energies

MDPI

Article

Towards Cross-Standard Compliance Readiness: Security Requirements Model for Smart Grid

Milan Stojkov [1,*], Nikola Dalčeković [1], Branko Markoski [2], Branko Milosavljević [1] and Goran Sladić [1]

[1] Faculty of Technical Sciences, University of Novi Sad, Trg D. Obradovića 6, 21000 Novi Sad, Serbia; nikola.dalcekovic@uns.ac.rs (N.D.); mbranko@uns.ac.rs (B.M.); sladicg@uns.ac.rs (G.S.)
[2] Technical Faculty Mihajlo Pupin, University of Novi Sad, Đure Đakovića bb, 23000 Zrenjanin, Serbia; markoni@uns.ac.rs
* Correspondence: stojkovm@uns.ac.rs

Abstract: The critical infrastructure is constantly under cyber and physical threats. Applying security controls without guidance or traceability can create a false sense of security. Security standards facilitate security knowledge and control best practices in a more systematic way. However, the number of standards is continually increasing. Product providers that operate in multiple geographical regions often face the obligation to comply with multiple standards simultaneously. This introduces the problem of the convenient interpretation of different standards. Thus, a comprehensive analysis of the requirements from different security standards and guidelines applicable to the smart grid has been performed to detect similarities that can be shaped into entities of the conceptual model for requirement representation. The purpose of the model—presented in a form of a Unified Modeling Language (UML) class diagram—is to give product providers a canonical way to map requirements from arbitrary standards, guidelines, and regulations and accelerate the cross-standard compliance readiness by defining priority for requirement implementation. In addition, the research showed that multiple vectors should impact the priority of the implementation of the security controls defined through the requirements: domain affiliation, the essence of the requirement, associated threats, risks, and social dependencies between actors involved in the implementation. To examine the model correctness, NISTIR 7628—de facto smart grid standard—was used to provide insights into how the model would be used for requirements implementation tracking. The structure of individual requirements was analyzed to detect the building blocks and extract relevant parts that can be mapped to the model components. Further, all requirements were classified into one of the defined domains to provide the basis for referencing similar requirements from different standards. Finally, one arbitrary requirement was used to demonstrate model usage, and depict all available information that can be provided to the users in a custom-made scenario where the need arises to have simultaneous alignment with three standards—NISTIR 7628, NIST 800-53, and IEC 62443-3-3.

Keywords: critical infrastructure protection; smart grid; standards; compliance; security requirements; requirement prioritization

check for updates

Citation: Stojkov, M.; Dalčeković, N.; Markoski, B.; Milosavljević, B.; Sladić, G. Towards Cross-Standard Compliance Readiness: Security Requirements Model for Smart Grid. *Energies* **2021**, *14*, 6862. https://doi.org/10.3390/en14216862

Academic Editor: Ahmed Abu-Siada

Received: 1 September 2021
Accepted: 14 October 2021
Published: 20 October 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Over the decades, humanity has made several leaps to improve the overall quality of life by making essential goods available to the common world in an efficient manner and at the lowest possible cost. Resources such as electric power, oil, gas, and water are being used in everyday life, but the goal is to always use them optimally and securely. Many systems—also referred to as critical infrastructures (CI)—are built to support that idea. In the Report of the United States of America President's Commission on Critical Infrastructure Protection (CIP) from 1997, the term infrastructure is interpreted as "a network of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow

of essential goods and services" [1]. Further, the USA Patriot Act of 2001 defines critical infrastructure as "systems and assets, whether physical or virtual, vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" [2]. The USA Presidential Policy Directive 21 (PPD-21) Critical Infrastructure Security and Resilience supersedes the initial reports and defines sixteen critical infrastructure sectors: chemical, commercial facilities, communications, critical manufacturing, dams, industrial base defense, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waste, transportation systems and water and wastewater systems [3]. The advances in information and telecommunication network technologies made it possible to construct new concepts such as the Energy Internet (EI) that combine power and electronics technology and a large number of power, petroleum, and natural gas networks. This opens the door for transitioning from traditional centralized control methods to distributed control based on artificial intelligence (AI) methods to solve optimization and security problems in energy management and control [4]. For example, Hua et al. in [5] incorporated curriculum learning with deep reinforcement learning to achieve noticeable minimization of overall operating costs in microgrids where future research can build upon.

Conversely, operations that are being performed with these systems can introduce increased risk to the health and safety of human lives and damage to the environment, as well as a serious financial impact on a nation's economy [6]. Considering the exceptional heft these definitions bear, CIP implies the existence of the processes of protecting critical infrastructure's physical assets, citizens, and critical cyber networks that are necessary for public safety, economy, and national security.

This paper focuses on the security aspect of critical infrastructures, especially in the smart grid sector. From this perspective, critical infrastructure systems can be analyzed in two ways—in isolation and as an integral part of the one large and unified ecosystem. If we analyze each system in isolation, we could potentially establish a greater security level, but we would ignore the natural dependencies and interdependencies that exist between different critical infrastructures. For example, energy stakeholders provide power to stakeholders in the water, information technology, and transportation sectors, and in return, the energy sector relies on water for electricity generation, on transportation for fuel delivery, or information technology for easier energy management. Rinaldi et al. in [7] describe four types of interdependencies that can be found between infrastructures that, if compromised, could result in a domino effect disrupting regular work of the system:

- Physical interdependency—if the state of one infrastructure is dependent on the outputs of the other;
- Cyber interdependency—if infrastructures' states depend on information transmitted through the information infrastructure;
- Geographic interdependency—if a local environmental event can create state changes in all infrastructures;
- Logical interdependency—if the state of one infrastructure depends on the state of the other via a mechanism that is not a physical, cyber, or geographic connection.

Years back, previously mentioned critical infrastructure sectors became more reliant on industrial control systems such as supervisory control and data acquisition (SCADA), programmable logic controllers (PLC), and distributed control systems (DCS) for monitoring, control, and operation of physical devices such as sensors, pumps, valves, meters, etc. In addition, due to further work and cost optimization, these systems are often integrated with business systems such as management information systems (MIS), billing systems, enterprise resource planning (ERP), and other external systems that require the use of more ordinary hardware and software besides the industrial one. This collaboration between the systems is inevitable, and making them secure is a big challenge since the innovative approaches for cyberattacks are exponentially increasing. Over the years, famous

attacks have happened—Black Energy, Stuxnet, Duqu, Triton, to name several. The energy sector is one of the main targets of cyber-attacks against critical infrastructure. Business Blackout—a joint report by Lloyd's and the University of Cambridge's Centre for Risk Studies—constructed a hypothetical scenario of an electricity blackout in the United States that could cause the total impact to the US economy at USD 243 bn, rising to more than USD 1trn in the most extreme version of the scenario [8].

Although multiple attacks were performed in the past, there is a modestly low amount of publicly available information about them despite the ever-growing awareness that is being promoted in various ways. Attacks that are focused on SCADA-oriented systems can be orchestrated through different routes from Internet connections, over business or enterprise networks to the level of the field devices. As described in [9], common attack vectors can vary from backdoors and holes in network perimeter, field devices, vulnerabilities in common protocols, database attacks, communication hijacking, and Man-in-the-middle attacks.

Attacks can be performed on each level of the Purdue Model [10]—an industry adopted reference model that shows the interconnections and interdependencies of all the main components of a typical Industrial Control System (ICS)—regardless of the type of the system architecture, traditional or influenced by the Internet of Things and edge computing.

To mitigate the potential damage that can be made, all these systems must be protected on multiple levels, by introducing and maintaining the defense in depth. The adequate mechanisms must be set in place not only from the technology standpoint, but they have to cover the people and processes too (to complete the people, process, and technology (PPT) framework). To achieve and maintain a certain level of security, these three parts of a whole have to be regulated through governance, security management, and security controls. This can be performed employing several techniques mentioned in no particular order of relevance:

- expanding knowledge base through information sharing;
- practicing regular vulnerability assessment and hardening security controls;
- practicing different kinds of tabletop exercises;
- practicing regular auditing;
- implementing requirements from relevant standards.

Information sharing is one of the approaches to build knowledge about new trends, attack- and defense-wide. This was recognized at a national level, and today, we have different organizations such as national Community Emergency Response Teams (CERTs), or more specifically, Electricity Information Sharing and Analysis Center (E-ISAC) in the United States, European Energy Information Sharing and Analysis Centre (EE-ISAC), Japan Electricity Information Sharing and Analysis Center (JE-ISAC), or Critical Infrastructure Gateway in Canada that are built to improve the resilience and security in the energy sector by sharing verified information. This is a good way to establish and strengthen that connection between different CI entities.

Vulnerability assessment or red team penetration testing are practices that have to be performed regularly and are obligatory to demonstrate the current security posture of the system as suggested by the North American Electric Reliability Corporation (NERC) for Critical Infrastructure Protection set of requirements. Since these techniques are considered invasive, it is suggested not to be performed in a production environment in a manner that can have an adverse impact [11]. By continually practicing these acts properly, the attack surface should reduce and the overall maturity of the system, as well as the organization, will increase.

Engaging in different exercises that simulate cyber and physical attacks are additional approaches for practicing security. GridEx [12] organized by NERC and Cyber Storm [13] organized by Cybersecurity and Infrastructure Security Agency (CISA) are good examples of events that give that opportunity. This is the least formal technique of the ones mentioned

here. It can be organized on a national level or only with the customers that are operating CI systems.

The Information Systems Audit and Control Association (ISACA) and Protiviti state that cybersecurity is positioned as the top technology challenge for IT audit professionals [14]. The cybersecurity audit is supposed to be a comprehensive review of the PPT that includes investigating different management practices, security controls that are employed, risk and compliance provisions, and governance at the system or organizational level. This can be challenging since the end-users can be engaged in activities that are only partially covered by the business purpose and the infrastructure that is used may not reside only in a private network of the organization. That is why clear audit boundaries and objectives must be defined. In addition, audits usually follow some framework or standard that has well-defined requirements that have to be satisfied. The study also states that organizations should consider continuously reviewing their IT audit plans to address cybersecurity threats and emerging technologies. It is also shown that conducting audits is equally important in all geographic regions (over 50%).

Nations across the world recognized the importance of cybersecurity and developed different legislative procedures, regulations, and recommendation acts to address security issues. Only in the past five years, the number of published acts in European countries has dramatically increased [15]. Security standards and recommendations developed by eminent bodies such as the International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Center for Internet Security (CIS), European Union through the European Programme for Critical Infrastructure Protection (EPCIP) [16] represent the proper guidelines that can help governments and companies not only to evolve and enhance their critical infrastructure systems posture but also to gain recognition in form of certification. These standards present the accumulated knowledge about cybersecurity in the form of formal security requirements that can be applied to different types of systems, varying from software used by small and medium-sized enterprises (SMEs) or CIP used by large corporations.

By looking at the techniques mentioned above, standards and audits usually come together. Understanding different standards and their requirements can be challenging, as well as preparing for the audit and formal certification. In addition, different standards have similar requirements that have to be satisfied. That is why these organizations, national or privately held, may have a dilemma which standards should follow, and understand the similarities and differences between them. By comparing standards side by side, organizations can gain a deeper understanding and can choose appropriate standards that define requirements which implementation can offer a high level of protection, relative to costs and effort that is required for their fulfillment. What is more important in terms of this paper, there is often a need to be compliant with more than one standard, especially for product providers that operate in different countries. There are multiple frameworks, maturity models, self-assessment tools that are supposed to help the organizations to see the current state of cybersecurity in their organization or systems, but usually one standard at the time. In addition, risk assessment is usually performed separately although, from the audit perspective, to design appropriate objectives this is advisable to have prepared all together. To complicate the story further, often the implementation of respectful security posture in the organization or the system does not follow the compliance with standards by default but is subsequently being corrected.

In this paper, we tackle these perplexities. We investigate if security requirements defined in different standards, guidelines, and regulations by various eminent standardization bodies can be transformed to the canonical form based on their similarities. This model can further serve as a foundation for building applications that can help security practitioners and decision makers in reasoning about which standards to comply with, their similarities, what controls to implement, where, and with what priority.

Concretely, to improve existing methods, our contribution is to define a conceptual model for requirement representation—presented as a Unified Modeling Language (UML)

class diagram—that can be used for tracking of implementation and compliance with multiple security standards, guidelines, and regulations simultaneously in a uniform manner. To accomplish that goal, the model is enriched by:

- Social actors' dependency chain that is used for easier tracking of the dependencies between actors that are involved in the security requirement implementation. The social actors are recognized as the entities that can introduce additional complexity into decision making about what requirements to implement in which order and their variable nature in different organizational setups mark them as the component that must be further discussed;
- Numerically expressed prioritization criteria that are dependent on the domain where the requirement is classified, the necessity of the requirement implementation based on the custom nomenclature, associated threats, risks, and social actors' dependency chain. These vectors all together provide insights for each requirement that is not implemented and help to place it higher or lower on the implementation priority map. This component is important because it contains a couple of vectors that together make the prioritization criteria the connecting unit between the plain model of the requirements and actual guidance for requirements implementation.

To achieve this, the research has gone through a three-stage methodology. The first stage used a mixture of quantitative and qualitative methods through grounded theory during systematic literature review to detect relevant standards, guidelines, and regulations that will bear adequate information that can be patterned. In further text, standards, guidelines, and regulations will jointly be referred to as publications. During the first stage, by detecting relevant patterns, not only entities that would comprise the model were extracted but the concrete interpretation of how to use them is defined and that was demonstrated in the model validation stage. Further, the assurance model for requirements classification was elicited and implementation prioritization strategy and appropriate actor dependencies were defined. The second stage used the results of the first stage as an input such as domain classifications that are used in different publications and security requirements themselves to create a conceptual model that can be used to represent each new requirement. In the final stage, to validate our model, one of the smart grid guidelines not participating in model creation was used.

This paper is structured as follows: Section 2 describes the state-of-the-art related work. Section 3 explains in a detailed manner the methods used to analyze publications and define domains, assurance model, actors, and implementation prioritization strategy. Section 4 shows the conceptual model for security requirements representation. A discussion of the results is presented in Section 5. Finally, Section 6 summarizes the conclusions the authors have drawn from this paper.

2. Related Work

Beckers et al. in [17] presented a conceptual model for security standards that contains concepts and phases from different security standards. The researchers created a template based on that model that can be further used for mapping and instantiating arbitrary standards. When the instances of the standards are made, they can be compared, and the main goal of the comparison is for the upper management to feel the difference between the standards and choose the right direction for certification. The template describes what and on which level of details information in standards is presented. Only a few similar standards were used (such as International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) 27001 and German IT-Grundschutz) as a base for a conceptual model. In addition, the authors attempted to define uniform terminology used in different standards.

Hale et al. [18] define a process based on semantic hierarchies that can extract relevant security requirements from control standards using three patterns—impose, perform, and protect. By using this process, security controls can be patterned and related to other controls in a form of semantic hierarchies using semantic relations. The approach is

demonstrated on the requirements in the audit domain of the NIST Special Publication (SP) 800-53, Department of Defense Instruction (DoDI) 8500.2, and ISO 15408-2 standards.

In [19], Leszczyna presented a systematic review to identify the most relevant smart grid standards, guidelines, technical reports, special publications, and regulations that present strong guidance for the security practitioners to make comprehensive security assessments. Standard selection and evaluation criteria are clearly presented. The study has shown that six smart grid or power systems' standards provide information on security assessment processes that can be applied to Industrial Automation and Control Systems (IACS), substations, or all smart grid components. These standards provide general guidance such that they can still be used as a reference for assigning responsibilities or scheduling security assessment actions. Similar research is performed by Alcaraz et al. in [20] and more specific comparison of a lower number of standards is performed in [21]. Since these papers can be classified as a systematic literature review, none of them further discuss potential model creation but present a good starting point for the work that is performed here.

Numerous methods for requirements prioritization have been proposed in the literature [22]. Most of the proposed methods, if not all of them, can be applied to security requirements. Tariq et al. presented an interesting approach to prioritization of the information security controls in the context of cloud computing networks and wireless sensor networks by using fuzzy analytical hierarchy process (AHP) [23]. The authors consulted decision makers and defined seven main criteria for security controls selection: implementation time, effectiveness, risk, budgetary constraints, exploitation time, maintenance cost, and mitigation time. Every control was assigned weight for each criterion and the control with the highest score was selected as the best control. The proposed approach was applied to ISO/IEC 27001 security controls. In [24] authors propose an extension to threat modeling with a goal to allow the prioritization of security requirements via a valuation graph that includes assets, threats, and countermeasures. There were also efforts to automate the prioritization of the requirements by utilizing data mining and machine learning techniques [25], although effectiveness is limited by the used algorithms, and efforts from the stakeholders are still needed.

A collaborative effort by the NIST and FedRAMP resulted in the creation of Open Security Controls Assessment Language (OSCAL) [26]. OSCAL provides a common machine-readable meta schema expressed in eXtensible Markup Language (XML), JavaScript Object Notation (JSON), and YAML Ain't Markup Language (YAML) for different compliance and risk management frameworks as well as sharing system security plans, security assessment plans, and reports. Its goal is to enable organizations to exchange information via automation and provide interoperability. It is architected in layers with the lowest layer being Controls Layer that has a Catalog Model that models security control definitions and control assessment objectives and activities from any cybersecurity framework as e.g., XML file. Each file has a well-defined structure for easy conversion between supported formats. The second part of the layer is the Profile Model that models control baselines which are a customized subset of controls selected from one or more catalogs for a given purpose or security posture. It provides placeholders for describing what to import, merge or modify from the Catalog Model. Since it is an ongoing development, there are only a few examples of future usage of some features, especially merging of similar security controls and their modification. The next layer is the Implementation Layer which consists of the Component Model with the purpose to allow the maintainers of assets to describe and share how the asset can be implemented to satisfy specific controls, and System Security Plan Model with the purpose to document the states of control implementation within an information system. The final layer is the Assessment Layer that consists of an Assessment Plan that allows assessment plan information to be defined, Assessment Results that collects information produced from a set of assessment activities, and the Plan of Actions and Milestones Model that provides a set of assessment findings. It is a promising initiative led

by respected organizations that can be built upon. Our model presented in the paper is compatible with foundational parts of the OSCAL as described in later sections.

There are also tools that are used for different types of self-assessment for cybersecurity resilience and standards compliance. These tools were analyzed to extract the model used for their construction. The Cyber Security Evaluation Tool (CSET) was developed by the Department of Homeland Security (DHS) [27]. The tool provides a framework for the analysis of the vulnerabilities that can affect ICS and IT infrastructures. The main goal of CSET is to lower the risk of the attack by detecting the vulnerability in the existing system. It serves as a centralized repository of security requirements. It has a rich database of security standards that are both free and paid. At the start of the assessment, the tool requires setting an adequate Security Assurance Level (SAL)—overall criticality rating based on user revisions of security scenarios and estimated consequences. The SAL level (low, medium, high, very high) determines the number of questions that are presented to the user. The SAL value is also used in consideration during unanswered question ranking. Besides custom questions that are built based on security requirements extracted from standards, the tool introduces the plugin for graphical modeling of the system components. This is further used to ask additional questions based on the selected components. CSET is a praiseworthy security assessment tool that can be used by a wide range of industries. It is focused on individual components of the system and not on the system as a whole. Analysis of the system architecture that can be drawn is limited to the general high-level requirements extracted from different standards. In addition, the tool does not provide more sophisticated risk analysis details. Further, if the user selects multiple security standards for self-assessment, requirements are not grouped by similarity, but only by the standard name. Further, the ranking and weighting of the questions are not explained in detail, instead it is mentioned that the subject matter experts were involved in that activity only on a component level.

In [28], the Control System Cyber Security Self-Assessment Tool (CS2SAT) is presented. The tool has to enable the users to assess the security of the control system. Its database consists of several security standards based on which questionnaire was developed. The tool requires that the organization forms a working group where the members are from different divisions, and they have to collect available documentation that has the information helpful for providing the answers to questions in the questionnaire. At the start of the assessment, the tool requires setting the SAL as in [27]. In addition, architectural diagrams of the observed solution with building components can be drawn based on which questions are added. Additionally, there is a set of questions related to selected standards based on which compliance reports can be generated. CS2SAT's algorithm prioritizes recommendations based on the criticality of the component for the system, relevance of the requirement, and the gap between system control and requirement fulfillment. These factors are used for proposing users with recommendations for mitigations. The software is the property of the US Department of Energy and is not publicly available to further inspect and confirm described features.

The authors in [29] present the Cyber Resilience Review Self-Assessment Package (CRR). The tool is a Portable Document Format (PDF) file enriched with macros where 365 questions are classified into 10 groups. Although the questions are formed based on different standards, the tool does not check the compliance against the standards but only gives the overall score. It is more of a high-level questionnaire that is constructed to be populated during the six-hour workshop. The only standout among the other analyzed tools is that CRR has the most maturity levels—six. There are more tools [30,31] that cover this topic, but their models are created for lower levels of complexity or are strictly tied with the specific domain.

By looking at previously mentioned papers, it can be concluded that similar or the same standards were used in some form as in our research. The idea of interoperability and easier exchange of standards in clearly defined form as in [26] is a step toward the renovation of the topic, but since it can be considered as a new initiative that is in the early

stage of development, the adoption rate among the organizations is yet to be determined. In addition, several tools aim to provide support for decision makers and security practitioners, but their documentation lacks the details about the reasoning behind several topics covered in our paper such as a scoring system for the prioritization of the requirements used in future final reports, approaches for requirements mapping, or clearer connection between the requirements and associated risks. Still, this collection of research is a valuable source of information that was used as a solid foundation for the work we have illustrated in this paper.

3. Materials and Methods

3.1. Publication Selection

From the first attempts in the 1980s with the publishing of orange and white books by the Trusted Computer System Evaluation Criteria (TCSEC) in the United States and the Information Technology Security Evaluation Criteria (ITSEC) in Europe, security standards evolution took a toilsome journey. First standards were more technical, but newer ones emphasize management notes, as well as best practices, certification, and security governance [32]. Without going into details of the specific standards, security officers and decision makers require a security assessment methodology that can systematically present what are the security requirements that have to be fulfilled [33,34]. The first part of the first stage was a systematic literature review and analysis followed by the selection of the relevant security publications for critical infrastructure protection. The aim was to find the publications that can help in the extraction of security control classes and construction of the model for security requirements that will help with cross-publication compliance checks and proper security assessments.

As with any literature review, the limitations of our review process must be noted. The analysis was performed based only on our interpretation of the papers. In addition, we cannot completely rule out the existence of other relevant standards that are used in some geographic regions but that were not included in the analysis. Some proposals may have not found their place in the review due to various reasons such as terminology used by authors which did not bring a paper to the attention of our analysis, a paper not being listed on the databases examined, or not consulting the gray literature. Nevertheless, the literature search method adopted helped to ensure an acceptable level of completeness of our literature review. Hence, we believe that the set of papers analyzed is representative and the results of the analysis may be generalized for the smart grid domain.

The literature review was conducted following the methodological approach proposed by authors in [35]. The aggregative databases Google Scholar and Semantic Scholar that contain papers of numerous publishers as well as recognized publishers such as IEEE and Springer were used in the search. Search keywords were “cybersecurity”, “security”, “standard”, and “requirements”, but as the results were too broad, additional keywords “smart grid”, “power grid”, and “electrical grid” were distinctively added in combination with the first four. Still, different search engines in the majority looked at each of the keywords individually; thus, the initial results had to be refined further by looking at the titles, keywords, abstracts, and eliminating duplicate and irrelevant studies, as well as employing backward and forward reference “snowballing” strategy. By employing that approach, the initial records count was significantly decreased and 34 papers that were relevant for the research were further analyzed. After a review of the selected papers, the greatest number of them only mentioned relevant publications in other contexts, and only a few of them presented the research more comprehensively. The occurrence of the most mentioned publications in relevant context is presented in Table 1.

Table 1. Publication occurrences in the study.

Publication	Type of Publication	Occurrence
NERC CIP	Regulation	16
IEC 62351	Standard	14
ISO/IEC 27001/27002	Standard	11
NISTIR 7628	Standard	11
NIST SP 800-53	Guideline	9
IEC 62443 (ISA 99)	Standard	8
NIST SP 800-82	Guideline	6
IEC 61850	Standard	4
GB/T 22239	Standard	3
DHS Catalog	Guideline	2

After the analysis, the selection of the relevant publications was performed. There are different qualitative [36–38] approaches that evaluate standards by their domain, structure, and maturity as well as quantitative [21] approaches that base their evaluation on the number of occurrences of specific keywords in the text. In this research, the initial selection was based on the quantitative approach followed by additional qualitative requirements for more fine-grained results. Based on the filtered papers and occurrences presented in Table 1, the selection of the relevant publications had to satisfy the following requirements:

- It has a published version in English;
- It is published by a standardization body or government institution;
- It has to specify security requirements that can be used for similarity and compliance testing.

Additional criteria that were applied consisted of the following rules:

- In the final set, there had to be general, not too domain-specific standards (as it is e.g., IEC 62351), guidelines, or regulations that can be adapted to the smart grid sector and that also provide better applicability to other sectors in the future;
- Standards had priorities over guidelines and guidelines had priorities over regulations. The reason for that lies in the fact that certifications aim for specific standards, guidelines are not obligatory for full compliance, and regulations are usually applied only at a national level not having large geographical coverage;
- The adoption level had to be high, and this could be checked only through grey literature.
- The final set of publications that were used for further analysis was the following:
- IEC 62443 (ISA 99)—represents a set of security standards for IACS prepared by the IEC technical committee. The goal of these standards is to provide a flexible framework that can address vulnerabilities in IACS and to apply required mitigations systematically. The concrete standard that was analyzed is IEC 62443-3-3:2013 System security requirements and security levels [39] that defines the security requirements for control systems related to the seven requirements defined in IEC 62443-1-1 and assigns system security levels to the system that is being constructed. The IEC 62443-3-3:2013 was selected since it represents the system level standard that can add diversity to the analysis;
- ISO/IEC 27001 and 27002—ISO 27001 represents one of the best-known IT security standards that is recognized all around the world. The official title of the standard is ISO/IEC 27001:2013; Information technology—Security techniques—Information security management systems—Requirements [40]. Its supplementary standard is ISO 27002 [41] that focuses on the information security controls that organizations might choose to implement and these controls are also listed in Annex A of ISO 27001. Although compliance with ISO 27001 standard alone would not be enough for securing the ICS ecosystem, this standard was selected as one general-purpose security standard that has the requirements that can be applied to different sectors;

- NIST SP 800-53—represents the guideline that is published by NIST with the official title: Special Publication (SP) 800-53 Recommended Security Controls for Federal Information Systems and Organizations (Revision 5). It is intended to be used as a toolbox containing a collection of safeguards, countermeasures, techniques, and processes to respond to security and privacy risks [42]. This guideline is versatile enough to be applied for the IT systems as well as ICS systems and even if originally aimed at systems that reside in the US, it is well recognized and applied worldwide. This publication is selected as a guideline representative;
- NERC CIP—represents the set of regulations that define how bulk electric systems (BES) prepare for cyber and physical threats that can affect the reliability of the system. Policies are required for defining, monitoring, and changing the configuration of critical assets, as well as governing access to those assets. NERC is subject to oversight by the US Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada [43]. All North American bulk power system owners, operators, and users must comply with NERC CIP standards. NERC CIP was selected as one of the most respected representatives of the regulatory type of documents and the publication with the most occurrences during the literature review.

3.2. Point of View and Controls

After the selection of the publications, an in-depth review of the security requirements of each was performed to find similarities based on which elements of the model could be extracted. There had to be a defined point of view that was suitable to approach the analysis systematically. This is necessary since direct mapping between two publications is more than challenging. For instance, if we were to compare NIST SP 800-53 and ISO/IEC 27001, we would have ISO/IEC 27001 controls that do not fully satisfy the intent of the NIST controls [44]. When more than two publications are compared, the job is more demanding since the expectation is that security requirements from different publications, if satisfied, should have to result in equivalent security posture in the end. Comparing two by two requirements for each pair of publications is not scalable at all. One common prism through which security requirements can be analyzed is defined within the NIST Cybersecurity Framework (CSF). The CSF is a risk-based approach to managing cybersecurity risk and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles [45]. The requirements are grouped by five functions that Framework Core defines to provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk: identify, protect, detect, respond, recover. CSF defines 23 domains (or categories, dimensions, or areas of knowledge) that are arranged in these functions. Categories are not fixed, and the framework allows for category extension and adjustment as in [46]. Conversely, the US Department of Homeland Security (DHS) issued a control system security report that broadly classified security sub controls into two categories—organizational sub controls that cover different security policies, organizational and personal security, and operational sub controls that cover different activities such as system acquisition or configuration management [47]. Other approaches define different numbers of domains for security requirements classification. For example, papers [27,48–51] define 26, 19, 18, 10, and 17 domains, separately. In addition, selected publications NIST800-53, IEC 62443 3-3, ISO/IEC 27001, and NERC CIP differentiate another 20, 7, 14, and 12 (with an additional 4 that are subject to enforcement in the future), respectively.

By comparing CSF with other previously mentioned approaches for defining domains for the classification of security requirements, we concluded that the initial list of the domains defined in CSF needs to be recalibrated to cover adequate aspects. By analyzing security requirements, extracting keywords that can be candidates for the domains, and cross-comparing existing domains from the selected standards and previously mentioned papers, the list of 24 domains, the new common prism, was defined and presented in Table 2.

Table 2. List of defined domains with scores.

Domain	Objective	Score
Business Continuity and Disaster Recovery	Define and practice backup and recovery procedures to recuperate in case of an incident.	4
Data Handling	Define data classification and analyze usage in the organization.	4
Identity Management and Access Control	Apply security controls for the identification, authentication, and access to the systems by complying with principles of least privilege and separation of duties.	4
Network Security	Apply security controls to protect network architecture and maintain defense-in-depth.	4
Secure Design, Implementation, and Validation	Practice secure design analysis, implementation, and validation to ensure the developed system is secure.	4
Security Monitoring	Employ security controls for the collection of security-related information.	4
Asset Management	Manage all technology assets throughout the whole lifecycle from the procurement until disposal.	3
Change Management	Employ and follow procedures to ensure only authorized changes can occur.	3
Compliance Capability	Employ regular assessments and internal audits to maintain targeted compliance.	3
Configuration Management	Establish and maintain consistency of the system's configuration within its lifecycle.	3
Endpoint Security	Apply security controls to protect endpoint devices and maintain defense-in-depth.	3
Incident Response	Define and maintain procedures for incident response.	3
Personnel Security	Practice background and psychological checks during the hiring process for a specific role.	3
Physical and Environmental Security	Apply physical and environmental controls to ensure that technology assets cannot be compromised.	3
Risk Management and Assessment	Detect, analyze, and assess all security risks that can affect human or technology assets.	3
Security Awareness and Training	Employ continuous development of the personnel by raising security awareness and culture within the organization and offer specialized training.	3
Security Operations	Employ mechanisms to implement operational security controls.	3
Security and Privacy Governance	Define an organization's systematic program to address security.	3
System, Data, and Communication Protection	Utilize well-known industry-recognized controls for securing data in transit and at rest.	3
System and Services Acquisition	Perform all needed examinations to make sure that all systems and services that are acquired comply with the organization's policies and do not introduce additional risk.	3
Vulnerability and Patch Management	Establish controls and processes to help identify vulnerabilities within the infrastructure and provide appropriate protection against threats that could adversely affect the security of the system.	3
Maintenance	Properly maintain all technology assets by applying vendor recommended configuration and industry best practices.	2
Portable Device Security	Detect, analyze, and assess all security risks that can affect human or technology assets.	2
Resource Management	Properly allocate and efficiently manage human and technology resources required for each new or existing project.	2

Next, all requirements from the selected publications were grouped into defined domains. Additionally, they were subjectively grouped by the similarity of the requirements inside a domain. During this process, by examining NIST SP 800-53, we concluded that this publication has a lot of requirement enhancements. These requirement enhancements can be grouped in different subcategories inside different domains. For example, SI-4 System Monitoring (23) Correlate Monitoring Information, IR-4 Incident Handling (4) Information Correlation, and AU-6 Audit Record Review, Analysis, and Reporting (3) Correlate Audit Record Repositories can be grouped. In addition, IEC 62443-3-3 defines four security levels that are assigned to the requirements and requirement enhancements. To be compliant with security levels above one, usually, one or more requirement enhancements have to be implemented. Based on this information, requirement enhancements were further treated as regular requirements that have the additional information from which requirements emerged.

After grouping, each requirement inside a domain was also labeled with one of the five functions (identify, protect, detect, respond, recover) as defined in CSF with each function representing a key chronological step in enhancing an organization's security. In CSF, functions represent top-level classes that amalgamate categories and subcategories. If we observe the requirements from selected publications a little more closely, we can conclude that the domains in CSF are roughly arranged into these functions. For example, CSF domain supply chain risk management is assigned to function identify. If we analyze NIST 800-53, the guideline has the domain with that name, but the requirements in that domain can be assigned differently to functions, e.g., the requirement SR-9 Tamper resistance and detection can be consequently assigned to function protect, SR-10 Inspection of systems or components to function detect and SR-2 Supply chain risk management plan to function identify. Similarly, our domain compliance capability, which does not exist in CSF, can have the requirements assigned to different functions, e.g., in ISO/IEC 27001 the requirement 9.1 Monitoring, measurement, analysis and evaluation and NIST 800-53 CA-2 Control assessments can be assigned to detect function, and ISO/IEC 27001 9.2 Internal audit and NERC CIP 014-2 R2 to identify the function. Our approach is slightly different from CSF in terms of how functions are used. Instead of observing requirements through domains up to functions, the requirements are directly labeled with one of the five functions. This approach gives more flexibility for security experts to drive risk management decisions prior to a cybersecurity event related to the requirement—identify, protect, detect—or what to do after one occurs—respond and recover. This vector is not included in the prioritization criteria described in later subsections because the degree of dependency on technology, people, and processes varies as we progress through the five functions as explained in the Cyber Defense Matrix [52].

To provide additional information for the prioritization criteria, domains had to be quantified. Some of the tools described in Section 2 have the capability to generate different reports that can sort unimplemented requirements by the importance and the implementation priority, but without a clear explanation of what methodology was used, or how many experts (and their professional backgrounds) were interviewed to construct the scoring system. We used a quantitative approach primarily based on the information extracted from the analyzed publications. The threshold values were roughly defined since this component plays a minor role in the overall priority score described in a later text, but it can be helpful to present nuances between the requirements.

The rules for calculating scores presented in Table 2 were the following:

- All 24 domains got an initial score of two on a scale of 1–2 based on the occurrence during the systematic literature review and domain definition described earlier. The scale of 1–2 is defined to support extending the domain list in the future where new domains would be assigned the value of one due to novelty and consequently immaturity of the domain. Examples of the new domains would be cloud security, edge security, or Internet of Things security;

- If the domain had over 50 requirements cumulatively, going through all publications, it got an additional one point because of the assumption that the domain can express its requirements in a fine-grained manner and leave limited to no space for the organization to interpret it more loosely. The threshold number was high since NIST SP 800-53 has a lot of requirement enhancements;
- If three or more security requirements from the same domain in three distinct publications were labeled as similar, the domain got an additional one point because of the assumption that the majority of the four different publications that were the subject of the analysis recognized the importance of that control. The similarity criteria are performed subjectively by defining subcategories inside a domain that more closely determine what is the aim of the specific requirement. For example, the domain Identity Management and Access Control can have subcategory Access Control Management where we can put IEC 62443-3-3 SR 2.1 Authorization enforcement, ISO 27001 Appendix A 9.1.1 Access control policy, NIST SP 800-53 AC-1 Access control policy and procedures, and NERC CIP 004-6 R4 Access Management program. That is sufficient for the domain to gain one additional point. Conversely, the domain Endpoint Security can have a subcategory Mobile Code where we can put on IEC 62443-3-3 SR 2.4 Mobile code and NIST SP 800-53 SC-18 Mobile code that is insufficient for the domain to improve score based on this subcategory.

3.3. Assurance Model

To construct a model, the problem needs to be tackled from multiple points. The core entity of the model are requirements, and they cannot be classified only by domain affinity but also by the additional vector—assurance level inside each domain. The assurance levels tend to provide a qualitative approach to express how sophisticated a security measure is defined in security requirements and how well the requirements are satisfied. This is one of the vectors that can be used for tracking the maturity of the security posture. Each advanced requirement requires more sophisticated attack means to make an exploit. Multiple sources describe different maturity levels [53–55] that suggest having it as one component of a model. The scale defined by Gilsinn et al. in [53] is directly incorporated into the IEC 62443-3-3 standard. Our proposed assurance level model is two dimensional—one dimension reflects the essence level and the other the maturity of implementation i.e., the implementation level.

The essence level represents the priority of the implementation of the requirements. The proposed nomenclature is numerical:

- 3—the requirement is mandatory and must be satisfied for the final solution to be acceptable;
- 2—the requirement is a high priority and should be included, if possible, within the delivery time frame with lower priority;
- 1—the requirement is desirable, but the priority is the lowest;
- 0—the requirement is not necessary to be addressed.

The numerical scale is descending to accommodate the prioritization criteria described in later sections. The specific values can be assigned driven by different goals. For example, if the goal for the organization is to prepare for IEC 62443-3-3 security level 1 certification, only requirement SR 1.1 Human user identification and authentication would be assigned the essence level 3, and all SR 1.1 requirement enhancements would be assigned the essence level 0, 1, or 2 since they are not necessary for the goal to be accomplished.

The maturity of the implementation represents the overall condition of security control implementation that is defined in the requirement. The proposed implementation levels are influenced by the scale defined in the Capability Maturity Model Integration (CMMI), concretely staged representation [55]. Although CMMI levels are process-oriented, they can be applied to all three pillars of the PPT framework since all of them can implement controls described in the requirements [42]. Since the CMMI model contributes to the performance of the product providers [56] whose needs were one of the drivers for our

research, the proposed implementation levels are highly influenced by this existing scale. The implementation levels are as follows:

- Initial—security controls introduced through requirement are implemented ad hoc with a low level of maturity and traceability;
- Managed—security controls are implemented and documented to comply with the requirement at the current point in time but without a clear vision for further improvement in case of an organizational or system change; possible requirement enhancements are not implemented;
- Defined—security controls are further improved by implementing requirement enhancements if they exist; trying to define process and technology invariants where that is possible;
- Quantitatively managed—security controls are quantitatively analyzed to identify deviations and implement further improvements;
- Optimizing—security controls are continually improved through incremental and innovative technological improvements, and lessons learned.

The second dimension—implementation levels—is the foundation for easier tracking of requirements fulfillment and expressing the overall maturity of the organization against the selected standard for compliance. For instance, the report can be generated based on the implementation levels assigned to requirements to provide statistical information about the percentage in which requirement implementation achieved e.g., optimizing level of maturity.

By introducing tracking, a clear metrics program must be defined for goals and objectives [57]. The goal represents the state that the organization tries to achieve. The actors involved in defining the goal only express the intention to achieve the goal but not the means to accomplish it. The key performance indicators (KPIs) represent information that is used to make decisions that will correct future actions that can be used to accomplish a specific goal. These KPIs can be broad and usually reflect the expectations and vision of the upper management. That is why this part of the model is supposed to be loose and conducted from the point of view of the actor. By using the previous example, the main goal can be the readiness for certification against an arbitrary standard, e.g., IEC 62443-3-3 that requires all mandatory requirements for a specific security level to be fulfilled. Here, one KPI can be the weekly burndown trend of fulfilled requirements per domain. This is interpreted by and heavily dependent on a human actor; thus, the social aspect also has to be added to the model.

3.4. Actors

It has been estimated that an error that is not identified and corrected in the requirements phase can cost a lot more to correct in subsequent phases [58]. This is also applicable to security requirements. A mitigating circumstance is that standards and guidelines already have a well-defined set of requirements, and the real challenge is shifted from the interpretation of the requirements to their implementation. As the main idea of the paper is to define a comprehensive model for the representation and tracking of compliance with security requirements based on widely used security standards, proposing a plain model of the security requirements purely based on the entities extracted from the previous section is not sufficient. Further fine-grained connections between those entities have to be defined. Since the model is aimed at security practitioners in companies, the relationship among them—the social actors—needs to be added. This changes the usual perspective of a strict organization or system-oriented requirements interpretation.

The important idea that can be used from [59] is that the i* framework identifies the domain stakeholders and models them as social actors who depend on one another for goals to be achieved. In that way, it is possible to determine why what and how requirements are being fulfilled and to verify how the final implementation matches initial needs. The i* framework proposes the concepts of social actors, goals, tasks, resources, and social dependencies to model both the system and its organizational operating environment. A

concept called an actor diagram is a graph whose nodes represent actors (agents, positions, or roles), while edges represent dependencies among them. A dependency represents an agreement between two actors where one actor (the depender) depends on another (the dependee) to fulfill a goal, perform a task or deliver a resource (the dependum). Dependencies may also involve soft goals which represent ambiguously defined goals, without clear criteria for their fulfillment. A part of these concepts can be adjusted to fit the needs of our model:

- Actor (depender and dependee) → actor involved in the implementation;
- Task as intentional element (dependum) → security requirement that is to be implemented;
- Task dependency → relationship between social actors (depender and dependee) and security requirement.

In this way, we can track all the dependencies that are involved in requirement implementation. To place this in real-life perspective, e.g., if the requirement is for an enterprise organization to provide security-related training (dependum), the security advisor (depender) needs to report the progress to the upper management in a form of a percent of people who successfully finished the training (KPI) and depends on the trainer (dependee) to organize and conduct the training, but also the trainer (depender) depends on the security engineers (dependees) to prepare the materials for the training. This forms the chain, i.e., a graph of dependencies between the social actors that allows us to have more than one actor depending on the others on each level. The chain with a big number of dependencies between actors is an early sign to start the implementation on time. Thus, for the security practitioners in the organization, it is of utmost importance to know the organizational structure or to have actors properly mapped to the business roles to track the requirement implementation dependency chain.

3.5. Prioritization Criteria

Since the model is the foundation for a better understanding of the security standards aimed at security practitioners in companies that plan compliance implementation, further prioritization of the requirements needs to be defined. There are various techniques for requirements prioritization that are often error-prone, have scalability issues, and lack the social actors' aspect [60]. Security requirements can also be closely coupled with associated threats and risks. The number of available methodologies for critical infrastructure risk assessment is large [61–63]. In many cases, existing methodologies are tailored to the organization's particular needs and biased to take into consideration only a subset of threats. There are multiple classifications but the most coarse-grained would be qualitative and quantitative approaches. As Cherdantseva et al. in [62] describe, both approaches possess a lot of disadvantages. The quantitative approaches use probabilistic methods where estimation of risk is never complete in the mathematical sense whereas qualitative ones rely on subjective data and numerous simplifying assumptions. The foundation of most of them is the construction of a security risk register where every risk has an owner that is usually someone from the management of the organization. Due to these constraints, the risk assessment component in the model has to be simplified with one goal—to boost the priority of the observed requirement. For every control that is not implemented but is requested through the requirement, there has to be an associated risk that the organization or the system is exposed to.

Further, risks are closely related to threats and often involved in calculating risk rating [64]. NIST SP 800-160 defines a threat as "an event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss" [65]. An event can include natural disasters such as floods, earthquakes, and fires as well as man-made threats such as utility service disruption or hacking. Thus, a well-established information security management system (ISMS) on the organizational level and security development lifecycle (SDL) on a system level can help in the early detection of threats. The asset or the resource of value that may be harmed by a threat is directly connected

to a requirement. Having that connection, the enumeration of the threats for each asset affected by the requirement can be defined. The actors defined in the previous section are the ones who maintain this list by constantly improving processes, expanding misuse cases, attack trees, or practicing regular threat modeling. Whatever the approach is, threats are another valuable vector that can be used to express the maturity of the organization or the system especially through the implementation levels described previously. The threats can significantly impact the risks associated with the requirements since if the threat materializes, security control defined through the requirement might not function as expected. For example, if an organization or a system operates in an area known for tornadoes, requirements labeled with respond and recover functions will impact risk rating more than those that reside in geographically safer areas. The mature threat enumeration list suggests better awareness of what assets must be protected by implementing controls defined in security requirements.

Finally, each requirement is associated with threats through affected assets and risk set that is derived from the risk register. In this way, we rely on the experts' opinions that have domain knowledge and organization or system familiarity.

The overall priority of the requirement implementation is simply the sum of all entities that have associated scores:

$$TS = DS + EL + \sum(RL \times L) + ACH, \quad (1)$$

where TS is the total priority score for the requirement. DS is the domain score on a scale of 1–4, EL is the essence level score on a scale of 1–3 where both scales are described in previous sections. RL is the risk level of the potential consequences that might result from the risk scenario if no additional response is provided. RL is assigned on a scale of 1–5 where the scale is derived from the existing risk management framework that has been used to determine grading structure in the risk register. Value one on a scale represents negligible and five catastrophic effects. L is the likelihood of the scenario occurring before any risk response and it is assigned on a scale of 1–5 where one represents improbable and five frequent occurrences. By multiplying these two values, we obtain a simple individual risk rating, and by summarizing all risk ratings calculated from the associated risk set we obtain an overall numerical risk value that can significantly boost the priority of the requirement. There are other more complex formulas for calculating risk rating [66–68], but since we use risk rating only for prioritization purposes, the basic ISO-like [69] multiplication of RL and L is sufficient. Finally, ACH is the number of actors in the social actors' dependency chain that, if it is long, can further indicate the above-average complexity of the requirement and put it higher on the priority map. In case multiple requirements have the same score, the precedence takes the requirement that has a greater risk rating score due to the biggest impact in terms of security, then essence level, social actors' dependency chain, and finally, a domain score.

By introducing multiple variables, prioritization becomes less prone to errors and less dependent on the security expert involved in the calculation of the overall priority. DS is driven by standards, EL by the business decision on which compliance level an organization or system certifies for, and ACH by organizational structure. The only room for error can be an inadequate or incomplete definition of the risk register, but since it involves multiple actors, the error space is reduced.

4. Model

4.1. Model Creation

In this paper, we went from eliciting relevant publications, over analyzing their requirements to expanding the analysis with assurance model, social actors' aspects, and prioritization criteria. All identified entities are elaborated, and the conceptual UML class diagram is constructed and presented in Figures 1 and 2.

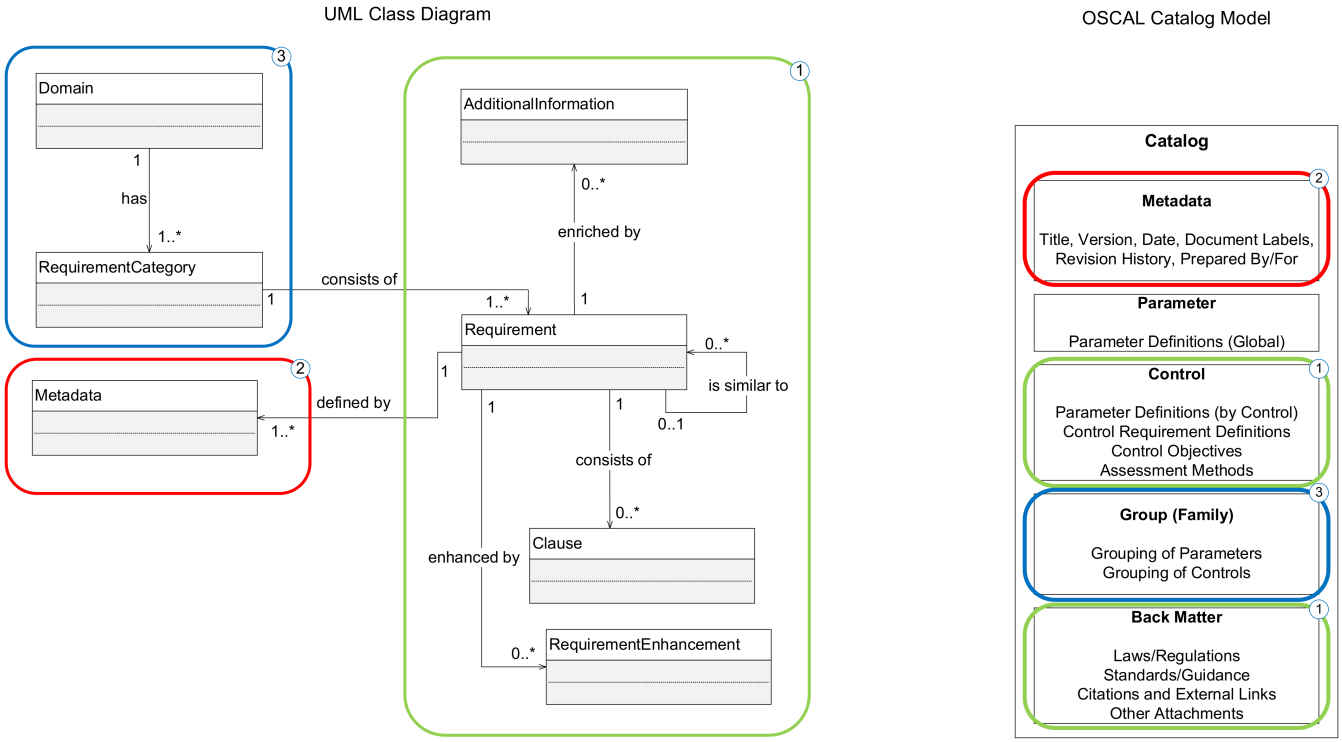


Figure 1. UML class diagram to OSCAL Catalog Model mapping.

The core model that represents only the requirement is straightforward to follow as shown in Figure 1. Different publications define their requirements in different forms. This is why we first have to detect relevant entities that each requirement is composed of. By analyzing the structure of the requirements defined in four selected standards, the generic form which can apply to all publications is defined and consists of the following elements:

- Domain—top-level category or family through which all requirements are interpreted. Each standard classifies the requirements into specific domains as discussed in Section 3, thus it is an inevitable part of the model;
- RequirementCategory—subcategory that can be used for further grouping of the requirements based on similarity. This component is omitted from the majority of the standards—only ISO/IEC 27002 defines some granulation, others have a flat structure inside a domain—and frameworks—only CSF defines subcategories and their purpose to some extent. The existence of this component is essential for finer granulation of the requirements and basis for future classification recalibration if the need arises;
- Requirement—the main entity that contains information about the requirement itself. It also has a recursive association that indicates the connection between approximately the same requirements from different publications, or requirement enhancements from the same publication;
- Clause—requirements may not be always flat as in IEC 62443-3-3, but can consist of multiple clauses, such as requirements defined in NIST SP 800-53 or NERC CIP. This dynamic nature of the requirements' definition is covered with this component;
- RequirementEnhancement—often base requirement has additional improvements. This entity can be used also for extending the base requirement with controls defined in different publications that are missing in the observed ones. This is also evidence for reaching the higher implementation levels;
- Metadata and Additional Information—consist of information such as publication name, author, version, type, the rationale for implementation, supplemental guidance, links, and other attachments.

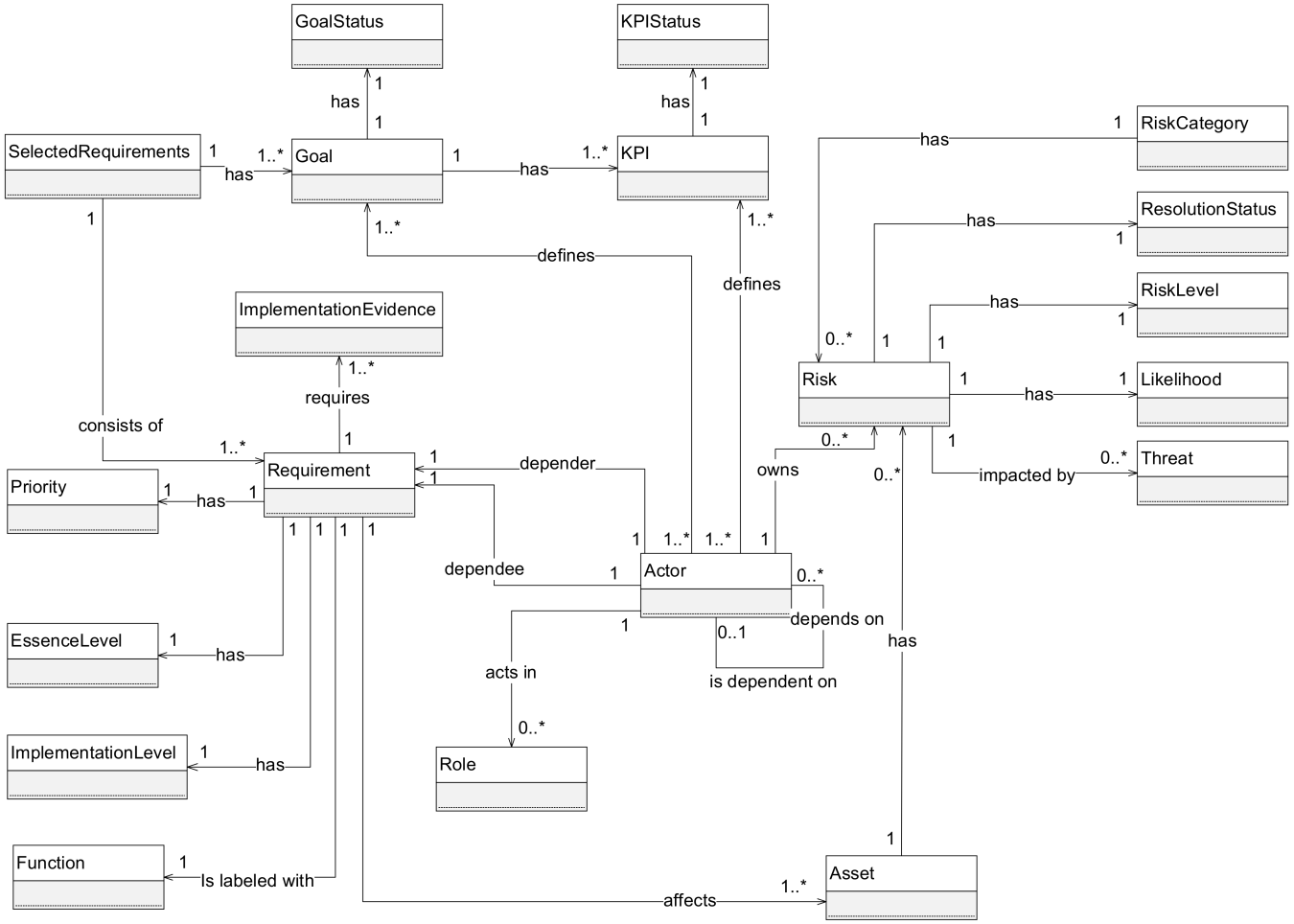


Figure 2. UML class diagram for a conceptual model.

These entities can be populated manually for each requirement, or the same information can be absorbed from OSCAL files automatically in the future. The OSCAL catalog model standardizes the exchange format of control definitions from different publications in the form of JSON, XML, or YAML files. The different document elements can be served into our model and that mapping with appropriate matching colors between the UML class diagram and OSCAL Catalog model is also presented in Figure 1. Figure 2 shows the rest of the implementation tracking model as described in Section 3.

The entities regarding the base requirement are omitted for better readability since they can be found in Figure 1. The remaining parts of the model are summarized as follows:

- SelectedRequirements—consists of the selected requirements for tracking and analysis. The selection of the requirements is heavily impacted by the goals of the project that have to be defined from the start. This is represented with Goal(s) and GoalStatus entities that are tracked through KPI(s) that are defined by the Actor(s) acting in a specific Role(s).
- Risk—represents the main component regarding prioritization criteria described in Section 3. It is associated with the Asset(s) that can be affected by the requirement implementation. Further, risks are impacted by the Threat(s), have their Likelihood, RiskLevel, and ResolutionStatus that are set after the risk analysis. Finally, every risk is owned by the Actor.
- Requirement—it is extended to give additional information essential for the implementation such as EssenceLevel of the requirement extracted from the standard, ImplementationLevel to mark the maturity of the security control, ImplementationEvidence to support the claims about the implementation, and Function (identify, protect,

detect, respond, recover). Every Requirement has the Priority that is calculated based on the Formula (1).

- Actor—it is defined as a recursive association to support the creation of actors' dependency chain that can be complex. Every Requirement has exactly one associated depender and dependee.

The activity diagram that represents the steps that are necessary for populating the database with new requirements based on the model is presented in Figure 3. Every requirement is analyzed individually. The process starts by populating relevant information about the requirement—metadata and additional information. Further, the requirement is placed in one of the categories inside a domain. After that, the detailed analysis of the main parts the requirement is constructed from—the clauses and enhancements—is carried out to better comprehend what is the objective. This can help in easier determining what function and the essence level to assign, and to make a connection with similar requirements from other standards right away during the import. This is one approach for building the knowledge database about similarities between different publications. Another approach enforces automation through already prepared OSCAL files where someone else made similarity analysis in advance, leaving the security expert only to configure additional parameters introduced with our model.

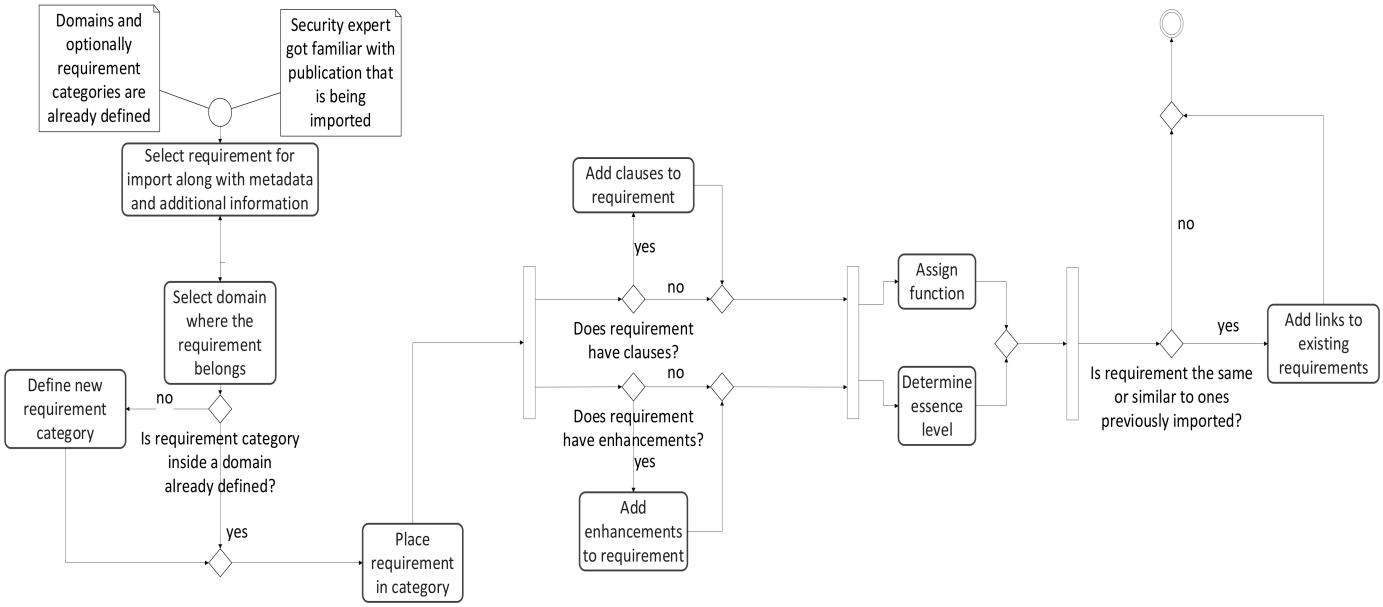


Figure 3. Process for import of new requirements.

The activity diagram that represents the initial setup for tracking the implementation of the requirements is given in Figure 4. The process starts with selecting actors or stakeholders which define goals that directly determine the subset of only relevant requirements. This subset can contain the whole standards for a specific scenario or just a fraction of them. Once the requirements are selected, they are grouped by domain and requirement category inside a domain, and their initial implementation levels are set. This can be considered as an important part of the flow that enforces the reusability of the previously collected knowledge. In other words, if the implementation level of the specific requirement is set to anything but "Initial" status by the nomenclature defined in previous sections, relevant information about risks, threats, actors' dependency chain, and evidence materials may already be familiar. This can speed up the overall analysis. In addition, by grouping the requirements by domain and subcategories, we are narrowing the similarity analysis of the requirements from different selected publications. Further, actors that will define KPIs for the analysis are defined. Then, individual requirement analysis starts by defining actors' dependency chains, risks, and threats. This stage is another good moment for making

a connection with similar requirements from other selected standards and updating the knowledge database. The initial setup ends with the assignment of the risk owner and the risk resolution.

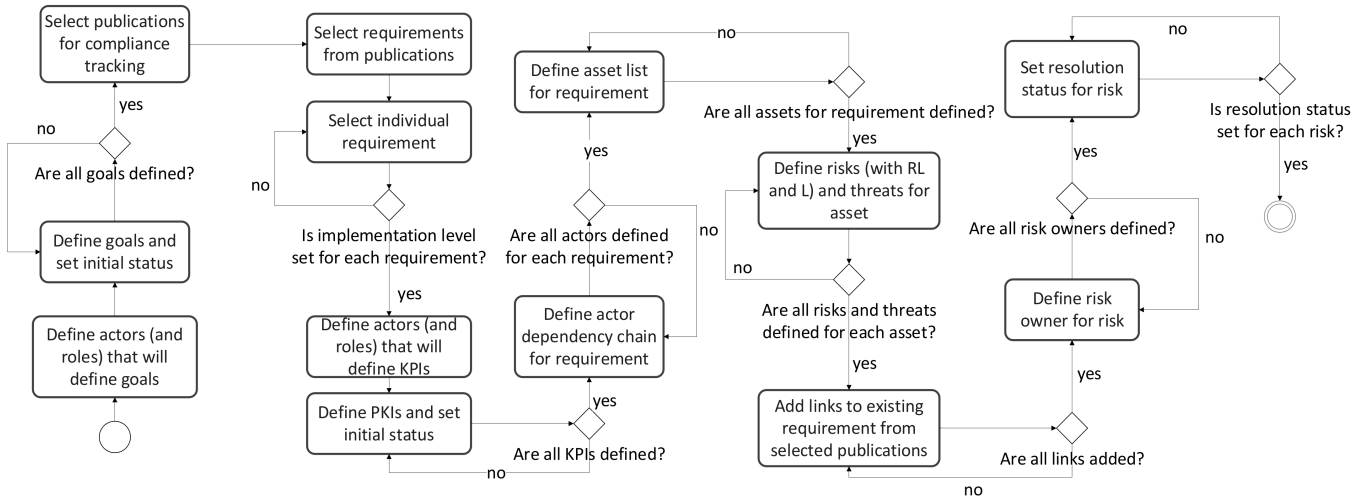


Figure 4. Initial setup for tracking requirement implementation.

By regularly updating the implementation levels for each requirement of the observed publication, overall maturity against that publication can be tracked. Progress of implementation is tracked through KPI status and overall goal status.

4.2. Model Validation

To validate our model, we used one publication that was not in the base set of standards—The National Institute of Standards and Technology (NIST) Internal or Interagency Report (IR) 7628 Guidelines for Smart Grid Cybersecurity—a highly positioned publication in Table 1 as a test publication. The goal of the validation step is to see how the requirements from this standard with their defined form respect the model that was constructed previously. NISTIR 7628 represents the three-volume report that describes an analytical framework that organizations can use to develop effective cybersecurity strategies tailored to their combinations of Smart Grid-related characteristics, risks, and vulnerabilities [70]. It was selected since it is considered as a de facto standard for Smart Grid and has well-defined requirements. Every requirement in NISTIR 7628 has a nicely defined structure where information of interest that can be used in our model are as follows:

- Name and unique identifier → can be mapped directly to class Metadata;
- Requirement base text → can be mapped directly to class Requirement;
- Requirement clauses → can be mapped directly to class Clause;
- Supplemental guidance → can be mapped to class Additional Information;
- Requirement enhancements → can be mapped directly to class RequirementEnhancement;
- Additional considerations → can be mapped to class Additional Information.

Only Supplemental guidance and Additional considerations do not map directly to the model entities, but this is understandable since this information in different publications comes in different forms. Thus, Additional Information is predicted to represent the adequate collector for these purposes.

Valuable information for requirement interpretation is presented, but not directly used in our model, in the following parts:

- Category—identifies whether the security requirement is a governance, risk, and compliance, common technical, or unique technical requirement. This information can help only during the initial mapping to closely determine in which requirement subcategory an observed requirement should be placed based on the similarity.

- The Impact Level Allocation—represents impact levels for confidentiality, integrity, and availability objectives expressed on a scale—low, moderate, and high. This information can be used by security experts for calculating prioritization criteria.

Based on the mappings, we can conclude is that the requirements from NISTIR 7628 can be represented as instances of the model which is a prerequisite for further comparison and tracking. One example instance is given in further text.

To be able to use NISTIR 7628 requirements with others from different publications, the second part of validation requires applying a domain-centric view to the NISTIR 7628 to try to classify each requirement into one of the 24 defined domains, if possible. This will demonstrate if domain definition in previous research covered all necessary aspects of the security controls. NISTIR 7628 has 197 requirements with 50 requirement enhancements originally classified into 19 domains. The mapping of the requirements to the proposed domains is given in Table 3. The enhancement requirements are mapped to the same domain as the original requirements and thus omitted from Table 3.

Table 3. NISTIR 7628 requirements mapping to domains.

Domain	Objective
Business Continuity and Disaster Recovery	SG.CP-1, SG.CP-2, SG.CP-3, SG.CP-4, SG.CP-5, SG.CP-6, SG.CP-7, SG.CP-8, SG.CP-9, SG.CP-10, SG.IR-10
Data Handling	SG.AC-20, SG.CM-9, SG.ID-1, SG.ID-2, SG.ID-3, SG.ID-4, SG.ID-5, SG.MP-1, SG.MP-2, SG.MP-3, SG.MP-4, SG.MP-5, SG.MP-6
Identity Management and Access Control	SV.AC-1, SG.AC-2, SG.AC-3, SG.AC-4, SG.AC-6, SG.AC-7, SG.AC-8, SG.AC-11, SG.AC-12, SG.AC-13, SG.AC-14, SG.AC-15, SG.AC-16, SG.AC-17, SG.AC-18, SG.AC-19, SG.AC-21, SG.CM-5, SG.IA-1, SG.IA-2, SG.IA-3, SG.IA-4, SG.IA-5, SG.SC-19
Network Security	SG.AC-5, SG.CA-4, SG.SC-2, SG.SC-5, SG.SC-7, SG.SC-18, SG.SC-21
Secure Design, Implementation, and Validation	SG.AC-9, SG.AC-10, SG.CP-11, SG.IA-6, SG.IR-9, SG.PL-2, SG.SA-8, SG.SA-10, SG.SC-3, SG.SC-4, SG.SC-6, SG.SC-22, SG.SC-24, SG.SC-25, SG.SC-27, SG.SC-28, SG.SC-29, SG.SC-30, SG.SI-6, SG.SI-8, SG.SI-9
Security Monitoring	SG.AU-1, SG.AU-2, SG.AU-3, SG.AU-4, SG.AU-5, SG.AU-6, SG.AU-7, SG.AU-8, SG.AU-9, SG.AU-10, SG.AU-13, SG.AU-15, SG.AU-16, SG.CA-6, SG.SI-4
Asset Management	SG.CM-8
Change Management	SG.CM-3, SG.CM-4
Compliance Capability	SG.AU-11, SG.AU-14, SG.CA-1, SG.CA-2
Configuration Management	SG.CM-1, SG.CM-2, SG.CM-6, SG.CM-7, SG.CM-10, SG.CM-11, SG.SA-6, SG.SA-7, SG.SA-9
Endpoint Security	SG.SC-13, SG.SC-16, SG.SC-23, SG.SI-3, SG.SI-7
Incident Response	SG.IR-1, SG.IR-2, SG.IR-3, SG.IR-4, SG.IR-5, SG.IR-6, SG.IR-7, SG.IR-8, SG.IR-11
Personnel Security	SG.PL-3, SG.PS-1, SG.PS-2, SG.PS-3, SG.PS-4, SG.PS-5, SG.PS-6, SG.PS-7, SG.PS-8, SG.PS-9, SG.SA-2
Physical and Environmental Security	SG.PE-1, SG.PE-2, SG.PE-3, SG.PE-4, SG.PE-5, SG.PE-6, SG.PE-7, SG.PE-8, SG.PE-9, SG.PE-10, SG.PE-11, SG.PE-12
Risk Management and Assessment	SG.PL-4, SG.PM-5, SG.RA-1, SG.RA-2, SG.RA-3, SG.RA-4, SG.RA-5
Security Awareness and Training	SG.AT-1, SG.AT-2, SG.AT-3, SG.AT-4, SG.AT-6, SG.AT-7
Security Operations	/
Security and Privacy Governance	SG.AT-5, SG.CA-3, SG.CA-5, SG.PM-1, SG.PM-2, SG.PM-3, SG.PM-4, SG.PM-6, SG.PM-8, SG.PL-5, SG.SI-1, SG.SI-5
System, Data, and Communication Protection	SG.SC-1, SG.SC-8, SG.SC-9, SG.SC-10, SG.SC-11, SG.SC-12, SG.SC-14, SG.SC-15, SG.SC-17, SG.SC-20, SG.SC-26
System and Services Acquisition	SG.SA-1, SG.SA-4, SG.SA-5, SG.SA-11
Vulnerability and Patch Management	SG.RA-6, SG.SI-2
Maintenance	SG.MA-1, SG.MA-2, SG.MA-3, SG.MA-4, SG.MA-5, SG.MA-6, SG.MA-7
Portable Device Security	/
Resource Management	SG.PL-1, SG.PM-7, SG.SA-3, SG.AU-12

As it is shown in Table 3, not every requirement originally classified into one domain necessarily belongs in that domain when a different approach for domain definition is introduced. Some of the requirements could be classified differently than represented in Table 3, but this would be driven by the knowledge base that security practitioners earlier developed. These results are expected since a similar conclusion was obtained in Section 3.2 during the initial analysis. None of the 197 requirements was left unclassified or forcibly classified into existing domains. Out of 19 domains, most of them (13) can have their requirements in major part mapped to one of 24 domains we introduced earlier in this paper. Information and Document Management (SG.ID) and Media Protection (SG.MP) are the two domains with most of the requirements mapped onto domain Data Handling. The same situation is with Access Control (SG.AC) and Identification and Authentication (SG.IA) that are mapped to the Identity Management and Access Control domain. Only six domains have their requirements dissipated to various domains: Planning (SG.PL), Security Assessment and Authorization (SG.CA), Security Program Management (SG.PM), Smart Grid Information System and Information Integrity (SG.SI), Smart Grid Information System and Communication Protection (SG.SC) and Smart Grid Information System and Services Acquisition (SG.SA). Out of 24 domains, 22 have at least one requirement assigned, while two—Security Operations and Portable Device Security—have none. Figure 5 summarizes the mapping from Table 3. From the charts we can conclude that NISTIR 7628 focuses on the same requirements as previously analyzed publications; thus, the initial domain scores defined in Table 2 stand in general, with the exceptions in Asset Management and Change Management that lack more requirements, and Maintenance domain that records the increased number due to dedicated domain in the original standard.

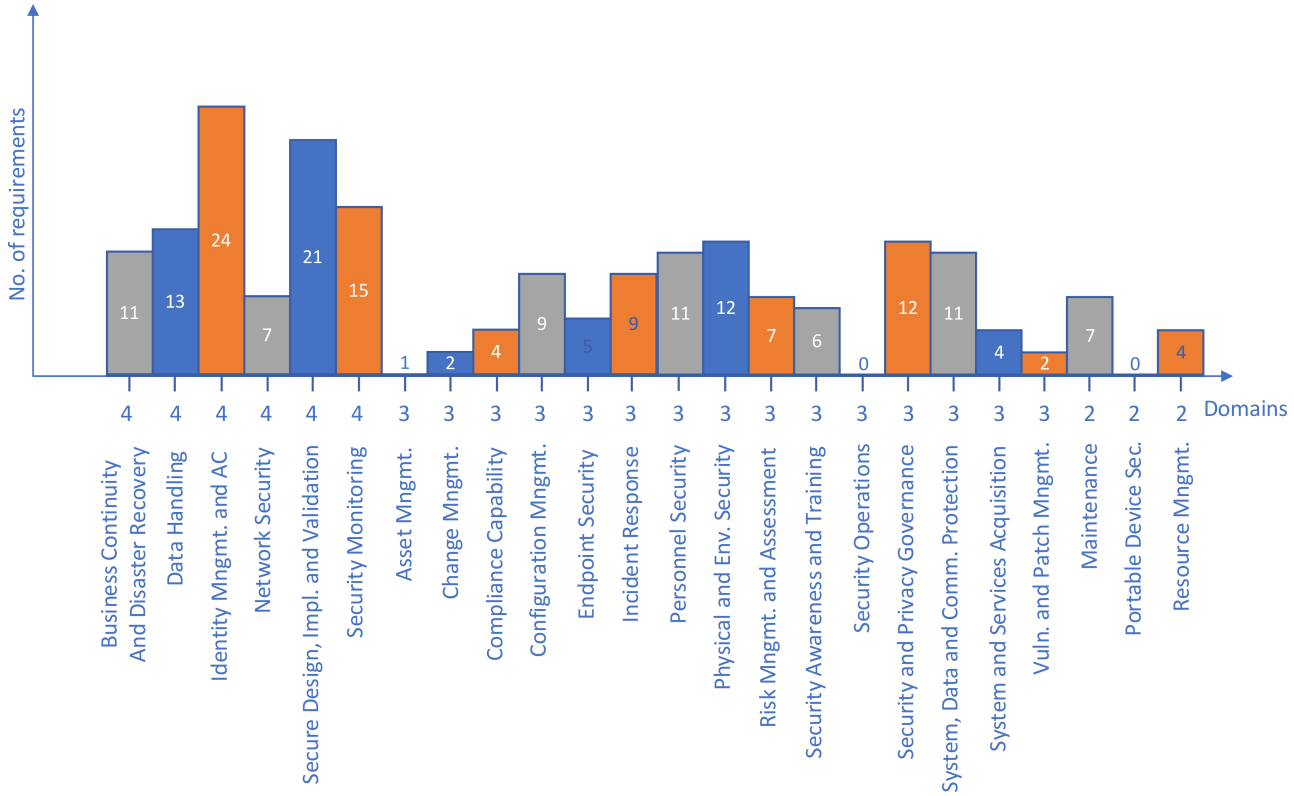


Figure 5. NISTIR 7628 requirements cumulative numbers per domain.

To visualize the requirements, the scenario in which the model can be used is defined. It is assumed that the large mature organization has its system already partially compliant with IEC 62443-3-3 and NIST SP 800-53 and wants to examine the readiness for compliance also with NISTIR 7628. Since compliance preparation for IEC 62443-3-3 and NIST SP

800-53 started earlier, actors, risks, and threats are already defined to some extent; thus, the compliance project for NISTIR 7628 has a head start.

NISTIR 7628 defines typical logical interface categories and diagrams of architectures used in production with sets of security requirements to help vendors and integrators during the design and development of security controls. For demonstration purposes, interface category 4 is chosen. It defines the interface between control systems and equipment without high availability and computational and/or bandwidth constraints such as SCADA systems. This interface category suggests the fulfillment of the following requirements: SG.AC-14, SG.IA-4, SG.IA-5, SG.IA-6, SG.SC-3, SG.SC-5, SG.SC-7, SG.SC-8, SG.SC-17, SG.SC-29 and SG.SI-7. As an example of the model usage, based on the activity diagrams presented in Figures 3 and 4, simplified information for the SG.IA-5 Device Identification and Authentication Enhancement 1 is provided in the form of one instance of a model in Figure 6. Here, the connection with similar requirements from relevant selected standards can also be found.

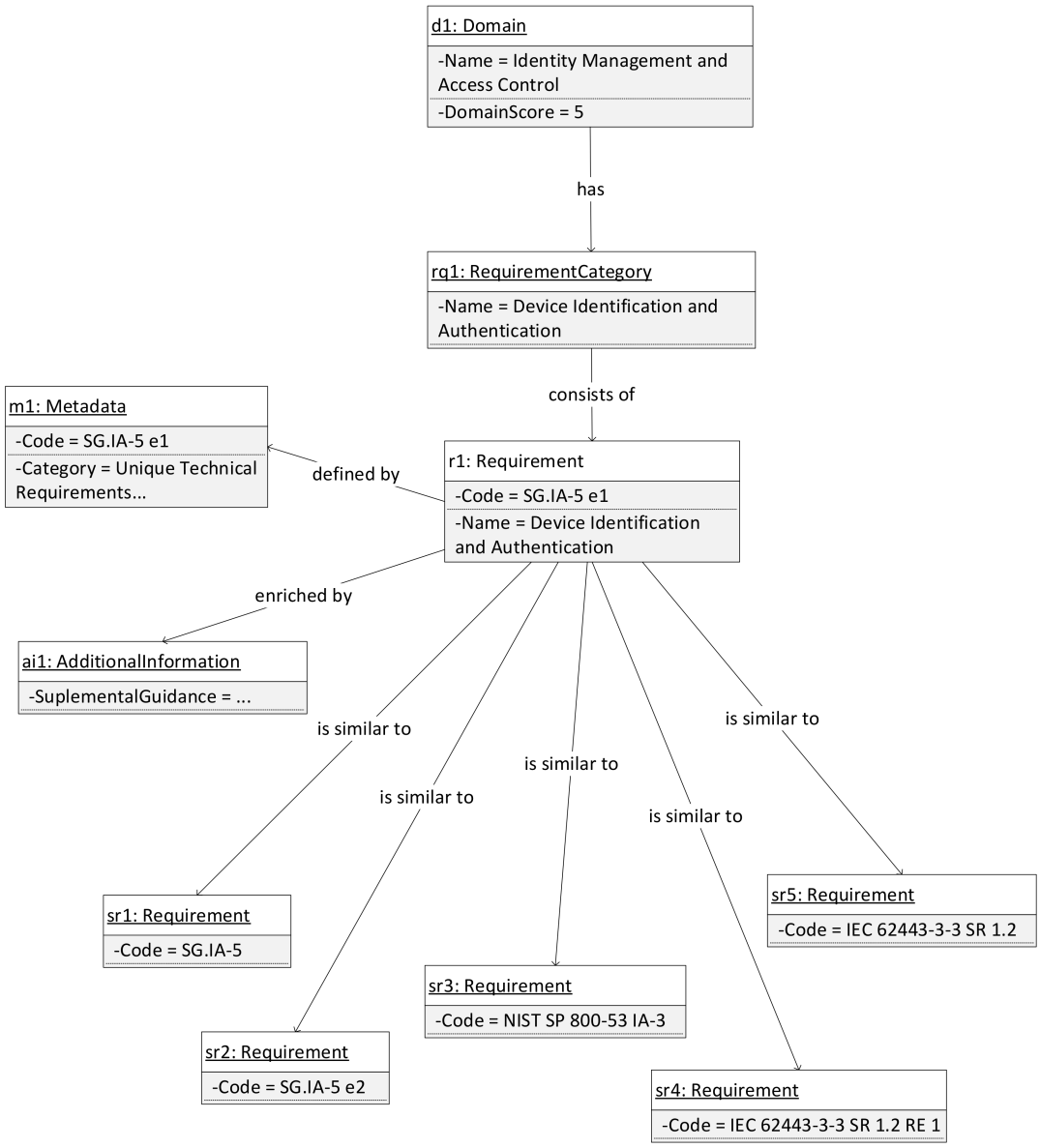


Figure 6. SG.IA-5 Device Identification and Authentication Enhancement 1 as a model instance.

For the initial population of the requested information based on the conceptual model, SG.IA-5 e1 requirement is given in Figure 7. For better readability, the number of assets

and risks in Figure 7 is reduced and simplified. Here, we have enough information to see what the goal of the exercise is, how it is measured, which assets and actors are involved, and their dependency chain, as well as associated risks. By repeating these steps for each requirement, using Formula (1) we can calculate the priority for requirement implementation.

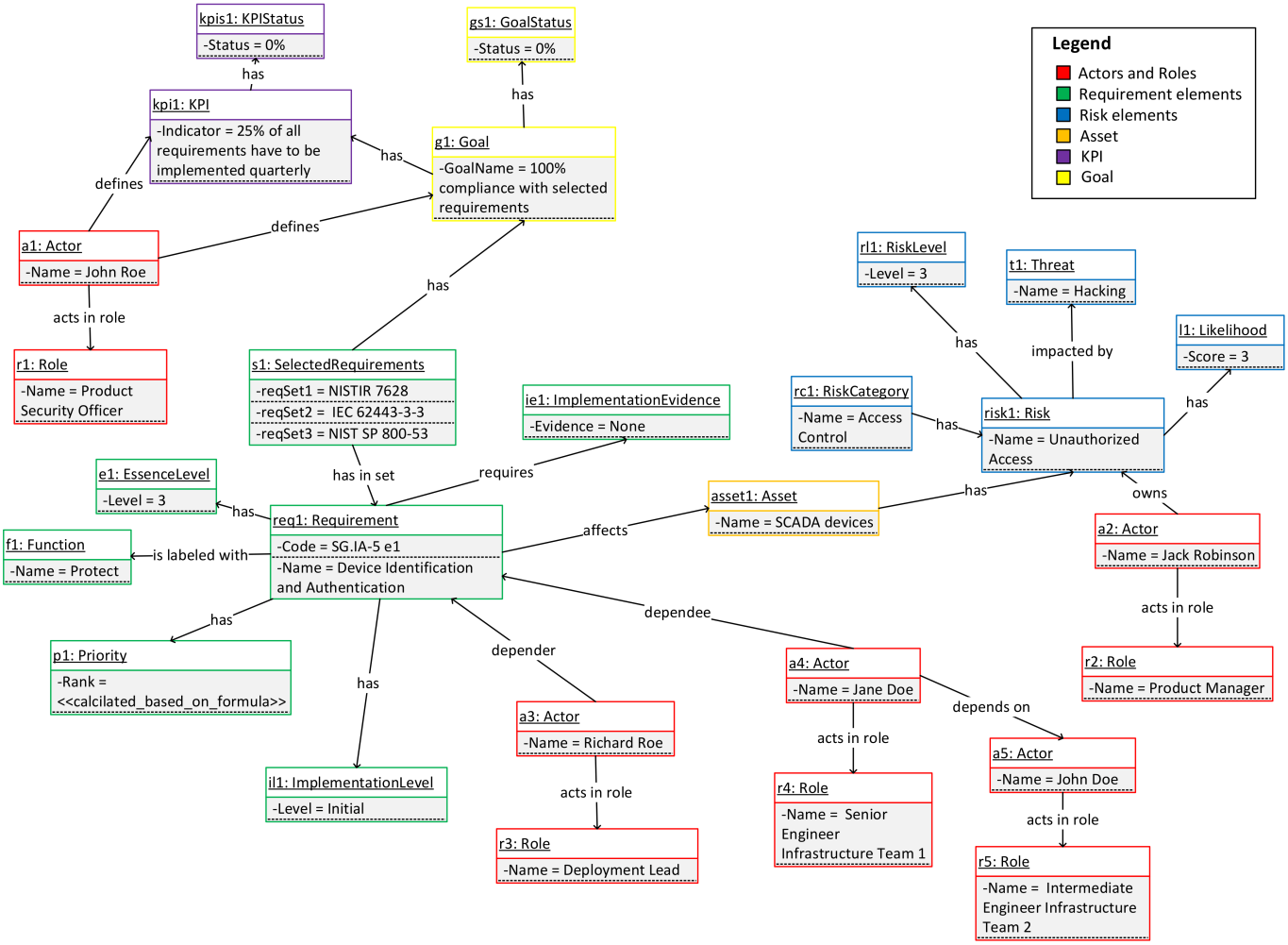


Figure 7. SG.IA-5 Enhancement 1—complete initial setup.

5. Discussion

In recent years, the security of critical infrastructure has become a priority topic all over the world. Ad hoc or partial security controls implementation is not sustainable anymore and a systematic approach is the only viable solution. In this security evolution, standardization brings the necessary value. The countries and standardization bodies form working groups to publish new, improved guidelines, directives, and standards to enforce better security. The organizations are consequently obligated to align with these standards, guidelines, and directives. The ever-increasing number of documents and constant need for compliance can be confusing and some sort of generalization that will present the summit for all of them is needed. Usually, the organizations are aligned with one standard, but an emerging number of new standards and especially guidelines and regulations applicable worldwide or only in a specific country dictate the need for alignment with more of them to demonstrate the readiness for growing the business. The requirements from different standards can usually be familiar and the construction of a model that can be the basis for every new standard is a good starting point for further automation. This was the main driver for our research. This also provides a unique template that can emphasize all the

similarities that different observed standards have. As a result, the cost of an alignment with the second and every next standard is greatly reduced since actors, threats, and risks are already familiar to a good extent.

This kind of model opens the doors for further development and improvement of existing processes in companies such as system security plans. To the best of our knowledge, the approach for model construction described in this paper that takes into consideration also the social actor aspect in the form of a dependency chain was not performed previously. Since the main actors that work on compliance preparations in companies are human individuals, this touch in the model can be beneficial for expressing the details about who and why have performed or not performed something to improve security posture. Further, the model is enriched with necessary components to make a connection with a risk assessment that is usually performed separately. This is performed in a form of the requirement prioritization criteria to allow usage of arbitrary risk assessment framework but also to put the emphasis on the requirement implementation rather than on a purely numeric estimation of risk. Having the requirements and associated risks more coupled can give more insights and better tracking of the implemented requirements and directly reduced or eliminated risks.

When we observe all entities that were described in previous sections, our interpretation of their purpose in the model gives us the framework—the prism or new point of view—for the requirement interpretation and enrichment with necessary information. All these components the model is composed of can provide a solid basis for requirement implementation tracking. With adequately defined KPIs, data extracted from model instances can provide sufficient information about the status of implementation such as the number or percentage of fulfilled requirements, their implementation priority, risks accepted or mitigated, and actors involved. In addition, the model is compatible with the OSCAL document format for requirements exchange, that is, even if it is in the early stage of development, projected to be de facto standard and thus the model can be ready for its early adoption. Applications built upon this model can use OSCAL documents as an exchange data format.

This approach, compared to others mentioned in previous sections, gives the users advantage of having one whole that enables the comparison of multiple standards at once, gives insights into the quantitative and qualitative nature of the requirement implementation through assurance model, and maintains the complexity of all involved social parties in form of a dependency chain. All individual components are based on the proven methods and further appropriately adjusted to fit the needs of the model.

One limitation can be loosely developed prioritization criteria. The main vector is focused on the risk assessment that has its drawbacks. Due to a vast number of proposed methodologies, the idea was to make a numeric estimation of risk that can impact enough the priority of the requirement implementation and help the security decision makers with the understanding of the current security posture of an organization or system and with the allocation of security funds to improve it. As the model is expandable and the risk register elements exist as entities that are the basis of every risk assessment, this can be further improved with a suitable methodology that will converge in the future.

Another limitation of the proposed solution is more oriented on the usage of the model through a defined framework than the model itself. Although 24 domains that were defined as a basis for the requirements classification are expandable, every new domain that is introduced afterward can potentially desynchronize the initial mappings of the requirements. For example, if the organization is heavily reliant on cloud technologies, introducing a new domain called cloud security would be a reasonable move. Consequently, this would require e.g., NIST 800-53 SA-9 External system services to transfer over from the asset management domain to the cloud security domain. This dynamic recalibration of the requirements classification by similarity without strong manual interference by the experts that are using this model as a basis requires expanding the requirements with new similarity factors that will help with the automation which is considered the future work.

6. Conclusions

In this paper, we propose the conceptual model for the representation and tracking of compliance with security requirements based on widely used security standards. The need for the model that will combine all relevant factors in implementing and tracking compliance on an organizational or system level comes from the analysis of different representations of security requirements. Product providers that serve in multiple regions have to demonstrate their security posture against more than one standard, guideline, or regulation whose requirements are defined on a different level of detail, especially when critical infrastructure is at stake. By introducing more than one set of requirements defined in different forms of publications can be a challenge to understand, track, and implement. Our model is constructed from the entities detected as relevant during the research that started with the analysis of security publications and gained its representation in the form of a UML class diagram at the end. Throughout the paper, we identified all the necessary entities, defined their roles, and in a way introduced a new domain-oriented view for the model usage. Although these entities are not new and a variety of solutions that tackle individual problems already exist, they are not observed from an organizational point of view, but more generally. We detected problems with existing solutions and gave our reasoning on how to tackle them jointly. The research clearly illustrates model creation and future usage, but also raises the question of dynamic recalibration in case of a requirements classification change. The model is validated on the NISTIR 7628 standard that was used as a control standard—it was not part of the set of standards used in research. The validation showed that an unknown set of requirements in advance can be mapped onto a model and be used in combination with other existing sets that belong to publications already in the knowledgebase. The model is expandable, giving the opportunity to adjust it if new constraints emerge. Based on these conclusions, the presented model could benefit security practitioners in different aspects of security requirements implementation.

Even if it is primarily focused on the smart grid, the model can be adjusted to other domains. Future work includes an analysis of the standards that apply to other CI sectors that require a high level of security such as financial services, nuclear reactors, water systems, or healthcare. In addition, future work will include building a prototype application and testing it on a case study in a company. This research is part of a series intended to improve critical infrastructure protection in various forms using conventional as well as modern approaches such as blockchain [71].

Author Contributions: Conceptualization, M.S., N.D. and G.S.; methodology, M.S.; validation, B.M. (Branko Markoski), B.M. (Branko Milosavljević) and G.S.; investigation, M.S.; resources, N.D., B.M. (Branko Markoski) and B.M. (Branko Milosavljević); writing—original draft preparation, M.S., N.D. and G.S.; writing—review and editing, B.M. (Branko Markoski), B.M. (Branko Milosavljević) and G.S.; visualization, M.S. and N.D.; supervision, B.M. (Branko Markoski), B.M. (Branko Milosavljević) and G.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing is not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Federation of American Scientists. President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures. 1997. Available online: https://fas.org/sgp/library/pccip.pdf (accessed on 2 August 2021).
2. Congress. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001. Available online: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf (accessed on 2 August 2021).
3. The White House President Barack Obama. Presidential Policy Directive (PPD-21): Critical Infrastructure Security and Resilience. Available online: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed on 2 August 2021).
4. Hua, H.; Wei, Z.; Qin, Y.; Wang, T.; Li, L.; Cao, J. Review of distributed control and optimization in energy internet: From traditional methods to artificial intelligence-based methods. *IET Cyber-Phys. Syst. Theory Appl.* **2021**, *6*, 63–79. [CrossRef]
5. Hua, H.; Qin, Z.; Dong, N.; Qin, Y.; Ye, M.; Wang, Z.; Chen, X.; Cao, J. Data-Driven Dynamical Control for Bottom-Up Energy Internet System. *IEEE Trans. Sustain. Energy* **2021**. [CrossRef]
6. National Institute of Standards and Technology (NIST). NIST SP 800-82 Rev.2 Guide to Industrial Control Systems (ICS) Security. Available online: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final (accessed on 3 August 2021).
7. Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control. Syst. Mag.* **2001**, *21*, 11–25. [CrossRef]
8. Centre for Risk Studies; University of Cambridge; Judge Business School. The Insurance Implications of a Cyber Attack on the US Power Grid. Available online: https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf (accessed on 2 August 2021).
9. Zhu, B.; Joseph, A.; Sastry, S. A Taxonomy of Cyber Attacks on SCADA Systems. In Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, Dalian, China, 19–22 October 2011; pp. 380–388. [CrossRef]
10. Williams, T.J. The Purdue Enterprise Reference Architecture. *Comput. Ind.* **1994**, *24*, 141–158. [CrossRef]
11. North American Electric Reliability Corporation (NERC). Frequently Asked Questions CIP Version 5 Standards Consolidated Comments Received Regarding May 1, 2015 Posting. Available online: https://www.nerc.com/pa/CI/tpv5impmntnstdy/CIPV5_FAQs_May_Posting_Consolidated_Comments_June_17_2015.pdf (accessed on 2 August 2021).
12. North American Electric Reliability Corporation (NERC). GridEx. Available online: https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx (accessed on 2 August 2021).
13. Cybersecurity & Infrastructure Security Agency. Cyber Storm: Securing Cyber Space. Available online: https://www.cisa.gov/cyber-storm-securing-cyber-space (accessed on 2 August 2021).
14. ISACA. 2019 Report: Annual ISACA/Protiviti Survey—Today's Toughest Challenges in IT Audit: Tech Partnerships, Talent, Transformation. Available online: https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpgl (accessed on 3 August 2021).
15. The Federation of German Industries (BDI). Cyber-Landscape I: Cyber Security Laws. Available online: https://web.archive.org/web/20210109145510/https://english.bdi.eu/article/news/cyber-security-laws/ (accessed on 9 January 2021).
16. EUR-Lex. Communication from the Commission on a European Programme for Critical Infrastructure Protection. Available online: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF (accessed on 3 August 2021).
17. Beckers, K.; Cote, I.; Fenz, S.; Hatebur, D.; Heisel, M. A Structured Comparison of Security Standards. In *Engineering Secure Future Internet Services and Systems, Lecture Notes in Computer Science*; Heisel, M., Joosen, W., Lopez, J., Martinelli, F., Eds.; Springer: Cham, Switzerland, 2014; Volume 8431, pp. 1–34. [CrossRef]
18. Hale, M.L.; Gamble, R.F. Semantic hierarchies for extracting, modeling, and connecting compliance requirements in information security control standards. *Requir. Eng.* **2019**, *24*, 365–402. [CrossRef]
19. Leszczyna, R. Standards on cyber security assessment of smart grid. *Int. J. Crit. Infrastruct. Prot.* **2018**, *22*, 70–89. [CrossRef]
20. Alcaraz, C.; Zeadally, S. Critical infrastructure protection: Requirements and challenges for the 21st century. *Int. J. Crit. Infrastruct. Prot.* **2015**, *8*, 53–66. [CrossRef]
21. Sommestad, T.; Ericsson, G.N.; Nordlander, J. SCADA system cyber security—A comparison of standards. In Proceedings of the IEEE PES General Meeting, Minneapolis, MN, USA, 25–29 July 2010; pp. 1–8. [CrossRef]
22. Hudaib, A.; Masadeh, R.; Haj Qasem, M.; Alzaqebah, A. Requirements Prioritization Techniques Comparison. *Mod. Appl. Sci.* **2018**, *12*, 2. [CrossRef]
23. Tariq, M.I.; Ahmed, S.; Memon, N.A.; Tayyaba, S.; Ashraf, M.W.; Nazir, M.; Hussain, A.; Balas, V.E.; Balas, M.M. Prioritization of Information Security Controls through Fuzzy AHP for Cloud Computing Networks and Wireless Sensor Networks. *Sensors* **2020**, *20*, 1310. [CrossRef] [PubMed]
24. Park, K.Y.; Yoo, S.G.; Kim, J. Security Requirements Prioritization Based on Threat Modeling and Valuation Graph. In *Communications in Computer and Information Science, Proceedings of the Convergence and Hybrid Information Technology, ICHIT 2011, Daejeon, Korea, 22–24 September 2011*; Lee, G., Howard, D., Ślęzak, D., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; Volume 206, pp. 142–152. [CrossRef]
25. Duan, C.; Laurent, P.; Cleland-Huang, J.; Kwiatkowski, C. Towards automated requirements prioritization and triage. *Requir. Eng.* **2009**, *14*, 73–89. [CrossRef]

26. National Institute of Standards and Technology (NIST). OSCAL: The Open Security Controls Assessment Language. Available online: https://pages.nist.gov/OSCAL/ (accessed on 3 August 2021).
27. Cybersecurity & Infrastructure Security Agency. The Cyber Security Evaluation Tool (CSET). Available online: https://us-cert.cisa.gov/ics/Downloading-and-Installing-CSET (accessed on 2 August 2021).
28. Lee, K.A. CS2SAT: The Control Systems Cyber Security Self-Assessment Tool. In Proceedings of the ISA EXPO 2007, Houston, TX, USA, 2–4 October 2007.
29. Cybersecurity & Infrastructure Security Agency. Cyber Resilience Review Self-Assessment Package (CRR). Available online: https://us-cert.cisa.gov/sites/default/files/c3vp/csc-crr-self-assessment-package.pdf (accessed on 2 August 2021).
30. Airports Council International. Cyber Self-Assessment Tool. Available online: https://aci.aero/about-aci/priorities/airport-it/cybersecurity/self-assessment-tool/ (accessed on 3 August 2021).
31. Center for Internet Security. CIS Controls Self Assessment Tool (CIS CSAT). Available online: https://www.cisecurity.org/controls/cis-controls-self-assessment-tool-cis-csat/ (accessed on 3 August 2021).
32. Barlette, Y.; Fomin, V.V. The Adoption of Information Security Management Standards: A Literature Review. In *Cyber-Security & Global Information Assurance: Threat, Analysis and Response Solutions*; Knapp, K.J., Ed.; IGI Global: New York, NY, USA, 2009; pp. 119–140. [CrossRef]
33. Leszczyna, R.; Fovino, I.N.; Masera, M. Approach to security assessment of critical infrastructures' information systems. *IET Inf. Secur.* **2011**, *5*, 135–144. [CrossRef]
34. Von Solms, R. Information security management: Why standards are important. *Inf. Manag. Comput. Secur.* **1999**, *7*, 50–58. [CrossRef]
35. Thome, A.M.T.; Scavarda, L.F.; Scavarda, A.J. Conducting systematic literature review in operations management. *Prod. Plan. Control.* **2016**, *27*, 408–420. [CrossRef]
36. Hunter, E.N. A Comparative Analysis of Cybersecurity Guidelines and Standards for Nuclear Power Plants. Master's Thesis, Department of Computer Science, Faculty of Information Technology, Tallinn University of Technology, Tallinn, Estonia, 2016.
37. Kuligowski, C. Comparison of IT Security Standards. Technical Report. Available online: https://web.archive.org/web/20161127054838/http://www.federalcybersecurity.org/CourseFiles/WhitePapers/ISOvNIST.pdf (accessed on 27 November 2016).
38. Gazis, V. A Survey of Standards for Machine-to-Machine and the Internet of Things. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 482–511. [CrossRef]
39. International Electrotechnical Commission (IEC). IEC 62443-3-3:2013 Industrial Communication Networks—Network and System Security—Part 3-3: System Security Requirements and Security Levels. Available online: https://webstore.iec.ch/publication/7033 (accessed on 2 August 2021).
40. ISO/IEC. *ISO/IEC 27001:2013: Information Technology Security Techniques Information Security Management Systems Requirements*; ISO: Geneva, Switzerland, 2013.
41. ISO/IEC. *ISO/IEC 27002:2013: Information Technology—Security Techniques—Code of Practice for Information Security Controls*; ISO: Geneva, Switzerland, 2013.
42. National Institute of Standards and Technology (NIST). NIST SP 800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations. Available online: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (accessed on 3 August 2021).
43. North American Electric Reliability Corporation (NERC). CIP Standards. Available online: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (accessed on 3 August 2021).
44. National Institute of Standards and Technology (NIST). NIST SP 800-53, Revision 5 Control Mappings to ISO/IEC 27001. Available online: https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/final/documents/sp800-53r5-to-iso-27001-mapping.docx (accessed on 3 August 2021).
45. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. Available online: https://www.nist.gov/cyberframework/framework (accessed on 3 August 2021).
46. National Cyber Security Framework. 2015 Italian Cyber Security Report a National Cyber Security Framework. Available online: https://www.cybersecurityframework.it/sites/default/files/CSR2015_ENG.pdf (accessed on 3 August 2021).
47. Alcaraz, C.; Zeadally, S. Critical Control System Protection in the 21st Century. *Computer* **2013**, *46*, 74–83. [CrossRef]
48. Cybersecurity & Infrastructure Security Agency. Catalog of Control Systems Security: Recommendations for Standards Developers. Available online: https://us-cert.cisa.gov/sites/default/files/documents/CatalogofRecommendationsVer7.pdf (accessed on 2 August 2021).
49. Sabillon, R.; Serra-Ruiz, J.; Cavaller, V.; Cano, J. A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM). In Proceedings of the 2017 International Conference on Information Systems and Computer Science (INCISCOS), Quito, Ecuador, 23–25 November 2017; pp. 253–259. [CrossRef]
50. Carias, J.F.; Borges, M.R.S.; Labaka, L.; Arrizabalaga, S.; Hernantes, J. The Order of the Factors DOES Alter the Product: Cyber Resilience Policies' Implementation Order. In *Advances in Intelligent Systems and Computing, Proccedings of the 13th International Conference on Computational Intelligence in Security for Information Systems, CISIS 2020, Burgos, Spain, 16–18 September 2020*; Herrero, A., Cambra, C., Urda, D., Sedano, J., Quintian, H., Corchado, E., Eds.; Springer: Cham, Switzerland, 2020; Volume 1267, pp. 306–315. [CrossRef]

51. Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification. Cybersecurity Maturity Model Certification (CMMC). Available online: https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf (accessed on 3 August 2021).
52. Cyber Defense Matrix. Available online: https://cyberdefensematrix.com/ (accessed on 3 August 2021).
53. Gilsinn, J.; Schierholz, R. Security Assurance Levels: A Vector Approach to Describing Security Requirements. Other, National Institute of Standards and Technology, Gaithersburg, MD, USA. 2010. Available online: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906330 (accessed on 3 August 2021).
54. Office of Cybersecurity, Energy Security, and Emergency Response. Cybersecurity Capability Maturity Model (C2M2). Available online: https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021_508.pdf (accessed on 3 August 2021).
55. Carnegie Mellon University. CMMI for Development, Version 1.3. Available online: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9661 (accessed on 3 August 2021).
56. Akinpelu, T.; van Eck, R.; Zuva, T. Maturity Models, Challenges and Open Issues. In *Software Engineering and Algorithms, CSOC 2021, Lecture Notes in Networks and Systems*; Silhavy, R., Ed.; Springer: Cham, Switzerland, 2021; Volume 230, pp. 110–118. [CrossRef]
57. Payne, S.C. A Guide to Security Metrics. SANS Institute. Available online: https://sansorg.egnyte.com/dl/kiYWJmz3vh/ (accessed on 3 August 2021).
58. Boehm, B.W. Software Engineering Economics. In *Pioneers and Their Contributions to Software Engineering*; Broy, M., Denert, E., Eds.; Springer: Berlin/Heidelberg, Germany, 2001; pp. 4–21. [CrossRef]
59. Yu, E. Modeling Strategic Relationships for Process Reengineering. Ph.D. Thesis, Department of Computer Science, University of Toronto, Ontario, ON, Canada, 1995.
60. Achimugu, P.; Selamat, A.; Ibrahim, R.; Mahrin, M.N. A systematic literature review of software requirements prioritization research. *Inf. Softw. Technol.* **2014**, *56*, 568–585. [CrossRef]
61. European Commission. Risk Assessment Methodologies for Critical Infrastructure Protection. Part I: A State of the Art. Available online: https://publications.jrc.ec.europa.eu/repository/handle/JRC70046 (accessed on 3 August 2021).
62. Cherdantseva, Y.; Burnap, P.; Blyth, A.; Eden, P.; Jones, K.; Soulsby, H.; Stoddart, K. A review of cyber security risk assessment methods for SCADA systems. *Comput. Secur.* **2016**, *56*, 1–27. [CrossRef]
63. Tweneboah-Koduah, S.; Buchanan, W.J. Security Risk Assessment of Critical Infrastructure Systems: A Comparative Study. *Comput. J.* **2018**, *61*, 1389–1406. [CrossRef]
64. Cox, L.A.T.J. Some Limitations of "Risk = Threat × Vulnerability × Consequence" for Risk Analysis of Terrorist Attacks. *Risk Anal.* **2008**, *28*, 1749–1761. [CrossRef] [PubMed]
65. National Institute of Standards and Technology (NIST). NIST 800-160 Vol. 1 Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. Available online: https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final (accessed on 3 August 2021).
66. Fine, W.T. Mathematical Evaluation for Controlling Hazards. *J. Saf. Res.* **1971**, *3*, 157–166.
67. National Institute of Standards and Technology (NIST). NIST 800-30 Rev. 1 Guide for Conducting Risk Assessments. Available online: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (accessed on 3 August 2021).
68. Joh, H.; Malaiya, Y.K. A Framework for Software Security Risk Evaluation Using the Vulnerability Lifecycle and CVSS Metrics. In Proceedings of the International Workshop on Risk and Trust in Extended Enterprises, San Jose, CA, USA, 1–4 November 2010; pp. 430–434.
69. ISO/IEC. *ISO/IEC 27005:2018: Information Technology Security Techniques Information Security Risk Management*; ISO: Geneva, Switzerland, 2018.
70. National Institute of Standards and Technology (NIST). NIST 7628 Rev.1 Guidelines for Smart Grid Cybersecurity. Available online: https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final (accessed on 3 August 2021).
71. Marjanovic, J.; Dalcekovic, N.; Sladic, G. Improving Critical Infrastructure Protection by Enhancing Software Acquisition Process Through Blockchain. In Proceedings of the 7th Conference on the Engineering of Computer Based Systems, Novi Sad, Serbia, 26–27 May 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 1–7. [CrossRef]