Received 26 June 2024; revised 31 July 2024; accepted 6 August 2024. Date of publication 9 August 2024;
date of current version 23 August 2024. The review of this article was arranged by Associate Editor Maria-Laura Caliusco.

Digital Object Identifier 10.1109/OJIES.2024.3441112

A Survey of Ontologies Considering General Safety, Security, and Operation Aspects in OT

SIEGFRIED HOLLERER [1], THILO SAUTER [2,3] (Fellow, IEEE), AND WOLFGANG KASTNER [1] (Senior Member, IEEE)

[1]Institute of Computer Engineering, TU Wien, 1040 Vienna, Austria
[2]Institute of Computer Technology, TU Wien, Vienna, Austria
[3]Institute of Integrated Sensor Systems, Danube University Krems, 3500 Krems an der Donau, Austria

CORRESPONDING AUTHOR: SIEGFRIED HOLLERER (e-mail: siegfried.hollerer@tuwien.ac.at)

This work was supported in part by the TÜV Austria #SafeSecLab Research Laboratory for Safety and Security in Industry, a research cooperation between the Technical University of Vienna (TU Wien) and TÜV AUSTRIA and in part by the TU Wien Bibliothek through its Open Access Funding Program.
Data is available online at https://github.com/SiegfriedHollerer/2024_OntologySMS_Dataset.

ABSTRACT The integration of information technology (IT) and operational technology (OT) is deepening, amplifying the interconnectedness of operational, safety, and security demands within industrial automation systems. Lacking comprehensive guidance, risk managers often resort to manual solutions based on best practices or rely on domain experts, who usually offer insights limited to their specific areas of expertise. Given the intricate interplay among these domains, employing ontologies for knowledge representation could hold the key to capturing all necessary relationships and constraints for effective risk management processes. This study conducts a systematic mapping analysis of ontologies published over the past five years, focusing on at least one domain relevant to OT system risk management. Its objective is to categorize papers, offer a panoramic view of research themes and contributors, discern potential publication patterns, and identify research avenues based on a comprehensive review of these ontologies. Findings indicate a relatively stable research interest, with most publications presenting proof of concepts or initial experimental results for their ontological applications. This study establishes a foundation for classifying comprehensive OT ontologies and pinpoints unresolved issues that can steer future research efforts. It offers insights into the current state-of-the-art within this research area.

INDEX TERMS Information technology/operational technology (IT/OT) convergence, OT security, risk management, safety, threat modeling.

I. INTRODUCTION

The increasing integration of information technology (IT) and operational technology (OT) in industrial automation presents a significant challenge, as it requires meeting diverse operational, quality, safety, and security requirements. Historically, IT and OT operated independently. IT encompasses office networks, enterprise systems, and software managing data from OT systems, while OT includes industrial communication systems, hardware, and software controlling and monitoring machine processes. The term OT encompasses a spectrum of industrial application domains, including manufacturing, aviation, automotive, building automation, process automation, public transport, and Internet of Things (IoT), within the scope of this research. Combining these OT elements forms an OT system composed of various OT components, owned by asset owners of such systems [1].

The security aspect, derived from the IT domain, prioritizes protecting data confidentiality, integrity, and availability (known as the CIA triad) against cyber threats [2]. Conversely, safety, derived from the OT domain, focuses on preventing harm to people and the environment caused by undesirable operations. Neglecting security jeopardizes safety, as cyber attacks can exploit the interdependence of safety and security, resulting in safety impacts.

In the OT domain, the CIA triad's prioritization differs due to the emphasis on availability and integrity during operation. Consequently, OT prioritizes availability, integrity, and confidentiality (AIC) in descending order, contrasting with IT's prioritization of CIA [3]. Therefore, security measures from IT cannot be directly applied to OT, requiring risk managers to select and implement security controls tailored to their OT system's operational needs [4], [5].

Ontologies offer a solution to this challenge by providing explicit and formal specifications of real-world concepts, interpretable by both humans and machines [6]. Semantic web languages, such as the web ontology language (OWL), facilitate knowledge representation and automated reasoning. Description Logicss (DLss), the foundation of OWL, enable the modeling of domain terminology, concepts, and roles, aiding in logical inference and decision-making. A concept is a set of individuals sharing common properties, and a role defines the relation between two individuals. For instance, in the domain *OT domain-specific model* relations, several DLs concepts may be defined, including *hardware*, and *software*, where multiple *software* individuals may be installed on one *hardware* individual [7]. To identify suitable ontologies considering safety, security, and operation aspects in OT, a literature review was conducted, analyzing scientific publications to classify relevant contributions addressing ontologies concerning security, safety, operational requirements, and their interdependencies in OT. This study aims to generate new knowledge, identify ontology characteristics, and guide ontology development to meet the interdisciplinary needs of risk managers in industry.

The study's goal is to present an overview of state-of-the-art ontologies concerning safety, security, and operational requirements in OT over the past five years. It also identifies open issues and discusses future research directions. The results and derived research directions are relevant to both research and industry stakeholders, serving as a reference for further studies and facilitating knowledge transfer between the academia and the industry [8], [9].

The rest of this article is organized as follows. Section II discusses background information and related work. Section III presents the chosen research method, the defined research questions, and the process of executing this study. Section IV describes and analyses the obtained results while visualizing them in several figures. Section V discusses potential threats to the validity of this work and undertaken mitigation strategies against them. Finally, Section VI concludes this article and points out research directions. The list of all publications analyzed in this mapping study is appended.

II. BACKGROUND

The systematic literature reviews (SLRs) stands as a well-established and extensively utilized methodology for impartially and replicably identifying, analyzing, and interpreting evidence [10]. This study employs a broader variant of SLRs, known as systematic mapping studies (SMSes) [8], [9], [11].

Achieving security by design proves particularly challenging, notably within the OT domain. A recent investigation [12] underscores the necessity of an information model encompassing security and automation engineering workflows as a stride toward security by design in OT. This study's resultant model facilitates security assessments for delineating security risks, requisites, and remedies. It can be leveraged for modeling data transmission between security-centric planning tools, change management, automated conflict resolution, and operational consistency checks. While promising for addressing production and security concerns in OT systems, this approach overlooks safety and its potential intersections with security.

The OT domain entails various standards worthy of consideration. A review of pertinent technological standards [13] was conducted, delineating diverse areas essential for OT system operation. Table I, adapted from [13], enumerates these standards organized by their respective application domains. The review also encompasses relevant security standards (e.g., IEC 62243 [14]), safety standards (e.g., IEC 61508 [15]), and production standards (e.g., IEC 61512 [16]), as integral components of the entire OT system. In addition, recent technologies such as Asset Administration Shell (AAS) published in IEC 63278 [17], and Reference Architectural Model Industrie 4.0 (RAMI4.0) published in DIN SPEC 91345 [18] alongside its substandards such as DIN SPEC 16593-1 [19], are included. Relevant NIST standards [20], [21] and the NAMUR open architecture concept [22] are also incorporated in Table I.

Ehrlich et al. [23] delved into exploring the alignment and potential automation of safety and security risk assessment processes in OT. The authors argue that the current methodology for risk assessment lacks the flexibility to adequately address emerging developments. Presently, there is a significant manual involvement from domain experts, leading to high costs, especially given the need for flexibility in Industry 4.0 (I4.0) applications such as Plug and Produce. To address this issue, the authors propose an information modeling scheme that incorporates safety and security aspects to facilitate risk assessments. However, it is worth noting that this scheme does not consider the technical processes or products generated by the OT system.

Formalizing security knowledge may be achieved through various ontologies, encompassing general security [6], enterprise IT-related aspects [24], and OT-related aspects [25]. The use of existing query languages, such as SPARQL Protocol And RDF Query Language (SPARQL) enables the processing of queries within these ontologies, effectively addressing security concerns in both OT and enterprise IT domains [24], [25].

Safety knowledge may be articulated through multiple hazard identification methodologies, including failure modes, effects, and criticality analysis (FMECA) as outlined in the standard IEC 60812 [26]. This approach not only identifies potential system failures but also pinpoints their causes, effects, severity, and recommended preventive or mitigative measures.

A comprehensive understanding of safety, security, and operational domains is essential for making informed decisions [4]. The holistic perspective depicted in Fig. 1 enables

TABLE 1. Overview of Applicable Standards Based on [13]

Smart connection	Data-to-information conversion	Cyber computation	Cognition	Configuration
ISO/IEC 15459	IEC/ISO 13236	ISO/IEC 8802	ISO 13374	IEC 61508
ISO/IEC 19762	ISO/IEC 27000 family	ISO/IEC 14476	IEC 62453	IEC 61512
ISO/IEC/IEEE 21450	IEC 61360	ISO/IEC 17826		IEC 62264
ISO/IEC/IEEE 21451	IEC 61804	ISO/IEC 20005		DIN SPEC 91345
IEC 61131	IEC 62443 family	IEC 61158		DIN SPEC 16593-1
IEC 61499	IEC 62714	IEC 61784		
	IEC 63278 family	IEC 62769		
	NAMUR NE 175	ISO/IEC 30101		
	NIST 800-53	ISO/IEC 30128		
	NIST SP 800-82			

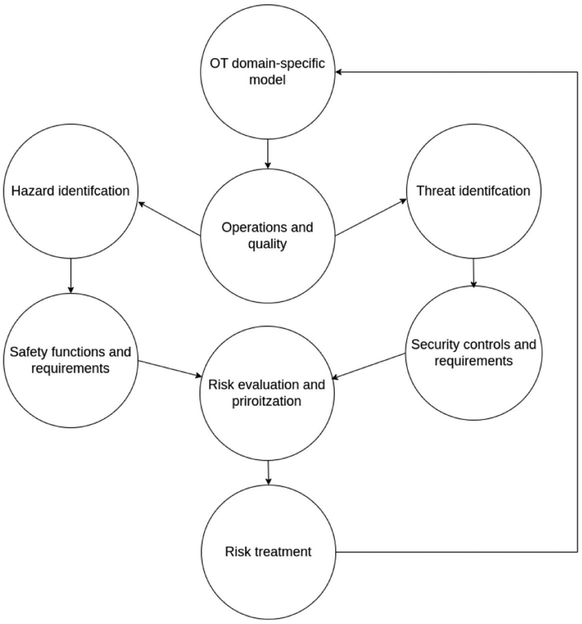

FIGURE 1. Domains needed for a holistic view [5].

asset owners of OT systems to navigate interdependencies between domains systematically, enhancing decision-making processes beyond isolated viewpoints.

An OT domain-specific model is essential for delineating the fundamental attributes and interconnections within an OT system [5]. The operational aspects and quality outcomes are integral facets, representing the technical processes and resultant products stemming from the OT system's operations. Depending on how the OT system is instantiated in operations and quality, distinct hazards and threats may manifest within it. Identifying these threats through threat identification mechanisms is crucial, with subsequent implementation of specific security controls mandated to fulfill security requisites, such as those outlined in IEC 62443 [14]. These threats may target elements intrinsic to the OT system or potentially impact the operational quality of manufactured products [1].

Furthermore, the process of threat identification may necessitate the implementation of additional security controls to mitigate the identified threats. Hazards may also emerge based on the OT system's configuration. For instance, if the OT system utilizes explosive gases in its technical processes, malfunctions may lead to injuries [1].

Similarly, akin to the security domain, safety functions must be integrated based on hazard identification to meet safety standards, such as those specified in IEC 61508 [15]. For example, at the component level, safety functions, such as light barriers can halt OT components when activated, ensuring safety. Different standards, such as IEC 61511 [27] for the process industry sector, dictate safety considerations based on the implemented technical processes [4].

The integration of safety functions and security controls, as dictated by the OT domain-specific model, may lead to conflicts in requirements. For instance, while ISO 13850 [28] mandates the constant availability of the emergency stop function, implementing authentication mechanisms, as required by IEC 62443-3-3 [29], might introduce delays in accessing critical functions [1]. Resolving such conflicts necessitates prioritizing safety over security or vice versa, or sometimes neglecting certain requirements altogether, potentially resulting in countermeasures that violate other requisites [4].

Moreover, the assessment and prioritization of risks, coupled with risk treatment strategies, play pivotal roles in addressing conflicts and ensuring cost-effective decision-making for asset owners [1]. Understanding the interplay between safety and security—ranging from antagonism to mutual reinforcement, conditional dependencies, or even independencies—is crucial for a comprehensive risk evaluation [23].

Ultimately, risk treatment strategies must align with the nature of risks and the stipulated safety and security requirements, precluding asset owners from accepting risks deemed likely to occur with severe consequences [30].

By integrating OT and IT, a system is created that must simultaneously meet safety and security standards. Changes in physical behavior can lead to changes in the system's state, and conversely, changes in the system can alter physical behavior. Therefore, safety and security are intrinsically linked within OT systems. In addition, the incorporation of more OT components increases the number of systems requiring updates. This contradicts the fundamental principle of easy and rapid integration into a reliable OT system, as these independently deployed updates can introduce uncertainties. The convergence of OT and IT blurs the line between the two, making both safety and security crucial in implementation.

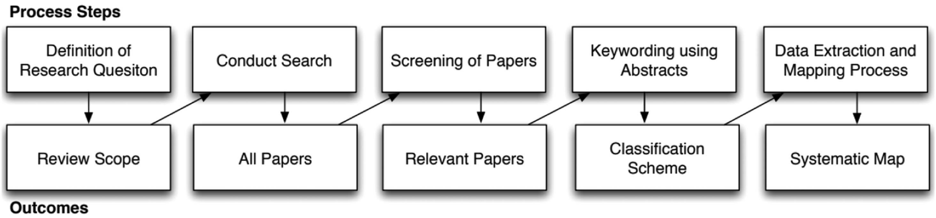

FIGURE 2. Systematic mapping process [33].

This new scenario could potentially introduce new risks that must be mitigated. Importantly, a safe system does not inherently ensure the safety of the entire application. Given the intertwined nature of safety and security, security must be considered from the outset, as their interaction can create new hazards in the face of cyber attacks [31].

The use of ontologies for knowledge representation addresses this problem effectively. Ontologies provide an explicit and formal specification of a conceptualization of a real-world domain, interpretable by both humans and machines [6]. Semantic web languages, designed to imbue web resources with machine-understandable meaning, leverage tools from artificial intelligence, such as rules and ontologies. These languages have been successfully applied across various fields, including industrial engineering [32]. A notable semantic web language is OWL, based on DLss, which offers machine-interpretable semantics grounded in classical first-order logic [7], [32]. Consequently, the reasoning mechanisms employed by DLss models are deterministic, ensuring consistent results with each execution.

III. METHODOLOGY

An SMSes was used as the research method to identify suitable ontologies that may provide or help to achieve a comprehensive operations, security, and safety view. This SMSes allows to cover and classify publications in a specific research area. This study focuses on the publications addressing ontologies considering at least one domain introduced in Fig. 1 and that were published between January 2019 and December 2023 to include only the most recent developments. This SMSes was performed from January 2024 until May 2024. The process for executing this SMSes is illustrated at Fig. 2.

The SMSes process [33] started with the definition of research questions. The result of this process phase were suitable research questions that define the scope of the review. Afterward, a literature search was conducted which results in providing all publications related to the defined review scope in the former process phase. Next, the obtained publications were screened to sort out irrelevant publications. The remaining publications passing the screening were analyzed and suitable keywords were derived from the abstracts that reflect the contribution of the corresponding publication, as Fig. 3 illustrates.

Keywording occurred in two stages as outlined in [33]. Initially, the authors examined abstracts to identify keywords

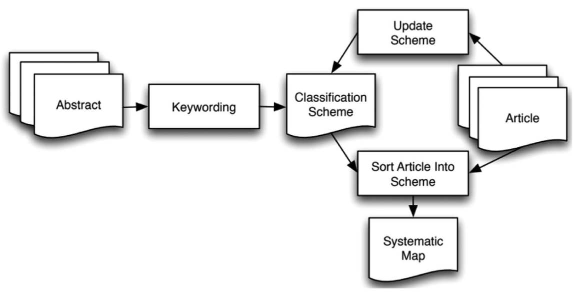

FIGURE 3. Building the classification scheme [33].

and concepts that represent the paper's contribution, simultaneously discerning the research context. Subsequently, the amalgamated keywords from various papers facilitated the development of a comprehension of the research's essence and contribution. This step aided in devising a set of categories reflective of the underlying population. If the abstracts were not suitable for deriving meaningful keywords, the introduction and conclusion were also used as a source for keyword generation. Once the definitive set of keywords was determined, they were clustered and employed to establish categories for the systematic map.

The output of this process phase was classified publications that are mapped systematically according to the research questions defined initially in this process.

A. DEFINITION OF RESEARCH QUESTIONS

The following research questions were defined to specify the scope of this mapping study.

1) *RQ1: Which publications addressing ontologies considering safety, security, and operation requirements in OT exist, and what are their bibliometric key facts?*
    a) Answering this research question should provide the number of relevant publications in the publication period from 2019 to 2023, their types (e.g., conference paper, journal paper, book chapter), and the used venues for publication.
2) *RQ2: Which scientific communities and main contributors research ontologies considering safety, security, and operation requirements?*
    a) This research question aims to identify and examine scientific communities working on ontologies

TABLE 2. Research Type Facets Based on [9], [33], [35]

Category	Description	Evaluation criteria
Validation Research	Techniques investigated are novel and have not yet been implemented in practice. Techniques used are, for example, experiments, i.e., work done in the laboratory.	Is the technique to be validated clearly described? Are the causal or logical properties of the technique clearly stated? Is the research method sound? Is the knowledge claim validated (i.e., is the conclusion supported by the paper) Is it clear under which circumstances the technique has the stated properties? Is this a significant increase in knowledge about this technique? Is there sufficient discussion of related work?
Evaluation Research	Techniques are implemented in practice, and an evaluation of the technique is conducted. That means, it is shown how the technique is implemented in practice (solution implementation) and what are the consequences of the implementation in terms of benefits and drawbacks (implementation evaluation). This also includes to identify problems in industry.	Is the problem clearly stated? Are the causal or logical properties of the problem clearly stated? Is the research method sound? Is the knowledge claim validated? Is this a significant increase of knowledge of these situations? Is there sufficient discussion of related work?
Solution Proposal	A solution for a problem is proposed; the solution can be either novel or a significant extension of an existing technique. The potential benefits and the applicability of the solution are shown by a small example or a good line of argumentation.	Is the problem to be solved by the technique clearly explained? Is the technique novel, or is the application of the techniques to this kind of problem novel? Is the technique sufficiently well described so that the author or others can validate it in later research? Is the technique sound? Is the broader relevance of this novel technique argued? Is there sufficient discussion of related work?
Philosophical Papers	These papers sketch a new way of looking at existing things by structuring the field in form of a taxonomy or conceptual framework.	Is the conceptual framework original? Is it sound? Is the framework insightful?
Opinion Papers	These papers express the personal opinion of somebody whether a certain technique is good or bad, or how things should been done. They do not rely on related work and research methodologies.	Is the stated position sound? Is the opinion surprising? Is it likely to provoke discussion?
Experience Papers	Experience papers explain on what and how something has been done in practice. It has to be the personal experience of the author.	Is the experience original? Is the report about it sound? Is the report revealing? Is the report relevant for practitioners?

considering safety, security, and operation requirements. This includes, for instance, ontologies defining OT-specific characteristics and relations, terms or means for threat or hazard identification or mitigation, or risk management in OT. Furthermore, this question identifies which authors or research groups are working on topics relevant to this study. The amount of citations of each publication is considered and serves as an indicator, if the corresponding community may be relevant. Moreover, this analysis may show if there is a network working on ontologies considering safety, security, and operation requirements.

3) *RQ3: In which category of research type facets are the resulting publications assigned?*
    a) The aim of this research question is to categorize the resulting publications according to a state-of-the-art schema [9], [34], [35]. To achieve this goal, the research type facets [33] listed in Table II are used. The alignment of the publications to the type facets provides insight into which research contexts ontologies considering safety, security, and operation requirements are used, for instance, evaluation, or (semi)automatization.

4) *RQ4: Which ontology domains are typically considered together?*
    a) In order to obtain a comprehensive ontology considering safety, security, and option requirements in OT, all relevant domains (cf. Fig. 1) have to be considered. This research question aims to identify which domains are typically considered together and which ones are typically viewed as isolated. Furthermore, the consideration of the standards mentioned in Table I is addressed by this research question.

B. CONDUCT SEARCH AND SCREENING OF PAPERS

The initial step of the SMSes process, following the establishment of research questions, involves pinpointing appropriate keywords to identify all relevant publications within the defined scope [9]. This search was conducted across three digital libraries chosen for their relevance to computer science and software engineering since they are referred to as key electronic databases [36].

TABLE 3. Conducting Search and Screening of Papers Based on [9], [33]

Step	Execution
Definition of keywords	Safety Ontology Security Ontology Process quality ontology OT ontology Product quality ontology Hazard identification ontology Threat identification ontology Manufacturing ontology Industrial process ontology
Sources for the search	Scopus[1] ACM Digital Library[2] IEEE Xplore Digital Library[3]
Limitation criteria	Published from January 2019 to December 2023 Search string restricted to publication title

Initially, the search yielded over 4000 papers, prompting a need for refinement to focus on recent comprehensive ontologies in ontology engineering in OT. Thus, to obtain more precise results reflecting the current state-of-the-art, the search parameters were constrained. Specifically, the search was limited to publications from January 2019 onward to capture the latest five years of research activity. In addition, the query was restricted to titles only, excluding publications that merely mentioned comprehensive ontologies in OT without substantial relevance. Consequently, only publications explicitly addressing comprehensive ontologies in OT were included in the analysis.

The refinement process was iterative, involving multiple updates to ensure a comprehensive collection of relevant publications that addressed the research questions. The final review of the result set was conducted on 13 May 2024.

Table III lists each step and its execution of the performed search and screening of publications.

C. SCREENING OF PUBLICATIONS

The exclusion criteria employed for screening publications based on [9] are outlined in Table IV. These criteria were applied to analyze all extracted publications. Following this screening process, a total of 207 publications were identified. The citation count for each publication, sourced from Google Scholar,[4] was taken into account. The comprehensive list of screened publications can be found in the appendix titled *SYSTEMATIC MAPPING STUDY REFERENCES*.

D. CLASSIFICATION

The papers were classified by applying adaptive reading depth [33], which analyzes the abstracts of a paper first. If the information provided in the abstract is sufficient for classification, the classification is done accordingly. If the abstract lacks important information for classification, other parts of the paper, e.g., conclusion and methodology, were also analyzed. If all parts of the papers were examined and still no classification was clearly possible, the authors discussed about the paper and the most experienced author in the corresponding area decided the classification ultimately. If the ontology described in the corresponding paper was available, we analyzed this ontology as well, regardless of the results of applying adaptive reading depth. Research type facets, detailed in Table II, were assigned based on the corresponding evaluation criteria [35] to each publication to gain a deeper understanding of their research context.

Using these research type facets as a classification schema during the SMSes phase to categorize the selected publications deviates from the original mapping process. Consequently, the process of keywording using abstracts (cf. Fig. 2) was adjusted since an established classification schema is already in use. This adaptation of the original SMSes methodology [8] has also been observed in other literature reviews [9].

In addition to mapping abstracts to research type facets, another crucial task is identifying the domains typically addressed by comprehensive ontologies in ontology engineering to ensure a holistic view (cf. Fig. 1). This helps to reveal trends in how domains are typically considered together or viewed in isolation. Table V sums up all tools used to perform these SMSes.

TABLE 4. Screening of Publications Via Exclusion Criteria Based on [9], [33]

Exclusion criteria	Description
Duplicates	A duplicate occurred when the same result was provided by different search engines.
Papers without matching abstract	For example, results focus on ontology optimization or evaluation which does not consider any of the domains illustrated in FIGURE 1.
Papers without an English or German abstract	These papers were excluded due to the author's language skills.
Papers with similar abstracts	Some publications demonstrate different development states of the very same project and ontology. These publications share a similar or slightly adapted abstract. In these cases, the most recent publication was included in the result set.
Papers with the very same abstracts	The unscreened result set contained publications with identical abstracts that were published at different venues, journals, or book chapters. In such cases, the corresponding publications were treated as duplicates and, therefore, only considered once.
Books	Books were not included in the screened result list of relevant publications since they are not necessarily peer-reviewed.
Theses	Theses consist of at least partly already published content, that would lead to duplicated if considered in the screened result set. Furthermore, the underlying project described by the corresponding thesis fits multiple type facets [9], [33].

TABLE 5. Tools Used to Perform This SMSes

Tool	Usage	Reference
Scopus	Search	https://www.scopus.com
ACM DL	Search	https://dl.acm.org
IEEE Xplore	Search	https://ieeexplore.ieee.org/Xplore/home.jsp
Google Scholar	Get Citations	https://scholar.google.com
Tag Crowd	Keyword cloud	http://tagcrowd.com

[4][Online]. Available: https://scholar.google.com/

IV. MAPPING OF PAPERS

This section discusses a use case derived from a stakeholder analysis [4] as a basis for conducting these SMSes. Furthermore, this section describes the answer to each of the defined research questions in Section III-A. The listed answers show the last output of the conducted SMSes.

A. USE CASE

Vendors supplying OT components, system integrators, and industrial asset owners collaborated on a stakeholder analysis to derive the chosen use case [4]. This analysis illuminates shared characteristics and application practices within OT environments from each stakeholder's perspective in the supply chain. Safety, security, and process operation experts from each of the participated stakeholders provided their views and experienced challenges to enable a holistic perception of an OT system. Furthermore, the provided insights from each stakeholder based on their discipline enabled the identification of interdependencies between safety, security, and operation requirements and characteristics. For instance, one stakeholder drew attention to the fact that an incident was introduced through a software update. The participant postulated that a significant proportion of safety-related issues are attributable to human error, e.g., individuals tend to underestimate the potential risks due to the presence of a backup system. After an incident, the backup was restored, resulting in an alert for missing data due to the age of the backup. Another stakeholder recognized the inherent risks associated with the interdependence between security and safety, citing an experience where a security incident could have potentially impacted safety. Nevertheless, the domains of safety, security, and operations are often regarded as distinct, largely due to the absence of dedicated organizational roles and responsibilities that encompass both the protection objectives and their interdependence [4].

Fig. 4 presents a derived use case from this collaborative effort that includes, besides its typical structure of an OT system, the existence of the discussed interdependencies between safety, security, and operation requirements. Safety-relevant OT components are highlighted with a red square, while security-relevant OT components are marked with a blue square, and operations-relevant OT components have a green square assigned to indicate the interdependencies of the corresponding requirements. The structure of this use case aligns with the Purdue Enterprise Reference Architecture (PERA) [14]. Since traditional office IT falls outside the scope of IEC 62443, the management level associated with it was not considered during the risk assessment of this particular use case. This use case contains commonly used OT components and their network connections of an OT system. Due to the IT/OT convergence, an OT system may consist also of IT elements, e.g., a domain controller at the supervisory level to implement central identity management, or a supervisory control and data acquisition (SCADA) server running on a Microsoft Windows-based operating system.

B. RQ1: BIBLIOMETRICS OF RELEVANT PUBLICATIONS

Initially, the distribution of publications in the period of January 2019 to December 2023 was analyzed. Second, the obtained result was mapped to the type of publications. Third, a list of venues and journals of the submitted publications was created. Fig. 5 illustrates the number of publications per year. The figure shows a slight fluctuation in publications throughout the years. The peak in 2022 demonstrates that most papers were published in 2022.

Fig. 6 analyses the results further and shows the number of publications per year from January 2019 until December 2023 w.r.t. the publication types article, illustrated as a blue line, proceedings, illustrated as a green line, and book chapter, illustrated as a red line. In total, 56.52% of the accepted publications were conference papers, whereas 36.23% and 7.27% were articles and book chapters, respectively.

In addition, RQ1 aims to answer, if the papers are spread around various venues and journals, or if there are a few selected venues to indicate if many different or just a small amount of research communities are researching about comprehensive ontologies in OT. The obtained results list 85 different conference venues and 63 journals that were used to submit the publications. Based on the derived results, conferences, and journals where at least two publications were submitted are considered as *prominent*. Tables VI and VII list the most prominent conferences and journals, respectively, used for publishing papers regarding comprehensive ontologies in OT. The column category lists the main research community of the corresponding conference venue or journal. Since the amount of two publications per venue can already seen also *prominent*, this results listed in Table VI and VII indicate that research about comprehensive ontologies in OT is scattered around various research communities.

The main conference venue is the International Conference Cyber Security on Information Systems Security and Privacy (ICISSP), which received four publications in the last five years. A reason for the prominence of ICISSP may be the focus on cyber security, modeling, management, and IoT. Therefore, the domains *OT domain-specific model*, *threat identification*, *security controls and requirements*, *risk evaluation and prioritization*, and *risk treatment* are covered by the topics of interest of this venue. The conference ACM International Conference on Availability, Reliability, and Security (ARES) is the second prominent venue. Its subject areas include network security, distributed systems security, and domain-specific security and privacy architectures. Therefore, the domains *OT domain-specific model*, *threat identification*, and *security controls and requirements* match with the topics of interest of this conference. The third prominent conference is ACM/IEEE International Conference on Model Driven Engineering Languages and Systems (MODELS). The focus of this venue is on modeling, knowledge representation, embedded systems, security, and sustainability. Therefore, the domains *OT domain-specific model*, *operations and quality*, *threat identification*, and *security controls and requirements* are addressed. The remaining conferences shown in Table VI

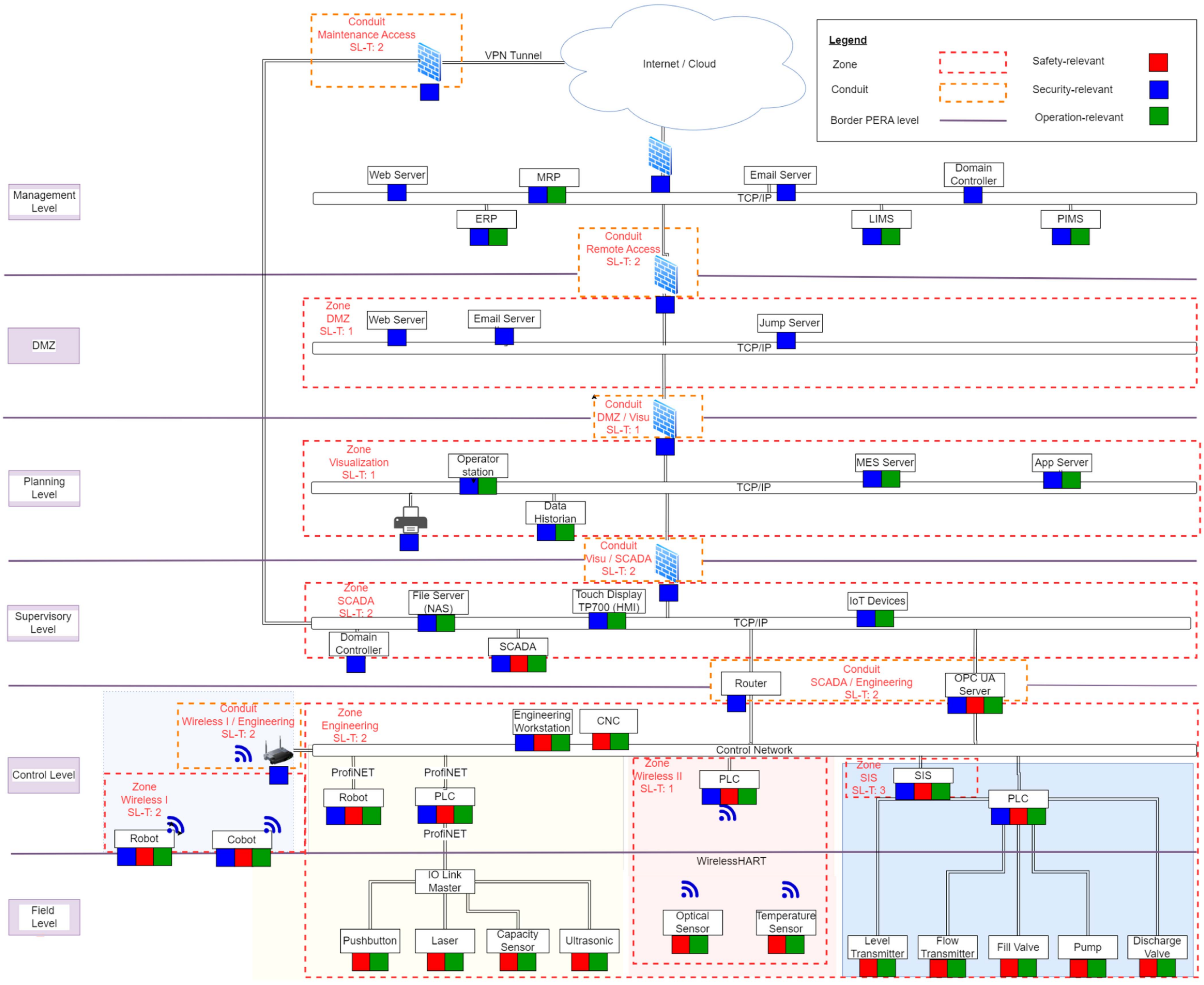

FIGURE 4. Generic use case derived from a stakeholder analysis adapted from [4] highlighting OT components as safety-relevant in red, security-relevant in blue, and operation-relevant in green.

cover at least one of the domains required for developing a comprehensive ontology in OT. The majority of the listed journals in Table VII are multidisciplinary, which makes them suitable to address all required ontology domains illustrated in Fig. 1.

Due to the information provided in the abstract of each publication, the corresponding publication was classified according to the addressed domains for comprehensive ontologies. This classification was done in a double-checking process, where two authors performed the classification process independently. After both authors had finished the isolated classification, the results were compared, and derivations were discussed to see if they had occurred. The papers that did not address any of the required domains (cf. Fig. 1) were not classified. During the classification process, 192 publications were identified as not classified. In summary, according to Tables VI and VII comprehensive ontologies in OT are experiencing interest mainly in the cyber security, software engineering, and automation sector.

C. RQ2: RESEARCH COMMUNITIES AND MAIN CONTRIBUTORS

Following [9], the analysis began by examining the number of authors and their publications. A total of 459 authors with relevant submissions were identified. In Fig. 7, the distribution of publications per author may be observed. This visual representation highlights that the majority of authors (408) have contributed only one publication addressing at least one domain essential for the development of a comprehensive ontology in OT. However, some authors who have delved deeper into this subject. Specifically, 40 authors have two publications to their credit, while eight authors have

TABLE 6. Most Prominent Conferences

Venue	Category	Pub. count
ICISSP (International Conference on Information Systems Security and Privacy)	Cyber Security	4
ARES (ACM International Conference on Availability, Reliability and Security)	Cyber Security	3
MODELS (ACM/IEEE International Conference on Model Driven Engineering Languages and Systems)	Software Engineering	3
MIPRO (International Convention on Information, Communication and Electronic Technology)	System Engineering	2
ICSC (IEEE International Conference on Semantic Computing)	Software Engineering	2
ETFA (IEEE International Conference on Emerging Technologies and Factory Automation	Automation	2
IC3K (International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management)	Software Engineering	2
ACM SIGSAC Conference on Computer and Communications Security	Cyber Security	2
European Interdisciplinary Cybersecurity Conference	Cyber Security	2
Pan-Hellenic Conference on Informatics	Software Engineering	2
ACM/SIGAPP Symposium on Applied Computing	Software Engineering	2
CCIS (Communications in Computer and Information Science)	Software Engineering	2

TABLE 7. Most Prominent Journals

Journal	Category	Pub. count
IEEE Access	Multidisciplinary, Electronics	4
Automation in Construction Electronics (Switzerland)	Automation	3
International Journal of Environmental Research and Public Health	Safety	2
Journal of Information Security and Application	Cyber Security	2
Procedia CIRP	Automation	2
Procedia Computer Science	Multidisciplinary, Computer Science	2

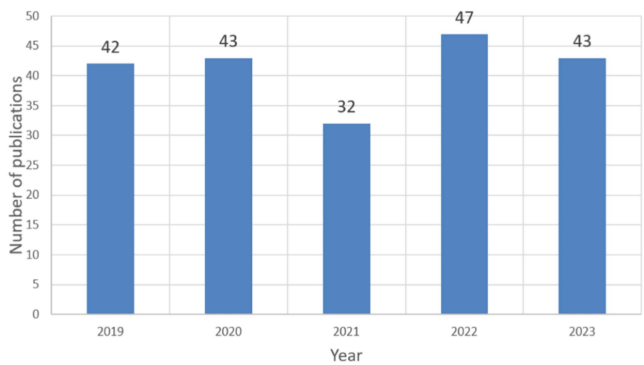

FIGURE 5. Number of publications per year in the period from 2019 to 2023 (included number of publications: 207).

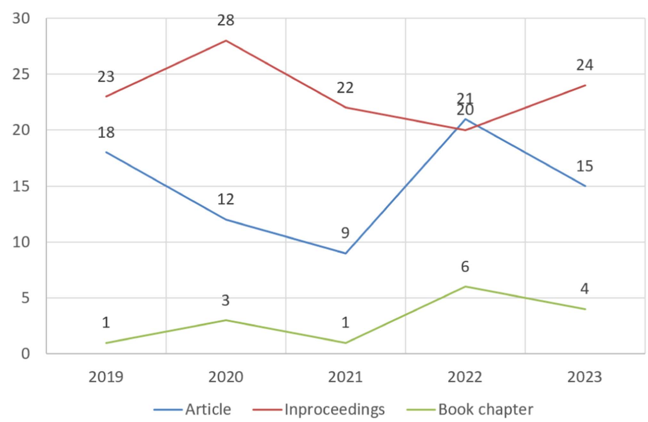

FIGURE 6. Number of publications per year w.r.t. publication type (included number of publications: 207).

three publications, and three authors have four publications each.

Examining the distribution of authors worldwide in terms of their affiliation, the study delved into both related and unrelated authors across different continents. As illustrated in Fig. 8, the majority of authors (45.29%) are affiliated in Europe, closely trailed by Asia (39.06%). A deeper analysis reveals that China boasts the highest number of affiliated authors, followed by the United Kingdom and France, as depicted in Fig. 9.

Furthermore, the influence of the screened publications on the scientific community was analyzed. To count the corresponding citation counts, Google Scholar was used since some digital libraries did not provide this information at all, or only the subset of citations of research papers indexed by the same database. Fig. 10 illustrates the distribution of citations. The top publication [37] was cited 40 times and addresses the domains *OT domain-specific model*, *operations and quality*, *safety functions*, *security controls*, *risk evaluation*, and *risk treatment*.

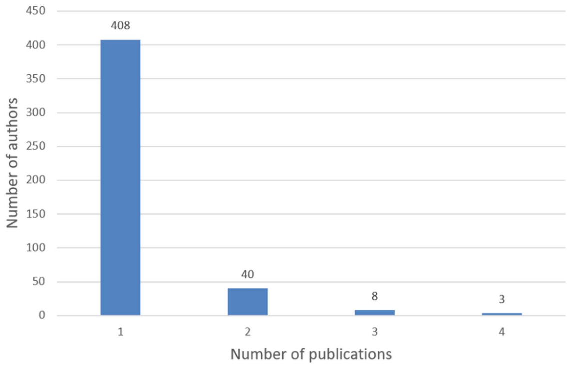

FIGURE 7. Number of publications per author in the period from January 2019 to December 2023 (included number of publications: 207).

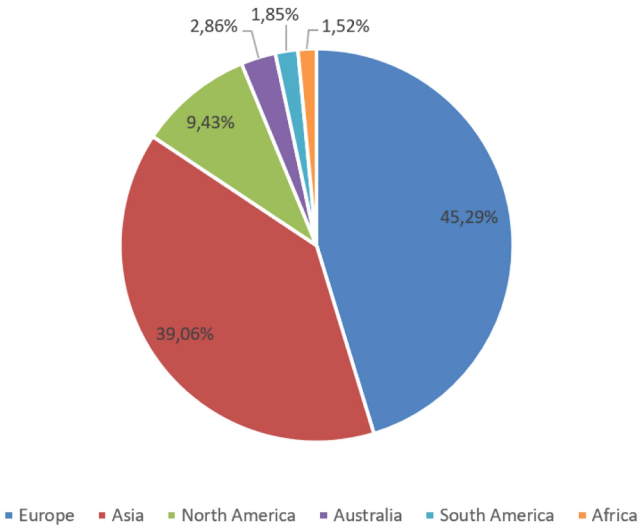

FIGURE 8. Percentage of authors per continent (included number of publications: 207).

D. RQ3: CLASSIFICATION OF RELEVANT PUBLICATIONS

In the classification process, the matching category of publication based on [33] described in Table II was assigned to each publication. This classification scheme enables to identify whether the corresponding ontology is evaluated and used, has obtained the first experiment results, a prototype or proof of concept is proposed, or a theoretical consideration. The results of this classification are provided in Fig. 11. In total, 28 evaluation papers, 67 validation papers, 71 solution proposals, 26 philosophical papers, six opinion papers, and nine experience papers were identified. This indicates that the majority of analyzed ontology papers provide at least a proof of concept.

E. RQ4: CONSIDERED ONTOLOGY DOMAINS

In addition to the categorization with the research type facets, the considered ontology domains are analyzed. Fig. 12 illustrates a tag cloud[5] based on the keywords of the screened publications created to visualize the most important terms to consider when searching for comprehensive ontologies. Conjunctions with keywords already used for conducting the search (cf. Section III-B) were excluded. The most frequent used keywords are *systems*, *data*, *knowledge*, *information*, and *modeling*.

Fig. 13 illustrates which ontology domains are typically considered together. Ontologies addressing an *OT domain-specific model* typically also consider *operations and quality*, *security controls*, *safety functions*, or *risk treatment*. Ontologies addressing *operations and quality* often consider *OT*

[5]Created with http://tagcrowd.com/

TABLE 8. Conclusion Validity Threats Based on [33]

Validity threat	Description
Subjective measures	Manually categorizing abstracts into research type facets [33] without clear criteria, may lead to validity threats.
Low statistical power	The selection of publications can greatly impact the outcome, potentially leading to varying rankings of prominent authors. This variability can arise from factors such as the criteria used for inclusion or exclusion of papers, which in turn affects the internal validity of the study.
Searching for specific results	Searching for specific results biases the results. This may be influenced by the selection of papers (cf. internal validity).
Publication bias	Less promising results may be underrepresented in such categorizations. This could be due to reviewers or editors being less inclined to accept or publish these studies, leading to a skewed representation of certain research types. For instance, early-stage research, such as philosophical or opinion papers, might be disproportionately underrepresented in the categorization process.

TABLE 9. Internal Validity Threats Based on [33]

Category	Validity threat	Description
Publication selection	Keywords	Keywords listed in Section III-B were used against the title of the papers.
	Publication period	The chosen publication period is from January 2019 to December 2023. This short time frame was elected to include only the most recent developments and state-of-the-art.
	Literature repositories	Three digital libraries were used as literature repositories, namely ACM Digital Library, IEEE Xplore Digital Library, and Scopus.
	Publication language	Due to the author's language skills, papers written in English, or German were in scope of this SMS.
	Manual filtering	Duplicates, books, and publications lacking a proper research context described in their abstract were excluded.
Instrumentation	Timeliness and completeness	The timeliness and comprehensiveness of digital libraries play a crucial role in influencing the venues that these repositories prioritize. There may be instances where published materials, such as post-proceedings, are delayed, resulting in them not being immediately accessible online.

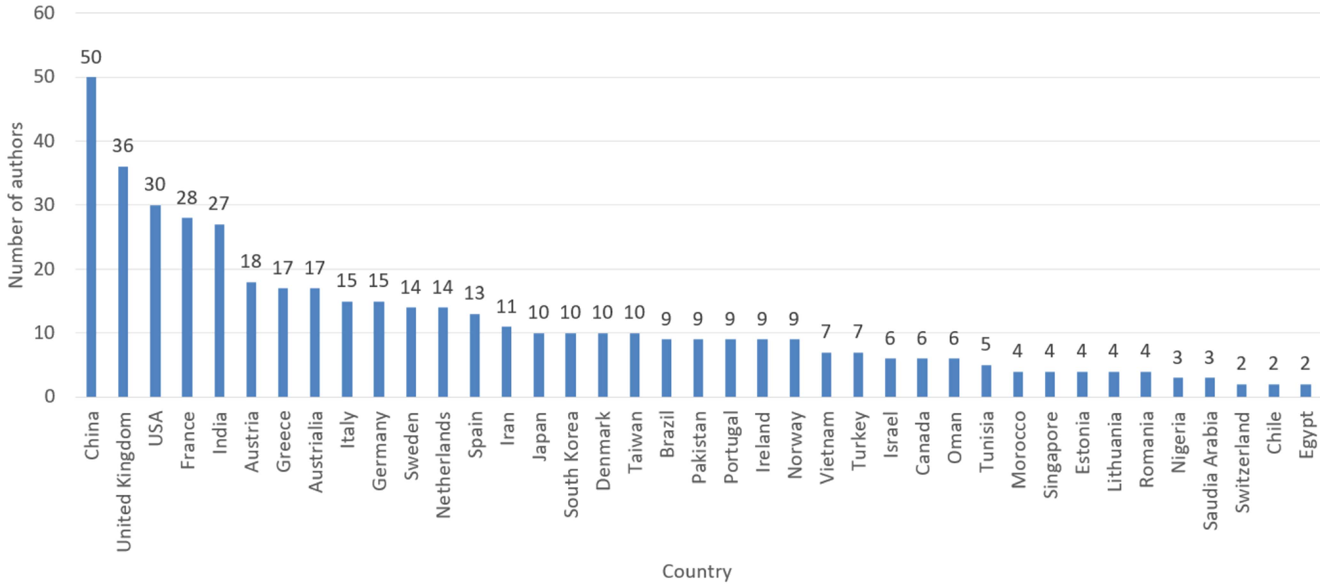

FIGURE 9. Number authors per country (included number of publications: 207).

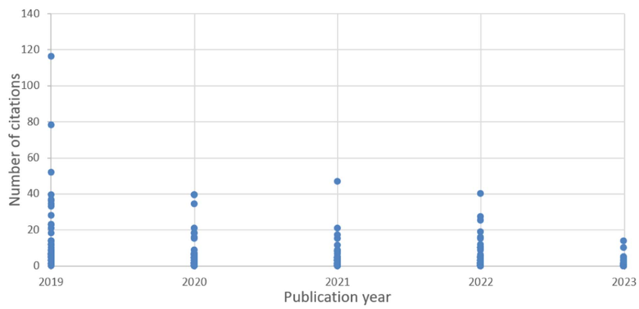

FIGURE 10. Distribution of citations of publications per year (included number of publications: 207).

domain-specific model aspects but typically neglect the other domains needed for a comprehensive ontology in OT. *Hazard identification* ontologies tend to also take *safety functions* and *risk treatment* into account. *Threat identification* ontologies often also address *security controls*. Ontologies focusing on *security controls* typically also consider aspects of *OT domain-specific model*, *risk evaluation*, and *risk treatment*. Ontologies mainly dealing with *safety functions* often also consider *OT domain-specific model* and *risk treatment* aspects. *Risk evaluation* is often viewed together with *risk treatment*, *security controls*, and *OT domain-specific model* characteristics. *Risk treatment* tends to be combined with *security controls*, *OT domain-specific model* aspects, and *risk evaluation*.

In addition, it was analyzed which standards are addressed by the screened publications, as Fig. 14 illustrates. The majority of addressed standards were the ISO 27000 family [38] considering general information security requirements, IEC 61499 [39] defining a generic architecture of distributed systems, IEC 61508 [15] a general functional safety standard, NIST 800-53 [20] focusing on OT security, ISO/IEC 20005 [40] considering collaborative information processing in intelligent sensor networks, and IEC 61512 [16] defining a reference model for batch production records. Furthermore, Fig. 14 shows that recent trends in digitization, for instance RAMI4.0 (published in standard DIN SPEC 91345 [18]), the usage and application of AAS (published in standard IEC 63278 [17]), or the NAMUR Open architecture concept (published in standard [22]) are only considered by a minority of the screened publications.

TABLE 10. Construct Validity Threats Based on [33]

Category	Validity threat	Description and mitigation
Design threat	Monomethod bias	This SMS is based on the systematic mapping process [33]. In this context, authors of different institutes have worked on this study.
	Confounding constructs and levels of constructs	This applies, for example, if during the categorization process to the research type facets, multiple type facets are applicable (e.g., evaluation research and validation research). In such cases, the most fitting research facet type was chosen after a dedicated discussion.
Social threat	Hypothesis guessing	Due to the familiarity of the authors with comprehensive ontologies in OT, some results may be expected, for example, the relatively low count of philosophical and opinion papers, or the strong interest of Europe into the analyzed research topic. This threat was addressed by the application of an open research design where expected knowledge was not just checked but also new knowledge was extracted.

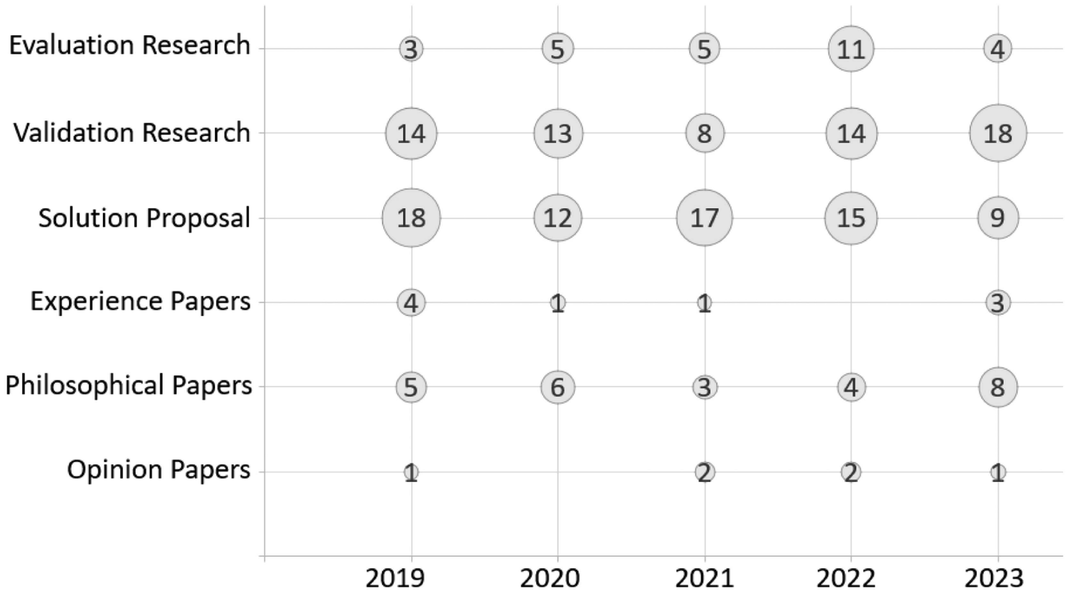

FIGURE 11. Amount of publications per year according to the type facet classification (included number of publications: 207).

TABLE 11. External Validity Threats Based on [33], [41]

Validity threat	Description
Interaction of participants and treatment	This phenomenon arises when the individuals comprising the subject population do not accurately reflect the broader population we aim to draw conclusions about. In other words, the participants in the experiment are not the appropriate representatives. For instance, a potential risk of this nature could involve exclusively choosing programmers for an inspection experiment, despite the fact that programmers, testers, and system engineers typically participate in such inspections.
Interaction of environment/setting and treatment	This threat addresses the consequence of lacking experimental settings or materials that accurately reflect industrial practices. For instance, utilizing outdated tools in an experiment while modern tools are prevalent in industry exemplifies this disparity. Similarly, conducting experiments on trivial or simplified problems results in an incorrect "place" or environment for meaningful analysis.
Interaction of history/timing and treatment	This threat describes how conducting an experiment at a specific time or day can influence the outcomes. For instance, if a survey about safety-critical systems is administered shortly after a significant software-related crash, responses are likely to differ compared to those obtained shortly before or some time after the incident.

FIGURE 12. Tag cloud of most important terms (included number of publications: 207).

F. RESULT SET

Table 12 in Appendix A lists the results of the screened papers w.r.t. the matching type facet and its domains according to Fig. 1 addressed as requirements to be included in this study, namely,

1) R1: OT domain-specific model;
2) R2: Operations and quality;
3) R3: Hazard identification;
4) R4: Threat identification;
5) R5: Safety functions and requirements;
6) R6: Security controls and requirements;
7) R7: Risk evaluations and prioritization;
8) R8: Risk treatment.

The full dataset used in these SMSes is publicly available online.

V. EVALUATION

Ontologies in the category of *evaluation research* (see Table II) were conceptually analyzed. Some ontologies cover multiple relevant domains of this study in a generic, system-agnostic manner. Others tend to focus either on security or

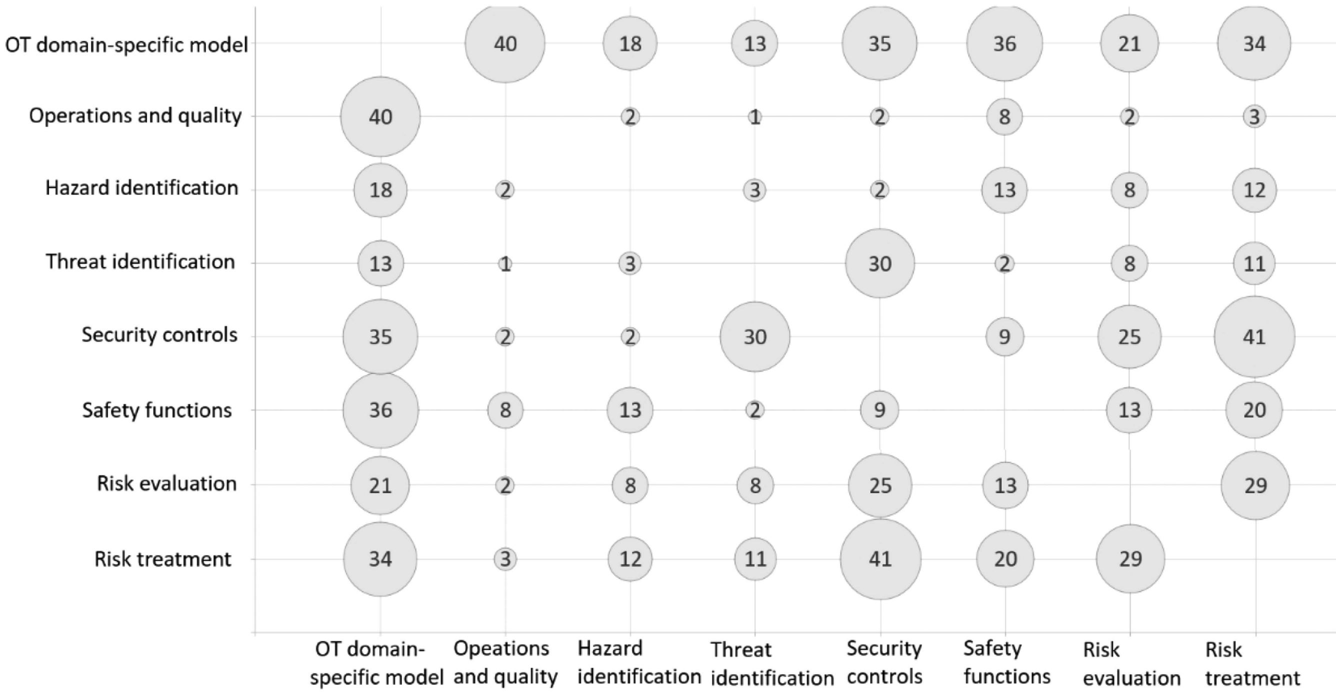

FIGURE 13. Distribution of addressing ontology domains (included number of publications: 207).

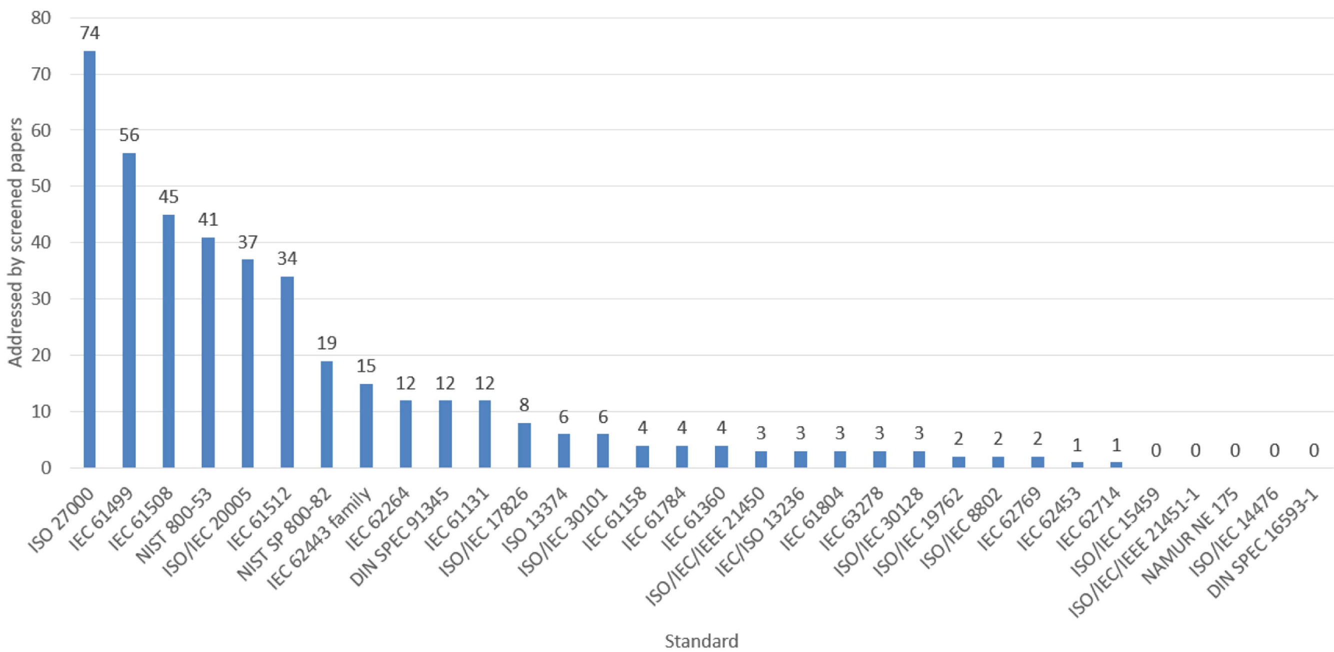

FIGURE 14. Distribution of addressing ontologies addressing applicable standards based on [13] (included number of publications: 207).

safety aspects within the OT systems, but not both. When these requirements are addressed in isolation, risk evaluation and treatment are constrained to either safety or security, due to the narrow scope of the corresponding ontology.

Each requirement addressed by the ontologies may be considered in varying depths of detail. For instance, virtualization layers used by hypervisors or containerized environments are often not represented in some ontologies, despite this information being crucial for identifying potential threats based on such technologies. This omission is significant as attackers might exploit techniques to compromise other virtualized systems running on the same hypervisor or the hypervisor itself.

In addition, some ontologies do not support application software [e.g., file transfer protocol (FTP) servers], including their versions, which means that vulnerabilities may not be modeled with the provided software classes. Ontologies that focus on security threat identification tend to overlook industrial communication systems such as control networks or machine to machine (M2M) communication not based on Internet Protocol (IP), as well as firmware used by embedded OT devices. Therefore, these ontologies cannot include these aspects in the proposed threat identification.

This study revealed that while ontologies addressing process hazards are available, those specifically considering safety for machinery are not yet accessible. Security attacks that lead to violations of quality requirements, resulting in significant financial losses due to valid but inefficient production, may remain undetected by the analyzed ontologies.

The following four types of threats to validity [41] were considered to evaluate the quality of the results:

1) Conclusion validity;
2) Internal validity;
3) Construct validity;
4) External validity.

A. CONCLUSION VALIDITY

Conclusion validity [41] as outlined in Table VIII, pertains to the potential challenges in drawing accurate conclusions or ensuring the replicability of a study. It emphasizes the importance of deriving correct conclusions based on the alignment between the study's design and the outcomes of the analysis.

To address subjective measures, the publications were categorized from the result set based on the classification detailed in Table II based on [33]. Each categorization was thoroughly discussed beforehand, with careful consideration given to edge cases. All authors were engaged in detailed examination and deliberation to arrive at well-reasoned classifications. Tie-breakers were unnecessary for this study, but had they arisen, the perspective of the most experienced author in the corresponding domain would have been deferred to.

To mitigate the threat to conclusion validity arising from low statistical power, the search was broadened across various digital libraries referred to as key electronic databases [36] to compile a comprehensive selection of publications. This approach aimed to reduce the risk of obtaining insufficient data. While comparing with a sampling method such as that discussed in [42] could have been pertinent, it fell beyond the scope of our study, which focused on different aspects.

In order to counter publication bias, multiple databases were utilized with diverse scopes. This strategy ensures that even if a publication might be missed by one database associated with a particular venue, it could still be found in another venue indexed by a different database.

B. INTERNAL VALIDITY

Threats outlined in this category [41] propose a causal connection, such as concealed variables or incidental correlations, respectively. Consequently, the objective of mitigating these threats is to guarantee that the methodologies employed in the study genuinely influence its outcomes. Table IX lists internal validity threats in the context of this SMSes.

This SMSes addresses threats within this category by exploring alternatives to prevent overly rigid constraints. For instance, diverse keywords reflecting the scope of mapping were utilized in the search procedure, a defined publication time frame was taken into account, and three prominent digital libraries were selected.

C. CONSTRUCT VALIDITY

Construct validity [33] considers the relation between observation and theory. Threats of this category deal with issues potentially arising during research design. Therefore, the used concept has to be verified. Table X lists construct validity threats and how those were mitigated in this study.

D. EXTERNAL VALIDITY

This threat categorization [33], [41] concerns possible generalization, thus if results of this study may also be applied outside of the scope of this SMSes. Table XI lists possible external validity threats.

The goals of this SMSes do not include generalization. Considering the scope of this study (e.g., keywords, publication period) this SMSes's goal is to get as close to completeness as possible since no thorough literature survey can ever be fully complete.

VI. CONCLUSION

This systematic mapping study analyzes comprehensive ontologies considering safety, security, and operation requirements in OT. Fig. 1 illustrates the domains that need to be considered to gain the necessary holistic view of OT systems that risk managers need to make accurate decisions. The results of this review show that each ontology analyzed focused on specific domains, but none modeled the holistic scope and the relationships between these domains. Thus, the full scope of a risk or site manager to be responsible or accountable for the operation of a dedicated OT system is not yet addressed by the state-of-the-art ontologies in the literature.

Research direction 1: Integrated view of security, safety, and product/process requirements.

The results of this study demonstrate, that there are numerous interdisciplinary ontologies existing already, that provide a combined view of some domains needed for a holistic view (cf. Fig. 13). However, while some domains are often viewed together such as *OT domain-specific models* with *operations and quality* requirements, there are also sets of domains tend to be viewed isolated frequently, for instance, *risk evaluation* with *hazard identification* and *threat identification*. Therefore, further investigation should be executed to provide risk managers of OT systems a holistic view of safety, security, and operation and quality requirements.

Research direction 2: Identifying and addressing interdependencies between requirements.

Ontologies that offer an integrated view of security, safety, and product or process requirements may be able to identify interdependencies between these requirements [4], [5]. In contrast, when isolated viewed, a safety-relevant emergency stop function has to be accessible at all times to fulfill the standard ISO 13850 [28]. In terms of security, the very same function would have to be only accessible by authenticated and authorized users to fulfill the least-privilege principle required by numerous security standards, e.g., IEC 62443 [29].

Such identified conflicts between different requirements [5] have to be addressed by providing compensating controls or measures considering the remaining domains, their properties, and their relations. For example, instead of encryption additional physical security layers, network segmentation, and whitelisting of hosts (e.g., based on their MAC or IP address) could address this issue without neglecting operations and safety requirements but still improve the security level of the overall OT system.

Fig. 13 illustrated that only a small subset of the analyzed publications provide the combined view of *security controls* and *hazard identification* or *safety functions* to be able to identify such conflicts between safety and security requirements. This indicates that potential conflicting requirements tend to be not addressed accordingly.

Research direction 3: Integrated risk management based on an integrated view.

In the industry, stakeholders are forced to make interdisciplinary decisions [4]. Without proper knowledge or information about the domains required for a holistic view (cf. Fig. 13), these decisions may be not optimal leading to impacts on product quality or increased severity of threats, or increased probability of hazards, respectively, to occur. Therefore, risk evaluation and risk treatment methodologies or schemes are needed that prioritize identified derivations of security, safety, or operation and quality requirements based on a holistic view.

Research direction 4: Deeper analysis of the publications for further research questions.

The results of this systematic mapping study also provided preliminary insights into the depth ontologies that address the domains according to Fig. 13. For, example, [43] considers *threat identification* and *security controls*, it does not support the modeling of application software such as FTP, domain name system (DNS), simple mail transfer protocol (SMTP), or remote desktop protocol (RDP) servers, respectively. Thus, attacks exploiting application software may not be addressed when using this ontology. On the other hand, [43] uses standardized security taxonomies, such as structured threat information expression (STIX), common weakness enumeration (CWE), common vulnerabilities and exposures (CVE), common vulnerability scoring system (CVSS), and common attack pattern enumeration and classification (CAPEC) to represent *security controls* in a wide accepted and applicable manner, increasing its compatibility with other security-related models. This result indicates that the communication technologies of different OT components that comprise the OT system, their vulnerabilities against cyber-attacks, and possible safety consequences should also be considered when developing a comprehensive ontology. This includes wireless and wired industry 4.0-compliant communication technologies, for instance, OPC unified architecture (OPC UA), message queuing telemetry transport (MQTT), and hypertext transfer protocol (HTTP).

APPENDIX A
RESULTS

TABLE 12. Result Set of This SMSes (Included Number of Publications: 207)

Paper	Research type facet	Domains addressed
[44]	Validation research	R1, R5, R6
[45]	Philosophical paper	R1, R3, R4
[46]	Evaluation research	R1, R3, R4, R5, R6, R7, R8
[47]	Philosophical paper	R1, R5
[48]	Solution proposal	R1, R5, R7, R8
[49]	Validation research	R3, R6
[50]	Solution proposal	R1, R3, R7, R8
[51]	Evaluation research	R4
[52]	Solution proposal	R4
[53]	Evaluation research	R4, R6
[54]	Evaluation research	R1, R6
[55]	Solution proposal	R4, R6
[56]	Philosophical paper	R4, R6
[57]	Solution proposal	R1, R4
[58]	Solution proposal	R6
[59]	Validation research	R1, R4
[60]	Validation research	R1, R2
[61]	Validation research	R1, R3, R5
[62]	Evaluation research	R1, R5
[63]	Validation research	R1, R2, R4, R6, R8
[64]	Evaluation research	R3, R6, R8
[65]	Opinion paper	R1, R6
[66]	Solution proposal	R6
[67]	Solution proposal	R4, R6
[68]	Validation research	R6, R7
[69]	Solution proposal	R1, R4, R6
[70]	Philosophical paper	R6
[71]	Solution proposal	R4
[72]	Philosophical paper	R1, R4, R6
[73]	Solution proposal	R6
[74]	Evaluation research	R4, R6
[75]	Solution proposal	R4, R6
[76]	Philosophical paper	R1, R6
[77]	Validation research	R6
[78]	Solution proposal	R4, R7
[79]	Validation research	R3
[80]	Evaluation research	R1, R4, R6
[81]	Solution proposal	R4, R6
[82]	Validation research	R4

TABLE 12. (Continued)

[83]	Experience paper	R1, R6
[84]	Experience paper	R4
[85]	Philosophical paper	R6
[86]	Validation research	R1, R3, R5
[87]	Solution proposal	R1, R5, R6
[88]	Evaluation research	R4, R6
[89]	Validation research	R1, R6
[90]	Validation research	R4, R6
[91]	Validation research	R2, R3, R7, R8
[92]	Evaluation research	R1, R5
[93]	Validation research	R4
[94]	Validation research	R1, R3, R5
[95]	Solution proposal	R4, R6
[96]	Opinion paper	R1, R4
[97]	Evaluation research	R1, R5, R7, R8
[98]	Validation research	R1, R5
[99]	Evaluation research	R1, R3, R7, R8
[100]	Solution proposal	R6, R7
[101]	Validation research	R1, R3, R5
[102]	Validation research	R1, R3, R5, R8
[103]	Opinion paper	R1, R2
[104]	Philosophical paper	R1, R2, R3
[105]	Solution proposal	R1, R5, R7, R8
[106]	Philosophical paper	R6, R7
[107]	Validation research	R1, R5, R7, R8
[108]	Evaluation research	R1, R5, R7, R8
[109]	Solution proposal	R1, R2
[110]	Validation research	R1, R5, R8
[111]	Evaluation research	R1, R3, R5, R8
[112]	Philosophical paper	R6, R7
[113]	Solution proposal	R6
[114]	Validation research	R1, R6, R7, R8
[115]	Evaluation research	R6, R7
[116]	Validation research	R6, R7
[117]	Solution proposal	R1, R2
[118]	Philosophical paper	R4, R8
[119]	Validation research	R6
[43]	Validation research	R1, R2, R5, R6, R7, R8
[120]	Validation research	R5
[121]	Solution proposal	R1, R6, R8
[122]	Evaluation research	R1, R6, R7, R8
[123]	Validation research	R3, R5
[124]	Solution proposal	R6
[125]	Solution proposal	R2, R4
[126]	Solution proposal	R3, R8
[127]	Validation research	R2
[128]	Opinion paper	R4, R8
[129]	Evaluation research	R1, R5, R8
[130]	Evaluation research	R2
[131]	Validation research	R1, R5, R7, R8
[132]	Solution proposal	R2
[133]	Solution proposal	R6, R7
[134]	Solution proposal	R5, R6, R7, R8
[135]	Solution proposal	R6, R8
[136]	Solution proposal	R2
[137]	Solution proposal	R2
[138]	Philosophical paper	R1, R3, R7, R8
[139]	Validation research	R6, R7, R8
[140]	Philosophical paper	R6, R7, R8
[141]	Validation research	R1, R2, R5
[142]	Solution proposal	R6, R8
[143]	Philosophical paper	R1, R6, R8
[144]	Validation research	R6, R8
[145]	Experience paper	R1, R5
[146]	Validation research	R1, R6, R7, R8
[147]	Evaluation research	R1, R2
[148]	Solution proposal	R6
[149]	Solution proposal	R1, R3
[150]	Validation research	R6
[151]	Validation research	R4, R6
[152]	Validation research	R1, R3, R4, R5, R6, R8
[153]	Solution proposal	R1, R2
[154]	Validation research	R2
[155]	Philosophical paper	R2
[156]	Solution proposal	R1, R2, R5
[157]	Validation research	R1, R5, R8
[158]	Opinion paper	R1, R6, R7, R8
[159]	Solution proposal	R6
[160]	Experience paper	R1, R3, R5, R7
[161]	Philosophical paper	R4, R6
[162]	Philosophical paper	R6
[163]	Philosophical paper	R1, R4
[164]	Validation research	R1, R2
[165]	Validation research	R1, R6
[166]	Solution proposal	R4, R6
[167]	Solution proposal	R1, R2, R5
[168]	Philosophical paper	R6, R7
[169]	Solution proposal	R5, R8
[170]	Validation research	R6, R8
[171]	Philosophical paper	R1, R4, R6
[172]	Solution proposal	R2
[173]	Solution proposal	R2
[174]	Validation research	R1, R2, R5
[175]	Solution proposal	R1, R2
[176]	Philosophical paper	R4, R6, R7
[177]	Solution proposal	R5, R7, R8
[178]	Validation research	R1, R6, R7
[179]	Solution proposal	R4, R6, R7, R8
[180]	Validation research	R1, R3, R5, R7, R8
[181]	Solution proposal	R1, R6, R8
[182]	Philosophical paper	R5, R6, R7
[183]	Validation research	R4, R6

TABLE 12. (Continued)

[184]	Validation research	R6, R7
[185]	Validation research	R1, R2, R5
[186]	Validation research	R1, R4, R6, R8
[187]	Solution proposal	R4, R6, R7, R8
[188]	Solution proposal	R1, R3, R5, R7, R8
[189]	Experience paper	R6, R8
[190]	Experience paper	R1, R6
[191]	Experience paper	R1, R5, R6
[192]	Solution proposal	R1, R2
[193]	Evaluation research	R1, R5, R6, R8
[194]	Validation research	R6, R7
[195]	Validation research	R2
[196]	Validation research	R6, R7
[197]	Validation research	R1, R6, R7, R8
[198]	Solution proposal	R1, R2
[199]	Solution proposal	R4, R6
[200]	Solution proposal	R4, R6, R8
[201]	Solution proposal	R1, R2
[202]	Solution proposal	R2
[203]	Experience paper	R6, R8
[204]	Validation research	R2
[205]	Validation research	R6, R8
[206]	Solution proposal	R1, R2, R5
[207]	Solution proposal	R1, R2
[208]	Solution proposal	R1, R2
[209]	Validation research	R1, R2
[210]	Solution proposal	R4
[211]	Philosophical paper	R6, R8
[212]	Validation research	R1, R6, R7, R8
[213]	Evaluation research	R1
[214]	Validation research	R1, R2
[215]	Validation research	R6, R7, R8
[216]	Validation research	R2
[217]	Validation research	R1, R2
[218]	Evaluation research	R2
[219]	Solution proposal	R4, R6, R7
[220]	Evaluation research	R2
[221]	Solution proposal	R1, R6, R8
[222]	Evaluation research	R1, R2
[223]	Validation research	R1, R2
[224]	Validation research	R2
[225]	Solution proposal	R1, R6, R7, R8
[226]	Evaluation research	R1, R2
[227]	Solution proposal	R1, R2
[228]	Validation research	R4, R7
[229]	Solution proposal	R1, R2
[230]	Solution proposal	R2
[231]	Solution proposal	R1, R2
[232]	Solution proposal	R6, R7, R8
[233]	Validation research	R1
[234]	Solution proposal	R6
[235]	Philosophical paper	R4, R7, R8

TABLE 12. (Continued)

[236]	Evaluation research	R1, R2
[237]	Solution proposal	R1, R2
[238]	Solution proposal	R1, R2
[239]	Philosophical paper	R1, R6
[240]	Validation research	R1, R2
[241]	Evaluation research	R6
[242]	Validation research	R1, R2
[243]	Solution proposal	R1, R2
[244]	Experience paper	R1
[245]	Evaluation research	R1, R6, R8
[246]	Opinion paper	R1, R6
[247]	Validation research	R1, R2
[248]	Solution proposal	R1, R2
[249]	Philosophical paper	R1, R2
		Concluded

REFERENCES

[1] S. Hollerer, T. Sauter, and W. Kastner, "Risk assessments considering safety, security, and their interdependencies in OT environments," in *Proc. 17th Int. Conf. Availability, Rel. Secur.*, 2022, pp. 1–8, doi: 10.1145/3538969.3543814.

[2] A. Treytl, T. Sauter, and C. Schwaiger, "Security measures in automation systems-A practice-oriented approach," in *Proc. IEEE Conf. Emerg. Technol. Factory Automat.*, 2005, pp. 847–855, doi: 10.1109/ETFA.2005.1612762.

[3] P. K. Garimella, "IT-OT integration challenges in utilities," in *Proc. IEEE 3rd Int. Conf. Comput., Commun. Secur.*, 2018, pp. 199–204, doi: 10.1109/CCCS.2018.8586807.

[4] S. Hollerer, W. Kastner, and T. Sauter, "Safety and security: A field of tension in industrial practice," in *Proc. IEEE 21st Int. Conf. Ind. Informat.*, 2023, pp. 1–7, doi: 10.1109/INDIN51400.2023.10217900.

[5] S. Hollerer, W. Kastner, and T. Sauter, "Towards a comprehensive ontology considering safety, security, and operation requirements in OT," in *Proc. IEEE 28th Int. Conf. Emerg. Technol. Factory Automat.*, 2023, pp. 1–4, doi: 10.1109/ETFA54631.2023.10275521.

[6] R. Studer, V. Benjamins, and D. Fensel, "Knowledge engineering: Principles and methods," *Data Knowl. Eng.*, vol. 25, no. 1, pp. 161–197, 1998, doi: 10.1016/S0169-023X(97)00056-6.

[7] I. Horrocks, P. F. P.-Schneider, and F. v. Harmelen, "From SHIQ and RDF to OWL: The making of a web ontology language," *J. Web Semantics*, vol. 1, no. 1, pp. 7–26, 2003, doi: 10.1016/j.websem.2003.07.001.

[8] B. A. Kitchenham, D. Budgen, and O. P. Brereton, "Using mapping studies as the basis for further research–a participant-observer case study," *Inf. Softw. Technol.*, vol. 53, no. 6, pp. 638–651, 2011, doi: 10.1016/j.infsof.2010.12.011.

[9] S. Wolny, A. Mazak, C. Carpella, V. Geist, and M. Wimmer, "Thirteen years of SysML: A systematic mapping study," *Softw. Syst. Model.*, vol. 19, no. 1, pp. 111–169, 2020, doi: 10.1007/s10270-019-00735-y.

[10] B. Kitchenham and P. Brereton, "A systematic review of systematic review process research in software engineering," *Inf. Softw. Technol.*, vol. 55, no. 12, pp. 2049–2075, 2013, doi: 10.1016/j.infsof.2013.07.010.

[11] P. H. Nguyen, S. Ali, and T. Yue, "Model-based security engineering for cyber-physical systems: A systematic mapping study," *Inf. Softw. Technol.*, vol. 83, pp. 116–135, 2017, doi: 10.1016/j.infsof.2016.11.004.

[12] E. Taştan, S. Fluchs, and R. Drath, "Warum wir ein security-engineering-informationsmodell brauchen," in *Proc. Tagungsbnd AALE 2022*, 2022, pp. 1–10, doi: 10.33968/2022.25.

[13] A. J. C. Trappey, C. V. Trappey, U. H. Govindarajan, J. J. Sun, and A. C. Chuang, "A review of technology standards and patent portfolios for enabling cyber-physical systems in advanced manufacturing," *IEEE Access*, vol. 4, pp. 7356–7382, 2016, doi: 10.1109/ACCESS.2016.2619360.

[14] Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design, IEC 62443-3-2, 2020.
[15] Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements, IEC 61508-1, 2010.
[16] *Batch control - Batch production records*, IEC 61512-4, 1997.
[17] *Asset administration shell for industrial applications - Part 1: Asset administration shell structure*, IEC 63278-1, 2023.
[18] *Referenzarchitekturmodell Industrie 4.0*," DIN SPEC 91345-4, 2016, doi: 10.31030/2436156.
[19] *Referenzmodell für industrie 4.0-Servicearchitekturen - teil 1: Grundkonzepte einer interaktionsbasierten architektur*, DIN SPEC 16593-1, 2016, doi: 10.31030/2436156.
[20] NIST (National Institute of Standards and Technology), "Security and privacy controls for federal information systems and organizations," NIST SP 800-53 Rev. 5, 2020.
[21] NIST (National Institute of Standards and Technology), "Guide to operational technology (OT) security," NIST SP 800-82 Rev. 3, 2023.
[22] NAMUR (Normen-Arbeitsgemeinschaft für Mess- und Regeltechnik in der Chemischen Industrie), "NAMUR empfehlung NE 175 - NAMUR open architecture–NOA concept," 2020.
[23] M. Ehrlich et al., "Alignment of safety and security risk assessments for modular production systems," *Österreichischer Verband für Elektrotechnik*, vol. 138, pp. 454–461, 2021, doi: 10.1007/s00502-021-00927-9.
[24] S. L. Schiavone, L. Garg, and K. L. Summers, "Ontology of information security in enterprises," *Electron. J. Inf. Syst. Eval.*, vol. 17, no. 1, pp. 71–87, 2014, https://api.semanticscholar.org/CorpusID:210176811
[25] A. Ekelhart, S. Fenz, M. Klemen, and E. Weippl, "Security ontologies: Improving quantitative risk analysis," in *Proc. IEEE 40th Annu. Hawaii Int. Conf. System Sci.*, 2007, pp. 156a–156a, doi: 10.1109/HICSS.2007.478.
[26] *Failure modes and effects analysis (FMEA and FMECA)*, IEC 60812, 2023.
[27] *Functional safety - Safety instrumented systems for the process industry sector, Part 3: Guidance for the determination of the required safety integrity levels*, IEC 61511-3, 2016.
[28] *Safety of machinery – Emergency stop function – Principles for design*, ISO 13850, 2015.
[29] *Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels*," IEC 62443-3-3, 2013.
[30] *Safety of machinery - Functional safety of safety-related control systems*, IEC 62061, 2021.
[31] S. Hollerer et al., *Challenges in OT Security and Their Impacts on Safety-Related Cyber-Physical Production Systems*. Berlin, Germany: Springer, 2023, doi: 10.1007/978-3-662-65004-2_7.
[32] M. Sabou, O. Kovalenko, F. J. Ekaputra, and S. Biffl, *Semantic Web Solutions in Engineering*. Cham, Switzerland: Springer Int. Publishing, 2016, doi: 10.1007/978-3-319-41490-4_11.
[33] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic mapping studies in software engineering," in *Proc. 12th Int. Conf. Eval. Assessment Softw. Eng.*, 2008, pp. 68–77, doi: 10.5555/2227115.2227123.
[34] M. Kuhrmann, D. M. Fernández, and M. Tiessler, "A mapping study on the feasibility of method engineering," *J. Softw.: Evol. Process*, vol. 26, no. 12, pp. 1053–1073, 2014, doi: 10.1002/smr.1642.
[35] R. Wieringa, N. Maiden, N. Mead, and C. Rolland, "Requirements engineering paper classification and evaluation criteria: A proposal and a discussion," *Requirements Eng.*, vol. 11, no. 1, pp. 102–107, Mar. 2006, doi: 10.1007/s00766-005-0021-6.
[36] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *J. Syst. Softw.*, vol. 80, no. 4, pp. 571–583, 2007, doi: 10.1016/j.jss.2006.07.009.
[37] J. Alanen et al., "Hybrid ontology for safety, security, and dependability risk assessments and security threat analysis (STA) method for industrial control systems," *Rel. Eng. Syst. Saf.*, vol. 220, 2022, Art. no. 108270. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0951832021007444
[38] *Information technology – Security techniques – information security management systems*, ISO 27000, 2018.
[39] *Function blocks - part 1: Architecture*, IEC61499, 2012.
[40] *Information technology – Sensor networks – Services and interfaces supporting collaborative information processing in intelligent sensor networks*, ISO 20005, 2013.
[41] C. Wohlin, P. Runeson, M. Hst, M. C. Ohlsson, B. Regnell, and A. Wessln, *Experimentation in Software Engineering*. Berlin, Germany: Springer Publishing Company, 2012, doi: 10.1007/978-3-642-29044-2.
[42] T. Kosar, S. Bohra, and M. Mernik, "A systematic mapping study driven by the margin of error," *J. Syst. Softw.*, vol. 144, pp. 439–449, 2018, doi: 10.1016/j.jss.2018.06.078.
[43] Z. Syed, A. Padia, T. W. Finin, M. L. Mathews, and A. Joshi, "UCO: A unified cybersecurity ontology," in *Proc. AAAI Workshop: Artif. Intell. Cyber Secur.*, 2016, pp. 1–8. [Online]. Available: https://api.semanticscholar.org/CorpusID:6896947
[44] R. Neupane and H. Mehrpouyan, "An ontology-based framework for formal verification of safety and security properties of control logics," in *Proc. 14th Int. Conf. Electron., Comput. Artif. Intell.*, 2022, pp. 1–8, doi: 10.1109/ECAI54874.2022.9847508.
[45] P. Bhosale, W. Kastner, and T. Sauter, "Integrated safety-security risk assessment for industrial control system: An ontology-based approach," in *Proc. IEEE 28th Int. Conf. Emerg. Technol. Factory Automat.*, 2023, pp. 1–8, doi: 10.1109/ETFA54631.2023.10275530.
[46] X. He, J. Liu, C.-T. Huang, D. Wang, and B. Meng, "A security analysis method of security protocol implementation based on unpurified security protocol trace and security protocol implementation ontology," *IEEE Access*, vol. 7, pp. 131 050–131 067, 2019.
[47] M. Kieviet and P. Iyenghar, "Integration of machine learning safety functions in the ontology of functional safety," in *Proc. IEEE 21st Int. Conf. Ind. Informat.*, 2023, pp. 1–5, doi: 10.1109/INDIN51400.2023.10217928.
[48] S. Wang, M. Li, K. Lu, X. Yao, and S. Wu, "Automatic modeling for Chinese ontology of safety risk knowledge in subway construction projects," in *Proc. Int. Conf. Urban Eng. Manage. Sci.*, 2020, pp. 69–71, doi: 10.1109/ICUEMS50872.2020.00025.
[49] M. Adach, K. Hänninen, and K. Lundqvist, "A combined security ontology based on the unified foundational ontology," in *Proc. IEEE 16th Int. Conf. Semantic Comput.*, 2022, pp. 187–194, doi: 10.1109/ICSC52841.2022.00039.
[50] D. Abdullah, H. Takahashi, and U. Lakhani, "Domain specific ontology enhancing communication accuracy in airport operation," in *Proc. IEEE 14th Int. Symp. Auton. Decentralized Syst.*, 2019, pp. 1–5, doi: 10.1109/ISADS45777.2019.9155591.
[51] C. He and F. Yan, "Research on fault prediction of fully automatic operation system based on ontology and Bayesian network," in *Proc. 34th Chin. Control Decis. Conf.*, 2022, pp. 1434–1439, doi: 10.1109/CCDC55256.2022.10033670.
[52] W. Aman and F. Khan, "Ontology-based dynamic and context-aware security assessment automation for critical applications," in *Proc. IEEE 8th Glob. Conf. Consum. Electron.*, 2019, pp. 644–647, doi: 10.1109/GCCE46687.2019.9015599.
[53] K. Zhang and J. Liu, "Ontology construction for security analysis of network nodes," in *Proc. Int. Conf. Commun., Inf. Syst. Comput. Eng.*, 2020, pp. 292–297, doi: 10.1109/CISCE50729.2020.00065.
[54] Y. Wang, A. Allakany, S. Kulshrestha, W. Shi, R. Bose, and K. Okamura, "Automatically generate e-learning quizzes from IoT security ontology," in *Proc. IEEE 8th Int. Congr. Adv. Appl. Informat.*, 2019, pp. 166–171, doi: 10.1109/IIAI-AAI.2019.00042.
[55] J.-W. Jung, S.-H. Park, and S.-W. Lee, "A tool for security requirements recommendation using case-based problem domain ontology," in *Proc. IEEE 29th Int. Requirements Eng. Conf.*, 2021, pp. 438–439, doi: 10.1109/RE51729.2021.00059.
[56] R. P. Pandey and S. Jebaraj, "Construction of ontology graphs in a cyber security framework (OCSF)," in *Proc. IEEE 6th Int. Conf. Contemporary Comput. Informat.*, 2023, pp. 1885–1889, doi: 10.1109/IC3I59117.2023.10398083.
[57] X. Liang et al., "Ontology based security risk model for power terminal equipment," in *Proc. IEEE 12th Int. Symp. Comput. Intell. Des.*, 2019, pp. 212–216, doi: 10.1109/ISCID.2019.10132.
[58] N. Han and Y. Zhao, "Research on university network security management assistant decision system based on semantic ontology," in *Proc. IEEE 2nd Int. Conf. Inf. Sci. Educ.*, 2021, pp. 1285–1288, doi: 10.1109/ICISE-IE53922.2021.00288.
[59] C. Choi and J. Choi, "Ontology-based security context reasoning for power IoT-cloud security service," *IEEE Access*, vol. 7, pp. 110 510–110 517, 2019.

[60] D. Kouzapas, N. Stylianidis, C. G. Panayiotou, and D. G. Eliades, "Ontology-based reasoning to reconfigure industrial processes for energy efficiency," in *Proc. 31st Mediterranean Conf. Control Automat.*, 2023, pp. 79–84, doi: 10.1109/MED59994.2023.10185805.

[61] A. Pedro, S. Baik, J. Jo, D. Lee, R. Hussain, and C. Park, "A linked data and ontology-based framework for enhanced sharing of safety training materials in the construction industry," *IEEE Access*, vol. 11, pp. 105 410–105 426, 2023.

[62] D. Zhao, J. Sun, X. Chen, X. Bo, M. Yi, and L. Xia, "Semi-automatic construction method of power safety ontology based on AR-K-means," in *Proc. IEEE Int. Conf. Power Electron., Comput. Appl.*, 2021, pp. 59–64, doi: 10.1109/ICPECA51329.2021.9362555.

[63] F. Alsubaei, A. Abuhussein, and S. Shiva, "Ontology-based security recommendation for the Internet of Medical Things," *IEEE Access*, vol. 7, pp. 48 948–48 960, 2019.

[64] C. Islam, M. A. Babar, and S. Nepal, "An ontology-driven approach to automating the process of integrating security software systems," in *Proc. IEEE/ACM Int. Conf. Softw. Syst. Processes*, 2019, pp. 54–63, doi: 10.1109/ICSSP.2019.00017.

[65] P. G.-Gil, A. F. Skarmeta, and J. A. Martinez, "Towards an ontology for IoT context-based security evaluation," in *Proc. Glob. IoT Summit*, 2019, pp. 1–6, doi: 10.1109/GIOTS.2019.8766400.

[66] A. P. Vale and E. B. Fernandez, "An ontology for security patterns," in *Proc. IEEE 38th Int. Conf. Chilean Comput. Sci. Soc.*, 2019, pp. 1–8, doi: 10.1109/SCCC49216.2019.8966393.

[67] M. Kim, S. Dey, and S.-W. Lee, "Ontology-driven security requirements recommendation for APT attack," in *Proc. IEEE 27th Int. Requirements Eng. Conf. Workshops*, 2019, pp. 150–156, doi: 10.1109/REW.2019.00032.

[68] S. Maroc and J. B. Zhang, "Context-aware security evaluation ontology for cloud services," in *Proc. IEEE 4th Adv. Inf. Technol., Electron. Automat. Control Conf.*, 2019, pp. 1012–1018, doi: 10.1109/IAEAC47372.2019.8997783.

[69] A. Canito, K. Aleid, I. Praça, J. Corchado, and G. Marreiros, "An ontology to promote interoperability between cyber-physical security systems in critical infrastructures," in *Proc. IEEE 6th Int. Conf. Comput. Commun.*, 2020, pp. 553–560, doi: 10.1109/ICCC51575.2020.9345163.

[70] V. Casola, R. Catelli, and A. D. Benedictis, "A first step towards an ISO-based information security domain ontology," in *Proc. IEEE 28th Int. Conf. Enabling Technol.: Infrastructure Collaborative Enterprises*, 2019, pp. 334–339, doi: 10.1109/WETICE.2019.00075.

[71] F. Mariotti, M. Tavanti, L. Montecchi, and P. Lollini, "Extending a security ontology framework to model CAPEC attack paths and TAL adversary profiles," in *Proc. 18th Eur. Dependable Comput. Conf.*, 2022, pp. 25–32, doi: 10.1109/EDCC57035.2022.00016.

[72] I. Tomičić and P. Grd, "Towards the open ontology for IoT ecosystem's security," in *Proc. IEEE 43rd Int. Conv. Inf., Commun. Electron. Technol.*, 2020, pp. 1064–1069, doi: 10.23919/MIPRO48935.2020.9245229.

[73] J. Steinmann and O. Ochoa, "Supporting security requirements engineering through the development of the secure development ontology," in *Proc. IEEE 16th Int. Conf. Semantic Comput.*, 2022, pp. 151–158, doi: 10.1109/ICSC52841.2022.00031.

[74] S.-F. Wen, M. M. Yamin, and B. Katt, "Ontology-based scenario modeling for cyber security exercise," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops*, 2021, pp. 249–258, doi: 10.1109/EuroSPW54576.2021.00032.

[75] A. Y.-Ofori, U. M. Ismail, T. Swidurski, and F. O.-Boateng, "Cyber-attack ontology: A knowledge representation for cyber supply chain security," in *Proc. Int. Conf. Comput., Comput. Modelling Appl.*, 2021, pp. 65–70, doi: 10.1109/ICCMA53594.2021.00019.

[76] B. Yankson, "Autonomous vehicle security through privacy integrated context ontology(PICO)," in *Proc. IEEE Int. Conf. Syst., Man, Cybern.*, 2020, pp. 4372–4378, doi: 10.1109/SMC42975.2020.9283180.

[77] D. Tsoukalas, M. Siavvas, M. Mathioudaki, and D. Kehagias, "An ontology-based approach for automatic specification, verification, and validation of software security requirements: Preliminary results," in *Proc. IEEE 21st Int. Conf. Softw. Qual., Rel. Secur. Companion*, 2021, pp. 83–91, doi: 10.1109/QRS-C55045.2021.00022.

[78] A. Shaked and O. Margalit, "Ontorisk–A formal ontology approach to automate cyber security risk identification," in *Proc. 17th Annu. Syst. Syst. Eng. Conf.*, 2022, pp. 74–79, doi: 10.1109/SOSE55472.2022.9812653.

[79] J. Bozic, Y. Li, and F. Wotawa, "Ontology-driven security testing of web applications," in *Proc. IEEE Int. Conf. Artif. Intell. Testing*, 2020, pp. 115–122, doi: 10.1109/AITEST49225.2020.00024.

[80] U. Tefek, E. Esiner, C. Cheh, and D. Mashima, "A smart grid ontology: Vulnerabilities, attacks, and security policies," in *Proc. IEEE Conf. Commun. Netw. Secur.*, 2023, pp. 1–6, doi: 10.1109/CNS59707.2023.10289085.

[81] I. Meriah, L. B. A. Rabai, and R. Khedri, "Towards an automatic approach to the design of a generic ontology for information security," in *Proc. Reconciling Data Analytics, Automat., Privacy, Secur.: A. Big Data Challenge*, 2021, pp. 1–8, doi: 10.1109/RDAAPS48126.2021.9452006.

[82] T. Zhao, U. Lechner, M. P.-Albuquerque, and D. Ongu, "An ontology-based model for evaluating cloud attack scenarios in cats–A serious game in cloud security," in *Proc. IEEE Int. Conf. Eng., Technol. Innov.*, 2023, pp. 1–9, doi: 10.1109/ICE/ITMC58018.2023.10332371.

[83] J. Illescas, L. Ehrlinger, G. Denk, and G. Buchgeher, "Towards an ontology for technical security standards," in *Proc. IEEE 28th Int. Conf. Emerg. Technol. Factory Automat.*, 2023, pp. 1–8, doi: 10.1109/ETFA54631.2023.10275669.

[84] Y. Wang, B. Zhao, W. Li, and L. Zhu, "An ontology-centric approach for network security situation awareness," in *Proc. IEEE 47th Annu. Comput., Softw., Appl. Conf.*, 2023, pp. 777–787, doi: 10.1109/COMPSAC57700.2023.00107.

[85] A. Patel, N. C. Debnath, and P. K. Shukla, "SecureONT: A security ontology for establishing data provenance in semantic web," *J. Web Eng.*, vol. 21, no. 4, pp. 1347–1370, 2022.

[86] K. Farghaly, R. K. Soman, W. Collinge, M. H. Mosleh, P. Manu, and C. M. Cheung, "Construction safety ontology development and alignment with industry foundation classes (IFC)," *J. Inf. Technol. Construction*, vol. 27, pp. 94–108, 2022. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85122752701&doi=10.36680%2fj.itcon.2022.005&partnerID=40&md5=8f4217b3a2ea98f9d3aac1eb2be91002

[87] C. Ukegbu, R. Neupane, and H. Mehrpouyan, "Ontology-based framework for boundary verification of safety and security properties in industrial control systems," in *Proc. Eur. Interdisciplinary Cybersecurity Conf.*, 2023, pp. 47–52, doi: 10.1145/3590777.3590785. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85161431576&doi=10.1145%2f3590777.3590785&partnerID=40&md5=7c64a674688d3adcb84d16695abea3bf

[88] M. Iqbal, A. Kormiltsyn, V. Dwivedi, and R. Matulevičius, "Blockchain-based ontology driven reference framework for security risk management," *Data Knowl. Eng.*, vol. 149, 2024, Art. no. 102257. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85179122332&doi=10.1016%2fj.datak.2023.102257&partnerID=40&md5=493d0f685c50a681e7b3ad2e76b6abb3

[89] C. Blanco, D. G. Rosado, A. J. V.-Vaca, M. T. G.-López, and E. F.-Medina, "Onto-CARMEN: Ontology-driven approach for cyber–physical system security requirements meta-modelling and reasoning," *Internet Things (Netherlands)*, vol. 24, 2023, Art. no. 100989. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85178212443&doi=10.1016%2fj.iot.2023.100989&partnerID=40&md5=7e67d873b1f01b23f07adbf3c7e16fe9

[90] P. Chaudhary, B. Gupta, and A. Singh, "Adaptive cross-site scripting attack detection framework for smart devices security using intelligent filters and attack ontology," *Soft Comput.*, vol. 27, no. 8, pp. 4593–4608, 2023. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85143732475&doi=10.1007%2fs00500-022-07697-2&partnerID=40&md5=1be0f8b21ab2bfb3d44b3a92b15d1754

[91] X. Diao, Y. Zhao, P. K. Vaddi, M. Pietrykowski, M. Khafizov, and C. Smidts, "Multiple aspects maintenance ontology-based intelligent maintenance optimization framework for safety-critical systems," *Artif. Intell. Eng. Des., Anal. Manuf.*, vol. 38, 2024, Art. no. e3. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85183453306&doi=10.1017%2fS0890060423000215&partnerID=40&md5=6e6d57ddab34bdf8da17edb581afd5f6

[92] M. Y. Aghdam, S. R. K. Tabbakh, S. J. M. Chabok, and M. Kheyrabadi, "Ontology generation for flight safety messages in air traffic management," *J. Big Data*, vol. 8, no. 1, 2021, Art. no. 61. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85104841959&doi=10.1186%2fs40537-021-00449-3&partnerID=40&md5=8a44e98aec656c5caa8e7893a80c5cc5

[93] W. Zheng, Z. Cai, P. Cheng, J. Yan, and Y. Xiao, "Research on network security threat analysis technology based on ontology," in *Proc. 3rd Int. Conf. Comput. Eng. Intell. Control*, 2022, pp. 1–5. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85148615112&partnerID=40&md5=d71a5605378149920bf0b64b542fad1f
[94] A. Pedro, A.-T. P.-Hang, P. T. Nguyen, and H. C. Pham, "Data-driven construction safety information sharing system based on linked data, ontologies, and knowledge graph technologies," *Int. J. Environ. Res. Public Health*, vol. 19, no. 2, 2022, Art. no. 794. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85122510565&doi=10.3390%2fijerph19020794&partnerID=40&md5=506cb9a8df6f65dda018482af5d8dbd3
[95] K. N. Durai, R. Subha, and A. Haldorai, "A novel method to detect and prevent SQLIA using ontology to cloud web security," *Wireless Pers. Commun.*, vol. 117, no. 4, pp. 2995–3014, 2021. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85082934164&doi=10.1007%2fs11277-020-07243-z&partnerID=40&md5=790b6f89bc9f7017191810e293e26e0b
[96] B. Liu, J. Yi, L. Yao, Y. Wang, Z. Ding, and X. Zhu, "Situational awareness ontology modeling for threat from space cyber operations," *Syst. Eng. Electron.*, vol. 45, no. 3, pp. 745–754, 2023. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85156117313&doi=10.12305%2fj.issn.1001-506X.2023.03.15&partnerID=40&md5=08b0ebb1734437fb8a5fce2502b2819f
[97] Y. Wu, Z. Li, L. Zhao, Z. Yu, and H. Miao, "Safety ontology modeling and verification on MIS of ship-building and repairing enterprise," *KSII Trans. Internet Inf. Syst.*, vol. 15, no. 4, pp. 1360–1388, 2021. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85105588147&doi=10.3837%2ftiis.2021.04.010&partnerID=40&md5=c5e77e2e01add7528ab9efdd59a46627
[98] I. Fitkau and T. Hartmann, "An ontology-based approach of automatic compliance checking for structural fire safety requirements," *Adv. Eng. Informat.*, vol. 59, 2024, Art. no. 102314. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85180530544&doi=10.1016%2fj.aei.2023.102314&partnerID=40&md5=6b4dc80ee8e750c3579e918619628e82
[99] B. Zhang, W. Yang, S. Ge, and X. Dong, "Construction and application of ontology knowledge base for hydropower plant operation and maintenance," *Shuili Fadian Xuebao/Journal Hydroelectric Eng.*, vol. 41, no. 10, pp. 86–98, 2022. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85142170511&doi=10.11660%2fslfdxb.20221007&partnerID=40&md5=b181c6afb54d13a17530dfa57acc9bb8
[100] O. Can and M. O. Unalir, "Improving data security and privacy for ontology based data access," *Commun. Comput. Inf. Sci.*, vol. 1851, pp. 72–90, 2023. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85169015137&doi=10.1007%2f978-3-031-37807-2_4&partnerID=40&md5=d259bf862672f0e7861cfb3d5e0cfe3c
[101] K. W. Johansen, C. Schultz, and J. Teizer, "Hazard ontology and 4D benchmark model for facilitation of automated construction safety requirement analysis," *Comput.-Aided Civil Infrastructure Eng.*, vol. 38, no. 15, pp. 2128–2144, 2023. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85149397204&doi=10.1111%2fmice.12988&partnerID=40&md5=9c51beb62e859a135c5f140bd5e7b649
[102] Y. Zhou, T. Bao, X. Shu, Y. Li, and Y. Li, "BIM and ontology-based knowledge management for Dam safety monitoring," *Automat. Construction*, vol. 145, 2023, Art. no. 104649. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85141340135&doi=10.1016%2fj.autcon.2022.104649&partnerID=40&md5=fbd0563cca5213872f946a062ffc90f9
[103] A. Yuguchi et al., "Toward robot-agnostic home appliance operation: A task execution framework using motion primitives, ontology, and GUI," *Adv. Robot.*, vol. 36, no. 11, pp. 548–565, 2022. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85130238752&doi=10.1080%2f01691864.2022.2070422&partnerID=40&md5=497078d5ad62626bd75ab6e0491cbf3f
[104] M. Alharbi and H. A. Karimi, "Towards developing an ontology for safety of navigation sensors in autonomous vehicles," in *Proc. 15th Int. Joint Conf. Knowl. Discov., Knowl. Eng. Knowl. Manage.*, 2023, pp. 231–239, doi: 10.5220/0012207300003598. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85179552723&doi=10.5220%2f0012207300003598&partnerID=40&md5=080846cd2604156209760ad615098ad3
[105] Y. Shen, M. Xu, Y. Lin, C. Cui, X. Shi, and Y. Liu, "Safety risk management of prefabricated building construction based on ontology technology in the BIM environment," *Buildings*, vol. 12, no. 6, 2022, Art. no. 765. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85131888906&doi=10.3390%2fbuildings12060765&partnerID=40&md5=ef5c298a3951471eb2506fa29fed11e5
[106] I. Oliveira, T. P. Sales, R. Baratella, M. Fumagalli, and G. Guizzardi, "An ontology of security from a risk treatment perspective," in *Proc. 41st Int. Conf. Conceptual Model.*, 2022, pp. 365–379. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85141712607&doi=10.1007%2f978-3-031-17995-2_26&partnerID=40&md5=a6d1be057992d09ed6b6543848f61417
[107] M. Megaraj et al., "Post lockdown industrial accidents and their safety ontology," *AIP Conf. Proc.*, vol. 2766, no. 1, 2023, Art. no. 020038, doi: 10.1063/5.0139346. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85164206398&doi=10.1063%2f5.0139346&partnerID=40&md5=152a7dec554b231173f6a01d358d9e1b
[108] S. Gao, G. Ren, and H. Li, "Knowledge management in construction health and safety based on ontology modeling," *Appl. Sci. (Switzerland)*, vol. 12, no. 17, 2022, Art. no. 8574. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85139554192&doi=10.3390%2fapp12178574&partnerID=40&md5=09b0e28a17b21cf1f0bdb18e4f002358
[109] S. Saha, W. Li, Z. Usman, and N. Shah, "Core manufacturing ontology to model manufacturing operations and sequencing knowledge," *Serv. Oriented Comput. Appl.*, vol. 17, no. 1, pp. 5–23, 2023. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85146647733&doi=10.1007%2fs11761-022-00355-3&partnerID=40&md5=279d416950b7bd0298765e545050bc94
[110] G. Liu, P. An, Z. Wu, and Z. Hu, "Ontology-based modeling and application of highway engineering safety knowledge," *Qinghua Daxue Xuebao/Journal Tsinghua Univ.*, vol. 64, no. 2, pp. 224–234, 2024. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85181686821&doi=10.16511%2fj.cnki.qhdxxb.2023.22.054&partnerID=40&md5=a58a328fdb1df33ad1422065754cb38f
[111] Q. Shen, S. Wu, Y. Deng, H. Deng, and J. C. P. Cheng, "BIM–based dynamic construction safety rule checking using ontology and natural language processing," *Buildings*, vol. 12, no. 5, 2022, Art. no. 564. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85129765064&doi=10.3390%2fbuildings12050564&partnerID=40&md5=daf30fc785a6b3bd429a37c448e94a48
[112] T. Li, X. Wang, and Y. Ni, "Aligning social concerns with information system security: A fundamental ontology for social engineering," *Inf. Syst.*, vol. 104, 2022, Art. no. 101699. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85098063129&doi=10.1016%2fj.is.2020.101699&partnerID=40&md5=ff64bba4552135aee2dfc24bc9b520e1
[113] M. Adach, K. Hänninen, and K. Lundqvist, "Security ontologies: A systematic literature review," in *Proc. 26th Int. Conf. Enterprise Des., Operations, Comput.*, 2022, pp. 36–53. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85140464807&doi=10.1007%2f978-3-031-17604-3_3&partnerID=40&md5=8179b0f609fd619066cb27e765d0b515
[114] M. Dart and M. Ahmed, "Cyber-AIDD: A novel approach to implementing improved cyber security resilience for large Australian healthcare providers using a unified modelling language ontology," *Digit. Health*, vol. 9, pp. 1–15, 2023. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85167344397&doi=10.1177%2f20552076231191095&partnerID=40&md5=b98b1e4e4653d47f454719957a5aed1d
[115] M. Khaleghi, M. R. Aref, and M. Rasti, "Context-aware ontology-based security measurement model," *J. Inf. Secur. Appl.*, vol. 67, 2022, Art. no. 103199. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85132359076&doi=10.1016%2fj.jisa.2022.103199&partnerID=40&md5=bdafcb5decac0af62ec7b0e54078e34a
[116] S.-F. Wen and B. Katt, "Ontology-based metrics computation for system security assurance evaluation," *J. Appl. Secur. Res.*,

vol. 19, no. 2, pp. 230–275, 2022. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85144311879&doi=10.1080%2f19361610.2022.2157190&partnerID=40&md5=e7ff2196c424a08e8e7295e87025bdcd

[117] P. Becker, M. F. Papa, G. Tebes, and L. Olsina, "Discussing the applicability of a process core ontology and aspects of its internal quality," *Softw. Qual. J.*, vol. 30, no. 4, pp. 1003–1038, 2022. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85130682243&doi=10.1007%2fs11219-022-09592-3&partnerID=40&md5=811fdae322ee3a921b29214b85eb233a

[118] K. A. Akbar, F. I. Rahman, A. Singhal, L. Khan, and B. Thuraisingham, "The design and application of a unified ontology for cyber security," in *Proc. 19th Int. Conf. Inf. Syst. Secur.*, 2023, pp. 23–41. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85180543289&doi=10.1007%2f978-3-031-49099-6_2&partnerID=40&md5=df4c5547d9ecd0a67ebb07a90fef7944

[119] S. Ramanauskaitė, A. Shein, A. Čenys, and J. Rastenis, "Security ontology structure for formalization of security document knowledge," *Electron. (Switzerland)*, vol. 11, no. 7, 2022, Art. no. 1103. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85127354593&doi=10.3390%2felectronics11071103&partnerID=40&md5=8f260c9c8f162dcde9d32724fb10c121

[120] D. Calvanese, A. Gianola, A. Mazzullo, and M. Montali, "SMT safety verification of ontology-based processes," in *Proc. AAAI Conf. Artif. Intell.*, 2023, pp. 6271–6279. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85167872930&partnerID=40&md5=e66fc63cc5c69624b6de1b906821c8bc

[121] G. Kiran and N. Nalini, "Ontology-based data access control model supported with grid computing for improving security in healthcare data," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 11, 2022, Art. no. e4589. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85133639207&doi=10.1002%2fett.4589&partnerID=40&md5=1690696a11d9d5c755685c6b0e60838f

[122] R. Nowrozy and K. Ahmed, "Enhancing health information systems security: An ontology model approach," in *Proc. Health Inf. Sci.: 12th Int. Conf.*, vol. 14305, 2023, pp. 91–100. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85175859153&doi=10.1007%2f978-981-99-7108-4_8&partnerID=40&md5=65619fae1bbb47c25a9b427d64883943

[123] O. Doukari, J. Wakefield, P. Martinez, and M. Kassem, "An ontology-based tool for safety management in building renovation projects," *J. Building Eng.*, vol. 84, 2024, Art. no. 108609. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85183205526&doi=10.1016%2fj.jobe.2024.108609&partnerID=40&md5=b3b4a5e55da0ddfaa2ac2045f945b7c3

[124] H. Zhang, J. Zhu, J. Chen, J. Liu, and L. Ji, "Zero-shot fine-grained entity typing in information security based on ontology [formula presented]," *Knowl.-Based Syst.*, vol. 232, 2021, Art. no. 107472. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85115635724&doi=10.1016%2fj.knosys.2021.107472&partnerID=40&md5=4332190f2defad1ed36abbb9cb8c169f

[125] A. Taher, F. Vahdatikhaki, and A. Hammad, "Formalizing knowledge representation in earthwork operations through development of domain ontology," *Eng., Construction Architectural Manage.*, vol. 29, no. 6, pp. 2382–2414, 2022. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85107798747&doi=10.1108%2fECAM-10-2020-0810&partnerID=40&md5=461586e7757246a6f56179c3a070c7d3

[126] M. Liu, R. Huang, and F. Xu, "Research on the construction of safety information ontology knowledge base and accident reasoning for complex hazardous production systems-taking methanol production process as an example," *Sustainability (Switzerland)*, vol. 15, no. 3, 2023, Art. no. 2568. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85147939207&doi=10.3390%2fsu15032568&partnerID=40&md5=22dfa2d7774d12daef6bc2c80d2021cc

[127] M. Wang, "Ontology-based modelling of lifecycle underground utility information to support operation and maintenance," *Automat. Construction*, vol. 132, 2021, Art. no. 103933. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85114610745&doi=10.1016%2fj.autcon.2021.103933&partnerID=40&md5=97913957ec0e218ba040d6269f2648e2

[128] Y. Liu and Y. Guo, "Towards real-time warning and defense strategy ai planning for cyber security systems aided by security ontology," *Electron. (Switzerland)*, vol. 11, no. 24, 2022, Art. no. 4128. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85144884501&doi=10.3390%2felectronics11244128&partnerID=40&md5=06a502a0e3d89b6304319a3f94d01a54

[129] H. K. Shakya et al., "Internet of Things-based intelligent ontology model for safety purpose using wireless networks," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–8, 2022. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85133976632&doi=10.1155%2f2022%2f1342966&partnerID=40&md5=bb291277ed17373883b14621852e26dd

[130] L. Qasim, A. M. Hein, S. Olaru, J.-L. Garnier, and M. Jankovic, "System reconfiguration ontology to support model-based systems engineering: Approach linking design and operations," *Syst. Eng.*, vol. 26, no. 4, pp. 347–364, 2023. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85147655644&doi=10.1002%2fsys.21661&partnerID=40&md5=8e12025c2ddefc47e1acbbf68296788e

[131] R.-G. Wang, P.-Y. Wu, C.-Y. Liu, J.-C. Tan, M.-L. Chuang, and C.-C. Chou, "Route planning for fire rescue operations in long-term care facilities using ontology and building information models," *Buildings*, vol. 12, no. 7, 2022, Art. no. 1060. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85137335259&doi=10.3390%2fbuildings12071060&partnerID=40&md5=bbc5d95aae5345ad01f12c875169909f

[132] F. Luo, S. Feng, Y. Yang, Z. Ao, X. Li, and Y. Chai, "Ontology modeling method applied in simulation modeling of distribution network time series operation," *Front. Energy Res.*, vol. 10, 2022, Art. no. 935026. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85139554548&doi=10.3389%2ffenrg.2022.935026&partnerID=40&md5=8e5da3a33f3cd103a6063a831cbcb3aa

[133] M. Heydari, H. Mouratidis, and V. H. F. Tafreshi, "OntoCyrene: Towards ontology-enhanced asset modelling for supply chains in the context of cyber security," in *Proc. Comput. Secur.. ESORICS Int. Workshops*, 2023, pp. 157–176. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85151049708&doi=10.1007%2f978-3-031-25460-4_9&partnerID=40&md5=b66cb8a29b50eea514ff5e6af127eaac

[134] D. Varvarigou, D. Espes, and G. Bersano, "Ontology-based solution for handling safety and cybersecurity interdependency in NFV safety architecture," *Procedia Comput. Sci.*, vol. 220, pp. 527–534, 2023, doi: 10.1016/j.procs.2023.03.067. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85164484838&doi=10.1016%2fj.procs.2023.03.067&partnerID=40&md5=6bf71d6920e65e55ed92bd3fd6e2bf22

[135] I. Williams, X. Yuan, M. Anwar, and J. T. McDonald, "An automated security concerns recommender based on use case specification ontology," *Automated Softw. Eng.*, vol. 29, no. 2, 2022, Art. no. 42. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85131887182&doi=10.1007%2fs10515-022-00334-0&partnerID=40&md5=82f51fc1fd8c888a702cce102ed96e51

[136] Z. Wu, J. C. P. Cheng, and Z. Wang, "An ontology-based framework for building energy simulation in the operation phase," *Lecture Notes Civil Eng.*, vol. 357, pp. 351–366, 2024. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85174719864&doi=10.1007%2f978-3-031-35399-4_27&partnerID=40&md5=03be9350020954814eaa9651dbb55cc7

[137] V. Kukkonen, A. Kücükavci, M. Seidenschnur, M. H. Rasmussen, K. M. Smith, and C. A. Hviid, "An ontology to support flow system descriptions from design to operation of buildings," *Automat. Construction*, vol. 134, 2022, Art. no. 104067. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85120734912&doi=10.1016%2fj.autcon.2021.104067&partnerID=40&md5=99b10d2e88f97c3c8bc022ebcd37d8d1

[138] Y. Deng, Y. Zhang, L. Luo, Y. Li, and L. Lin, "Research on subway operation safety risk management based on ontology technology," *China Saf. Sci. J.*, vol. 33, pp. 35–41, 2023. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85175977277&doi=10.16265%2fj.cnki.issn1003-3033.2023.S1.2536&partnerID=40&md5=4a83acde32c112cc479038edf45e1342

[139] B.-J. Kim and S.-W. Lee, "Understanding and recommending security requirements from problem domain ontology: A cognitive three-layered approach," *J. Syst. Softw.*, vol. 169, 2020, Art. no. 110695. [Online]. Available: https://www.scopus.com/inward/

record.uri?eid=2-s2.0-85086587944&doi=10.1016%2fj.jss.2020.110695&partnerID=40&md5=533147a9762e34955b4c6dbbf582d9a5

[140] M. R. Faria, G. B. d. Figueiredo, K. d. F. Cordeiro, M. C. Cavalcanti, and M. L. M. Campos, "Applying multi-level theory to an information security incident domain ontology," in *Proc. CEUR Workshop*, 2019, pp. 1–12. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85077562452&partnerID=40&md5=d217be3e22c7d61ceb62480d67542c7c

[141] I. Fitkau and T. Hartmann, "Building ontology for preventive fire safety," in *Proc. 28th Int. Workshop Intell. Comput. Eng. Eur. Group Intell. Comput. Eng.*, 2021, pp. 218–227. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85134257665&partnerID=40&md5=cd4427bc3d7cb15f0fdbb92ff818897a

[142] M. Alenezi, "Ontology-based context-sensitive software security knowledge management modeling," *Int. J. Elect. Comput. Eng.*, vol. 10, no. 6, pp. 6507–6520, 2020. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85092158827&doi=10.11591%2fIJECE.V10I6.PP6507-6520&partnerID=40&md5=36843e89607ec9bdf2096a966e3c32fd

[143] P. G.-Gil, J. A. Martinez, and A. F. Skarmeta, "Lightweight data-security ontology for IoT," *Sensors (Switzerland)*, vol. 20, no. 3, 2020, Art. no. 801. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85079030976&doi=10.3390%2fs20030801&partnerID=40&md5=4f446aaf55530da4d6c269794870f7d8

[144] S. Veloudis et al., "Achieving security-by-design through ontology-driven attribute-based access control in cloud environments," *Future Gener. Comput. Syst.*, vol. 93, pp. 373–391, 2019. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85056484265&doi=10.1016%2fj.future.2018.08.042&partnerID=40&md5=c9a109c52384b1710edee8ea39143ab7

[145] A. Lališ, R. Patriarca, J. Ahmad, G. D. Gravio, and B. Kostov, "Functional modeling in safety by means of foundational ontologies," *Transport. Res. Procedia*, vol. 43, pp. 290–299, 2019, doi: 10.1016/j.trpro.2019.12.044. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85084937697&doi=10.1016%2fj.trpro.2019.12.044&partnerID=40&md5=5c3abef7fa521875753fbdcb768410f2

[146] G. M. Kiran and N. Nalini, "Enhanced security-aware technique and ontology data access control in cloud computing," *Int. J. Commun. Syst.*, vol. 33, no. 15, 2020, Art. no. e4554. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85089403928&doi=10.1002%2fdac.4554&partnerID=40&md5=cbfd87b4c85c4af498c643de5487ae62

[147] A. Dourgnon, A. Antoine, and M. Samba, "Ontologies combining design semantics and semantics used in operation and maintenance: Feedback from EDF power plants case studies," in *Proc. Interoperability Enterprise Syst. Appl. Workshops*, 2020, Art. no. hal-03560236. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85109615541&partnerID=40&md5=acd8ee22ce9809f8b27aeae3e69d6744

[148] S.-F. Wen and B. Katt, "Managing software security knowledge in context: An ontology based approach," *Inf. (Switzerland)*, vol. 10, no. 6, 2019, Art. no. 216. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85069850847&doi=10.3390%2fINFO10060216&partnerID=40&md5=5c8dea433c85d391d089f755af6b4942

[149] P. Hughes, R. Robinson, M. F.-Esteban, and C. v. Gulijk, "Extracting safety information from multi-lingual accident reports using an ontology-based approach," *Saf. Sci.*, vol. 118, pp. 288–297, 2019. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85065928257&doi=10.1016%2fj.ssci.2019.05.029&partnerID=40&md5=35ed3d6303010988c7e2099570a9293a

[150] S.-F. Wen and B. Katt, "Development of ontology-based software security learning system with contextualized learning approach," *J. Adv. Inf. Technol.*, vol. 10, no. 3, pp. 81–90, 2019. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85119878519&doi=10.12720%2fjait.10.3.81-90&partnerID=40&md5=1f7ee6ff344115056f185b76621a7653

[151] M. Katsantonis and I. Mavridis, "Ontology-based modelling for cyber security E-learning and training," in *Proc. 18th Int. Conf. Web-Based Learn.*, 2019, pp. 15–27. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85076783987&doi=10.1007%2f978-3-030-35758-0_2&partnerID=40&md5=3fc9eb24499a05924d31dccd2bbaa395

[152] D. P. Pereira, C. Hirata, and S. N.-Tehrani, "A stamp-based ontology approach to support safety and security analyses," *J. Inf. Secur. Appl.*, vol. 47, pp. 302–319, 2019. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85066634864&doi=10.1016%2fj.jisa.2019.05.014&partnerID=40&md5=71092fe8bb1f5987d456b8afafe33771

[153] X. Wang, H. Wei, N. Chen, X. He, and Z. Tian, "An observational process ontology-based modeling approach for water quality monitoring," *Water (Switzerland)*, vol. 12, no. 3, 2020, Art. no. 715. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85082673059&doi=10.3390%2fw12030715&partnerID=40&md5=fe32e4764b010cd044bffcbe95a87dd1

[154] C. Gróf and A. Kamtsiuris, "Ontology-based process reengineering to support digitalization of MRO operations: Application to an aviation industry case," *Procedia CIRP*, vol. 104, pp. 1322–1327, 2021, doi: 10.1016/j.procir.2021.11.222. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85121574511&doi=10.1016%2fj.procir.2021.11.222&partnerID=40&md5=b5ff41d2912d16499131439ee4daf30c

[155] C. Pénicaud et al., "Relating transformation process, eco-design, composition and sensory quality in cheeses using PO^2 ontology," *Int. Dairy J.*, vol. 92, pp. 1–10, 2019. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85060920902&doi=10.1016%2fj.idairyj.2019.01.003&partnerID=40&md5=6027dc9bd4ce01a2b71df8049b135ffb

[156] C. Brecher, M. Buchsbaum, F. Ziegler, and S. Storms, "Ontology-based data management for adaptable safety functions in cyber-physical production systems," *Procedia CIRP*, vol. 104, pp. 194–199, 2021, doi: 10.1016/j.procir.2021.11.033. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85121647139&doi=10.1016%2fj.procir.2021.11.033&partnerID=40&md5=952b1d2c847777fb72ef4b566399c923

[157] H. Park and R. Liu, "Improving for construction safety design: Ontology model of a knowledge system for the prevention of falls," in *Proc. Construction Res. Congress*, 2020, pp. 463–471, doi: 10.1061/9780784482872.050 [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85096940008&doi=10.1061%2f9780784482872.050&partnerID=40&md5=462147325aa3502123f08256134efdd6

[158] D. Mandal and C. Mazumdar, "Towards an ontology for enterprise level information security policy analysis," in *Proc. 7th Int. Conf. Inf. Syst. Secur. Privacy*, 2021, pp. 492–499, doi: 10.5220/0010248004920499. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85176302606&doi=10.5220%2f0010248004920499&partnerID=40&md5=28c399934dd94ff32f272f956ddd1db6

[159] W. Lin and R. Haga, "Matching cyber security ontologies through genetic algorithm-based ontology alignment technique," *Secur. Commun. Netw.*, vol. 2021, pp. 1–7, 2021. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85121594979&doi=10.1155%2f2021%2f4856265&partnerID=40&md5=19d7fc11b6a7dc4ba2193b75dd4758e6

[160] X. Wang, J. Zhu, X. Meng, and Y. He, "A model of safety monitoring and early warning for coal mine based on ontology and association rules," *Mining Saf. Environ. Protection*, vol. 46, no. 3, pp. 27–31, 2019. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85097821194&partnerID=40&md5=04766f300179cd003b5fc692497407bc

[161] T. Grant, C. v. Wout, and B. v. Niekerk, "An ontology for cyber ISTAR in offensive cyber operations," in *Proc. 19th Eur. Conf. Cyber Warfare Secur.*, 2020, pp. 117–125, doi: 10.34190/EWS.20.066. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85094680232&doi=10.34190%2fEWS.20.066&partnerID=40&md5=0afcf50899d1531b26491ced2eca70ae

[162] I. Meriah and L. B. A. Rabai, "Comparative study of ontologies based iso 27000 series security standards," *Procedia Comput. Sci.*, vol. 160, pp. 85–92, 2019, doi: 10.1016/j.procs.2019.09.447. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85079103610&doi=10.1016%2fj.procs.2019.09.447&partnerID=40&md5=75597c3591270173bb5b2edb3b10d839

[163] M. A. Butakova, A. V. Chernov, I. K. Savvas, and G. Garani, "Data warehouse design for security applications using distributed ontology-based knowledge representation," *Stud. Comput. Intell.*, vol. 868, pp. 140–145, 2020. [Online].

Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85075553142&doi=10.1007%2f978-3-030-32258-8_16&partnerID=40&md5=8c766af1906dd05c80036ed3a58c55d0
[164] A.-M. Koufakis et al., "OntoAqua: Ontology-based modelling of context in water safety and security," in *Proc. 13th Int. Conf. Knowl. Eng. Ontol. Develop.*, 2021, pp. 194–201. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85146200297&partnerID=40&md5=ff251e6dcd9fbc4fa91361d6db007165
[165] I. Tomicic and P. Grd, "Towards the open ontology for IoT ecosystem's security," in *Proc. 43rd Int. Conv. Inf., Commun. Electron. Technol.*, 2020, pp. 1064–1069, doi: 10.23919/MIPRO48935.2020.9245229. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85097236136&doi=10.23919%2fMIPRO48935.2020.9245229&partnerID=40&md5=ef8b1558b3d0f20c9a465a1dec5dc844
[166] M. A. E.-Dosuky and G. H. Eladl, "DOORchain: Deep ontology-based operation research to detect malicious smart contracts," *Ad. Intell. Syst. Comput.*, vol. 930, pp. 538–545, 2019. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85064882628&doi=10.1007%2f978-3-030-16181-1_51&partnerID=40&md5=e94061b3b98fed9aa530954a08b5d2be
[167] A. Taher, F. Vahdatikhaki, and A. Hammad, "Integrating earthwork ontology and safety regulations to enhance operations safety," in *Proc. New Knowl. Inf. Syst. Technol.*, 2019, pp. 477–484, doi: 10.22260/isarc2019/0064. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85071439464&doi=10.22260%2fisarc2019%2f0064&partnerID=40&md5=be36d4dc8810813a3e844fc13d75a912
[168] S. Sarkar and S. Das, "Security knowledge representation of e-government data centre through ontology," *Electron. Government*, vol. 16, no. 4, pp. 379–409, 2020. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85094895219&doi=10.1504%2fEG.2020.110602&partnerID=40&md5=98edbaacdb42b04ebd031f3ad854bfa9
[169] D. Calvanese, A. Gianola, A. Mazzullo, and M. Montali, "SMT-based safety verification of data-aware processes under ontologies (preliminary results)," in *Proc. 34th Int. Workshop Description Logics*, 2021, pp. 1–15. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85114444874&partnerID=40&md5=5f4e2a8fdcf754c1919649bcea379354
[170] F. Patzer and J. Beyerer, "Efficient semantic representation of network access control configuration for ontology-based security analysis," in *Proc. 7th Int. Conf. Inf. Syst. Secur. Privacy*, 2021, pp. 550–557. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85103004714&partnerID=40&md5=dd8d5ed30bc5724ab039e7428e9d588 d
[171] A. M. Shaaban, C. Schmittner, G. Quirchmayr, A. B. Mohamed, T. Gruber, and E. Schikuta, "Toward the ontology-based security verification and validation model for the vehicular domain," *Commun. Comput. Inf. Sci.*, vol. 1142, pp. 521–529, 2019. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85089617493&doi=10.1007%2f978-3-030-36808-1_57&partnerID=40&md5=4df099216965a95f489c23aa17b2b41e
[172] S. Ghalibafan, B. Behkamal, M. Kahani, and M. Allahbakhsh, "An ontology-based method for improving the quality of process event logs using database bin logs," *Int. J. Metadata, Semantics Ontol.*, vol. 14, no. 4, pp. 279–289, 2020. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85108026470&partnerID=40&md5=421d5058e99afdd9b0447980f05ba131
[173] S. Badawi, S. N. Ciolofan, N. G. Badr, and M. Drăgoicea, "A service ecosystem ontology perspective: SDG implementation mechanisms in public safety," *Lecture Notes Bus. Inf. Process.*, vol. 377, pp. 304–318, 2020. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85080902850&doi=10.1007%2f978-3-030-38724-2_22&partnerID=40&md5=f8a70b5b0f77e2f944eb2cd99a1c231e
[174] M. Rodríguez and J. Laguía, "An ontology for process safety," *Chem. Eng. Trans.*, vol. 77, pp. 67–72, 2019. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85073455112&doi=10.3303%2fCET1977012&partnerID=40&md5=39076e06b5218361ca1b4c64fb433e31
[175] S. A.-Lamallam, I. Sebari, R. Yaagoubi, and O. Doukari, "IFCInfra4OM: An ontology to integrate operation and maintenance information in highway information modelling," *ISPRS Int. J. Geo- Inf.*, vol. 10, no. 5, 2021, Art. no. 305. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85106498120&doi=10.3390%2fijgi10050305&partnerID=40&md5=a43905a559ab70ec39f9c6631d3ac658
[176] Z. Fan, C. Tan, and X. Li, "A hierarchical method for assessing cyber security situation based on ontology and fuzzy cognitive maps," *Int. J. Inf. Comput. Secur.*, vol. 14, no. 3–4, pp. 242–262, 2021. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85105635788&doi=10.1504%2fijics.2021.114704&partnerID=40&md5=7eb78d5044f6eab57dd5c04292d6dade
[177] M. Ledvinka, A. Lališ, and P. Křemen, "Toward data-driven safety: An ontology-based information system," *J. Aerosp. Inf. Syst.*, vol. 16, no. 1, pp. 22–36, 2019. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85066781305&doi=10.2514%2f1.I010622&partnerID=40&md5=56b3b5f9972f9dedae1c95fadd8b182a
[178] M. R. Machado and M. P. Bax, "Using ontology to assist in cyber security assessment of critical infrastructure in the energy sector: Brazilian perspective; [utilização de ontologia para auxílio na avaliação de segurança cibernética da infraestrutura crítica do setor elétrico: Perspectiva brasileira]," in *Proc. CEUR Workshop Proc.*, 2020, pp. 292–297. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85096111638&partnerID=40&md5=26189898de999575c28b485cf642a0d7
[179] O. T. Arogundade, A. A.-Alli, and S. Misra, "An ontology-based security risk management model for information systems," *Arabian J. Sci. Eng.*, vol. 45, no. 8, pp. 6183–6198, 2020. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85084131553&doi=10.1007%2fs13369-020-04524-4&partnerID=40&md5=886a079801d42adecaf4c79d5431c8bf
[180] X. Xing, B. Zhong, H. Luo, H. Li, and H. Wu, "Ontology for safety risk identification in metro construction," *Comput. Ind.*, vol. 109, pp. 14–30, 2019. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85063985495&doi=10.1016%2fj.compind.2019.04.001&partnerID=40&md5=2937f16234a4a875e8e54bd747279899
[181] D. Mandal and C. Mazumdar, "Towards an ontology for enterprise level information security policy analysis," in *Proc. 7th Int. Conf. Inf. Syst. Secur. Privacy*, 2021, pp. 492–499. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85102992993&partnerID=40&md5=7c27542c8e355ce9ff9ce695afea944b
[182] F.-Z. Hannou, F. Atigui, N. Lammari, and S. S.-s. Cherfi, "Safecare-Onto: A cyber-physical security ontology for healthcare systems," in *Proc. 32nd Int. Conf. Database Expert Syst. Appl.*, 2021, pp. 22–34. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85115248312&doi=10.1007%2f978-3-030-86475-0_3&partnerID=40&md5=9b179ab978a1edf0fed6975b3d5b7d71
[183] A. Brazhuk and E. Olizarovich, "Format and usage model of security patterns in ontology-driven threat modelling," in *Proc. 18th Russian Conf. Artif. Intell.*, 2020, pp. 382–392. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85092136990&doi=10.1007%2f978-3-030-59535-7_28&partnerID=40&md5=30fdcc3c40724a866f1ff9321b368257
[184] I. Williams and X. Yuna, "Identifying security concerns based on a use case ontology framework," in *Proc. Int. Conf. Softw. Eng. Knowl. Eng.*, 2020, pp. 83–88, doi: 10.18293/SEKE2020-136. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85090510385&doi=10.18293%2fSEKE2020-136&partnerID=40&md5=aa66f802e21b1e58aa2e3cb2db9f042f
[185] Y. Xu, Y. Huang, L. Xiong, S. Leng, and X. Zhu, "Model building approach for nuclear power operation procedure based on ontology," *Hedongli Gongcheng/Nuclear Power Eng.*, vol. 41, no. 5, pp. 142–145, 2020. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85093512366&doi=10.13832%2fj.jnpe.2020.05.0142&partnerID=40&md5=24a2de46f1f81dd546a7e20ff9c9a4e9
[186] A. M. Shaaban, C. Schmittner, and T. Gruber, "Tackling the challenges of IoT security testing using ontologies," in *Proc. Innov. Trans. Digit. World - 27th Interdiscipl. Inf. Manage. Talks*, 2019, pp. 411–418. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85071471419&partnerID=40&md5=e0e22b8bfa97e324f05bbadb05f80479
[187] M. Iqbal and R. Matulevičius, "Corda security ontology: Example of post-trade matching and confirmation," *Baltic J. Modern Comput.*, vol. 8, no. 4, pp. 638–674, 2021. [Online].

Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85099197402&doi=10.22364%2fBJMC.2020.8.4.11&partnerID=40&md5=e5da28c261c17d98b6afb45658b1784 d

[188] X. Jiang, S. Wang, J. Wang, S. Lyu, and M. Skitmore, "A decision method for construction safety risk management based on ontology and improved CBR: Example of a subway project," *Int. J. Environ. Res. Public Health*, vol. 17, no. 11, 2020, Art. no. 3928. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85086008384&doi=10.3390%2fijerph17113928&partnerID=40&md5=b25cd4bd723c64d99057fde31aa9c4ce

[189] F. Patzer and J. Beyerer, "Efficient semantic representation of network access control configuration for ontology-based security analysis," in *Proc. 7th Int. Conf. Inf. Syst. Secur. Privacy*, 2021, pp. 550–557, doi: 10.5220/0010285305500557. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85176298921&doi=10.5220%2f0010285305500557&partnerID=40&md5=019a2dd9a25790fa87b72a83dd0839b7

[190] A. Shifa, M. N. Asghar, M. Fleury, and M. S. Afgan, "Ontology-based intelligent security framework for smart video surveillance," *Adv. Intell. Syst. Comput.*, vol. 881, pp. 118–126, 2019. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85055915059&doi=10.1007%2f978-3-030-02683-7_10&partnerID=40&md5=01db85d62500080b3a84dd0256474ae5

[191] R. Garcia, H. Harris, M. Beach, D. Couch, and S. U. Khan, "UAS integration safety and security technology ontology," in *Proc. Int. Conf. Res. Adaptive Convergent Syst.*, 2023, pp. 1–6, doi: 10.1145/3599957.3606210.

[192] D. Stefanidis et al., "The ICARUS ontology: A general aviation ontology developed using a multi-layer approach," in *Proc. 10th Int. Conf. Web Intell., Mining Semantics*, 2020, pp. 21–32, doi: 10.1145/3405962.3405983.

[193] C. Ukegbu, R. Neupane, and H. Mehrpouyan, "Ontology-based framework for boundary verification of safety and security properties in industrial control systems," in *Proc. Eur. Interdiscipl. Cybersecurity Conf.*, 2023, pp. 47–52, doi: 10.1145/3590777.3590785.

[194] E. Doynikova, A. Fedorchenko, and I. Kotenko, "Ontology of metrics for cyber security assessment," in *Proc. 14th Int. Conf. Availability, Rel. Secur.*. 2019, pp. 1–8, doi: 10.1145/3339252.3341496.

[195] J. Stang, D. Walther, and P. Myrseth, "Data quality as a microservice: An ontology and rule based approach for quality assurance of sensor data in manufacturing machines," in *Proc. 2nd Int. Workshop Softw. Eng. AI Data Qual. Cyber-Phys. Syst./Internet Things*, 2022, pp. 3–9, doi: 10.1145/3549037.3561272.

[196] G. Engelberg, M. Fumagalli, A. Kuboszek, D. Klein, P. Soffer, and G. Guizzardi, "An ontology-driven approach for process-aware risk propagation," in *Proc. 38th ACM/SIGAPP Symp. Appl. Comput.*, 2023, pp. 1742–1745, doi: 10.1145/3555776.3577795.

[197] A. M. Shaaban, C. Schmittner, T. Gruber, A. B. Mohamed, G. Quirchmayr, and E. Schikuta, "Ontology-based model for automotive security verification and validation," in *Proc. 21st Int. Conf. Inf. Integration Web-Based Appl. Serv.*, 2020, pp. 73–82, doi: 10.1145/3366030.3366070.

[198] H. Fei, C. Youling, and X. Dongsheng, "Formal description of manufacturing process based on domain ontology construction," in *Proc. 2nd World Symp. Softw. Eng.*, 2020, pp. 246–251, doi: 10.1145/3425329.3425377.

[199] Z. Liu et al., "STIX-based network security knowledge graph ontology modeling method," in *Proc. 3rd Int. Conf. Geoinformatics Data Anal.*, 2020, pp. 152–157, doi: 10.1145/3397056.3397083.

[200] A. M. Shaaban, T. Gruber, and C. Schmittner, "Ontology-based security tool for critical cyber-physical systems," in *Proc. 23rd Int. Syst. Softw. Product Line Conf.*, 2019, pp. 207–210, doi: 10.1145/3307630.3342397.

[201] R. Delabeye, O. Penas, and R. Plateaux, "Scalable ontology-based V&V process for heterogeneous systems and applications," in *Proc. 25th Int. Conf. Model Driven Eng. Lang. Syst.: Companion Proc.*, 2022, pp. 341–350, doi: 10.1145/3550356.3561577.

[202] B. Liu, J. Wu, L. Yao, and Z. Ding, "Ontology-based fault diagnosis: A decade in review," in *Proc. 11th Int. Conf. Comput. Model. Simul.*, 2019, pp. 112–116, doi: 10.1145/3307363.3307381.

[203] S.-F. Wen and B. Katt, "Preliminary evaluation of an ontology-based contextualized learning system for software security," in *Proc. 23rd Int. Conf. Eval. Assessment Softw. Eng.*, 2019, pp. 90–99, doi: 10.1145/3319008.3319017.

[204] N. Voit, S. Kirillov, and S. Bochkov, "Converting diagram to a timeline ontology," in *Proc. 2020 6th Int. Conf. Comput. Technol. Appl.*, 2020, pp. 80–86, doi: 10.1145/3397125.3397151.

[205] M. Thinyane and D. Christine, "SMART citizen cyber resilience (SC2R) ontology," in *Proc. 13th Int. Conf. Secur. Inf. Netw.*, 2021, pp. 1–8, doi: 10.1145/3433174.3433617.

[206] P. Tsoutsa, P. Fitsilis, and O. Iatrellis, "Towards an ontology for smart city competences," in *Proc. 25th Pan-Hellenic Conf. Inform.*, 2022, pp. 254–259, doi: 10.1145/3503823.3503871.

[207] N. Chichkova, A. Begler, and V. Vlasov, "Modeling city land use with an ontology," in *Proc. 13th Int. Conf. Theory Pract. Electron. Governance*, 2020, pp. 851–854, doi: 10.1145/3428502.3428638.

[208] J. Hviid, A. Johansen, F. C. Sangogboye, and M. B. Kjærgaard, "OPM: An ontology-based package manager for building operating systems," in *Proc. 11th Int. Conf. Internet Things*, 2022, pp. 118–125, doi: 10.1145/3494322.3494338.

[209] Z. Zhou, Y. Chen, R. Wu, and J. Tao, "Ontology-based case representation of mechatronic product eco-design and development of a cloud-based case library," in *Proc. 7th Int. Conf. Comput. Sci. Appl. Eng.*, 2023, pp. 1–7, doi: 10.1145/3627915.3627925.

[210] R. Christian, S. Dutta, Y. Park, and N. Rastogi, "An ontology-driven knowledge graph for android malware," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2021, pp. 2435–2437, doi: 10.1145/3460120.3485353.

[211] Q. Ismail, O. Saleh, M. Hashayka, A. Awad, A. Hawash, and O. Othman, "Improve the firewall accuracy by using dynamic ontology," in *Proc. 4th Int. Conf. Future Netw. Distrib. Syst.*, 2021, pp. 1–5, doi: 10.1145/3440749.3442607.

[212] R. Islam, T. Cerny, and D. Shin, "Ontology-based user privacy management in smart grid," in *Proc. 37th ACM/SIGAPP Symp. Appl. Comput.*, 2022, pp. 174–182, doi: 10.1145/3477314.3508383.

[213] X. Xue, C. Jiang, C. Yang, H. Zhu, and C. Hu, "Artificial neural network based sensor ontology matching technique," in *Proc. Web Conf.*, 2021, pp. 44–51, doi: 10.1145/3442442.3451138.

[214] A. Zaji, Z. Liu, T. Bando, and L. Zhao, "Ontology-based driving simulation for traffic lights optimization," *ACM Trans. Intell. Syst. Technol.*, vol. 14, no. 3, pp. 1–26, Mar. 2023, doi: 10.1145/3579839.

[215] M. Charalambous et al., "Analyzing coverages of cyber insurance policies using ontology," in *Proc. 17th Int. Conf. Availability, Rel. Secur.*. 2022, pp. 1–7, doi: 10.1145/3538969.3544453.

[216] Y. Pikus, N. Weißenberg, B. Holtkamp, and B. Otto, "Semi-automatic ontology-driven development documentation: Generating documents from RDF data and DITA templates," in *Proc. 34th ACM/SIGAPP Symp. Appl. Comput.*, 2019, pp. 2293–2302, doi: 10.1145/3297280.3297508.

[217] F. He, D. Wang, and Y. Sun, "Ontology integration for building systems and energy storage systems," in *Proc. 10th ACM Int. Conf. Syst. Energy-Efficient Buildings, Cities, Transp.*, 2023, pp. 212–215, doi: 10.1145/3600100.3623720.

[218] A. Afanasyev, N. Voit, M. Ukhanova, S. Kirillov, and S. Bochkov, "Ontology-based organizational and technical components semantic model development," in *Proc. 3rd Int. Conf. Geoinformatics Data Anal.*, 2020, pp. 163–167, doi: 10.1145/3397056.3397089.

[219] Y. Merah and T. Kenaza, "Ontology-based cyber risk monitoring using cyber threat intelligence," in *Proc. 16th Int. Conf. Availability, Rel. Secur.*. 2021, pp. 1–8, doi: 10.1145/3465481.3470024.

[220] D. S. Chang, G. H. Cho, and Y. S. Choi, "Ontology-based knowledge model for human-robot interactive services," in *Proc. 35th Annu. ACM Symp. Appl. Comput.*, 2020, pp. 2029–2038, doi: 10.1145/3341105.3373977.

[221] M. F. Arruda and R. F. B. Neto, "Toward a lightweight ontology for privacy protection in IoT," in *Proc. 34th ACM/SIGAPP Symp. Appl. Comput.*, 2019, pp. 880–888, doi: 10.1145/3297280.3297367.

[222] M. Cornelis, Y. Vanommeslaeghe, B. V. Acker, and P. D. Meulenaere, "An ontology DSL for the co-design of mechatronic systems," in *Proc. 25th Int. Conf. Model Driven Eng. Lang. Syst.: Companion Proc.*, 2022, pp. 633–642, doi: 10.1145/3550356.3561534.

[223] A. T. Orozco, A. Mouakher, I. B. Sassi, and C. Nicolle, "An ontology-based thermal comfort management system in smart buildings," in *Proc. 11th Int. Conf. Manage. Digit. EcoSystems*, 2020, pp. 300–307, doi: 10.1145/3297662.3365824.

[224] P. S. S. Júnior, J. a. P. A. Almeida, and M. Barcellos, "Towards federated ontology-driven data integration in continuous software engineering," in *Proc. 37th Braz. Symp. Softw. Eng.*, 2023, pp. 31–36, doi: 10.1145/3613372.3613380.

[225] S. S. L. Chukkapalli, S. B. Aziz, N. Alotaibi, S. Mittal, M. Gupta, and M. Abdelsalam, "Ontology driven ai and access control systems for smart fisheries," in *Proc. ACM Workshop Secure Trustworthy Cyber-Physical Syst.*, 2021, pp. 59–68, doi: 10.1145/3445969.3450429.

[226] A. Mor, M. Kumar, and S. Chaudhury, "Smart city umbrella ontology: Context -driven framework for traffic planning," in *Proc. 13th Annu. Meeting Forum Inf. Retrieval Eval.*, 2022, pp. 83–90, doi: 10.1145/3503162.3503170.

[227] J. Cerqueira, "An ontology for context-aware middleware for dependable medical systems," in *Proc. 11th Latin-Amer. Symp. Dependable Comput.*, 2023, pp. 79–83, doi: 10.1145/3569902.3569947.

[228] V. S. C. Putrevu, H. Chunduri, M. A. Putrevu, and S. Shukla, "A framework for advanced persistent threat attribution using zachman ontology," in *Proc. Eur. Interdiscipl. Cybersecurity Conf.*, 2023, pp. 34–41, doi: 10.1145/3590777.3590783.

[229] E. Negm, S. Makady, and A. Salah, "Towards ontology-based domain specific language for Internet of Things," in *Proc. 9th Int. Conf. Softw. Inf. Eng.*, 2021, pp. 146–151, doi: 10.1145/3436829.3436833.

[230] B. Wang, J. Luo, and S. Zhu, "Research on domain ontology automation construction based on Chinese texts," in *Proc. 8th Int. Conf. Softw. Comput. Appl.*, 2019, pp. 425–430, doi: 10.1145/3316615.3316685.

[231] O. S. Oguz, W. Rampeltshammer, S. Paillan, and D. Wollherr, "An ontology for human-human interactions and learning interaction behavior policies," *J. Hum.-Robot Interact.*, vol. 8, no. 3, pp. 1–26, Jul. 2019, doi: 10.1145/3326539.

[232] T. Gupta and S. Sural, "Ontology-based evaluation of abac policies for inter-organizational resource sharing," in *Proc. 9th ACM Int. Workshop Secur. Privacy Analytics*, 2023, pp. 85–94, doi: 10.1145/3579987.3586572.

[233] A. Belhadi, Y. Djenouri, G. Srivastava, and J. C.-W. Lin, "Fast and accurate framework for ontology matching in Web of Things," *ACM Trans. Asian Low-Resour. Lang. Inf. Process.*, vol. 22, no. 5, pp. 1–19, May 2023, doi: 10.1145/3578708.

[234] R. Niyazova, A. Aktayeva, and L. Davletkireeva, "An ontology based model for user profile building using social network," in *Proc. 5th Int. Conf. Eng. MIS*, 2019, pp. 1–4, doi: 10.1145/3330431.3330453.

[235] K. A. Akbar, S. M. Halim, A. Singhal, B. Abdeen, L. Khan, and B. Thuraisingham, "The design of an ontology for ATT&CK and its application to cybersecurity," in *Proc. 13th ACM Conf. Data Appl. Secur. Privacy*, 2023, pp. 295–297, doi: 10.1145/3577923.3585051.

[236] Y. Huang, S. Dhouib, L. P. Medinacelli, and J. Malenfant, "Enabling semantic interoperability of asset administration shells through an ontology-based modeling method," in *Proc. 25th Int. Conf. Model Driven Eng. Lang. Syst.: Companion Proc.*, 2022, pp. 497–502, doi: 10.1145/3550356.3561606.

[237] E. Lallas, I. Santouridis, G. Mountzouris, V. C. Gerogiannis, and A. Karageorgos, "An ontology based conceptualization of data integrity regulatory compliance in pharmaceutical industry: The SPuMoNI case," in *Proc. 25th Pan-Hellenic Conf. Inform.*, 2022, pp. 460–465, doi: 10.1145/3503823.3503907.

[238] L. B. Oliveira, M. A. Araujo, and M. A. Dantas, "A case study on the development of an ontology for maintenance services of heavy machinery electronic components," in *Proc. 12th Latin-Amer. Symp. Dependable Secure Comput.*, 2023, pp. 188–191, doi: 10.1145/3615366.3625069.

[239] M. A. Jarwar, J. Watson, CBE FREng, U. P. D. Ani, and S. Chalmers, "Industrial Internet of Things security modelling using ontological methods," in *Proc. 12th Int. Conf. Internet Things*, 2023, pp. 163–170, doi: 10.1145/3567445.3571103.

[240] Y. Afacan and E. Surer, "Modeling a user-oriented ontology on accessible homes for supporting activities of daily living (ADL) in healthy aging," in *Proc. 5th EAI Int. Conf. Smart Objects Technol. Social Good*, 2019, pp. 67–71, doi: 10.1145/3342428.3342662.

[241] M. Alenezi, H. A. Basit, F. I. Khan, and M. A. Beg, "A comparison study of available sofware security ontologies," in *Proc. 24th Int. Conf. Eval. Assessment Softw. Eng.*, 2020, pp. 499–504, doi: 10.1145/3383219.3383292.

[242] A. Elhabbash, V. Nundloll, Y. Elkhatib, G. S. Blair, and V. S. Marco, "An ontological architecture for principled and automated system of systems composition," in *Proc. IEEE/ACM 15th Int. Symp. Softw. Eng. Adaptive Self-Manag. Syst.*, 2020, pp. 85–95, doi: 10.1145/3387939.3391602.

[243] E. Mansour, R. Chbeir, and P. Arnould, "HSSN: An ontology for hybrid semantic sensor networks," in *Proc. 23rd Int. Database Appl. Eng. Symp.*, 2019, pp. 1–10, doi: 10.1145/3331076.3331102.

[244] S. Pattar et al., "SoCo-ITS: Service oriented context ontology for intelligent transport system," in *Proc. 7th Int. Conf. Inf. Technol.: IoT Smart City*, 2020, pp. 503–508, doi: 10.1145/3377170.3377274.

[245] N. Laamech, M. Munier, and C. Pham, "IDSM-O: An IoT data sharing management ontology for data governance," in *Proc. 14th Int. Conf. Manage. Digit. EcoSystems*, 2022, pp. 88–95, doi: 10.1145/3508397.3564825.

[246] L. Alkhariji, S. De, O. Rana, and C. Perera, "Poster: Ontology enabled chatbot for applying privacy by design in IoT systems," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2022, pp. 3323–3325, doi: 10.1145/3548606.3563504.

[247] Q. Lu et al., "Learning electronic health records through hyperbolic embedding of medical ontologies," in *Proc. 10th ACM Int. Conf. Bioinf., Comput. Biol. Health Inform.*, 2019, pp. 338–346, doi: 10.1145/3307339.3342148.

[248] C. Cérin, F. Andres, and D. G.-Feniger, "Towards an emulation tool based on ontologies and data life cycles for studying smart buildings," in *Proc. Int. Workshop Big Data Emergent Distrib. Environ.*, 2021, Art. No.: 8, doi: 10.1145/3460866.3461772.

[249] F. He, X. Zhang, and D. Wang, "Cement-α: An ontology-based data access system for building analytics with multiple data sources," in *Proc. 13th ACM Int. Conf. Future Energy Syst.*, 2022, pp. 436–437, doi: 10.1145/3538637.3538838.

SIEGFRIED HOLLERER received the master's degree in information security from the St. Pölten University of Applied Sciences, in 2016. He has several years of experience as a Penetration Tester analyzing web applications and the IT/OT infrastructure, system hardening, and social engineering attacks. He performed security risk assessments based on the industrial security standard family IEC 62443. Since 2023, he has been working with the Austrian Federal Ministry of the Interior to supervise and enforce the Austrian implementation of the EU NIS directive.

THILO SAUTER (Fellow, IEEE) received the doctoral degree in electrical engineering from TU Wien, Vienna, Austria, in 1999.

He was a Founding Director of the Department of Integrated Sensor Systems, University for Continuing Education Krems. He is currently a Professor with the Institute for Computer Technology, TU Wien, Vienna, Austria. His research interests include intelligent sensors, and industrial communication systems focusing on questions regarding real-time, safety, security, and integration.

WOLFGANG KASTNER (Senior Member, IEEE) received the doctoral degree in informatics from TU Wien, Vienna, Austria, in 1997.

He is currently a Full Professor with the Institute of Computer Engineering and leads the Research Unit Automation Systems at TU Wien, Vienna, Austria. His research interests include the design, analysis, and modeling of distributed automation systems and their seamless integration into the Internet of Things in the industrial domain focusing on knowledge representation and safety and security aspects.