool is proposed by the work.

Summing up, as reported in Table 3, the great majority of the works do not cover all the steps of ZCR 5, focusing mainly on the identification of threats. Concerning the management of the complexity of the risk assessment process, the usage of automated approaches or HAZOP-like or THROP-like analyses can reduce the time and effort spent on this activity. However, the usage of broad standardized lists of attacks, e.g. MITRE ATT&CK, can lead to a rapid increase of the number of cases to be considered. Several works propose ways to identify countermeasures, but they are mainly i) in the form of generic recommendations, or ii) tailored for very specific threats, which again can lead to more complex analyses. In the analyzed works the asset owner is typically involved only at the beginning of the process and for the approval of the results. Finally, some works provide support tools within the methodologies, especially those proposing automated or semi-automated approaches.

In literature, there are other works on cybersecurity risk assessment that are not specific to IACS and do not take into account the ISA/IEC 62443, but take into account CPS in general and address some topics related to our methodology, such as attack path analysis, residual risk estimation and optimal control selection.

Regarding attack path analysis, the authors of [18] present a method for identifying and analyzing attack paths in interconnected CPSs. This method takes into account the criticality of each sub-system in the path discovery process, as well as the risk each path poses to the overall system, in order to analyze and prioritize the attack paths. Then, [1] presents a generic graph-based vulnerability and risk assessment attack tree approach to detect threats in an IoT network. The attack paths are identified using the Depth First Search (DFS) algorithm.

The paper in [21] introduces a residual cybersecurity risk management framework aligned with the ISO/SAE 21434 standard for road vehicles. This approach audits the implemented defenses along the identified attack paths for the corresponding threats and system components. Flow networks are employed to calculate both the mitigated risk and the remaining residual risk of the threat, considering the selected countermeasures.

In [19] a method for analyzing risk propagation and aggregation in complex CPSs is proposed, utilizing the results of risk assessments of their individual components. Additionally, a method is proposed employing evolutionary programming to automate the selection of an optimal set of cybersecurity controls from a list of available options, with the aim of minimizing residual risk and the cost associated with implementing these measures.

6 Limitations

As discussed along this paper, the proposed methodology brings several beneficial aspects in implementing the risk assessment process for IACS, and it has distinguishing characteristics compared with the with related works available in the literature. In this section we will discuss the current limitations of the proposed methodology and some ongoing research directions.

Specification of threats. To reduce the complexity of the analysis, in our methodology we reason at a high abstraction level in terms of threat categories, instead of considering single threats. However, for an asset owner/system integrator, it might be important to investigate some specific threats strictly related to the considered system or application domain. In this case the determination of the risk should be tailored to these specific threats, for example using well-established threat ontologies like MITRE ATT&CK) as done in some works that we have identified in the literature (e.g., [7, 13]). We are currently working on adapting the proposed methodology for treating specific threats along the process besides the more general threat categories, and in particular when evaluating consequences/impact, likelihood and risk. The identification of the countermeasures could be specialized as well to the specific threat, still considering the mapping between known mitigations and the FR (as proposed in [7]).

Unapplicability of countermeasures. In our approach we derive the countermeasures from the FR of 62443-3-3 to address specific threat categories over specific assets. In some cases the particular countermeasure suggested by the standard could not be applicable to a specific asset considering its nature, its development process, its functionalities. In this case other specific countermeasures have to be identified to achieve the required SL-T. We believe that this problem cannot be solved on a methodological level, but requires security experts to identify specific security countermeasures to implement on a case-by-case basis.

Restricted Data Flow FR. The mapping between the STRIDE threat categories and the 62443-3-3 FR does not include the FR of type Restricted Data Flow, which seems to partially impair the applicability of the approach. Actually, this specific FR concerns network segmentation and zone boundary protection, so it has to be considered in the conduits analysis and not in the analysis of the zones.

Insider adversaries. Regarding the attack path generation, when analyzing a specific zone we generate only attack paths which start from external entities, i.e., assets which are outside the boundaries of the analyzed zone. With this limitation we are not considering the possible attack paths that may start from an assets within the analyzed zone. We are currently working to relax this assumption in the attack path generation phase, which will allow to generate attack paths starting from outside and inside the zone's boundaries.

Support framework. The methodology relies on a chain of tools: Draw.io is used for the creation of DFDs; Python scripts are employed for the derivation of attack paths; spreadsheets are adopted throughout the whole process to support the gathering of information, the representation of matrices and the information management and analysis. Even if the tools are integrated in the process, the development of an ad hoc tool would facilitate the applicability of the methodology.

7 Conclusions

In this paper, we presented a methodology for the detailed cybersecurity risk assessment of IACS, in compliance with the ISA/IEC 62443-3-2 standard. The approach has been built, applied, and refined on several interactions with companies and IACS owners. The methodology manages the complexity of the assessment process using a THROP analysis based on STRIDE threat categories. Moreover, the methodology fosters the assignment of a SL-T not only to the zones of the SUC but also to each asset that is contained within a zone. Hence, it is possible to identify tailored countermeasures for the specific assets that are contained in a zone, rather than applying all the security requirements that would be needed to achieve the SL-T of the zone. This is done relying on the generation and analysis of attack paths and on the FRs provided by the 62443-3-3 part of the standard. To the best of our knowledge, this is the first risk assessment methodology integrating these distinguishing elements, and capable of meeting the basic corporate needs from an industrial point of view. As future work we plan to investigate and possibly address the limitations that we have stated in section 6.

Statements and Declarations

Funding: This work was partially supported by the project IES Factory 2014/2020 EU FESR POR Puglia, by the project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union — NextGenerationEU, and by the European Union under NextGenerationEU PRIN 2022 (Prot. n. 202297YF75).

Competing interests: The authors declare they have no financial interests.

References

1. Arat, F., Akleylek, S.: Attack path detection for iiot enabled cyber physical systems: Revisited. Computers & Security **128**, 103,174 (2023). DOI https://doi.org/10.1016/j.cose.2023.103174
2. Baybulatov, A., Promyslov, G.: A metric for the iacs availability risk assessment. In: Proceedings - 2022 International Russian Automation Conference, RusAutoCon 2022, p. 750 – 754 (2022). DOI 10.1109/RusAutoCon54946.2022.9896250
3. Casey, T.: Threat Agent Library helps identify information security risks. Intel White Paper (2007). DOI 10.13140/RG.2.2.30094.46406
4. Denzler, P., Hollerer, S., Frühwirth, T., Kastner, W.: Identification of security threats, safety hazards, and interdependencies in industrial edge computing. In: 2021 IEEE/ACM Symposium on Edge Computing (SEC), pp. 397–402 (2021). DOI 10.1145/3453142.3493508
5. Djebbar, F., Nordstrom, K.: A comparative analysis of industrial cybersecurity standards. IEEE Access **11**, 85,315 – 85,332 (2023). DOI 10.1109/ACCESS.2023.3303205
6. Eckhart, M., Ekelhart, A., Weippl, E.: Automated security risk identification using automationml-based engineering data. IEEE Transactions on Dependable and Secure Computing **19**(3), 1655 – 1672 (2022). DOI 10.1109/TDSC.2020.3033150
7. Ehrlich, M., Broring, A., Diedrich, C., Jasperneite, J., Kastner, W., Trsek, H.: Determining the target security level for automated security risk assessments. In: IEEE International Conference on Industrial Informat-

ics (INDIN), vol. 2023-July (2023). DOI 10.1109/INDIN51400.2023.10217902

8. Ehrlich, M., Bröring, A., Diedrich, C., Jasperneite, J.: Towards automated risk assessments for modular manufacturing systems process analysis and information model proposal. At-Automatisierungstechnik **71**(6), 453 – 466 (2023). DOI 10.1515/auto-2022-0098
9. European Committee for Electrotechnical Standardization (CENELEC): CENELEC CLC/TS 50701, railway applications – cybersecurity (2021)
10. Geddes, A., Hatch, D.: Chase - visualising cyber security vulnerabilities and risk. In: Institution of Chemical Engineers Symposium Series, vol. 166 (2019)
11. Hassani, H.L., Bahnasse, A., Martin, E., Roland, C., Bouattane, O., Mehdi Diouri, M.E.: Vulnerability and security risk assessment in a iiot environment in compliance with standard iec 62443. In: Procedia Computer Science, vol. 191, p. 33 – 40 (2021). DOI 10.1016/j.procs.2021.07.008
12. Heluany, J.B., Galvão, R.: Iec 62443 standard for hydro power plants. Energies **16**(3) (2023). DOI 10.3390/en16031452
13. Hollerer, S., Sauter, T., Kastner, W.: Risk assessments considering safety, security, and their interdependencies in ot environments. In: ACM International Conference Proceeding Series (2022). DOI 10.1145/3538969.3543814
14. Howard, M., Lipner, S.: The Security Development Lifecycle. Microsoft Press, USA (2006)
15. Iaiani, M., Tugnoli, A., Cozzani, V.: Risk identification for cyber-attacks to the control system in chemical and process plants. Chemical Engineering Transactions **90**, 409 – 414 (2022). DOI 10.3303/CET2290069
16. Iaiani, M., Tugnoli, A., Cozzani, V.: Identification of cyber-risks for the control and safety instrumented systems: a synergic framework for the process industry. Process Safety and Environmental Protection **172**, 69 – 82 (2023). DOI 10.1016/j.psep.2023.01.078
17. International Standards on Auditing (ISA), International Electrotechnical Commission (IEC): ISA/IEC 62443, security for industrial automation and control systems (2020)
18. Kavallieratos, G., Katsikas, S.: Attack path analysis for cyber physical systems. In: S. Katsikas, F. Cuppens, N. Cuppens, C. Lambrinoudakis, C. Kalloniatis, J. Mylopoulos, A. Antón, S. Gritzalis, W. Meng, S. Furnell (eds.) Computer Security, pp. 19–33. Springer International Publishing, Cham (2020)
19. Kavallieratos, G., Spathoulas, G., Katsikas, S.: Cyber risk propagation and optimal selection of cybersecurity controls for complex cyberphysical systems. Sensors **21**(5) (2021). DOI 10.3390/s21051691
20. Kern, M., Taspolatoglu, E., Scheytt, F., Glock, T., Liu, B., Betancourt, V.P., Becker, J., Sax, E.: An architecture-based modeling approach using data flows for zone concepts in industry 4.0. In: ISSE 2020 - 6th IEEE International Symposium on Systems Engineering, Proceedings (2020). DOI 10.1109/ISSE49799.2020.9272013
21. Khan, A., Bryans, J., Sabaliauskaite, G.: Framework for calculating residual cybersecurity risk of threats to road vehicles in alignment with iso/sae 21434. In: J. Zhou, S. Adepu, C. Alcaraz, L. Batina, E. Casalicchio, S. Chattopadhyay, C. Jin, J. Lin, E. Losiouk, S. Majumdar, W. Meng, S. Picek, J. Shao, C. Su, C. Wang, Y. Zhauniarovich, S. Zonouz (eds.) Applied Cryptography and Network Security Workshops, pp. 235–247. Springer International Publishing, Cham (2022)
22. Matta, G., Chlup, S., Shaaban, A.M., Schmittner, C., Pinzenöhler, A., Szalai, E., Tauber, M.: Risk management and standard compliance for cyber-physical systems of systems. Infocommunications Journal **13**(2), 32 – 39 (2021). DOI 10.36244/ICJ.2021.2.5
23. Schiavone, E., Nostro, N., Brancati, F.: A mde tool for security risk assessment of enterprises. In: Anais Estendidos do X Latin-American Symposium on Dependable Computing, pp. 5–7. SBC, Porto Alegre, RS, Brasil (2021). DOI 10.5753/ladc.2021.18530
24. Schmidt, D.: Guest editor's introduction: Model-driven engineering. Computer **39**(2), 25–31 (2006). DOI 10.1109/MC.2006.58
25. Teglasy, B.Z., Katsikas, S., Lundteigen, M.A.: Standardized cyber security risk assessment for unmanned offshore facilities. In: Proceedings - 3rd International Workshop on Engineering and Cybersecurity of Critical Systems, EnCyCriS 2022, p. 33 – 40 (2022). DOI 10.1145/3524489.3527302
26. Wang, J.H., Huang, C.Y., Chou, H.Y., Wang, C.Y., Kuo, H.J., Ting, V.: Security service architecture design based on iec 62443 standard. In: 2023 IEEE 3rd International Conference on Electronic Communications, Internet of Things and Big Data, ICEIB 2023, p. 483 – 486 (2023). DOI 10.1109/ICEIB57887.2023.10169989
27. Williams, T.J.: The purdue enterprise reference architecture. Computers in Industry **24**(2), 141–158 (1994). DOI https://doi.org/10.1016/0166-3615(94)90017-5