Wirtschaftsinformatik 2024 Proceedings Wirtschaftsinformatik

2024

Cyber Security in the Smart Grid: Mapping Standards

Laura Niemann
OFFIS - Institute for Information Technology, laura.niemann@offis.de

Arlena Wellßow
OFFIS - Institute for Information Technology, arlena.wellssow@offis.de

René Kuchenbuch
OFFIS - Institute for Information Technology, rene.kuchenbuch@offis.de

Oliver Werth
OFFIS - Institute for Information Technology, oliver.werth@offis.de

Mathias Uslar
OFFIS - Institute for Information Technology, mathias.uslar@offis.de

Recommended Citation
Niemann, Laura; Wellßow, Arlena; Kuchenbuch, René; Werth, Oliver; and Uslar, Mathias, "Cyber Security in the Smart Grid: Mapping Standards" (2024). *Wirtschaftsinformatik 2024 Proceedings*. 123.
https://aisel.aisnet.org/wi2024/123

Cybersecurity in the Smart Grid: Mapping Standards
Research Paper

Laura Niemann[1], Arlena Wellßow[1,2], René Kuchenbuch[1], Oliver Werth[1], and Mathias Uslar[1]

[1] OFFIS – Institute for Information Technology, Oldenburg, Germany
{laura.niemann, arlena.wellssow, rene.kuchenbuch, oliver.werth, mathias.uslar}@offis.de
[2] Carl von Ossietzky University Oldenburg, Oldenburg, Germany
{arlena.wellssow@uni-oldenburg.de}

Abstract. The integration of information and communication technology (ICT) into the energy grid, making it the smart grid, necessitates enhanced security measures due to the potential impact of component failures on critical infrastructures. To ensure comprehensive security coverage, organizations should establish information security measures. There are various guidelines available that describe information security measures. It is important to compare the various information security guidelines in this area to ensure comprehensive information security. This paper compares NISTIR 7628 with the ISO/IEC 27000 family and the German IT Grundschutz Compendium. A security recommendation table is created to systematically identify variations in security requirements across these standards. The discrepancies between ISO/IEC 27002 edition 2013 and 2022 are also considered. The identified differences are highlighted and emphasized, and it is demonstrated that a uniform language for the different documents would be beneficial.

Keywords: Cybersecurity, Smart Grid, ISO/IEC 27002, NISTIR 7628, IT Grundschutz Compendium

1 Introduction

Today's world is fast-paced, and global connectivity is facilitated by technology. Information and communication technologies (ICT) are integrated almost everywhere, which has implications for the security measures needed. ICT has been increasingly integrated into the energy grid, resulting in the development of the smart grid (IEA 2019, Bush 2014). As the energy grid is considered a critical infrastructure, it is crucial to implement security measures. With the addition of ICT components, the failure of these components can lead to severe incidents in the smart grid. It is essential to cover this new area as these components have a significant impact on the grid (Mathas et al. 2021, Soltan et al. 2018, Huang et al. 2019).

To maintain a certain level of information security, organizations can select from various standards and guidelines (Susanto et al. 2011). Several studies have already compared different standards, revealing insights into their roles and functionalities (Sommestad et al. 2010, Susanto et al. 2011, NIST 2021). This paper aims to examine the information security standards utilized in the context of smart grids. For this purpose,

19th International Conference on Wirtschaftsinformatik
September 2024, Würzburg, Germany

we select the standards that are currently in use in this field. NISTIR 7628 serves as a central guideline for the security of smart grids, thereby underscoring its great importance in this area (Hasan et al. 2024, Stojkov et al. 2021, Leszczyna 2018, de Kinderen et al. 2022). ISO/IEC 27002, specifically adapted to the energy sector by extending ISO/IEC 27019, is also widely used and has recently undergone an update (ISO/IEC 2022, Topa & Karyda 2019). The European Commission's M/490 mandate referenced the three standards in the preliminary set of standards delineated for the security of smart grids (CEN et al. 2012). Therefore, we examine these three standards and, as a further study component, include the IT Grundschutz Compendium as a national security guideline (Federal Office for Information Security 2022*a*).

Therefore, with this study, we want to investigate the compatibility and uniformity of information security standards in the smart grid. Hence, our research questions are:

RQ 1 What are the differences between the security requirements of NISTIR 7628, ISO/IEC 27002/27019 and IT Grundschutz Compendium?

RQ 2 How do standards like NISTIR 7628, ISO/IEC 27002/27019, and the IT Grundschutz Compendium contribute to the consistency and reliability of security requirements?

We aim to motivate the need for uniform concepts and terminologies of security standards in the smart grid context. We also target the benefits of a unified international standard or unifiable national standards in combination with a matching international standard. In addition, we will present some gaps that have arisen in the process of creating a mapped security recommendation table. The paper is intended to stimulate discussion about the effectiveness of standards for information security management and their impact on organizations' operations. The contribution compares the NISTIR 7628 with the ISO/IEC 27002 and ISO/IEC 27019, as well as the IT Grundschutz Compendium, including a mapping table (Federal Office for Information Security 2021).

The next section provides an overview of the study's background. Section 3 presents the methodology, and Section 4 presents the results. Section 5 discusses the implications of the aforementioned findings and Section 6 concludes this work.

2 Background

2.1 Comparison and Selection of Security Standards

The comparison of security standards is a topic of considerable interest and is addressed in several academic works. Methodologies have been developed to facilitate comparisons between different standards. One study introduced a conceptual model for security standards, enabling the instantiation of a template with diverse security standards, while another focused on assisting product vendors in meeting multiple security standards across different regions (Beckers et al. 2014, Stojkov et al. 2021). Additionally, some studies compare different standards with each other. A study from Susanto et al. (2011) compared ITIL, COBIT, ISO/IEC 27001, BS 7799, and PCIDSS, revealing that each standard fulfills a distinct role. Another study from Sommestad et al. (2010) compared SCADA cybersecurity standards and guidelines with ISO/IEC 27002, and there is also a mapping between NIST SP 800-53 and ISO/IEC 27001 (NIST 2021). In addition, studies examine the effectiveness of the combination of different security controls within organizations or compare the extent to which organizations comply with a security standard (Hassandoust et al. 2021, Hajizada et al. 2024).

Selecting and examining standards relevant to the smart grid is important to enable a meaningful comparison of standards in the smart grid. In the M/490 mandate of the European Commission, the Smart Grid Coordination Group identified a preliminary set of standards derived from existing documents relating to security in the smart grid (CEN et al. 2012). Among these, they identified the NISTIR 7628 guideline as a key reference. Furthermore, NISTIR 7628 continues to be regarded as a pivotal security standard in the smart grid (Hasan et al. 2024, Stojkov et al. 2021, Leszczyna 2018, de Kinderen et al. 2022). Accordingly, NISTIR 7628 represents the fundamental basis for the study. Furthermore, the Smart Grid Coordination Group identified the widely used standard ISO/IEC 27002, which has been tailored to the energy sector through its extension ISO/IEC 27019 (CEN et al. 2012, 2014). A new version of this standard underlines the relevance of ISO/IEC 27002, published in early 2022, and includes changes to the structure and individual security requirements (ISO/IEC 2022, Topa & Karyda 2019). For this reason, we include both standards in the study. The IT Grundschutz Compendium is also included in the study, as it serves as a national security guideline and represents a fundamental publication on IT baseline protection (Federal Office for Information Security 2022*a*).

2.2 Standards and Guidelines

The NISTIR 7628 is a three-volume report that organizations can use to address cybersecurity effectively (NIST 2014). The report focuses on the smart grid domain. It aims to establish appropriate security requirements in a complex and highly interconnected environment. This paper focuses on Volume 1, describing the individual security requirements being compared. The security requirements are divided into categories based on NIST SP 800-53 (NIST 2020). Furthermore, all safety requirements are assigned a safety level (low [L], moderate [M], or high [H]). Safety requirements may include additional specifications for medium or high-impact levels in certain instances (NIST 2014).

The IT Grundschutz Compendium describes security measures that ensure adequate protection for all information within an institution (Federal Office for Information Security 2022*a*). The German Federal Office for Information Security published the Compendium, which contains standardized security requirements suitable for typical deployment scenarios. The document is divided into modules listing security requirements for their target objects and grouping individual topics accordingly. The security requirements are divided into basic requirements, standard requirements, and requirements for increased protection needs. The basic requirements represent the minimum of reasonably implementable security measures. Adequate security according to the state of the art is only achieved by implementing the standard requirements. The exemplary requirements for increased protection needs have also proven themselves in practice, indicating how an institution can additionally secure itself in the face of heightened security requirements (Federal Office for Information Security 2022*a*).

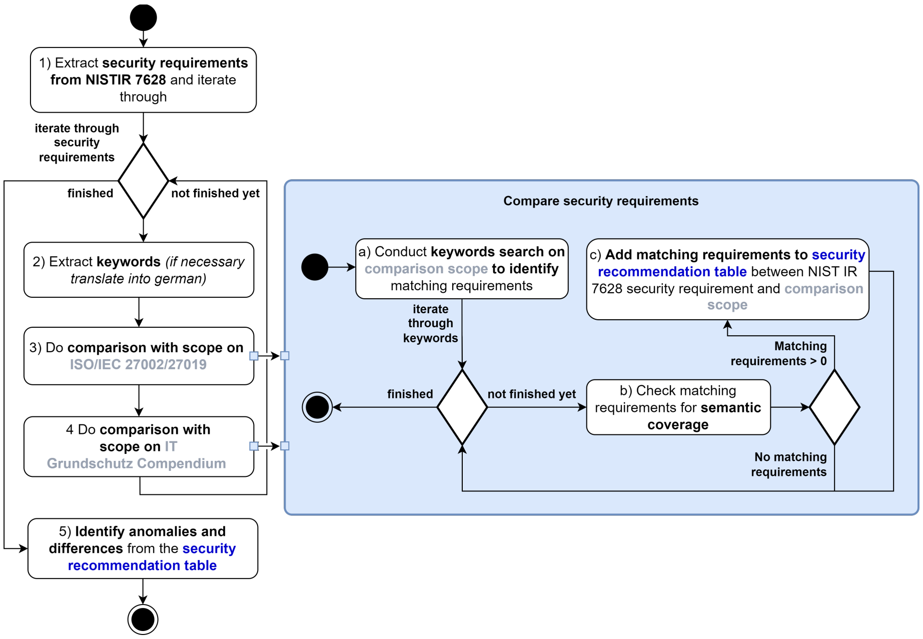
ISO/IEC 27002 is an international standard for information security management systems (DIN 2017). It offers guidance on organizational policies and management practices related to information security and includes measures considering the context of information security risks within an organization. In this paper, we refer to the standard EN ISO/IEC 27002:2017, which is the German version of ISO/IEC 27002:2013, and which we will refer to as ISO/IEC 27002 in the following (DIN 2017). The standard is divided into 14 information security sections and lists 114 security requirements. This version of the standard has been used for comparison in this paper as there is an extended ISO/IEC 27019 for this version (ISO/IEC 2017). In February 2022, a revised version of ISO/IEC 27002:2022 was published, which we will also consider (ISO/IEC 2022). ISO/IEC 27019, in its current 2017 version, extends ISO/IEC 27002:2013 to include information security management measures for process control systems and automation technology and provides supplementary guidance and sector-specific measures. This document is specifically tailored to the information security requirements of the energy sector, which is crucial given the critical infrastructure status of energy systems (ISO/IEC 2017). The relevance of including both security standards lies in that ISO/IEC 27019 extends ISO/IEC 27002 by not repeating the security requirements already described but by referring to them and providing additional specifications.

The German Federal Office for Information Security issued the mapping table, which maps the IT Grundschutz Compendium to the ISO/IEC 27001/27002 (Federal Office for Information Security 2021). The table lists the ISO/IEC 27001/27002 security requirements and assigns one or more of the IT Grundschutz Compendium security requirements to them. Since the mapping table was only available for the IEC 27002:2013 version and the IT Grundschutz Compendium Edition 2021, the document, which defines the changes between the IT Grundschutz Compendium Edition 2021 and 2022, was also included (Federal Office for Information Security 2022*b*).

3 Methodology of Standardization Mapping

To compare the NISTIR 7628 and the IT Grundschutz Compendium, as well as the ISO/IEC 27002 and ISO/IEC 27019, we analyze the text passages describing each mitigation. The procedure is shown in Figure 1. The process begins with 1) extracting the security requirements from NISTIR 7628 to iterate through them. We 2) select the initial security requirement and extract its relevant keywords. The keywords were selected based on their relevance to the field of information security and their pivotal role in the security requirement. The keywords are translated into German and used in German texts, including their variations. For example, we take the security requirement AC-4 Access Enforcement: "The organization requires smart grid information systems to enforce assigned authorizations for controlling access to the smart grid information system in accordance with organization-defined policy" (NIST 2014) and extract the keywords "authorization" (German: Berechtigungen) and "controlling access" (German: Zugangskontrolle, Zugriffskontrolle, Zugangsrecht, Zugangssteuerung).

We then carry out 3) the comparison with ISO/IEC 27002 and ISO/IEC 27019 by performing a) a keyword search to identify matching elements. The identified security requirements were then analyzed and checked for semantic coverage (step b). We looked closely at what parts of the security requirements were and might not be covered. Three researchers conducted the checks to minimize errors and increase objectivity. If the test resulted in a match, we mapped the corresponding security requirement from the ISO/IEC 27002 and/or ISO/IEC 27019 in a security recommendation table to the corresponding security requirement of NISTIR 7628 (step c). To illustrate, the search for the keywords in ISO/IEC 27002 led to the identification of 15 security requirements (9.1.1, 9.1.2, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.4.1, 9.4.2, 9.4.5, 11.2.6, 12.4.3, 14.3.1, 15.1.2) as well as ISO/IEC 27019 security requirement 7.1.2. Subsequently, we subject the security requirements to analysis and review of semantic coverage. We determined that the security requirements 9.1.2, 9.2.2, and 9.2.3 in ISO/IEC 27002 address the AC-4 of the NISTIR 7628. Consequently, we included these in the security recommendation table for AC-4. After that, or if there is no match, we move on to the next keyword. If no keywords are left, the process is finished, and we move to step 4). Steps a to c are repeated. If there are additional security requirements, we repeat the process from step 2. Otherwise, we will finish the iteration because we have already compared all the security requirements. The results of the comparisons are two comprehensive security recommendation tables, one for the NISTIR 7628 with ISO/IEC 27002/27019 and one for the NISTIR 7628 with the IT Grundschutz Compendium. These two security recommendation tables provide an overview of the similarities and differences between the mapped standards and can be used to investigate the anomalies and differences (step 5).



1) Extract security requirements from NISTIR 7628 and iterate through
iterate through security requirements
finished
not finished yet
2) Extract keywords (if necessary translate into german)
3) Do comparison with scope on ISO/IEC 27002/27019
4 Do comparison with scope on IT Grundschutz Compendium
5) Identify anomalies and differences from the security recommendation table
Compare security requirements
a) Conduct keywords search on comparison scope to identify matching requirements
iterate through keywords
finished
not finished yet
b) Check matching requirements for semantic coverage
Matching requirements > 0
No matching requirements
c) Add matching requirements to security recommendation table between NIST IR 7628 security requirement and comparison scope

Figure 1. Description of the method

Afterward, we compare the mappings of ISO/IEC 27002 and the IT Grundschutz Compendium to the security requirements of NISTIR 7628 using the mapping table

(Federal Office for Information Security 2021). To ensure that the mappings between the security requirements of these two documents and NISTIR 7628 are reflected, we have reviewed the mappings listed in the mapping table. We subject any anomalies or differences to a second examination by manually comparing the generated security recommendation table with the mapping table. Additionally, the document, which defines the changes between the IT Grundschutz Compendium Edition 2021 and 2022, was utilized to clarify the differences between the editions of the IT Grundschutz Compendium, ensuring consistency between the two (Federal Office for Information Security 2022*b*). This comparison of ISO/IEC 27002 and the IT Grundschutz Compendium led to a review of the mappings to the NISTIR 7628. However, deviations from the mapping table were deliberately accepted. This was because not all of the assigned security requirements of the IT Grundschutz Compendium matched due to different orientations of a security requirement of NISTIR 7628 compared to ISO/IEC 27002.

4 Results

4.1 Evaluating Discrepancies in Comparisons

The analysis first focused on the frequency of different terms used in the security requirements of the various documents. To achieve this, we extracted the terms and their frequency from the security requirements of the standards and guidelines to be examined, excluding filler words from the analysis. A summary is presented in Table 1. The term "information security" was used sparingly in NISTIR 7628 and ISO/IEC 27019, appearing only 12 and 22 times, respectively. In contrast, the German translation of the term, "Informationssicherheit", was used frequently, appearing 141 times in ISO/IEC 27002 and 119 times in the IT Grundschutz Compendium. The German documents rarely use the term security ("Sicherheit"), whereas it appears frequently in NISTIR 7628 (361 times) and ISO/IEC 27019 (72 times). NISTIR 7628 uses the term "information system" 523 times, while in the other documents (German translation "Informationssystem"), it appears minimally, with 0-37 occurrences. The term "access" corresponds to the German words "Zugang", "Zutritt", or "Zugriff", each with slightly different meanings that require context for accurate interpretation. Additionally, while NISTIR 7628 and ISO/IEC 27019 consistently use "organization", ISO/IEC 27002 prefers the German translation "Organisation" and the IT Grundschutz Compendium uses "Institution". These examples illustrate the differences in terminology and demonstrate the challenges of mapping.

The mapping of a security recommendation table reveals that individual security requirements from NISTIR 7628 are rarely covered by a single security requirement from the IT Grundschutz Compendium or ISO/IEC 27002 and ISO/IEC 27019 combined (see Figure 2). Only 18 cases allow for the coverage of a security requirement of NISTIR 7628, with only one security requirement from the IT Grundschutz Compendium, compared to 28 in the ISO/IEC 27002/27019. As seen in the Figure 2, in 121 cases, four or more security requirements of the IT Grundschutz Compendium are required to cover one security requirement of the NISTIR 7628. In the ISO/IEC 27002/27019 there are 56 cases. However, the total number of security requirements in the ISO/IEC 27002/27019

Table 1. Frequency of different terms

term	German translations	NISTIR 7628	IT Grundschutz Compendium	ISO/IEC 27002	ISO/IEC 27019
Information security		12			22
	Informationssicherheit		119	141	
security		361			72
	Sicherheit		23	27	
information system		523			4
	Informationssystem		0	37	
access		146			54
	Zugang		15	45	
	Zugriff		99	21	
	Zutritt		19	12	
organization		466			50
	Organisation		13	205	
	Institution		380	0	

is significantly lower than in the IT Grundschutz Compendium, and we count security requirement identifiers only once when the baseline requirement from IEC 27002 and the matching additional requirement from IEC 27019 were mapped both. Nevertheless, it is clear that in most cases, there is no clear correspondence of security requirements between the NISTIR 7628 and the mapped documents.

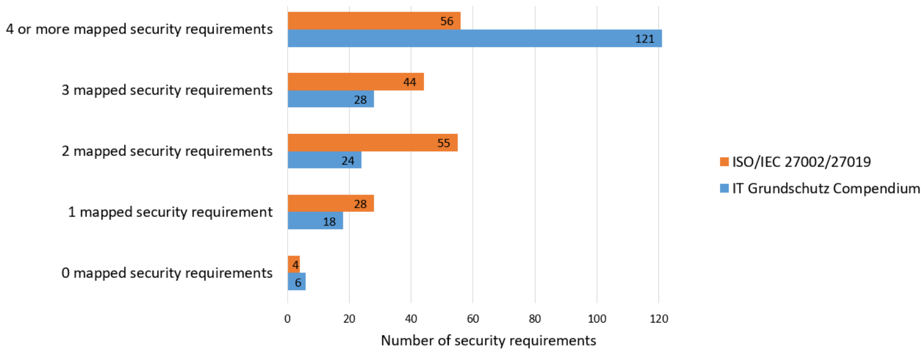


Figure 2. Number of security requirements in the IT Grundschutz Compendium and the ISO/IEC 27002/27019 that were mapped to one security requirement of NISTIR 7628

It can also be seen in Figure 2 that 6 security requirements of NISTIR 7628 are not covered by the IT Grundschutz Compendium, compared to 4 in the ISO/IEC 27002/27019 (for comparison with the 2022 version see subsection 4.2). The NISTIR 7628 security requirements AC-18, IA-2, SC-23, SC-24, SC-27, and SC-28 are not covered in the IT Grundschutz Compendium, while AC-11, SC-24, SC-25, and SC-28 are not covered in the ISO/IEC 27002/27019 (see Table 2). It is noticeable that if one of the two documents does not address a security requirement of NISTIR 7628, the other document also fails to provide comprehensive coverage. In the ISO/IEC 27002/27019 and the IT Grundschutz Compendium, paragraphs SC-24 and SC-28 are not covered. This implies that NISTIR 7628 is the sole document that addresses using honeypots and deploying virtualization strategies to represent gateway elements as disparate component types or components with disparate configurations (NIST 2014).

Table 2. Security requirements not covered

Standard	Security requirements from NISTIR 7628 not covered
ISO/IEC 27002/2019	AC-11 Concurrent Session Control, SC-24 Honeypots, SC-25 Operating System-Independent Applications, SC-28 Virtualization Techniques
IT Grundschutz Compendium	AC-18 Use of External Information Control Systems, IA-2 Identifier Management, SC-23 Thin Nodes, SC-24 Honeypots, SC-27 Heterogeneity, SC-28 Virtualization Techniques

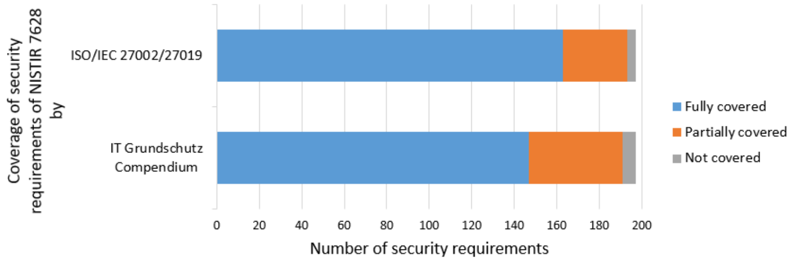


Figure 3. Coverage of the security requirements of NISTIR 7628 by ISO/IEC 27002/27019 and the IT Grundschutz Compendium

Additionally, to the security requirements that are not addressed at all, some security requirements are partially but not fully addressed (see Figure 3). In addition to the four security requirements that are not covered, ISO/IEC 27002/27019 addresses 30 security requirements to some extent and 163 in total. The IT Grundschutz Compendium covers 44 security requirements only partially and 147 completely. The extent to which the security requirements in NISTIR 7628 are covered by ISO/IEC 27002/27019 and the IT Grundschutz Compendium differs. Both documents partially cover security requirement AC-4 in the NISTIR 7628 and lack the sensitization and training record for each user (NIST 2014). In contrast, AC-8 is fully covered by the IT Grundschutz Compendium, while the ISO/IEC 27002/27019 lacks the mention of the maximum number of consecutive invalid login attempts (NIST 2014). The opposite applies as well, such as in the case of AC-10, which is fully covered by the ISO/IEC standards. At the same time, the IT Grundschutz Compendium does not mention informing the user about previous logins/login attempts (NIST 2014). It is possible that ISO/IEC 27002/27019 and the IT Grundschutz Compendium partially cover a security requirement in NISTIR 7628, but each addresses different aspects. MA-4 of NISTIR 7628 exemplifies this. The IT

Grundschutz Compendium does address the topic of maintenance, however, it does so in the context of remote maintenance and with a narrow focus on general maintenance. In contrast, the ISO/IEC 27002/27019 lacks the approval and monitoring of maintenance tools. It is important to note that the mentioned security requirements are just examples, and there are other similar cases. This is, therefore, the reason for the discrepancies in the mapping table (Federal Office for Information Security 2021).

Figure 4 shows the number of assignments of the IT Grundschutz Compendium modules to the NISTIR 7628 security requirements. As can be seen, there is a range of 0 to 54 occurrences. The security requirements from OPS.1 of the IT Grundschutz Compendium, which deals with IT operations in internal environments, were assigned most frequently (54 times). This underlines the unevenness of the formulated security requirements. Some individual security requirements in the IT Grundschutz Compendium have a high frequency of e.g. 21 (ISMS.1) or 19 (ORP.5.A1) occurrences, showing that different approaches have been taken to formulate the security requirements in the various documents. In addition, the security levels in NISTIR 7628 and the IT Grundschutz Compendium are partly different. An example is SYS.4.1.A22 in the IT Grundschutz Compendium, which is a baseline requirement. In NISTIR 7628, MP-6 identifies the same requirements as SYS.4.1.A22, but implementation is only required at medium or high impact levels.

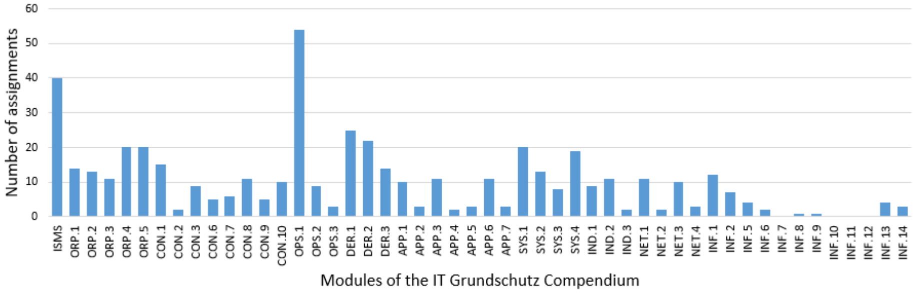


Figure 4. Number of assignments of the modules of the IT Grundschutz Compendium to the security requirements of NISTIR 7628

The security recommendation table confirmed the relevance of ISO/IEC 27019. In some cases, ISO/IEC 27019 was able to cover the security requirements of NISTIR 7628 that were not (fully) covered by ISO/IEC 27002. For example, the combination of the 12.6.2 of ISO/IEC 27002 and the 14.2.10 of ISO/IEC 27019 fully covers the security requirement SC-23 of NISTIR 7628. Another example is AC-18 (NISTIR 7628), which has no equivalent in IEC 27002 (and in the IT Grundschutz Compendium) but is covered by the security requirements 6.1.6, 11.3.3, 13.1.5 of ISO/IEC 27019.

4.2 Comparison with ISO/IEC 27002:2022

This part contains the updates to ISO/IEC 27002:2022 (ISO/IEC 2022). We will focus primarily on the changes that differ from IEC 27002. The structure has been adjusted and

Table 3. Merged security requirements

ISO/IEC 27002:2022	ISO/IEC 27002	Mapped to NISTIR 7628
5.36	18.2.2, 18.2.3	AU-14, CA-6
5.8	6.1.5, 14.1.1	CA-2
8.1	6.2.1, 11.2.8	-

various security measures have been added, removed, or merged. The annex to ISO/IEC 27002:2022 (ISO/IEC 2022) includes an overview of the changes. Upon examination of the merged security requirements, it is unclear whether the structure has converged with NISTIR 7628. A selection can be seen in Table 3. For example, we jointly mapped the ISO/IEC 27002 security requirements 18.2.2 and 18.2.3 to NISTIR 7628 security requirements in the security recommendation table. These two security requirements have been merged into security requirement 5.36 in ISO/IEC 27002:2022. Another example is 6.1.5 and 14.1.1 from ISO/IEC 27002, merged into security requirement 5.8 in ISO/IEC 27002:2022. In the recommendation table, security requirement 6.1.5 is only mapped to CA-2 of NISTIR 7628 together with 14.1.1. In contrast, security requirements 6.2.1 and 11.2.8 from ISO/IEC 27002 have been merged into security requirement 8.1 in ISO/IEC 27002:2022. These two security requirements have not been mapped to a NISTIR 7628 security requirement in the security recommendation table.

We compared the security requirements added in ISO/IEC 27002:2022 to the identified gaps, namely AC-11, SC-24, SC-25, and SC-28 of NISTIR 7628. ISO/IEC 27002:2022 explicitly addresses security requirement SC-24 in section 8.12, which covers honeypots. Additionally, this new security requirement addresses parts of SC-28. However, the new security requirements do not cover AC-11 and SC-25. Furthermore, the new security requirements of ISO/IEC 27002:2022 cover the security requirements of NISTIR 7628 that were previously only partially covered in the security recommendation table. For instance, ISO/IEC 27002:2022's security requirement 8.9 specifies the configuration management plan's contents, fully covering the security requirement CM-11 of NISTIR 7628.

The ISO/IEC 27002:2022 introduces a new security requirement, 8.28, which pertains to secure coding. NISTIR 7628 covers the topic in SA-8, SA-9, and SA-10. While ISO/IEC 27002 addresses this issue in various security requirements in section 14.2, the new edition summarizes secure coding under a single security requirement and provides more detailed information. As Burgdorf & Jendria (2022) points out, ISO/IEC 27002 now explicitly includes security requirements that were previously only implied. Furthermore, it is worth noting that ISO/IEC 27002:2022 introduces new security requirements, e.g., 5.23, that are not currently covered in NISTIR 7628.

5 Discussion and Implications

As evidenced by the study, there is no direct method for rapidly comparing the standards and guidelines with one another due to the disparate structures and terminologies employed. Other studies also highlight the ambiguity of formulations and the different information positions in the standards (Dori & Thomas 2021, Asprion et al. 2023). In addition, the different degrees of detail, completeness, and difficulty of information presentation were listed (Dori & Thomas 2021, de Kinderen et al. 2022, Asprion et al. 2023). Updating standards and the multitude of correlation tables between the old and new standards further complicate maintaining an overview. However, organizations are subject to a multitude of standards and guidelines about information security - further augmented by sector-specific regulations (Leszczyna 2018, Taherdoost 2022, CEN et al. 2014). Therefore, it can be challenging for organizations to ascertain which information security guidelines are currently in force and which are being implemented, as well as the transition to newer standards. The creation of security recommendation tables can facilitate the recognition of the distinctions and similarities between different standards and guidelines, thereby enabling organizations to adapt their measures in a more informed manner. Concurrently, this research has enriched the scientific discourse on security standards, which is in line with the ongoing importance of security standards (Romano & John 2024, Oberhofer et al. 2024).

The identified gaps and differences, as well as the variations in the scope of the standards and the fact that different standards encompass distinct risks and security requirements, suggest that implementing a single standard does not encompass the entirety of cybersecurity risks. The different orientations and focus of the standards have already been recognized and discussed in other works (Taherdoost 2022, Asprion et al. 2023). Consequently, it may be advisable to consider multiple standards to achieve an adequate level of information security within the organization. While some organizations already design the application of standards on a project- or region-specific basis, some only refer to one standard (de Kinderen et al. 2022). Establishing uniform standards could assist organizations in facilitating the implementation of standards and information security within their respective organizations. Furthermore, it could facilitate fulfilling all security requirements by applying a single standard. At the same time, it should not be overlooked that an organization has specific characteristics regarding its business objectives, people, processes, and/or technologies, and selected security requirements should fit the context (Paananen & Siponen 2023). In addition, the literature also lists other factors, such as cultural aspects, individual characteristics and values, habits, and costs, which have not yet been considered in some standards (Topa & Karyda 2019).

A comparison of standards, as carried out in this study, can also benefit other areas and thus facilitate discourse on security guidelines beyond the smart grid. In other domains, such as Industry 4.0, there is also a considerable number of different information security standards, some of which overlap with those from our study (e.g., IT Grundschutz Compendium, ISO/IEC 27000 family) (Meyer et al. 2021, Karie et al. 2021). The lack of standardized approaches poses a major challenge in developing and implementing security control measures (Karie et al. 2021). The methodology employed would benefit from further elaboration and comparison with other content analytical methods. It is not possible to conclude with certainty whether the findings can be generalized to the use of other standards or other domains. In the context of Industry 4.0, for instance, overlapping standards and the lack of standardized approaches suggest that the results may be partially transferable and provide valuable insights. The harmonization of standards could, therefore, also be beneficial for other areas.

6 Conclusion and Future Work

The integration of information and communication technologies into critical infrastructure, particularly the smart grid, necessitates robust information security measures to address potential risks and vulnerabilities. Established standards like NISTIR 7628, the ISO/IEC 27000 family, and the IT Grundschutz Compendium provide a foundation for information security policies and rule-setting. As highlighted in this contribution, standardized concepts and terms play a crucial role in enabling the comparison of existing documents. The use of different terms with identical meanings can create confusion and limit consistency, ultimately diminishing reliability due to the need for double-checking every term. Repetitive mapping of the same security requirements results in redundancy, thus obstructing clarity.

By comparing the existing standards, we identified gaps and inconsistencies, which allowed for improvements and enhancements to information security practices in the smart grid sector. NISTIR 7628, the ISO/IEC 27000 family, and the IT Grundschutz Compendium have different structures and focal topics. Changing structures in standards with different mapping tables can make clarity even more difficult. Additionally, we showed that ISO/IEC 27019 provides added value for the energy sector. However, it should be noted that the comparison of the standards may reflect different interpretations and priorities. The ongoing development of standards, including the recent revisions to ISO/IEC 27002, highlights the ever-changing nature of cybersecurity and the importance of staying up-to-date with advancements in the field.

Moving forward, it is imperative to address the identified gaps and work toward harmonizing information security standards to ensure comprehensive protection of critical infrastructure. This contribution provides a basis for further research and development in this critical area and underscores the need for continuous improvement and adaptation to evolving cybersecurity challenges. The newly revised version of IEC 27002 addresses some of these gaps. However, the update to IEC 27019 is still forthcoming; during the study, a mapping table between the standards was published (Bundesnetzagentur 2022). Further research could also examine other standards and guidelines (Schlegel et al. 2017, CEN et al. 2014, ENISA 2012, European Commission 2024, Leszczyna 2018). This could be used to investigate whether the results are transferable to other domains. In addition, the security recommendation tables could be integrated into a toolchain that provides organizations with the relevant security recommendations from different standards.

7 Acknowledgements and Data Availability

The data that support the findings of this study are available upon request.
This research is funded by German Federal Ministry for Economic Affairs and Climate Action (BMWK) under agreement no. 03EI4043A (Redispatch3.0).

References

Asprion, P., Gossner, P. & Schneider, B. (2023), ‘Cybersecurity Governance – An Adapted Practical Framework for Small Enterprises’, *Hawaii International Conference on System Sciences 2023 (HICSS-56)* .

Beckers, K., Côté, I., Fenz, S., Hatebur, D. & Heisel, M. (2014), *A Structured Comparison of Security Standards*, Springer International Publishing, Cham, pp. 1–34.

Bundesnetzagentur (2022), ‘Mapping-Tabelle zwischen ISO/IEC 27019:2020 und ISO/IEC 27002:2022’, `https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/Mapping-Tabelle.html`. Accessed: 22.02.2024.

Burgdorf, M. & Jendria, K. (2022), ‘ISO 27002 revisited’, *Datenschutz und Datensicherheit - DuD* **46**, 301–304.

Bush, S. F. (2014), *Smart Grid: Communication-enabled Intelligence for the Electric Power Grid*, IEEE, John Wiley & Sons, Chichester, UL.

CEN, CENELEC & ETSI (2012), ‘SGCG/M490/D Smart Grid Information Security’, `https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Smart%20Grids%20and%20Meters/Smart%20Grids/security_smartgrids.pdf`. Accessed: 20.02.2024.

CEN, CENELEC & ETSI (2014), ‘SGCG/M490/G Smart Grid Set of Standards’, `https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Smart%20Grids%20and%20Meters/Smart%20Grids/1_sgcg_standards_report.pdf`. Accessed: 20.02.2024.

de Kinderen, S., Kaczmarek-Heß, M. & Hacks, S. (2022), ‘Towards Cybersecurity by Design: A multi-level reference model for requirements-driven smart grid cybersecurity’, *ECIS 2022 Research Papers* .

DIN (2017), Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27002:2017, DIN EN ISO/IEC 27002, Deutsches Institut für Normung, Berlin, Germany.

Dori, A. & Thomas, M. A. (2021), A Comparative Analysis of Governance in Cyber Security Strategies of Australia and New Zealand, *in* ‘PACIS 2021 Proceedings’, Vol. 107.

ENISA (2012), Smart Grid Security Recommendations, Technical report, European Union Agency for Cybersecurity, Heraklion, Greece.

European Commission (2024), ‘EU network code on cybersecurity for the electricity sector’, `https://energy.ec.europa.eu/news/new-network-code-cybersecurity-eu-electricity-sector-2024-03-11_en`. Accessed: 12.04.2024.

Federal Office for Information Security (2021), ‘Zuordnungstabelle ISO zum IT-Grundschutz’, `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Zuordnung_ISO_und_IT_Grundschutz.pdf`. Accessed: 20.02.2024.

Federal Office for Information Security (2022*a*), 'IT-Grundschutz Kompendium', `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2022.pdf`. Accessed: 20.02.2024.

Federal Office for Information Security (2022*b*), 'Änderungen in der Edition 2022 des IT-Grundschutz Kompendiums', `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/FD_Aenderungen2022.pdf`. Accessed: 20.02.2024.

Hajizada, A., Adams, M. & Moore, T. (2024), Construction and Analysis of a Large-Scale Firm-Level Cybersecurity Posture Dataset, *in* 'AMCIS 2024 Proceedings'.

Hasan, M. K., Abdulkadir, R. A., Islam, S., Gadekallu, T. R. & Safie, N. (2024), 'A review on machine learning techniques for secured cyber-physical systems in smart grid networks', *Energy Reports* **11**, 1268–1290.

Hassandoust, F., Subasinghage, M. & Singh, H. (2021), Information systems security - "How much is enough?", *in* 'PACIS 2021 Proceedings'.

Huang, B., Cardenas, A. A. & Baldick, R. (2019), Not Everything is Dark and Gloomy: Power Grid Protections Against IoT Demand Attacks, *in* 'Procedings of the 28th USENIX Security Symposium', Usenix Association, Santa Clara, CA, USA.

IEA (2019), Status of Power System Transformation 2019, resreport, International Energy Agency, Paris, France. CC-BY-SA 4.0.

ISO/IEC (2017), Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry, Technical Report ISO/IEC 27019:2017, International Organization for Standardization/International Electrotechnical Commission, Geneva, Switzerland.

ISO/IEC (2022), Information security, cybersecurity and privacy protection — Information security controls, Technical Report ISO/IEC 27002:2022, International Organization for Standardization/International Electrotechnical Commission, Geneva, Switzerland.

Karie, N. M., Sahri, N. M., Yang, W., Valli, C. & Kebande, V. R. (2021), 'A Review of Security Standards and Frameworks for IoT-Based Smart Environments', *IEEE Access* **9**, 121975–121995.

Leszczyna, R. (2018), 'A review of standards with cybersecurity requirements for smart grid', *Computers & Security* **77**, 262–276.

Mathas, C.-M., Vassilakis, C., Kolokotronis, N., Zarakovitis, C. C. & Kourtis, M.-A. (2021), 'On the Design of IoT Security: Analysis of Software Vulnerabilities for Smart Grids', *MDPI Energies* **14**(10), 2818.

Meyer, M., Schoop, M. & Schoop, D. (2021), 'Systematic Comparison of Methods in Threat and Risk Analysis of ICT Security in Industry 4.0', *UK Academy for Information Systems Conference Proceedings 2021* .

NIST (2014), Guidelines for Smart Grid Cybersecurity Revision 1, Technical Report NISTIR 7628 Revision 1, National Institute of Standards and Technology, Gaithersburg, MD.

NIST (2020), Security and Privacy Controls for Information Systems and Organizations, Technical Report NIST SP 800-53 Revision 5, National Institute of Standards and Technology, Gaithersburg, MD.

NIST (2021), ‘NIST SP 800-53, Revision 5 Control Mappings to ISO/IEC 27001’, `https://csrc.nist.rip/csrc/media/publications/sp/800-53/rev-5/final/documents/sp800-53r5-to-iso-27001-mapping.docx`. Accessed: 20.02.2024.

Oberhofer, D., Hornsteiner, M. & Schönig, S. (2024), Process-Aware Security Standard Compliance Monitoring and Verification for the IIoT, *in* ‘ECIS 2024 Proceedings’.

Paananen, H. & Siponen, M. (2023), ‘Organization Members Developing Information Security Policies: a Case Study’, *ICIS 2023 Proceedings* .

Romano, R. & John, B. (2024), A Cybersecurity Standards and Frameworks Knowledge Graph For The Education Of Sustainable Australian Smaller Businesses, *in* ‘ECIS 2024 TREOS’.

Schlegel, R., Obermeier, S. & Schneider, J. (2017), ‘A security evaluation of IEC 62351’, *Journal of Information Security and Applications* **34**, 197–204.

Soltan, S., Mittal, P. & Poor, V. H. (2018), BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid | USENIX, *in* ‘Proceedings of the 28th Usenix Security Symposium’, Usenix Association, Baltimore, MA, USA.

Sommestad, T., Ericsson, G. N. & Nordlander, J. (2010), SCADA system cyber security — A comparison of standards, *in* ‘IEEE PES General Meeting’, pp. 1–8.

Stojkov, M., Dalčeković, N., Markoski, B., Milosavljević, B. & Sladić, G. (2021), ‘Towards Cross-Standard Compliance Readiness: Security Requirements Model for Smart Grid’, *Energies* **14**(21).

Susanto, H., Almunawar, M. N. & Tuan, Y. C. (2011), ‘Information Security Management System Standards: A Comparative Study of the Big Five’, *International Journal of Electrical Computer Sciences IJECSIJENS* **11**, 23–29.

Taherdoost, H. (2022), ‘Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview’, *Electronics* **11**(14).

Topa, I. & Karyda, M. (2019), ‘From theory to practice: guidelines for enhancing information security management’, *Information & Computer Security* **27**(3), 326–342.