Usage of Cybersecurity Standards in Operational Technology Systems

Kristian Kannelønning[0000−0002−1480−0709] and Sokratis Katsikas[0000−0003−2966−9683]

Department of Information Security and Communication Technology, NTNU - Norwegian University of Science and Technology, Postboks 191, Gjøvik, 2802, Norway
{kristian.kannelonning,sokratis.katsikas}@ntnu.no
http://www.ntnu.edu.iik

Abstract. The escalating frequency of cyber attacks against industrial installations over the past decade underscores the growing imperative to fortify cybersecurity in organizations. The advent of Industry 4.0 has interconnected factories with the external world, intensifying cybersecurity risks. While international standards are advocated as a source of knowledge to enhance cybersecurity efforts, scant information exists regarding their applicability and usage in Industry 4.0. Diverse cybersecurity standards are available, either specialized for Information Technology (IT) or Operational Technology (OT) or formulated as universal umbrella standards to guide organizations' efforts. In this paper, two data sources are deployed - a Semi-Systematic Literature Review (SSLR) and interviews- to unveil the extent of utilization of cybersecurity standards for OT systems in the Industry and to identify potential barriers to cybersecurity standard usage. The results indicate a low applicability of cybersecurity standards within OT systems. Additionally, the size and lack of practical guidelines in OT cybersecurity standards act as entry barriers, especially for Small and Medium Enterprises (SMEs) with limited resources. The interviews reveal that the organizations mitigate the identified barriers by creating bespoke internal OT standards appropriate for the organization's size and goals.

Keywords: Cybersecurity standards · Industry 4.0 · Operational Technology · IEC62443.

1 Introduction

The network connections between factories and the outside world are increasing. A common term for this highly connected integration is Industry 4.0. The term was first coined in 2011 at the Hannover fair, and [2] defines Industry 4.0 as the connection between production and information- and communication technologies, ICT. The merging of production- and process data with machine data enables machines to communicate with each other. The motivation for this increased adoption of Industry 4.0 with its internet-connected factories and plants is to improve efficiency and effectiveness [10]. A common term in conjunction

with Industry 4.0 is the Cyber-Physical System (CPS). Cyber-physical systems identify anything that integrates computation, networking, and physical processes—binding together the virtual digital world of computers and software and its interaction with the physical analog world. The Industrial Internet of Things (IIoT) is made up of networked CPSs. In these Internet-connected industrial contexts, cybersecurity issues represent one of the most relevant challenges to be dealt with [10]. Another common term that encompasses the terms Industry 4.0 and CPS is Operational Technology (OT). OT includes a broad range of programmable systems and devices that interact with the physical environment. Examples of OT systems are industrial control systems, physical access control systems, and transportation systems. One crucial difference between IT and OT systems is that the latter directly affects the physical world [19].

In the last decade, an increasing number of cyber attacks against industries, including critical infrastructure, highlights the need for organizations, governments, and society to be aware and prepare for unwanted events. Such cyber attacks can potentially inflict severe consequences on organizations and the public. Well-known examples of such attacks are those against the Maroochy County Water System in 2000, the Stuxnet attack in 2010, the power outtake in Ukraine in 2015, the attack on Norsk Hydro in 2019, the attack on the US Colonial pipeline in 2021 and the most recent attack when Russian hackers hit twenty-two Danish power companies. The attack on the Danish power companies began in May 2023 and aimed to gain comprehensive access to Denmark's decentralized power grid. These are a few examples from a much longer list of severe publicly known attacks that grow larger yearly. Threat actors, the perpetrators responsible for these events, range from insiders to criminals and nation-states [17]. In 2022, manufacturing had the highest share of cyber attacks among the leading industries worldwide. During that year, cyber attacks in manufacturing companies accounted for nearly 25 percent of the total cyber attacks.

Given the above, the importance of securing the Industry against cyber attacks is ever-increasing as the number of attacks continues to rise. As cybersecurity risk will persist as a significant challenge for organizations in the coming years, developing and fortifying the organizational cybersecurity posture will be of great importance. Several paths exist toward securing an organization. Organizations can install technical solutions like firewalls, intrusion detection systems, and the like to enhance cybersecurity. However, a holistic perspective addressing technology, processes, and people must be deployed for an organization to be secure and maximize its cybersecurity posture. For an organization to achieve holistic cybersecurity fortification, cross-functional collaboration is required. The effort is not restricted to one person or department; every member must adhere to the organization's prescribed policies.

The knowledge and structure to improve an organization's cybersecurity can be found in international cybersecurity standards. Cybersecurity standards serve as a set of recommendations that specify how organizations should carry out their operations and processes. They are often embraced because they are proven effective in providing well-structured cybersecurity requirements and controls. They

provide a multitude of benefits that justify the time and financial resources required to produce and apply them [4]. Some are dedicated to specialized domains, e.g., IT or OT. Others are developed as general umbrella standards to be used anywhere by everyone, regardless of domain or organizational size. The use of cybersecurity standards should be deployed in their intended domain. A multitude of standards exist, and substantial research has classified differences and overlapping features of the most used standards [4, 8, 9, 20].

International standards are highlighted as a path for improved cybersecurity [4]. However, little is known about the applicability or the usage of cybersecurity standards for OT systems in Industry 4.0 organizations. This paper aims to uncover to what degree such standards are used and what the potential barriers to their utilization are. To this end, two separate data sources are deployed, namely, a literature review by means of a Semi-Systematic Literature Review (SSLR) and semi-structured interviews with senior industry personnel responsible for OT.

The remainder of this paper is organized as follows: Section 2 describes the employed research methods, i.e., the SSLR and the interviews. In Section 3, the results and the findings are presented. These are further discussed in Section 4, while our conclusions and outlines for further research are found in Section 5.

2 Methods

A literature review aims to broaden the understanding of where the current knowledge resides and to support the need and significance for future research in contributing to expanding knowledge [6]. As Fink suggested in [6], descriptive reviews are particularly relevant when randomized controlled trials or rigorous observational studies are scarce or unavailable. The results are descriptive synthesizes based on data abstraction from included articles. The validity of the findings from the literature review depends on the reviewer's expertise and critical imagination in combination with the quality of available literature.

On the other hand, interviews are great for understanding the "how" and "why" of a particular contemporary event [21]. An interview lets the participant explain why they answered the questions the way they did [5]. Although interviews, especially with few interviews conducted, cannot be generalizable to populations or universes, they can be generalizable to theories (analytic generalizations) [21]. Furthermore, utilizing two data sources, namely interviews and the analyzed literature, strengthens the results by data triangulation in developing convergent evidence [21].

2.1 Literature Review

The literature review followed the guidelines of the Preferred Reporting Items for Systematic Reviews and Meta-Analysis, PRISMA, by Page et al. [13] and [6, 15]. Even though the review followed the guidelines from PRISMA and [6, 15], the most appropriate terminology for this review is Semi-Systematic Literature Review, SSLR. An SSLR is most suited when a topic has been researched by

different groups of researchers or within different disciplines; that is, reviewing every article that could be relevant to a topic is simply impossible [16]. The use of specific search words has limited this review, and consequently, the included literature cannot be claimed to be exhaustive for all related research areas.

Firstly, one must investigate if a similar review has already been conducted. No such evidence was found. The benefit of preliminary searches is that they help refine research questions, optimize search strings, and verify that the planned review and the chosen research questions are relevant and valuable to the body of knowledge. A systematic review is, unlike subjective reviews, comprehensible and easily reproducible [6]. Research questions, search strategy, inclusion and exclusion criteria, and the data extraction method are defined before the research commences.

Predefined research questions must be formulated to ensure that relevant knowledge is captured. These must be broad enough to include relevant literature and be precise enough to guide the review [6]. This research aims to better understand how much research has been done within cybersecurity standards in the context of OT systems and to what degree practitioners apply standards. Subsequently, the following research questions have been defined:

- RQ1: What does research report on the applicability of cybersecurity standards for OT systems?
- RQ2: Are there barriers limiting the use of standards, and if so, how can the barriers be reduced?
- RQ3: Are cybersecurity standards perceived as one size fits all? (Small, medium, and large enterprises)

The results in this SSLR stem from searches in the following databases: Scopus, IEEE, Springer, Engineering Village, ScienceDirect, and ACM. Keywords deployed were the same across the databases. However, the search string was modified according to the search database syntax, e.g., (Standard OR Security Standard) AND (Operational Technology OR OT) AND (Cyber security OR Cybersecurity) to capture all relevant publications. The search term OT or Operational Technology was selected instead of the broader terms Industry 4.0 or CPS to limit irrelevant publications to a reasonable amount. Limiting the results with narrower search terms consequently defined the research method as an SSLR instead of an SLR. However, as a precaution and to ensure that the selected terms Operational Technology or OT would yield relevant results, a test was performed on the IEEE and ScienceDirect database, replacing OT with the wider, more encompassing term "Industry 4.0" in the search string. This received a significantly higher number of publications. Searches with OT in the search string received 487 results while replacing OT with Industry 4.0 received 3692 results in the two databases. A review of the first 1636 of the 3692 publications (approximately 44%) did not result in any new relevant publications. Therefore, it is assumed that the searches are exhaustive and all relevant papers have been identified in the context of cybersecurity standards within OT. Searches were restricted to titles, abstracts, and keywords in publications from 2002 until 2023.

After duplicates were removed, the following exclusion and inclusion criteria were applied:

Exclusion criteria:

- Non-peer-reviewed studies from organizational reports, guidelines, and technical opinion reports;
- Research design – exclude reviews, editorials, and testimonials;
- Non-research literature.

Inclusion criteria:

- Written in English;
- Published in (2002-2023);
- Original studies using theoretical or empirical data;
- Studies published in Journals, Conference Proceedings, and books/book sections.

2.2 Interviews

Semi-structured interviews were conducted to unearth a more profound understanding of the application of cybersecurity standards within OT systems. Seven interviews were completed during the spring of 2023. Before conducting the interviews, an interview guide was developed and tested on members from academia and personnel within the Norwegian Industry working with OT systems. The interviews took about one hour and were completed online using Microsoft Teams, with recordings transcribed before analysis.

Four organizations were approached to inquire about participating in the study. To understand how each organization works with cybersecurity, personnel from the OT and IT departments within the same organization were interviewed, except for one organization, where only IT participated. However, this participant was responsible for both OT and IT security. All participants have more than 20 years of experience in their field of expertise and hold cybersecurity responsibilities in their organization within their domain of either OT or IT.

One organization operates in discrete manufacturing, producing finalized end-products; two in process manufacturing, and one in food and beverage. Three organizations are classified as large enterprises with over 1,000 employees, while the smallest currently has around 150 employees.

The interviews and interview guide covered three broad thematic topics; one topic covered the application of standards used in general and cybersecurity standards in particular. The allotted time spent on each topic was dependent upon the responses. The sections tended to be brief for those with little experience or knowledge regarding standards. However, short sessions regarding standards often meant longer sessions on the two other topics, resulting in an approximately equal duration of each interview. The interview guide was pretested, and questions regarding standards started wide and in general terms and eventually turned increasingly narrower into cybersecurity standards. Below is an excerpt of the questions:

- Not restricted to cybersecurity; are standards used, and to what extent in your organization?
- If any, within what domain? (Safety, cybersecurity, or others?)
- What standards are you familiar with?
- To what extent do standards contribute to your organization's cybersecurity program?
- When using cybersecurity standards, how would you describe the material's content?
- In your opinion, what are the pros and cons of using standards? Are there better alternatives?

Analysis of the interviews relies on template analysis. The transcripts are coded by using predefined code. These codes are also referred to as a codebook. The start of the analysis relies on the predefined codes. However, codes do not remain static. Modifications or additional codes are allowed as the analysis progresses. The template is organized concerning different themes defined by the researcher and most commonly involves some hierarchical structure [7]. An often-used approach is to sort text with similar codes into separate categories for final distillation into major themes [3]. A significant advantage of template analysis stems from the highly flexible approach that can be modified to accommodate any study in a particular area. It does not come with many prescriptions and procedures, and the principles behind the technique are easily grasped by those unfamiliar with qualitative methods, partly due to the similarities of content analysis [7].

3 Results

Searches from the selected databases resulted in 1183 records after removing duplicates. The first step in conducting the SSLR is to perform an assessment based on the title and abstract [15]. This first assessment removed 1074 articles, leaving 109 records in the second analysis step. The substantial removal of 91% of the records indicates that the search and used search strings fetched a broad result, and it is therefore expected that all relevant records have been included in the results. The second step includes an assessment of the introduction and conclusion of the records. For this SSLR, the records method section was also investigated at this step. The second step reduced the number from 109 to 13 records eligible for full-text analysis. The results from the different databases are listed with the initial search result and records included in the complete text analysis: ScienceDirect (377/5), IEEE (110/7), Engineering Village (333/0), Scopus (246/1), ACM (117/0). The complete process is graphically depicted in Figure 1.

Of the six articles included in the analysis, three were published in journals and three in conferences, with publication dates ranging from 2017 to 2023.

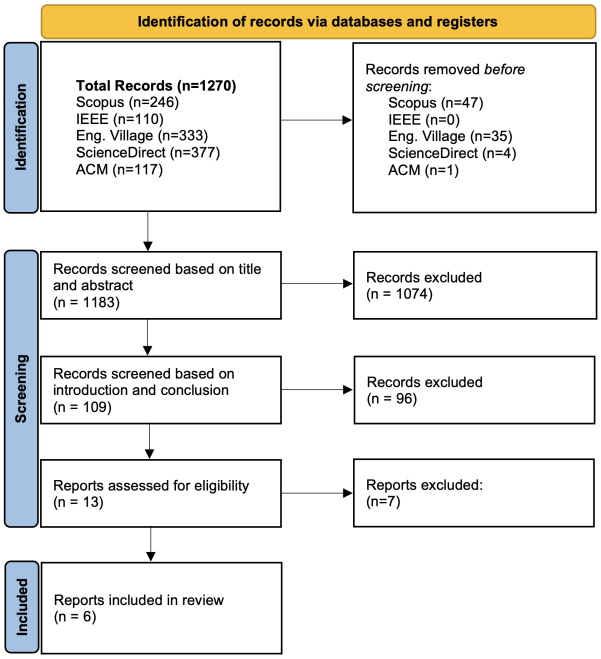

Fig. 1. SSLR Process

3.1 Findings

The results described above lead to the following findings, the presentation of which is structured to follow the research questions defined in Section 2.

What does research report on the applicability of cybersecurity standards for OT systems? Very few articles address the research question regarding the applicability of cybersecurity standards for OT systems. With the word applicability, the goal is to find quantitative results indicating the degree of usage of cybersecurity standards. To what extent do practitioners use standards, and which standards do practitioners use? Several articles, including [20], present exciting quantitative findings, but the results rely on secondary data, e.g., a survey performed by a third party. Such papers are excluded according to the criteria put forth in this review. Only two of the identified articles provide quantitative results that include OT standards.

In [14], Pawar reports on their results from a survey with 115 SME participants from a wide range of industries and geographical locations. Participants also included personnel of organizations within manufacturing. According to [14], 49% of SMEs have no cybersecurity standards or framework in place. The NIST CSF is implemented by 8% of the SMEs. The other standards presented in the results are not OT-specific, and neither is information regarding the partici-

pant's main business activities available. However, since an unknown percentage of participants operate within manufacturing, it is reasonable to include the results. One interesting finding in the paper is worth lingering on. Although the application of standards is found to be low, 56% still report having cybersecurity controls implemented [14]. Organizations implement security measures, but the effort is not motivated by compliance to a standard.

The second article providing quantitative results is [12]. The paper reports on results from a survey of 25 organizations, all operating within the German Industry, particularly in or near North Rhine-Westphalia, with 21 of the 25 organizations categorized as operating within discrete manufacturing. Results suggest that cybersecurity standards and best practices are only somewhat implemented. As much as 80% of the large organizations participating in the survey have implemented cybersecurity measures from the German BSI IT-Grundschutz, a standard comparable to IEC27001. At the same time, only 35% of SMEs do the same. The numbers are reduced when focusing on specific OT cybersecurity standards, e.g., IEC 62443. 65% of large organizations report having an IEC 62443-related project already conducted, while the corresponding number for SMEs is less than 25%. The paper does not clarify what an IEC 62443-related project entails.

These two papers indicate a low applicability for using standards, particularly cybersecurity standards for OT. Similar results have been found in a recent unpublished study by the authors. Organizations within the Norwegian Industry were surveyed through a questionnaire regarding the usage of cybersecurity controls. In the survey, the respondents, n=34, also reported, "To what degree has international cybersecurity standards, IEC 62443 or similar, influenced your organization's cybersecurity program?". Of the n=34 respondents, only 32% (n=11) responded that their organization has either a very important- or important influence from international standards. Similar results are found in the interviews conducted in this study. Although the number of interviews is low, only seven, the theme is consistent with the literature and unpublished survey findings. The usage of security standards from the OT-responsible participants is non-existent. Even familiarity with cybersecurity standards is non-existent. A compilation of their responses could be distilled into this statement: "I am focusing on keeping the factory running. I do not know the international cybersecurity standards, so I put my trust into what vendors or machine builders tell me is sufficient for security". Responses from IT responsible favor using standards, and they express a higher knowledge and familiarity towards both IT and OT standards. However, the reported usage of specific OT standards is still low. In contrast, the applicability of adhering to IT-specific standards is high. Three of the four organizations are ISO 27001 certified and hence are compliant with an international IT standard, while the fourth organization is planning for ISO certification in the future.

Are there barriers limiting the use of standards, and if so, how can the barriers be reduced? Several of the included articles highlight that the

applicability of standards is low, with various reasons for the shortage of usage. Quantitative results are not required to explain why implementation gaps exist and what could potentially bridge the identified gaps.

Both [18, 20] find that the lack of comprehensible implementation guidelines also referred to as practical guidelines, is highlighted as one of the reasons for low implementation. Even though a high-level description exists in all standards and guidelines, Staves found in [17], that only 54% of them provide technical guidance when investigating thirty-one such resources in the context of cybersecurity incidents and response. The identified lack of practical advice could act as a barrier to the implementation of OT cybersecurity controls [17, 18].

The sheer volume and complexity of some cybersecurity standards, particularly IEC 62443, is also an argument for the identified shortage of implementation. In [20], Wagner reports that many resources are needed for an enterprise just to understand which parts in general and which topics in particular of the standard series are relevant for the organization. Staves [17] found through eight interviews that several participants raised concerns regarding the volume and depth of existing standards and guidelines from a usability perspective. This is also confirmed by the interviews conducted in this study. Among respondents familiar or very familiar with the different standards, IEC 62443 was specifically mentioned in this context, and the consensus among respondents is that the content and scope are too extensive. The scope and number of pages make using standards anything but trivial. One respondent highlighted that even after attending seminars to learn about IEC 62443, the material is still too heavy to combine with your day-to-day job, "We are reliant on external consultants to help with this work."

An interesting finding from [17] reveals that OT personnel find available standards and guidelines to be information-focused instead of function-focused, lacking tools and frameworks that adequately cover OT. Participants from IT could see direct similarities between IT and OT and that the separation and need for independent guidance will be counter-productive usage of time and resources. Separation of IT and OT is also presented in [12], who found that about 50% of the organizations applied the same rules for IT and OT regarding incident handling, indicating a desire to standardize the process landscape. The authors of [12] do raise the question, without providing an answer, of whether global rules meet the different requirements of IT and OT devices and processes.

Pawar's and Palivela's article focusing on SMEs states that there exist gaps in the implementation of cybersecurity controls [14]. SMEs cannot relate their cybersecurity efforts or measures against business priorities. Reference [14] proposes a framework called the Least Cybersecurity Control Implementation (LCCI) to bridge this gap. The LCCI will be based on implementing the least cybersecurity controls according to the defense-in-depth concept and the organization's prioritization of the CIA (Confidentialty, Integrity, Availability) triangle for mission-critical assets. The LCCI follows a seven-step process to secure mission-critical assets. It is not transparent which standards are used as the foun-

dation for the development of LCCI, or if the framework is based on standards at all.

Our interviews revealed an interesting path for organizations to bridge the gap of voluminous standards with a lack of practical advice. Development of an organizational bespoke standard. Three of the four organizations in this study have developed these bespoke standards individually. The bespoke standards are developed at the corporate level and distributed throughout the OT department and different locations of the organization. This new bespoke internal standard is based on international standards; however, the organization's employees do not know which standards have been used as the basis. By applying this method, a made-to-order standard is available to the OT responsible that includes practical advice in a smaller format suitable to the organization's size and goals. The organizational standard thereby removes the identified gaps regarding the volume and complexity of interpreting standards, a task given to the organization's few corporate functions.

Are cybersecurity standards perceived as one size fits all? (Small, medium, and large enterprises). Cybersecurity standards must be applicable for practical use in their intended domain. Reference [20] compared IEC62443, NIST SP 800-82, and VDI/VDE 2182 in terms of general aspects, process models, and best practice measures. The process model in VDI/VDE 2182 is found to be the most applicable for both SMEs and large enterprises, with relatively detailed steps, practical application examples, and usability for beginners, which are contributing factors to the decision. However, VDI/VDE lacks the coverage found in the comparison of the other two standards. IEC 62443 is most suitable for large organizations as it covers both technical and organizational best practice measures. It also provides coverage and certification opportunities for integration service providers and product suppliers. The downside is the standard's size, making it less desirable for SMEs constrained by resource limitations.

Lack of resources is also pointed out in [1], where they exemplify some obstacles for SMEs when adopting standards. In preparation for using the NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF) version 1.1, a 55-page document has been developed just to describe the implementation process. Additionally, [1] highlights that NIST CSF, although designed for all organizations, regardless of size, states that the framework is very complicated to comprehend and implement. Therefore, a detailed 55-page guidebook is available for readers to learn the new vocabulary for a better understanding of the standard. This is no easy task for an SME with limited resources. The same is found in the interviews. Although only one of the four organizations is classified as an SME, it is apparent and clearly expressed that without a good financial situation and management's interest in hiring external expertise, complying with a cybersecurity standard is nearly impossible.

As referred to in the subsection on RQ1, an unpublished survey by the authors, with responses from organizations within the Norwegian Industry, indicates a low usage of international security standards, with only 32% of orga-

nizations having a significant influence from standards in their cybersecurity programs. Of the organizations reported to follow a security standard, all are defined as large organizations with over 250 employees. This result aligns with [20], who found that IEC 62443 is most suited for large organizations. Both the organization's size and the OT department's size are found in the survey to influence an organization's inclination to follow such security standards.

4 Discussion

The results pertaining to RQ1 in the literature review section of this study include very few studies providing quantifiable answers to the degree of application of cybersecurity standards for OT systems. Only [12] is dedicated to OT systems, whereas [14] have included manufacturing organizations as participants and are therefore included. The results indicate low applicability or usage of standards within OT, which corroborates the findings from the interviews in this study. Similar results are found in the aforementioned unpublished survey, where only 32% of the respondents report that cybersecurity standards have significantly influenced their organization's cybersecurity program. With such few references, interviews, and a relative few, n=34, responses for the survey that are limited to a geographical location, a conclusive answer to the widespread usage of standards within OT systems cannot be given. However, there is reason to suspect that the applicability of cybersecurity standards is low. Does a low applicability of standards constitute a low or poor cybersecurity posture for OT? Are organizations inherently vulnerable due to the lack of prescription for dedicated OT cybersecurity standards? Answers to such questions are outside the scope of this study. However, this study can provide some answers and indicative reasons as to why the usage is low, if low applicability eventually would be concluded.

IT standards like the ISO 27000 series or equivalent are present in several of the included articles and in the interviews, where three of the four organizations are ISO 27001 certified. Reference [12] states that 80% of large enterprises adhere to the German BSI IT-Grundschutz, a German standard comparable with ISO 27001, and over 50% of German organizations are ISO 27001 certified according to [11]. When an organization follows or, even better, is certified as ISO 27001 compliant, a set of measures is in place. Governance documents, restricting employees' online behavior, IT security training, incident handling, and recovery procedures to mention a few. These IT-driven processes and procedures will also include parts of the OT section of an organization. i.e., personnel working within OT will have policies regarding their online behavior. So effectively, organizations could have a standard-driven cybersecurity posture even though dedicated OT standards enjoy low implementation.

Reference [11] finds that the key obstacle for organizations to be ISO 27001 certified is time and high cost. Is it then reasonable for organizations to implement two cybersecurity standards that are partly overlapping or have similarities when viewed from an IT perspective [17]? With time and high cost highlighted as key obstacles, would not deciphering and interpreting a voluminous standard

like IEC 62443, with its 800 pages and lack of practical guidance [17, 18], drain an organization for resources that have already been highlighted as key obstacles? The decision of whether to comply with one or two cybersecurity standards leads the discussion to the organization of and responsibility for OT cybersecurity.

OT operations are inherently different from IT. It is an area requiring specialized knowledge and experience. Even with the introduction of Industry 4.0 and the integration of IT with OT, there still are vital differences between the two, such as patch management, prioritization towards the CIA triangle, and safety aspects concerning CPS, to mention a few. The technical differences between IT and OT are well documented in research. Running a OT system, requires OT personnel. The interviews revieled an interesting difference between IT and OT personnel regarding familiarity with standards in general and cybersecurity in particular. Employees with IT backgrounds had a much broader understanding of governance and the need for implementing procedures in the organization. In contrast, the focus of OT personnel was explicitly stated to keep the system running and avoid downtime. Several avenues could give answers to this difference. One avenue apparent in the interviews is differences in education. IT personnel with education within IT will typically follow a curriculum that includes at least a basic understanding of governance and policies. In contrast, personnel within OT do not have this knowledge as a baseline from their education. No further investigation has been done to determine if the difference, or to what degree, education contributes to the lower implementation of cybersecurity standards in OT systems. Still, the two groups have distinct differences in this regard. What is apparent is that OT representatives must, due to the distinct differences between IT and OT, be part of implementing and managing cybersecurity efforts designated for OT. Given the differences in priorities and unfamiliarity with standards for OT personnel interviewed, this is not a simple task.

5 Conclusion

Of the substantial number of 1183 records found through searches in the databases, only 13 were found to be eligible for complete text analysis, and of those, only five provided answers to the defined research questions. The limited number of records included in this review can indicate a shortage in research on the defined research questions. Several publications without peer reviews and the rigor deployed in scientific papers, e.g., whitepapers or industry reports, provide interesting insights. Still, such reports are not material for developing empirical truths like scientific papers. This could indicate that the cybersecurity field for OT is pushed forward by industry players rather than research.

However, what is valid for both the number of articles and the degree of applicability towards RQ1 - both are low. Definitive conclusions regarding the usage of standards cannot be based on only two papers, but it is at least an indication of the degree of applicability. Findings in the literature are substantiated by findings from the seven interviews and the survey, with n=34, done in the Norwegian Industry. What is more apparent is that several gaps have been

identified and exist. The size and lack of practical guidelines in OT cybersecurity standards appear as entry barriers to application. This is even more true for SMEs with limited resources, highlighted by the fact that exclusively large organizations in the unpublished survey follow a security standard.

As these gaps become apparent, few ways to bridge them have been identified in the literature. However, the interviews uncovered an interesting finding: Organizations create bespoke standards. These organizational bespoke standards are developed and compiled at the corporate level. The work is done without local OT personnel's involvement, and the resulting standard is designed to remove the barriers identified in the literature for practitioners. These bespoke standards provide OT with easy, hazel-free access to an organizational standard based on international standards containing practical advice with a scope that fits the organization.

Following the finding in [17] that from an IT perspective, standards have similarities, applying two, one for IT and one for OT, will be a waste of resources. As found in the interviews and the literature reviewed, many organizations comply with IT standards. If an organization believes that the effort to implement two standards is time not well spent, future research investigating the amount or degree of usage of OT cybersecurity standards will not provide evidence towards questions like "how much cybersecurity effort is put forth by an organization or an industry". Future research should, therefore, investigate what cybersecurity controls organizations implement to improve their cybersecurity posture. As found in [14], organizations have cybersecurity measures in place, even though they do not adhere to a cybersecurity standard. Such research will have significant implications for both researchers and practitioners.

References

1. Benz, M. & Chatterjee, D. Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons* 63(4), 531-540 (2020), https://www.sciencedirect.com/science/article/pii/S0007681320300392
2. Corallo, A., Lazoi, M. & Lezzi, M. Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers In Industry.* **114** pp. 103165 (2020), https://www.sciencedirect.com/science/article/pii/S0166361519304427
3. Dicicco-Bloom, B. & Crabtree, B. The qualitative research interview. *Medical Education.* **40**, 314-321 (2006)
4. Djebbar, F. & Nordström, K. A Comparative Analysis of Industrial Cybersecurity Standards. *IEEE Access.* pp. 85315-85332 (2023)
5. Edgar, T. & Manz, D. Introduction to Science. *Research Methods For Cyber Security.* pp. 3-31 (2017)
6. Fink, A. Conducting research literature reviews. (SAGE Publications,2019)
7. King, N. Using Templates in the Thematic Analysis of Text. *Essential guide to qualitative methods in organizational research.*, pp.256-270 (SAGE Publications, 2004)
8. Leszczyna, R. A review of standards with cybersecurity requirements for smart grid. *Computers & Security.* **77** pp. 262-276 (2018), https://www.sciencedirect.com/science/article/pii/S0167404818302803

9. Leszczyna, R. Cybersecurity and privacy in standards for smart grids – A comprehensive survey. *Computer Standandard and Interfaces.* **56** pp. 62-73 (2018)
10. Lezzi, M., Lazoi, M. & Corallo, A. Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers In Industry.* **103** pp. 97-110 (2018), https://www.sciencedirect.com/science/article/pii/S0166361518303658
11. Mirtsch, M., Blind, K., Koch, C. & Dudek, G. Information security management in ICT and non-ICT sector companies: A preventive innovation perspective. *Computers & Security.* **109** pp. 102383 (2021), https://www.sciencedirect.com/science/article/pii/S0167404821002078
12. Nüßer, W., Koch, E., Trsek, H., Schumann, R. & Mahrenholz, D. Cyber security in production networks — An empirical study about the current status. *2017 22nd IEEE International Conference On Emerging Technologies And Factory Automation (ETFA).* pp. 1-4 (2017)
13. Page, M., McKenzie, J., Bossuyt, P., Boutron, I., Hoffmann, T., Mulrow, C., Shamseer, L., Tetzlaff, J., Akl, E., Brennan, S., Chou, R., Glanville, J., Grimshaw, J., Hróbjartsson, A., Lalu, M., Li, T., Loder, E., Mayo-Wilson, E., McDonald, S., McGuinness, L., Stewart, L., Thomas, J., Tricco, A., Welch, V., Whiting, P. & Moher, D. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ.* Vol 372 pp. n71 (2021)
14. Pawar, S. & Palivela, D. LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal Of Information Management Data Insights.* **2**(1), 100080 (2022)
15. Silva, R. & Neiva, F. Systematic literature review in computer science - A practical guide. *Relatórios Técnicos Do DCC/UFJF* **1**(8) (2016)
16. Snyder, H. Literature review as a research methodology: An overview and guidelines. *Journal of Business Research.* **104**. pp. 333-339. doi: 10.1016/j.jbusres.2019.07.039 (2019).
17. Staves, A., Anderson, T., Balderstone, H., Green, B., Gouglidis, A. & Hutchison, D. A Cyber Incident Response and Recovery Framework to Support Operators of Industrial Control Systems. *International Journal Of Critical Infrastructure Protection.* **37** pp. 100505 (2022), https://www.sciencedirect.com/science/article/pii/S187454822100086X
18. Staves, A., Maesschalck, S., Derbyshire, R., Green, B. & Hutchison, D. Learning to Walk: Towards Assessing the Maturity of OT Security Control Standards and Guidelines. *2023 IFIP Networking Conference (IFIP Networking).* pp. 1-6 (2023)
19. Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., (MITRE), MT: NIST Guide to Operational Technology (OT) security. Tech. Rep. NIST SP 800-82r3, National Institute of Standards and Technology, Gaithersburg, MD (2023). DOI https://doi.org/10.6028/NIST.SP.800- 82r3. URL https://csrc.nist.gov/pubs/sp/800/82/r3/final
20. Wagner, P., Hansch, G., Konrad, C., John, K., Bauer, J. & Franke, J. Applicability of Security Standards for Operational Technology by SMEs and Large Enterprises. *2020 25th IEEE International Conference On Emerging Technologies And Factory Automation (ETFA).* **1** pp. 1544-1551 (2020)
21. Yin, R. Case Study Research and applications: Design and methods. (SAGE Publications,2017)