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.

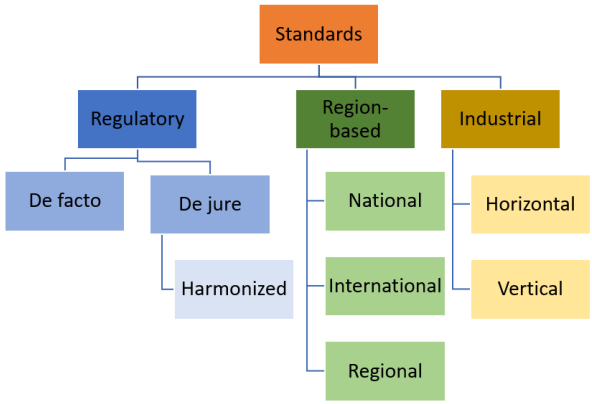

FIGURE 1. Organizing cybersecurity Standards.

- 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

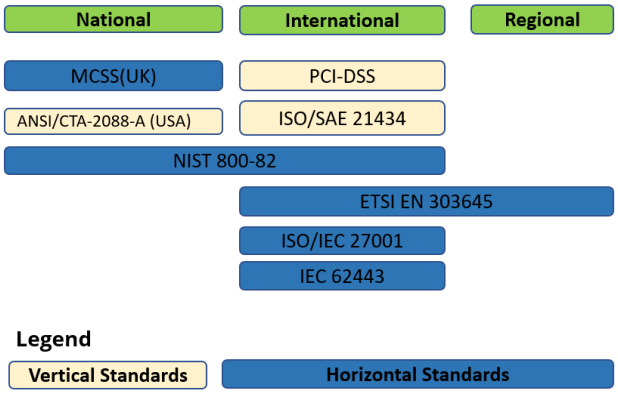

FIGURE 2. Industrial Security Standards: A classification example under region-based criteria.

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

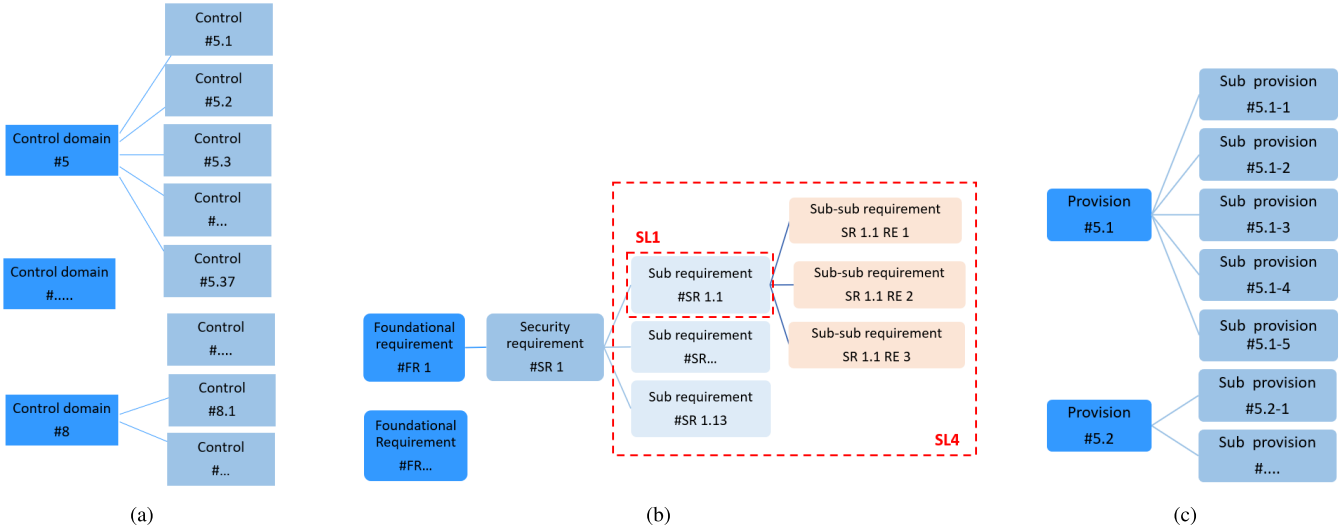

FIGURE 3. Security controls and requirements hierarchy of ISO/IEC 27001:2022 [13] (a) , ISA/IEC 62443-3-3 [28](b) and ETSI EN 301 645 [11](c). The red dashed squares is used to illustrate the security requirements (SRs) in a foundational requirement (FR) that could be included in a SL1 and SL4).

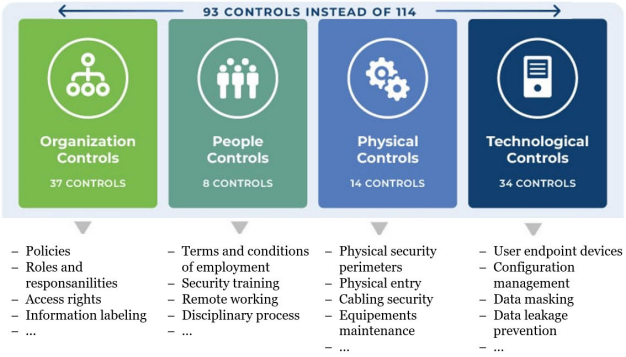

FIGURE 4. Controls areas in ISO 27001:2022.

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

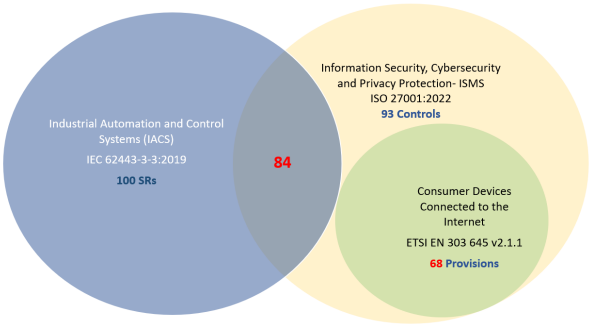

FIGURE 5. Security standards coverage.

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	✓	✓	✓

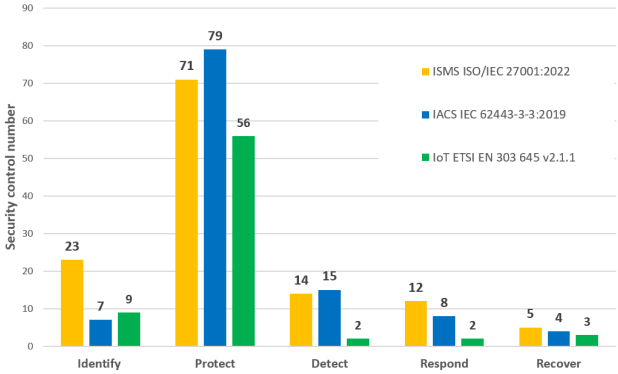

FIGURE 6. Security standards controls coverage.

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.