IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 8 July 2023, accepted 28 July 2023, date of publication 7 August 2023, date of current version 16 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3303205

RESEARCH ARTICLE

A Comparative Analysis of Industrial Cybersecurity Standards

FATIHA DJEBBAR[1], (Member, IEEE), AND KIM NORDSTRÖM[2]
[1]Department of Engineering Science, Högskolan Väst, 46153 Trollhättan, Sweden
[2]Cybersecurity Product Compliance Group, 10392 Stockholm, Sweden
Corresponding author: Fatiha Djebbar (fatiha.djebbar@hv.se)

ABSTRACT Cybersecurity standards provide a structured approach to manage and assess cybersecurity risks. They are the primary source for security requirements and controls used by organizations to reduce the likelihood and the impact of cybersecurity attacks. However, the large number of available cybersecurity standards and frameworks make the selection of the right security standards for a specific system challenging. The absence of a comprehensive comparison overlap across these standards further increases the difficulty of the selection process. In situations where new business needs dictate to comply or implement additional security standard, there may be a risk of duplicating existing security requirements and controls between the standards resulting in unnecessary added cost and workload. To optimize the performance and cost benefits of compliance efforts to standards, it is important to analyze cybersecurity standards and identify the overlapping security controls and requirements. In this work, we conduct a comparative study to identify possible overlaps and discrepancies between three security standards: ETSI EN 303 645 v2.1.1 for consumer devices connected to the internet, ISA/IEC 62443-3-3:2019 for industrial automation and control systems, and ISO/IEC 27001:2022 for information security management systems. The standards were carefully chosen for their broad adoption and acceptance by the international community. We intentionally selected standards with different areas of focus to illustrate the significant overlaps that can exist despite being designed for different environments. Our objective is to help organizations select the most suitable security controls for their specific needs and to simplify and clarify the compliance process. Our findings show a significant overlap among the three selected standards. This information can help organizations gain a comprehensive understanding of common security requirements and controls, enabling them to streamline their compliance efforts by eliminating duplicated work especially when meeting the requirements of multiple standards.

INDEX TERMS Cybersecurity, security controls, security standards, cybersecurity concepts, threats, security requirements.

I. INTRODUCTION

Embracing emerging technologies have resulted in remarquable added capabilities, values and experiences. However, these new technologies have been consistent target of diverse threat actors, each driven by different motivations and capabilities [1]. To fully benefit from the competitive advantage of these technologies, cybersecurity is currently a top priority and a major theme in industrial sectors and consumers market. Statistics showed that in 93% of cases, an external attacker can breach an organization's network perimeter and gain access to local network resources [2]. Cybersecurity standards and frameworks provide guidelines and best practices for organizations to follow to enhance their overall security posture. Implementing cybersecurity frameworks also helps businesses to comply with relevant regulations and laws [3]. The chair of multiple committees in the recognized European Telecommunications Standards Institute (ETSI), affirms that ''Cybersecurity standards are critical to the collective effort to prevent attacks in the first place and reduce the

The associate editor coordinating the review of this manuscript and approving it for publication was Agostino Forestiero.

effectiveness of successful incursions'' [4]. Therefore, various standard organizations have taken a proactive approach to develop, best practices, guidelines, and other resources to assist organizations in securing their data and systems. This has led to broad collaboration on the creation and implementation of cybersecurity standards among organizations such as: the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the International Society of Automation (ISA), ETSI, the International Telecommunication Union - Telecommunication (ITU-T), European Union Agency for Network and Information Security (ENISA). Furthermore, there have been recent updates and releases of several regulations. The EU Cybersecurity Act (CSA) was enacted on April 17, 2019 (Regulation (EU) 2019/881) [5] to strengthen the mandate of the EU cybersecurity. This act granted ENISA a permanent mandate to address cybersecurity threats and establish an EU-wide cybersecurity certification framework to enhance the security of connected products, Internet of Things (IoT) devices as well as critical infrastructure through such certificates. This framework incorporates security features in the initial stages of their technical design and development. The EU Network and Information Security (NIS) directive was adopted in 2016 (EU 2016/1148) [6] and was the first piece of EU-wide cybersecurity legislation. The updated NIS 2 Directive [7] include improved cybersecurity risk management and new reporting obligations across sectors such as digital infrastructure. The scope of the Radio Equipment Directive (RED) 2014/53/EU [8] has been updated in February 2022 to include cybersecurity requirements for radio products which will become mandatory in August 2024 through a Delegated Act on Internet-connected radio equipment. The General Data Protection Regulation (GDPR) [9] was entered into force in May 2018 and established security requirements for data protection to safeguard EU citizens. Other regulation proposals, such as the Artificial Intelligence Act, the Data Act, and the Cybersecurity Resilience Act, aim to address risks and establish rules regarding the use of data generated by connected products, protecting consumers and businesses who use digital components in products or software. Various industrial sectors, such as road vehicles, industrial automation and control systems, information security management systems, and consumer devices connected to the Internet, have shown significant activity in developing standards that specifically address their specific security needs. Notable examples include cybersecurity standards like ISO/SAE 21434 [10], ETSI EN 303 645 [11], ISA/IEC 62443 [12], and ISO/IEC 27001 [13]. These standards and regulations promote the development and implementation of security requirements to ensure the protection of organizations, critical infrastructures, and consumers' products.

Disconcerted by the substantial number of cybersecurity standards, this study aims at identifying and reviewing commonly adopted cybersecurity standards. The goal is to understand their security control objectives to uncover overlapping requirements, and contradictions. The results of this study can assist organizations, cybersecurity professionals, academics, and researchers in understanding the current state of the art and in selecting the best standards for their needs, balancing performance and cost-effectiveness. Furthermore, the objective of this study is to identify any existing gaps within the selected standards and address challenges arising from overlapping requirements and controls, irrespective of their specific application context. As a contribution, this paper aims to fulfil the following objectives:

1) To conduct a comprehensive review of commonly adopted cybersecurity standards, and present a literature review on the current state of the art.
2) To identify prevalent domain-specific cybersecurity standards that form a strong basis to mitigate cybersecurity threats.
3) To identify the overlap and gaps in security requirements and controls between the studied standards with the aim of avoiding redundant efforts when complying with multiple standards.
4) To identify and discuss the challenges related to the creation and compliance to multiple security standards.

As for the remaining part of the paper, section II presents an overview and motivation for this study while the background and existing research work are presented in section III. Section IV provides a formal classification for security standards and section V explains the research methodology used in this study followed by section VI which presents reviews on the analyzed standards and the mapping outcomes. Section VII discusses the findings, while section VIII highlights the challenges associated to the implementation of these standards. Finally, section IX concludes the paper and proposes future research work.

II. OVERVIEWS AND MOTIVATION

The rapid pace adoption of digital technology is leading to the creation of new business models and market opportunities. As the volume of interconnected products and services rises, the importance of cybersecurity also grows in tandem with the expanding digitization and connectivity [9], [14], [15], [16]. To effectively combat the growing risk of cybercrime, it is essential to integrate systematic and well-structured cybersecurity measures into a comprehensive strategy that encompasses individuals, processes, and technology. This entails, in part, adopting appropriate standards and frameworks to ensure a robust defense against cyber threats. ISO defines a standard as ''a document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context'' [18]. Standards have special significance in the domain of cybersecurity addressing confidentiality, integrity, and availability of data [19]. They are collections of best practices created by experts to protect organizations from cyber threats and help improve their cybersecurity posture by protecting their most valuable assets at an effective spending. These

best practices emphasize the importance of implementing a comprehensive security program that includes a range of controls to protect organizational assets. These security controls are generally organized into five categories: Identify-Detect-Respond-Protect-Recover (IDRPR) [20], [21]. By organizing security controls into these categories, organizations can better understand the specific areas they need to focus on to build a robust security program. The approach allows organizations to effectively and efficiently manage specific cybersecurity risks to data and systems.

There exists a large number of security standards. For instance, ISO/IEC 27000 series alone encompasses over 60 standards that address a broad spectrum of information security concerns. This proliferation and diversification in security standards can be confusing, and in most of the cases complex to cybersecurity practitioners and organizations. The requirements for cybersecurity are distributed across numerous standards, resulting in a fragmentation issue. This can lead to the implementation of redundant or conflicting security controls when an organization must comply with multiple standards.

This work is driven by the belief that proper alignment of security controls with an organization's business needs, goals, and objectives is crucial for ensuring the effective security of their endpoint devices, data, networks, and critical infrastructure. Although standards are the primary structured source for security controls and requirements that protect organizations and systems from cyber threats, other sources of protection also exist, such as frameworks, guidelines, and legislation. Table 1 provides definitions, examples, authoritative level and scope for these additional sources of protection.

While it is very important for organizations to implement a cybersecurity standard to safeguard their valuable assets and digital space, so is the selection of the appropriate set of security controls to be implemented. In some business areas such as e-commerce, it is obligatory to comply with governmental or commercial regulatory standards. In other areas, standards adoption is voluntary or may be required in the near future. In the case where there is a need to comply with more than one standard, it can be confusing, time consuming and financially overwhelming if these standards are in part overlapping. This situation can occur especially when a new environment is added to the organization. For example, a manufacturing organization is expanding to include e-commerce. Initially, this organization had to comply with ISA/IEC 62443 [12] for example and it will need also to comply with the Payment Card Industry Data Security Standard (PCI-DSS) [22], which encompasses a set of security standards applicable to any organization handling payment card information to maintain the security and trustworthiness of the payment card industry. Even though these standards may differ based on their scope, they may include in part, similar security controls objectives. Identifying these security controls will help organizations remove overlapping controls and streamline their cyber defence mechanisms. Thus, simplifying the process of compliance and reducing the implementation time and cost for of the whole standards. Additionally, contradictory security controls objectives in standards are equally important to identify to avoid inconsistent security enforcement. An analysis of commonly adopted security standards is therefor imposed in order to expose forms of similarities and possible contradictions in security standards. This study also identifies and discusses open issues and challenges based on a mapping process to selected standards. Discussing and evaluating individual standards is outside the scope of this study, however, future research may consider individual discussions and evaluations of specific standards identified as well.

III. BACKGROUND AND RELATED WORK

A. BACKGROUND

A key responsibility of cybersecurity is to ensure the confidentiality, integrity, and availability of data and systems [23]. This can be achieved, in part, by implementing a suitable set of controls, policies, processes as well as organizational structures that support a systematic mitigation of cyber risks. Cybersecurity will continue to pose a significant challenge in the years ahead. The implementation of best practices in organizations is greatly supported by the use of standards [24]. These documents serve as a set of regulations that specify how organizations should carry out their operations and processes. Security standards are often embraced because they are proved to be effective in providing well-structured security requirements and controls. They provide a multitude of benefits that justify the time and financial resources required to produce and apply them. A raising number of manufacturers and vendors are using these standards in order to produce and sell standards-compliant products and services. Governments and businesses increasingly mandate the implementation of security standards as well. According to a recent survey conducted by Gartner, Inc. [25], 75% of organizations are actively seeking security vendor consolidation in 2022, which marks a significant increase from 29% in 2020. The requirement for secure integration and compatibility of ICT systems using technical standards is increasingly necessary. This is especially relevant in open markets where individuals have the ability to combine equipment and services from various providers, resulting in cost-saving benefits for organizations. The rapid growth of IoT devices, cyber-physical systems, and algorithm-controlled embedded systems like autonomous vehicles and digital twins is also contributing to this need [10]. Cloud computing relies heavily on standardization of hardware, software, and the services they run to ensure interoperability [26]. However, as cloud computing expands, connected systems will be exposed to new and evolving cybersecurity threats. In response, a growing number of organizations are participating and contributing to the development of cybersecurity standards. This has resulted in a significant increase in the number of standards. This trend is expected to continue, necessitating the development of new standards in the future.

TABLE 1. External Security Requirements and Control Sources.

Source	Objective	Selected sources	Owner	Focus area
Standard	Insights into security controls recommendations meant to establish Minimum Security Requirements (MSR) that ensure systems, applications and processes are designed and operated to include appropriate cybersecurity and privacy protections.	ISO/IEC 27001:2022 [13]	ISO and IEC	Addresses cybersecurity requirements.
		ISO/IEC 27002:2022 [27]	ISO and IEC	Addresses cybersecurity controls.
		ISA/IEC 62443-3-3:2019 [28]	ISA and IEC	Addresses Network and system security for Industrial Automation and Control Systems.
		PCI-DSS- The Payment Card Industry Data Security Standard [22]	PCI Security Standards Council – USA	Focus on protecting consumer financial information when stored electronically.
		ISO/SAE 21434 [10]	ISO and the Society of Automotive Engineers (SAE)	focuses on the cybersecurity risks inherent in the design and development of car electronics.
		ETSI EN 303 645 [11]	ETSI	Focus on security and data protection provisions for consumer IoT devices.
Framework	Security best practices, methods, and guidelines that organizations can embrace to get the best results for implementing a successful program.	NIST 800-37 [29]	National Institute of Standards and Technology (NIST) – USA	Provides guidelines for applying the (Risk Management Framework) RMF to information systems and organizations.
		ISO/IEC 29100 [30]	ISO and IEC	Provides high-level framework for protection of personally identifiable information within information and communication technology systems.
		COBIT- Control Objectives for Information Technology	The Information Systems Audit and Control Association (ISACA) [31].	focuses on IT security, governance, and management in organizations that want to improve product quality and, at the same time, adhere to enhanced security best practices.
		CMMC- Cybersecurity Maturity Model Certification [32]	Department of Defense (DoD)-USA	Focus on normalizing and standardizing cybersecurity preparedness across the federal governments defense industrial base (DIB).
		TARA: Threat Assessment and Remediation Analysis [33]	Jackson E. Wym. The MITTRE Corporation	Identifying and assessing cyber vulnerabilities and selecting effective countermeasures to mitigate them.
Guideline	Recommended practices that are based on industry-recognized secure practices. They lack the level of consensus and formality associated with standards.	IoT code of practice [34]	Australian Cybersecurity Center	Provides code of Practice for IoT Security for manufacturers, with guidance for consumers on smart devices at home.
		OWASP- Open Web Application Security Project [35].	Open Web Application Security Project Foundation	Focus on web security, application security and vulnerability assessment.
		NIST 800-53 [36]	NIST	Focus on security and privacy controls for information systems and organizations.
		VDI/VDE. 2182 [37]	VDI/VDE- VDI (The Association of German Engineers)	Identifying and assessing cyber vulnerabilities and selecting effective describes how specific measures can be implemented to guarantee the IT security of automated machines and plant.
Legislation	These are the highest levels of documentation in relation to cybersecurity from which other documents are created. It can incorporate security controls and standards. It is mandated by a government body, and required by law, to be complied with.	GDPR [9]	European Parliament and Council of the European Union (EU)	Focus on data protection and privacy in the European Economic Area.
		HIPAA- Health Insurance Portability and Accountability act [14]	Department of Health and Human Services (HSS)- USA.	Focus on the security and privacy of sensitive health information.
		UNECE WP29 [38]	Inland Transport Committee (ITC) of the United Nations Economic Commission for Europe (UNECE).	Focus on protecting road vehicles and road users from cybersecurity threats.
		NIS2 EU directive [7]	European Parliament and Council of the EU.	Focus on improving Member State cybersecurity capabilities, developing cybersecurity risk management in the internal market and encouraging information sharing.
		RED 2014/53/EU [8]	European Parliament and Council of the EU.	Focus on establishing a regulatory framework for radio equipment, setting essential requirements for safety and health, electromagnetic compatibility (EMC) and radio spectrum efficiency.
		Cybersecurity act [5]	European Parliament and Council of the EU.	Aims to achieve a high level of cybersecurity, cyber resilience, and trust in the EU.
		New Zealand privacy act [39]	New Zealand	Promotes and protect individual privacy.

B. RELATED WORK

In this section, we present a survey of various research works on cybersecurity standards. These studies generally emphasize the scope of applicability of different standards, the challenges, and the evolution of the taxonomy of the field. The authors in [16] report the results of a questionnaire among industry sectors and found two standards that are most applied in industry: ISO/IEC 27000-series, and the Common Criteria ISO/IEC 15408 for Information security, cybersecurity and privacy protection [17]. They also

provide a valuable table of standards that are used for specific sectors of industry. While they provide survey results of commonly used standards, they do not contrast or compare these standards. The work presented in [15] surveyed and compared commonly used standards for creating secure software applications. The authors suggest that many standards might not cover all the security requirements for secure software development when used individually. Instead, a process for creating secure software relies on implementing more than one standard, particularly to comply with regulations or obtain certification for a secure software application. Authors in [40] reviewed the development of design notations, models, and languages that can be applied to describing the IoT security and privacy requirements. The authors also discussed possible risk assessment methods and how they can be incorporated in the IoT applications and systems. The authors explained why it is important to integrate privacy in the early stage of system development. Their study shows that while most of the research articles analyze security in some way, they seldom investigate data privacy. In this survey, the authors emphasized the potential challenges and opportunities for proactive design tools that support IoT privacy. Moreover, the authors identified six research challenges related to privacy in IoT systems and their implications for the IoT research community about how to address these challenges. In [41], the authors analyzed multiple authoritative cybersecurity standards, manuals, handbooks, and literary works to present the unanimous meaning and construct of the term cyber threat. The author's work reveals that although cyber threat definitions are mostly consistent, most of them lack the inclusion of disinformation in their list/glossary of cyber threats. Hence, they conducted an in-depth comparative analysis of disinformation and its similar nature and characteristics with the prevailing and existing cyber threats. They, therefore, argue for its recommendation as an official and actual cyber threat. The authors recommend a taxonomy correction and hope that it influences future policies and regulations in combating disinformation and its propaganda In [42], the authors reviewed some of the most common industrial security standards. In total, they reviewed five standards: ISA/IEC 62443, ISO/IEC 27000 series, ISO/IEC 15408, VDI/VDE 2182, and NIST SP 800-82. It has been concluded that standards are not always one-size-fits-all. The applicability and implementation of security standards in the industrial domain may differ significantly depending on the size of the organization. Some of the mentioned standards are more applicable for larger organizations, making it more challenging for smaller organizations to implement them. This issue often results in smaller industrial organizations hiring external cybersecurity personnel that do not understand the attributes and characteristics of the domain. To help organizations adopt the cybersecurity standard or framework that best fits their cybersecurity requirements, authors in [43] reviewed published papers in the academic database to extract commonly used industrial systems cybersecurity standards. The findings of their study highlighted the comprehensive coverage of both technical and organizational best practice measures in ISA/IEC 62443. The authors in [44], discussed cybersecurity strategies and challenges in standardization and government policies with close attention to the Cybersecurity Incident Management Framework (CIMF). The authors have also provided recommendations for effective cyber defense and cybersecurity. The standards PCI DSS and ISO 17799 are reviewed and compared in [45]. The study has concluded that although both standards have similar objectives, they differ significantly in terms of scope. ISO 17799 is applicable to all types of organizations, regardless of their size and type; however, PCI is applicable for a limited range of information systems, and its implication costs depend on the maturity of the systems and the security processes and controls within a system.

While previous research have greatly advanced our understanding of security standards adoption and implementation. There remain gaps in addressing the issue of streamlining compliance efforts. Through the identification of similarities between standards, organizations can eliminate redundant work and simplify the compliance process. This, will reduce both the implementation time and the cost associated with meeting the full set of standards. The objective of this research is to provide a comprehensive evaluation of widely adopted security standards in key industry sectors demonstrating the benefits of recognizing the similarities between them.

IV. STANDARDS CLASSIFICATION

To better manage and understand the large number of cybersecurity standards that currently exist, formal classification schemes have been proposed [46], [47]. Standards can generally be categorized into regulatory, best practice (industrial), or regional as elaborated next. A full view of standards classification is depicted in Figure 1.

A. REGULATORY STANDARDS

There are two main recognized types of regulatory standards [48]:

1) DE JURE STANDARDS

De jure standards refer to standards that are established by law. They are often established by industry groups, a government body or internationally or nationally recognized standards bodies. The development process often involves negotiations between parties with different interests in the standard and these standards are often critically assessed before being approved. Each such standard is ratified through the corresponding organization's official procedures and before approval. De jure standards reflect a state of affairs that is in accordance with law and non-compliance with the standard may therefore be officially sanctioned [48]. Within the European Union, standards organisations like ETSI [11], the European Committee for Standardization (CEN) and the

European Committee for Electrotechnical Standardization (CENELEC) [49] have been a key factor in the creation of a single European market that is governed by harmonized standards [3], which we define next.

a: EU HARMONIZED STANDARDS

Harmonized standards provide the technical details to meet the essential requirements of a specific legal act within the European Union. They apply in all EU countries and replace any conflicting national standards [50]. When harmonized standards are used and applied in a correct way, they give a presumption of conformity that legal requirements are fulfilled. By implementing a harmonized standard, manufacturers and service providers can therefore demonstrate that their services or products comply with relevant EU legislation. Only harmonised standards referred to and published in the Official Journal of the European Union (OJEU) [51] are valid.

2) DE FACTO STANDARDS

De facto standards are those which have been widely accepted as the best standard for their purpose (e.g. ETSI EN 303 645) [48]. Such standards are also referred to as market-driven standards. This is often because they have a proven track record for efficiency and reliability. A De facto standard that become accepted by an industry are also known as industry standards or professional standards. They can also be formalized and turned into de jure standards with the approval of an official standards organization,

B. INDUSTRIAL STANDARDS

Many of these standards must be purchased [52], some may be downloaded for free of charge [11]. Paid standards often offer more comprehensive details and specifications. However, legal and financial obligations need to be considered by organizations when opting for such standards. Furthermore, standards can be viewed as vertical or horizontal standards as explained next (Figure 1).

- Vertical standards: apply to a particular industry, for example: PCI DSS which is specific to the ''payment Card Industry Data Security''.
- Horizontal standards: are generic, they have broad scope (e.g., ISO/IEC 27001) and are adopted by multiple industries, including automotive, banking, manufacturing and service providers.

C. REGION-BASED STANDARDS

In addition to the regulatory and industrial classification of standards, there exist also a classification based on the region or country where the standard is developed or adopted. Region-based standards can be developed by national, international or regional standardization organizations as shown in Figure 1. Classifying standards by region ensures that they meet the specific needs and requirements of a given country or region.

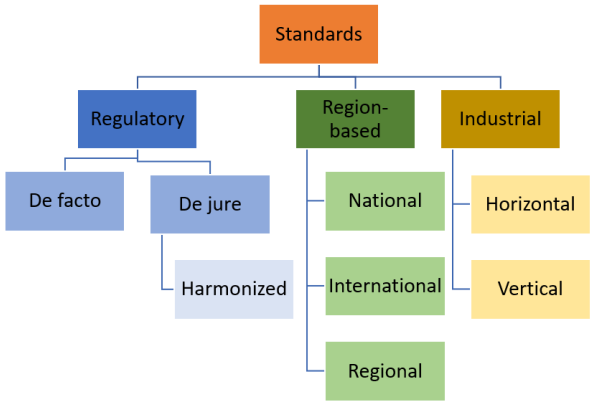


FIGURE 1. Organizing cybersecurity Standards.

- International standards are developed by international organizations such as ISO and IEC which can be adopted by countries worldwide.
- Regional standards are created by regional organizations such as the European Union (EU) and can be adopted by countries within that specific region.
- National standards are developed by a specific country such as ANSI/CTA-2088-A in the United States and the Minimum Cybersecurity Standard (MCSS) for UK.

Standards can vary in their content based on their purpose and the regulations and requirements of the region or country in which they are developed. Despite this, a standard can still belong to multiple categories. For instance, NIST 800-82 is initially a US national standard, but it has attained international recognition due to its widespread adoption. Additionally, it is also classified as an horizontal industrial standard. Similarly, ETSI EN 303 645, which was originally a European standard (regional), has gained international recognition and transformed into an international standard due to its extensive adoption. Figure 2 provides an illustrative example of these classifications. The aforementioned standards categorization, often result in security practitioners not paying enough attention to differences between organizations and their unique situational security requirements [43], [53].

This classification of scalability considerations influences the implementation of security controls, which may differ in common or unique form based on factors such as the organization's size, complexity, the importance of the information system's mission, and the organization's control scope.

V. METHODOLOGY

The overall goal for the mapping is to be as specific as possible, leaning towards under-mapping versus over-mapping. In this study, the general approach entails identifying all the elements encompassed by a control in a particular standard and then determining if a corresponding control in the compared standard articulates the exact same concept [54]. In order to accomplish this objective, we will employ the teleological interpretation method, which holds great significance within

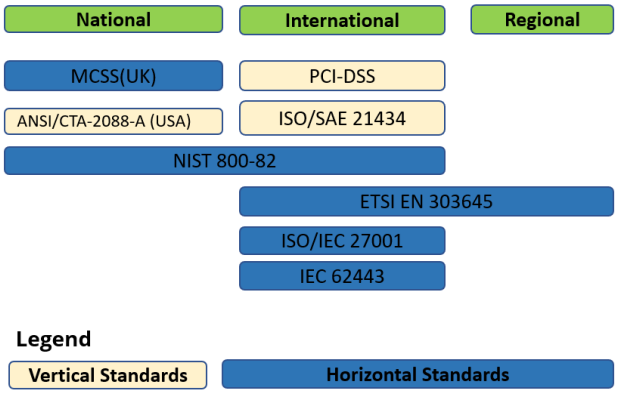


FIGURE 2. Industrial Security Standards: A classification example under region-based criteria.

the legal domain. Teleology comes from two Greek words: telos, meaning ''end, purpose or goal'', and logos, meaning ''explanation or reason'' [55]. Teleology is hence a method of explaining something through its function or purpose, rather than the thing itself. Both European national constitutional courts and the European Court of Human Rights utilize this method when justifying the interpretation of a legal rule in a concrete case. They maintain that such an interpretation can be justified by considering the goal (telos) that the rule is intended to realize [56]. As control objectives are intended to meet specific security goals outlined by a particular standard, the application of teleological interpretation is a valid approach for determining the meaning of a control. Hence, in this work, the requirements and the controls have been interpreted, compared and mapped according to their wording as well as their purpose or goal. More precisely, if the wording of the two controls are the same, they are matched with the relationship ''**Equivalent**''. If the controls have not identical wording but achieve the same purpose or goal, the type of the relationship between two defensive countermeasures is further analysed and the relationship is considered as ''**Related**''. As an example:

1– ISO/IEC 27001:2022 requirement 8.24 ''Use of cryptography'' is ***Equivalent*** to ISA/IEC 62443-3-3:2019 requirement 8.5 SR 4.3 ''Use of cryptography''.

2– ISO/IEC 27001:2022 requirement 8.21 ''Networks security'' is ***Related*** to ETSI EN 303 645 requirement 5.6-1 ''All unused network and logical interfaces shall be disabled''.

VI. MAPPING ISO/IEC 27001:2022 TO ISA/IEC 62443-3-3 AND ETSI EN 303645

In this section, we, first, present a comprehensive overview of the selected security standards ETSI EN 303 645 v2.1.1 [11], ISO/IEC 27001:2022 [13] and ISA/IEC 62443-3-3:2019 [28]. Subsequently, we perform a mapping analysis to uncover any similarities and disparities in the security requirements among the standards, providing a comprehensive examination of our findings. For this comparative analysis, we have mapped both ISA/IEC 62443-3-3 and ETSI EN 303 645 to ISO 27001:2022, a widely recognized security standard that serves as a reference for many organizations. Considering its extensive acceptance, the decision to use ISO 27001:2022 as the baseline for this comparison was a reasonable and expected choice.

The mapping process encompasses all the security controls outlined in ISO/IEC 27001:2022. Each control is thoroughly examined and evaluated, then the teleological interpretation method is applied to determine if a corresponding control exists in the standards being compared. If the security control encompasses multiple sub-controls (Figure 3), they are also included in the mapping. To accommodate the extensive number of security controls in each of the analyzed standards, the mapping tables in Appendix IX (Tables 5 and 6) solely display the controls that demonstrate alignment between the standards. Controls that lack a corresponding entry are excluded from these tables.

A. OVERVIEW OF THE SELECTED STANDARDS

The choice of the aforementioned security standards was made deliberately and thoughtfully, to showcase that despite their distinct application environments, there are still potential similarities among them. In addition, these standards are widely accepted, produced by various standardization bodies, and regarded as the best practices in their specific domains. They encompass a comprehensive set of cybersecurity controls for Information Security Management Systems (ISMS) [52], industrial systems [12], and IoT consumers [11] and are relevant to a range of environments, both horizontal and vertical. In the following sections, a more in-depth examination of each selected standard will be provided.

1) ISO/IEC 27001:2022

The ISO/IEC 27001:2022 standard outlines security controls for setting up, implementing, maintaining, and continually enhancing an Information Security Management System (ISMS). This includes administrative aspects of cybersecurity, such as security policies, as well as the human factors involved in privacy protection. A comprehensive list of all controls can be found in ISO/IEC 27001:2022 Annex A. ISO/IEC 27001:2022 is part of the ISO 27000 series, and is widely adopted by various countries and industries [52]. It can serve as a reference for identifying and implementing security controls in an ISMS, or as a source of guidance for creating industry-specific cybersecurity controls.

ISO/IEC 27001:2022 is the most recent update made by ISO, incorporating 93 high level controls (Figure 3) integrated into four distinct areas in terms of organizational, people, physical, and technology as presented in Figure 4. Each of these area controls must be addressed to respond to the challenges associated with ISMS cybersecurity.

This new version supersedes ISO 27001:2013, which comprised 114 controls across 14 categories, and introduces enhanced requirements and controls to address privacy protection, as well as the impact of technological advancements

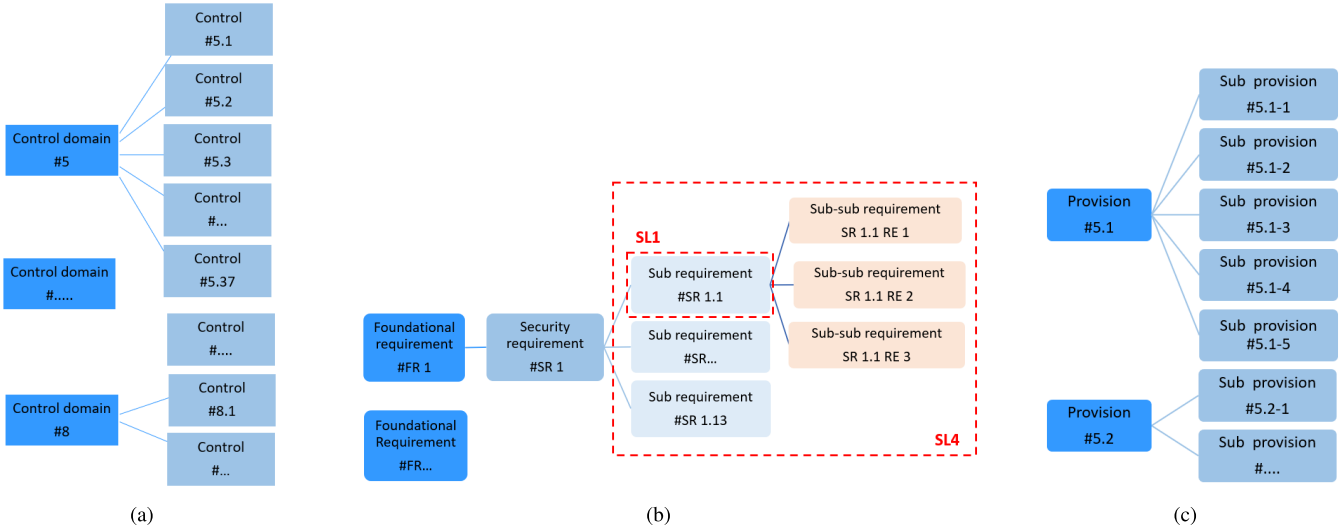


FIGURE 3. Security controls and requirements hierarchy of ISO/IEC 27001:2022 [13] (a) , ISA/IEC 62443-3-3 [28](b) and ETSI EN 301 645 [11](c). The red dashed squares is used to illustrate the security requirements (SRs) in a foundational requirement (FR) that could be included in a SL1 and SL4).

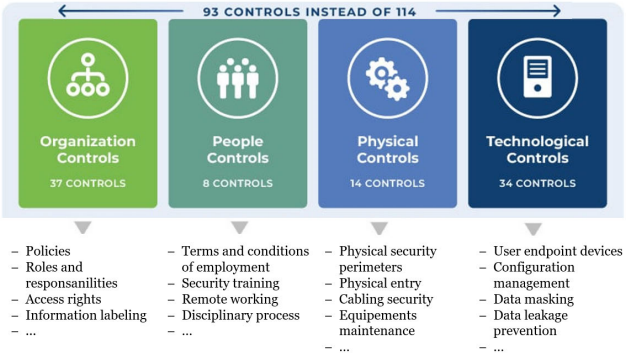


FIGURE 4. Controls areas in ISO 27001:2022.

TABLE 2. Security levels (SLs) in ISA/IEC 62443 [12].

Security Level	Description
SL0	No specific requirements or security protection.
SL1	Protection against casual or coincidental violation.
SL2	Protection against intentional violation using simple means with low resources, generic skills and low motivation.
SL3	Protection against intentional violation using sophisticated means with moderate resources, system-specific skills and moderate motivation.
SL4	Protection against intentional violation using sophisticated means with extended resources, system specific skills and high motivation

and evolving industrial practices. These changes reflect current security challenges in relation to modern risks and their associated controls.

2) ISA/IEC 62443-3-3:2019

The International Society of Automation (ISA) and The International Electro-technical Commission (IEC) jointly developed a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs). ISA/IEC 62443 includes detailed technical control system requirements (SRs) and requirement enhancements (RE) for Industrial Automation and Control Systems (IACSs) related to seven foundational requirements (FRs) (Figure 3), which define the requirements for control system capability security levels (SLs) and their components [12]. The industrial control system architecture should according to the standard be split into segments of zones and conduits, where the segmentation is an outcome of a security risk assessment. A zone is a collection of assets that have common security requirements. Conduits on the other hand is a logical grouping of communication channels between two or more zones. To achieve the desired security level and an acceptable level of risk for their network and components, organizations have the option to select from five different security levels, namely SL0 to SL4 as described in Table 2. As the security level increases, the number of necessary security controls also increases.

ISA/IEC 62443 standard consists of 12 standards arranged into 4 packages that address various aspects or levels of IACS security, including system availability, protection of the plant, and time-critical system response [12] enforced by various access control and network security requirements. For the purpose of limiting the extent of this study, we concentrate on the ISA/IEC 62443-3-3 standard, which provides specific documentation for system security requirements and security levels. It is deemed as a crucial standard within the ISA/IEC 62443 framework. The complete rundown of the security requirements are detailed in the standard document.

3) ETSI EN 303 645 v2.1.1

In 2020, ETSI introduced the standard ETSI EN 303 645 [11] with the objective of establishing high-level security and data protection provisions for consumer Internet of Things (IoT) devices connected to network infrastructure. This standard targets all parties that are involved in manufacturing and developing products and appliances that work based on the Internet of Things technology. The standard consists of 13 high-level recommendations that encompass 68 provisions, of which 33 are mandatory and the remaining are recommendations, applicable to general horizontal or sector-specific security requirements. The comprehensive listing of the provisions is accessible in the standard document [11]. Essentially, ETSI EN 303 645 places a strong emphasis on the protection of consumer data, the security of IoT devices and the protection of consumer's privacy. The standard has become a widely recognized reference for securing IoT devices globally and is utilized in various cybersecurity certification programs. As the first globally applicable cybersecurity standard for consumer IoT devices, ETSI EN 303645 is suitable for a diverse range of consumer products and is a demonstration of security best practice through voluntary industry compliance.

B. MAPPING ETSI EN 303 645 TO ISO/IEC 27001:2022

The mapping analysis, including ISO/IEC 27001:2022 controls and ETSI EN 303645 v.2.1.1 high-level and low-level provisions, shows that all ETSI EN 303 645 requirements can be aligned with ISO/IEC 27001:2022. This result is plausible as IoT consumer products can be considered as information technology devices. Therefore, it can be safely concluded that, to some extent, implementing ISO/IEC 27001:2022 can also fulfill the requirements of ETSI EN 303 645. Nevertheless, the study also shows that 64 out of the 93 ISO/IEC 27001 controls do not have a corresponding provision in ETSI EN 303 645, found particularly within the category of organizational controls which focuses on organizational leadership and employment aspects. This discrepancy can be justified as these requirements are typically not relevant to individuals, for instance:

- ISO/IEC 27001 controls ranging from 5.2 to 5.13: ensure that security policies are written and reviewed in accordance with the organization's information security practices and establish a framework for adequately implementing and maintaining these practices. These controls are directed towards organizations and do not apply to individuals.
- ISO/IEC 27001:2022 controls from 6.2 to 6.6: focus on defining the employment and termination conditions for organizational employees, and are viewed as a logical gap because they are crucial for employees but have no relevance for individuals in a personal capacity.
- ISO/IEC 27001:2022 controls 7.1 to 7.12: outline physical access controls and are not applicable to IoT environment. It is also expected that a device intended for personal use would not require physical access controls.
- ISO/IEC 27001:2022 controls 8.29 to 8.31: pertain to technological controls for security testing and monitoring and reviewing activities related to outsourced system development, but do not apply to personal devices.

The full mapping result of this comparison is displayed in Appendix IX (Table 5).

C. MAPPING ISA/IEC 62443-3-3:2019 TO ISO/IEC 27001:2022

The comparison between ISO/IEC 27001:2022 to ISA/IEC 62443-3-3, as depicted in Appendix IX (Table 6), reveals that while there are a large overlap between the two standards, we also found several gaps (see Table 3). Some of the omissions in ISA/IEC 62443-3-3 standard may be addressed in other parts of the ISA/IEC 62443 standards series. For instance, the security policy controls in ISO 27001:2022, have not been addressed in ISA/IEC 62443-3-3, but they are covered in ISA/IEC 62443-2-1. This suggests that the ISA/IEC 62443 standard series is designed to be complementary, with each part addressing different aspects of ICS security and filling in any gaps left by other parts. Other gaps can be justified as follows:

- ISA/IEC 62443-3-3 Req 6.4 and 6.5: Wireless connections and wireless endpoints devices are similar to other types of network connections but wireless devices can require a different set of security controls. Requirements related to wireless connectivity also differ to some extent between ISA/IEC 62443-3-3 and ISO/IEC 27001:2022. The requirements for wireless industry automation components based on ISA/IEC 62443-3-3 note the importance on strict use control measures where the focus is on identifying unauthorized wireless devices. In ISO/IEC 27001:2022 on the other hand is highlighting the challenge in controlling wireless network perimeter and procedures for configuration of wireless network devices. Radio coverage adjustments is here mentioned as a control for segregation of wireless networks. Requirements in ISA/IEC 62443-3-3 related to configuration of portable and mobile devices are more strict and indicate automatic enforcement of configurable usage restrictions.
- ISA/IEC 62443-3-3 Req 6.6: it covers requirements for mobile code technologies and indicate for example the need for capabilities to prevent execution of mobile code as well as restricting transfer of mobile code to/from devices. A similar requirement is not defined in ISO/IEC 27001:2022.
- ISA/IEC 62443 Req 9.4: The ISA/IEC 62443 series standards has introduced the concept of security zones, where a zone is a group of logical or physical assets that share common security requirements. Security controls can be defined both for zone boundaries and controls that are valid within a specific zone. ISA/IEC 62443-3-3 also include requirements for zone boundary protection. An

equivalent control system that would provide capabilities to monitor and control communications and connections between system boundaries is not included in ISO/IEC 27001:2022. Segregation of networks with the purpose to split the network into security boundaries and control the network perimeter of each domain using e.g. gateways is defined in ISO/IEC 27001:2022, but it is not analogous the concept of zones in ISA/IEC 62443-3-3.

– ISA/IEC 62443 Req 9.5: prohibits all general purpose person-to-person communications which is an example of a industry automation specific requirement. From an industry control system perspective it is essential to prohibit the usage of the industrial automation system for the purpose of private communication, since this could potentially be an attack vector to exploit vulnerabilities in a factory environment. It is understandable that a corresponding requirement is not included in ISO/IEC 27001:2022 due to the fact that the scope is different.

VII. DISCUSSION OF THE MAPPING RESULTS

The objective of this study was to analyse the similarities and differences between the security controls of three well-established industrial cybersecurity standards: ISO/IEC 27001, ISA/IEC 62443-3-3, and ETSI EN 303 645. The study also aims at identifying strengths and weaknesses of each of the mentioned standards. Although the mapping analysis revealed some gaps between the standards as illustrated in Table 4, it can be reasonably argued that there are numerous common, generic cybersecurity requirements (Figure 5) that are valid and applicable to various industries and ICT environments. It also showed that all the three analyzed standards encompass a collection of generic requirements that can enhance an organization's cybersecurity posture. In order to provide further insight into the results of the mapping study, we aligned the security controls of each standard to one of the cybersecurity functions, as defined in ISO/IEC 27001:2022, ISO/IEC TS 27110 [21] and the NIST cybersecurity Framework (CSF) [57]. These standards categorize cybersecurity functions, referred to as cybersecurity concepts, into five categories such as: Identify, Protect, Detect, Respond, and Recover. By doing so, one can determine which areas of system security each standard prioritizes. The strength or weaknesses of a specific area are demonstrated by the number of security controls created for each concept. The analysis indicates that ISO 27001:2022 has a more comprehensive set of controls for each cybersecurity concept with a total of 125 controls compared to 113 in ISA/IEC 62443-3-3:2019 and 72 in ETSI EN 303 645 V2.1.1 (as depicted in Figure 6), suggesting its superiority compared to the other two standards. Next we will elaborate on the distinctive characteristics of each standard.

A. ISO/IEC 27001:2022

ISO/IEC27001:2022 views cybersecurity as a combination of requirements and controls related to organization, people, process, and technology as highlighted in Table 4. The

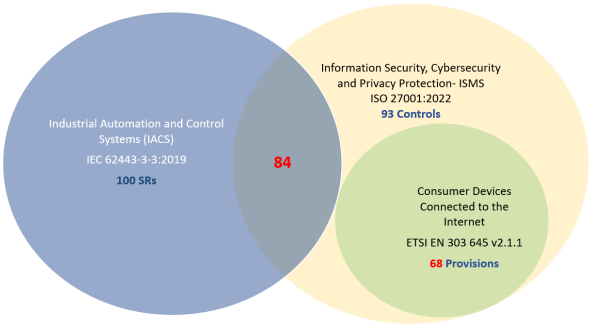


FIGURE 5. Security standards coverage.

study revealed that ISO/IEC 27001:2022 emphasized human resource security with controls for employment, termination, and changes of employment, applying to both employees and contractors, a feature lacking in the other two standards. The findings also indicate that ISO/IEC 27001:2022 had a clear advantage over the other two standards in facilitating and simplifying the mapping process. All ISO/IEC27001:2022 requirements are written at a high-level and do not include any low-level requirements. However, ETSI EN 303 645 and ISA/IEC 62443-3-3 were more challenging to map as each control encompasses additional sub-controls that required careful examination (Figure 3), sometimes leading to ambiguity and confusion. For instance, ETSI EN 303 645's provision "no default passwords 5.1-1" includes additional low-level provisions for authentication mechanisms. Figure 6 illustrates how ISO/IEC 27001:2022 has been updated to include a more comprehensive coverage of cybersecurity concepts of 125 controls. All of the standards contain a greater number of controls dedicated to the protection of the system, compared to the other cybersecurity concepts. In particular, ISO/IEC 27001:2022 supersedes both standards with controls that are crucial to identify the risk, respond to, and recover from attacks. The emphasis on risk identification highlights the standard's increased focus on preventing attacks and minimizing the costs associated with mitigation. Furthermore, the ISO standard places greater emphasis on implementing measures to respond to and recover from a cyber attack, which demonstrates its commitment to promoting system resilience and facilitating a rapid return to normal operations in the event of an attack.

B. ETSI EN 303 645 V2.1.1

The ETSI EN 303 645 standard provides baseline security provision for consumer IoT focusing on data protection and consumer privacy. Since the devices addressed by this standard are intended for personal use, the focus is primarily on protection measures and risk identification with very limited controls to detect, respond and recover from attacks (Figure 6). Furthermore, unlike the ISO/IEC 27001:2022 standard, it does not address people and physical controls as they are not applicable to ETSI standard scope (Table 4). From the mapping analysis presented in

TABLE 3. Unmapped ISA/IEC 62443-3-3:2019 requirements.

Requirement identifier	Requirement name	Description
6.4	SR 2.2 – Wireless use control	The control system shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the control system according to commonly accepted security industry practices.
6.4.3.1	SR 2.2 RE 1 – Identify and report unauthorized wireless devices.	The control system shall provide the capability to identify and report unauthorized wireless devices transmitting within the control system physical environment.
6.5	SR 2.3 – Use control for portable and mobile devices.	The control system shall provide the capability to automatically enforce configurable usage restrictions.
6.5.3.1	SR 2.3 RE 1 – Enforcement of security status of portable and mobile devices.	The control system shall provide the capability to verify that portable or mobile devices attempting to connect to a zone comply with the security requirements of that zone.
6.6	SR 2.4 – Mobile code.	The control system shall provide the capability to enforce usage restrictions for mobile code technologies based on the potential to cause damage to the control system.
6.6.3.1	SR 2.4 RE 1 – Mobile code integrity check	The control system shall provide the capability to verify integrity of the mobile code before allowing code execution.
6.12	SR 2.10 – Response to audit processing failures	The control system shall provide the capability to alert personnel and prevent the loss of essential services and functions in the event of an audit processing failure. The control system shall provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.
9.4	SR 5.2 – Zone boundary protection.	The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.
9.4.3.1	SR 5.2 RE 1 – Deny by default, allow by exception.	The control system shall provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception).
9.4.3.2	SR 5.2 RE 2 – Island mode	The control system shall provide the capability to prevent any communication through the control system boundary (also termed island mode). NOTE Examples of when this capability may be used include where a security violation and/or breach has been detected within the control system, or an attack is occurring at the enterprise level.
9.4.3.3	SR 5.2 RE 3 – Fail close	The control system shall provide the capability to prevent any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms (also termed fail close). This 'fail close' functionality shall be designed such that it does not interfere with the operation of a SIS or other safety-related functions.
9.5	SR 5.3 – General purpose person-to-person communication restrictions.	The control system shall provide the capability to prevent general purpose person-to-person messages from being received from users or systems external to the control system.
9.5.3.1	SR 5.3 RE 1 – Prohibit all general-purpose person-to-person communications	The control system shall provide the capability to prevent both transmission and receipt of general-purpose person-to-person messages.
11.8.3.1	SR 7.6 RE 1 – Machine-readable reporting of current security settings.	The control system shall provide the capability to generate a report listing the currently deployed security settings in a machine-readable format.

TABLE 4. Control domains coverage.

Control domains	ISMS ISO/IEC 27001:2022	IACS ISA/IEC 62443-3-3:2019	Consumer IoT ETSI EN 303 645 v2.1.1
Organizational requirements	✓		✓
People requirements	✓		
Physical requirements	✓	✓	
Technological requirements	✓	✓	✓

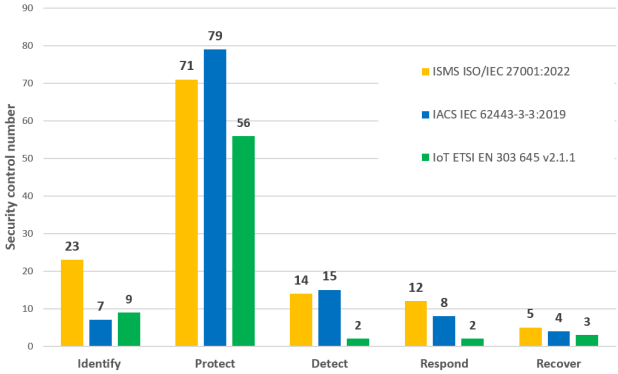


FIGURE 6. Security standards controls coverage.

Appendix IX (Table 5), it can be safely concluded that the organization and technology controls in the ISO/IEC 27001:2022 standard provide full coverage of the ETSI EN 303 645 standard. This is supported by the fact that all 68 ETSI EN provisions were successfully mapped to 29 ISO/IEC 27001 controls (Figure 5). Therefore, organizations can leverage the ISO/IEC 27001:2022 standard to effectively implement the security requirements outlined in the ETSI EN 303 645 standard for their consumer IoT devices. When using the ISO/IEC 27001:2022 standard to implement the security requirements of the ETSI EN 303 645 standard, it is important for organizations to consider that the ETSI standard covers devices without passwords, such as household appliances with limited computing power like coffee makers or refrigerators. This means that they have to implement controls that are appropriate and effective for these devices by prioritizing practical solutions over complex security measures like authentication and authorization. The objective is to provide practical household connectivity solutions that make everyday tasks more manageable, like remotely starting a washing machine or cooking utensil, prioritizing ease of use over extensive security measures.

TABLE 5. Mapping ETSI EN 303 645 to ISO 27001:2022.

ISO/IEC 27002:2022 control identifier	ISO/IEC 27002:2022 control name	ETSI EN 303 645 requirement identifier	ETSI EN 303 645 requirement name
5.1	Policies for information security	5.2-1	The manufacturer shall make a vulnerability disclosure policy publicly available.
5.14	Information transfer	5.5-1	The consumer IoT device shall use best practice cryptography to communicate securely.
		5.5-6	Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk, and usage.
		5.8-1	The confidentiality of personal data transiting between a device and a service, especially associated services, should be protected, with best practice cryptography.
		5.8-2	The confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage.
5.15	Access control	5.1-3	Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage.
		5.6-8	The device should include a hardware-level access control mechanism for memory.
5.17	Authentication information	5.1-1	Where passwords are used and, in any state, other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user.
		5.1-2	Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.
		5.1-3	Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk, and usage.
		5.1-4	Where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value used.
5.29	Information security during disruption	5.9-1	Resilience should be built into consumer IoT devices and services, taking into account the possibility of outages of data networks and power.
		5.9-2	Consumer IoT devices should remain operating and locally functional in the case of a loss of network access and should recover cleanly in the case of restoration of a loss of power.
		5.9-3	The consumer IoT device should connect to networks in an expected, operational and stable state and in an orderly fashion, taking the capability of the infrastructure into consideration.
5.30	ICT readiness for business continuity	5.9-1	Resilience should be built into consumer IoT devices and services, considering the possibility of outages of data networks and power.
		5.9-2	Consumer IoT devices should remain operating and locally functional in the case of a loss of network access and should recover cleanly in the case of restoration of a loss of power.
		5.9-3	The consumer IoT device should connect to networks in an expected, operational and stable state and in an orderly fashion, taking the capability of the infrastructure into consideration.
5.34	Privacy and protection of PII	5.8-1	The confidentiality of personal data transiting between a device and a service, especially associated services, should be protected, with best practice cryptography.
		5.8-2	The confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage.
		5.8-3	All external sensing capabilities of the device shall be documented in an accessible way that is clear and transparent for the user.
		5.11-1	The user shall be provided with functionality such that user data can be erased from the device in a simple manner.
		5.11-2	The consumer should be provided with functionality on the device such that personal data can be removed from associated services in a simple manner.
		5.11-3	Users should be given clear instructions on how to delete their personal data.
		5.11-4	Users should be provided with clear confirmation that personal data has been deleted from services, devices and applications.
		6-1	The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes, for each device and service.
		6-2	Where personal data is processed based on consumers' consent, this consent shall be obtained in a valid way.
		6-3	Consumers who gave consent for the processing of their personal data shall have the capability to withdraw it at any time.
		6-4	If telemetry data is collected from consumer IoT devices and services, the processing of personal data should be kept to the minimum necessary for the intended functionality.
		6-5	If telemetry data is collected from consumer IoT devices and services, consumers shall be provided with information on what telemetry data is collected, how it is being used, by whom, and for what purposes.
7.13	Equipment maintenance	5.12-1	Installation and maintenance of consumer IoT should involve minimal decisions by the user and should follow security best practice on usability.
7.14	Secure disposal or reuse of equipment	5.11-1	The user shall be provided with functionality such that user data can be erased from the device in a simple manner.
		5.11-2	The consumer should be provided with functionality on the device such that personal data can be removed from associated services in a simple manner.
		5.11-3	Users should be given clear instructions on how to delete their personal data.
		5.11-4	Users should be provided with clear confirmation that personal data has been deleted from services, devices, and applications.
8.5	Secure authentication	5.1-3	Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk, and usage.
		5.1-5	When the device is not a constrained device, it shall have a mechanism available which makes brute-force attacks on authentication mechanisms via network interfaces impracticable.
8.8	Management of technical vulnerabilities	5.2-2	Disclosed vulnerabilities should be acted on in a timely manner.
		5.2-3	Manufacturers should continually monitor for, identify, and rectify security vulnerabilities within products and services.

TABLE 5. *(Continued.)* **Mapping ETSI EN 303 645 to ISO 27001:2022.**

8.9	Configuration management	5.6-3	Device hardware should not unnecessarily expose physical interfaces to attack.
		5.6-4	Where a debug interface is physically accessible, it shall be disabled in software.
		5.6-5	The manufacturer should only enable software services that are used or required for the intended use or operation of the device.
		5.12-2	The manufacturer should provide users with guidance on how to securely set up their device.
		5.12-3	The manufacturer should provide users with guidance on how to check whether their device is securely set up.
8.10	Information deletion	5.11-1	The user shall be provided with functionality such that user data can be erased from the device in a simple manner.
		5.11-2	The consumer should be provided with functionality on the device such that personal data can be removed from associated services in a simple manner.
		5.11-3	Users should be given clear instructions on how to delete their personal data.
		5.11-4	Users should be provided with clear confirmation that personal data has been deleted from services, devices, and applications.
8.12	Data leakage prevention	5.4-1	Sensitive security parameters in persistent storage shall be stored securely by the device.
		5.5-1	The consumer IoT device shall use best practice cryptography to communicate securely.
		5.5-2	The consumer IoT device should use reviewed or evaluated implementations to deliver network and security functionalities, particularly in the field of cryptography.
8.14	Redundancy of information processing facilities	5.9-1	Resilience should be built in to consumer IoT devices and services, taking into account the possibility of outages of data networks and power.
8.15	Logging	5.10-1	If telemetry data is collected from consumer IoT devices and services, such as usage and measurement data, it should be examined for security anomalies.
		6-3	If telemetry data is collected from consumer IoT devices and services, the processing of personal data should be kept to the minimum necessary for the intended functionality.
		6-4	If telemetry data is collected from consumer IoT devices and services, consumers shall be provided with information on what telemetry data is collected, how it is being used, by whom, and for what purposes.
8.16	Monitoring activities	5.7-2	If an unauthorized change is detected to the software, the device should alert the user and/or administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function.
		5.10-1	If telemetry data is collected from consumer IoT devices and services, such as usage and measurement data, it should be examined for security anomalies.
		6-3	If telemetry data is collected from consumer IoT devices and services, the processing of personal data should be kept to the minimum necessary for the intended functionality.
		6-4	If telemetry data is collected from consumer IoT devices and services, consumers shall be provided with information on what telemetry data is collected, how it is being used, by whom, and for what purposes.
8.19	Installation of software on operational systems	5.3-1	All software components in consumer IoT devices should be securely updateable.
		5.3-2	When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates.
		5.3-3	An update shall be simple for the user to apply.
		5.3-4	Automatic mechanisms should be used for software updates.
		5.3-5	The device should check after initialization, and then periodically, whether security updates are available.
		5.3-6	If the device supports automatic updates and/or update notifications, these should be enabled in the initialized state and configurable so that the user can enable, disable, or postpone installation of security updates and/or update notifications.
		5.3-7	The device shall use best practice cryptography to facilitate secure update mechanisms.
		5.3-8	Security updates shall be timely.
		5.3-9	The device should verify the authenticity and integrity of software updates.
		5.3-10	Where updates are delivered over a network interface, the device shall verify the authenticity and integrity of each update via a trust relationship.
		5.3-11	The manufacturer should inform the user in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by that update.
		5.3-12	The device should notify the user when the application of a software update will disrupt the basic functioning of the device.
		5.3-13	The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period.
		5.3-14	For constrained devices that cannot have their software updated, the rationale for the absence of software updates, the period and method of hardware replacement support and a defined support period should be published by the manufacturer in an accessible way that is clear and transparent to the user.
		5.3-15	For constrained devices that cannot have their software updated, the product should be isolable and the hardware replaceable.
		5.3-16	The model designation of the consumer IoT device shall be clearly recognizable, either by labelling on the device or via a physical interface.
		5.7-1	The consumer IoT device should verify its software using secure boot mechanisms.
		5.7-2	If an unauthorized change is detected to the software, the device should alert the user and/or administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function.
		5.12-1	Installation and maintenance of consumer IoT should involve minimal decisions by the user and should follow security best practice on usability.
8.20	Networks security	5.6-1	All unused network and logical interfaces shall be disabled.
		5.6-2	In the initialized state, the network interfaces of the device shall minimize the unauthenticated disclosure of security-relevant information.
8.24	Use of cryptography	5.1-3	Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk, and usage.
		5.3-7	The device shall use best practice cryptography to facilitate secure update mechanisms.
		5.4-1	Sensitive security parameters in persistent storage shall be stored securely by the device.
		5.5-1	The consumer IoT device shall use best practice cryptography to communicate securely.

TABLE 5. *(Continued.)* **Mapping ETSI EN 303 645 to ISO 27001:2022.**

		5.5-2	The consumer IoT device should use reviewed or evaluated implementations to deliver network and security functionalities, particularly in the field of cryptography.
		5.5-3	Cryptographic algorithms and primitives should be updateable.
		5.5-6	Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk, and usage.
		5.8-1	The confidentiality of personal data transiting between a device and a service, especially associated services, should be protected, with best practice cryptography.
		5.8-2	The confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage.
8.25	Secure development life cycle	5.6-9	The manufacturer should follow secure development processes for software deployed on the device.
8.26	Application security requirements	5.5-1	The consumer IoT device shall use best practice cryptography to communicate securely.
		5.5-2	The consumer IoT device should use reviewed or evaluated implementations to deliver network and security functionalities, particularly in the field of cryptography.
		5.13-1	The consumer IoT device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices.
8.27	Secure system architecture and engineering principles	5.4-1	Sensitive security parameters in persistent storage shall be stored securely by the device.
		5.4-2	Where a hard-coded unique per device identity is used in a device for security purposes, it shall be implemented in such a way that it resists tampering by means such as physical, electrical or software.
		5.4-4	Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services in device software shall be unique per device and shall be produced with a mechanism that reduces the risk of automated attacks against classes of devices.
		5.5-3	Cryptographic algorithms and primitives should be updateable.
		5.5-4	Access to device functionality via a network interface in the initialized state should only be possible after authentication on that interface.
		5.5-5	Device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication.
		5.5-6	Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk, and usage.
		5.5-7	The consumer IoT device shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces.
		5.5-8	The manufacturer shall follow secure management processes for critical security parameters that relate to the device.
		5.6-1	All unused network and logical interfaces shall be disabled.
		5.6-2	In the initialized state, the network interfaces of the device shall minimize the unauthenticated disclosure of security-relevant information.
		5.6-7	Software should run with least necessary privileges, taking account of both security and functionality.
8.28	Secure coding	5.4-3	Hard-coded critical security parameters in device software source code shall not be used.
		5.6-4	Where a debug interface is physically accessible, it shall be disabled in software.
		5.6-6	Code should be minimized to the functionality necessary for the service/device to operate.
		5.13-1	The consumer IoT device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices.
8.32	Change management	5.7-2	If an unauthorized change is detected to the software, the device should alert the user and/or administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function.

C. ISA/IEC 62443-3-3:2019

The concept of a risk based segmented architecture with zones, conducts and security levels differentiates the ISA/IEC 62443-3-3 from the other standards we have analysed in this study. This approach allows organizations to apply security controls based on the level of acceptable risk and protection needed. Lower security levels such as SL0 or SL1 may suffice for non-critical industrial environments, while higher security levels such as SL3 or SL4 are essential for high-risk or critical systems. Despite these particularities, Appendix IX (Table 6) testifies on the large overlap between ISO 27001 and ISA/IEC 62443. In fact, out of 100 requirements from ISA/IEC 62443-3-3, 84 have been mapped to equivalent or related controls in ISO/IEC 27001 (Figure 5). The unmapped requirements as shown in Table 3 indicates a number of requirement enhancements used in SL3 or SL4 that are relevant and important for high-level security systems such as critical systems. Therefore it might in some cases be justified to implement a set of baseline cybersecurity requirements defined in ISO/IEC 27001 in a non-critical industrial automation environment. In a high risk or critical industrial environments additional system level requirements designed to protect against intentional violations needs to be considered. ISA/IEC 62443-3-3 places greater emphasis on technical protection measures with a total of 79 protective controls compared to 71 in ISO 27001:2022. Additionally, ISA/IEC 62443-3-3 focuses on controls to detect attacks, but places less importance on controls for pre- and post-attacks. This direction has also been followed in the other two standards. It is important to note that all controls in ISA/IEC 62443-3-3 are physical or technological requirements as shown in Table 4, as this standard is intended for system requirements. Organizational and people controls are addressed in other parts of the ISA/IEC 62443 standard package.

VIII. CHALLENGES

The evolving nature of the cybersecurity area, characterized by the emergence of new threats and vulnerabilities, makes unrealistic to establish a permanent and steady level of system security over time. Instead cybersecurity is optimized to a level business leaders define, balancing the limited resources available to the acceptable risk appetite. Complying to a cybersecurity standard can partially manage cybersecurity challenges, attacks opportunities and cyber risks. However, not all risks can be mitigated through standards and frameworks. Given the cross-functional nature of cybersecurity, the development and implementation of effective security standards and frameworks present additional challenges that

TABLE 6. Mapping ISA/IEC 62443-3-3:2019 to ISO/IEC 27002:2022.

ISO/IEC 27002:2022 control identifier	ISO/IEC 27002:2022 control name	ISA/IEC 62443-3-3:2019 requirement identifier	ISA/IEC 62443-3-3:2019 requirement name
5.3	Segregation of duties	5.3	SR 1.1 – Human user identification and authentication
		6.3	SR 2.1 – Authorization enforcement
		6.3.3.1	SR 2.1 RE 1 – Authorization enforcement for all users
5.9	Inventory of information and other associated assets	11.10	SR 7.8 – Control system component inventory
5.14	Information transfer	8.3	SR 4.1 – Information confidentiality
		8.3.3.1	SR 4.1 RE 1 – Protection of confidentiality at rest or in transit via untrusted networks
		8.3.3.2	SR 4.1 RE 2 – Protection of confidentiality across zone boundaries
5.15	Access control	5.3	SR 1.1 – Human user identification and authentication
		5.3.3.1	SR 1.1 RE 1 – Unique identification and authentication
		5.3.3.2	SR 1.1 RE 2 – Multifactor authentication for untrusted networks
		5.3.3.3	SR 1.1 RE 3 – Multifactor authentication for all networks
		5.4	SR 1.2 – Software process and device identification and authentication
		5.4.3.1	SR 1.2 RE 1 – Unique identification and authentication
5.16	Identity management	5.6	SR 1.4 – Identifier management
		5.7	SR 1.5 – Authenticator management
		5.7.3.1	SR 1.5 RE 1 – Hardware security for software process identity credentials
		5.8	SR 1.6 – Wireless access management
		5.8.3.1	SR 1.6 RE 1 – Unique identification and authentication
5.17	Authentication information	5.9	SR 1.7 – Strength of password-based authentication
		5.9.3.1	SR 1.7 RE 1 – Password generation and lifetime restrictions for human users
		5.9.3.2	SR 1.7 RE 2 – Password lifetime restrictions for all users
5.18	Access rights	5.5	SR 1.3 – Account management
		5.5.3.1	SR 1.3 RE 1 – Unified account management
		6.3	SR 2.1 – Authorization enforcement
		6.3.3.1	SR 2.1 RE 1 – Authorization enforcement for all users
		6.3.3.2	SR 2.1 RE 2 – Permission mapping to roles
		6.3.3.4	SR 2.1 RE 4 – Dual approval
5.28	Collection of evidence	6.10	SR 2.8 – Auditable events
		6.10.3.1	SR 2.8 RE 1 – Centrally managed, system-wide audit trail
5.29	Information security during disruption	7.8	SR 3.6 – Deterministic output
		11.3	SR 7.1 – Denial of service protection
		11.3.3.1	SR 7.1 RE 1 – Manage communication loads
		11.3.3.2	SR 7.1 RE 2 – Limit DoS effects to other systems or networks
		11.4	SR 7.2 – Resources management
5.30	ICT readiness for business continuity	11.5	SR 7.3 – Control system backup
		11.5.3.1	SR 7.3 RE 1 – Backup verification
		11.5.3.2	SR 7.3 RE 2 – Backup automation
		11.6	SR 7.4 – Control system recovery and reconstitution
		11.7	SR 7.5 – Emergency power
5.33	Protection of records	7.11	SR 3.9 – Protection of audit information
		8.3	SR 4.1 – Information confidentiality
		8.3.3.1	SR 4.1 RE 1 – Protection of confidentiality at rest or in transit via untrusted networks
		8.3.3.2	SR 4.1 RE 2 – Protection of confidentiality across zone boundaries
5.34	Privacy and protection of PII	8.3	SR 4.1 – Information confidentiality
		8.3.3.1	SR 4.1 RE 1 – Protection of confidentiality at rest or in transit via untrusted networks
		8.3.3.2	SR 4.1 RE 2 – Protection of confidentiality across zone boundaries.
6.6	Confidentiality or non-disclosure agreements	8.3	SR 4.1 – Information confidentiality
6.7	Remote working	5.15	SR 1.13 – Access via untrusted networks
		5.15.3.1	SR 1.13 RE 1 – Explicit access request approval
7.7	Clear desk and clear screen	8.3	SR 4.1 – Information confidentiality
7.10	Storage media	8.3	SR 4.1 – Information confidentiality
7.11	Supporting utilities	11.7	SR 7.5 – Emergency power
8.1	User endpoint devices	6.7	SR 2.5 – Session lock
8.2	Privileged access rights	5.3	SR 1.1 – Human user identification and authentication
		5.4	SR 1.2 – Software process and device identification and authentication
8.4	Access to source code	7.6	SR 3.4 – Software and information integrity
		7.6.3.1	SR 3.4 RE 1 – Automated notification about integrity violations
8.5	Secure authentication	5.3	SR 1.1 – Human user identification and authentication
		5.3.3.2	SR 1.1 RE 2 – Multifactor authentication for untrusted networks
		5.3.3.3	SR 1.1 RE 3 – Multifactor authentication for all networks
		5.9	SR 1.7 – Strength of password-based authentication
		5.9.3.1	SR 1.7 RE 1 – Password generation and lifetime restrictions for human users
		5.9.3.2	SR 1.7 RE 2 – Password lifetime restrictions for all users
		5.10	SR 1.8 – Public key infrastructure (PKI) certificates
		5.11	SR 1.9 – Strength of public key authentication
		5.11.3.1	SR 1.9 RE 1 – Hardware security for public key authentication
		5.12	SR 1.10 – Authenticator feedback
		5.13	SR 1.11 – Unsuccessful login attempts
8.6	Capacity management	6.11	SR 2.9 – Audit storage capacity
		6.11.3.1	SR 2.9 RE 1 – Warn when audit record storage capacity threshold reached
8.9	Configuration management	11.10	SR 7.8 – Control system component inventory
8.10	Information deletion	8.4	SR 4.2 – Information persistence
		8.4.3.1	SR 4.2 RE 1 – Purging of shared memory resources
8.11	Data masking	8.3	SR 4.1 – Information confidentiality

TABLE 6. *(Continued.)* **Mapping ISA/IEC 62443-3-3:2019 to ISO/IEC 27002:2022.**

8.12	Data leakage prevention	8.3	SR 4.1 – Information confidentiality
8.13	Information backup	11.5	SR 7.3 – Control system backup
		11.5.3.1	SR 7.3 RE 1 – Backup verification
		11.5.3.2	SR 7.3 RE 2 – Backup automation
8.14	Redundancy of information processing facilities	11.4	SR 7.2 – Resource management
8.15	Logging	6.10	SR 2.8 – Auditable events
		6.14	SR 2.12 – Non-repudiation
		6.14.3.1	SR 2.12 RE 1 – Non-repudiation for all users
		7.4	SR 3.2 – Malicious code protection
		7.4.3.1	SR 3.2 RE 1 – Malicious code protection on entry and exit points
		7.4.3.2	SR 3.2 RE 2 – Central management and reporting for malicious code protection
		10.3	SR 6.1 – Audit log accessibility
8.16	Monitoring activities	10.4	SR 6.2 – Continuous monitoring
8.17	Clock synchronization	6.13	SR 2.11 – Timestamps
		6.13.3.1	SR 2.11 RE 1 – Internal time synchronization
		6.13.3.2	SR 2.11 RE 2 – Protection of time source integrity
8.18	Use of privileged utility programs	6.3	SR 2.1 – Authorization enforcement
		6.3.3.3	SR 2.1 RE 3 – Supervisor override
8.19	Installation of software on operational systems	7.6	SR 3.4 – Software and information integrity
8.20	Networks security	11.8	SR 7.6 – Network and security configuration settings
8.21	Security of network services	11.8	SR 7.6 – Network and security configuration settings
8.22	Segregation of networks	9.3	SR 5.1 – Network segmentation
		9.3.3.1	SR 5.1 RE 1 – Physical network segmentation
		9.3.3.3	SR 5.1 RE 3 – Logical and physical isolation of critical networks
8.23	Web filtering	9.5	SR 5.3 – General purpose person-to-person communication restrictions
8.24	Use of cryptography	7.3	SR 3.1 – Communication integrity
		7.3.3.1	SR 3.1 RE 1 – Cryptographic integrity protection
		8.5	SR 4.3 – Use of cryptography
8.26	Application security requirements	7.8	SR 3.6 – Deterministic output
		7.9	SR 3.7 – Error handling
		9.6	SR 5.4 – Application partitioning
8.27	Secure system architecture and engineering principles	6.8	SR 2.6 – Remote session termination
		6.9	SR 2.7 – Concurrent session control
		7.10	SR 3.8 – Session integrity
		7.10.3.1	SR 3.8 RE 1 – Invalidation of session IDs after session termination
		7.10.3.2	SR 3.8 RE 2 – Unique session ID generation
		7.10.3.3	SR 3.8 RE 3 – Randomness of session Ids
		11.9	SR 7.7 – Least functionality
8.28	Secure coding	7.6	SR 3.4 – Software and information integrity
		7.7	SR 3.5 – Input validation
8.29	Security testing in development and acceptance	7.5	SR 3.3 – Security functionality verification
		7.5.3.1	SR 3.3 RE 1 – Automated mechanisms for security functionality verification
		7.5.3.2	SR 3.3 RE 2 – Security functionality verification during normal operation

demand close coordination among multiple stakeholders. Selecting a framework or standard can be challenging, considering the excess of security standards, the resulting security controls fragmentation and the complexity of implementing the standards across different domains.

When organizations are mandated to comply with several standards, they may end up implementing redundant or conflicting security controls. In order to overcome this challenge, organizations can focus on identifying duplicated controls to simplify the process and minimize expenses. However, mapping controls between standards can be a difficult task because controls are written in various ways, with some being written at a high-level, while others have low-levels requirements and some may even contain ambiguous requirements that require careful examination. Another challenge or common mistake is addressing cybersecurity on a system-by-system basis. Consequently, the security perspective of the entire system, including its intended use, operational environment, and characteristics, should be evaluated from end-to-end. This approach is recommended by the ISA/IEC 62443 standard for establishing an industrial automation and control system security (IACSs) program. However, implementing a security management program for IACSs based on the ISA/IEC 62443 framework can turn out to be a time consuming exercise. The wide-ranging management system encompassing policies, procedures, and personnel utilizing the IACSs in addition to the IACS itself. It is important to emphasize that industrial automation and control systems are employed across various industries, and it is essential to acknowledge that not all industrial systems and applications should be classified as critical. In fact it is not unusual to use commercial off-the-shelf (COTS) components and consumer products in an industrial environment. In a critical systems these kind of products may not be robust enough from a cybersecurity perspective, but in a non-critical industrial automation setup they might be appropriate to use. Ultimately, cybersecurity remains the art of tolerating imperfection. Despite organizations' best efforts to implement cybersecurity measures, there is always a possibility of vulnerabilities, breaches, and other security incidents. Cybersecurity professionals must constantly adapt and respond to new and emerging threats, and prioritize their efforts based on the level of risk and available resources. In this regard, a framework or standard can be a valuable tool to assess risks, implement mitigation controls, and work in a structured way.

IX. CONCLUSION AND FUTURE WORK

The realm of cybersecurity encompasses a wide range of standards at various levels, including national, international, regional, and industry-specific. These standards can often

be overly generic, complex and hard to follow, neglecting the fact that each organization has its own distinct security needs based on its size and business type. In this study, we performed a comparative analysis between the security requirements and controls across three widely adopted standards, namely ISA/IEC 62443-3-3:2019 which addresses network and system requirements, ISO/IEC 27001:2022 deals with information security management systems and ETSI EN 303 645 v2.1.1 serves as a baseline standard for consumer IoT products. The findings of our study suggest that despite being designed for distinct environments and scopes, these standards exhibit significant similarities in their security requirements and controls. Notably, ISO/IEC 27001:2022 fully encompasses the security provisions outlined in ETSI EN 303645, while it largely covers ISA/IEC 62443-3-3 requirements. The observed gaps between the standards is attributed to the specificity of ETSI 303 645 in providing provisions for devices with limited computing capabilities that do not require complex security solutions, such as those without passwords. In contrast, ISA/IEC 62443-3-3 includes security requirements for critical industrial systems, which demand unique security considerations, resulting in differing security requirements compared to the other two standards. Our study also revealed that ISO 27001:2022 provides controls covering organization, physical, technology, and people security requirements. ETSI focuses on provisions for organization and technology security, while ISA/IEC 62443:2019 places emphasis on physical and technology security requirements. Additionally, the findings show that while all three standards prioritize protection controls, only ISO27001:2022 emphasizes the need for cyber resilience. The standard provides measures for responding to and restoring systems and operations after an attack, which is not adequately covered by the other two standards. Our work holds practical future prospects. By identifying and addressing overlaps and gaps in industrial standards security controls, we can streamline compliance efforts for organizations facing the challenge of adhering to multiple standards simultaneously. This streamlining can save valuable resources, reduce redundancy, and improve overall efficiency in cybersecurity implementation. Moreover, it can promote consistency across different standards, fostering a more integrated and effective cybersecurity framework. Since this case study involves three environment-specific standards, we will expand our efforts in the future to include additional well-established security standards to evaluate potential overlaps. Our goal is to find out a more comprehensive standard that can contribute in addressing the fragmentation issue and reduce the additional cost and effort required when complying with multiple security standards.

APPENDIX

See Tables 5 and 6.

REFERENCES

[1] P. K. Joshi. (2023). *Governance, Risk Management, and Compliance in the Cybersecurity Framework*. Accessed: Jul. 7, 2023. [Online]. Available: https://www.eccouncil.org/cybersecurity-exchange/whitepaper/governance-risk-and-compliance/

[2] C Brooks. (2022). *Alarming Cyber Statistics For Mid-Year 2022 That You Need to Know*. Accessed: Jun. 26, 2023. [Online]. Available: https://www.forbes.com/

[3] ENISA. (2020). *Standards*. Accessed: Jun. 26, 2023. [Online]. Available: https://www.enisa.europa.eu/topics/standards

[4] Alex Leadbeater. *Interview With Alex Leadbeater, Chair of TC Cyber at ETSI*. Accessed: Jun. 26, 2023. [Online]. Available: https://cybersecurity-magazine.com/interview-with-alex-leadbeater-chair-of-tc-cyber-at-etsi/

[5] European Union. (2019).*The EU Cybersecurity Act*. Accessed: Jul. 1, 2023. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2019/881/oj

[6] European Union. (2016). *The EU Network and Information Security (NIS) Directive*. Accessed: Jun. 27, 2023. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[7] European Union. (2022). *NIS 2 Directive*. Directive (EU) 2022/2555. Accessed: Jun. 27, 2023. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[8] European Parliament and Council of the EU. *On the Harmonisation of the Laws of the Member States Relating to the Making Available on the Market of Radio Equipment and Repealing Directive*. Accessed: Jul. 2, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0053&from=E

[9] European Union. (2016). *General Data Protection Regulation*. Regulation (EU) 2016/679. Accessed: Jul. 1, 2023. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[10] ISO/SAE. *Road Vehicles—Cybersecurity Engineering*, Standard ISO/SAE 21434, 2021. [Online]. Available: https://www.iso.org/standard/70918.html

[11] ETSI. (2020). *Cybersecurity for Consumer Internet of Things*. Accessed: Jul. 2, 2023. ETSI EN 303 645v02. [Online]. Available: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[12] ISA/IEC. *Security of Industrial Automation and Control Systems (IACS)-IEC*, Standard ISA/IEC 62443, 2019. [Online]. Available: https://isagca.org/isa-iec-62443-standards

[13] ISO/IEC. *Information Security Management Systems*, Standard ISO/IEC 27001, 2022. [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html

[14] The U.S. Department of Health and Human Services (HHS). (1996). *Health Information Privacy*. Health Insurance Portability and Accountability Act (HIPAA). Accessed: Jul. 7, 2023. [Online]. Available: https://www.hhs.gov/hipaa/for-individuals/index.html

[15] A. Ramirez, A. Aiello, and S. J. Lincke, "A survey and comparison of secure software development standards," in *Proc. 13th CMI Conf. Cybersecurity Privacy (CMI)-Digit. Transformation-Potentials Challenges*, Nov. 2020, pp. 1–6.

[16] L. Shan, B. Sangchoolie, P. Folkesson, J. Vinter, E. Schoitsch, and C. Loiseaux, "A survey on the application of safety, security, and privacy standards for dependable systems," in *Proc. 15th Eur. Dependable Comput. Conf. (EDCC)*, Sep. 2019, pp. 71–72.

[17] *Information Security, Cybersecurity and Privacy Protection—Evaluation Criteria for IT Security*, Standard ISO/IEC 15408-1, 2022. [Online]. Available: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

[18] ISO. *Consumers and Standards: Partnership for a Better World*. Accessed: Jul. 1, 2023. [Online]. Available: https://www.iso.org/sites/ConsumersStandards/6_review_questions.html

[19] Fortinet. *CIA Triad*. Accessed: Jul. 1, 2023. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/cia-triad

[20] G. Mutune. *Top Cybersecurity Frameworks*. Accessed: Jul. 3, 2023. [Online]. Available: https://cyberexperts.com/cybersecurity-frameworks/#2_NIST_Cybersecurity_Framework3

[21] ISO/IEC. *Information Technology, Cybersecurity and Privacy Protection—Cybersecurity Framework Development Guidelines*, Standard ISO/IEC TS 27110, 2021. [Online]. Available: https://www.iso.org/standard/72435.html

[22] (2022). *PCI-Security Standards Council, PCI DSS: V4.0*. Accessed: Jul. 1, 2023. [Online]. Available: https://www.pcisecuritystandards.org/document_library/

[23] Office of Information Security. *Confidentiality, Integrity, and Availability: The CIA Triad*. Accessed: Jul. 1, 2023. [Online]. Available: https://informationsecurity.wustl.edu/items/confidentiality-integrity-and-availability-the-cia-triad/

[24] U.S. IT Governance. *Cybersecurity Standards and Frameworks*. Accessed: Jul. 1, 2023. [Online]. Available: https://www.itgovernanceusa.com/cybersecurity-standards
[25] Gartner. (2022). *Top Trends in Cybersecurity 2022—Vendor Consolidation*. Accessed: Jun. 25, 2023. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2022-09-12-gartner-survey-shows-seventy-five-percent-of-organizations-are-pursuing-security-vendor-consolidation-in-2022
[26] NIST. *The NIST Cloud Federation Reference Architecture*, Standard NIST-SP 500-332, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-332.pdf
[27] *Information Security, Cybersecurity and Privacy Protection—Information Security Controls*, Standard ISO/IEC 27002, 2022. [Online]. Available: https://www.iso.org/standard/75652.html
[28] *Industrial Communication Networks—Network and System Security*, Standard ISA/IEC 62443-3-3, 2019. [Online]. Available: https://www.nen.nl/en/nen-en-iec-62443-3-3-2019-en-258484
[29] *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Standard NIST 800-37r2, 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
[30] *Information Technology—Security Techniques—Privacy Framework*, Standard ISO/IEC 29100, 2020. [Online]. Available: https://www.sis.se/api/document/preview/80022590
[31] ISACA. (2019). *COBIT—Control Objectives for Information Technology*. COBIT 5 Framework. Accessed: Jul. 1, 2023. [Online]. Available: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoCDEA0
[32] OUSD(A&S) and United States DoD. *Cybersecurity Maturity Model Certification (CMMC 2.0)*. Accessed: Jul. 1, 2023. [Online]. Available: https://www.acq.osd.mil/cmmc/
[33] J. E. Wynn. *Threat Assessment and Remediation Analysis (TARA)*. Accessed: Jul. 1, 2023. [Online]. Available: https://www.mitre.org/news-insights/publication/threat-assessment-and-remediation-analysis-tara
[34] Australian Cybersecurty Center. *IoT Code of Practice: Guidance for Manufacturers*. Accessed: Jul. 1, 2023. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/publications/iot-code-practice-guidance-manufacturers
[35] Open Web Application Security Project (OWASP) Foundation. (2021). *OWASP Application Security Verification*. Accessed: Jul. 1, 2023. [Online]. Available: https://github.com/OWASP/ASVS/raw/v4.0.3/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.3-en.pdf
[36] *Security and Privacy Controls for Information Systems and Organizations*. Standard NIST.SP.800-53r5, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
[37] Verband der Elektrotechnik, Elektronik und Informationstechnik. (2020). *IT-Security for Industrial Automation—Recommendations for the Implementation of Security Properties for Components, Systems, and Equipment*. VDI/VDE 2182. Accessed: Jul. 1, 2023. [Online]. Available: https://www.vdi.de/en/home/vdi-standards/details/vdivde-2182-blatt-4-it-security-for-industrial-automation-recommendations-for-the-implementation-of-security-properties-for-components-systems-and-equipment
[38] The United Nations Economic Commission for Europe (UNECE). (2000). *World Forum for Harmonization of Vehicle Regulations*. UNECE WP29. Accessed: Jul. 1, 2023. [Online]. Available: https://unece.org/transport/vehicle-regulations/world-forum-harmonization-vehicle-regulations-wp29
[39] New Zealand. (2020). *Privacy Act*. Accessed: Jul. 1, 2023. [Online]. Available: https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html
[40] N. M. Karie, N. M. Sahri, W. Yang, C. Valli, and V. R. Kebande, "A review of security standards and frameworks for IoT-based smart environments," *IEEE Access*, vol. 9, pp. 121975–121995, 2021.
[41] K. M. Caramancion, Y. Li, E. Dubois, and E. S. Jung, "The missing case of disinformation from the cybersecurity risk continuum: A comparative assessment of disinformation with other cyber threats," *Data*, vol. 7, no. 4, p. 49, Apr. 2022.
[42] C. Shearon, "The new standard for cybersecurity," in *Proc. Pan Pacific Microelectron. Symp. (Pan Pacific)*, 2020, pp. 1–9.
[43] P. Wagner, G. Hansch, C. Konrad, K.-H. John, J. Bauer, and J. Franke, "Applicability of security standards for operational technology by SMEs and large enterprises," in *Proc. 25th IEEE Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, vol. 1, Sep. 2020, pp. 1544–1551.
[44] H. Taherdoost, "Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview," *Electronics*, vol. 11, no. 14, p. 2181, Jul. 2022.
[45] J. Srinivas, A. K. Das, and N. Kumar, "Government regulations in cybersecurity: Framework, standards and recommendations," *Future Gener. Comput. Syst.*, vol. 92, pp. 178–188, Mar. 2019.
[46] ENISA, "Standardization in support of the cybersecurity certification," Eur. Union Agency Cybersecur., Greece, Dec. 2019.
[47] European Commission. *Internal Market, Industry, Entrepreneurship and SMEs: Harmonised Standards*. Accessed: Jul. 1, 2023. [Online]. Available: https://single-market-economy.ec.europa.eu/single-market/european-standards/harmonised-standards_en
[48] T. Carpenter, "9—Electronic publishing standards," in *Academic and Professional Publishing*. U.K.: Chandos Publishing, 2012, pp. 215–241.
[49] CEN-CENELEC. *The European Committee for Standardization and the European Committee for Electrotechnical Standardization*. Accessed: Jun. 25, 2023. [Online]. Available: https://www.cencenelec.eu/
[50] European Commission. *Harmonised Standards*. Accessed: Jul. 7, 2023. [Online]. Available: https://single-market-economy.ec.europa.eu/single-market/european-standards/harmonised-standards_en
[51] European Union. *Official Journal of the European Union (OJEU)*. Accessed: Jul. 6, 2023. [Online]. Available: https://eur-lex.europa.eu/homepage.html
[52] B. Shojaie, H. Federrath, and I. Saberi, "The effects of cultural dimensions on the development of an ISMS based on the ISO 27001," in *Proc. 10th Int. Conf. Availability, Rel. Secur.*, Aug. 2015, pp. 159–167.
[53] M. Siponen and R. Willison, "Information security management standards: Problems and solutions," *Inf. Manag.*, vol. 46, no. 5, pp. 267–270, Jun. 2009.
[54] Center for Internet Security. *CIS Critical Security Controls Version 8*. Accessed on: Jun. 25, 2023. [Online]. Available: https://www.cisecurity.org/controls/v8#v8-mappings
[55] E. T. Feteris, "The pragma-dialectical analysis and evaluation of teleological argumentation in a legal context," *Argumentation*, vol. 22, no. 4, pp. 489–506, Nov. 2008.
[56] O. Pollicino, "Legal reasoning of the court of justice in the context of the principle of equality between judicial activism and self-restraint," *German Law J.*, vol. 5, no. 3, p. 289, 2004. [Online]. Available: http://www.germanlawjournal.com/index.php?pageID=11&artID=402
[57] (2018). *NIST Cybersecurity Framework*. NIST CSF 1.1. Accessed: Mar. 22, 2023. [Online]. Available: https://www.nist.gov/cyberframework/online-learning/five-functions

FATIHA DJEBBAR (Member, IEEE) received the B.Sc. and M.Sc. degrees in computer science from the University of Quebec, Canada, and the Ph.D. degree in signal and image processing from the University of Bretagne Occidental, Brest, France. She is currently a Senior lecturer with Högskolan Väst, Sweden. Prior to this role, she was a cybersecurity product compliance specialist in Sweden. Her general research interests include network security, the IoT security, information security, digital forensics, and cybersecurity, in particular cybersecurity risk assessment, privacy preserving techniques, and cyber physical system protection.

KIM NORDSTRÖM received the B.Sc. degree in computer science from the Arcada University of Applied Sciences, Helsinki, Finland, the M.Sc. degree in business administration from Åbo Akademi Univerisity, Turku, Finland, and the master's degree in law from the University of Turku, Finland. He is currently a cybersecurity product compliance specialist in Sweden. He holds CISA and CISM CRISC certificates in cybersecurity.

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 28 October 2022, accepted 16 November 2022, date of publication 18 November 2022,
date of current version 28 November 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3223440

RESEARCH ARTICLE

CyberTOMP: A Novel Systematic Framework to Manage Asset-Focused Cybersecurity From Tactical and Operational Levels

MANUEL DOMÍNGUEZ-DORADO[1], JAVIER CARMONA-MURILLO[2], DAVID CORTÉS-POLO[3], AND FRANCISCO J. RODRÍGUEZ-PÉREZ[2]

[1]Department of Information Systems and Digital Toolkit, Public Business Entity Red.es., 28020 Madrid, Spain
[2]Department of Computing and Telematics Engineering, Universidad de Extremadura, 10003 Cáceres, Spain
[3]Department of Signal Theory and Communications and Telematics Systems and Computing, Rey Juan Carlos University, Móstoles, 28933 Madrid, Spain

Corresponding author: Manuel Domínguez-Dorado (manuel.dominguez@red.es)

This work was supported in part by Project TED2021-131699B-I00 and Project MCIN/AEI/10.13039/501100011033; in part by the European Union NextGenerationEU''/The Recovery, Transformation and Resilience Plan (PRTR); and in part by the Regional Government of Extremadura, Spain, under Grant GR21097.

ABSTRACT Currently different reference models are used to manage cybersecurity, although practically none are applicable ''as is'' to lower levels as they do not detail specific procedural aspects for them. However, they urge organizations to develop a methodological foundation to manage cybersecurity at those levels. Although they allow organizations to adhere to a recognized standard at the strategic level, this advantage vanishes when organizations must define specific low-level procedures, allowing the appearance of inconsistency at tactical and operational levels between departments of the same organization or between organizations. The design of these elements with the required holism and homogeneity is difficult, and this is why generic processes focused on getting certified regarding a standard are usually originated, but they are insufficient to obtain effective cybersecurity because they are not focused on dealing with real cyber threats. Because of the great responsibility of lower levels to achieve effective cybersecurity, this lack of methodological definition makes it difficult to adapt cybersecurity to the highly dynamic cyber context with the required holism and strategic alignment. Our proposal provides CyberTOMP, a process for managing cybersecurity at lower levels, as well as a set of methodological elements that support it. The novelty of these contributions is that they complement the strategic standard selected by the organization, providing it with a set of procedural elements ready to be used out of the box, contributing those aspects required by high-level frameworks to manage cybersecurity at lower levels, for which there is no alternative with a managerial approach.

INDEX TERMS Business asset, cybersecurity management, cybersecurity metrics, cyber threats, CyberTOMP, holistic cybersecurity, strategic alignment, tactical and operational cybersecurity, unity of action.

I. INTRODUCTION

Currently, various approaches to the security aspects of the digital world coexist. These strategies correspond to different organizations' digital evolution stages from decades ago to the present. Over time, the organizations' degree of digitization has increased, causing their most relevant assets at those moments to have been affected by a different threat context and, therefore, have required a specific risk analysis and a particular way of dealing with them. Depending on the specific stage, we can use an information technologies *(IT)* security approach [1], [2], an information security approach [3], [4], [5] or a cybersecurity approach [6], [7] among the main ones.

A. EVOLUTION TOWARDS A CYBERSECURITY APPROACH

Around the decades of the fifties and sixties, under an IT security approach, the most important organizations asset was the technology itself; this was a time when the cost of the first

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

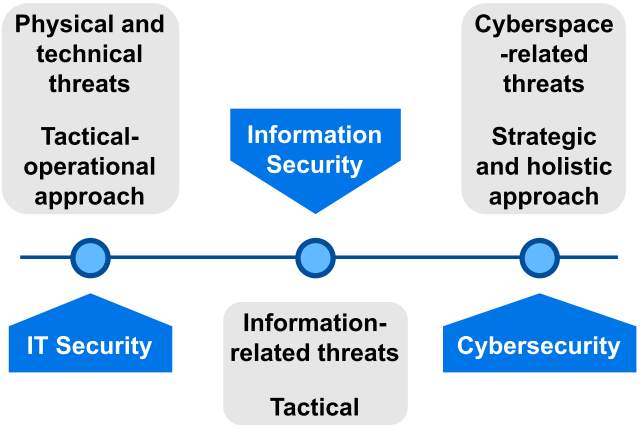


FIGURE 1. From IT security to Cybersecurity. Moving from a single-departmental approach to an organization-wide approach.

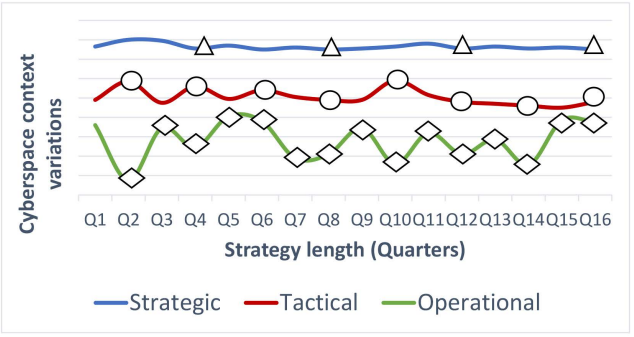


FIGURE 2. Cybersecurity checkpoints agenda at different levels during a four-years strategy. The tactical and operational levels must deal with the greatest variations of the cyber threats context. These variations are often hidden to higher levels due to the observation of variables that do not correctly reflect variations in the short and medium term.

mainframes constituted a large investment. The associated risks were mainly circumscribed to the technical and physical spheres and were addressed by most technical departments within the organizations. As information systems evolved, the value provided by the information increased, transforming it into a highly valued asset and forcing organizations to adapt their strategies towards an information security approach. Different departments that owned that information began to be involved in managing and handling the risks associated with it. They started to understand the threats that could affect the information and, by extension, the normal development of their own activities.

This paradigm has been prevailing for many years and is still used as the main approach in many organizations today. However, with the irruption of cyberspace, the information security approach has become insufficient. Cyberspace, understood as a set of interconnected information systems through communication networks in which people and entities interact and accomplish their activities, has unique characteristics: high dynamism; it is a common playing field where each organization controls only part of it; it has a high dependency on third parties; it requires the focus to be placed not so much or not only on information, but also on the continuity of business processes/assets; there is a need for cyber resilience, etc.

Parallel to the massive adoption of cyberspace, a set of specific threats has emerged that can potentially affect the capability of organizations to develop their activities, interact with third parties, and even preserve their image, reputation, and the trust vested in them. To deal with this evolution (fig. 1), with an increasing cyber threat context, the only approach to properly manage the current cyber risks and cyber threats is cybersecurity, mistakenly understood as information security synonymous on many occasions [8], [9]. This is not only because of cyberspace features but also because the greater digital dependency of organizations on cyberspace has brought to light new vital organizational assets, affected by cyber threats, which cannot be analyzed easily by employing an information security approach [10]: reputation, trust placed by third parties, people's physical integrity, supply chains, the organization's capabilities, Internet of Things *(IoT)* specific threats [11], etc.

Cybersecurity requires unity of action from the whole organization, leadership from strategic levels [12] and a high degree of holism [13], from its conception to its practical application, focusing on business assets [14]. It demands a proactive attitude that takes into account the response and recovery from cyber incidents as well as business continuity [15], aspects that must be managed throughout the entire life cycle, carefully considering the critical success factors to achieve effective cybersecurity [16].

B. RESPONSIBILITY OF TACTICAL AND OPERATIONAL LEVELS IN CYBERSECURITY

The main standards and reference models used for cybersecurity provide guidelines for its evaluation, although this is a high-level evaluation. This implies that variations in the state of cybersecurity can only be measured at the strategic level in the medium/long term. In scopes other than cybersecurity, assessing within such periodicity might be acceptable if the context is not very changing and significant corrective or adaptive actions are not frequently required. Under these circumstances, high-level assessments and corrections may be sufficient to maintain the state of the organization aligned with strategic goals.

However, this does not occur in the field of cybersecurity. Cyberspace and its associated cyber threat context evolve very dynamically, intensely, and frequently. For this reason, most corrective or adaptive actions, as well as the measurement of their effects, must be carried out in the medium/short term, that is, at tactical and operational levels within the organization. Thus, a large part of the responsibility for preserving the cybersecurity state aligned with an organization's cybersecurity strategy falls on them, who are also responsible for maintaining the unity of action and the holistic approach required by cybersecurity. Accomplishing these requirements from lower levels that are distributed

throughout the organization in several departments and areas that usually operate as silos and have different chains of command is very difficult.

Regrettably, the aforementioned standards and frameworks do not supply these levels, out of the box, with detailed methodological elements to help them manage and evaluate cybersecurity; neither do they provide standardized mechanisms to maintain the strategic alignment nor to quickly detect new cyber threats and nimbly apply the necessary actions to deal with them (fig. 2). Consequently, it cannot be taken for granted that these levels have the necessary mechanisms to carry out this work for the mere fact that the organization has adhered to a high-level standard in the strategic sphere.

C. CONTRIBUTIONS OF OUR WORK

From the current state-of-the-art, which we detail in later sections, needs are identified in the frameworks commonly used to manage cybersecurity. They are defined at a strategic, level and almost all urge organizations to develop a methodological base to be used in cybersecurity management at lower levels so that the cybersecurity strategy can be broken down and transferred correctly to the whole organization. As explained in the previous paragraphs, and we will expand on it in the article, we understand that the responsibility of these levels in the management of cybersecurity is relevant, but it encounters a series of challenges derived, on the one hand, from these aspects not covered by high-level frameworks and on the other hand by the structural rigidity of many organizations. Using any of the existing high-level frameworks, organizations can adhere to a widely recognized standard at the strategic level. But by having to define their own cybersecurity management process and procedures for the lower levels of the organization, this advantage, in a way, vanishes, inducing inconsistency between different organizations or even within different departments and functional areas of the same organization at tactical and operational levels.

Defining these elements is not always simple; it is almost never homogeneous and seldom consider cyber threats, but simply organizational aspects. On more occasions than is recommended, the difficulty in developing methodological elements for the tactical and operational levels leads to generic processes and procedures that are sufficient to obtain a certification with respect to the selected strategic framework, but insufficient to obtain effective cybersecurity.

Our work provides CyberTOMP as a means of managing cybersecurity at the tactical and operational levels, as well as a set of methodological elements, knowledge bases and concepts on which it is based. They are designed to complement the standard selected by the organization in the strategic sphere, providing it with a set of processes and procedures ready to be used out of the box. They contribute aspects required by the methodological guidelines of the high-level framework and by the organization to manage cybersecurity at tactical and operational level, levels for which there is no alternative with a managerial approach. Our proposal constitutes a procedural and methodological solution and not a technical one. Specifically, our proposal supplies lower levels with:

- Mechanisms to manage cybersecurity at tactical and operational levels, regardless of the higher-level standard or framework adopted by the organization, are thus a complement and not a disruptive element.
- A set of techniques and metrics focused on business assets to quantitatively and homogeneously assess cybersecurity, at different levels and degrees of aggregation.
- A homogeneous set of expected cybersecurity outcomes that arises from the analysis and combination of well-recognized international sources.
- The capability to maintain alignment with the cybersecurity strategy, under a holistic approach, from the tactical and operational levels, engaging all functional areas involved in the process.
- Procedures to incorporate the dynamic variations of the real cyber threats context, in an agile way, into cybersecurity daily grinds.

D. ORGANIZATION OF THIS DOCUMENT

The remainder of this work is organized as follows: in section II, the aspects found in the current state of the art that must be overcome to achieve effective cybersecurity management at low levels of the organization, are identified; in section III the methodological elements, knowledge bases and concepts developed in our proposal as support for the practical application of cybersecurity management at tactical and operational levels, are described; the section IV defines and describes in detail the CyberTOMP, our core contribution that, based on the rest of the elements detailed in section III, allows the organization to manage cybersecurity at tactical and operational levels; in this section recommendations and guidelines for its practical application are proposed as well.

II. STATE OF THE ART AND PROBLEM STATEMENT

From a theoretical perspective, the adoption of a cybersecurity approach does not have apparent complexity. However, based on the current standards commonly used for cybersecurity at a strategic level, there are different aspects that hinder its practical adoption in organizations when it is applied from lower levels, especially considering the differentiating characteristics of cybersecurity with respect to previous approaches and the need to change the way it is addressed [17]. In the following subsections we identify the current problems that our proposal addresses.

A. LACK OF HIGH-LEVEL STANDARDS THAT PROVIDE PROCEDURAL ELEMENTS FOR TACTICAL AND OPERATIONAL LEVELS

There are many frameworks and standards that can be useful, in certain cases, to manage cybersecurity [18], which sometimes makes it difficult to choose one and implement it in organizations [19]. A large number of them, such

as Capability Maturiry Model Integration *(CMMI)* [20], [21], [22] or Information Technology Infrastructure Library *(ITIL)* [23], [24] are generic and applicable to multiple spheres. When applied to cybersecurity, they can contribute to managing it. Some even contain elements related to security in the digital field [25]. However, they are, in no case, specific models for cybersecurity, so their advantages are very limited in this regard [26], in addition to being defined at a very high level [27].

Other frameworks and standards are focused on information security management, not on cybersecurity, for instance, the ISO 27000 family of standards [28], [29], the Model of Indicators for the Improvement of Cyber Resilience *(IMC)* [30], [31] or even the Spanish National Security Scheme *(ENS)* [32], [33], [34], [35]. They are commonly used to address cybersecurity, although they are based on or bear a clear perspective of information security and do not properly cover the specific aspects of the cybernetic context; therefore, they do not allow, *per se*, meeting the requirements of a cybersecurity model.

To conclude, there are other works, such as the one developed by MITRE in the Adversarial Tactics, Techniques and Common Knowledge matrix *(ATT&CK©)* [36], [37] (used in various works on threat intelligence [38], [39]), the Critical Security Controls for Effective Cyber Defense *(CSC)* [40], [41] from the Center for Internet Security *(CIS)*, even with its shortcomings [42], the Open Web Application Security Project *(OWASP)* Top 10 project [43], [44], the Community Defense Model *(CDM)* [45] from the CIS, that aligns the CSC to cover the threats documented by MITRE, helping to implement the mitigations that it proposes [46] or those known as nine D's of cybersecurity described in [47] (so called because they are recommendations that all begin with this letter). All of them are sets of recommendations, good practices and specific tools for cybersecurity, which are very useful but disconnected from a comprehensive framework that covers all organizations' levels.

Among the analyzed models, the Framework for Improving Critical Infrastructure Cybersecurity [48], [49], from the National Institute of Standards and Technology *(NIST)* stands out. It is a complete framework for cybersecurity that is accompanied by the SP-800 series of guides [50] (where guide SP-800-53 [51] can be especially highlighted), which provides the organization with high levels of cyber resilience under a cybersecurity approach. This framework in conjunction with the Cybersecurity Maturity Model *(CMM)* [52], [53] also allows the evaluation of third parties that must be part of the organization's supply chain. There are other less common models as, for example, the one developed in [54], [55] which focuses on the managerial aspects of cybersecurity to protect critical infrastructure. It is defined at a very high level of abstraction and does not provide procedural elements for direct application. However, it provides a modern view that cybersecurity is not only related to technical domains but also involves the whole organization.

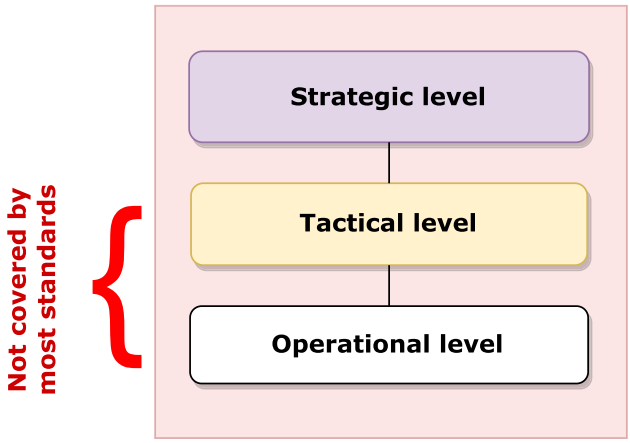


FIGURE 3. It is necessary to provide the tactical and operational levels with homogeneous methodological tools for cybersecurity management.

There are published works that focus on cybersecurity very applied to specific and particular cases. A deeper literature review and an analysis of the body of knowledge in the field of cybersecurity can be found in [56], [57], [58], [59], [60], and [61], for general cases and also specific ones. They generally follow technical approaches that do not address organizational cybersecurity from a procedural perspective. But it is also important to study the problem from the managerial point of view within the current standards and new contributions such as the one we will describe in this paper.

Nevertheless, none of these frameworks or initiatives, and even the NIST framework, includes a detailed methodological description of how cybersecurity should be managed at the organization's tactical/operational levels. This means that none of them are applicable without being complemented, since cybersecurity must be administered on many occasions from these levels (fig. 3). It is the responsibility of each organization to design the set of processes and procedures indicated by these frameworks for their lower levels.

By not including specific standardized guidelines, the tactical/operational application of these models can be completely different between organizations, between areas within the same organization, or it cannot even take place.

There are several factors why an organization could choose to use them even though they are not fully defined options to address cybersecurity at all levels of the organization: because they are certifiable standards that allow positioning against competitors, because they are widespread and finding workers trained in them is easier, because they are required by third parties to access contracts, or because they are mandatory rules according to the legal framework surrounding the organization. For these reasons, replacing these frameworks in the organization is not always an option, but they should be complemented to provide them with what they lack. They should be provided with methodological elements that apply at the

lowest levels to address the deficiencies in this area. Hence, it is necessary to provide tactical and operational levels with homogeneous cybersecurity management mechanisms that allow them to adapt to the cyber threat context and maintain alignment with the strategic cybersecurity objectives.

In [62], a use case in Portugal for the implementation of information security actions in a group of SMEs was explained in detail. Some aspects of this work are similar to those adopted in our proposal: a set of information security controls from a recognized standard, which have been grouped into different groups of controls to respond to different needs. Subsequently, the characterization of each control depends on the type of organization and other aspects.

However, this very well-prepared work has, in our opinion, some limitations. It is based on the ISO 27001 standard, a standard for information security and not for cybersecurity. At the procedural level, it does not detail the elements of management, processes and procedures used at tactical and operational levels to coordinate the efforts of the organization's workforce. This is most likely because their destination is small and medium-sized companies, where this distinction between levels makes perhaps less sense.

Paraphrasing the conclusions of the authors of this work: *However, ISO-27001:2013 is a single tool for achieving the project goal and it can be seen as a limitation in this study. In that sense, other best practices and frameworks should be addressed, implemented, and compared.*

In our work, we present a wider solution based on several standards and initiatives specific to cybersecurity and not information security. It also contributes the required processes, procedures and metrics to be used out of the box that can be applied to tactical and operational levels.

B. LACK OF MECHANISMS TO PROVIDE HOLISM FROM LOWER LEVELS

Cybersecurity requires something that, until now, none of the previous approaches related to digital security required [63]: a holistic approach, promotion from the strategic levels to the whole organization, unity of action to address cybersecurity risks, and proactive mindset and focus on cyber incident response and recovery tasks.

Since a large part of the initiative in cybersecurity must be driven at tactical and operational levels, the interdepartmental coordination required to provide a holistic approach must also be addressed from these levels.

Notwithstanding, the areas or units that compose these levels do not have direct visibility, communication, and coordination between them, and usually work under different chains of command in isolated silos. Habitual conflict escalation mechanisms are useful for inter-area communication in specific situations, but not for managing the daily grinds at lower levels. Under these circumstances, it is difficult for lower levels to achieve the coordination, unity of action, and holistic and proactive vision required by cybersecurity (fig. 4).

This situation is amplified when the organization is more distributed in silos. In any event, this communication is

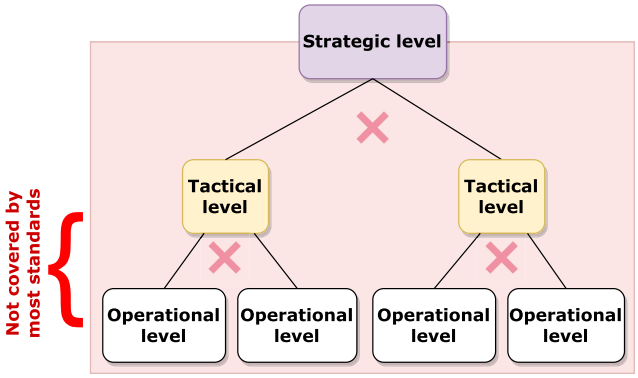


FIGURE 4. The distribution of the organization in silos hinders a fluent communication and collaboration between functional units and the achievement of the holism and unity of action required by a cybersecurity approach.

fundamental because people from different functional areas of the organization must agree on the actions they have to implement, on the metrics that will affect them, on the weight and responsibility that each one will have with respect to the cybersecurity of business assets, and so on. This should not be done independently but jointly, coordinated, taking advantage of existing synergies and forming a team.

For these reasons, it is necessary to provide these levels with tools that ensure that they can design and execute joint cybersecurity actions proactively, quickly, with holistic vision and unity of action; avoiding the appearance of conflicts despite the distribution of teammates among several functional areas.

C. LACK OF HOMOGENEOUS CYBERSECURITY EVALUATION CRITERIA

What has not been measured cannot be improved. This statement, extrapolated to cybersecurity, implies the need to evaluate the effectiveness of cybersecurity controls [64] and safeguards, from a holistic and multidisciplinary perspective, and offer a shared vision of the organization's cybersecurity posture.

When people from different functional areas collaborate to ensure the cybersecurity status of business assets and meet strategic cybersecurity objectives, there is a need to measure progress [65] because this allows continuous decision-making at different levels [66], [67]. But current standards and frameworks define neither measurement mechanisms nor assessment criteria that can be used by tactical and operational levels to fit this need, aspects with which all the parties should agree, and that allow focusing on solutions and not on resolving the differences around the assessment process itself. Otherwise, several discrepancies and conflicts will tend to arise between the areas co-responsible for cybersecurity, which prevents having a clear vision of their real cybersecurity state.

When different organization units, follow non-identical assessment criteria to evaluate the same element

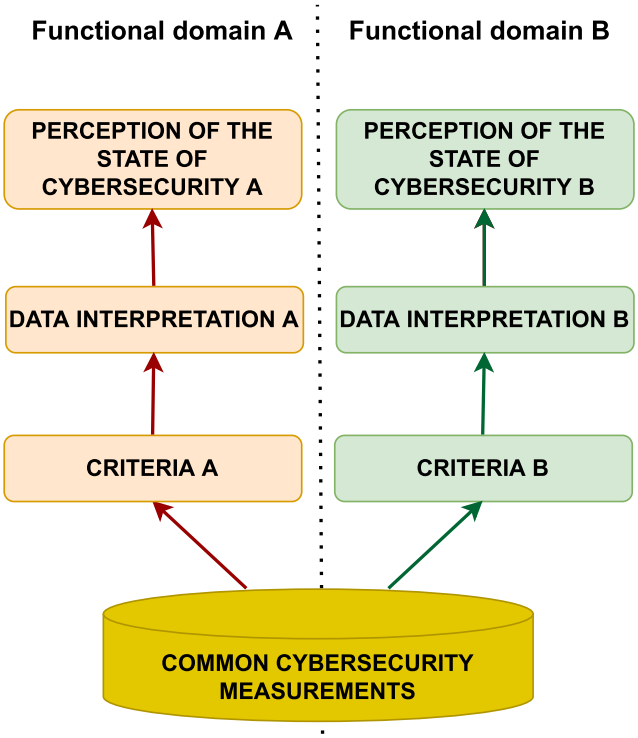


FIGURE 5. Silos in organizations frequently imply the existence of different criteria and disjointed interpretations of the real state of cybersecurity, even when the same data is valued. A common standard should be defined for the evaluation of cybersecurity at these levels.

(cybersecurity in this case), it is likely that none of these evaluations coincide with the rest (fig. 5) unless they share a common vision, which is a common way of interpreting the measurements, leading to a lack of coordination in cybersecurity due to different perceptions. For these reasons, it is necessary to have standardized and homogeneous tools that provide a common shared measurement of the performance and state of cybersecurity at these levels, and also allow quantitative evaluation of the effectiveness of the implemented actions for decision-making in the short and middle terms.

III. TOOLKIT TO SUPPORT CYBERSECURITY MANAGEMENT FROM TACTICAL-OPERATIONAL LEVELS

After a review of models and initiatives commonly used to manage cybersecurity, we designed a proposal that combines the existing elements that may be useful for the purpose of our work with other specific elements designed in our study that complete it to address all the needs identified in Section II. We have always tried that our solution consists of an evolution or a combination of fundamentals already consolidated and accepted, and not of a theoretically excellent proposal but difficult to run in practice by any organization. In addition, special emphasis has been placed on keeping the solution limited to management at lower levels (tactical/operational), assuming that the organization will have specific frameworks for managing at higher levels (strategic/tactical), although

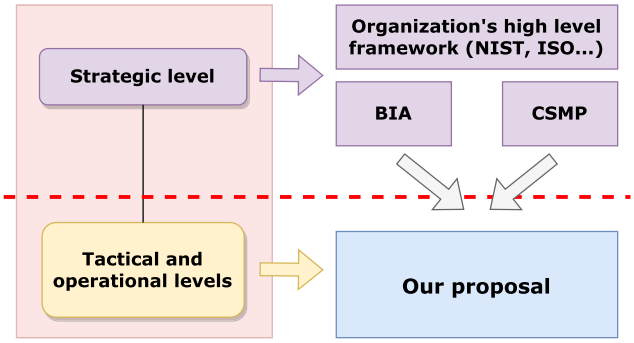


FIGURE 6. BIA and CSMP, both slightly modified, connect the organization's strategic framework to our proposal for tactical and operational levels.

perhaps they may not be appropriate "as is" for cybersecurity management, as explained in Section II.

In the following paragraphs, every decision and auxiliary solution that makes up our proposal will be discussed, justifying the reasons for it.

A. CONNECTING OUR PROPOSAL WITH THE CORPORATE STRATEGY

In our proposal, we chose to minimize the dependence on the high-level framework used at the strategic level to ensure its applicability in different organizations while guaranteeing that it serves as a cybersecurity management tool at tactical and operational levels of the organization and maintain alignment with the corporate strategy from these levels. However, a method is needed to connect and align the activity of lower levels towards the strategy. For this, we propose to use two elements present in almost any medium-sized organization, regardless of the regulatory framework to which they have adhered: the Business Impact Analysis *(BIA)* and the Cybersecurity Master Plan *(CSMP)*, or the set of cybersecurity projects, if applicable, that come from the application of the framework used at strategic levels (fig. 6).

1) BIA REQUIREMENTS FOR ASSET FOCUS AND BUSINESS CONTINUITY

The concept of business continuity refers to the ability of an organization to identify threats that can become disruptive events that affect its activity, and plan the response and recovery in advance to guarantee the normal development of business activities [68], [69]. The greater this capacity, the more resilient is the company.

It is not a new concept, nor is it solely focused on cybersecurity. An entity could be affected by multiple events; some recent events such as the lock-down suffered by the COVID-19 pandemic, but also natural disasters, labor conflicts, lack of qualified workers, events linked to information security, or cybersecurity incidents.

The requirements for cybersecurity are in many ways similar to the requirements for ensuring business continuity: holistic view; impulse from the strategic level to the entire

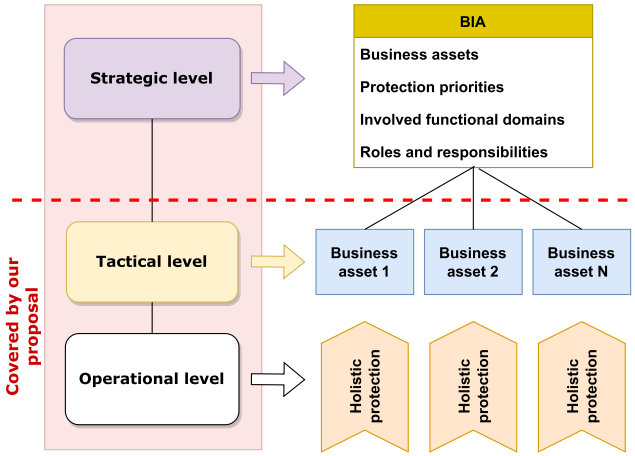


FIGURE 7. Using the BIA to connect the strategic level to the lower ones provides this proposal with the capability of integrating cybersecurity-related business continuity requirements and a focus on the business assets in the daily cybersecurity grinds.

organization; unity of action in crisis management; proactive approach; development of plans to respond and recover in the face of different situations and actions that reduce the impact when crises break out. Therefore, with organizations making massive use of cyberspace and with a great dependence on this medium, cybersecurity, correctly put into practice, contributes significantly to business continuity in crisis situations caused by cybersecurity incidents [70].

In their business continuity management, it is common for organizations to carry out the BIA [71], generating a document in which the organization details aspects such as the critical business processes, the assets on which these processes depend, the criticality of each one, the maximum tolerable interruption times, or the tolerable recovery times. The BIA is, therefore, a strategic declaration of intent coming from the highest level of the organization, where it is evaluated and indicated which assets to protect (and recover, where appropriate) and with what intensity, to ensure that the impact of a crisis on the overall business is as small as possible. It is also common for BIA to define roles, responsibilities, strategies, communication mechanisms, etc. for all areas, and for cybersecurity.

Our proposal provides mechanisms that allow organizations to align cybersecurity with business continuity requirements, as the maximum expression of the organization's survival needs. In particular, at tactical and operational levels, which are often the executors of recovery actions. However, business continuity associated with cybersecurity, expressed as a whole, is difficult to understand at operational and tactical levels. It is too broad and difficult to manage and, therefore, difficult to understand, communicate, and plan at those levels. For this reason, the first decision in our proposal is the application of the "divide and conquer" paradigm to have a smaller and more manageable scope at such levels. In addition, it is more understandable, allowing greater cohesion between the multidisciplinary and holistic operational team in charge of its cybersecurity and continuity.

Since the BIA identifies and prioritizes the business assets that support the organization's activity, we propose focusing cybersecurity efforts on them [72] and assign them as a basic unit at the tactical and operational levels for their cyber protection, understanding that this element is sufficiently manageable at these levels.

Each organization develops a BIA according to its needs, although it is common for a BIA to include information relevant to the business. Nevertheless, to provide it with the utility intended in this work, the BIA must include at least:

- Identification of business assets.
- Functional areas responsible for business assets and those that depend on their results.
- Continuity strategies for different crisis scenarios.
- The parameters in which business assets can be discontinued without generating a disproportionate impact, and therefore, the levels of this discontinuity acceptable to the organization.
- The impact on the business in the event of a discontinuity that extends beyond the parameters considered acceptable by the organization.
- A map of high-level dependencies between the different business assets.
- Based on the above, prioritization that reflects the protection required by business assets. On a scale of three values, LOW, MEDIUM, and HIGH.

In this way in our proposal, the BIA becomes one of the two points of interconnection between the strategic area of the organization and the rest of the lower levels (fig. 7). This provides the following four main strengths for cybersecurity:

- This allows for a more manageable and understandable scope for lower levels of the organization.
- Allows maintaining the focus on the business asset and its derivative assets.
- It allows the integration of business continuity strategies related to cybersecurity in daily activity.
- It allows the incorporation of the risk-based approach (related to business continuity) [73], [74] so that business cyber continuity risk requirements can be introduced in the tactical and operational cybersecurity management cycle.

2) CSMP REQUIREMENTS FOR A STRATEGIC ALIGNMENT

CSMP is a tool commonly used by cybersecurity managers to orchestrate all the needs and context of cybersecurity in a portfolio of cybersecurity programs and projects aligned with the needs of the organization. In this way, the cybersecurity effort and the necessary budget are focused on achieving the organization's strategic cybersecurity objectives and, by extension, the company's business goals.

The design of CSMP includes systematic phases so that it covers all aspects of cybersecurity in an integral way, which allows focusing and optimizing resources to achieve the interests of the company in this area. It includes, among many other aspects, cybersecurity guidelines; strategic

cybersecurity objectives; the definition of high-level cybersecurity controls and safeguards; the definition of cybersecurity architecture, covering all areas where cybersecurity is applicable; the definition of roles, responsibilities, processes, and procedures; the quantification of expenses and investments in cybersecurity, and the high-level planning of cybersecurity actions/projects. This allows an incremental development of the cybersecurity strategy and the achievement of short, medium and long-term goals. From all of the above, which represents a high-level comprehensive plan for cybersecurity management throughout the organization, we would like to emphasize that it is in this CSMP that the framework and regulatory framework related to cybersecurity are defined and the cybersecurity projects required by the organization, as well as the strategic cybersecurity objectives and the specific objectives of each designed project.

Theoretically, CSMP is an optimal tool for providing cybersecurity with a comprehensive vision. However, and this is relevant, during the preparation of this plan, the strategic framework that the organization will use for the direction and management of cybersecurity must be defined, as well as the associated processes and procedures. But if the execution of the CSMP depends on any of the main existing frameworks ''as is'', the problem described in the section II resurfaces, since practically all of the high-level frameworks and standards do not provide methodological tools applicable to tactical and operational levels and focus mainly on the strategic levels; so that even with a CSMP, organizations must develop their processes and procedures to manage cybersecurity at the tactical and operational level. Most of these high-level frameworks indicate that this methodological base should be developed. And this is precisely what our proposal provides. Our proposal can be used to complete the methodological guidelines of high-level frameworks and can be included in the CSMP to be used in cybersecurity management at the tactical and operational levels of the organization.

In our solution, the use of CSMP is proposed as a second point of connection with the strategic level of the organization (fig. 8). To do this, CSMP projects, or cybersecurity projects in the event that there is no properly defined CSMP, must meet certain requirements:

- Every business assets must have their own project in the CSMP. A project may cover more than one asset if its cybersecurity objectives coincide with others.
- These projects must be defined at a high level and specify the objective, but not detail the tactical/operational actions, so that rolling wave planning can be carried out [79] at lower levels as information from the context analysis becomes available. The planning of CSMP projects is therefore simplified.
- The objectives of the indicated projects must be defined based on the cybersecurity metrics and indicators described in our proposal, as developed later in this section.

Building the CSMP as described in our proposal provides four main benefits:

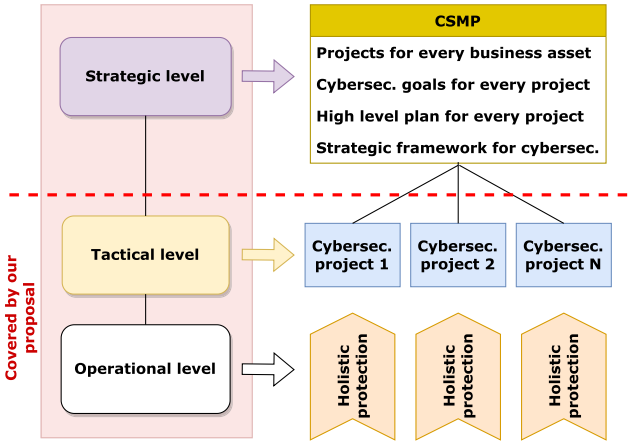


FIGURE 8. Using the CSMP to connect the strategic level to the lower ones provides this proposal with the capability of integrating cybersecurity risks and cybersecurity strategic goals in low levels' activities.

- It allows for more manageable and understandable cybersecurity projects for lower levels of the organization.
- Allows maintaining focus on strategic objectives for business assets and their derivative assets.
- It allows alignment towards the cybersecurity strategy in the daily activity of its management from the lower levels.
- It allows the incorporation of the risk-based approach (related to cybersecurity) [75], [76], [77], [78], so that cybersecurity risks requirements can be introduced in the tactical and operational cybersecurity management cycle.

B. CYBERSECURITY FUNCTIONS FOR BUSINESS ASSETS

With the use of BIA and CSMP as described in our proposal, a multidisciplinary operational team in charge of the cybersecurity of a certain business asset would have a manageable scope. Even so, in our work we propose to make this scope even more manageable to further increase its understanding and facilitate the evaluation of its cybersecurity state. Among the frameworks reviewed in Section II, the most complete and focused on cybersecurity is the NIST cybersecurity framework, which organizes different cybersecurity safeguards in a tree-like manner, very useful, in continuous security functions, categories, and subcategories. The functions provide a high-level strategic view of the cybersecurity risk management process life cycle and their subsequent breakdown into categories, and sub-categories brings this strategic view closer to the tactical and operational levels:

1) **Identify**. This function enables a greater understanding of organization's context to focus and prioritize its efforts in accordance with the risk management strategy and its needs.
2) **Protect**. The purpose is to develop and implement appropriate safeguards and controls to ensure the delivery of critical services. This is the basis for the

subsequent limitation or containment of the impact of a possible cybersecurity incident.

3) **Detect**. The purpose is to develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
4) **Respond**. The purpose purpose is to develop and implement appropriate activities to take action regarding a detected cybersecurity incident. It allows, among other aspects, containing the impact of cybersecurity incidents.
5) **Recover**. Its purpose is to develop and implement appropriate activities to maintain resilience plans and recover any capacity or service affected by a cybersecurity incident. Allows the recovery of the usual activities of the organization.

This functional classification is easily understandable and, following it, a tactical/operational team could focus on different aspects of the cybersecurity of the business asset, which could also be evaluated separately. The identification of specific responsibilities of each functional area of cybersecurity is facilitated and favors the creation of specialized operational subgroups in each of the functions, categories or subcategories. In addition, the ''Response'' and ''Recovery'' functions are closely linked to business continuity and cyber resilience, so they fit very well in cybersecurity focused on business assets from the BIA, as indicated in our proposal.

The subcategories (expected outcomes) and categories defined within the NIST framework [48] contribute hierarchically to the achievement of the objectives of each function on which they depend. Each is traceable to the most relevant regulatory frameworks and initiatives, such as CIS CSC, NIST SP 800-53, ISO 27001, which facilitates coexistence with these standards.

Therefore, we have considered it convenient to reuse this classification in functions, categories, and subcategories in our proposal. The NIST framework will not be used in most strategic aspects in order four our proposal to remain independent of the higher level regulatory framework used in the organization: NIST, CMMI, ISO 27001, ENS, etc.

In the rest of our proposal, it is considered that any activity carried out by tactical and operational teams for the cybersecurity of a business asset must be included in one of the defined cybersecurity functions or in its derived hierarchy.

C. UNIFIED LIST OF EXPECTED OUTCOMES FOR THE CYBERSECURITY OF BUSINESS ASSETS

The finest grain level of the NIST classification is a subcategory. In that model they are also called ''expected outcomes'' which is very appropriate because it reflects that these subcategories are the goals, which are achieved with the operational implementation of the corresponding controls and safeguards. In our proposal, we reuse the NIST definition of ''expected outcomes'' since implicitly this denomination is a proactive requirement for the teams in charge of executing cybersecurity actions, an aspect that we consider essential for modern cybersecurity.

However, the expected outcomes from the NIST framework are not the only source of relevant information clearly focused on cybersecurity, and being a fairly broad set, it is true that it is not updated very frequently. There are other sources that are either updated more frequently or simply supplement NIST's set of expected outcomes. For example, in [36], MITRE identifies cyberattacks observed in the real world and the tactics, techniques, and procedures followed by cyber attackers to carry them out: the *modus operandi*. The main mitigation actions for each case are solso defined. In [40], the CIS details the most critical cybersecurity controls that should be implemented in any organization. For this, it uses what it calls the ''Implementation Group'' (IG), numbered from 1 to 3. IGs are a way to identify groups of controls that need to be implemented together to address existing threats. IG1 controls, once implemented, allow for dealing with a wide variety of cyber threats. The IG2 controls include those from IG1, and the IG3 controls include all. Consequently, depending on the context of the organization and the protection needs it requires, it must implement IG1, IG2, or IG3 controls. IG3 is the most complete and allows for a higher level of cybersecurity against the most complex threats (it also includes the most complex and costly controls). The CIS itself, in [45], calculates the level of coverage of the threats identified by MITRE after the implementation of the different IGs, ranging from 77% of threats in the worst case by implementing IG1 to 95% in the best case, implementing IG3; a relevant coverage in any of the cases. Finally, in [47], a series of recommendations are defined, which are applicable to any cybersecurity scenario and can be very useful for minimizing exposure to cyber threats: the nine D's of cybersecurity.

As expected outcomes will determine what cybersecurity actions operational teams need to take, we consider it essential in our proposal to have an expanded list of expected outcomes that brings together not only information from the NIST framework but also from the cited sources. That is why we have approached this task by thoroughly analyzing these sources and integrating them into a Unified List of Expected Outcomes (ULEO) that:

- Retains the same classification of functions, categories, and subcategories as NIST.
- Groups the expected outcomes in the same implementation groups defined by the CIS, with the same meaning.
- Expands the focus and number of original expected outcomes from the NIST model, including inputs from other complementary or more up-to-date sources.
- Maintains alignment with the work of MITRE, so that the application of each IG allows addressing a certain percentage of cyber threats observed in the real world.

When building the ULEO we have been especially careful in the process of integrating controls from other cybersecurity initiatives, to ensure that this range of threat coverage is not altered downwards. In all cases, stricter controls than those proposed by the NIST have been added or replaced by more extensive controls, but in no case the controls were

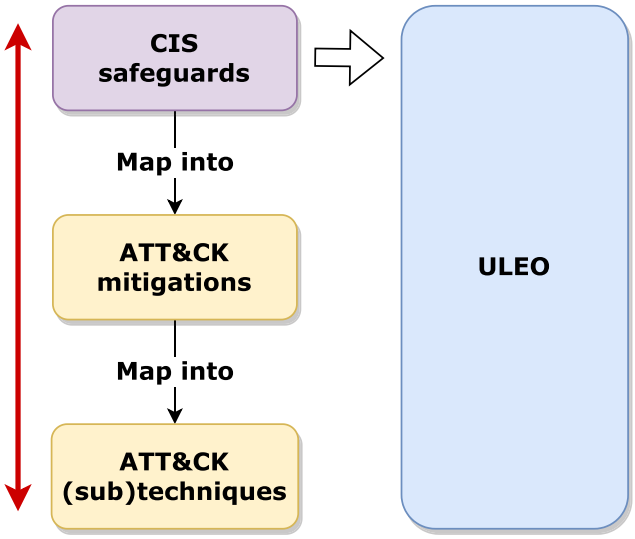


FIGURE 9. Our proposal indirectly incorporates the mitigations and TTPs of MITRE to the ULEO through the inclusion of the corresponding CIS safeguards.

relaxed, which is the reason why these ranges of coverage can be ensured. Therefore, the proposed method maintains or improves the coverage percentages calculated by the CIS in [45].

The following subsections define ULEO and describe the process followed for its analysis and construction.

1) PHASE I. FUSION OF MITRE RECOMMENDATIONS WITH CIS CONTROLS AND NIST SUBCATEGORIES. CREATION OF INITIAL ULEO

The starting point for the construction of ULEO in our proposal is the complete set of functions, categories, and subcategories defined in the NIST framework.

Our proposal does not directly include the mitigations identified by MITRE to address the cyberattacks documented in the ATT&CK©matrix. In [45], the CIS does an excellent job analyzing in depth which of its controls and safeguards allow the implementation of the necessary mitigations to face the Tactics, Techniques and Procedures *(TTPs)* employed in the cyberattacks documented by MITRE. These requirements were grouped into each of the three IGs used in our study. Thus, in our proposal we take advantage of this effort by including the CSCs from CIS which also allows us to indirectly include the needs and requirements identified by MITRE (fig. 9).

In [80], the CIS performed a comparative analysis of the equivalence between the expected outcomes from NIST and CIS CSCs. In our proposal we have taken this initial comparative analysis as a basis, which does not merge elements but rather identifies them, to make the first combination of the expected outcomes of the NIST and CIS CSCs, as follows:

1) Cases where a CIS control or safeguard does not have a related NIST subcategory. In this case, we have that control or safeguard to the list, considering that it complements the NIST model itself, covering cases that it did not consider.
2) Cases where a CIS control or safeguard further defines and completes a similar subcategory within the NIST framework. In this case, we replaced the NIST subcategory with CIS control or safeguard that addresses the same problem, but with greater completeness.
3) Cases in which CIS control or safeguard is defined in less detail and completes a similar subcategory within the NIST framework. In this case, we have maintained the NIST subcategory, ignoring CIS controls or safeguards that address the same problem but with less completeness than NIST.
4) Cases in which CIS controls or safeguards equivalently define a similar subcategory within the NIST framework. In this case, we chose to maintain the NIST subcategory as it addresses the same problem under equal conditions. Choosing an equivalent CIS control or safeguard would not have added or subtracted anything.
5) Cases in which a CIS control or safeguard partially defines a NIST subcategory and vice versa; that is, both NIST and CIS address the same problem, but neither of them does so completely, rather they intersect. In this case, we included both the NIST subcategory and the CIS control or safeguard because both offer a better response to the same problem than either of the two separately.
6) Cases in which a NIST subcategory does not have an equivalent CIS control or safeguard; that is, it is something that only exists within the NIST framework and not within the CIS framework. In this case, we maintained this NIST subcategory because we understand that it provides a security plus.

The previous combination was carried out by analyzing each control, safeguard, and expected outcome, one by one, to identify, after an analysis of the textual description of each item, to which NIST function, category, and subcategory it belonged. In addition, to determine the implementation group it should be placed in. The result of this process is the first version of ULEO.

2) PHASE II. INCORPORATION OF THE NINE D's OF CYBERSECURITY TO THE ULEO

The nine D's of cybersecurity are textual recommendations that lack a classification system. Therefore, in the first place, we have provided each of them with a code that can be shown in Table 1, similar to the functions, categories, and subcategories of the NIST or the controls and safeguards of the CIS in their respective models. We assimilate each of them at the level of a subcategory or expected outcome.

Subsequently, the textual descriptions of each of them were analyzed in the same way that was done with the CSCs of CIS, to identify which function or category of cybersecurity they contribute to. The nine D's of cybersecurity were systematically analyzed with respect to the controls,

TABLE 1. Identifiers assignment for the nine D's of cybersecurity.

ID	Description
9D-1	Deter attacks
9D-2	Detect attacks
9D-3	Drive up difficulty
9D-4	Differentiate protections
9D-5	Dig beneath the threat
9D-6	Diffuse protection throughout the payload
9D-7	Distract with decoys
9D-8	Divert attackers to other targets
9D-9	Depth of defense

safeguards, and subcategories of the initial ULEO previously generated, so that:

1) Cases in which a D does not have a related subcategory in the initial ULEO. We choose to add such D considering that it complements the set.
2) Cases in which a D defines a subcategory of the initial ULEO in a more detailed and complete manner. We decided to replace it with that D which addresses the same problem, but with greater completeness.
3) Cases in which a D defines a subcategory of the initial ULEO in a less detailed or complete manner. We choose to retain this subcategory and not include this D because it addresses the same problem in less depth or detail.
4) Cases in which a D defines a subcategory of the initial ULEO with the same level of detail and depth. We choose to retain this subcategory because they address the same problem under equal conditions. Choosing an equivalent D does not add or subtract anything.
5) Cases in which a D partially defines the same case as a subcategory of the initial ULEO and vice versa, that is, both cases address the same problem, but neither of them does so completely, rather they intersect. In this case, we included both the previously existing subcategory in the initial ULEO and the corresponding D because both offer a better answer to the same problem than either of them separately.
6) Cases in which a subcategory of the initial ULEO does not have an equivalent D, that is, it is something that exists only in the initial ULEO and not in [47]. In this case, we maintained this subcategory because we understood it provides a plus of security.

After this combination, we finished the inclusion of all the intended information in the ULEO: expected outcomes from NIST, controls and safeguards from CIS, the nine D's of cybersecurity, and, indirectly, mitigations from MITRE.

3) PHASE III. FILTERING AND GENERATION OF THE FINAL ULEO

After the two previous phases, the resulting ULEO contained redundant expected outcomes, whose only difference was the application in different IGs, an example of which is shown in Table 2. To remediate this redundancy, we performed a cleaning process consisting of consolidating these redundancies into a single expected outcome, leaving a single appearance that will apply to these IGs. In Table 3 the result of redundancy removal for the case presented in Table 2, can be shown.

TABLE 2. Example of redundant expected outcomes that apply to different IGs.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Identify	ID.AM	ID.AM-1	✓	✓	✓
Identify	ID.AM	ID.AM-1		✓	✓
Identify	ID.AM	ID.AM-1			✓

TABLE 3. Example of redundancy reduction.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Identify	ID.AM	ID.AM-1	✓	✓	✓

The final ULEO was obtained by repeating this process. It incorporates a total of 169 expected outcomes organized in the same functions and categories used by the NIST framework, but keeping traceability to MITRE mitigations while including information from the nine D's of cybersecurity and the CIS CSCs. In Appendix V, Tables 4 to 26 show the ULEO for each function and category. The expected outcomes are referenced by their code, being those that begin with 'CSC' those from the set of CSCs from CIS; those that start with '9D' those corresponding to the nine Ds of cybersecurity as indicated in the Table 1 and the rest, the original of the NIST framework.

4) ULEO BENEFITS

The ULEO we have built provides several advantages to the solution we propose:

- It classifies the expected outcomes into three IGs, following the same approach that the CIS uses for its critical controls. In practice, this allows to obtain three different sets of expected outcomes applicable to three different scenarios where the cybersecurity needs are LOW, MEDIUM, or HIGH.
- As it has been built, it incorporates the best recommendations of the NIST, the CIS, and the 9 D's of cybersecurity, eliminating the existing redundancies between them. It also brings together the best of each approach: security functions (and their division into categories and subcategories), IGs, etc. Moreover, based on the unified list of expected results of the NIST Cybersecurity Framework, not only cybersecurity controls are

considered in our proposal, but also the main controls related to privacy, closely linked, as detailed in [81].
- The expected outcomes of each implementation group allow for effective cyber defense against the TTPs documented by MITRE (and associated cyber threats).
- Its hierarchical arrangement allows the state of cybersecurity to be evaluated with different granularity and to easily identify which aspects must be improved to achieve the expected outcomes.
- Although our proposal should not be understood as a cyber-incident management process, it helps to deal with cyber-incidents by facilitating to the organization to acquire the skills and elements necessary for it, as a consequence of the implementation of the expected results of the functions ''Detect'' and ''Respond'' of the ULEO.
- The mere use of ULEO makes it possible to reduce the risks related to cybersecurity and business continuity by facilitating the organization to acquire the necessary skills and elements for it, as a consequence of the implementation of the expected results of the ''Identify'' and ''Recover'' functions. In addition, the ULEO has been built in such a way that there is a direct mapping from it to the mitigations defined by MITRE to face the most important real cyber threats.

D. CYBER SECURITY DOMAINS

As mentioned throughout this work, many organizations manage their cybersecurity using information security regulatory frameworks. For this reason, it is likely that they have not assimilated the need for participation in many of the functional areas whose involvement is required for cybersecurity. This is a clear mistake that must be corrected if organizations intend to deal with cyber threats using a cybersecurity approach, so it is necessary to change this trend and adopt a much broader and more integrated vision.

To help with this purpose, in our proposal we use the main cybersecurity domains of [82], because it is the most complete work and at the same time focused on cybersecurity of the sources that we have analyzed. To the previous ones, we added an additional domain related to corporate communication, marketing and institutional relations, which we consider essential to face the emerging cyberattacks in the last two years, with an impact on the supply chain and on the image and reputation of the organization; and because it is a necessary area to achieve some of the cybersecurity expected outcomes of the ULEO. In our work we will understand the domains of cybersecurity as the functional areas of an organization with responsibilities in cybersecurity. The complete list of functional areas of cybersecurity included in our proposal can be found in Table 27 (Appendix V), with the following scope:

- **FA1**. In charge of IoT device security.
- **FA2**. Active defense, vulnerability management, threat hunting, SIEM operation, cybersecurity operations center activities, or incident response [83].
- **FA3.** Prepare human resources regarding cybersecurity threats through continuous training and its reinforcement, as well as the design and execution of practical cybersecurity exercises [84].
- **FA4**. In charge of the analysis of internal and external threats, the exchange of threat intelligence with third parties or the preparation and incorporation of Indicators Of Compromise *(IOCs)*.
- **FA5**. With tasks related to the surveillance of applicable regulations and their incorporation into cybersecurity. In addition, the monitoring of different performance indicators, and the establishment of strategies, policies, standards, processes, procedures or corporate instructions.
- **FA6**. Focused on risk treatment, business continuity management, crisis management, establishing the organization's position regarding cyber risks, insurance contracting, risk registration, auditing, defining groups of risk management, or defining those responsible and owners of the processes and assets [85].
- **FA7**. Responsible for cybersecurity risk analysis, vulnerability scanning, supply chain risk identification and analysis, asset inventory, risk monitoring, and penetration testing of infrastructure, people, or systems of information, among others.
- **FA8**.With the mission of leading the secure software development cycle, continuous integration and deployment, user experience security, software quality, API security, identification of information flows in information systems, management of the free software used, or the static or dynamic analysis of the code.
- **FA9**. In charge of the management, development, implementation, and verification of compliance with the standards and regulations defined at the corporate level for cybersecurity: CIS controls, MITRE matrix, NIST framework for the improvement of cybersecurity of critical infrastructures, or the family of standards ISO27000 [19].
- **FA10**. With activities such as management, definition, implementation, operation, prevention, etc., in relation to cryptography, key and certificate management, encryption standards, security engineering, access controls with or without multiple authentication factors, single sign-on, privileged access management, identity management, identity federation, cloud security, container security, endpoint security, data protection and prevention of data leakage, network design to prevent distributed denial of service attacks, development and secure configuration of systems, patch and update management or the establishment of secure reference configurations.
- **FA11**. To promote study, education, and training, attendance at conferences, or participation in related professional groups, training, or certification.
- **FA12**. Specific activities include internal and external corporate communication, social networks

management, marketing, or the establishment and maintenance of institutional relationships with interested third parties with whom the organization maintains some type of contact.

E. AGGREGATED CYBERSECURITY ASSESSMENT

Cybersecurity assessment, especially in environments involving different functional areas, is often problematic because of its ambiguity, different interpretations, or different interests. However, having a unified, realistic and unbiased view of the state of cybersecurity is essential. Based on what was previously discussed in this study, our proposal defines the necessary aspects to provide a shared vision of cybersecurity.

1) IG IDENTIFICATION

In our work, we have elaborated on the ULEO in such a way that it allows a direct association between the protection priority indicated in the BIA for each business asset and different IGs. The correspondence between the priority established in the BIA and the IGs that should be applied to the asset can be shown in Table 28 (Appendix V), in such a way that, to provide cybersecurity to a business asset cataloged with LOW priority, actions must be put in place to achieve all the expected outcomes of the IG1 implementation group. For the assets cataloged with MEDIUM and HIGH priorities, those of the IG2 and IG3 groups, respectively. These groups and their associated actions are homogeneous for all business assets in the organization.

2) RELATIVE WEIGHT OF EACH SECURITY FUNCTION

The hierarchical structure embedded in the ULEO allows us to infer the weight of each cybersecurity function (fig. 10) for each IG with respect to the global cybersecurity of the business asset. These weights can be calculated as a percentage (or normalized between 0.00 and 1.00). In our proposal we calculated the weights of each security function for IG1, IG2 and IG3. These weights have been rounded to the second decimal place and are shown in table 29, Table 30 and Table 31 (Appendix V), respectively, where:

- F, represents the continuous cybersecurity function.
- N_c, represents the number of categories that the function F includes for the corresponding IG.
- W_f, represents the relative weight of the F function with respect to the global cybersecurity value of the asset.

3) RELATIVE WEIGHT OF EACH CATEGORY AND EXPECTED OUTCOME

For the same reasons expressed in the previous point, the ULEO allows determining the weight of each category, for each IG, with respect to each cybersecurity function, as well as the weight of each expected outcome with respect to its category. In our proposal, we calculated the weights of each category and expected outcomes, as shown in Appendix C. The weights corresponding to 'Identify' categories and expected outcomes can be seen in Tables 32 to 34; those related to 'Protect' categories and expected outcomes in Tables 35 to 37; values related to 'Detect' sub-items are shown in Tables 38 to 40; the weights of categories and expected outcomes belonging to 'Respond' are in Tables 41 to 43, and those corresponding to the 'Recover' function are shown in Tables 44 to 46. In all cases:

- C, represents the category.
- N_o, represents the number of expected outcomes of that category.
- W_c, represents the relative weight of C category with respect to its function (rounded to the second decimal place).
- W_o, represents the relative weight of each expected outcome with respect to its category.

A visual description of category weights for functions 'Identify', 'Protect', 'Detect', 'Respond' and 'Recover' is shown in figs. 11, 12, 13, 14 and 15, respectively.

The previous calculations allow a tree-like set of weights to be calculated in an aggregated way for the cybersecurity posture of the business asset in relation to its criticality. At all levels, expected outcome, category, function, or global.

4) DISCRETE LEVELS OF IMPLEMENTATION

It is convenient to define unambiguous values to establish the achievement/implementation status of each expected outcome. This issue is a common source of discrepancies and conflicts in organizations, either because each functional area has different perspectives on implementation status or because they do not have the ability to adequately measure at such a detailed level. Therefore, in our proposal, we have chosen to use Discrete Levels of Implementation *(DLIs)*, as standardized values to communicate the status of implementation of the cybersecurity actions that allows obtaining the expected outcomes (fig. 16). In our study these are the only possible values for expressing the state of progress in the implementation of each action related to an expected outcome.

Because they are not subject to interpretation and have the same meaning regardless of the functional area, action or expected outcome in question, *DLIs* are a good communication mechanism that avoids conflicts between functional areas and provides the same and shared perception of cybersecurity status.

5) ASSET BREAKDOWN

The main element of this proposal is the business asset, understanding that this unit is sufficiently small to be addressed at lower levels without too many problems. However, there may be situations where it is necessary to break down such business assets into secondary assets, for example, because it is easier to take care of cybersecurity in this way or because it facilitates the distribution of tasks between different operational groups of the same functional area or different functional areas. If necessary, the asset can be broken down as many times as necessary, following the guidelines designed

FIGURE 10. Relative weights of each cybersecurity function and the three IGs.

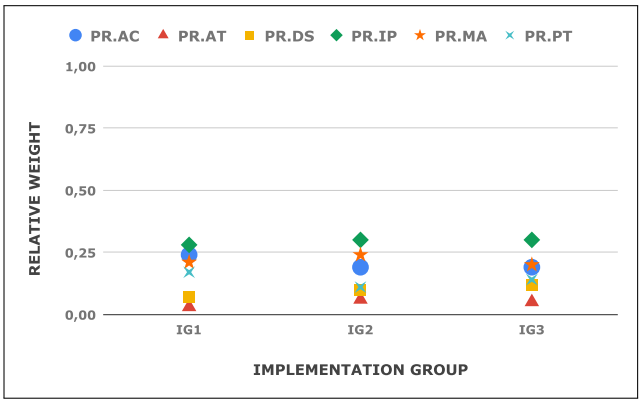


FIGURE 12. Relative weights of every category in 'Protect' function and the three IGs.

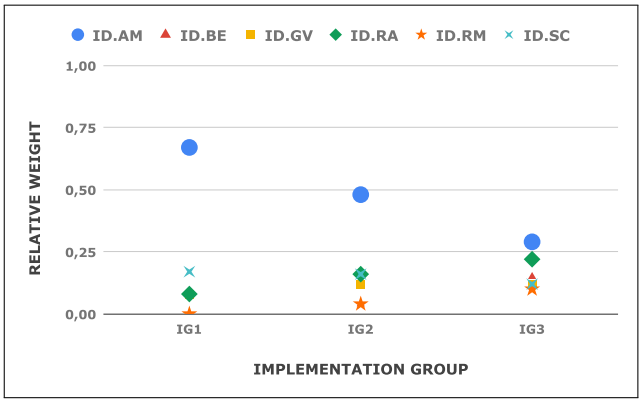


FIGURE 11. Relative weights of every category in 'Identify' function and the three IGs.

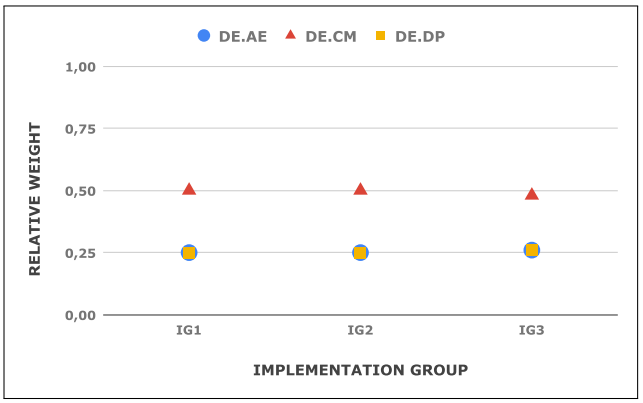


FIGURE 13. Relative weights of every category in 'Detect' function and the three IGs.

in our proposal. Bearing in mind that L represents the level of the asset, with L0 being the business asset and increasing to L1, L2... as the assets are broken down into more manageable assets:

- Each asset that is broken down must be broken down into elements that constitute an independent whole by themselves, as shown in equation 1.

$$Asset(L) \Rightarrow \bigcap_{i=1}^{n} Asset(L+1)_i = 0 \tag{1}$$

- The sub-assets in which an asset is broken down must represent the total of the asset on which they depend. In other words, the total top-level asset has been broken down into the sub-assets that make it up, as shown in equation 2.

$$Asset(L) = \sum_{i=1}^{n} Asset(L+1)_i \tag{2}$$

- Each sub-asset must have a weight (ω), as a reflection of its contribution to the higher-level asset, consisting of a normalized value between 0.00 and 1.00, equivalent to a percentage between 0% and 100% of the parent asset, respectively, as shown in equation 3.

$$Asset(L) = \sum_{i=1}^{n} \omega_i \cdot Asset(L+1)_i \tag{3}$$

subject to the following restriction (equation 4)

$$\sum_{i=1}^{n} \omega_i = 1, \forall \omega \in \mathbb{R}, \omega \subset [0,1] \tag{4}$$

- The implementation group corresponding to the parent asset will apply to all its sub-assets, as specified in equation 5.

$$IG(Asset(L+1)) = IG(Asset(L)) \tag{5}$$

Likewise, there are two types of assets/sub-assets: those that have been broken down into sub-assets, which we call 'inner assets', and those that have not been broken down into sub-assets, which we call 'leaf assets'. It is important to understand this distinction which is necessary for an aggregate evaluation of asset cybersecurity.

Figure 17 shows an example of a properly performed breakdown of a fictitious business asset at three levels. The weights and number of sub-actives in the figure are invented and placed like this for merely didactic purposes. However, it

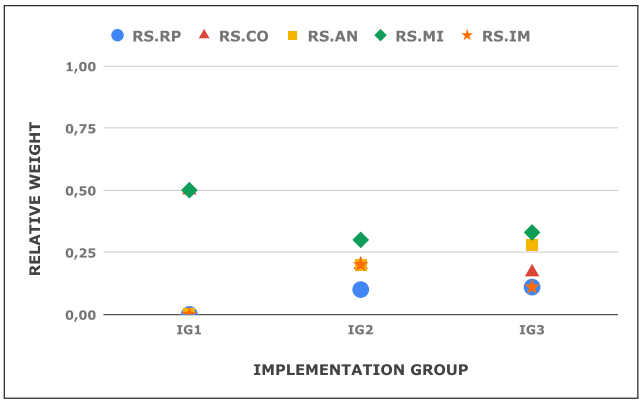


FIGURE 14. Relative weights of every category in 'Respond' function and the three IGs.

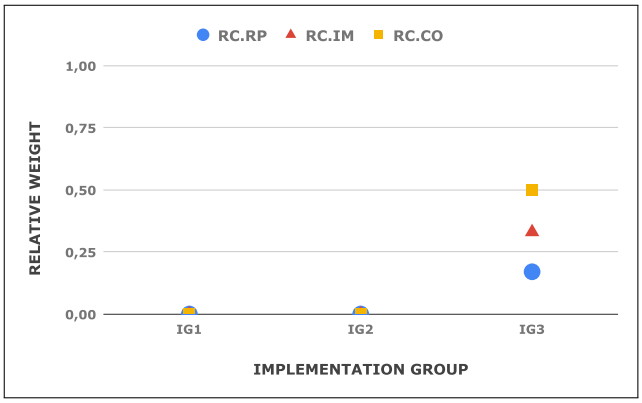


FIGURE 15. Relative weights of every category in 'Recover' function and the three IGs.

is necessary, as can be seen in the figure, that the sum of the weights of the sub-assets into which an asset has been broken down, is 1.00 in all cases. The figure also shows in different colors the inner assets (blue) and the leaf assets (yellow).

6) ASSET's CYBERSECURITY IDEAL STATE AND ASSET's CYBERSECURITY EXPECTED STATE

The Asset's Cybersecurity Ideal State *(ACIS)* will always be 1.00, which is achieved when a DLI of 1.00 has been reached for all the expected outcomes that correspond to it according to the applicable IG. It is important to understand this nuance, since the same level of implementation for the same expected outcomes that for an asset could represent an *ACIS*, for another asset it could represent a state of, for example, 0.54 (so not ideal), simply because a different implementation group applies to it.

The Asset's Cybersecurity Expected State *(ACES)*, will be determined by the organization as a cybersecurity objective, referring to a specific value of one, several, or all cybersecurity functions, categories, or expected outcomes. This expected state could result from any combination of DLIs applied to any applicable set of expected outcomes, which allows reaching that value. Understand this distinction.

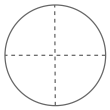
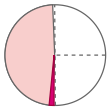
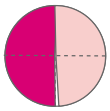
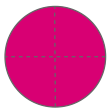
COVERAGE	DLI	EXPLANATION
	0.00	None of the necessary actions have been implemented to obtain the expected outcome.
	0.33	Some of the actions necessary to obtain the expected outcome have been implemented, but less than half.
	0.66	Half of the actions necessary to obtain the expected outcome, or more, have been implemented.
	1.00	All the necessary actions have been implemented to obtain the expected outcome.

FIGURE 16. Discrete levels of implementation (DLIs). black shows the minimum coverage required to be qualified as the corresponding DLI. Pink shows the maximum coverage (together with the black portion) before hopping to the next DLI.

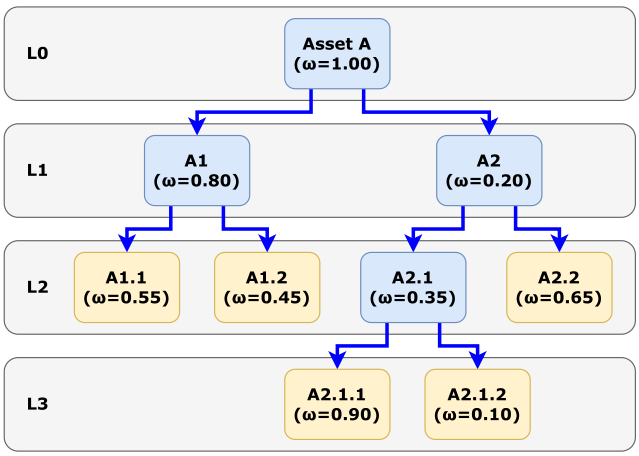


FIGURE 17. Example of a correct asset breakdown.

Although there is only one option to achieve an *ACIS* (the one described in the previous paragraph), to achieve an *ACES*, there may be multiple possible combinations on which a selection process will have to be carried out; this is covered in Section IV.

7) COMPUTING THE ASSETS' CYBERSECURITY STATUS

The defined structure and weights calculated in our proposal allow the evaluation of the cybersecurity status of an asset by adding information in a bottom-up process. The formulas that we have designed in our solution are easy to implement in any programming language or dashboard solution. Its tree-like structure facilitates the implementation of navigation through the organization, assets, sub-assets, functions, categories, and expected outcomes, to detect deficiencies in cases in which

the state of cybersecurity is not the expected or planned at any of these levels.

In the case of a leaf asset, the evaluation is performed as follows:

- **First step.** It consists of assigning to each expected outcome that applies the DLI that best reflects the status of the implementation of the associated actions. Thus, this information can be propagated upwards, starting by calculating the Category's Cybersecurity State (CCS_i) of each cybersecurity categories of the model of our proposal (equation 6).

$$CCS_i = \sum_{j=1}^{n} Wo_{ij} \cdot DLI_{ij} \tag{6}$$

  That is, the weighted sum of the discrete level of implementation of each expected outcome included in the category is calculated, based on its relative weight with respect to this category.
- **Second step**. Once the CCS_i values are known for all categories, the metrics can continue to be propagated upwards to calculate the Function's Cybersecurity State (FCS_i) of each cybersecurity function of the model of our proposal (equation 7).

$$FCS_i = \sum_{j=1}^{n} Wc_{ij} \cdot CCS_{ij} \tag{7}$$

  That is, the weighted sum of the cybersecurity status of each category of the function is calculated, considering its relative weight with respect to this function.
- **Third step**. And finally, having already calculated the FCS_i values for each function, we can calculate, going higher, the Asset's Cybersecurity Status (ACS_i) for each evaluated leaf asset (equation 8).

$$ACS_t = \sum_{j=1}^{n} Wf_{tj} \cdot FCS_{tj} \tag{8}$$

  This formula calculates the weighted sum of the cybersecurity status of each function applied to the asset, considering its relative weight with respect to its global cybersecurity. The t sub-index means that the ACS value is computed at a given moment, and subsequent measurements can throw different values.

In the case of inner assets, the calculation is based on previous knowledge of the ACS_i value of each sub-asset using the technique explained in the previous steps. Once these values are known, this information can be added, and the value of ACS_i for the inner asset can be calculated as follows (equation 9):

$$ACS_t = \sum_{j=1}^{n} Wsa_{tj} \cdot ACSsa_{tj} \tag{9}$$

where $ACSsa_{tj}$ is the ACS_{tj} value calculated independently for each sub-asset and Wsa_i is the relative weight of that sub-asset. In other words, the weighted sum of the cybersecurity status of each sub-asset is calculated while considering its relative weight with respect to the parent asset.

Because of the possibility of having different ACS_t values depending on the moment when the measurement is taken, our proposal allows computing the behavior of the ACS value over the time ($ACSev$), as shown in equation 10.

$$ACSev = \frac{t\sum_{i=1}^{t} t_i ACS_i - \sum_{i=1}^{t} t_i \sum_{i=1}^{t} ACS_i}{t\sum_{i=1}^{t} t_i^2 - (\sum_{i=1}^{t} t_i)^2} \tag{10}$$

$ACSev$ will take values from 0.00 to 1.00, because it is an additive time series. Values close to 1.00 indicate that the $ACIS$ for that asset will be achieved quickly, whereas values close to 0.00 predict ACS for that asset increases slowly and, therefore, it will take longer to achieve its $ACIS$.

8) COMPUTING THE ORGANIZATION's CYBERSECURITY STATUS

Although our proposal does not intend to address the strategic area, thanks to this, it is possible to evaluate the Organization's Cybersecurity Status (OCS) by continuing with bottom-up aggregation, in a similar way to what was explained in the previous section.

If the organization has identified weights for business assets that comply with the provisions for asset breakdown, the OCS can be calculated as follows (equation 11):

$$OCS_t = \sum_{j=1}^{n} Wba_{tj} \cdot ACSba_{tj} \tag{11}$$

where:

- Wba_{tj} is the relative weight of each business asset of the organization.
- $ACSba_{tj}$ is the cybersecurity status of each business asset calculated as described in the previous section. The t subindex, again, means that the $ACSba$ value is computed at a given moment and subsequent measurements can throw different values.

The above formula calculates the weighted sum of the cybersecurity status of each business asset, using its relative weight with respect to the organization. As in the previous paragraphs, owing to the possibility of having different OCS_t values depending on the moment when the measurement is taken, our proposal allows the calculation of the behavior of the OCS value over time ($OCSev$), as shown in equation 12.

$$OCSev = \frac{t\sum_{i=1}^{t} t_i OCS_i - \sum_{i=1}^{t} t_i \sum_{i=1}^{t} OCS_i}{t\sum_{i=1}^{t} t_i^2 - (\sum_{i=1}^{t} t_i)^2} \tag{12}$$

$OCSev$ will take values from 0.00 to 1.00, because it is an additive time series. Values close to 1.00 indicate that the cybersecurity status for the organization will be achieved quickly, whereas values close to 0.00 predict the OCS increases slowly and, therefore, it will take longer to achieve the expected cybersecurity status.

IV. CYBERSECURITY TACTICAL AND OPERATIONAL MANAGEMENT PROCESS

A. OVERVIEW

To articulate all the elements defined in Section III and that in this way our proposal constitutes a systematic mechanism, we have developed a Cybersecurity Tactical and Operational Management Process (CyberTOMP).

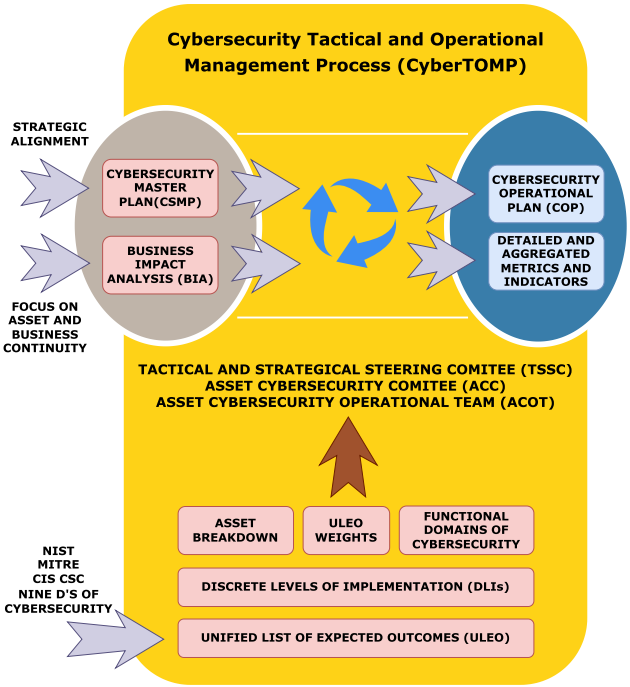


FIGURE 18. CyberTOMP high-level view.

Fig. 18 shows a coarse-grained view of the process, with the main inputs, outputs, and involved elements. The high-level objective of this process is to facilitate cybersecurity management by focusing on a business asset in each case. For this to be possible, the process, which will be discussed in the following sections, will be based on the organization's CSMP and BIA. This, together with the requirements expressed in Section III, provides the necessary alignment with the strategic objectives of the organization, both in terms of cybersecurity and business continuity, as well as a focus on business assets.

As a result of the application of CyberTOMP, a specific Operational Cybersecurity Plan *(COP)* is obtained for the business asset whose cybersecurity is being managed, as well as a set of metrics and indicators detailed and addable upwards. Both results, agreed upon by all functional areas involved in cyber defense/cyber protection of business assets. CyberTOMP facilitates the application of change management techniques [86] by following an inclusive and progressive approach.

The process that we developed achieves the necessary cooperation between all the functional areas of the organization in cybersecurity matters through three multidisciplinary bodies that participate at different times:

- **The Tactical-Strategic Steering Committee *(TSSC)*.** An interdepartmental multidisciplinary committee composed of members of the organization's steering committee, who preferably, participated in both the preparation of the CSMP and the BIA. With initial inclusion, if necessary, of tactical personnel.
- **The Asset's Cybersecurity Committee *(ACC)*.** An interdepartmental multidisciplinary committee made up of all intermediate positions with responsibilities at a tactical level for the business asset to be protected. With sporadic participation, if necessary, of operational personnel.
- **The Asset's Cybersecurity Operational Team *(ACOT)*.** An interdepartmental multidisciplinary team made up of all positions in the organization with responsibilities at the operational level, as well as external personnel incorporated into the organization belonging to service providers, who regularly participate in the daily work of the organization. In both cases, when these tasks are related to the business asset to be protected.

Each of these bodies must include people from all areas of knowledge of the organization that must participate in the cybersecurity of the business asset. In this way, these will be the bodies that facilitate the unity of action and holistic approach. Their participation in the process will be in increasing order, with the TSSC being the body that has to use the least effort in the process and the ACOT being the one that has to make the most.

At a greater level of detail, CyberTOMP includes five phases, that are similar to those commonly accepted for project management [87], with some modifications in the final phase becasue, although considering that the protection of assets emanates from projects defined in the CSMP, it is an ongoing task. These phases are: Initiating, Planning, Execution, Monitoring and Controlling, and Continuous Improvement, each containing a series of clear steps, as presented in fig. 19, which shows CyberTOMP's detailed view.

These phases, as well as the activities included in them, their peculiarities, and their explanations are detailed in the following sections with the intention of serving as a guide for their practical application in any organization. We believe this level of detail is necessary because precisely what our work tries to solve is the lack of procedural elements to manage cybersecurity at the tactical and operational levels.

B. INITIATING

This initial phase of the process is focused on:

- Ensure that cybersecurity management focuses on business assets, using those identified in the BIA.
- Ensure strategic alignment by assigning requirements derived from the BIA as well as tasks, objectives, and high-level requirements from different projects defined in the CSMP.

- Ensure that the required holism is provided to protect the business asset on a daily basis.
- Ensure that guidelines are provided to achieve shared leadership and co-governance in cybersecurity management for each business asset.

These elements have a marked strategic nature, are defined at a high level, and are presumably endowed with greater stability over time. The 'Initiation' phase consists of two main activities as detailed below.

1) DEFINE INITIAL ACC

In this activity (fig. 20), the TSSC analyzes the information contained in both the CSMP and BIA to determine the following:

- The business assets identified in the BIA and their high-level cybersecurity and continuity needs, including the potential needs for actions to respond to cybersecurity incidents and/or to recover from unavailability with regard to cybersecurity.
- The projects defined at a high level in the CSMP for each of the assets established in the BIA, their objectives, and their actions at a high level.
- Based on the above, the functional areas of the organization that should be involved in the cybersecurity of each business asset established in the BIA.
- People, at a tactical level, identified in each of these areas.

This group of individuals identified by the TSSC will form the initial ACC. If the TSSC deems it necessary, it may consult those people directly to determine more accurately whether other people not considered should also be part of the initial ACC. The initial ACC should include, for each person, high-level reasons why that person should be part of the ACC and high-level expectations for the cybersecurity of the business asset from their functional area.

As a guideline for this step, the set of cybersecurity functional domains identified in Section III can be used, which provides a fairly detailed representation of the functional areas involved in cybersecurity. The TSSC will define as many ACCs as business assets need cyber protection.

2) DEFINE INITIAL CYBERSECURITY ASSIGNMENT

In this step (fig. 21), based on the analysis of the BIA and CSMP, the TSSC will prepare a high-level list of cybersecurity and continuity needs and objectives (in relation to cybersecurity) for the business asset and will formalize a cybersecurity assignment for the asset, which will be delivered to the people who form the initial ACC. The needs and objectives will be extracted from the cybersecurity projects included in the CSMP and will be expressed in the form of high-level *ACES*, preferably as requirements on the metrics ACS_i or FCS_i of the asset indicated in the assignment. For example, the objectives of the business asset cybersecurity assignment can be:

- Increasing the ACS_i a 10%.
- Increasing the FCS_i, for the 'Respond' function, a 12%.
- Keeping the ACS_i at the current 75% relative to the current threat context.
- Keeping the ACS_i after a change in prioritization of business assets in the BIA.
- Keeping the ACS_i after a remodeling of the organizational structure.
- Assessing the ACS_i.
- Achieving the *ACIS*.

Or similar objectives. The cybersecurity assignment for the asset includes the indicated goals, the group of people that will form the initial ACC, the written statement of the assignment, and each area or functional unit represented. For practical reasons, it may be more agile to carry out this delivery through a joint meeting where the details of the assignment can be explained. Finally, the assignment must reach all the members of the initial ACC in a more formal way.

The assignment will include a period for the ACC to refine, adjust, and complete it after a more detailed analysis at the tactical level as a step prior to its final formalization.

The TSSC will carry out as many cybersecurity assignments as business assets need cyber protection.

C. PLANNING

This phase of the process is intended to delve into the details of the actions that must be undertaken to achieve the objectives requested in the assignment. For this, a series of iterative activities is carried out until the granularity that allows:

- Breaking down the business assets if it is considered necessary for a better distribution of tasks, greater control, or in general, to facilitate the management of the work to be carried out at tactical and operational levels.
- Identifying and distributing the scope of actions among different areas of knowledge represented in the ACC.
- Providing context to the cybersecurity needs of the assignment and adapting the actions that must be undertaken to the reality of the moment in the cyber field, from a multidisciplinary and holistic approach.
- Agreeing on the distribution of cybersecurity metrics and indicators.
- Updating the initial cybersecurity assignment, completing it with the aspects considered necessary.

In this phase, the ACC deals with planning in two stages that allow:

- Having a tactical-strategic planning, with a minimum participation of the TSSC.
- Having a later tactical-operational planning, more detailed, without the participation of the TSSC, and with the growing involvement of the operational teams.

The 'Planning' phase is consists of eight activities, which are detailed below.

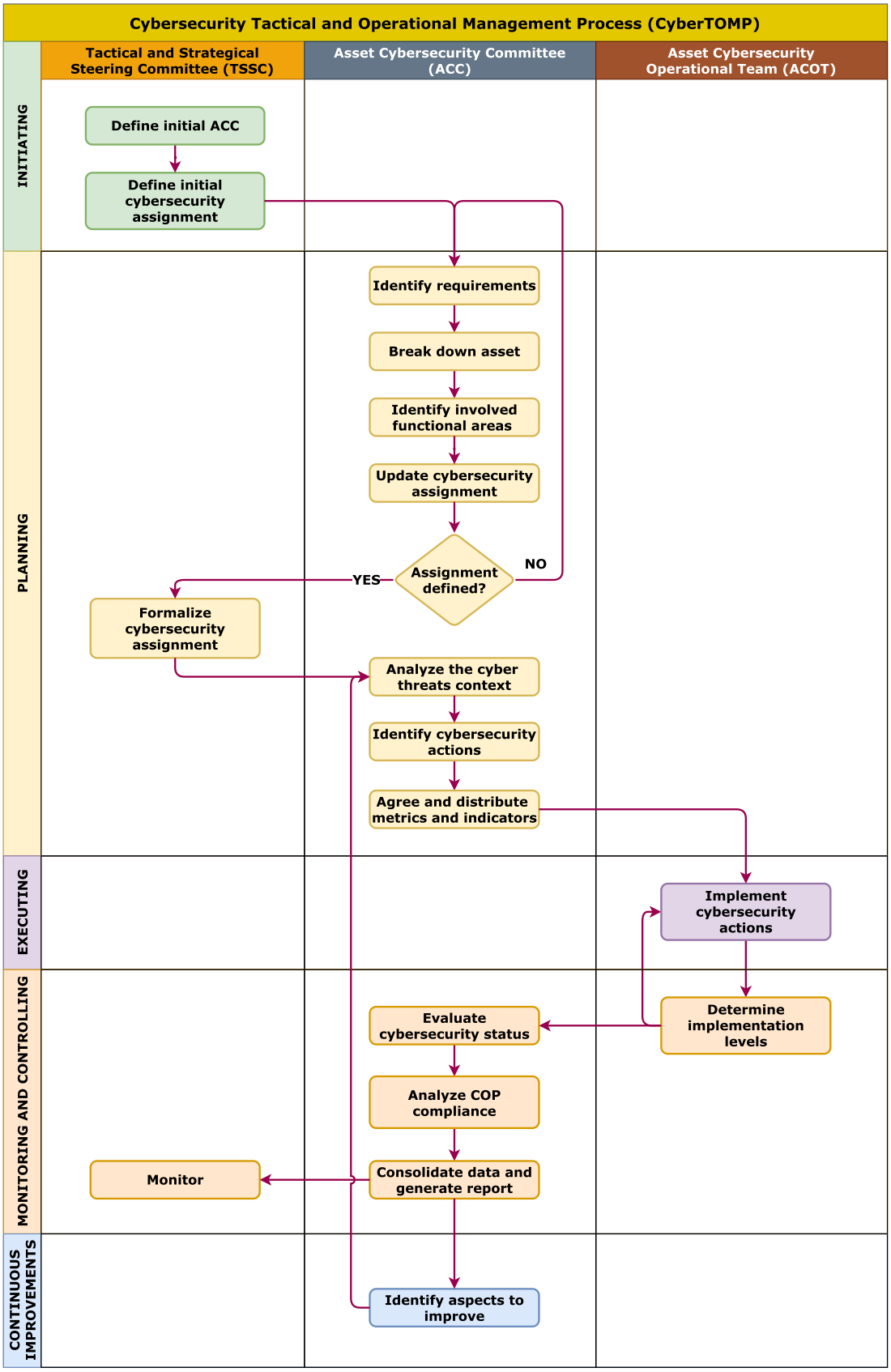


FIGURE 19. Detailed CyberTOMP steps and activities.

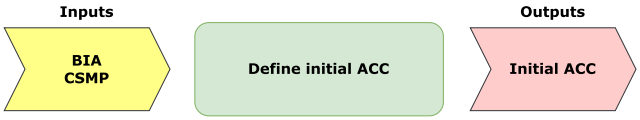


FIGURE 20. Inputs and outputs of 'Define initial ACC' activity.

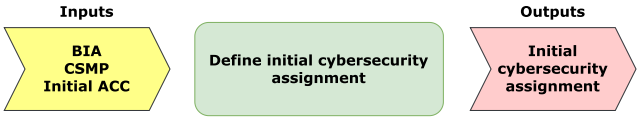


FIGURE 21. Inputs and outputs of 'Define initial cybersecurity assignment' activity'.

1) IDENTIFY REQUIREMENTS

In this activity (fig. 22), the ACC in the cybersecurity assignment for the asset will receive the priority corresponding to it, as the organization has assigned to that asset in the BIA. Accordingly, ACC will be able to directly identify the corresponding IG from the ULEO defined in this study, as described in Section III. Because each IG determines the expected outcomes for each existing function and category, the ACC will know all the expected outcomes whose implementation would allow the business asset to reach the *ACIS*. This value will be used as a reference for the maximum cybersecurity with which the asset must be provided.

The ACC must analyze the objectives (the *ACES*) set by the TSSC in the cybersecurity assignment and determine the categories or expected outcomes of the ULEO that will need to be taken into consideration to achieve that objective without going deeper into the specific actions that involve each of them. The ACC will add this additional detail to the cybersecurity assignment and update the *ACES* to reflect on what was identified.

This step begins with tactical-strategic planning of the actions required for the cybersecurity of the business asset.

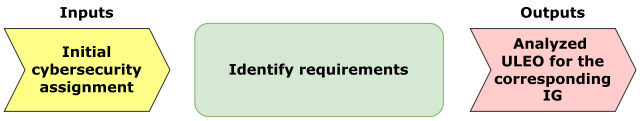


FIGURE 22. Inputs and outputs of 'Identify requirements' activity.

2) BREAK DOWN ASSET

If greater ease of management or understanding is needed, the ACC may break down the asset (fig. 23) into others of smaller caliber. The breakdown mechanism is presented in detail in Section III. Each sub-asset generated in this process is managed by the same ACC within the same assignment.

This subdivision allows different members of the ACC to focus more (although coordinated) on some of the broken-down sub-assets. It can also facilitate the assignment of activities between different areas or operational groups with greater

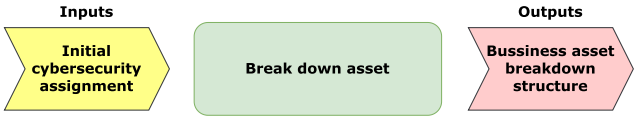


FIGURE 23. Inputs and outputs of 'Break down asset' activity.

specialization in specific tasks, without losing alignment with the proposed objective from the strategic level.

3) IDENTIFY INVOLVED FUNCTIONAL AREAS

It is likely that after the analysis of the requirements and the possible breakdown of assets into smaller ones, the need to incorporate some additional functional areas that must participate in the cybersecurity of the asset will be detected. If this is the case, the ACC will include tactical managers of such functional areas in CyberTOMP (fig. 24). The functional areas described in Section III are clear candidates.

FIGURE 24. Inputs and outputs of 'Identify functional areas involved' activity.

4) UPDATE CYBERSECURITY ASSIGNMENT

The ACC updates the cybersecurity assignment for the business asset (fig. 25) by documenting the identified requirements, the expected outcomes that must be considered to achieve the objectives, the new functional areas identified that must participate in the cybersecurity of the asset, the estimated breakdown of the business asset, and the agreed weights for all. In short, it should provide a more complete vision of cybersecurity assignment and provide the necessary justifications for it.

Once the assignment has been updated, it will be analyzed whether it can be considered complete and final, in which case the ACC will request formal approval from the TSSC. Otherwise, the process iterates, returning to the ''Identify requirements'' step.

An assignment cannot be considered complete if new functional areas are added to the process. If this happens, to prevent this inclusion from being merely cosmetic and ultimately causing tensions due to the assumption of non-agreed responsibilities, it will be necessary to iterate again (from the first step of 'Planning' phase) so that these functional areas can participate in all the steps prior to the final definition of the cybersecurity assignment.

5) FORMALIZE CYBERSECURITY ASSIGNMENT

TSSC analyzes the updated cybersecurity assignment for the asset submitted by ACC. It will evaluate its content, its convenience and feasibility, and the existence of the necessary

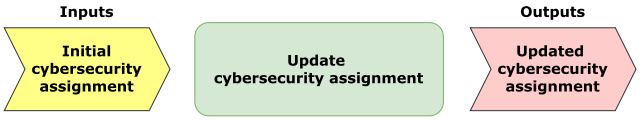


FIGURE 25. Inputs and outputs of 'Update cybersecurity assignment' activity.

consensus to provide holism and unity of action. It will approve the assignment (fig. 26) by signing it, the TSSC as a whole, the Chief Information Security Officer *(CISO)*, or the Chief Executive Officer *(CEO)*. It sends it to all members of the ACC as a final cybersecurity assignment for the protection of the business asset.

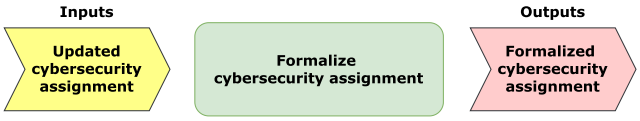


FIGURE 26. Inputs and outputs of 'Formalize cybersecurity assignment' activity.

This step ends the tactical-strategic planning of the actions required for cybersecurity of the business asset.

6) ANALYZE THE CYBER THREATS CONTEXT

In this phase, the ACC, supported by members of the ACOT, if necessary, will analyze the organization's cybersecurity context (fig. 27) in detail. In addition to the cyber threat context, in relation to business assets that they have been commissioned to protect. From both internal and external perspectives.

In this phase, renewed knowledge is acquired regarding the evolution of threats to the business in the cyber context. To express this in more detail, the cybersecurity status of a business asset can be altered simply because the context has changed, new threats have emerged, or there are exceptional situations that involve variations in the exposure level to different cybersecurity risks.

From this point is when the tactical-operational levels use their creativity, skills, and effort to cushion the enormous fluctuations in the cyber context and thus contribute, from the lower levels, to the strategic objectives of cybersecurity and the maintenance of the long-term corporate strategy.

This step is extremely important because allows a later definition of the form ('how') in which different cybersecurity actions must be implemented to ensure the achievement of the expected outcomes.

As a result of this step, it will be documented how low-level assets are impacted by the internal and external cyber context.

In this activity, in the event that it is a second or later iteration, the improvement opportunities identified in the continuous improvement phase of CyberTOMP will also be considered.

This step begins with tactical-operational planning of the actions required for the cybersecurity of the business asset.

FIGURE 27. Inputs and outputs of 'Analyze the cyber threats context' activity.

7) IDENTIFY CYBERSECURITY ACTIONS

In this activity, it is important to understand that expected outcomes are called that way precisely because they are the results that will presumably be obtained by carrying out different actions. Actions defined in greater detail in the textual description of each expected outcome.

For example, the CIS safeguard 'CS-11.1 Establish and Maintain a Data Recovery Process' would be the expected outcome, whereas the actions defined by the CIS for that safeguard would be those that allow it to be achieved: 'Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard'. Only when everything described for that safeguard is done, it can be indicated that it is fully implemented.

As explained in the previous sections, there is only one way to obtain the *ACIS*, but there are many combinations to obtain the *ACES*. Therefore, both *ACC* and *ACOT* must analyze the different existing options that allow reaching the required *ACES*.

In this activity, the ACC will take the approved cybersecurity assignment, where the expected outcomes for which specific actions must be designed have already been identified, as well as the analysis carried out in the cyber threat context. (fig. 28). For each, the *ACC* will analyze the details of its description:

- For ULEO subcategories from the NIST cybersecurity framework, they should review the relevant description [48] in the framework itself or in the associated guides [50], [51].
- For the subcategories included in the ULEO and coming from the CIS, the relevant description [40] in the list of CSCs can be reviewed.
- For the subcategories incorporated into the ULEO and coming from the nine D's of cybersecurity, they should consult the description of each D [47] described in the original work.

The objective of this activity is to identify the potential list of cybersecurity actions that would address the cyber threat

FIGURE 28. Inputs and outputs of 'Identify cybersecurity actions' activity.

context to achieve the goals included in the cybersecurity assignment.

8) AGREE AND DISTRIBUTE METRICS AND INDICATORS

In this activity, the *ACC* and *ACOT* will reach a consensus (fig. 29) to select the expected outcomes and the actions that lead to them, among those identified, in a way that optimizes resources, management is facilitated, the workload and responsibilities of the different participating functional areas are reasonably distributed, existing technologies or knowledge can be reused; conflicts are minimized, etc.

With the above, each functional area of the *ACOT* will have the expected outcomes and the associated tasks that they have to undertake from their scope, the description of such tasks, the roles and responsibilities, metrics and weights, planning of the actions and milestones, their dependencies, and the periods to evaluate the progress. All this, as a whole, will constitute the Cybersecurity Operational Plan *(COP)* for the asset accompanied by the corresponding metrics and indicators. This plan will be fully aligned with the corresponding cybersecurity assignment mandated by the *TSSC* and, by extension, with the BIA and associated CSMP project.

The *ACC* defines a minimum DLI for each expected outcome, which must allow the achievement of what is required by the *TSSC* in the cybersecurity assignment for the asset. In this way, each person from the *ACOT* will know the target level of implementation for the actions that correspond to them. This step ends the tactical-operational planning of the actions required for cybersecurity of the business asset.

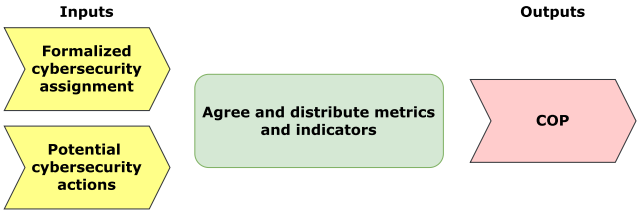


FIGURE 29. Inputs and outputs of 'Agree and distribute metrics and indicators' activity.

D. EXECUTING

The objective of this phase effectively implement the actions planned in the *COP*.

1) IMPLEMENT CYBERSECURITY ACTIONS

In this activity, the *ACOT* will be the team in charge of implementing the specific measures to achieve the expected outcomes that have been assigned (fig. 30), so that the micromanagement of these actions can be carried out in a decentralized manner in each *ACOT* functional area once the *ACC* has already agreed on the set of precise actions.

In practice, this step allows the performance of short-term tasks in a semi-autonomous and self-organized manner, ultimately contributing to the organization's cybersecurity and business continuity objectives (in relation to cybersecurity).

The different members of the *ACOT* can be helped, especially in the more technical functional areas, by the different existing guides, such as, for example, [33], [50] o [46].

FIGURE 30. Inputs and outputs of 'Implement cybersecurity actions' activity.

E. MONITORING AND CONTROL

This phase is focused on evaluating the cybersecurity status of business assets in relation to the cybersecurity assignment ordered by the *TSSC* and the corresponding *COP* generated in previous phases, to build valuable information so that the different levels of the organization can clearly understand the cybersecurity situation of the asset, with the necessary detail, and make decisions in this regard.

The evaluation of the state of cybersecurity will be carried out at three levels: operational, tactical, and strategic, which will be carried out with different frequencies, the most frequent being the operational evaluation, followed by the tactical one and the least frequent, the strategic evaluation, for a correct assessment of the impact of the actions as well as the new needs in the short, medium, and long term, respectively.

1) DETERMINE IMPLEMENTATION LEVELS

In this activity, with the periodicity indicated by the *ACC*, each member of the *ACOT* establishes the current *NDI* for each expected outcome that has been assigned (fig. 31), as indicated in Section III. In this way, the *ACC* will have the *NDI* for all expected outcomes included in the *COP* of the asset.

Together with this information, the *ACOT* will succinctly detail difficulties, synergies, proposals arising during the course of the work, or unexpected situations or situations not initially analyzed, if they exist. This will be performed individually for each expected outcome.

Progress information, together with the relevant information that allows its contextualization, will be included in an Operational Cybersecurity Report *(OCR)*, which can be as complex or simple as the organization requires.

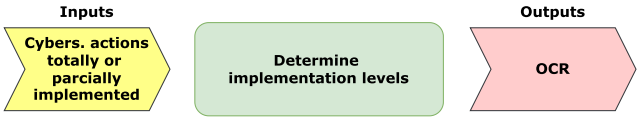


FIGURE 31. Inputs and outputs of 'Determine implementation levels' activity.

2) EVALUATE CYBERSECURITY STATUS

In this activity, with the agreed frequency, the *ACC* will receive the *OCRs* sent by the *ACOT* and proceed to evaluate the cybersecurity of the asset (fig. 32) using the *DLIs* contained in that report. They will do it following what is specified in Section III, taking into account the relative weights and calculating, for the business asset, the values CCS_i, FCS_i and ACS_i, so that at the end, the information aggregation and construction process will have, for each asset and sub-asset into which the business asset has been broken down:

- The status of achievement of each expected outcome.
- The cybersecurity status with respect to each category.
- The cybersecurity status with respect to each function.
- The cybersecurity status of the business asset.

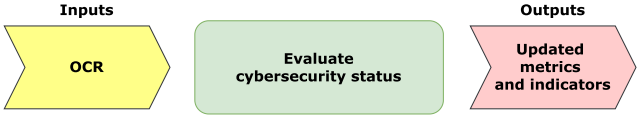


FIGURE 32. Inputs and outputs of 'Evaluate cybersecurity status' activity.

3) ANALYZE COP COMPLIANCE

In this activity, with the frequency that has been agreed upon for the tactical evaluation of cybersecurity, the *ACC* will analyze the current state and evolution of the different metrics and indicators associated with the cybersecurity assignment (fig. 33), calculated and aggregated in the previous step using the different *OCRs* that the *ACOT* has been sending to it and that have not yet been jointly analyzed or compared with the *COP* forecasts. It is recommended that this activity coincide with the last release of *OCR* by *ACOT* in order to have the most up-to-date view possible.

In addition, it will use the relevant information provided by the *ACOT* in the *OCRs* to contextualize possible deviations from what was planned and understand the circumstances that may have caused such deviations or the synergies and opportunities that may exist. All of this will be included in the Tactical Cybersecurity Report *(TCR)*.

Finally, the *ACC* updates, if it exists, the organization's cybersecurity dashboard with the current CCS_i, FCS_i, and ACS_i values.

4) CONSOLIDATE DATA AND GENERATE REPORT

In this activity, with the periodicity required by the *TSSC*, the *ACC* will analyze the degree of achievement of what is required in the cybersecurity assignment for the business asset, using such an assignment as a source and also the information of the different *TCRs*. It is recommended that this task is carried out coinciding with the generation of the last *TRC* to obtain the most up-to-date and recent view. With all this, it will generate a Strategic Cybersecurity Report *(SCR)* that will broadly identify the advances or delays and their main causes, as well as evolutionary data and tactical decisions taken or planned, if appropriate, in a very executive way (fig.34).

The *ACC* will report the status to the *TSSC*, forwarding that report.

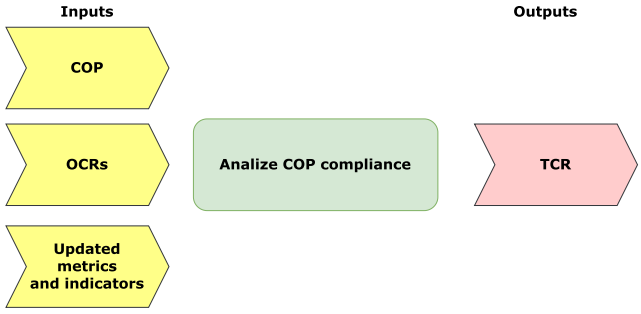


FIGURE 33. Inputs and outputs of 'Analyze COP compliance' activity.

5) MONITORING

The *TSSC* receives, with the required frequency, the last *SCR* regarding cybersecurity assignment for the protection of the business asset. With this information and that of the rest of the cybersecurity assignments they have assigned, they can, if desired, calculate the *OCS* value, taking into account the weights that could have been defined at a strategic level for each business asset.

FIGURE 34. Inputs and outputs of 'Consolidate data and generate report' activity.

The TSSC will use this monitoring information (fig. 35) to modify or update the cybersecurity assignment for strategic decision-makers in general or to generate additional strategic information that it deems necessary. This aspect is not addressed in detail in CyberTOMP, whose main scope is the tactical and operational levels.

F. CONTINUOUS IMPROVEMENT

The purpose of this phase is to identify the margins for improvement in different aspects, which can later be used as a basis for designing and executing additional actions in cybersecurity.

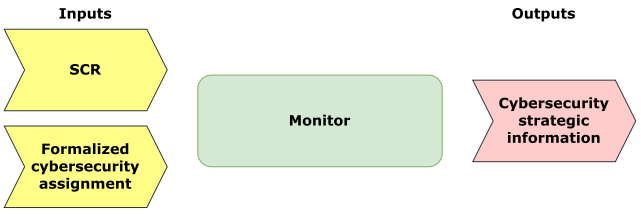


FIGURE 35. Inputs and outputs of 'Monitor' activity.

1) IDENTIFY ASPECTS TO IMPROVE

In this activity (fig. 36), the *ACC* will analyze the information from the *TCR*, paying attention not so much to possible deviations, but to the relevant information provided by the different members of the *ACOT*, which may include identified synergies, barriers found, opportunities, difficulties, and so on. The improvements likely to be identified in this activity are, without being an exhaustive list:

- New mechanisms for better coordination between functional areas.
- New mechanisms for better coordination and communication in the *ACC*.
- The need to search for alternatives for the implementation of operational actions that have been more complex or costly to implement in practice than initially planned.
- The use of tools that allow greater agility in work.
- The possibility of including common elements that suppose an optimization of costs and effort.
- The need to reinforce the operational work with new staff.
- Others of a similar nature.

This identification must be the result of a joint debate within the *ACC* and must not focus on the search for solutions, an aspect that is dealt with in the new analysis of the context, but on the identification and documentation of improvement opportunities.

Once this activity is done, the process must iterate again from the activity "Analyze the cyber threats context". Thus, CyberTOMP allows design of a new modified *COP* to include new cybersecurity actions to improve the detected weaknesses and adapt to the dynamic cyber threat context.

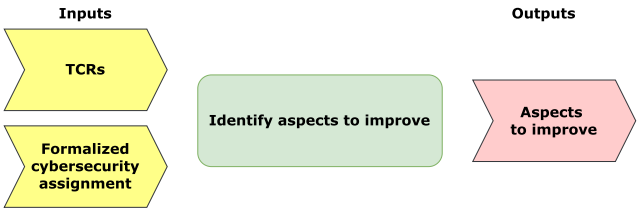


FIGURE 36. Inputs and outputs of 'Identify aspects to improve' activity.

G. PERIODICITY AND END OF THE PROCESS

CyberTOMP only ends when the *TSSC* carries out a new cybersecurity assignment for the same business asset or when it is decided from by strategic sphere of the organization. Otherwise, CyberTOMP will continue even if the *ACES* or *ACIS* has been reached. This is because, as has been commented on throughout this document, that state can change simply because the context changes. For example:

- If the context of cyberspace varies significantly and controls currently in place for the cybersecurity of the asset no longer have the same validity.

TABLE 4. ULEO for 'Identify' function and 'Assets Management' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Identify	ID.AM	CSC-1.1	✓	✓	✓
Identify	ID.AM	CSC-12.4		✓	✓
Identify	ID.AM	CSC-14.1	✓	✓	✓
Identify	ID.AM	CSC-2.2	✓	✓	✓
Identify	ID.AM	CSC-3.1	✓	✓	✓
Identify	ID.AM	CSC-3.2	✓	✓	✓
Identify	ID.AM	CSC-3.6	✓	✓	✓
Identify	ID.AM	CSC-3.7		✓	✓
Identify	ID.AM	ID.AM-1	✓	✓	✓
Identify	ID.AM	ID.AM-2	✓	✓	✓
Identify	ID.AM	ID.AM-2		✓	✓
Identify	ID.AM	ID.AM-3		✓	✓

TABLE 5. ULEO for 'Identify' function and 'Business Environment' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Identify	ID.BE	9D-1		✓	✓
Identify	ID.BE	ID.BE-1			✓
Identify	ID.BE	ID.BE-2			✓
Identify	ID.BE	ID.BE-3			✓
Identify	ID.BE	ID.BE-4			✓
Identify	ID.BE	ID.BE-5			✓

TABLE 6. ULEO for 'Identify' function and 'Governance' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Identify	ID.GV	CSC-17.4		✓	✓
Identify	ID.GV	ID.GV-1	✓	✓	✓
Identify	ID.GV	ID.GV-2		✓	✓
Identify	ID.GV	ID.GV-3			✓
Identify	ID.GV	ID.GV-4			✓

TABLE 7. ULEO for 'Identify' function and 'Risk Assessment' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Identify	ID.RA	9D-1		✓	✓
Identify	ID.RA	CSC-18.2		✓	✓
Identify	ID.RA	CSC-18.5			✓
Identify	ID.RA	CSC-3.7		✓	✓
Identify	ID.RA	ID.RA-1	✓	✓	✓
Identify	ID.RA	ID.RA-2			✓
Identify	ID.RA	ID.RA-3			✓
Identify	ID.RA	ID.RA-4			✓
Identify	ID.RA	ID.RA-6			✓

TABLE 8. ULEO for 'Identify' function and 'Risk Management Strategy' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Identify	ID.RM	9D-8		✓	✓
Identify	ID.RM	ID.RM-1			✓
Identify	ID.RM	ID.RM-2			✓
Identify	ID.RM	ID.RM-3			✓

TABLE 9. ULEO for 'Identify' function and 'Supply Chain Risk Management' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Identify	ID.SC	ID.SC-1		✓	✓
Identify	ID.SC	ID.SC-2	✓	✓	✓
Identify	ID.SC	ID.SC-3		✓	✓
Identify	ID.SC	ID.SC-4			✓
Identify	ID.SC	ID.SC-5	✓	✓	✓

- If there are organizational changes that eliminate, add, or reorganize the functional areas or personnel associated with it.
- If the implemented solutions depend on formalized contracts with service providers that end.
- If the business asset is expanded or reduced with new functionalities or components.
- If employees leave the organization or move horizontally and are replaced by others with different skills or training, or they are not replaced.
- If there is a budget reduction that prevents the maintenance of cybersecurity measures implemented around the asset.

TABLE 10. ULEO for 'Protect' function and 'Identity Management and Access Control' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Protect	PR.AC	CSC-12.5		✓	✓
Protect	PR.AC	CSC-12.6		✓	✓
Protect	PR.AC	CSC-13.4		✓	✓
Protect	PR.AC	CSC-4.7	✓	✓	✓
Protect	PR.AC	CSC-5.2	✓	✓	✓
Protect	PR.AC	CSC-5.6		✓	✓
Protect	PR.AC	CSC-6.8			✓
Protect	PR.AC	PR.AC-1	✓	✓	✓
Protect	PR.AC	PR.AC-2			✓
Protect	PR.AC	PR.AC-3		✓	✓
Protect	PR.AC	PR.AC-3	✓	✓	✓
Protect	PR.AC	PR.AC-4	✓	✓	✓
Protect	PR.AC	PR.AC-5	✓	✓	✓
Protect	PR.AC	PR.AC-6			✓
Protect	PR.AC	PR.AC-7	✓	✓	✓

TABLE 11. ULEO for 'Protect' function and 'Awareness and Training' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Protect	PR.AT	CSC-14.9		✓	✓
Protect	PR.AT	CSC-15.4		✓	✓
Protect	PR.AT	PR.AT-1	✓	✓	✓
Protect	PR.AT	PR.AT-2		✓	✓

TABLE 12. ULEO for 'Protect' function and 'Data Security' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Protect	PR.DS	9D-6			✓
Protect	PR.DS	CSC-3.4	✓	✓	✓
Protect	PR.DS	PR.DS-1		✓	✓
Protect	PR.DS	PR.DS-2		✓	✓
Protect	PR.DS	PR.DS-3	✓	✓	✓
Protect	PR.DS	PR.DS-4			✓
Protect	PR.DS	PR.DS-5			✓
Protect	PR.DS	PR.DS-6		✓	✓
Protect	PR.DS	PR.DS-7		✓	✓
Protect	PR.DS	PR.DS-8			✓

H. RECOMMENDATIONS FOR A CORRECT APPLICATION

Practical implementation of CyberTOMP can be facilitated or improved by applying a series of recommendations:

TABLE 13. ULEO for 'Protect' function and 'Information Protection Processes and Procedures' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Protect	PR.IP	9D-3		✓	✓
Protect	PR.IP	9D-5		✓	✓
Protect	PR.IP	9D-8		✓	✓
Protect	PR.IP	9D-9	✓	✓	✓
Protect	PR.IP	CSC-11.1	✓	✓	✓
Protect	PR.IP	CSC-16.1		✓	✓
Protect	PR.IP	CSC-16.14			✓
Protect	PR.IP	CSC-18.4			✓
Protect	PR.IP	CSC-2.5		✓	✓
Protect	PR.IP	CSC-2.6		✓	✓
Protect	PR.IP	CSC-2.7			✓
Protect	PR.IP	CSC-4.3	✓	✓	✓
Protect	PR.IP	PR.IP-1	✓	✓	✓
Protect	PR.IP	PR.IP-10		✓	✓
Protect	PR.IP	PR.IP-11	✓	✓	✓
Protect	PR.IP	PR.IP-12		✓	✓
Protect	PR.IP	PR.IP-2		✓	✓
Protect	PR.IP	PR.IP-3			✓
Protect	PR.IP	PR.IP-4	✓	✓	✓
Protect	PR.IP	PR.IP-5			✓
Protect	PR.IP	PR.IP-6	✓	✓	✓
Protect	PR.IP	PR.IP-7		✓	✓
Protect	PR.IP	PR.IP-8			✓
Protect	PR.IP	PR.IP-9	✓	✓	✓

TABLE 14. ULEO for 'Protect' function and 'Maintenance' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Protect	PR.MA	9D-5		✓	✓
Protect	PR.MA	9D-9		✓	✓
Protect	PR.MA	CSC-12.1	✓	✓	✓
Protect	PR.MA	CSC-12.3		✓	✓
Protect	PR.MA	CSC-13.5		✓	✓
Protect	PR.MA	CSC-16.13			✓
Protect	PR.MA	CSC-18.3		✓	✓
Protect	PR.MA	CSC-4.2	✓	✓	✓
Protect	PR.MA	CSC-4.6	✓	✓	✓
Protect	PR.MA	CSC-4.8		✓	✓
Protect	PR.MA	CSC-4.9		✓	✓
Protect	PR.MA	CSC-7.3	✓	✓	✓
Protect	PR.MA	CSC-8.1	✓	✓	✓
Protect	PR.MA	CSC-8.10		✓	✓
Protect	PR.MA	CSC-8.3	✓	✓	✓
Protect	PR.MA	CSC-8.9		✓	✓
Protect	PR.MA	PR.MA-1			✓

TABLE 15. ULEO for 'Protect' function and 'Protective Technology' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Protect	PR.PT	9D-4		✓	✓
Protect	PR.PT	9D-7			✓
Protect	PR.PT	CSC-4.12			✓
Protect	PR.PT	CSC-4.4	✓	✓	✓
Protect	PR.PT	CSC-4.5	✓	✓	✓
Protect	PR.PT	CSC-9.5		✓	✓
Protect	PR.PT	PR.PT-1	✓	✓	✓
Protect	PR.PT	PR.PT-2	✓	✓	✓
Protect	PR.PT	PR.PT-3			✓
Protect	PR.PT	PR.PT-4			✓
Protect	PR.PT	PR.PT-5	✓	✓	✓

- **Application of change management techniques**. In the development of our proposal, we understand the following circumstances concur:
  - A collaborative habit is required to reach consensus.
  - By employing three collegiate groups for decision-making, those roles that would normally have the possibility of making decisions individually may understand it as an attack on their competencies and present opposition to the changes.

  To facilitate both, we recommend the professional application of specific techniques for change management that ease the applicability of this proposal. For example, finding change agents to actively participate in the implementation. This change management approach should include training in soft skills that will equip participants with the ability to achieve win-win agreements.
- **The necessary role of CISO**. In light of what is stated in our solution, this could give the impression that the role of the CISO is diluted, becoming a point of potential conflict. It is recommended that the CISO have a relevant leadership role in the *TSSC*. Leadership, not necessarily hierarchical superiority. However, as the role with the most developed skills in cybersecurity, it should be the person responsible for ensuring the correct execution of CyberTOMP and who mediates in the case of conflicts or doubts.
- **Automation**. The use of tools to automate the calculation of metrics and indicators in the cybersecurity evaluation process can significantly facilitate the use of CyberTOMP and the generation of reports. All metrics and indicators have been defined in such a way that they can be easily automated and information can be provided

TABLE 16. ULEO for 'Detect' function and 'Anomalies and Events' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Detect	DE.AE	CSC-8.12			✓
Detect	DE.AE	DE.AE-1		✓	✓
Detect	DE.AE	DE.AE-2		✓	✓
Detect	DE.AE	DE.AE-3	✓	✓	✓
Detect	DE.AE	DE.AE-4			✓
Detect	DE.AE	DE.AE-5			✓

TABLE 17. ULEO for 'Detect' function and 'Security Continuous Monitoring' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Detect	DE.CM	CSC-13.1		✓	✓
Detect	DE.CM	CSC-13.5		✓	✓
Detect	DE.CM	CSC-3.14			✓
Detect	DE.CM	DE.CM-1		✓	✓
Detect	DE.CM	DE.CM-2			✓
Detect	DE.CM	DE.CM-3			✓
Detect	DE.CM	DE.CM-4	✓	✓	✓
Detect	DE.CM	DE.CM-5			✓
Detect	DE.CM	DE.CM-6			✓
Detect	DE.CM	DE.CM-7	✓	✓	✓
Detect	DE.CM	DE.CM-8		✓	✓

TABLE 18. ULEO for 'Detect' function and 'Detection Processes' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Detect	DE.DP	CSC-17.1	✓	✓	✓
Detect	DE.DP	CSC-17.4		✓	✓
Detect	DE.DP	CSC-17.5		✓	✓
Detect	DE.DP	DE.DP-2			✓
Detect	DE.DP	DE.DP-3			✓
Detect	DE.DP	DE.DP-5			✓

at all levels in almost real time, reducing the workload of the *ACC*.

- **Gradual implementation**. A progressive application is recommended, starting with a business asset that is relatively simple to manage and with few functional areas involved, and subsequently including others of greater complexity until this proposal is applied to all the business assets of the organization. The application to simpler cases in the first instance allows the refinement of the process, training of the team and obtaining good results that serve as a hook for the expansion of the solution.

TABLE 19. ULEO for 'Respond' function and 'Analysis' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Respond	RS.AN	CSC-17.9			✓
Respond	RS.AN	RS.AN-1		✓	✓
Respond	RS.AN	RS.AN-2			✓
Respond	RS.AN	RS.AN-3			✓
Respond	RS.AN	RS.AN-5		✓	✓

TABLE 20. ULEO for 'Respond' function and 'Communications' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Respond	RS.CO	CSC-17.4	✓	✓	✓
Respond	RS.CO	CSC-17.5		✓	✓
Respond	RS.CO	RS.CO-5			✓

TABLE 21. ULEO for 'Respond' function and 'Improvements' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Respond	RS.IM	RS.IM-1		✓	✓
Respond	RS.IM	RS.IM-2		✓	✓

TABLE 22. ULEO for 'Respond' function and 'Mitigation' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Respond	RS.MI	CSC-1.2	✓	✓	✓
Respond	RS.MI	CSC-4.10		✓	✓
Respond	RS.MI	CSC-7.7		✓	✓
Respond	RS.MI	RS.MI-1			✓
Respond	RS.MI	RS.MI-2			✓
Respond	RS.MI	RS.MI-3			✓

TABLE 23. ULEO for 'Respond' function and 'Response Planning' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Respond	RS.RP	CSC-17.6		✓	✓
Respond	RS.RP	RS.RP-1			✓

V. CONCLUSION

Tactical and operational levels are responsible for the practical implementation of cybersecurity. The standards used for

TABLE 24. ULEO for 'Recover' function and 'Communications' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Recover	RC.CO	RC.CO-1			✓
Recover	RC.CO	RC.CO-2			✓
Recover	RC.CO	RC.CO-3			✓

TABLE 25. ULEO for 'Recover' function and 'Improvements' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Recover	RC.IM	RC.IM-1			✓
Recover	RC.IM	RC.IM-2			✓

TABLE 26. ULEO for 'Recover' function and 'Recovery Planning' category.

Function	NIST Category	Unified expected outcome	IG1	IG2	IG3
Recover	RC.RP	RC.RP-1			✓

TABLE 27. Functional areas involved in cybersecurity, reused and improved in our proposal.

FA ID	Main cybersecurity responsibilities
FA1	Physical security
FA2	Security operations
FA3	User education
FA4	Threat intelligence
FA5	Governance
FA6	Enterprise risk management
FA7	Risk assessment
FA8	Application security
FA9	Frameworks and standards
FA10	Security architecture
FA11	Career development
FA12	Corporate communications

TABLE 28. Correspondence between cyberprotection priorities and IGs.

Cyberprotection priority (from BIA)	Corresponding IG
LOW	IG1
MEDIUM	IG2
HIGH	IG3

TABLE 29. Weights of cybersecurity functions for IG1.

F	N_c	W_f
Identify	4	0.27
Protect	6	0.40
Detect	3	0.20
Respond	2	0.13
Recover	0	0.00

TABLE 30. Weights of cybersecurity functions for IG2.

F	N_c	W_f
Identify	6	0.30
Protect	6	0.30
Detect	3	0.15
Respond	5	0.25
Recover	0	0.00

TABLE 31. Weights of cybersecurity functions for IG3.

F	N_c	W_f
Identify	6	0.26
Protect	6	0.26
Detect	3	0.13
Respond	5	0.22
Recover	3	0.13

TABLE 32. Weights for category 'Identify' and IG1.

C	N_o	W_c	W_o
ID.AM	8	0.67	0.125
ID.BE	0	0.00	0.00
ID.GV	1	0.08	1.00
ID.RA	1	0.08	1.00
ID.RM	0	0.00	0.00
ID.SC	2	0.17	0.50

TABLE 33. Weights for category 'Identify' and IG2.

C	N_o	W_c	W_o
ID.AM	12	0.48	$1/12$
ID.BE	1	0.04	1.00
ID.GV	3	0.12	$1/3$
ID.RA	4	0.16	0.25
ID.RM	1	0.04	1.00
ID.SC	4	0.16	0.25

cybersecurity encourage organizations to develop procedural elements for effective cybersecurity management at these levels, but do not provide such a procedural basis so that it can be used as is. This causes indeterminacy in how each organization manages cybersecurity at lower levels, often resulting in a lack of holism, strategic alignment, differing perceptions of the state of cybersecurity or difficulty quickly adapting to a changing cyber threat landscape.

TABLE 34. Weights for category 'Identify' and IG3.

C	N_o	W_c	W_o
ID.AM	12	0.29	$1/12$
ID.BE	6	0.15	$1/6$
ID.GV	5	0.12	0.20
ID.RA	9	0.22	$1/9$
ID.RM	4	0.10	0.25
ID.SC	5	0.12	0.20

TABLE 35. Weights for category 'Protect' and IG1.

C	N_o	W_c	W_o
PR.AC	7	0.24	$1/7$
PR.AT	1	0.03	1.00
PR.DS	2	0.07	0.50
PR.IP	8	0.28	0.125
PR.MA	6	0.21	$1/6$
PR.PT	5	0.17	0.20

TABLE 36. Weights for category 'Protect' and IG2.

C	N_o	W_c	W_o
PR.AC	12	0.19	$1/12$
PR.AT	4	0.06	0.25
PR.DS	6	0.10	$1/6$
PR.IP	18	0.30	$1/18$
PR.MA	15	0.24	$1/15$
PR.PT	7	0.11	$1/7$

TABLE 37. Weights for category 'Protect' and IG3.

C	N_o	W_c	W_o
PR.AC	15	0.19	$1/15$
PR.AT	4	0.05	0.25
PR.DS	10	0.12	0.10
PR.IP	24	0.30	$1/24$
PR.MA	17	0.20	$1/17$
PR.PT	11	0.14	$1/11$

TABLE 38. Weights for category 'Detect' and IG1.

C	N_o	W_c	W_o
DE.AE	1	0.25	1.00
DE.CM	2	0.50	0.50
DE.DP	1	0.25	1.00

TABLE 39. Weights for category 'Detect' and IG2.

C	N_o	W_c	W_o
DE.AE	3	0.25	$1/3$
DE.CM	6	0.50	$1/6$
DE.DP	3	0.25	$1/3$

TABLE 40. Weights for category 'Detect' and IG3.

C	N_o	W_c	W_o
DE.AE	6	0.26	$1/6$
DE.CM	11	0.48	$1/11$
DE.DP	6	0.26	$1/6$

TABLE 41. Weights for category 'Respond' and IG1.

C	N_o	W_c	W_o
RS.RP	0	0.00	0.00
RS.CO	1	0.50	1.00
RS.AN	0	0.00	0.00
RS.MI	1	0.50	1.00
RS.IM	0	0.00	0.00

TABLE 42. Weights for category 'Respond' and IG2.

C	N_o	W_c	W_o
RS.RP	1	0.10	1.00
RS.CO	2	0.20	0.50
RS.AN	2	0.20	0.50
RS.MI	3	0.30	$1/3$
RS.IM	2	0.20	0.50

TABLE 43. Weights for category 'Respond' and IG3.

C	N_o	W_c	W_o
RS.RP	2	0.11	0.50
RS.CO	3	0.17	$1/3$
RS.AN	5	0.28	0.20
RS.MI	6	0.33	$1/6$
RS.IM	2	0.11	0.50

TABLE 44. Weights for category 'Recover' and IG1.

C	N_o	W_c	W_o
RC.RP	0	0.00	0.00
RC.IM	0	0.00	0.00
RC.CO	0	0.00	0.00

Our proposal comprises a common set of expected cybersecurity results rooted in the most recognized cybersecurity standards and initiatives, as well as a set of metrics that allow a homogeneous evaluation of cybersecurity at different levels. This is orchestrated by CyberTOMP, a process for managing cybersecurity at tactical and operational levels.

Together, these elements complement the standard for cybersecurity used at a strategic level, regardless of what

TABLE 45. Weights for category 'Recover' and IG2.

C	N_o	W_c	W_o
RC.RP	0	0.00	0.00
RC.IM	0	0.00	0.00
RC.CO	0	0.00	0.00

TABLE 46. Weights for category 'Recover' and IG3.

C	N_o	W_c	W_o
RC.RP	1	0.17	1.00
RC.IM	2	0.33	0.50
RC.CO	3	0.50	$1/3$

this standard is, being able to be used as is, out of the box, for the holistic management of cybersecurity at all levels while maintaining alignment with the corporate cybersecurity strategy.

This proposal is being implemented in an entity in the Public Sector, a process that will provide the necessary feedback for its evolution and formal validation, results we hope to share with the scientific community in a future study.

APPENDIX A
ULEO TABLES

See Tables 4–26.

APPENDIX B
FUNCTIONAL AREAS INVOLVED IN CYBERSECURITY AND CORRESPONDENCE CYBERPROTECTION PRIORITIES - IGs

See Tables 27 and 28.

APPENDIX C
WEIGHTS OF EVERY CYBERSECURITY FUNCTION, CATEGORY AND EXPECTED OUTCOME

See Tables 29–46.

REFERENCES

[1] F. Y. Sattarova and T. H. Kim, "IT security review: Privacy, protection, access control, assurance and system security," *Int. J. Multimedia Ubiquitous Eng.*, vol. 2, no. 2, pp. 17–32, 2007.

[2] J. L. Fennelly, *Effective Physical Security*. Oxford, U.K.: Butterworth-Heinemann, 2016.

[3] M. E. Whitman and J. Herbert Mattord, *Management of Information Security*. Boston, MA, USA: Cengage Learning, 2013.

[4] R. von Solms, "Information security management: Why standards are important," *Inf. Manage. Comput. Secur.*, vol. 7, no. 1, pp. 50–58, Mar. 1999.

[5] M. E. Whitman and J. H. Mattord, *Principles of Information Security*. Boston, MA, USA: Cengage Learning, 2021.

[6] T. Chmielecki, P. Pacyna, P. Potrawka, N. Rapacz, R. Stankiewicz, and P. Wydrych, "Enterprise-oriented cybersecurity management," in *Proc. Ann. Comput. Sci. Inf. Syst.*, Sep. 2014, pp. 1–8.

[7] N. Kshetri, *Cybersecurity Management: An Organizational and Strategic Approach*. Toronto, ON, Canada: University of Toronto Press, 2021.

[8] R. von Solms and J. van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, Oct. 2013, doi: 10.1016/j.cose.2013.04.004.

[9] R. Reid and J. Van Niekerk, "From information security to cyber security cultures," in *Proc. Inf. Secur. South Afr.*, Aug. 2014, pp. 1–7.

[10] J. V. D. Ham, "Toward a better understanding of 'Cybersecurity,'" *Digit. Threats, Res. Pract.*, vol. 2, no. 3, pp. 1–3, Sep. 2021.

[11] M. Roopak, G. Y. Tian, and J. Chambers, "An intrusion detection system against DDoS attacks in IoT networks," in *Proc. 10th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2020, pp. 562–567.

[12] R. A. Rothrock, J. Kaplan, and F. Van der Oord, "The board's role in managing cybersecurity risks," *MIT Sloan Manag. Rev.*, vol. 59, no. 2, pp. 12–15, 2018.

[13] K. T. Dean, "Cyber-security holism: A system of solutions for a distributed problem," Marine Corps Command and Staff College, Quantico, VA, USA, Tech. Rep. ADA601717, 2013.

[14] H. I. Kure and S. Islam, "Assets focus risk management framework for critical infrastructure cybersecurity risk management," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 4, no. 4, pp. 332–340, Dec. 2019.

[15] R. Phillips and B. Tanner, "Breaking down silos between business continuity and cyber security," *J. Bus. Continuity Emergency Planning*, vol. 12, no. 3, pp. 224–232, 2019.

[16] R. Rajan, N. P. Rana, N. Parameswar, S. Dhir, Sushil, and Y. K. Dwivedi, "Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management," *Technol. Forecasting Social Change*, vol. 170, Sep. 2021, Art. no. 120872.

[17] I. N. Fovino, "Cybersecurity, our digital anchor," Eur. Union, Luxembourg, Tech. Rep. JRC121051, 2020, doi: 10.2760/352218.

[18] D. Sulistyowati, F. Handayani, and Y. Suryanto, "Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS," *Int. J. Informat. Visualizat.*, vol. 4, no. 4, p. 225, Dec. 2020.

[19] A. Bahuguna, R. K. Bisht, and J. Pande, "Roadmap amid chaos: Cyber security management for organisations," in *Proc. 9th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2018, pp. 1–6.

[20] R. Miñana. (2021). *?'Qué es Capability Maturity Model Integration? (CMMI)*. Accessed: Jul. 7, 2022. [Online]. Available: https://www2.deloitte.com/es/es/pages/technology/articles/que-es-cmmi-capability-maturity-modelintegration.html

[21] K. Balla, M. Tang, P. Mowat, M. Rasking, S. Chaobo, E. van Veenendaal, and Z. Hongbao, "Changes in CMMI 2.0 and how they can affect TMMi," TMMi Foundation, Bulverde, TX, USA, Tech. Rep., 2020.

[22] ISACA. *CMMI Adoption & Transition Guidance 2021*. Accessed: Jul. 7, 2022. [Online]. Available: https://cmmiinstitute.com/getattachment/5868888b-5f37-4715-bc8b-c43250ec0abc/attachment.aspx

[23] C. Agutter, "ITIL 4 essentials, second edition," IT Governance Publishing Ltd., Cambridge, U.K., Tech. Rep. 5524, 2020.

[24] *ITIL Foundation. ITIL 4 Edition. Glossary*, Axelos, London, U.K., 2019.

[25] R. Jašek, L. Králík, and M. Popelka, "ITIL and information security," in *Proc. AIP Conf.*, Helsinki, 2015, Art. no. 550020.

[26] E. R. Larrocha, G. Díaz, J. M. Minguet, M. Castro, and A. Vara, "Filling the gap of information security management inside ITIL: Proposals for posgraduate students," in *Proc. IEEE EDUCON Conf.*, Apr. 2010, pp. 907–912.

[27] J. Gillingham. (Aug. 2021). *An Introduction To Information Security Management in ITIL*. Accessed: Jul. 7, 2022. [Online] Available: https://www.invensislearning.com/blog/information-security-management/

[28] *UNE-ISO/IEC 27001. Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información (SGSI) Requisitos*. AENOR, Madrid, Spain, 2014

[29] *UNE-ISO/IEC 27002. Tecnología de la Información. Técnicas de Seguridad. Código de Prácticas Para Los Controles de Seguridad de la Información*, AENOR, Madrid, Spain, 2015.

[30] H. R. Suárez, J. D. P. Álvarez, and M. G. Hidalgo, "Ciber-resiliencia. Aproximación a un marco de medición," Nat. Inst. Commun. Technol. (INTECO), Tech. Rep., 2014.

[31] *IMC_01—Metodología de Evaluación de Indicadores Para Mejora de la Ciberresiliencia (IMC)*, Spanish Nat. Cybersecur. Inst. (INCIBE), 2020.

[32] G. D. España, "Real decreto 311/2022, de 3 de mayo, por el que SE regula el esquema nacional de seguridad," *Boletín Oficial del Estado*, vol. 106, pp. 61715–61804, May 2020.

[33] CCN. *Guías Esquema Nacional de Seguridad 2022*. Accessed: Jul. 7, 2022. [Online] Available: https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html

[34] *Guía de Seguridad CCN-STIC-806. Esquema Nacional de Seguridad, Plan de Adecuación*, Centro Criptológico Nacional, Madrid, Spain, 2011.

[35] Centro Criptológico Nacional. (2021). *Adecuación al ENS y Seguimiento del Progreso*. Accessed: Jul. 7, 2022. [Online]. Available: https://www.ccn-cert.cni.es/gestion-de-incidentes/lucia/2-uncategorised/48-adecuacion-al-ens-y-seguimiento-del-progreso.html
[36] MITRE. *MITRE ATT&CK©, 2021*. Accessed: Jul. 7, 2022. [Online] Available: https://attack.mitre.org/
[37] E. S. Blake, A. Andy, P. M. Doug, C. N. Kathryn, G. P. Adam, and B. T. Cody, "MITRE ATT&CK©: Design and philosophy," MITRE, McLean, VA, USA, Tech. Rep., 2020
[38] R. Kwon, T. Ashley, J. Castleberry, and S. N. G. Gourisetti, "Cyber threat dictionary using MITRE ATT&CK matrix and NIST cybersecurity framework mapping," in *Proc. Resilience Week (RWS)*, Oct. 2020.
[39] W. Xiong, E. Legrand, and O. Åberg, and R. Lagerström, "Cyber security threat modeling based on the MITRE Enterprise ATT&CK matrix," *Softw. Syst. Model.*, vol. 21, pp. 157–177, Jun. 2021.
[40] *CIS Security Controls, Version 8*, CIS, East Greenbush, NY, USA, 2021
[41] B. Shamma, *Implementing CIS Critical Security Controls for Organizations on a Low-Budget*. Ann Arbor, MI, USA: ProQuest LLC, 2018.
[42] S. Gros, "A critical view on CIS controls," in *Proc. 16th Int. Conf. Telecommun. (ConTEL)*, Jun. 2021, pp. 122–128.
[43] OWASP. (2021). *OWASP TOP 10 Project*. Accessed: Jul. 7, 2022. [Online] Available: https://owasp.org/www-project-top-ten/
[44] M. Bach-Nutman, "Understanding the top 10 OWASP vulnerabilities," 2020, *arXiv:2012.09960*.
[45] *Center for Internet Security, CIS Community Defense Model, Version 2.0*, CIS, East Greenbush, NY, USA, 2021.
[46] MITRE. (2022). *MITRE ATT&CK© Enterprise Mitigations*. Accessed: Jul. 7, 2022. [Online] Available: https://attack.mitre.org/mitigations/enterprise/
[47] K. S. Wilson and M. A. Kiy, "Some fundamental cybersecurity concepts," *IEEE Access*, vol. 2, pp. 116–124, 2014.
[48] *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, NIST, Gaithersburg, MD, USA, 2018
[49] Organización de los Estados Americanos y AWS, "Ciberseguridad, marco NIST. Un abordaje integral de la ciberseguridad," Org. Amer. States (OEA), USA, White Paper, 5th ed. OEA, 2019.
[50] NIST Computer Security Resource Center. *SP 800 Series, 2021*. Accessed: Jul. 7, 2022. [Online] Available: https://csrc.nist.gov/publications/sp800
[51] *NIST Special Publication 800–53. Revision 5. Security and Privacy Controls for Information Systems and Organizations*, NIST, Gaithersburg, MD, USA, 2020
[52] *Adquisition and sustainment, Cybersecurity Maturity Model Certification (CMMC) Model Overview. Version 2.0*, Office of the Under Secretary of Defense, Department of Defense, Richmond, VA, USA, 2021
[53] Office of the Under Secretary of Defense. (Dec. 2021). *Adquisition and Sustainment, CMMC 2.0 Spreadsheet and Mapping*. Accessed: Jul. 7, 2022. [Online] Available: https://www.acq.osd.mil/cmmc/docs/CMMCModel_V2_Mapping.xlsx
[54] T. Limba, T. Plėta, K. Agafonov, and M. Damkus, "Cyber security management model for critical infrastructure," *Entrepreneurship Sustainability Issues*, vol. 4, no. 4, pp. 559–573, 2017, doi: 10.9770/jesi.2017.4.4(12).
[55] M. Tvaronaviciene, T. Pleta, and S. D. Casa, "Cyber security management model for critical infrastructure protection," in *Proc. Int. Sci. Conf. Contemp. Issues Bus., Manag. Econ. Eng.*, 2021, pp. 133–139.
[56] K. Barbara, E. W. N. Bernroider, and R. Walser, "Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST cybersecurity framework," in *Proc. Nordic Conf. Secure IT Syst.*, Cham, Switzerland: Springer, 2018, pp. 369–384.
[57] N. Tissir, S. El Kafhali, and N. Aboutabit, "Cybersecurity management in cloud computing: Semantic literature review and conceptual framework proposal," *J. Reliable Intell. Environments*, vol. 7, no. 2, pp. 69–84, Jun. 2021.
[58] L. Maximilian, E. Markl, and M. Aburaia, "Cybersecurity management for (industrial) Internet of Things-challenges and opportunities," *J. Inf. Technol. Softw. Eng.*, vol. 8, no. 5, pp. 1–9, 2018.
[59] S. Ali, "Cybersecurity management for distributed control system: Systematic approach," *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 11, pp. 10091–10103, Nov. 2021.
[60] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, "Harnessing artificial intelligence capabilities to improve cybersecurity," *IEEE Access*, vol. 8, pp. 23817–23837, 2020.
[61] F. Alrimawi, L. Pasquale, and B. Nuseibeh, "On the automated management of security incidents in smart spaces," *IEEE Access*, vol. 7, pp. 111513–111527, 2019.
[62] M. Antunes, M. Maximiano, R. Gomes, and D. Pinto, "Information security and cybersecurity management: A case study with SMEs in Portugal," *J. Cybersecurity Privacy*, vol. 1, no. 2, pp. 219–238, Apr. 2021.
[63] M. S. Tisdale, "Architecting a cybersecurity management framework," *Issues Inf. Syst.*, vol. 17, no. 4, pp. 1–284, 2016.
[64] L. Axon, A. Erola, A. Janse van Rensburg, J. R. C. Nurse, M. Goldsmith, and S. Creese, "Practitioners' views on cybersecurity control adoption and effectiveness," in *Proc. 16th Int. Conf. Availability, Rel. Secur.*, Aug. 2021, pp. 1–10.
[65] United States Government Accountability Office, "Critical infrastructure protection. Sector-specific agencies need better measure cybersecurity progress," U.S. Government Accountability Office (GAO), USA, Tech. Rep. GAO-16-79, 2015.
[66] T. Kissoon, "Optimum spending on cybersecurity measures," *Transforming Government, People, Process Policy*, vol. 14, no. 3, pp. 417–431, doi: 10.1108/TG-11-2019-0112.
[67] J. Breier and L. Hudec, "On selecting critical security controls," in *Proc. Int. Conf. Availability, Rel. Secur.*, Sep. 2013, pp. 582–588.
[68] P. Speight, "Business continuity," *J. Appl. Secur. Res.*, vol. 6, no. 4, pp. 529–554, 2011.
[69] B. Zawada, "The practical application of ISO 22301," *J. Bus. Continuity Emergency Planning*, vol. 8, no. 1, pp. 83–90, 2014.
[70] M. H. Bejarano, R. J. Rodriguez, and J. Merseguer, "A vision for improving business continuity through cyber-resilience mechanisms and frameworks," in *Proc. 16th Iberian Conf. Inf. Syst. Technol. (CISTI)*, Jun. 2021, pp. 1–5.
[71] R. L. Tammineedi, "Business continuity management: A standards-based approach," *Inf. Secur. J., A Global Perspective*, vol. 19, no. 1, pp. 36–50, Mar. 2010.
[72] M. Clark, J. Espinosa, and W. Delone, "Defending organizational assets: A preliminary framework for cybersecurity success and knowledge alignment," in *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, 2020, pp. 4283–4292.
[73] H. Kure, S. Islam, and M. Razzaque, "An integrated cyber security risk management approach for a cyber-physical system," *Appl. Sci.*, vol. 8, no. 6, p. 898, May 2018.
[74] A. Couce-Vieira, D. R. Insua, and A. Kosgodagan, "Assessing and forecasting cybersecurity impacts," *Decis. Anal.*, vol. 17, no. 4, pp. 356–374, Dec. 2020.
[75] Z. A. Collier and I. Linkov, and J. H. Lambert, "Four domains of cybersecurity: A risk-based systems approach to cyber decisions," *Environ. Syst. Decis.*, vol. 33, pp. 2194–5411, Nov. 2013.
[76] A. M. Rea-Guaman, J. Mejía, T. San Feliu, and J. A. Calvo-Manzano, "AVARCIBER: A framework for assessing cybersecurity risks," *Cluster Comput.*, vol. 23, no. 3, pp. 1827–1843, Sep. 2020.
[77] C. T. Harry and N. Gallagher, "An effects-centric approach to assessing cybersecurity risk," Center Int. Secur. Stud., Univ. Maryland, College Park, MD, USA, Tech. Rep. resrep20424, 2019.
[78] A. A. Ganin, P. Quach, M. Panwar, Z. A. Collier, J. M. Keisler, D. Marchese, and I. Linkov, "Multicriteria decision framework for cybersecurity risk assessment and management," *Risk Anal.*, vol. 40, no. 1, pp. 183–199, Jan. 2020.
[79] J. R. S. Cristóbal, "Complexity in project management," *Proc. Comput. Sci.*, vol. 121, pp. 762–766, Jan. 2017.
[80] CIS. (2021). *CIS Critical Security Controls V8 Mapping to NIST CSF*. Accessed: Jul. 7, 2022. [Online] Available: https://www.cisecurity.org/white-papers/cis-controlsv8-mapping-to-nist-csf/
[81] NIST. (2021). *Mappings: Cybersecurity Framework and Privacy Framework to Rev. 5*. Accessed: Sep. 23, 2022. [Online] Available: https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/final/documents/csf-pf-to-sp800-53r5-mappings.xlsx
[82] H. Jiang. (2021). *Cybersecurity Domain Map Ver 3.0*. Accessed: Jul. 7, 2022. [Online]. Available: https://www.linkedin.com/pulse/cybersecurity-domain-map-ver-30-henry-jiang/
[83] A. Ahmad, K. C. Desouza, S. B. Maynard, H. Naseer, and R. L. Baskerville, "How integration of cyber security management and incident response enables organizational learning," *J. Assoc. Inf. Sci. Technol.*, vol. 71, no. 8, pp. 939–953, Aug. 2020.
[84] N. Chowdhury and V. Gkioulos, "Cyber security training for critical infrastructure protection: A literature review," *Comput. Sci. Rev.*, vol. 40, May 2021, Art. no. 100361.
[85] H. I. Kure, S. Islam, M. Ghazanfar, A. Raza, and M. Pasha, "Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system," *Neural Comput. Appl.*, vol. 34, no. 1, pp. 493–514, Jan. 2022.

[86] A. Zimmermann, *Gestión del Cambio Organizacional: Caminos y Herramientas*, 2nd ed. Quito: Ediciones Abya-Yala, 2000.
[87] *A guide to the Project Management Body of Knowledge. PMBoK Guide*. 7th ed., Project Management Institute, Newtown Square, PA, USA, 2021.

MANUEL DOMÍNGUEZ-DORADO received the B.Sc. and M.Sc. degrees in computer science from the University of Extemadura and the master's degree in cybersecurity management (CISO) from the International Institute for Global Security Studies. He worked as a Researcher with the University of Extemadura. Nowadays, he works as the Cybersecurity Manager of the Public Business Entity Red.es. His research interests include cybersecurity in organizations and in communications networks and cybersecurity management.

JAVIER CARMONA-MURILLO received the Ph.D. degree in computer science and communications from the University of Extremadura, Spain, in 2015. From 2005 to 2009, he was a Research and Teaching Assistant. Since 2009, he has been an Associate Professor with the Department of Computing and Telematics System Engineering, Universidad de Extremadura. During the past years, he has spent research periods with the Centre for Telecommunications Research, King's College London, U.K., and Aarhus University, Denmark. His current research interests include 5G networks, mobility management protocols, performance evaluation, and the quality of service support in future mobile networks.

DAVID CORTÉS-POLO received the degree in computer science from the University of Extremadura, Spain, and the Ph.D. degree in telematics from the University of Extremadura, in 2015. From 2011 to 2014, he worked as a Researcher and a Teaching Assistant with the University of Extremadura. From 2020 to 2022, he was an Associate Professor with the Department of Computing and Telematics System Engineering, Universidad de Extremadura. Since September 2022, he has been an Assistant Professor at King Juan Carlos University, Madrid. His research interests include IP-based mobility management protocols, performance evaluation, and network CDR analytics.

FRANCISCO J. RODRÍGUEZ-PÉREZ received the degree in computer science engineering and the Ph.D. degree from the University of Extremadura, Spain, in 2000 and 2015, respectively. His research interests include the design and implementation of algorithms and signaling techniques to improve reliability, performance, delay, computing load, and energy consumption, and other metrics of prioritized quality of service aware flows over multiprotocol label switching packet transport networks, the Internet of Things systems, wireless *ad-hoc* networks, and smart cities environments.

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 13 June 2023, accepted 13 July 2023, date of publication 20 July 2023, date of current version 11 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3297446

RESEARCH ARTICLE

Safety and Cybersecurity Assessment Techniques for Critical Industries: A Mapping Study

IEVGEN BABESHKO[1,2] AND FELICITA DI GIANDOMENICO[2]

[1]Computer Systems, Networks and Cybersecurity Department, National Aerospace University "Kharkiv Aviation Institute," 61070 Kharkiv, Ukraine
[2]Istituto di Scienza e Tecnologie dell'Informazione Alessandro Faedo-CNR, 56127 Pisa, Italy

Corresponding author: Ievgen Babeshko (ievgen.babeshko@isti.cnr.it)

ABSTRACT The paper presents a mapping study of safety and cybersecurity assessment techniques used in critical industries such as nuclear power plants, the oil and gas sector, autonomous vehicles, railways, etc., with particular emphasis on instrumentation and control systems (I&C). Modern I&Cs are complex electronic systems comprising thousands of components, therefore their reliability and safety when employed in critical application domains are challenging. With the development and integration of Industry 4.0 technologies such systems become more open for communication and flexible usage due to gradual interconnection with public networks and the Internet, but new cybersecurity and safety challenges are introduced. This paper states research questions and provides analysis results of recent relevant sources. Initially, 320 records (acquired between 2018 and 2022 inclusive) were identified. Later on, 187 studies were processed to check eligibility criteria. Overall, this mapping study includes 49 papers, after examining the pre-defined criteria and guidelines. The results of the analysis performed allow to systemize techniques being utilized in practice right now, as well as to identify trends of further techniques development. In fact, although the techniques used are not novel and most of them have been used for decades, our study shows that there are still some new trends in this field. In particular, the unified safety and cybersecurity assessment technique is a promising research direction, worth further investigation.

INDEX TERMS Safety, cybersecurity, assessment techniques, instrumentation and control systems.

I. INTRODUCTION

Safety and cybersecurity issues have always been among the top priorities in critical industries, but today they are becoming even more urgent. Assessment of modern critical instrumentation and control systems is a complicated process, principally due to the size (system consists of many components) and volatility (system perpetually evolves throughout lifecycle) problem. Cybersecurity contributes to safety and sometimes conflicts with it, but it is not always considered at all lifecycle stages together with safety. The results of the assessment are considerably dependent on metrics/techniques/assumptions chosen. Therefore, arranging an assessment process based on solid methodologies/techniques is of high importance, because there is a risk of safety underestimation or overestimation, with potential severe impact on the service delivered. With the focus on critical sectors, this paper considers the following domains: nuclear power plants, the oil and gas sector, autonomous vehicles, and railways.

The purpose of the work is to survey recent literature in order to develop a mapping study useful to understand:

- which 'classical' (described in standards or other normative documents) assessment techniques are used in recent primary studies;
- advancements of such "classical" techniques, to respond to needs posed by modern critical systems;
- application of specific techniques to assess different metrics/properties they were originally developed for (i.e. modification of reliability assessment techniques for cybersecurity assessment);
- combinations of techniques used;
- needs for additional research in the generalization of assessment techniques so as to provide a unified assessment approach.

The associate editor coordinating the review of this manuscript and approving it for publication was Diana Gratiela Berbecaru.

The paper is organized as follows. In Section II we analyze existing systematic literature reviews, surveys, and mapping studies on adjacent topics. A description of the approach used, as well as research questions, are provided in Section III. In section IV we present our analysis of the collected data and our results in response to the research questions. In Section V we list key findings. Section VI presents the threats to the validity. Finally, we make conclusions and outline future research directions in Section VII.

II. COMPARISON WITH RELATED WORKS

This study fills a gap in research on cybersecurity and safety assessment techniques: although several reviews exist, to the best of the authors' knowledge no previous work provides a comprehensive and up-to-date systematic mapping study that covers different critical domains. To facilitate comparison, related works are summarized in Table 1. For each work, the following information is presented:

- Reference;
- Year of publication;
- Application domain;
- The number of references included in the paper.

TABLE 1. Comparison with other systematic literature reviews, surveys, and mapping studies.

Ref.	Year	Domain	Number of references
[19]	2019	Nuclear	32
[24]	2021	Nuclear	52
[30]	2021	Critical Infrastructures	107
[41]	2020	Autonomous Vehicles	23

The review made in [19] discusses U.S. Nuclear Regulatory Commission (NRC)'s proposed vulnerability assessment methodology, as well as additions and changes that must be made to increase its efficacy. It mainly includes references to normative documents for the nuclear field, not research studies.

In [24], the focus is put on the identification of scientific papers discussing cybersecurity frameworks, standards, guidelines, best practices, and any additional cybersecurity protection measures for the nuclear domain. Safety issues are not covered, as well as cybersecurity and safety co-engineering were not addressed in this report.

Report [30] focuses on studies that combine Bayesian Networks and Graph Theory for safety and cybersecurity integrated assessment. Other techniques and their combinations are not covered.

In [41], blockchain-based methods are discussed for cybersecurity assurance in the autonomous vehicles domain.

III. REVIEW APPROACH

A. GENERAL INFORMATION

This study was performed according to guidelines on systematic literature reviews and surveys [59] and guidelines for conducting systematic mapping studies [60]. First of all, a set of research questions that our study aims to answer was formulated. These research questions address safety and cybersecurity techniques used, as well as their combinations and modifications, and are listed in Section III-B. From the research questions, we defined the research query and then the search strategy, as presented in Section III-C. We applied this search strategy to the following popular electronic databases:

- IEEE Explore (https://ieeexplore.ieee.org/);
- ScienceDirect (https://www.sciencedirect.com/);
- SpringerLink (https://link.springer.com/);
- Wiley (https://onlinelibrary.wiley.com/);
- MDPI (https://www.mdpi.com/).

After that, the selection process described in Section III-D was applied so as to identify the set of relevant primary studies that we analysed to answer the research questions. We present the results of our analysis in Section IV and Section V.

B. RESEARCH QUESTIONS

Implementation of deep and throughout safety assessment was a strong requirement for critical industries for a long time, but the essential rise of cyberattacks and malware targeted for this particular sector during the last 5 years has intensified the discussions around the convergence of safety and cybersecurity.

Traditional safety assessment approaches either did not focus on cybersecurity, leaving its issues to particular separate disciplines, or at most referred to generic cybersecurity approaches and guidelines which were not feasible to follow or implement.

To overcome the abovementioned challenges, traditional approaches were modified in different ways, so as to consider cybersecurity-related threats and make assessment more comprehensive. Such modifications could be the following:

- assessment techniques determine the impact of cybersecurity threats and vulnerabilities on system safety as an adjunct to 'traditional' hazards; an example of such an approach is Hazard Analysis and Risk Assessment (HARA) combined with Threat Analysis and Risk Assessment (TARA);
- adaptation of traditional dependability and safety assessment techniques to the cybersecurity domain; an example of such an approach is Intrusion Modes, Effects, and Criticality Analysis (IMECA), where the traditional Failure Modes, Effects, and Criticality Analysis (FMECA) approach is utilized for intrusion analysis;
- include combinations of several safety and cybersecurity assessment techniques.

Despite the variety of approaches safety and cybersecurity assessment for critical industries is still a challenge requiring further investigation.

The following research questions were formulated to attain such investigation:

- (RQ1) Which safety indicators (metrics) are considered during safety assessment?
- (RQ2) Which cybersecurity indicators (metrics) are considered during cybersecurity assessment?
- (RQ3) Which techniques (classical, modified, combinations) are used for safety assessment?
- (RQ4) Which techniques (classical, modified, combinations) are used for cybersecurity assessment?
- (RQ5) Which limitations are applied to techniques currently used?

C. SEARCH STRATEGY

The search string used for the selection of studies is presented in Table 2. Only studies published from 2018 through 2022 inclusive were considered.

TABLE 2. Search string.

({safety} < OR > {cybersecurity} < OR > {security}) < AND > ({assessment} < OR > {evaluation} < OR > {analysis}) < AND > ({nuclear} < OR > {oil} < OR > {vehicle} < OR > {transport} < OR > {railway} < OR > {automotive})

D. SELECTION PROCESS

The following inclusion and exclusion criteria (Table 3) were applied to the studies identified using the search string (figure 1).

TABLE 3. Inclusion and exclusion criteria.

Inclusion Criteria
• Papers published in journals or conference proceedings. • Studies presenting a modified technique or combination of several techniques and description of usage • Studies providing use cases to support the performed assessment or introducing a tool • Studies that are peer-reviewed
Exclusion Criteria
• Studies that are PhD thesis, published in workshop proceedings and book chapters. • Studies from fields different from safety and cybersecurity assessment in critical industries domains (nuclear, aerospace, maritime, oil and gas, railway, automotive) • Studies that do not provide clear evidence of the benefits obtained through a proposed modified technique (criteria of clearness: measurable results compared to unmodified technique(s)) • Multiple studies authored by the same researchers on the same/similar topic (in this case the more relevant source was chosen, i.e. journal paper had priority over conference proceeding, most recent one had priority over older ones) • Studies that are not written in English

To ensure quality assessment the following questions were addressed:

- Are claims clearly defined?
- Is it possible to reuse the presented assessment technique, its modification or a combination of techniques (is description detailed enough)?

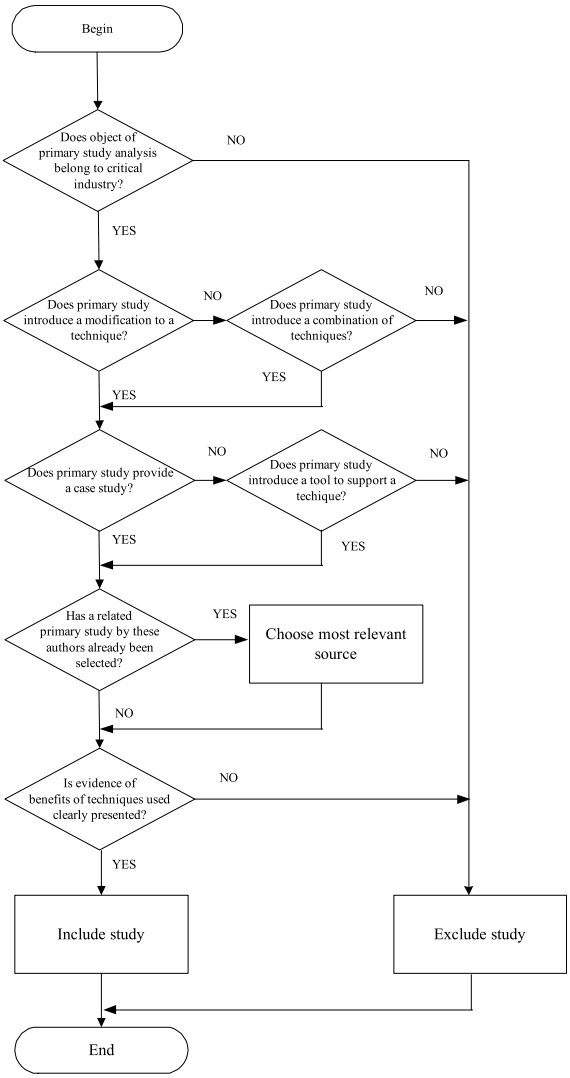


FIGURE 1. Flowchart of the selection process for each primary study.

Initially, 320 records (acquired between 2018 and 2022 inclusive) were identified according to the search string. After examining titles, abstracts and keywords, the number of records was reduced to 187 by excluding not relevant studies.

After the application of the selection process shown on Fig. 1, 49 papers were selected from a total number of 187.

IV. DATA ANALYSIS

A. DISTRIBUTION BY YEAR AND TYPE

The distribution of primary studies by years in the window 2018-2022 is shown in Fig. 2.

Most of the studies are journal papers as shown in Table 4 and Fig. 3, but conference proceedings were also analysed.

B. OVERVIEW OF THE ADOPTED TECHNIQUES AND ASSESSMENT METRICS

The performed research has shown that techniques listed in Table 5 below are typically used during the safety and/or cybersecurity assessment process.

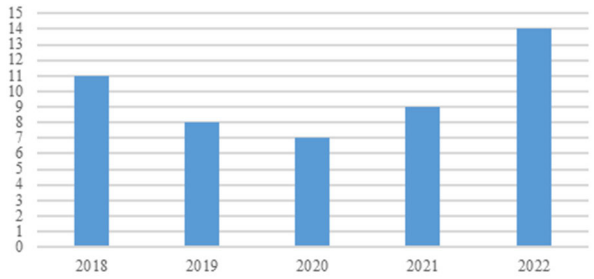


FIGURE 2. Distribution of primary studies by year.

TABLE 4. Year and type of primary studies.

Year	Type	List of References
2018	Conference	[26], [27], [50]
	Journal	[18], [21], [29], [32], [39], [40], [45], [51]
2019	Conference	[38]
	Journal	[1], [23], [33], [34], [35], [37], [47]
2020	Conference	-
	Journal	[12], [20], [22], [36], [46], [49], [52]
2021	Conference	[2], [4], [6], [7], [42], [48]
	Journal	[11], [28], [31]
2022	Conference	[3], [14]
	Journal	[5], [8], [9], [10], [13], [15], [16], [17], [25], [44], [43], [53]

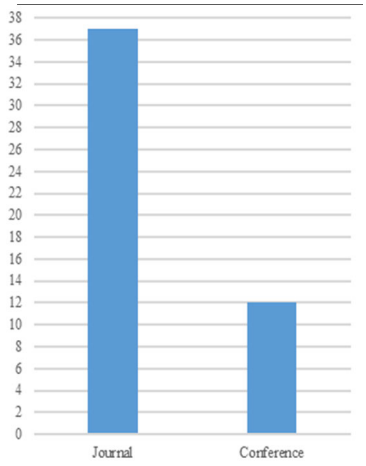


FIGURE 3. Distribution of primary studies by type.

We classified techniques listed in Table 5 by their focus (safety or cybersecurity) and analysis process (spreadsheet-based, scenario-based, tree-based, and model-based) and prepared a taxonomy shown in Fig. 4.

By spreadsheet-based process (Fig. 5) we mean an approach that gathers data into a single spreadsheet and the main deliverables (metrics, assessment results) are based

TABLE 5. Techniques used for safety and cybersecurity analysis.

Technique Id	Abbreviation	Technique Title
T1	FMEDA	Failure Modes, Effects, and Diagnostics Analysis
T2	FTA	Fault Tree Analysis
T3	BDMP	Boolean-driven Markov process
T4	HARA	Hazard Analysis and Risk Assessment
T5	RBD	Reliability Block Diagram
T6	RBI	Risk-based inspection
T7	ATA	Attack tree analysis
T8	PSA	Probabilistic safety assessment
T9	SM	Semi-Markov
T10	BN	Bayesian Networks
T11	MC	Monte-Carlo Simulation
T12	BA	Bowtie Analysis
T13	ETA	Event Tree Analysis
T14	FMEA / FMECA	Failure Modes and Effects Analysis / Failure Modes, Effects, and Criticality Analysis
T15	STAMP	Systems-Theoretic Accident Model and Process
T16	DVAG	Dynamic Vulnerability Assessment Graph
T17	MBAEM	Model-based Assurance Evidence Management.
T18	TARA	Threat Analysis and Risk Assessment
T19	IMECA	Intrusion Modes, Effects, and Criticality Analysis
T20	CRA	Cybersecurity Risk Assessment

on processing the spreadsheet data. A typical example of a spreadsheet-based process is a failure mode, effect, and diagnostic analysis (FMEDA), a systematic analysis technique to obtain subsystem/product level failure rates, failure modes, and diagnostic capability. The main purpose of FMEDA is to evaluate hardware architecture metrics and safety goal violations due to random hardware failures and provide sufficient information to improve safety gaps if the required hardware safety level is not fulfilled [54].

Another example of spreadsheet-based process is a risk-based inspection (RBI) which is well-established and used in the Oil& Gas and Chemical industries. This approach, along with risk-based maintenance, is described by API RP 581 [55], originally developed for application in the refining industry. The standard represents a correlation between maintenance activities and main events in the industries. RBI is also adapted and applied in many other sectors and inspection activities, allowing for the identification of failure mechanisms and rates based on equipment status.

Instead, tree-based techniques (Fig. 6) process graphical representation in the form of a tree. The classical example of a tree-based technique is a fault tree analysis (FTA) used for the reliability assessment of a system. FTA is a deductive

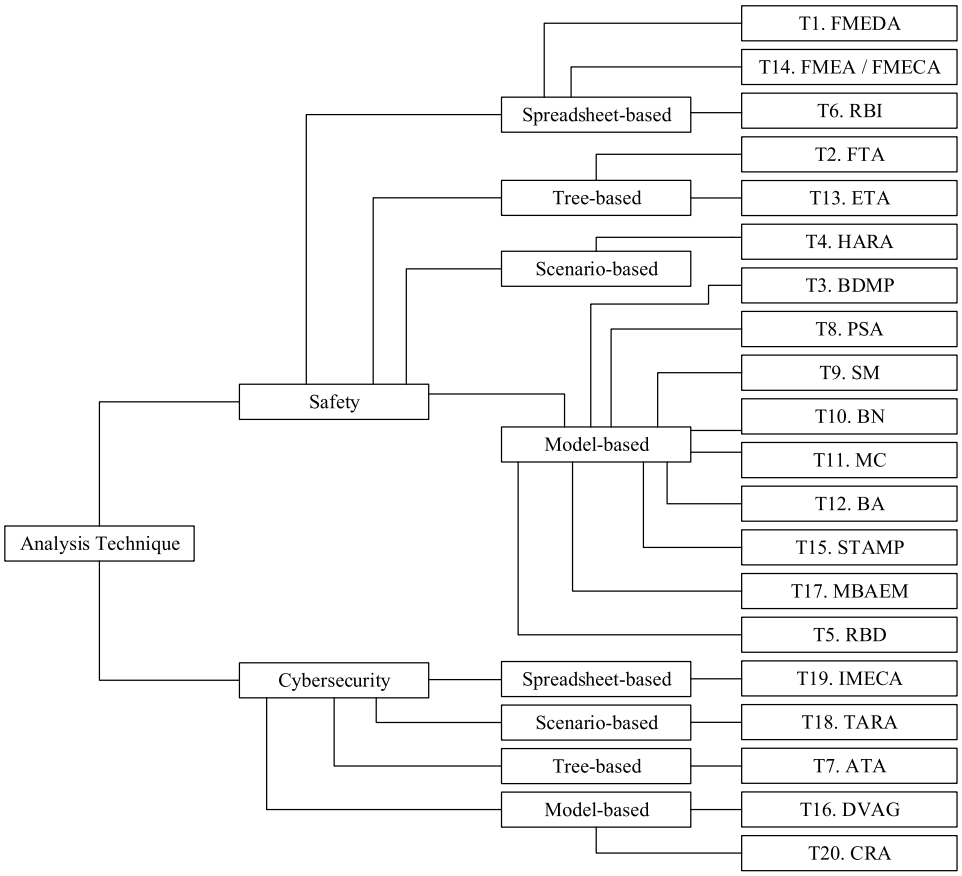


FIGURE 4. Taxonomy of analysis techniques.

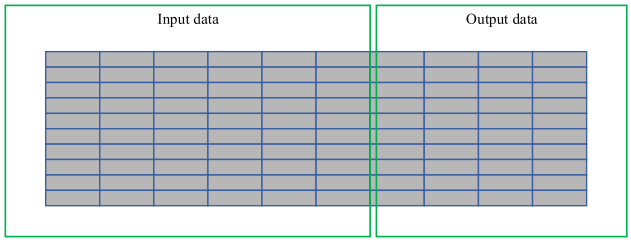


FIGURE 5. Spreadsheet-based technique.

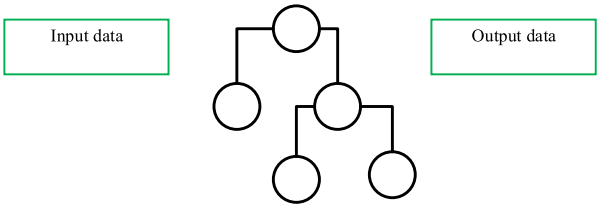


FIGURE 6. Tree-based technique.

process by means of which an undesirable event, called the top event, is postulated, and after that, the possible ways for this event to occur are systematically deduced. The deduction process is performed so that the fault tree embodies all

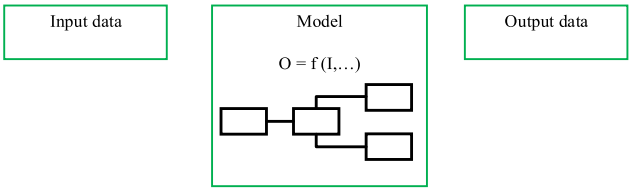


FIGURE 7. Model-based technique.

component failures (i.e., failure modes) that contribute to the occurrence of the top event. The fault tree itself is a graphical representation of the various combinations of failures that led to the occurrence of the top event [56]. In [45] it is proposed to apply FTA for cybersecurity assessment by using a model that integrates fault tree analysis, decision theory, and fuzzy theory to ascertain the current causes of cyberattack prevention failures and determine the vulnerability of a given cybersecurity system. Moreover, for cybersecurity assessment, another tree-based technique called attack tree analysis (ATA) is actively utilized [57].

By model-based techniques (Fig. 7) we mean approaches that perform an assessment using different models – graphs, equations etc.

For example, reliability block diagrams (RBD) represent sequences of system components and their connections. Each

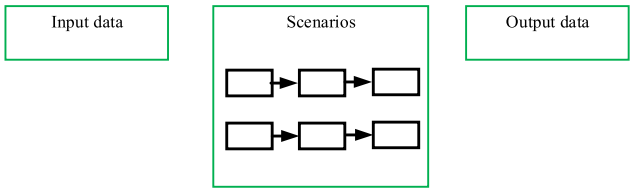


FIGURE 8. Scenario-based technique.

sequence consists of an input point and output point, several blocks representing system components, and the multiple paths from the input point to the output point that represent successful system operations, where an interruption of these paths may lead to the failure of the whole system. Therefore, an RBD model represents the static topology of I&C reliability, where the topology can be a serial, parallel or a combination of serial and parallel sections. Contrary to FTA, RBD models are success-oriented sequences that describe the function of a system by probabilistic means. Component blocks in an RBD are arranged to illustrate the proper combinations of working components that keep the entire system operational and, therefore, safe. Failure of a component can be represented by removing the component as well as its connections with other components from the sequence. When the number and position of failed components in the RBD model are such that there is no connection between the input and output point, the whole system fails.

Another example is a Bayesian network (BN) that represents a hypothesis of rationalizing from uncertain evidence to uncertain conclusions since it can perform the factorization of the collective distribution of variables, based on the conditional dependencies. BN helps to address uncertainty and incompleteness problems; thus, it is extensively applied in several domains. BNs are generally utilized for examining the hazards and vulnerabilities of networks, which are acyclic graphs that provide a quantitative and qualitative assessment of risks.

Model-based assurance evidence management (MBAEM) is another model-based technique that considers different activities for assurance evidence management, namely the determination of the evidence to provide, the possibility of reusing evidence, the collection of evidence information, tracing, evaluation, and change impact analysis of assurance evidence, and the use of the evidence for, e.g., compliance management and argumentation.

Finally, Probabilistic Safety Assessment (PSA) is the most common method to assess the risk of a nuclear power plant. It employs a graphical approach based on event and fault tree methods.

As for scenario-based processes (Fig. 8), they are typically based on profiling of scenarios collection obtained from different sources (accident, research, expert data, etc.) by focusing on safety and/or cybersecurity-relevant scenarios.

A typical example of a scenario-based process is HARA, where malfunctions and/or the functional insufficiencies are analyzed in terms of identification of both safety-relevant scenarios (known-safe and known-unsafe), as well as a set of unknown-unsafe scenarios, with further focus on required countermeasures.

The list of metrics is given in Table 6 and includes both safety and cybersecurity related metrics.

TABLE 6. Assessment metrics.

Metric Id	Metric Name
M1	SFF – Safe Failure Fraction
M2	SIL – Safety Integrity Level
M3	SPFM – Single-Point Fault Metric
M4	LFM – Latent (Multi-Point) Fault Metric
M5	PMHF – Probabilistic Metric for Hardware Failures
M6	PFH – Probability of Failure on Demand per Hour
M7	SL – Security Level
M8	ASIL – Automotive Safety Integrity Level
M9	Risk
M10	CDF – core damage frequency
M11	InTo-CSI – Intrusion Tolerance-based Cyber Security Index
M12	MTTC – Mean Time To Compromise
M13	CVSS – common vulnerability scoring system

SFF is a metric used to measure the likelihood of getting a dangerous failure that is not detected by diagnostics.

SIL is used to claim that all safety instrumented functions are operating satisfactorily under all stated conditions within a stated period of time.

SPFM is a hardware architectural metric used to show the sufficiency of safety mechanisms to prevent risk from single-point faults.

LFM is a hardware architectural metric used to show the sufficiency of safety mechanisms to prevent risk from latent faults.

PMHF is a probability of a safety goal violation caused by a random hardware failure.

PFH is the probability of dangerous failure that would prevent the system to be able to perform its safety function when required.

SL is a metric to measure how well a system component is protected from a certain level of threat and potential vulnerabilities.

ASIL is a risk classification metric.

CDF is a metric used to measure frequency and consequences considering initiating event frequency with system failure probabilities and fatalities (or environmental effects).

InTo-CSI is an index defined through relative comparison of two security states of the same system: a system without any cyber security controls, and a system with scrutiny controls.

The value of MTTC is the estimated figure of the time required for the valid attack assuming uniformly expended efforts.

CVSS is used to evaluate the severity of vulnerabilities, representing the virtual consequences on the vulnerable component in terms of confidentiality, integrity, and availability.

A considerable number of studies use Risk to represent the outputs of assessment technique utilization. In most cases, this metric represents the likelihood of the hazardous event and the severity of its consequences. Typical examples of what is used as a risk in the analysed studies are provided below. In [1], [4], [7], and [9] traditional risk priority number (RPN) is used, which is determined by three indicators: effect severity, occurrence probability, and detection difficulty. In [3] it is extended to cover risk interaction. In [5] risk assessment objectivity and accuracy are enhanced by the utilization of fuzzy confidence interval number (FCIN), generalized trapezoidal fuzzy numbers (GTrFN) evaluation model and the evaluation parameter sensitivity analysis. In [6] risk is calculated using the severity of the hazard, the exposure of that particular situation and the controllability of the system to mitigate hazardous situations. In [8] fairness risk is also considered separately from safety risk. In [10] special attention is given to considering assurance risks. In [12] risk is computed using potential risk impact due to vulnerabilities/attacks and the likelihood of the risk. In [13] risk includes attack cost, attack difficulty, and detected possibility.

C. USING PRIMARY STUDIES TO ANSWER RESEARCH QUESTIONS

To answer research questions (RQ1) and (RQ2), we have arranged the selected primary studies in the form of a table with the following columns (see Table 7):

- Reference;
- Techniques used (see Table 5);
- Metrics (see Table 6).

Based on the analysed studies, the resulting most popular techniques are listed in Table 8 below.

Therefore, the answer to RQ1 includes the following metrics: PFH, SFF, SIL, and ASIL are the most popular safety metrics. Also, in many studies, generic risk metric is used.

As for cybersecurity (RQ2), SL, MTTC, InTo-CSI, and CVSS scores are used as quantitative metrics. Just like with safety, the major part of studies considers generic risk metric more appropriate and comprehensive.

To answer research questions (RQ3) and (RQ4), we have arranged the list of selected primary studies in the form of a table with the following columns (see Table 10):

- Reference;
- Focus on safety;
- Focus on cybersecurity;
- Usage of several assessment techniques;
- Usage of modified assessment techniques;

TABLE 7. Techniques and metrics of primary studies.

Ref.	Techniques	Metrics
[1]	T14, T2	M9
[2]	T1, T2	M3, M4, M5
[3]	T14	M9
[4]	T14	M9
[5]	T14	M9
[6]	T4	M9
[7]	T14	M9
[8]	T14	M9
[9]	T14	M9
[10]	T17	M9
[11]	T18, T4	M8
[12]	T18	M9
[13]	T20	M9
[14]	T19	M9
[15]	T10	M13
[16]	T7	M9
[17]	T1,T14	M9
[18]	T11	M9
[20]	T8, T2, T13	M9, M10
[21]	T13	M11, M12
[22]	T9, T2, T13	M9
[23]	T2, T8, T13	M9
[25]	T16	M9
[26]	T8	M7, M9
[27]	T2	M9
[28]	T6	M9, M6
[29]	T10	M9
[31]	T15	M9
[32]	T10	M9
[33]	T10	M9
[34]	T16	M9
[35]	T10	M9
[36]	T10	M9
[37]	T2, T4, T14	M5, M6
[38]	T9, T10	M9
[39]	T12, T7	M9
[40]	T14	M9
[42]	T4, T18	M9
[43]	T2, T14	M9
[44]	T1	M1, M2, M3, M4, M5, M8
[45]	T2	M9
[46]	T2, T14	M8
[47]	T2	M9
[48]	T2	M9
[49]	T1	M9

TABLE 7. *(Continued.)* **Techniques and metrics of primary studies.**

[50]	T2, T9	M9
[51]	T2	M9
[52]	T5	M9
[53]	T10	M9

TABLE 8. **The most used techniques for safety and cybersecurity assessment.**

Technique Id	Number of references	References
T2	10	[1], [2], [20], [22], [23], [46], [47], [48], [50], [51]
T14	9	[1], [3], [4], [5], [7], [8], [9], [17], [37], [46]
T10	7	[29], [32], [33], [35], [36], [38], [53]
T1	4	[2], [17], [44], [49]
T13	4	[20], [21], [22], [23]
T9	3	[22], [38], [50]
T8	3	[20], [23], [26]

TABLE 9. **Types of case studies.**

Case study type Id	Case study type
C0	No case study provided.
C1	The provided case study is only theoretical (formulas are provided, but no calculations are performed).
C2	The provided case study is demonstrated using a simulated environment and artificial input values.
C3	The provided case study is demonstrated using a simulated environment, but real input values are used.
C4	The provided case study demonstrates application on a real system with real values used.

- Generalization (i.e. utilization of techniques initially designed for safety assessment to assess cybersecurity with minor modifications of the technique itself) of assessment techniques;
- Availability of case study and its type according to Table 9 below.

The list of possible types of case studies was prepared after a preliminary analysis of primary studies. Types and corresponding identifiers are provided in Table 9.

For safety assessment (RQ3), modifications of well-known reliability assessment techniques like FMEA/FMECA, FTA, and Bayesian networks are mostly used.

As for cybersecurity (RQ4), either specific modifications are utilized (like IMECA), or in most cases cybersecurity assessment is integrated into the overall safety assessment process. In most cases, the assessment process is risk-based, including risk identification, risk analysis, risk evaluation, and documentation.

The main limitations identified (RQ5) include dimension issues (the approach is not applicable due to a huge number of components to be analyzed) and too strict assumptions (like independent failures or attacks). To overcome such limitations, modifications to methodologies used are being introduced, for example, focusing only on elements that are part of the safety function for complex safety systems, etc.

V. KEY FINDINGS

The discussion on key findings focuses primarily on the most interesting results regarding the adopted assessment techniques, namely their combined usage, proposed modifications, and attempts toward generalization. A few other general findings are also highlighted.

A. USE OF SEVERAL ASSESSMENT TECHNIQUES

As shown in Table 7, altogether 28 studies were focusing on several assessment techniques utilization. The main motivation to use several techniques derives from the fact that the results of one technique usually either don't cover all the non-functional aspects of interest (i.e. the technique is focused on safety and doesn't consider cybersecurity issues) or need to be verified through a different technique (i.e. different techniques are used in parallel and then the obtained results are being compared and processed).

Though cybersecurity analysis is implemented in the overall I&C design procedure, it is generally not combined with the safety analysis development. In several analysed studies, the introduced approaches comprehended the significance of integrated safety and cybersecurity analysis and intended to incorporate both into a joint methodological process. For instance, two applicable techniques, which describe the integration of cybersecurity into safety analysis (cybersecurity-informed safety, or security-informed safety), recommend a merging of fault tree analysis (FTA) with attack tree analysis (ATA) or Boolean-driven Markov processes (BDMP). Other introduced approaches either combine safety and cybersecurity methods, e.g., ATA and bowtie analysis, or integrate both fields (i.e. implement strategies devoted to ''unintentional'' (safety) events as well as to ''intentional'' (cybersecurity) chains).

In [42], the scenario-based approach utilizing HARA and TARA techniques is pursued. In particular, correlation of damage scenario and hazard scenario is performed, so as to show the connection of safety with cybersecurity.

The authors of [37] present a framework for performing safety analyses, risk assessment, and safety requirements management using semi-formal and formal techniques like FMEA, FMECA, and FTA. The framework implements a compositional V-cycle methodology, covering all phases of the system development lifecycle. Future integration of other assessment techniques into the framework is planned by the authors.

TABLE 10. The focus of the primary studies.

Ref.	Safety	Cybersecurity	Several assessment techniques	Modification of assessment techniques	Assessment technique generalization	Availability of case study
[1]	√		√	√		C1
[2], [46]	√		√			C0
[3], [8], [9], [33], [48], [49]	√			√		C1
[4],[22]	√			√		C3
[5], [7]	√			√		C2
[6], [38]	√		√			C2
[10]	√		√	√	√	C2
[11], [17]	√	√	√		√	C1
[12], [51]		√	√	√		C1
[13], [14], [26]		√	√	√		C2
[15], [18], [21], [25]		√		√		C2
[16], [36], [53]		√	√			C1
[20]		√	√			C2
[23], [40], [45]		√		√		C1
[27]	√	√		√		C2
[28], [29], [32]	√		√			C1
[31]	√	√	√		√	C2
[34]	√	√	√	√	√	C1
[35]	√	√	√			C1
[37], [47]	√		√	√		C1
[39]	√	√		√	√	C1
[42]	√	√	√			C2
[43]	√	√	√	√	√	C2
[44], [50]	√		√	√		C2
[52]	√	√	√	√		C1

B. MODIFICATION OF ASSESSMENT TECHNIQUES

In 33 studies, listed in Table 10, modifications of assessment techniques are considered. Among the reasons of modification, the following are mentioned: dimension problem of the technique, reduction of resources required to perform the analysis, and application of well-known approaches to different domains.

In [5] FMEA is modified by the introduction of the risk evaluation methodology for controlling multi-uncertainties in the assessment process. It is shown that the proposed methodology can significantly improve the risk assessment results and the risk discrimination of failure modes, but at the current stage controlling only a single uncertainty is implemented.

Authors of [4] propose a novel approach to calculate risk priority numbers based on factors like severity, occurrence, and detection during the application of FMEA, and outline that classical FMEA only considers risk factors regarding safety, ignoring other factors (i.e. cybersecurity or economic impacts).

In [27] initial events for FTA include not only safety-related issues like failures in components or subsystems but also cybersecurity ones like attacks.

It cannot be too highly stressed that several reviewed studies provide evidence that methods originally intended for reliability assessment could be successfully utilized for safety and/or cybersecurity assessment with minor modifications. For example, the probabilistic risk assessment method which is the most general method to get the risk information could be applied to cybersecurity, safety block diagrams, and cybersecurity block diagrams, etc.

Finally, on the aspect of safety and cybersecurity protection mechanisms, it is suggested that they could be based on recent technologies successfully used in other sectors, such as blockchain technology [41], [52].

C. ASSESSMENT TECHNIQUES GENERALIZATION

Generalization of assessment techniques is addressed only in 7 studies but looks as a promising direction for research. The main idea is to develop generic approaches that could be parametrized, so as to be 'tuned' to a required domain or set of metrics. The relatively limited number of studies could be explained by the complexity of such task and the amount of resources needed to provide representative case studies.

In [43], a hybrid ontology is presented that could be utilized for safety and cybersecurity assessment. The authors claim that a true combined approach also needs to include dependability engineering to harmonize the basic concepts between all three disciplines: safety, cybersecurity and dependability. It is also highlighted that focusing on cybersecurity risks requires more effort compared to safety risk analyses due to risk nature: safety risks are based on systematic faults or quite well-known random faults and allow implementation of a systematic assessment approach, while cybersecurity risks are mainly caused by malicious acts which originate a huge number of possible threat scenarios.

The authors of [31] propose an ontological metamodel that considers safety, cybersecurity, and resiliency. Co-engineering of safety and cybersecurity is based on a system losses approach, i.e. system losses caused either by safety or cybersecurity violations are prioritized so as to provide a structured approach for their mitigation. It is claimed that such an approach allows achieving an overall increase in scalability, usability, and unification of already existing models.

In [17] a generic XMECA (FMECA + IMECA = XMECA) technique is presented, intended to cover different domains – safety and cybersecurity – using a unified approach. Verification of XMECA results is performed using EUMECA (E – error, U – uncertainty) with a focus on decisions and judgments made by experts during the XMECA process.

D. METRICS AND CASE STUDIES

Techniques used in a majority of the analysed studies are tailored to risk assessment (risk-based approach), covering only failures, only vulnerabilities, or covering both of them.

Some cybersecurity risk assessment methods with application on real I&C systems are based on national standards. An example is the Chinese national standard GB/T 36466-2018: Information security technology-Implementation guide [58]. According to this document, four risk elements including asset, threat, vulnerability, and protection capability would be first identified and assessed adopting a combination of qualitative methods of expert evaluation and quantitative methods of numerical calculation. Possibility of, and loss from, security incidents then would be calculated through the above four elements and, finally, the risk value is obtained.

Aiming at providing an internationally valid reference methodology, a common international method for combined safety and security modeling, design and assessment is an open and active research topic.

The major part of the case studies presented in the reviewed publications are theoretical ones or taken from realistic contexts but adopting artificial inputs (case studies classified as C1 and C2 in Table 9). Although application to real systems would be highly desirable, this is not expected to be possible in the foreseeable time due to the limitations stated. Indeed, the assumptions adopted to make the technique manageable (e.g., with reference to scalability) are sources of inaccuracy in the obtained results when analyzing realistic systems that do not fully adhere to such assumptions. Devising assessment techniques suitable to deal with real system contexts is an active, challenging research direction.

E. GENERAL FINDINGS

The performed review shows that the focus of recent publications is more on cybersecurity and less on safety as a whole. This could be explained by the modernization of control systems in critical industries, especially towards more flexibility, but a drawback is that new potential cybersecurity issues are introduced.

With the integration of information systems and physical systems, the cybersecurity of information systems and functional safety of physical systems interact with each other, resulting in a type of new comprehensive problem and introducing serious risks. New approaches addressing this issue are needed.

Existing technologies of the I&C system, including programmable logic controllers (PLCs) and FPGA-based platforms, are vulnerable as they are attractive targets for the cyberattack threats. Appropriate risk assessment that includes not only failure analysis and reliability issues but possible intrusions can strongly contribute to enhancing cybersecurity and safety, by providing support to the development of preventive measures in avoiding/mitigating potential cyberattacks.

VI. THREATS TO THE VALIDITY OF THIS STUDY

In this section, we discuss major threats to the validity of this mapping study.

The possibility exists that some relevant studies have not been chosen due to the expertise of the authors. We mitigated this threat, as much as possible, by examining the titles, abstract, and keywords at the first stage and going deeper into

the checks at the second stage, following the steps shown in Figure 1. Moreover, several meetings have been carried out during the selection process, to discuss possible doubts.

Another potential threat relates to the defined search string, since a different set of primary studies may be derived with even slight variation of the search string. This threat characterizes all systematic surveys. To mitigate it, we discussed in depth the goal of the planned study, for which clear and relevant research questions were then identified and used to build the search question.

Regarding the quality of reviewed studies, we did not adopt any specific quality criteria, as usually recommended when performing systematic literature reviews and mapping studies. However, we excluded studies that had not undergone a peer-review process, thus assuring the scientific quality of the selected papers.

Potential issues on generalization of the obtained results constitute another threat that is common to all the mapping studies. While it is not feasible to generalize the drawn conclusions to the whole universe of primary studies on a specific topic, to mitigate this threat we considered only primary studies published during the last 5 years, thus focusing mainly on current trends in the field.

VII. CONCLUSION

This mapping study analysed 49 papers dealing with cybersecurity and safety assessment. Major concluding points include:

- It is observed that out of the 49 included studies, 16 focus on cybersecurity only, 23 focus on safety only, and the remaining 10 are based on a joint approach to safety and cybersecurity. This distribution trend testifies that needs in the different application domains are rather wide in terms of metrics of primary interest.
- It should be particularly emphasized that the majority of techniques used in studies were either based on simulation analysis or theoretical concepts.
- A great majority of the studies (33 out of 49) propose modifications/extensions of classical assessment techniques, either to address joint safety and cybersecurity analysis, or to accommodate new needs of the application context. This trend shows that classical assessment techniques, well consolidated by long-lasting practice, are still very popular and constitute a basis for enhancements to satisfy more sophisticated analysis needs.

The results of the performed survey indicate the lack of a systematic process of unified safety and cybersecurity assessment.

Among future research directions for safety and cybersecurity integration:

- There is a clear need in putting efforts into developing a generic technique (method or standard) supported by tool to combine cybersecurity and safety, which can be helpful for different applications in critical industries, since the significance of integrating both measures was demonstrated in this mapping study, and a generic approach may offer benefits such as feasibility and flexibility.
- It is observed that there are various approaches for evaluating the indicators of interest, including the usage of different assessment techniques and comparison of their outputs for validation purposes. A more extended investigation is necessary to estimate the accuracy and efficiency of assessment mechanisms, in order to find the optimal option to employ in a specific context, guided by criteria of accuracy and cost.

REFERENCES

[1] X. Zhang, Y. Li, Y. Ran, and G. Zhang, "A hybrid multilevel FTA-FMEA method for a flexible manufacturing cell based on meta-action and TOPSIS," *IEEE Access*, vol. 7, pp. 110306–110315, 2019, doi: 10.1109/ACCESS.2019.2934189.

[2] C. Kymal and O. G. Gruska, "Integrating FMEAs, FMEDAs, and fault trees for functional safety," in *Proc. Annu. Rel. Maintainability Symp. (RAMS)*, May 2021, pp. 1–6, doi: 10.1109/RAMS48097.2021.9605786.

[3] P. Liu, Y. Xu, and Y. Li, "An improved failure mode and effect analysis model for automatic transmission risk assessment considering the risk interaction," *IEEE Trans. Rel.*, early access, Oct. 27, 2022, doi: 10.1109/TR.2022.3215110.

[4] S. K. Akula and H. Salehfar, "Risk-based classical failure mode and effect analysis (FMEA) of microgrid cyber-physical energy systems," in *Proc. North Amer. Power Symp. (NAPS)*, College Station, TX, USA, Nov. 2021, pp. 1–6, doi: 10.1109/NAPS52732.2021.9654717.

[5] Y. Liu, B. Chen, Q. Dong, W. Liu, W. Nie, and C. Yang, "Failure mode risk assessment methodology for controlling multi-uncertainties in the evaluation process," *Eng. Appl. Artif. Intell.*, vol. 116, Nov. 2022, Art. no. 105470, doi: 10.1016/j.engappai.2022.105470.

[6] A. R. Patel and P. Liggesmeyer, "Machine learning based dynamic risk assessment for autonomous vehicles," in *Proc. Int. Symp. Comput. Sci. Intell. Controls (ISCSIC)*, Rome, Italy, Nov. 2021, pp. 73–77, doi: 10.1109/ISCSIC54682.2021.00024.

[7] L. Pokoradi, S. Kocak, and E. Toth-Laufer, "Fuzzy hierarchical failure mode and effect analysis," in *Proc. IEEE 19th Int. Symp. Intell. Syst. Informat. (SISY)*, Sep. 2021, pp. 71–76, doi: 10.1109/SISY52375.2021.9582523.

[8] J. Li and M. Chignell, "FMEA-AI: AI fairness impact assessment using failure mode and effects analysis," *AI Ethics*, vol. 2, no. 4, pp. 837–850, Nov. 2022, doi: 10.1007/s43681-022-00145-9.

[9] S. E. Fatollah, R. Dabbagh, and A. S. Jalavat, "An extended approach using failure modes and effects analysis (FMEA) and weighting method for assessment of risk factors in the petrochemical industry," *Environ., Develop. Sustainability*, pp. 1–26, Oct. 2022, doi: 10.1007/s10668-022-02609-8.

[10] J. L. de la Vara, A. S. García, J. Valero, and C. Ayora, "Model-based assurance evidence management for safety–critical systems," *Softw. Syst. Model.*, vol. 21, no. 6, pp. 2329–2365, Dec. 2022, doi: 10.1007/s10270-021-00957-z.

[11] C. Schwarzl, N. Marko, H. Martin, V. E. Jiménez, J. C. Triginer, B. Winkler, and R. Bramberger, "Safety and security co-engineering for highly automated vehicles," *Elektrotechnik Informationstechnik*, vol. 138, no. 7, pp. 469–479, Nov. 2021, doi: 10.1007/s00502-021-00934-w.

[12] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan, "IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process," *EURASIP J. Inf. Secur.*, vol. 2020, no. 1, pp. 1–18, Dec. 2020, doi: 10.1186/s13635-020-00111-0.

[13] H. Guo, L. Ding, and W. Xu, "Cybersecurity risk assessment of industrial control systems based on order—A divergence measures under an interval-valued intuitionistic fuzzy environment," *IEEE Access*, vol. 10, pp. 43751–43765, 2022, doi: 10.1109/ACCESS.2022.3169133.

[14] A. Abakumov and V. Kharchenko, "Combining IMECA analysis and penetration testing to assess the cybersecurity of industrial robotic systems," in *Proc. 12th Int. Conf. Dependable Syst., Services Technol. (DESSERT)*, Athens, Greece, Dec. 2022, pp. 1–7, doi: 10.1109/DESSERT58054.2022.10018823.

[15] Y. Wang, B. Yu, H. Yu, L. Xiao, H. Ji, and Y. Zhao, "Automotive cybersecurity vulnerability assessment using the common vulnerability scoring system and Bayesian network model," *IEEE Syst. J.*, vol. 17, no. 2, pp. 2880–2891, Jun. 2023, doi: 10.1109/JSYST.2022.3230097.

[16] S.-G. Tân, I.-H. Liu, and J.-S. Li, "Threat analysis of cyber security exercise for reservoir testbed based on attack tree," in *Proc. 10th Int. Symp. Comput. Netw. Workshops (CANDARW)*, Himeji, Japan, Nov. 2022, pp. 375–379, doi: 10.1109/CANDARW57323.2022.00023.

[17] I. Babeshko, O. Illiashenko, V. Kharchenko, and K. Leontiev, "Towards trustworthy safety assessment by providing expert and tool-based XMECA techniques," *Mathematics*, vol. 10, no. 13, p. 2297, Jun. 2022, doi: 10.3390/math10132297.

[18] W. Wang, A. Cammi, F. D. Maio, S. Lorenzi, and E. Zio, "A Monte Carlo-based exploration framework for identifying components vulnerable to cyber threats in nuclear power plants," *Rel. Eng. Syst. Saf.*, vol. 175, pp. 24–37, Jul. 2018.

[19] J. Peterson, M. Haney, and R. A. Borrelli, "An overview of methodologies for cybersecurity vulnerability assessments conducted in nuclear power plants," *Nucl. Eng. Des.*, vol. 346, pp. 75–84, May 2019.

[20] J. W. Park and S. J. Lee, "A quantitative assessment framework for cyber-attack scenarios on nuclear power plants using relative difficulty and consequence," *Ann. Nucl. Energy*, vol. 142, Jul. 2020, Art. no. 107432.

[21] C. Lee, H. B. Yim, and P. H. Seong, "Development of a quantitative method for evaluating the efficacy of cyber security controls in NPPs based on intrusion tolerant concept," *Ann. Nucl. Energy*, vol. 112, pp. 646–654, Feb. 2018.

[22] Y. Zhao, L. Huang, C. Smidts, and Q. Zhu, "Finite-horizon semi-Markov game for time-sensitive attack response and probabilistic risk assessment in nuclear power plants," *Rel. Eng. Syst. Saf.*, vol. 201, Sep. 2020, Art. no. 106878.

[23] J. W. Park and S. J. Lee, "Probabilistic safety assessment-based importance analysis of cyber-attacks on nuclear power plants," *Nucl. Eng. Technol.*, vol. 51, no. 1, pp. 138–145, Feb. 2019.

[24] N. Chowdhury, "CS measures for nuclear power plant protection: A systematic literature review," *Signals*, vol. 2, no. 4, pp. 803–819, Nov. 2021, doi: 10.3390/signals2040046.

[25] A. Boudermine, R. Khatoun, and J.-H. Choyer, "Attack graph-based solution for vulnerabilities impact assessment in dynamic environment," in *Proc. 5th Conf. Cloud Internet Things (CIoT)*, Marrakesh, Morocco, Mar. 2022, pp. 24–31, doi: 10.1109/CIoT53061.2022.9766588.

[26] D. Liu, Y. Chen, J. Shi, and D. Chen, "Study on cyber security risk assessment of digital instrumentation & control system of nuclear power plant," in *Proc. Int. Conf. Power Syst. Technol. (POWERCON)*, Guangzhou, China, Nov. 2018, pp. 4742–4750.

[27] R. B. Ferreira, D. M. Baum, E. C. P. Neto, M. R. Martins, J. R. Almeida, P. S. Cugnasca, and J. B. Camargo, "A risk analysis of unmanned aircraft systems (UAS) integration into non-segregate airspace," in *Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS)*, Dallas, TX, USA, Jun. 2018, pp. 42–51, doi: 10.1109/ICUAS.2018.8453455.

[28] B. H. Davatgar, N. Paltrinieri, and R. Bubbico, "Safety barrier management: Risk-based approach for the oil and gas sector," *J. Mar. Sci. Eng.*, vol. 9, no. 7, p. 722, Jun. 2021, doi: 10.3390/jmse9070722.

[29] M. Bucelli, N. Paltrinieri, and G. Landucci, "Integrated risk assessment for oil and gas installations in sensitive areas," *Ocean Eng.*, vol. 150, pp. 377–390, Feb. 2018.

[30] S. Pirbhulal, V. Gkioulos, and S. Katsikas, "Towards integration of security and safety measures for critical infrastructures based on Bayesian networks and graph theory: A systematic literature review," *Signals*, vol. 2, no. 4, pp. 771–802, 2021, doi: 10.3390/signals2040045.

[31] G. Bakirtzis, T. Sherburne, S. Adams, B. M. Horowitz, P. A. Beling, and C. H. Fleming, "An ontological metamodel for cyber-physical system safety, security, and resilience coengineering," *Softw. Syst. Model.*, vol. 21, no. 1, pp. 113–137, Feb. 2022, doi: 10.1007/s10270-021-00892-z.

[32] Y. Zhou, C. Li, C. Zhou, and H. Luo, "Using Bayesian network for safety risk analysis of diaphragm wall deflection based on field data," *Rel. Eng. Syst. Saf.*, vol. 180, pp. 152–167, Dec. 2018.

[33] H. Xu, Y. Zhang, H. Li, M. Skitmore, J. Yang, and F. Yu, "Safety risks in rail stations: An interactive approach," *J. Rail Transp. Planning Manage.*, vol. 11, Oct. 2019, Art. no. 100148.

[34] C. Chen, G. Reniers, and N. Khakzad, "Integrating safety and security resources to protect chemical industrial parks from man-made domino effects: A dynamic graph approach," *Rel. Eng. Syst. Saf.*, vol. 191, Nov. 2019, Art. no. 106470.

[35] N. U. I. Hossain, R. Jaradat, S. Hosseini, M. Marufuzzaman, and R. K. Buchanan, "A framework for modeling and assessing system resilience using a Bayesian network: A case study of an interdependent electrical infrastructure system," *Int. J. Crit. Infrastruct. Protection*, vol. 25, pp. 62–83, Jun. 2019.

[36] R. Arief, N. Khakzad, and W. Pieters, "Mitigating cyberattack related domino effects in process plants via ICS segmentation," *J. Inf. Secur. Appl.*, vol. 51, Apr. 2020, Art. no. 102450.

[37] M. Adedjouma and N. Yakymets, "A framework for model-based dependability analysis of cyber-physical systems," in *Proc. IEEE 19th Int. Symp. High Assurance Syst. Eng. (HASE)*, Hangzhou, China, Jan. 2019, pp. 82–89, doi: 10.1109/HASE.2019.00022.

[38] M. Galagedarage Don and F. Khan, "Process fault prognosis using hidden Markov model–Bayesian networks hybrid model," *Ind. Eng. Chem. Res.*, vol. 58, no. 27, pp. 12041–12053, Jul. 2019.

[39] H. Abdo, M. Kaouk, J.-M. Flaus, and F. Masse, "A safety/security risk analysis approach of industrial control systems: A cyber bowtie—Combining new version of attack tree with bowtie analysis," *Comput. Secur.*, vol. 72, pp. 175–195, Jan. 2018.

[40] A. Asllani, A. Lari, and N. Lari, "Strengthening information technology security through the failure modes and effects analysis approach," *Int. J. Quality Innov.*, vol. 4, no. 1, pp. 1–14, Dec. 2018, doi: 10.1186/s40887-018-0025-1.

[41] R. Gupta, S. Tanwar, N. Kumar, and S. Tyagi, "Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review," *Comput. Electr. Eng.*, vol. 86, Sep. 2020, Art. no. 106717.

[42] M. Khatun, M. Glaß, and R. Jung, "An approach of scenario-based threat analysis and risk assessment over-the-air updates for an autonomous vehicle," in *Proc. 7th Int. Conf. Autom., Robot. Appl. (ICARA)*, Prague, Czech Republic, Feb. 2021, pp. 122–127, doi: 10.1109/ICARA51699.2021.9376542.

[43] J. Alanen, J. Linnosmaa, T. Malm, N. Papakonstantinou, T. Ahonen, E. Heikkilä, and R. Tiusanen, "Hybrid ontology for safety, security, and dependability risk assessments and security threat analysis (STA) method for industrial control systems," *Rel. Eng. Syst. Saf.*, vol. 220, Apr. 2022, Art. no. 108270, doi: 10.1016/j.ress.2021.108270.

[44] K.-L. Lu and Y.-Y. Chen, "Safety-oriented system hardware architecture exploration in compliance with ISO 26262," *Appl. Sci.*, vol. 12, no. 11, p. 5456, May 2022, doi: 10.3390/app12115456.

[45] A. P. H. D. Gusmão, M. M. Silva, T. Poleto, L. C. E. Silva, and A. P. C. S. Costa, "Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory," *Int. J. Inf. Manage.*, vol. 43, pp. 248–260, Dec. 2018.

[46] G. Xie, Y. Li, Y. Han, Y. Xie, G. Zeng, and R. Li, "Recent advances and future trends for automotive functional safety design methodologies," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 5629–5642, Sep. 2020.

[47] M. Ghadhab, S. Junges, J.-P. Katoen, M. Kuntz, and M. Volk, "Safety analysis for vehicle guidance systems with dynamic fault trees," *Rel. Eng. Syst. Saf.*, vol. 186, pp. 37–50, Jun. 2019.

[48] S. Atsushi, "A framework for performing quantitative fault tree analyses for subsystems with periodic repairs," in *Proc. Annu. Rel. Maintainability Symp. (RAMS)*, Orlando, FL, USA, May 2021, pp. 1–6.

[49] J. Famfulik, M. Richtar, R. Rehak, J. Smiraus, P. Dresler, M. Fusek, and J. Mikova, "Application of hardware reliability calculation procedures according to ISO 26262 standard," *Qual. Rel. Eng. Int.*, vol. 36, no. 6, pp. 1822–1836, Oct. 2020.

[50] T. Wang, X. Chen, Z. Cai, J. Mi, and X. Lian, "A mixed model to evaluate random hardware failures of whole-redundancy system in ISO 26262 based on fault tree analysis and Markov chain," *Proc. Inst. Mech. Eng. D, J. Automobile Eng.*, vol. 233, no. 4, pp. 890–904, Mar. 2019.

[51] C.-S. Cho, W.-H. Chung, and S.-Y. Kuo, "Using tree-based approaches to analyze dependability and security on I&C systems in safety-critical systems," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1118–1128, Jun. 2018, doi: 10.1109/JSYST.2016.2635681.

[52] A. Gu, Z. Yin, C. Cui, and Y. Li, "Integrated functional safety and security diagnosis mechanism of CPS based on blockchain," *IEEE Access*, vol. 8, pp. 15241–15255, 2020, doi: 10.1109/ACCESS.2020.2967453.

[53] Y. Tian, J. Li, and X. Huang, "A cybersecurity risk assessment method and its application for instrumentation and control systems in nuclear power plants," *IFAC-PapersOnLine*, vol. 55, no. 9, pp. 238–243, 2022, doi: 10.1016/j.ifacol.2022.07.042.

[54] *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)*, Standard IEC 61508, 2010.

[55] *Risk-Based Inspection Methodology*, Standard API RP 581, 3rd ed., Oct. 2020.
[56] *Fault Tree Analysis (FTA)*, IEC 61025, 2006.
[57] C. E. Budde, C. Kolb, and M. Stoelinga, "Attack trees vs. fault trees: Two sides of the same coin from different currencies," in *Quantitative Evaluation of Systems* (Lecture Notes in Computer Science), vol. 12846. Cham, Switzerland: Springer, 2021, doi: 10.1007/978-3-030-85172-9_24.
[58] *Information Security Technology—Implementation Guide to Risk Assessment of Industrial Control Systems*, Standard GB/T 36466-2018, 2018.
[59] A. Carrera-Rivera, W. Ochoa, F. Larrinaga, and G. Lasa, "How-to conduct a systematic literature review: A quick guide for computer science research," *MethodsX*, vol. 9, Jan. 2022, Art. no. 101895, doi: 10.1016/j.mex.2022.101895.
[60] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Inf. Softw. Technol.*, vol. 64, pp. 1–18, Aug. 2015, doi: 10.1016/j.infsof.2015.03.007.

IEVGEN BABESHKO is currently a Graduate Fellow with the Software Engineering & Dependable Computing Laboratory, Institute of Information Science and Technologies "Alessandro Faedo," and an Associate Professor with the Computer Systems, Networks and Cybersecurity Department, National Aerospace University "Kharkiv Aviation Institute." He is also the Head of the Functional Safety Division, Ukrainian Technical Committee TC185 "Industrial Automation." He covered a contributor roles in several European projects, including TEMPUS/ERASMUS+ (MASTAC, SAFEGUARD, SEREIN, CABRIOLET, CERES, and ALIOT) and Horizon 2020 (ECHO). He is involved as a regular member of Program Committee of IEEE DESSERT Conference. He is the coauthor of more than 50 scientific papers and reports, including ten monographs. His professional and research interests include reliability, safety, cybersecurity assessment, assurance and certification of industrial control systems, the dependability and resilience of IIoT systems, and academia-industry cooperation.

FELICITA DI GIANDOMENICO is currently the Research Director of ISTI-CNR, Pisa, Italy, where she is also leading the Software Engineering and Dependable Computing Research Laboratory. Her research interests include the design of dependable computing systems, software implemented fault/intrusion tolerance, and the modeling and evaluation of dependability attributes, with a focus on critical infrastructures. She covered the role of a principal investigator of CNR and/or the Work-Package Leader in several European projects (including Caution++, CRUTIAL, SAFEDMI, CHESS, and SmartC2Net) and national projects (more recently, TENACE). She has been the Chair of the IEEE Technical Committee on Dependable Computing and Fault Tolerance, from January 2017 to December 2018, and the Chair of the IEEE/IFIP DSN Steering Committee, from January 2017 to December 2018. She is routinely involved in program committee of the most relevant conferences in the dependability area. She was the Program Co-Chair of SRDS 2008, DSN 2009, SAFECOMP 2014, and SERENE 2019. She is a member of the IFIP WG10.4 on Dependable Computing and Fault Tolerance and a member of the Steering Committee of the Conferences IEEE/IFIP DSN and EDCC.

Open Access funding provided by 'Consiglio Nazionale delle Ricerche-CARI-CARE-ITALY' within the CRUI CARE Agreement