# Learning to Walk: Towards Assessing the Maturity of OT Security Control Standards and Guidelines

Alexander Staves
*Lancaster University*
Lancaster, UK
a.staves@lancaster.ac.uk

Sam Maesschalck
*Lancaster University*
Lancaster, UK
s.maesschalck@lancaster.ac.uk

Richard Derbyshire
*Orange Cyberdefense*
London, UK
ric.derbyshire@orangecyberdefense.com

Benjamin Green
*Lancaster University*
Lancaster, UK
b.green2@lancaster.ac.uk

David Hutchison
*Lancaster University*
Lancaster, UK
d.hutchison@lancaster.ac.uk

***Abstract*—The convergence of IT and OT has presented OT environments with several challenges, such as increasing the attack surface of its real time systems to include more commonplace enterprise vulnerabilities. As OT is used across heavily regulated sectors, including water and nuclear, many standards and guidelines are available to these sectors, providing them with assistance towards continued improvements from a cyber security perspective. However, these standards and guidelines are not always as mature as their IT counterparts. This paper proposes a model to benchmark the maturity of OT focused standards and guidelines, which we then use to analyse seven commonly adopted resources. Based on this analysis, we find that these OT standards and guidelines do not always provide in-depth implementation guidance, and often refer instead to IT standards and guidelines for more information. Improvements are urgently needed in security and risk mitigation for interconnected OT and IT systems, as security controls in OT are typically re-appropriated IT controls. To help achieve this goal, OT standards must mature further.**

***Index Terms*—Standards & Guidelines, Operational Technology, Industrial Control Systems, Security Controls**

## I. Introduction

Over the past decade, the integration of Information Technology (IT) within Operational Technology (OT) environments has led to a noticeable increase in process optimisation and efficiency within industrial environments, including sectors that form part of a country's Critical National Infrastructure (CNI) [1]. While, historically, IT and OT were segregated as described by the Purdue Model [2], an increasing volume of standardised technology (including IT software and hardware) is being integrated into OT systems that operate within the Manufacturing and Cell/Area Zones. Despite the benefits that this technological integration provides, it has also led to an increased attack surface for threat actors to target [3], [4], resulting in several notable cyber attacks specifically aimed at industrial environments, including CNI facilities [5], [6].

In response, standards bodies and government organisations have provided support in the form of standards and guidelines, designed for use by asset owners to assess and improve the cyber security of their environments [7], [8]. Of particular note is guidance provided for the implementation of relevant security controls. These are defined by the National Institute of Standards and Technology (NIST) as "safeguards or countermeasures prescribed for an organization designed to meet a set of defined security requirements" [9]. The implementation of these controls within OT environments has recently seen a shift [10], with 37.7% of organisations in 2022 stating that OT asset owners or operators and engineering managers are responsible for this task; this is a significant increase from the previous year, when this responsibility was more likely to be assigned to IT managers. This survey also highlights the misconception that IT security practices, including security controls, can be directly applied to OT environments, which may not always be the case. However, the 2021 SANS survey [11] also claimed that despite significant progress in recent years, industrial organisations are yet to fully adapt to the changes brought by the integration of IT and OT, especially concerning the implementation of security controls informed by standards and guidelines.

Mature standards provide comprehensive security controls, clear guidance, consistency, continuous improvement, enhanced credibility, and regulatory compliance, ultimately offering a robust framework for effectively safeguarding systems and data against various threats. While IT-based standards such as ISO/IEC 27001 are widely adopted in practice due to their maturity, the plethora of standards and guidelines that have recently been published for OT, including sector-specific guidance, makes it difficult for OT asset owners to know which route to take when it comes to the selection and implementation of security controls. Therefore, this paper proposes a model towards the maturity evaluation of OT-focused security control-related standards and guidelines. In turn, OT asset owners can use this model's process to aid them in the selection of standards and guidelines most suited to their needs.

The core contributions of this paper are:

This work is funded, in part, through the NG-CDI Prosperity Partnership funded by UK's EPSRC and British Telecom plc (EP/R004935/1).

**ISBN 978-3-903176-57-7** 

- The proposal of a model based on existing IT standards, towards the maturity evaluation of security control-related guidance provided by OT-specific standards and guidelines.
- An example usage of the proposed methodology on seven commonly adopted OT standards.

The remainder of this paper is structured as follows. Section II describes related work. Section III describes a method for developing the proposed maturity evaluation model. Section IV presents example usage of the proposed model through its application to seven OT standards and guidelines. Section V concludes the paper and explores areas for future work.

## II. Related Work

Several recent works have discussed the maturity of OT standards and guidelines. For example, Francia et al. [12] provide a survey on security best practices and risk assessment for OT, and develop a new framework (CORAS). Using the CORAS framework, the authors propose a model-based risk assessment methodology enabled by these standards and guidelines. However, it is noted that although some OT-specific standards are closely aligned to IT-specific standards, there are discrepancies between them. For example, while the security controls detailed in NIST SP 800-53 [13] closely align with those in NERC CIP [14], the "business risk reduction" needs to be met differently due to NIST SP 800-53 solely focusing on information security controls.

Gentile et al. [15] provide a survey of standards and best practices for patch management within particle accelerators. In this work, the authors conclude that while the reviewed standards share some principles, certain concepts present challenges when merging these into a single reference standard, highlighting differences in maturity between these. As a result, a workflow for patch management is proposed.

Kulik et al. [16] propose an approach for formally verifying compliance with OT security standards. In this work, the authors note that standards are commonly validated only through model checking, and they demonstrate that formal verification can be used to implement security control from these standards.

Wagner et al. [17] discuss the applicability of OT standards within Small and Medium-sized Enterprises (SMEs) compared to large enterprises. Results from this conclude that SMEs have a higher barrier to entry when adopting OT standards. In particular, IEC 62443 [18] is considered too complex for SMEs to implement effectively. However, while VDI/VDE 2182 [19] is better suited for smaller enterprises, it only addresses risk management.

Knowles et al. [20] provide a survey on cyber security management for industrial control systems. In this work, the authors note that despite being extensively used in OT environments, IT standards and guidelines present several limitations as they are tailored towards information security, and consequently cannot be applied comprehensively within OT environments. Additionally, many existing OT standards provide guidance at a high level, and therefore further technical guidance is also required. These publications are also highly inconsistent in the quality of the guidance provided, including a typical lack of quantifiable metrics.

Previous work also highlighted the inconsistencies of OT-focused standards and guidelines when assessing and improving cyber incident response and recovery [21]. While some standards were found to have sufficient maturity regarding their use in practice, the inconsistencies that were identified could result in a less than complete picture when selecting specific standards over others.

While existing work discusses the limitations concerning OT standards and guidelines, the primary focus is on specific controls or topics within these standards, such as patch management, risk management, or response and recovery. An emphasis is also made on comparing OT standards with each other rather than assessing their maturity. The following section, therefore, proposes a methodology for assessing the maturity of security control focused standards and guidelines.

## III. Model Proposal

### A. Method

Security controls are discussed here across a variety of literature, including industry-led standards and guidelines, training materials, and academic works. Controls are implemented to provide safeguards or countermeasures against the realisation of security risks to assets, where assets are defined as any organisational resource (data, systems, humans, etc.) [22]. To help us develop the proposed model for benchmarking security controls within OT standards and guidelines, ISO/IEC 27001 [23], ISO/IEC 27002 [24], and NIST SP 800-53 [13] have been selected for review due to their prevalence within the IT space, providing a view of what "good" looks like.

ISO/IEC 27001, which also references its sister standards 27000 and 27002, has been selected due to its common use across a range of organisations, both in terms of size and service offering; the latter may include additional legal and regulatory factors. ISO/IEC 27001 is said to be designed in such a way as to allow flexibility, and therefore it is adopted globally and has been considered the "common language" for information security for over a decade [25], [26]. NIST 800-53 has also been selected because it targets United States Federal information systems and organisations. Kurii et al. explain how the use of NIST SP 800-53 within the US Federal government has made it one of the most commonly adopted standards to this day [27].

In order to provide clear contextualisation for the discussion around security controls, an understanding of how an organisation selects and implements security controls is required. The following section discusses an organisation's information security policy, including definitions and examples from the selected industry standards, and a brief discussion on how organisations outline key security policy requirements, i.e., the factors via which they are derived. In doing so, precise requirements can be defined for the development of a benchmark model.

### B. Model Requirements

*1) Security Policy:* An organisation's security requirements are typically shaped around broad strategy/objectives, regula-

tory requirements, threat information, legislation, etc. Embodied within the information security policy, they are designed to provide a baseline set of requirements on which further, more detailed decisions, can be made around the practical selection and implementation of security controls. Taking ISO/IEC 27002 as an initial reference point [24], this standard discusses the requirements for an organisation's information security policy. The objective of an information security policy is "To provide management direction and support for information security following business requirements and relevant laws and regulations". This initial objective is expanded to include a more comprehensive set of requirements, such as organisational strategy, regulations, legislation, etc. ISO/IEC 27001 [23] provides complementary guidance to that of ISO/IEC 27002, covering the "requirements for information security objectives and planning to achieve them".

Overall, the core organisational strategy/objectives and other important factors, such as regulatory requirements and legislation, should be considered in creating an organisation's information security policy. From this security policy, specific information security objectives can be defined. Once a set of objectives has been defined, the process of security control selection and implementation can begin. To better understand what the term "security control" means, the following section includes definitions and examples from the aforementioned sources.

*2) Security Control Definition:* To create a baseline definition of security controls, the selected documents will provide a comprehensive view of how security controls are defined and discussed. This will lead to a more detailed discussion on categorisation and guidance and, ultimately, the development of a benchmarking model.

ISO/IEC 27001 [23] references its sister document ISO/IEC 27000 for a baseline definition of a control as a "Measure that is modifying risk. Controls include any process, policy, device, practice, or other activities which modify risk. Controls may not always exert the intended or assumed modifying effect" [28]. From this baseline definition, ISO/IEC 27001 includes details on security controls to cover a number of organisational assets, from media handling to access control. The controls are broken down into overarching categories, subcategories, one or more sub-subcategories, and a security control presented as a descriptive requirement. From the security requirement, reference is then made to ISO/IEC 27002, where a more detailed control implementation guide is available [24].

An initial definition of a security control is provided by NIST SP 800-53 as "A safeguard or countermeasure prescribed for an information system or an organisation designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements." This initial definition takes a similar approach to that of ISO/IEC 27001 [23]. A broad outline of overarching categories is defined, with one or more sub-subcategories presented as tables. Additional information around priority baselines (i.e., is the control prioritised as Low, Moderate, or High) is also provided.

*3) Security Control Objectives:* The selection and implementation of security controls must be based on clearly defined goals; this allows for a review of their success post-implementation. When considering a security control's selection and implementation parameters, the term "control objectives" may be applied to outline the required outcome of the applied control(s).

ISO/IEC 27001 [23] references its sister document ISO/IEC 27000 [28] for its baseline definition of an objective as a "statement describing what is to be achieved as a result of implementing controls". ISO/IEC 27001 then provides control objectives for each of its subcategories of controls. NIST SP 800-53 [13] does not explicitly apply, and therefore the term control objectives is defined within the standard. However, reviewing the supplementary information that is provided, a similar approach to ISO/IEC 27001 [23] is applied.

Although the examples discussed here do not necessarily apply the term "control objective", each describes what the control category or subcategory expects to achieve through implementation. These descriptions fall in line with how one could interpret "control objective" and, therefore, how it could be defined as such. When reviewing the applied categorisations, ISO/IEC 27001 [23] and NIST 800-53 [13] are similar in their approach.

*4) Security Control Requirements:* When turning to industry standards and guidelines, one must identify appropriate controls to meet set objectives derived from the organisation's information security policy. As discussed in Section III-B3, this has been achieved in slightly different ways. However, once a relevant control category has been selected, how is the control requirement defined, and is this sufficient for further development towards practical selection and implementation?

For example, in ISO/IEC 27001 [23], control "I.D A.9.4.3" is defined as "Password management systems shall be interactive and shall ensure a quality password". While this requirement is clearly defined, the term "quality password" is open to broad interpretation. For further clarification on the practical implementation of this control and to reduce some level of ambiguity and individual interpretation, one must turn to ISO/IEC 27002 [28] and its parallel implementation guidance. This parallel guidance presents nine key requirements of A.9.4.3 and an additional paragraph on other information.

To provide another example, NIST SP 800-53's [13] control "IA-2(1)" is defined as "The information system implements multi-factor authentication for network access to privileged accounts". As with ISO/IEC 27001 [23], the described requirement is open to interpretation. However, unlike ISO/IEC 27001, no implementation guidance is directly available for this control. Instead, a high level of detail is provided around the parent category (IA-2) and an additional related control category (AC-6). Upon inspection of the related control category, a detailed description of the category is provided, with several sub-categories providing more granular levels of detail.

Through these examples, it is clear that the level of detail provided within the control requirements is ample for further

exploration into practical control implementation. However, adding implementation guidance and related controls helps reduce any ambiguity and focuses attention towards more suitable practical implementation. Where lower-level categorisation is absent, more detailed requirements are essential due to the broader scoping nature of the control category.

*5) Security Control Classification:* Security controls and their associated objects (discussed in Section III-B6) broadly fall into one of two categories: Social or Technical. Technical control relates to the use of technology to control system or human actions. An example could be to control data flows through a network using access control lists or network segregation. In comparison, Social control relates to any control impacting human interaction. An example could be restricting access to data outside of an individual's role through user access policies.

*6) Security Objects:* A term not often used to describe elements of cyber security is "Security Object". NIST [29], for example, describes a computer security object as "Information objects that convey information used to maintain the security of resources in a computerised environment". This definition is close to that of the one adopted within the proposed model, in that security objects convey information used to maintain the security of resources. However, for further clarity and additional scope, the applied definition is described as "Any device, document, or agreement harbouring a set of security controls used to maintain the security of an organisational asset, be it computerised or otherwise".

While the selected standards do not provide explicit examples of security objects, an example can be taken from ISO/IEC 27001 [23]. The implementation description concerning control "A.12.3.1" states: "Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy". From this description, it is possible to hypothetically specify two security objects: the software applied to backup copies of information, software, and system images, and the documentation outlining the backup policy. Essentially, the security controls residing within these two objects are the backup software and supporting document's content. These have been embodied within the two security objects (backup software and documentation).

### C. The Model

Using the method discussed in Section III-A and the requirements defined in Section III-B, the proposed model, depicted in Figure 1, displays the flow of information from broad organisation strategy down to local level security control implementation. Seven processes constitute the proposed model, using existing approaches derived from the selected standards and guidelines. This provides a benchmark by which evaluation of discussion on security controls can be performed. The processes within the model are as follows:

- Broad organisation strategy, including legislation, regulatory requirements, etc. is considered in the development of an organisation's security policies.
- Security objectives are derived from the security policy.
- Relevant control categories are selected based on pre-outline security objectives.
- Control sub-categories are selected from control categories based on clearly defined sub-category objectives.
- Individual controls are selected, with their requirements clearly defined. Furthermore, where applicable, recommendations towards related control categories are provided for additional guidance.
- Control-specific implementation guidance is provided, to aid in the identification of key feature requirements, applied during practical implementation of the control.
- Practical implementation of the selected control is applied within a security object.

| ID | Criteria |
|---|---|
| A | Is an information security policy discussed? |
| B | Are a range of information policy requirements defined? (e.g., contractual, legislative, regulatory…) |
| C | Are security objectives discussed? |
| D | Are controls split into categories? |
| E | Are controls split into sub-categories? |
| F | Are individual control categories provided? |
| G | Are individual control category requirements outlined? |
| H | Are individual social controls provided? |
| I | Are individual technical controls provided? |
| J | Is implementation guidance provided for each individual control? |
| K | Are resources that are external to the series provided? |
| L | Are resources that are internal to the series provided? |

TABLE I
SECURITY CONTROL BENCHMARK CRITERIA SET

Using this model, criteria (Table I) can be defined to evaluate the maturity of other standards, specifically those tailored towards OT environments.

## IV. ANALYSIS

To provide an example implementation of the benchmark model proposed in Section III, seven OT standards and guidelines were selected for analysis. These are: the NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF) [8]; IEC 62443 [18]; and NIST SP 800-82 [30], reported as the most commonly adopted OT-specific standards by SANS in 2021 [11]. Additionally, ISO/IEC 27019 [31], ONR SyAPs [32], and NERC CIP [14] were selected to assess sector-specific standards and guidelines. Finally, the NCSC CAF [7] was selected to assess government-provided guidelines for security controls.

In Table II and across the following subsections, we have provided an evaluation of the selected standards and guidelines using the criteria set derived from the benchmark model. We define external resources as other standards or guidance that are not part of the same family or series. For example, ISO/IEC 27019 and ISO/IEC 27002 are in the same family and are, therefore, considered internal to each other. However, while the NIST CSF references NIST SP 800-53, it is not part of the same series and is therefore considered external.

*1) NIST CSF:* The NIST CSF provides a comprehensive overview of requirements, categories, and controls required to effectively implement security measures for critical infrastructure. It covers many aspects, including technical and social

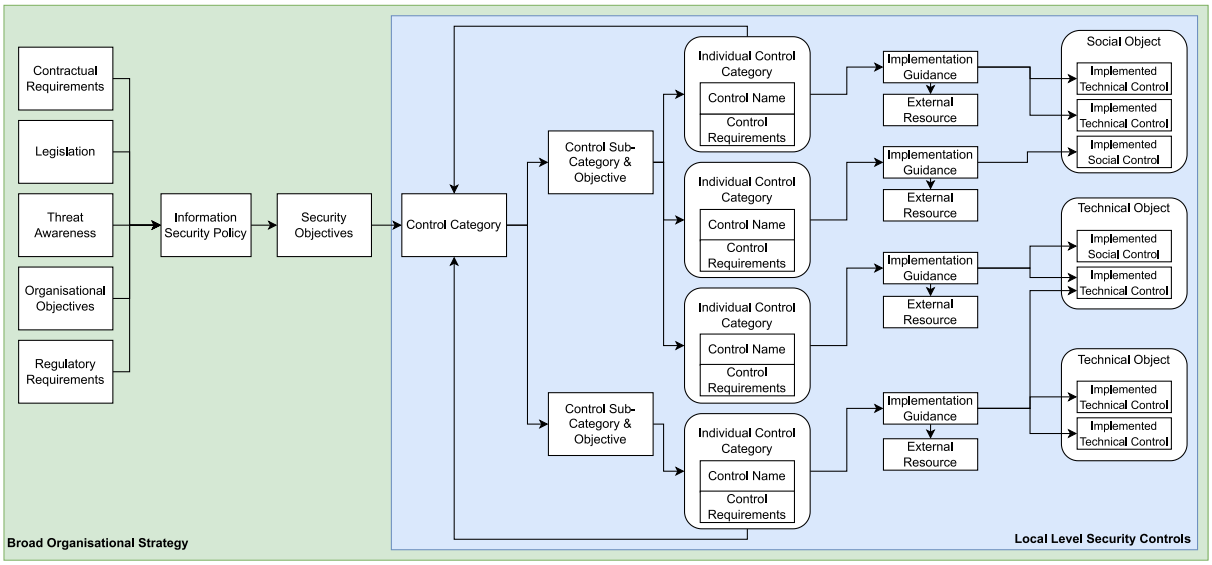


Fig. 1. Security Control Benchmark Model

| | A | B | C | D | E | F | G | H | I | J | K | L |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| NIST CSF | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | |
| IEC 62443 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | (✓) | |
| NIST SP 800-82 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | (✓) | | ✓ |
| ISO/IEC 27019 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | (✓) | (✓) | ✓ |
| NCSC CAF | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | (✓) | ✓ | |
| ONR SyAPs | ✓ | ✓ | | ✓ | | ✓ | ✓ | ✓ | ✓ | (✓) | | |
| NERC CIP | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | (✓) | | |

TABLE II
ANALYSIS RESULTS

controls and links back to organisational security policies. However, although comprehensive in its overview, it does not provide guidance for implementing controls but refers to external resources for this advice.

*2) IEC 62443:* IEC 62443 is an exhaustive series of standards that provide a range of both requirements and controls. Specific implementation guidance is provided for each control. A particular aspect is how it provides requirement enhancements for the controls discussed, which can be beneficial during implementation. Additionally, it covers four different security levels for the life cycle of the controls. However, although it refers to external resources, it does not refer to these at an individual control level.

*3) NIST SP 800-82:* NIST SP 800-82 provides an overview of multiple control categories, sub-categories, and individual controls, which link back to various policy requirements. It also provides multiple control requirements for assessing levels of implementation (low, medium, high) for individual controls, which allows for greater depth. However, guidance is only provided where OT-specific guidance is required; otherwise, it refers back to NIST SP 800-53. No references to external resources are made within the guidelines.

*4) ISO/IEC 27019:* ISO/IEC 27019 consists of a thorough set of objectives and controls for OT, which are mapped to security policies within other documents of the same family. It presents OT-specific supplementary guidance for controls provided in ISO/IEC 27002, on which it heavily relies, but does not provide controls where it deems that no OT-specific commentary is needed. There are no references to external resources for each control; however, the document does refer to external resources within the bibliography.

*5) NCSC CAF:* The NCSC CAF uses an outcome-based approach consisting of four high-level objectives, each containing control categories and sub-categories. It does not explicitly refer to information security policies; instead, it does this implicitly. However, it does cover a range of requirements, such as regulatory requirements. Within the document, there is high-level guidance for implementing controls, but the examples provided can also be used as guidance. The framework heavily references and relies on external resources for further implementation and guidance, including IEC 62443 and ISO/IEC 27001.

*6) ONR SyAPs:* The ONR Security Assessment Principles focus on the nuclear sector and guidance towards its regulation. We identified no direct security objectives in the documents, but these can be derived from the provided control categories. No in-depth control implementation is provided, but the requirements are extensive and can be used as high-level guidance. Throughout the SyAPs, there are no references to external resources.

*7) NERC CIP:* The NERC Critical Infrastructure Protection standards comprise a comprehensive set of documents covering many controls. There are multiple documents that contain different control categories which have multiple sub-categories. Although no in-depth implementation guidance is provided, example evidence can be used as high-level guidance. Additional use of Violation Severity Levels is incorporated to determine the level of non-compliance to the standard. There are no references to external resources.

*8) Discussion:* Our analysis of the seven selected OT standards and guidelines, based on the defined criteria set, has led to several key findings. Overall, the majority of the standards examined meet most of the established criteria. The broad conclusion is that the security controls present within

these OT standards and guidelines are generally mature and comparable to their IT counterparts. However, there are a few notable areas where improvements can be made, which are discussed here.

Significantly, many of the OT standards and guidelines do not provide explicit implementation guidance. Instead, they often refer back to primarily IT-focused parent standards, or provide only implicit guidance through example evidence or requirements for correctly implementing each control. This can make it challenging for organisations to effectively adapt and apply these controls to their OT environments, as the guidance may not be tailored specifically to OT systems.

During our analysis, several inconsistencies across the standards in terms of content were also identified. For instance, while the NCSC CAF does discuss controls for improving Response and Recovery capabilities, the NIST CSF provides more detailed guidance in these areas. This discrepancy may result in varying levels of implementation quality and effectiveness, as organisations following different standards might focus on different aspects of security controls depending on the guidance provided.

## V. Conclusion

This paper proposes a model to benchmark OT standards and guidelines and evaluate their maturity. The review of seven OT standards and guidelines shows that they do well against the defined criteria; however, deficiencies were found concerning the practical implementation of the provided security controls. The structure and high-level overview of controls were found to be adequate; however, areas concerning practical implementation require further development. The parent documents of the reviewed standards are mostly IT-focused or do not cover the applicability or implementation of novel security approaches, such as honeypots [33], for OT environments.

Given the convergence of the IT and OT environments, a greater level of maturity is required from these standards. Considering the challenges of IT/OT convergence, more attention must be paid to interconnected IT and OT systems. Such additional attention should also be reflected in the OT standards and guidelines, which are often less up-to-date than those of their IT counterparts. For example, NIST SP 800-53 was last updated in 2020, whereas NIST SP 80-82 was last updated in 2015. This can lead to a lack of consistency in the quality of implementation guidance for OT systems. Inconsistencies also exist between some of these documents when defining specific terms, which could lead to confusion where multiple standards and guidelines are adopted simultaneously.

Using the proposed model, future work needs to assess a more complete set of OT standards and guidelines. This will provide a more complete overview of their maturity, thus allowing a comprehensive set of recommendations for their improvement to be identified.

## References


[1] K. Schwab, *The fourth industrial revolution*. Currency, 2017.

[2] P. Didier, F. Macias, J. Harstad, R. Antholine, S. A. Johnston, S. Piyevsky, D. Zaniewski, S. Zuponcic, M. Schillace, and G. Wilcox, "Converged plantwide ethernet (CPwE) design and implementation guide," *Rockwell Automation*, vol. 9, p. 564, 2011.

[3] B. Green, R. Derbyshire, M. Krotofil, W. Knowles, D. Prince, and N. Suri, "Pcaad: Towards automated determination and exploitation of industrial systems," *Computers & Security*, vol. 110, p. 102424, 2021.

[4] S. Maesschalck, A. Staves, R. Derbyshire, B. Green, and D. Hutchison, "Walking under the ladder logic: Plc-vbs: a plc control logic vulnerability scanning tool," *Computers & Security*, vol. 127, 2023.

[5] R. Derbyshire, B. Green, D. Prince, A. Mauthe, and D. Hutchison, "An analysis of cyber security attack taxonomies," in *IEEE European Symposium on Security and Privacy Workshops*. IEEE, 2018.

[6] T. Miller, A. Staves, S. Maesschalck, M. Sturdee, and B. Green, "Looking Back to Look Forward: Lessons learnt from Cyber-Attacks on Industrial Control Systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 35, p. 100464, 2021.

[7] NCSC, "NCSC CAF guidance," http://bit.ly/3FDvAOO, 2022.

[8] NIST, "Framework for improving critical infrastructure cybersecurity," bit.ly/3Y8G92M, 2018.

[9] NIST, "Security control - definition," https://bit.ly/3ZgijmW, 2023, last accessed: 13/02/2023.

[10] D. Parsons, "The state of ICS/OT cybersecurity in 2022 and beyond," 2022.

[11] M. Bristow, "A SANS 2021 survey: OT/ICS cybersecurity," 2021.

[12] G. A. Francia, D. Thornton, and J. Dawson, "Security best practices and risk assessment of SCADA and industrial control systems," 2012.

[13] NIST, "NIST Special Publication 800-53, Revision 5," https://bit.ly/3ZfiVJs, 2020.

[14] North American Electric Reliability Corporation, "Nerc cip standards," http://bit.ly/3JxBbHl, 2006.

[15] U. Gentile and L. Serio, "Survey on international standards and best practices for patch management of complex industrial control systems: the critical infrastructure of particle accelerators case study," *Int. J. Crit. Comput. Based Syst.*, vol. 9, pp. 115–132, 2019.

[16] T. Kulik and P. Larsen, "Towards formal verification of cyber security standards," vol. 30, 10 2018, pp. 79–94.

[17] 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 *25th IEEE ETFA*, vol. 1, 2020, pp. 1544–1551.

[18] IEC, "IEC 62443," 2019.

[19] The Association of German Engineers, "VDI/VDE 2182," 2020.

[20] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones, "A survey of cyber security management in industrial control systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 9, pp. 52–80, 2015.

[21] A. Staves, T. Anderson, H. Balderstone, B. Green, A. Gouglidis, and D. Hutchison, "A Cyber Incident Response and Recovery Framework to Support Operators of Industrial Control Systems," *International Journal of Critical Infrastructure Protection*, vol. 37, no. 100505, pp. 1–24, 2022.

[22] M. Whitman and H. Mattord, *Principles of Information Security*. Cengage Learning, 2011.

[23] ISO/IEC, "BS EN ISO/IEC 27001:2022," 2022.

[24] ——, "BS EN ISO/IEC 27002:2022," 2022.

[25] E. Humphreys, "Information security management standards: Compliance, governance and risk management," *Information Security Technical Report*, vol. 13, no. 4, pp. 247–255, 2008.

[26] P. Roy, "A high-level comparison between the nist cyber security framework and the iso 27001 information security standard," in *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)*, 2020, pp. 1–3.

[27] Y. Kurii and I. Opirskyy, "Analysis and comparison of the NIST SP 800-53 and ISO/IEC 27001: 2013," *CEUR Workshop Proceedings*, 2022.

[28] ISO/IEC, "BS EN ISO/IEC 27000:2018," 2018.

[29] NIST, "Computer security objects register," http://bit.ly/3JTXYP8, 2022.

[30] K. Stougger, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security, Revision 2," https://bit.ly/3lqq6Qu, 2015.

[31] ISO/IEC, "BS EN ISO/IEC 27019:2017," 2017.

[32] Office for Nuclear Regulation, "Security Assessment Principles for the Civil Nuclear Industry," bit.ly/3YWvMiN, 2017.

[33] S. Maesschalck, V. Giotsas, B. Green, and N. Race, "Don't get stung, cover your ics in honey: How do honeypots fit within industrial control system security," *Computers & Security*, vol. 114, 2022.