

Enterprise Architecture Modeling for Cybersecurity Analysis in Critical Infrastructures - A Systematic Literature Review

Yuning Jiang^{a,*}, Manfred A. Jeusfeld^b, Michael Mosaad^c and Nay Oo^{a,d}

^aNational University of Singapore, Singapore 639798, Singapore

^bUniversity of Skövde, Skövde 541 28, Sweden

^cDeloitte & Touche (M.E.), Abu Dhabi 990, United Arab Emirates

^dNCS Cyber Special Ops-R&D, Singapore 569141, Singapore

ARTICLE INFO

Keywords:

Enterprise Architecture
Enterprise Model
Cybersecurity
Critical Infrastructure

ABSTRACT

As digital landscapes become increasingly complex, safeguarding sensitive information and systems against cyber threats has become a paramount concern for organizations. This paper provides a comprehensive review of how enterprise architecture modeling is used in the context of cybersecurity assessment, particularly focusing on critical infrastructures. The use of enterprise architecture models for cybersecurity is motivated by the main purpose of enterprise architecture, namely to represent and manage business and IT assets and their interdependence. While enterprise architecture modeling originally served to assess Business/IT alignment, they are increasingly used to assess the cybersecurity of the enterprise. The research questions explored include the types of enterprise architecture models used for cybersecurity assessment, how security aspects are incorporated into these models, the theoretical frameworks and reference theories applied, the research methods used for evaluation, and the strengths and limitations of these models in supporting cybersecurity assessment. This review encompasses research papers published before 2024, focusing on high-quality research from peer-reviewed journals and reputable conferences, thereby providing a structured and comprehensive overview of the current state of research in this domain.

1. Introduction


The governance of information security within enterprise information technology (IT) management has become increasingly vital, especially in organizations characterized by complex IT and industrial control systems (ICSs) landscapes, coupled with a substantial dependence on automated information processing involving many operational technology (OT) components. This is particularly true for critical infrastructure (CI) enterprises, which utilize sophisticated ICSs, including supervisory control and data acquisition (SCADA) systems (Makrakis, Kolias, Kambourakis, Rieger and Benjamin, 2021; Masi, Sellitto, Aranha and Pavleska, 2023). These systems are prevalent across various sectors such as energy, manufacturing, transportation, healthcare, environmental management, and smart urban development, as highlighted by Yaacoub, Salman, Noura, Kaaniche, Chehab and Malli (2020). The integration of such advanced technologies has been a driving force behind the digital transformation of physical entities and their interconnectivity in cyberspace, fulfilling the stringent demands for ultra-reliable services in critical systems (Colombo, Karnouskos, Kaynak, Shi and Yin, 2017).

The cybersecurity landscape has been marked by significant threats to CIs, particularly targeting ICSs, as evidenced by instances like the Stuxnet worm (Falliere, Murchu and Chien, 2011) and the WannaCry ransomware (Mohurle

and Patil, 2017). Attackers frequently aim to disrupt business operations by targeting key enterprise goals, thereby affecting applications and their underlying infrastructure, such as platform systems. Vulnerabilities in one segment can lead to repercussions in others, thereby magnifying potential losses through the inter-dependencies of different layers (Longueira-Romero, Iglesias, Flores and Garitano, 2022). These attacks, which exploit system vulnerabilities, have led to substantial disruptions and economic impacts, including production halts in European automotive factories, as analyzed by Santangelo, Colacino and Marchetti (2021).

In this context, managing cybersecurity within enterprises is an ongoing, dynamic endeavor, requiring continuous adaptation to changing environmental conditions (Nahar and Gill, 2022). It is imperative to perceive cybersecurity not as a standalone operation, but as an integral component of broader enterprise-level strategies. To do so, enterprises need to have a comprehensive understanding of their IT infrastructure and how its business depends on it. A comprehensive overview of such dependencies is of great importance to critical infrastructure operators due to the very large number of assets in the IT and OT domain.

Conceptual modeling, in particular enterprise modeling, has emerged as a valuable tool to support enterprise security analysis. Defined by Mylopoulos (1992) as a formal description of certain aspects of the world for understanding and communication, conceptual modeling aids in managing complexity and fostering communication among stakeholders. It offers benefits such as promoting a shared understanding of threats, linking IT assets to enterprise processes, and facilitating automated reasoning. The use of modeling languages necessitates specificity to enhance the value of

 yuning_j@nus.edu.sg (Y. Jiang)

ORCID(s): 0000-0003-4791-8452 (Y. Jiang); 0000-0002-9421-8566

(M.A. Jeusfeld); 0009-0002-2370-5356 (M. Mosaad); 0009-0006-3414-4696

(N. Oo)

the analysis, particularly in enterprise modeling. Several modeling approaches, like risk assessment methods (Hannou, Rihany, Lammari, Hamdi, Mimouni, Atigui, Cherfi and Tourron, 2022; Ellerhold, Schnagl and Schreck, 2023), have been developed to aid security analysis across various abstraction levels, from organizational to individual software systems.

Enterprise architecture offers a detailed overview of business operations, highlighting the inter-dependencies among business assets, processes, and information technology (Narang, Sharma and Berry, 2023; McClintock, Falkner, Szabo and Yarom, 2020; Loft, He, Yevseyeva and Wagner, 2022). Integrating enterprise architecture practices into the development and implementation of security strategies enables organizations to effectively manage complex business processes and enhance their overall business strategies (Loft et al., 2022; Andrews, Monk and Johnston, 2014). Ekstedt and Sommestad (2009) presented one of the initial proposals for employing enterprise architecture in cybersecurity. They emphasized the creation of attack and defense trees as formal components within the meta-model for enterprise architectures. Reference models typically act as the foundational framework for developing specific architectures, including enterprise architecture modeling (de Kinderen, Kaczmarek-Heß and Hacks, 2023; Hacks, Kaczmarek-Heß, de Kinderen and Töpel, 2022). Adherence to a reference model ensures the use of standardized definitions, terms, and concepts within the enterprise modeling, fostering consistency and interoperability.

Researchers have made efforts to understand the current state of security frameworks, enterprise models, and the integration of information security into enterprise architectures (Ekstedt and Sommestad, 2009; Diefenbach, Lucke and Lechner, 2019; McClintock et al., 2020; Kinderen, Kaczmarek-Heß and Hacks, 2023). However, there is a lack of a comprehensive literature review that analyzes, in a fine-grained manner, the current research and gaps in enterprise architecture modeling, particularly in terms of the utilized semantic foundations, reference frameworks, methods, and cybersecurity perspectives.

The goal of this paper is to simplify the process for researchers and practitioners seeking pertinent studies in the field of enterprise architecture modeling for cybersecurity assessment, especially in the context of critical infrastructures. Additionally, by methodically and thoroughly structuring the literature, we aim to highlight areas that are under-researched. Our goal is to pinpoint these gaps in knowledge and potential areas for further investigation, thereby directing the trajectory of future research in this domain.

1.1. Research Questions

The research questions specifically addressed by this study are as follows:

RQ1: What enterprise architecture reference frameworks and models have been explored for cyber security

assessment? This question aims to catalog the various enterprise architecture reference frameworks and models that have been studied or proposed for addressing cybersecurity concerns.

RQ2: What semantic foundations are applied in these models to incorporate security aspects? The goal here is to identify the underlying semantic foundations that inform the design and implementation of enterprise architecture models in the context of cybersecurity.

RQ3: Which research methods have been used to evaluate these models? This question intends to identify and categorize the research methods (conceptual, empirical, case studies, etc.) used to assess the effectiveness of enterprise architecture models in cybersecurity.

RQ4: What are the integrated cybersecurity aspects in enterprise modeling, especially in the context of critical infrastructures? The aim is to summarize and analyze findings from existing research to understand how different enterprise models address cybersecurity risks.

1.2. Scope

This paper focuses on enterprise architectures and models proposed for cyber security analysis and assessment, while particularly explored such model usage in critical infrastructures.

1.3. Contribution

For this review, we have defined the time frame to include studies published in Scopus, IEEE Xplore and ACM Digital Library before 2024. Our focus is on high-quality research, which entails considering only those articles published in peer-reviewed journals and presented at reputable conferences. In doing so, this paper contributes to the following:

- The paper delves into the methodologies and approaches used by different enterprise architectures and models to incorporate security aspects, with identification of the theoretical frameworks and reference theories that underpin these enterprise architecture models.
- The paper also categorizes and discusses the various research methods, such as conceptual analysis, empirical studies, and case studies, used to evaluate the effectiveness of these enterprise architectures and models in addressing cyber security issues.

1.4. Structure of the Paper

Section 2 provides background of the foundational concepts, including cybersecurity standards, conceptual models, and enterprise architecture models. This section also includes discussions and gap identification in related works. Section 3 details the research methodology utilized for executing the systematic literature review. In Section 4, we delve into an analysis of the results, systematically addressing the five research questions that form the core of this

study. Section 5 offers a comprehensive discussion of the key findings and their implications, also considering the potential threats to the validity of our research. The paper concludes in Section 7, where we summarize our findings and propose directions for future research, thereby setting the stage for subsequent investigations in this domain.

2. Background and Related Works

This section provides an in-depth overview of the foundational concepts, including cybersecurity standards, conceptual models, and enterprise architecture models, establishing the necessary background and terminology for the study. Additionally, this section engages with related work in the field, situating our study within the broader context of existing research.

We summarize the commonly used terminologies in this paper, as shown in Table 1. In the literature, the terms enterprise architecture and enterprise model are sometimes used as synonyms and indeed they overlap to a large extent. An enterprise architecture is a rather informal framework on how the IT systems of an enterprise are aligned with the business goals. A widely used standard for enterprise architectures is TOGAF (Josey, 2016). It does not only specify, which aspects of an enterprise shall be included in an architecture but also formulates rules for architecture governance, such as defining roles and responsibilities. TOGAF is technology-independent. Specifically, it does not prescribe the use of certain modeling languages. Enterprise models are explicit representations of enterprise assets using a set of modeling constructs. They can be seen as multi-perspective conceptual modeling languages. A widely used example is ArchiMate (Lankhorst, Proper and Jonkers, 2010). It closely follows the architecture layers of TOGAF but has a specific set of constructs, i.e. it commits to a certain language to represent information about an enterprise. To summarize, an enterprise architecture is about what to represent, and an enterprise model is about how to represent it. An early precursor of ArchiMate is Aris (Scheer, 1993). It covers similar aspects of an enterprise but lacks the clear differentiation of layers found in ArchiMate. Likewise, a predecessor of TOGAF is the Zachman framework (Sowa and Zachman, 1992). It identifies architecture levels (such as conceptual, logical and physical) and perspectives such as the data perspective and the goal perspective. Like TOGAF, the Zachman framework is informal and does not prescribe any modeling language. A notable difference between an enterprise model and an enterprise architecture is that the latter is rather agnostic of the dependencies between the different layers and perspectives. In contrast, one of the prime functions of an enterprise model is to support tracing dependencies between artifacts defined in different layers, e.g. the dependency between business goals and the IT systems used for the business processes that shall accomplish the goals.

The ISO 42010 standard defines an architecture as the fundamental concepts of an entity and its environment, and

an architecture description is a work product to express an architecture. In this sense, an enterprise model is an architecture description. An early framework for enterprise modeling is GERAM (Bernus, Noran and Molina, 2014), with the goal to facilitate the integration of enterprise application systems.

While enterprise architectures and models were initially designed for Business-IT alignment (Njanka, Sandula and Colomo-Palacios, 2021) including IT security, they have increasingly drawn the attention of cyber security experts in the last decade. Rather than only assessing the cyber security based on hardware and software components, an enterprise architecture model allows to explicitly link security assessments to the building blocks of an enterprise at all levels, from strategic, business, application to networks, hardware, and physical processes.

2.1. Cybersecurity Standards

This paper adopts the following definition from Craigen, Diakun-Thibault and Purse (2014): “*Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights*”. As noted by Burgess (2010), cybersecurity research fundamentally revolves around the elements, tenets, and contexts that create a conceptual foundation. This allows primary stakeholders to collaboratively comprehend and decide on appropriate responses to security challenges.

To facilitate the effective utilization of security metrics, cybersecurity standards have been developed to offer metrics that measure the outcomes of each milestone, enabling organizations to assess historical issues, current stances, ongoing improvements, and projected goals. Currently, the most recognized and adopted cybersecurity frameworks are laid out by the Center for Internet Security (CIS), the International Standards Organization (ISO), and the National Institute of Standards and Technology (NIST) (Chapman and Reithel, 2021).

Community (2021) enumerates 18 primary controls for managers to bolster the security of their information systems. Some key controls from this list encompass secure configurations for both hardware and software, account management, diligent maintenance and analysis of audit logs, defenses against malware, capabilities for data recovery, boundary protections and access controls based on necessity (Sedano and Salman, 2021).

ISO has released a series of standards under the ISO 27000 family, each tailored to specific technological areas to assess varying risk levels and their consequences (Echeverría et al., 2021). A notable instance is ISO/IEC 27001, recognized globally as the standard for overseeing information security (Hamdi, Norman, Molok and Hassandoust, 2019).

2.2. Critical Infrastructure Cybersecurity

As defined by the U.S. Cybersecurity & Infrastructure Security Agency (CISA) and the European Program for Critical Infrastructure Protection (Lindström and Olsson,

Table 1
Definitions of Some Key Terms

Key terms	Descriptions
Conceptual model	Refers to a formal description that abstractly represents and organizes key principles and structures of a system or concept, focusing on essential aspects and relationships relevant to a specific domain Mylopoulos (1992).
Enterprise architecture	Refers to a comprehensive framework that defines an organization's structure and operation, aligning its business processes, information systems, technologies, and infrastructures with strategic objectives. Examples include TOGAF (Josey, 2016) and Zachman framework (Sowa and Zachman, 1992).
Enterprise model	Refers to a detailed representation of an organization's structure, processes, information, and policies, serving as a blueprint for analyzing, designing, and improving operations and supporting strategic planning. Examples include Archimate (Lankhorst et al., 2010) and Aris (Scheer, 1993).
Cybersecurity framework	Refers to a set of guidelines and best practices for managing cybersecurity risks, providing a structured approach to identify, protect, detect, respond to, and recover from cyber threats and vulnerabilities (Juma et al., 2023). Examples include (Community, 2021) and (Echeverría et al., 2021).

2009; Krassnig, 2011), CIs play a pivotal role in societal sustenance. For instance, the critical manufacturing sector produces essential items for other sectors, such as power grids. Such systems employ an interconnected array of sensors, devices, and actuators to understand and influence a physical process, often necessitating assured performance standards set by safety-critical applications (Lewis, 2019). For instance, the smart grid integrates various electric power generation facilities with diverse loads, utilizing dynamic load-balancing and pricing to align with demand-response tactics (Vernotte, Välja, Korman, Björkman, Ekstedt and Lagerström, 2018). This integration is heavily dependent on ICSs.

The Framework for Improving Critical Infrastructure Cybersecurity by NIST offers a structured methodology to address security-related risks, tailored to meet the distinct needs of critical infrastructure providers (Alexander and Panguluri, 2017; Barrett, 2018). This framework is structured around five pivotal, ongoing functions: Identify, Protect, Detect, Respond, and Recover. Collectively, these functions enable organizations to articulate their cybersecurity risk management from a strategic perspective. The foundational elements of the NIST framework guide the delineation of the application context, the formulation and execution of requisite protection and detection mechanisms, and the establishment of mitigation measures and recovery strategies to ensure system robustness and resilience.

The NIST Special Publication 800-82 - Guide to Industrial Control Systems Security (Stouffer, Pease, Tang, Zimmerman, Pillitteri and Lightman, 2022) stands apart from ISO27001 and other cybersecurity frameworks by specifically targeting cybersecurity concerns pertinent to ICS, a crucial information asset within CIs. NIST categorizes ICS to encompass SCADA systems, Distributed Control Systems (DCS), and other related control configurations like Programmable Logic Controllers (PLC), taking into account their distinct demands for performance, reliability, and safety (Jillepalli, Sheldon, de Leon, Haney and Abercrombie, 2017). These systems are integral to the functionality of

the US's critical infrastructures, which are often characterized by significant inter-connectivity and inter-dependence.

2.3. Related Works

Korman, Sommestad, Hallberg, Bengtsson and Ekstedt (2014) compared 12 established methods and examines how well ArchiMate, a modeling language for enterprise architecture, can accommodate the information suggested by these methods.

Diefenbach et al. (2019) offered a comprehensive literature review concerning the integration of information security into enterprise architectures. A key observation is the existing contribution of enterprise architecture management in enhancing risk and information security management. Nonetheless, they contend that further research is imperative to seamlessly weave information security and risk management principles into enterprise architectures.

Ellerm and Morales-Trujillo (2020) discussed the lack of elements to model security in current enterprise architecture modeling languages, with a specific focus on the micro-mobility context.

McClintock et al. (2020) evaluated 25 existing security frameworks and identify a lack of research process and a disjointed focus. Yet they argue that with proper design and integration, enterprise architecture can address the identified organizational security gaps and provide security benefits by reducing unnecessary costs, improving process innovation, standardizing business processes, increasing risk management effectiveness, and improving business/IT alignment.

Insights are also provided on the challenges of integrating enterprise models with security analysis. For example, Kinderen et al. (2023) presents challenges identified through interactions with domain experts, which provide insights into the practical uptake of modeling. These challenges include automated model creation, accounting for changing security requirements, multi-level model management, and incentivizing users.

These identified challenges not only highlight the complexities in integrating enterprise modeling with security

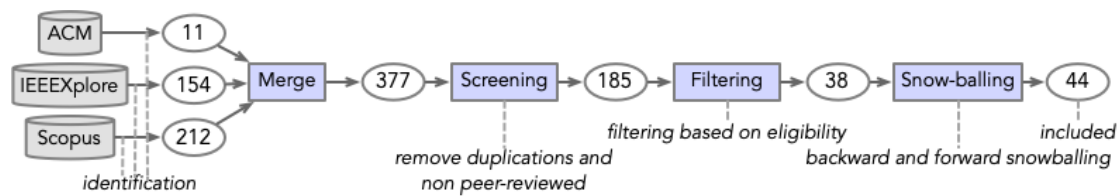


Figure 1: The Process of Paper Collection

measures but also underscore a critical need for a systematic review paper (Brooks and Hause, 2023). Our paper delves into these issues, exploring the current state of enterprise architecture modeling in the context of cybersecurity, and identifying potential areas for further research and development to address these pressing challenges.

3. Research Methodology

Systematic literature reviews (SLR) is chosen to comprehensively identify relevant empirical evidence on the pre-defined research questions by following explicit, systematic methods while ensuring transparency, inclusiveness, explanatory and heuristic qualities (Snyder, 2019).

For example, Lacerda and von Wangenheim (2018) focused on usability capability/maturity models and emphasizes a structured approach to evaluating these models. This method is particularly well-suited for maturity models in usability contexts, offering a robust framework for assessing usability attributes. Fink (2019) provided guidelines for conducting research literature reviews provide a thorough and practical approach, especially valuable for its step-by-step procedures. However, Fink's methods are generally broad and may lack the specificity needed for certain fields like information systems. Page, McKenzie, Bossuyt, Boutron, Hoffmann, Mulrow, Shamseer, Tetzlaff, Akl, Brennan et al. (2021) offered PRISMA guidelines that are essential for ensuring transparency and completeness in systematic reviews. They are particularly effective in the health sciences for their stringent reporting standards, ensuring thorough and unbiased reviews.

In this paper, we adhere to the 8-step SLR methods outlined by Okoli and Schabram (2015), which are based on the frameworks proposed by Webster and Watson (2002) and Levy and Ellis (2006) for analyzing information systems. This 8-step SLR method by Okoli and Schabram (2015) is specifically tailored for information systems research and encompasses a comprehensive approach from planning to reporting, ensuring the inclusion and synthesis of both quantitative and qualitative studies.

This section clearly defines the criteria for literature selection, databases, and search keywords used, as well as inclusion and exclusion criteria. These principles enable a more objective summary of the search findings while minimizing selection bias, publication bias, and data extraction bias (Nightingale, 2009), as summarized in Figure 1. The planning stage is already introduced in Section 1 and is therefore not discussed here.

3.1. Databases and Search Keywords

Our chosen keywords for the search were "Enterprise Model", "Enterprise Architecture", "Cyber Security" and "Critical Infrastructure". These keywords were selected by examining the most frequently cited papers in the Scopus database. This approach aimed to minimize the inclusion of papers that might inadvertently feature terms with similar meanings. We apply our search strings, see table 2, in three digital libraries, namely IEEE Xplore, Scopus, and the ACM Digital Library.

To ensure the inclusion of papers where the full term is present in the abstract or title, abbreviations were excluded. This was done to avoid artificially increasing the search results with texts where those abbreviations might have different meanings. Consequently, the search query was structured to focus on titles, keywords, and abstracts, targeting papers published before 2024. Querying IEEE Xplore Command Search, Scopus Advanced Search and ACM Digital Database Advanced Search engines using the search strings listed in Table 2 gave us 154, 212 and 11 results published before 2024, respectively. Combining all the search results we got an initial pool of 377 papers, as of the query result on May 6th, 2024.

3.2. Inclusion and Exclusion Criteria

After removing duplicates, we still have 356 papers in the pool. Our methodology for selection was structured into three distinct phases: an initial assessment based on the publication titles, followed by a detailed examination of the abstracts, and culminating in a thorough analysis of the full documents. The inclusion criteria were specifically designed to encompass papers that either introduce new enterprise architectures or models, or contribute segments to existing ones, or provide validation on existing approaches.

Conversely, our exclusion criteria were stringent, disqualifying papers consider that following perspectives:

- Relevant Content: Papers that do not directly address the research questions and objectives of this study will be excluded.
- Language: Any papers not published in English will be excluded.
- Standard of Quality: Our review will exclude any papers that are not peer-reviewed.

Beyond applying our inclusion and exclusion criteria, we assessed the quality of the identified studies. We prioritized

Table 2
Search Strings for the Review

Database	Search string
IEEE Xplore	((("Full Text & Metadata": <i>"enterprise arch"</i> OR "Full Text & Metadata": <i>"enterprise mod"</i>) AND ("Full Text & Metadata": <i>"cyber sec"</i> OR "Full Text & Metadata": <i>"cybersec"</i>) AND ("Full Text & Metadata": <i>"critical infra"</i>)) (Note that manual setting in year range to <i>"-2023"</i> is needed.)
Scopus	(<i>"enterprise arch"</i> OR <i>"enterprise mod"</i>) AND (<i>"cyber sec"</i> OR <i>cybersec</i>) AND <i>"critical infra"</i> AND PUBYEAR < 2024
ACM	((Fulltext:(<i>enterprise mod?</i>) OR Fulltext:(<i>enterprise arch?</i>)) AND ((Fulltext:(<i>cyber sec?</i>) OR Fulltext:(<i>cybersec?</i>)) AND Fulltext:(<i>critical infra?</i>) AND ((Keyword:(<i>enterprise mod?</i>) OR Keyword:(<i>enterprise arch?</i>) AND ((Keyword:(<i>cyber sec?</i>) OR Keyword:(<i>cybersec?</i>)) AND (E-Publication Date: (01/01/1908 TO 12/31/2023))

articles that provided substantial details and insights into enterprise architectures or models, including a comprehensive description of their components and their application within the context of cybersecurity.

This process was collaboratively executed by two researchers, each bringing a specialized lens to the study: one with expertise in the cybersecurity domain and the other in enterprise modeling. The cybersecurity researcher was responsible for steering the entire search and selection process, while the enterprise modeling expert provided critical insights through inclusion and exclusion. Then two other researchers who were not involved in the screening process further checked through the included and excluded papers to ensure quality. After this thorough filtering process, 38 papers remained to be reviewed in depth.

Subsequent to the initial filtering round, each article underwent a further round of snowballing based scrutiny, in both backward and forward manners. In the forward snowballing process, we examined the subsequent literature that cited each of the selected papers using Google Scholar which provided an efficient means to track these citations. Conversely, the backward snowballing involved a thorough examination of the references within each paper to ascertain if any pertinent research had been overlooked. This backward review was iteratively conducted until no additional relevant papers were discovered. Particularly, this process extended beyond the references of the initially accepted articles, encompassing the references of the cited papers as well, thereby implementing multiple layers of snowballing. The initial exclusion step led to the snowballing process uncovering a significant number of additional papers, totaling 6. Consequently, the overall count of papers considered in this study amounted to 44, with yearly distribution illustrated in Figure 2 which shows more efforts in this field in the recent five years.

3.3. Data Extraction

A template was employed for the purpose of extracting data, which included several fields: paper ID, authors, title, publication year, source of the publication, type of document, abstract, and key words. We then manually extract and categorize the reviewed literature based on their utilized methodologies, theories, evaluations, and whether real-world applications are involved, following the suggestions

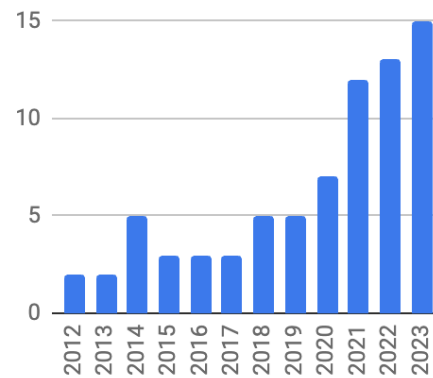


Figure 2: Yearly Distribution of Included Papers

of added values through literature review discussed by Wee and Banister (2016). We mapped relationships among these articles based on their predominant methodologies, design features and implemented frameworks to analyze possibilities for synthesis. Qualitative aspects are introduced through summarizing the contributions of the reviewed papers remaining after rigorous filtering via SLR approach introduced by Okoli and Schabram (2015).

Throughout the coding process, we conducted regular quality checks and spot checks to identify and rectify any coding errors or inconsistencies. This process is collaboratively carried out by two researchers, and further checked by the other two researchers, to reduce potential misinterpretation of text or coding bias.

4. Findings

The findings are structured according to each Research Question (RQ), with the primary papers being classified based on their respective contributions to these RQs.

4.1. Answer to RQ1: What enterprise architecture reference frameworks and models have been explored for cyber security assessment?

Table 3 provides a comprehensive summary of the enterprise architecture reference frameworks and standards employed in the 44 papers reviewed. This includes the utilization of traditional enterprise architecture frameworks

Table 3
Utilized Reference Frameworks

Reference Framework	Number	Paper
SABSA	2	(Burkett, 2012)(Pleinevaux, 2016)(Wood et al., 2017)
TOGAF	2	(Pleinevaux, 2016)(Aldea et al., 2021)
Zachman	1	Tatar et al. (2019)

like Zachman, GERAM, SABSA, and newer ones like ArchiMate. Meanwhile, modeling languages like the Unified Modeling Language (UML) is also integrated to model software-intensive enterprise architecture. UML, primarily a modeling framework, lacks built-in concepts for enterprise artifacts, functioning without domain-specific constructs. Its meta-concepts encompass elements such as "class", attribute, association, actors, and task, among others. In contrast, frameworks like ArchiMate offer a more extensive array of domain-specific constructs. These include, but are not limited to, business goals, software applications, and network infrastructure, providing a richer and more nuanced toolkit for enterprise architecture modeling. This diversity in frameworks reflects the varied approaches and methodologies adopted in the field, each contributing uniquely to the understanding and development of enterprise architecture.

4.1.1. Traditional Commercial Enterprise Architectures

Traditional commercial EAs include the Zachman Framework by Zachman (1987), GERAM (IFIP-IFAC Task Force on Architectures for Enterprise Integration, 1999), TOGAF (Josey, 2016), and SABSA (Sherwood, 2005).

Zachman (1987) presented a structured framework that systematically classifies architectural depictions using a matrix-based approach. Specifically, the framework delineates unique representations for data, process, and location from the perspectives of the owner, designer, and builder. Zachman underscores the distinctiveness of each description, noting that while they may refer to the same entity, they are crafted for specific purposes and should be viewed as independent constructs. Tatar et al. (2019) explored how the Zachman Framework can be applied to depict the United States' program for protecting critical infrastructure. While the Zachman Framework allows for a comprehensive representation of the roles and responsibilities of stakeholders, it has limitations in terms of complexity, flexibility, and standardization.

In comparison, the Generalized Enterprise Reference Architecture and Methodology (GERAM) offers a comprehensive framework that covers a wide range of facets related to enterprise engineering (IFIP-IFAC Task Force on Architectures for Enterprise Integration, 1999). It lays out a collection of guiding principles, models, and methodologies tailored for shaping and progressing enterprise systems. In terms of adaptability, GERAM exhibits greater flexibility to suit varied organizational scenarios, in contrast to the more structured, matrix-centered approach of the Zachman

Framework (Lapalme, Gerber, Van der Merwe, Zachman, De Vries and Hinkelmann, 2016).

The Sherwood Applied Business Security Architecture (SABSA) has a structure similar to the Zachman framework, but specifically aimed at risk and security aspects. SABSA employs a matrix organized around the interrogative terms: What, Why, How, Who, Where, and When (Sherwood, 2005). SABSA analyzes trust relationships between entities to identify security requirements. Burkett (2012) leveraged SABSA to infuse information security considerations into the enterprise architecture landscape. Their methodology aligns with renowned enterprise architecture frameworks like the Zachman framework and TOGAF. Instead of introducing a novel framework, they advocated for enhancing existing enterprise architecture frameworks with security dimensions. They did not employ a formal enterprise modeling language. Yet Loft, He, Janicke and Wagner (2021) identified in their study that very few security failures linked to 'Where', while 'Who' presented intricate and diverse failures, encompassing aspects like end-user behaviors, oversight challenges, and governance complications. Loft et al. (2021) further suggested that the configuration of mainstream enterprise architecture frameworks does not aptly address the fundamental causes of security failures. Wood et al. (2017) focused on the contextual and conceptual layers of the SABSA framework. Pleinevaux (2016) highlighted the importance of Attributes, Domains, and Risks in the SABSA framework. The proposed meta-model for SABSA in this study focuses only on the conceptual level and does not include elements needed at other levels such as the logical or physical component architecture levels.

Adhering to these frameworks necessitates significant resources and dedication, as they mandate the creation of specific documentation and the systematic integration of enterprise architecture activities with business operations (Kotusev, Singh and Storey, 2015). Consequently, many practical enterprise architecture implementations diverge from the theoretical constructs presented in enterprise architecture frameworks (Kotusev and Kurnia, 2021).

Contrasts with a more ubiquitous implementation of security across the entire organization, the guiding philosophy of the Open Group Architecture Framework (TOGAF) standard (Josey, 2016) is identification and application of security measures, specifically tailored to those segments of an organization that necessitate such protections. In terms of implementation, TOGAF exhibits parallels with SABSA, as both frameworks are recognized for their efficacy in providing robust technical structures for EAs.

Table 4
Utilized Modeling Language

Modeling Language	Number	Paper
Archimate	10	(Grandry et al., 2013)(Feltus et al., 2014)(Feltus and Khadraoui, 2016)(Zhi et al., 2018)(Cadete and da Silva, 2018)(Hacks et al., 2019)(Hacks et al., 2021)(Aldea et al., 2021)(Aldea and Hacks, 2022)(San Martín et al., 2022)
UML	3	(Johnson et al., 2014)(Feltus et al., 2014)(Moreno et al., 2021)

4.1.2. Archimate

When integrating cyber security into enterprise models, model-driven engineering (MDE) offers significant tools and methodologies (Schmidt et al., 2006; Neisse, Fovino, Baldini, Stavroulaki, Vlacheas and Giffreda, 2014). Particularly, enterprise modeling frameworks such as Aris Architecture (Scheer and Nüttgens, 2000) and ArchiMate (Manzur, Ulloa, Sánchez and Villalobos, 2015) aim at creating integrated models of the business and IT levels of an enterprise and to establish their dependencies, to support model-driven security analysis, as presented in Table 4.

ArchiMate (Manzur et al., 2015) is increasingly becoming the standard language within the enterprise architecture modeling communities, largely due to its alignment with TOGAF (Band, Engelsman, Feltus, Paredes and Diligens, 2015). Korman et al. (2014) found that ArchiMate is capable of modeling a significant portion of the information required for information security risk assessment. In ArchiMate, enterprise models are categorized into three primary layers for simplicity and clarity. The business layer focuses on elements like business processes and roles. The application layer deals with software applications, their services, and interfaces. Finally, the technology layer is about system software (like operating systems) and physical hardware, such as computers and network devices.

According to the survey conducted by Ellerm and Morales-Trujillo (2020), ArchiMate is the most commonly used modeling languages for security till Jan 2020, but it is also the most criticized due to limitations in its existing security modeling capabilities. It allows representation of both enterprise architecture management and security risk management domains. The Motivation Extension in ArchiMate, incorporating the Business Motivation Model, proves especially effective in articulating the distinct motivations related to risk analysis for architectural principles and decisions. For example, Grandry et al. (2013) refined the ArchiMate meta-model by integrating cybersecurity elements from a domain-specific framework ISSRM (or information system security risk management) following enterprise model integration (EMI) approach, including risks, threats, vulnerabilities, security objectives, and preventive actions.

San Martín et al. (2022) adopted ArchiMate to model the business layer and developing 19 transformation rules in the Atlas Transformation Language (ATL) to map these elements to BPsec, a security-enhanced version of BPMN, aiming to derive secure business process models from enterprise architecture models by integrating security requirements.

The analysis demonstrates that these transformation rules effectively handle complex mappings, ensuring accurate correspondences between enterprise architecture elements and business process models. Nonetheless, implementing this approach requires expertise in both enterprise architecture and model-driven transformation techniques.

Similar efforts are seen to enrich ArchiMate with security information. For example, Zhi et al. (2018) developed a method that integrates quantitative evaluation with system architecture using ArchiMate. They developed the Intra Model Security Assurance (IMSA) approach, combining security assurance cases and architecture diagrams with quantitative evaluation methods. Aldea et al. (2021) proposed a method for enhancing resilience in enterprise architecture by integrating resilience considerations from the design phase. They used ArchiMate to model the current state of an organization's processes, systems, data, and infrastructure, using resilience-focused viewpoints. For example, the OR and AND junctions of ArchiMate are used to model disruption and redundancy, respectively. They also adopted the definitions of probability and impact from TOGAF standard in their risk assessment. The analysis reveals that this approach enhances the system's ability to withstand disruptions and aligns business processes with resilience objectives.

4.1.3. Other Architecture Models

Korman, Lagerström, Välja, Ekstedt and Blom (2016) argued that a standalone reference model might fall short in addressing aspects like flexibility, availability, and constraint validation. However, when paired with a modeling tool, these challenges can be addressed more comprehensively.

Accordingly, some works utilized UML that provides a standardized notation and set of diagrams to get visual representation and documentation of the system's structure, behavior, and interactions.

For instance, Feltus et al. (2014) aimed to enhance cybersecurity protection for critical infrastructures by generating security policies for SCADA systems using UML Use Cases. When modeling cybersecurity policies, they represent roles as actors, and depict collaborations to show connections. Similarly, Moreno et al. (2021) discussed the need for security in cyber-physical systems (CPS) and proposes a security reference architecture for CPS using UML, consisting of business layer, orchestration layer, application layer, service layer, infrastructure layer, sensor & actuator layer and network fabric.

Johnson et al. (2014) developed a Predictive, Probabilistic Architecture Modeling Framework (P^2 AMF) in the form of UML classes while integrating the Object Constraint Language (OCL) with a probabilistic inference mechanism. Their goal was to enhance prediction accuracy for system properties under uncertainty. Holm, Shahzad, Buschle and Ekstedt (2014) combined and extended P^2 AMF and CySeMoL (Sommestad, Ekstedt and Holm, 2012) into P^2 CySeMoL for cyber security analysis while focusing on logical and physical components that can be compromised by attackers. Their model supports prediction and analysis of the probability of successful cyber-attacks, validated through real-world scenarios. Korman et al. (2016) further extended P^2 AMF into a reference architecture that melds advanced metering infrastructure with cybersecurity analysis. In this context, their smart metering model, adhering to UML syntax, serves as a manifestation of their meta-model. Their subsequent enhancements to the smart-grid model yield architectures that facilitate automated security assessments and cyber-attack simulations, with a primary emphasis on smart metering and load-balancing functionalities.

Similar to the other proposed enterprise architectures, a data model called CRUSOE is introduced by Komárková, Husák, Laštovička and Továřík (2018) as a layered data model consisting of business, application, technical, and physical layers. It is created through interviews with incident handlers and formalizes the requirements for modern network environments, and then further extended by Husák, Sadlek, Špaček, Laštovička, Javorník and Komárková (2022).

Akailvi, Gautam, Bhandari, Rashid, Huff and Springer (2022) proposed a software architecture and prototype HELOT that enables the continuous capture of events in OT systems, IT systems, and interconnected networks. HELOT facilitated the real-time capture of forensic artifacts and the automation of cybersecurity operations. The architecture supports proactive threat hunting and incident response in OT environments. The proposed architecture is validated in two application cases: capturing forensics artifacts from a live OT system and automating cybersecurity operations in combined IT/OT environments.

Casola, De Benedictis, Mazzocca and Montanari (2022) developed their layered model by extending the foundational structure of the Purdue Enterprise Reference Architecture (PERA), or the Purdue Model. Purdue model is originated from Purdue University in the 1990s. Purdue model systematically delineates five distinct levels, starting from physical components at Level 0 and extending up to the enterprise network at Level 4/5. Purdue framework encompasses various critical aspects, including control systems at Level 1, supervisory systems at Level 2, manufacturing operations systems at Level 3, and the integration of data collection for informed business decision-making at the highest levels. This layered approach effectively captures the complexity and hierarchical nature of modern industrial systems.

In conclusion, traditional frameworks such as Zachman, GERAM, TOGAF, and SABSA provide robust structures for integrating security considerations into enterprise architecture, each with unique strengths and limitations. Zachman and GERAM offer comprehensive, flexible frameworks, while SABSA and TOGAF emphasize risk and security aspects. ArchiMate stands out with its domain-specific constructs and alignment with TOGAF, despite some limitations in security modeling capabilities. Other models like UML and CRUSOE extend the flexibility required for specific cybersecurity contexts or provide better visibility.

4.2. Answer to RQ2: What semantic foundations are applied to incorporate security aspects into enterprise architecture models?

Utilizing ontology, taxonomy, and domain-specific language (DSL), these approaches focus on integrating detailed security aspects into enterprise architecture models. The principal aim is to reduce the complexity of creating various enterprise architecture artifacts in the security domain by abstracting security-specific details into domain models and using model-driven tools.

4.2.1. Ontology

Ontology provides a structured framework for representing knowledge as a set of concepts within a domain, and the relationships between those concepts. In enterprise modeling, ontology is used to define and standardize the terminology, enabling consistent interpretation of the model elements across different stakeholders and systems.

The SafecareOnto ontology presented by Hannou et al. (2022) models cyber-physical security and uses propagation rules to understand the cascading effects of security incidents in hospitals. The SafecareOnto ontology further consists of three sub-ontologies, namely Asset ontology, Protection ontology, and Impact ontology. Each module supports a specific task dimension related to cyber-physical security within healthcare infrastructures.

Janulevičius, Marozas, Čenys, Goranin and Ramanauskaitė (2017) employed an ontology to delineate enterprise architecture elements pertinent to cloud computing, enriching the enterprise architecture model with security-centered concepts. They specifically address the security dimensions of governance, virtualization, and cloud service operations. This ontology aims to steer the design of enterprise architecture.

DSLs are tailored to a specific aspect of enterprise modeling, providing semantics that are particularly suited to that domain. For example, a DSL might be designed specifically for modeling supply chain processes or IT infrastructure.

Jiang, Jeusfeld, Atif, Ding, Brax and Nero (2018) proposed a DSL and repository in relation to cyber security for smart grids is to categorize and represent the components of power grids and their related IT systems. Their taxonomy and smart grid models are represented in Telos (Mylopoulos, Borgida, Jarke and Koubarakis, 1990) language and

Table 5
Meta Models and Domain Specific Languages

Semantic Meta Model	Number	Paper
Meta Attack Language based	6	(Zhi et al., 2018)(Hacks et al., 2019)(Hacks et al., 2021)(Hacks and Katsikeas, 2021)(Aldea and Hacks, 2022)(Xiong et al., 2022)
Archimate based	4	(Feltus et al., 2014)(Kriaa et al., 2015)(Feltus and Khadraoui, 2016)(Hacks et al., 2019)
ConceptBase (Telos) based	3	(Jiang et al., 2018)(Leune and Kim, 2021)(Jiang et al., 2023)
Other Meta Model	7	(Sommestad et al., 2012)(Neisse et al., 2014)(Kriaa et al., 2015)(Pleinevaux, 2016)(Zhi et al., 2018)(Hannou et al., 2022)(De Rosa et al., 2022)

implemented through ConceptBase (Jeusfeld, 2009). ConceptBase provides a database that stores both the classes (taxonomy) and instances (sample models) of smart grids. This integration allows for the extension of the taxonomy even when sample smart grids are already represented. The properties of smart grid components, such as serial number, model, version, and vendor, are attached using the "property" relation in ConceptBase. Jiang, Jeusfeld, Ding and Sandahl (2023) built upon the CPS taxonomy to allow complex CI dependence analysis, partitioning dependencies into cyber and cyber-physical functional dependencies. They conducted cascade modeling for vulnerability assessment, and proposed power-grid reference models to allow enterprise architecture related information reused for security analysis.

Similarly, Leune and Kim (2021) positioned services as the core of their enterprise modeling instrument. These services are characterized by their providers, the data exchanges among them, and communication channels. The framework is built upon ConceptBase and leverages its query functionalities to scrutinize vulnerabilities within a specified enterprise model.

Hause (2020) presented how Unified Architecture Framework (UAF) enable engineers to define security goals and requirements and implement them throughout the architecture, on top of Systems Modeling Language (SysML) (Holt and Perry, 2008). Hoffmann, Pereira and Nishimura (2023) utilized UAF to delineate the overarching objectives, strategies, capabilities, interactions, standards, operational architectures, and system patterns. They also pointed out a limitation in UAF as it permits the development of architectural elements that may be inconsistent or incoherent.

4.2.2. Meta Models

In enterprise modeling, meta-models define the syntax and semantics of the modeling language, ensuring that models are built in a consistent and standardized manner. In total, 18 (out of 44) papers address meta models in their works, as shown in Table 5.

Sommestad et al. (2012) introduced a meta-probabilistic rational model comprising classes with attributes such as countermeasures and attack steps, as well as reference slots that link to other classes, expressing the relationships between them. This probabilistic rational model was further

developed into the Cyber Security Modeling Language (CySeMoL), which centers on assessing the probability of success for attempted attack paths, given the defined model elements and their interconnections.

Hacks et al. (2019) proposed the use of domain-specific attack languages, specifically the Meta Attack Language (MAL), encompassing 56 attack steps spread over 28 diverse assets, to codify common attack logic in the power sector. The tool set of MAL is combined with ArchiMate notation to model security domains and create instances of MAL that reflect the concepts modeled in ArchiMate. This combination is used to assess the safety and security of power infrastructure by simulating attacks on power grids and plants. A number of MAL-based DSLs are developed, such as coreLang (Hacks and Katsikeas, 2021; Aldea and Hacks, 2022) that models IT entities and vehicleLang that support attack simulation in vehicles. The structure of coreLang includes concepts such as Application, Network, Data, Connection, Vulnerability, Exploit, and Defense, which can be used to model different aspects of the architecture and simulate attacks. On top of coreLang, Hacks et al. (2021) created a method to convert Business Process Modeling Notation (BPMN) into coreLang, enabling the automatic transformation of these models into a graph format for conducting attack simulations using securiCAD (Ekstedt, Johnson, Lagerström, Gorton, Nydrén and Shahzad, 2015). MAL has also being extended to represent the behavior of adversaries, their tactics, techniques, and procedures (TTPs) through mapping to the MITRE ATT&CK Matrix, as seen in the works of Xiong et al. (2022).

Meta models are created on top of ArchiMate or integrating Archimate with other languages. Feltus et al. (2014) modified the structure of ArchiMate to fit the specificity and domain constraints of SCADA components, and validate their model in the field of petroleum supply chains. Feltus and Khadraoui (2016) further evaluated their proposed meta-model and policy management method through a laboratory case study and feedback from the users. They also enriched the SCADA meta-model to provide support for the definition and deployment of semantic and cognitive policies.

Several other meta-models have been developed, each grounded in diverse semantic foundations tailored to specific system requirements. For instance, Neisse et al. (2014) developed SecKit, a model-based security toolkit that adopts

an enterprise architecture approach for security engineering, particularly in IoT systems. This toolkit is based on the principles of the Interaction System Design Language (ISDL), forming a versatile and comprehensive framework applicable to a broad spectrum of distributed systems.

Similarly, Kriaa et al. (2015) introduced the S-cube model, a unique approach for the joint modeling of safety and security in SCADA systems. This model encompasses a meta-model that delineates the components of digital industrial architectures, their attributes, and potential security (attacks) and safety (failures) events affecting each component.

Furthermore, De Rosa et al. (2022) introduced ThreMA, a proposal for a standard meta-model accompanied by a formal vocabulary, specifically designed for modeling ICT infrastructures. These diverse meta-models, each with their unique semantic underpinnings, contribute significantly to the field by addressing specific needs and challenges in system architecture and security.

4.2.3. Reference Models

Reference models play a pivotal role in system modeling and model-based system engineering, particularly in facilitating security-centric analyses, as noted by Vernotte et al. (2018). These models are instrumental in encapsulating the standard topological configurations and functional interconnections inherent in various architectures.

Among the reviewed 44 papers, 7 works research into reference models has been conducted within the domain of CI studies (Vernotte et al., 2018; Moreno et al., 2021; Sellitto, Masi, Pavleska and Aranha, 2021; Hacks et al., 2022; Jiang et al., 2023; Kinderen et al., 2023; Pavleska, Aranha, Masi, Grandry and Sellitto, 2019). The SEGRID project (SEGRID Consortium, 2017), for example, offered insightful reference models for smart grids, with a concentration on communication and enterprise modeling, sidelining the physical components. More specially, their model includes SCADA systems as part of the overall architecture and analyzes their role, functions, and data flows within the smart grid, specifically in relation to load balancing of renewable energy (Vernotte et al., 2018). Their guidance on network control and associated elements remains somewhat circumscribed.

Pavleska et al. (2019) crafted a guideline to assess enterprise cyber security embedded within reference architecture. Their theoretical framework encompasses security objectives, susceptibilities, potential threats, and protective measures, all interconnected with the overarching enterprise model. This conceptual framework serves as a manual guide to evaluate an enterprise's security posture through its enterprise model. The proposed framework was integrated to assess high-level design artifacts and operational solutions, validated through practical application in the e-SENS project.

Sellitto et al. (2021) adeptly mapped their enterprise architecture views, which were utilized to depict a cooperative intelligent transport system use case, into a threat-focused Digital Twin. This mapping was conducted in accordance

with the Reference Architecture Model for Industry 4.0 (RAMI 4.0), facilitating a comprehensive description of the system's life cycle.

Reference models for CIs are usually multi-level, whereby two predominant strategies exist: top-down and bottom-up techniques. The top-down strategy initiates modeling from the highest abstraction level, first outlining concepts at the upper echelons of classification. These concepts are then further elaborated upon as one descends to more detailed classification tiers. Conversely, the bottom-up strategy starts at a detailed abstraction level. As commonalities among these foundational concepts are discerned, they are abstracted into broader concepts at superior levels. In instances where shared properties are identified across multiple concepts, their definitions are elevated to these higher tiers. For example, Töpel and Kaczmarek-Heß (2022) advocated for a flexible creation process that intertwines top-down and bottom-up strategies, particularly for models created using the XModeler and the Flexible Meta-Modeling and Execution Language (FMMLx). FMMLx is utilized by Hacks et al. (2022) to align two reference models, namely NISTIR 7628 and powerLang. NISTIR 7628 is a reference architecture for defining ideal-type smart grid scenarios and associated security requirements.

Jiang et al. (2023) constructed their reference model by integrating and aligning with established and reliable frameworks, notably the Purdue model, NIST SP 800-82, and the IEC 62351 series.

Kinderen et al. (2023) developed a multi-level reference model that integrates terminology from the community, good practices, and existing standards. This model provides an integrated view of relevant aspects such as assets, vulnerabilities, and attacks. The method also includes a process model that consists of six main steps, primarily supported by the reference model.

Utilizing reference models can lead to significant time savings in the modeling process and reduce the risk of service disruptions often associated with real scanning processes. As such, reference models are particularly well-suited for situations where data collection is either not feasible or restricted, such as in the domains of CIs.

4.2.4. Formal Semantics and Logical Foundations

Formal semantics in modeling provides a rigorous and precise interpretation of the model's elements and their relationships, often using mathematical logic or other formal systems. It ensures that the model's meaning is clear, unambiguous, and consistent.

Some works ground their concepts in foundational ontologies such as Object Constraint Language (OCL). OCL is a formal language that allows the user to state expressions on UML models, specifying invariant conditions and queries over objects in the model. It is compatible with UML and provides the necessary expressive power for system property analysis. For instance, Johnson et al. (2014) integrated their proposed framework with OCL, which enables the handling

of uncertainties in both attribute values and model structures, making the framework suitable for various analyses, including performance, reliability, security, and compliance with regulations.

Logical foundations provide a basis for reasoning about the model and verifying properties like consistency and completeness. We also assessed how the reviewed papers use logical foundations in their modeling, including the use of predicate logic, description logics, or other formal logical systems to define the semantics of the model.

The probabilistic rational model proposed by Sommesstad et al. (2012) integrates qualitative parameters, expert inputs, and quantitative parameters for conditional probability distributions. It models both logical dependencies with deterministic influences and probabilistic dependencies with uncertain impacts.

Johnson et al. (2014) incorporated probability distribution mechanisms into their model, grounding it in first-order logical relations to establish a foundation for deductive formalism. Their approach to probabilistic reasoning is based on the Monte Carlo method, which allows for the effective handling of uncertainty and complexity in their model.

The S-cube KB model, as proposed by Kriaa et al. (2015), leverages the object-oriented capabilities of the Figaro modeling language, complemented by tools based on Figaro. This integration facilitates the importation of system architectures through intuitive graphical representations. Figaro, incorporates an inheritance mechanism, is adept at constructing probabilistic models. This feature of Figaro enhances the model's ability to handle complex probabilistic scenarios, making it a robust tool in the realm of system architecture modeling.

Deductive rules have been effectively implemented in the cyber-physical dependence rules and reference architecture as proposed by Jiang et al. (2018), supporting statistic query analysis. This implementation has been further refined and formalized in the subsequent work of Jiang et al. (2023). Similarly, De Rosa et al. (2022) developed a formal vocabulary for modeling ICT infrastructures, a threat catalog, and a set of inference rules based on the Semantic Web Rule Language (SWRL) to support automated threat identification.

Valenza, Karafili, Steiner and Lupu (2022) provided a framework for modeling system entities, their interrelationships, and their relationships with potential threats. Building upon this foundational model, the authors then formulated a set of derivation rules to systematically infer which entities could become vulnerable, compromised, or experience malfunctions as a consequence of the defined threats and system inter-dependencies.

In summary, the review of semantic foundations for incorporating security aspects into enterprise architecture models highlights several approaches. Ontologies, such as SafecareOnto, provide structured frameworks for representing knowledge and ensuring consistent interpretation across stakeholders. Domain-Specific Languages (DSLs) like those proposed by Jiang et al. (2018) and Feltus and Khadraoui

(2016) for smart grids, offer tailored semantics for specific modeling needs, facilitating detailed security representations. Meta models, like MAL (Hacks et al., 2019), integrate with tools such as ArchiMate to model and simulate security domains. Reference models play a crucial role in system modeling and model-based system engineering, enabling security-centric analyses and encapsulating standard configurations and functional interconnections, as seen in works like SEGRID for smart grids (Vernotte et al., 2018). Formal semantics, using mathematical logic or other formal systems, provide a rigorous interpretation of model elements, ensuring clarity and consistency, as demonstrated in frameworks using OCL and probabilistic models like CySeMoL (Johnson et al., 2014; Sommesstad et al., 2012).

As seen in these works, risk modeling languages (e.g., semantic maps and ontology) for model-based security engineering have been proven to be scalable and flexible. Such method not only ensures robust and well-defined security within the architecture but also facilitates the generation of security mechanisms, protocols, and the identification of potential vulnerabilities. Additionally, it allows modelers to develop these artifacts with minimal need for in-depth technological knowledge, exemplified by the separation of process definitions from simulation and security performance aspects in business process simulations for security, enabling automated transitions between different facets.

4.3. Answer to RQ3: What research methods have been used to evaluate these models?

Out of the 44 papers selected for review, 20 do not specify any form of evaluation or validation. Conversely, 24 studies do incorporate validation, with 16 of these papers extending their validation efforts to real-world systems or scenarios, as shown in Table 6.

18 researches utilize case studies for validation. For example, by incorporating domain knowledge through ontology, Vålja et al. (2020) proposed a framework to enhance the precision and accuracy of automated threat models, and is validated using three different case studies, namely a small-scale utility lab, water utility control network, and university IT environment. Dedousis et al. (2021a) introduced a security-aware framework that utilized material flow networks (MFN) for modeling and designing the physical system, aiming to ensure the safety and security of critical infrastructures right from the early design stages. Their proposed framework is evaluated by modeling and assessing the production chain of an oil refinery plant's liquefied petroleum gas purification process. The ThreMA approach proposed by De Rosa et al. (2022) is validated through case studies from the Italian Public Sector, demonstrating its effectiveness in automating threat modeling and enhancing threat identification processes. Similarly, Jiang et al. (2023) performed validation through two case studies of instantiated power-grid models and expert interviews demonstrated the structural and functional adequacy, compatibility, and coverage of the proposed taxonomy and models.

Table 6
Utilized Validation Method for Enterprise Modeling

Validation Method	Number	Paper
Case Study	18	(Sommestad et al., 2012)(Holm et al., 2014)(Feltus and Khadraoui, 2016)(Zhi et al., 2018)(Vernotte et al., 2018)(Jiang et al., 2018)(Välja et al., 2020)(Hacks et al., 2019)(Aldea et al., 2021)(Dedousis et al., 2021a)(Dedousis et al., 2021b)(Akailvi et al., 2022)(Hannou et al., 2022)(De Rosa et al., 2022)(Hacks et al., 2022)(Valenza et al., 2022)(Masi et al., 2023)(Ellerhold et al., 2023)
Simulation/Experiment	6	(Holm et al., 2014)(Zhi et al., 2018)(Hacks et al., 2019)(Aldea and Hacks, 2022)(Xiong et al., 2022)(Ellerhold et al., 2023)
Interview	4	(Holm et al., 2014)(Aldea et al., 2021)(Kinderen et al., 2023)(Jiang et al., 2023)
Questionnaire	3	(Pavleska et al., 2019)(Aldea et al., 2021)(Hannou et al., 2022)

6 papers employed interviews or questionnaires as methods to collect user insights for validation purposes. Aldea et al. (2021) initially conducted a case study within an actual production organization in Lithuania. Subsequently, they expanded their research methodology to include survey questionnaires and expert panel studies, aiming to gather comprehensive feedback on their proposed enterprise architecture model. Meanwhile, Kinderen et al. (2023) utilized interviews to obtain feedback on the practicality and applicability of their proposed reference model, specifically focusing on its relevance to a power grid operator's network that encompasses both IT and OT components.

6 works adopt experiments or simulations for validation. For instance, Ekstedt et al. (2015) presented a CAD tool for enterprise cyber security management called SecuriCAD as a modeling framework and calculation engine that estimates the cyber security of systems-of-systems-level architectures. Aldea and Hacks (2022) and Hacks et al. (2021) performed analysis of the possible security vulnerabilities with the help of the SecuriCAD attack simulations. (Ellerhold et al., 2023) utilized a combination of probability distributions and Monte Carlo simulations to quantify the potential risk associated with a loss event.

Overall, nearly half of the reviewed papers (20 out of 44) lack any form of evaluation or validation, raising concerns about the reliability and applicability of the proposed models in practical scenarios. The diversity in validation methods, including case studies, simulations, experiments, interviews, and questionnaires, highlights the importance of multi-faceted evaluation approaches in advancing research and practice in this field.

4.4. Answer to RQ4: What are the integrated cybersecurity aspects in enterprise modeling, especially in the context of critical infrastructures?

The enterprise-central methodology for cybersecurity necessitates the concurrent execution of risk management across various layers, including business, application, data, and technology, integrating these aspects cohesively (Korman et al., 2014) (Chmielecki, Cholda, Pacyna, Potrawka, Rapacz, Stankiewicz and Wydrych, 2014). Fundamental to

risk assessment is the business impact analysis, while business continuity planning stands as the cornerstone of risk response. Both these processes demand accurate and detailed information about the enterprise. This knowledge should, at a minimum, encompass a simplified set of principles that define the enterprise's mission and the methods employed to achieve it. Moreover, the enterprise architecture should guide the process of change management, encompassing significant updates in security policies and their execution.

4.4.1. Explored Critical Infrastructure Sectors

The reviewed 44 papers reveal a diverse range of CI sectors being addressed in enterprise architecture modeling, with a predominant focus on the energy sector, with 13 papers, indicating it as the most explored area, as presented in Table 7. Transportation also receives notable attention with 4 papers. In contrast, sectors like healthcare and public health, food and agriculture, water and wastewater systems, and critical manufacturing are less represented, each discussed in only one paper.

The prominent representation of the energy sector in enterprise modeling research can be attributed to its critical role in modern infrastructure systems and the intricate interconnections within its network (White, 2019; Gaspar, Cruz, Lam and Simões, 2023). Energy systems frequently serve as a foundation for other vital sectors, naturally positioning them as a focal point for enterprise modeling research endeavors. Particularly, the communication, energy, transportation, water, and waste sectors are regarded as "lifeline" infrastructures by the US Department of Homeland Security (CISA, 2013).

In contrast, sectors like healthcare, public health, food and agriculture, water and wastewater systems are less represented, each discussed in only one paper. This disparity may stem from several factors. For instance, the healthcare sector, while critical, may have unique complexities and regulatory challenges that make it less amenable to general enterprise modeling approaches.

Additionally, there are 5 papers addressing CIs in a more general context without specifying a particular sector. This distribution highlights a strong research focus on energy and transportation, while other critical sectors like healthcare and water systems present opportunities for further exploration in enterprise modeling.

Table 7

Critical Infrastructure Sectors Involved in the Enterprise Modeling

Critical Infrastructure Sector	Number	Paper
Energy	13	(Feltus et al., 2014)(Feltus and Khadraoui, 2016)(Vernotte et al., 2018)(Jiang et al., 2018)(Hacks et al., 2019)(Dedousis et al., 2021a)(Dedousis et al., 2021b)(Valenza et al., 2022)(Hacks et al., 2022)(de Kinderen et al., 2022)(Narang et al., 2023)(Kinderen et al., 2023)(Jiang et al., 2023)
Transportation	4	(Sellitto et al., 2021)(San Martín et al., 2022)(Masi et al., 2023)(Hoffmann et al., 2023)
Healthcare and Public Health	1	(Hannou et al., 2022)
Food and Agriculture	1	(Aldea et al., 2021)
Water and Wastewater Systems	1	(Välja et al., 2020)
Critical Manufacturing	1	(Kriaa et al., 2015)
Unspecified but within CIs	5	(Neisse et al., 2014)(Wood et al., 2017)(Cadete and da Silva, 2018)(Pavleska et al., 2019)(Tatar et al., 2019)(De Rosa et al., 2022)

4.4.2. Enterprise Modeling for Cyber Security

Table 8 categorizes the reviewed papers based on different security perspectives in the context of enterprise modeling. The most prominent category is "Attack Simulation" with 12 papers, indicating a strong research focus on simulating cyber attacks to test system defenses.

"Security by Design" follows with 7 papers, emphasizing the integration of security measures in the initial design stages of systems. 4 papers explicitly incorporate the concept of 'security by design' in their discussions and analyses, while 3 more papers utilize this concept in their reference models. Each of these studies emphasizes the importance of integrating security considerations into the design phase of system development, underscoring the critical role of proactive security measures in contemporary enterprise modeling. In the works of Casola et al. (2022), for example, their conceptual model of CPS supports the implementation of the model-based moving target defense (MTD) approach by providing a comprehensive system model that describes the main architectural elements (assets) and the associated data flow. The MTD techniques, as described in their work, encompass a strategy of continuously altering the system's configuration. This dynamic reconfiguration serves to augment uncertainty for potential attackers, thereby diminishing the likelihood of successful cyber attacks.

"Security by Design" emphasizes integrating security considerations into the early stages of system development, ensuring that security measures are inherent in the system's architecture and design principles (Kinderen et al., 2023). In contrast, works focused on security requirements primarily concentrate on identifying and specifying the security needs and objectives for a given system, typically as a part of the overall functional and non-functional requirements elicitation process (San Martín et al., 2022).

Initiatives (5 out of 44 papers) are being undertaken to enhance the reusability of threat models within the context of enterprise architecture models. For instance, Sellitto et al. (2021) emphasized the importance of incorporating security measures from the early stages of development and addresses the challenges of cost-effectiveness in analyzing security countermeasures. ThreMA, proposed by De Rosa

et al. (2022), utilizes ontology and inference rules to automate the threat modeling process.

Enterprise architecture models are utilized to enhance resilience analysis of such complex systems. For example, Cadete and da Silva (2018) conducted a comparative evaluation to determine the usefulness of their proposed resilience assessment framework (RAF), both with and without the incorporation of the enterprise architecture model. Their conclusion affirmed the hypothesis that the inclusion of an enterprise model significantly enhances the assessment of resilience. Hoffmann et al. (2023) applied enterprise architecture modeling to analyze and address security and resilience in the context of urban air mobility operations.

To effectively identify vulnerabilities, a comprehensive risk analysis is required, encompassing a top-down evaluation from business principles and objectives to business functions, and extending to security controls (Hacks et al., 2022; Jiang et al., 2023). This should be complemented by a bottom-up approach for thorough traceability and assessment. Such an analysis is facilitated by a detailed understanding of the enterprise architecture, coupled with a corresponding risk assessment.

Researchers have proposed quantitative risk analysis methods aimed at evaluating the impacts of risks on enterprises. Ellerhold et al. (2023) incorporated the MITRE ATT&CK Matrix into their approach, mapping it to a unified kill chain model. This integration enabled them to account for chronological factors within their factor analysis of risk and risk calculation processes. Furthermore, system dependencies are analyzed to support fine-grained risk analysis. As an illustration, Dedousis et al. (2021b) employed a risk assessment and dependency analysis methodology to evaluate the cascading impacts resulting from process disruptions. Their approach involved constructing a material flow network graph and utilizing a recursive algorithm to calculate the associated dependency risks.

4.4.3. Challenges of Integrating Security

The papers under review shed light on the integration of cybersecurity within enterprise modeling, particularly

Table 8
Enterprise Modeling for Cyber Security

Security Perspective	Number	Paper
Attack Simulation	12	(Sommestad et al., 2012)(Holm et al., 2014)(Ekstedt et al., 2015)(Kriaa et al., 2015)(Ver- notte et al., 2018)(Hacks et al., 2019)(Välja et al., 2020)(Hacks et al., 2021)(Sellitto et al., 2021)(Xiong et al., 2022)(Aldea and Hacks, 2022)(Ellerhold et al., 2023)
Security by Design	7	(Moreno et al., 2021)(Aldea et al., 2021)(Sellitto et al., 2021)(Dedousis et al., 2021b)(Casola et al., 2022)(Kinderen et al., 2023)(Narang et al., 2023)
Dependence Analysis	6	(Jiang et al., 2018)(Dedousis et al., 2021a)(Dedousis et al., 2021b)(Hannou et al., 2022)(Valenza et al., 2022)(Jiang et al., 2023)
Threat Modeling	5	(Välja et al., 2020)(Hacks and Katsikeas, 2021)(De Rosa et al., 2022)(Xiong et al., 2022)(Valenza et al., 2022)
Security Policy	3	(Feltus et al., 2014)(Neisse et al., 2014)(Feltus and Khadraoui, 2016)
Resilience Analysis	3	(Cadete and da Silva, 2018)(Aldea et al., 2021)(Hoffmann et al., 2023)
Risk Management	3	(Grandry et al., 2013)(Pleinevaux, 2016)(Wood et al., 2017)
Risk Calculation	3	(Dedousis et al., 2021b)(Hannou et al., 2022)(Ellerhold et al., 2023)
Defense Mechanism	2	(Vernotte et al., 2018)(Casola et al., 2022)
Vulnerability Analysis	2	(Hacks et al., 2022)(Jiang et al., 2023)
Incident Response	2	(Komárková et al., 2018)(Akailvi et al., 2022)
Safety & Security	1	(Kriaa et al., 2015)
Security Assurance	1	(Zhi et al., 2018)
Security Requirement	1	(San Martín et al., 2022)

evident in their modeling processes and the validation of their proposed models.

Hause (2020) addressed the difficulties in integrating security into existing architectural frameworks. They highlighted the frameworks' lack of traceability between security requirements and corresponding architectural elements, limited coverage of security requirements, and inadequate support for trade-off analysis.

de Kinderen et al. (2022) delved into the challenges associated with employing reference models for cybersecurity objectives. These challenges encompass the simultaneous consideration of both broad and specific elements, the difficulty in articulating variability while minimizing repetition within the model, and the complexities inherent in facilitating the application and modification of a reference model while ensuring compliance with standards.

Aldea and Hacks (2022) identified a significant deficiency in enterprise architecture models concerning security. They observed that commonly used enterprise modeling languages, such as ArchiMate, do not possess the necessary features for conducting security analysis. This gap indicates that enterprise architecture models lack critical information required for performing security evaluations, thereby presenting substantial challenges in identifying specific vulnerabilities and conducting thorough security assessments. Moreover, the vastness of enterprise model repositories, combined with a lack of comprehensive security expertise among enterprise architects, presents considerable obstacles to the automation of cybersecurity analysis in this domain.

Furthermore, the scale of enterprise architecture model repositories and the scarcity of in-depth security expertise among enterprise architects are major hindrances to the automation of cybersecurity analysis. For instance, Kinderen

et al. (2023) identified practical challenges in adopting modeling, such as automated model creation, adaptation to evolving security requirements, management of multi-level models, and incentivization of users. Aldea and Hacks (2022) also noted that popular enterprise modeling languages like ArchiMate are deficient in capabilities for conducting security analysis. This limitation impedes the identification of vulnerabilities and the execution of comprehensive security assessments. These challenges underscore the complexities in effectively integrating enterprise modeling with security measures, emphasizing the necessity for continued research and development in this field to surmount these barriers.

To summarize, while significant progress has been made in integrating cybersecurity into enterprise modeling, several challenges remain. The energy sector has received the most attention, reflecting its critical importance, while other vital sectors like healthcare and water systems are under-represented, indicating areas that require further research. Cybersecurity perspectives such as attack simulations and security-by-design are commonly incorporated into enterprise modeling, yet other crucial aspects like security assurance are often overlooked. Simultaneously, the lack of comprehensive security features in widely-used modeling languages and the complexity of integrating detailed security requirements highlight the ongoing need for research and development in this field. Addressing these challenges is pivotal to enhancing the robustness and practical applicability of enterprise architecture models in safeguarding critical infrastructures against ever-evolving cyber threats.

5. Discussion

5.1. Status of Current Models

Research efforts in the realm of CIs, especially within the sub-domain of smart grids, have been directed towards offering structured and clear directives for the design of CI frameworks, as seen in Table 7. It has been observed that previously proposed enterprise architecture models tend to be specific to particular domains and technologies. While the principles underlying the creation of an enterprise architecture framework can be adapted to new domains, modifications from the original framework are often necessary.

Among the 44 papers reviewed, only 14 incorporate a meta-model (as seen in Table 5). This observation highlights a significant gap in the current research landscape, emphasizing the necessity for a comprehensive, CI agnostic meta-model. The absence of such a model underscores the challenges associated with domain or industry-specific enterprise architecture models, which often suffer from limited adaptability and reduced applicability across various contexts. Furthermore, another limitation in the current methodologies is evident in defining components and their interrelationships within these frameworks (only 7 out of 44 papers include reference models). The existing lack of detail hinders a thorough understanding that is essential to navigate the complex realm of ICS.

The review of 44 papers on enterprise modeling for security reveals a concerning trend regarding the maturity of these models, particularly in terms of their validation. As presented in Table 6, the fact that nearly half of the papers (20 out of 44) do not specify any form of evaluation or validation underscores a significant gap in the field. This lack of validation raises questions about the reliability and applicability of the proposed models in real-world scenarios. Among the papers that do incorporate validation, the majority rely on case studies. While case studies, such as those conducted by Vålja et al. (2020) and Dedousis et al. (2021a), provide valuable insights into the practical application of these models, they may not fully capture the complexity and variability of real-world environments. Case studies often focus on specific scenarios or contexts, which may limit the generalizability of the findings. Moreover, the diversity in the case studies – ranging from utility labs to university IT environments – suggests a wide range of application areas, yet it also indicates a potential lack of standardized approaches in validation.

5.2. Threats to Validity

We discuss how we address database-related threats to validity, including selection bias, reliability of findings, and review bias, to ensure the robustness of our analysis:

1. To mitigate selection bias, we employed a systematic approach to database selection and search term inclusion. We utilized multiple databases spanning various disciplines relevant to our research topic, including Scopus, IEEE Xplore, and the ACM Digital Library. Additionally, we utilized a comprehensive

set of search terms to ensure a thorough retrieval of relevant literature.

2. To assess the reliability of findings, we evaluated factors such as publication bias, author affiliation, and study methodology to gauge the methodological rigor and validity of the included studies.
3. To address the potential for review bias, we developed clear inclusion and exclusion criteria to guide the selection of studies, and multiple reviewers independently conducted screening and data extraction processes to minimize the risk of bias.

5.3. Recommendations

We draw the the following recommendations from this review, to address gaps and to develop the potential of enterprise architecture models for assessing the cyber security of enterprises:

1. Standardize the enterprise architecture framework for cybersecurity assessment. The reviews shows that ArchiMate is most-widely used and thus appears as a prominent candidate for standardization. The standardization would allow easier sharing of cybersecurity assessment methods.
2. Improve the semantic foundation of enterprise architecture models. While ArchiMate is most widely used, it lacks a strong semantic foundations to detect flaws and weaknesses in enterprise models, in particular relating to cybersecurity assessment.
3. Include more artifact types in enterprise modeling languages to model OT components to allow for a more comprehensive representation of modern enterprise systems that often involve a convergence of IT and OT elements.
4. Support the extraction of partial models from enterprise architecture models, such as models of the computer network, as input for external analysis tools such as attack simulators.
5. Develop tools for automatic elicitation of enterprise architecture models from existing sources such as software registries and log files. A manual maintenance of enterprise architecture models is increasingly difficult at the high rate of changes in the real enterprise. In particular for cybersecurity assessment, an up-to-date enterprise architecture model is important.

5.4. Models, Standards, and Practical Considerations

Practitioners lean on established models and standards to craft secure and resilient OT environments. A historical bedrock of this field is the Purdue model as also discussed earlier. This model structured OT environments hierarchically from Levels 0 to 4, offering a systematic approach to understanding information flow. The model found practical application in operational segmentation, enhancing security by isolating critical control systems from enterprise networks.

Complementing this, the IEC62443 series, developed by the International Electrotechnical Commission (IEC) and International Society of Automation (ISA), stands as a contemporary set of standards tailored for industrial automation and control systems security. These standards have evolved from the collaborative efforts of international organizations, reflecting a response to the increasing sophistication of cyber threats in industrial environments. IEC62443 takes a comprehensive approach, encompassing risk assessment, policies, procedures, and technical controls, providing practitioners with a robust toolkit. The standards also feature sector-specific adaptations, ensuring applicability across diverse industries and offering tailored security measures.

While the Purdue Model stands as a pioneering framework, its roots in a pre-Industry 4.0 era pose challenges in adapting to the dynamic, interconnected nature of modern industrial environments. The model's historical focus on traditional systems may not fully address the security implications of emerging technologies, leading to gaps in overall cyber resilience.

In contrast, the IEC62443 series, grounded in international collaboration, represents a responsive effort to the evolving threat landscape. Despite its strengths, the depth of IEC62443 can pose challenges in implementation, particularly for smaller enterprises with limited resources. The standards emphasize robust guidelines for mitigating cyber threats, yet there's a perceived bias toward reactive measures rather than proactive strategies. A more anticipatory approach to threat prevention is desired to enhance overall cybersecurity resilience, aligning with the dynamic nature of emerging threats. Understanding these limitations is crucial for organizations aiming to implement the IEC62443 standards effectively within the context of existing industrial environments. Despite these challenges, the standards remain a valuable tool for enhancing the cybersecurity posture of ICS when implemented thoughtfully and with due consideration for the specific context of each organization.

However, as the cybersecurity landscape evolves with the integration of more sophisticated technologies, a critical challenge emerges. The focus of current standards and models, while predominantly security-oriented, may not adequately address the need for end-to-end visibility in the entire ICS architecture. The increasing complexity of industrial environments requires a balanced approach across all architecture layers, encompassing not only security aspects but also the broader design considerations. The absence of a comprehensive end-to-end reference model hinders practitioners from gaining holistic insights and designing ICS environments that are not only secure but also optimized for efficiency and resilience.

One challenge arises from the difficulty to identify and manage assets in both IT and OT environments. In OT environments, only about 20% of the assets are traditional IT systems, which can be easily documented using standard IT asset discovery tools (Samanis, Gardiner and Rashid, 2022). The remaining 80% of OT assets, however, are challenging to identify and document due to their non-standard protocols.

This leads to limited visibility over these assets, as information is often manually collected and maintained, increasing the risk of missing assets. The heterogeneity of industrial environments, with a mix of devices from various vendors and both legacy and modern systems, further complicates comprehensive asset documentation.

Stakeholders, who have varied responsibilities, currently face the absence of a unified framework, which obstructs effective collaboration and communication. Consider a scenario where a CI depends on a heterogeneous network of devices, encompassing both legacy systems and contemporary technologies. In traditional IT environments, frameworks like TOGAF provide specific data architecture artifacts that guide the organization and management of data. However, these established norms may not be directly applicable to OT systems, presenting a distinct challenge. The lack of a detailed understanding of data architecture components and their interrelationships in the OT domain poses significant challenges for stakeholders in selecting and implementing suitable cybersecurity controls.

The current state of affairs, characterized by an incomplete representation in the ICS architecture, underscores a challenge in achieving comprehensive insights across diverse layers, including business, data, application, and technology. Existing standards and frameworks, while providing valuable guidance, often exhibit gaps that hinder a holistic understanding of the entire industrial control landscape. This leaves asset owners ill-equipped to make informed decisions on cybersecurity measures. The adoption of emerging technologies in ICS further amplifies this challenge, as traditional frameworks may not adequately address the security implications of these advancements. This limitation not only affects the current cyber security posture but also creates a hurdle in anticipating changes from both cyber and operational perspectives in the unique context of ICS. The void in understanding restricts the ability to proactively assess and mitigate potential risks, especially in the face of accelerating technological advancements.

6. Conclusion

In conclusion, this paper has provided a comprehensive exploration of enterprise architecture models in the context of cybersecurity, particularly within CIs. Our systematic literature review on papers published in Scopus, IEEE Xplore and ACM Digital Library before 2024 has highlighted the various methodologies, theoretical frameworks, and research methods employed in the development and evaluation of enterprise architecture models for cybersecurity assessment. We have identified key areas where enterprise architecture models excel in integrating security aspects and pinpointed their strengths and limitations in supporting cybersecurity assessments.

Our findings reveal that while enterprise architecture models are instrumental in navigating complex business processes and enhancing security strategies, there are still gaps in their application and effectiveness. The diversity in

methodologies and approaches used across different enterprise architecture models indicates a need for more standardized practices. Additionally, the varying strengths and limitations of these models underscore the necessity for continuous refinement and adaptation to evolving cybersecurity threats.

While there are efforts to validate enterprise modeling for security, the current state reflects a certain level of immaturity. The reliance on case studies, while valuable, is not sufficient to fully validate the models. There is a need for more standardized, rigorous, and diverse validation methods, including controlled experiments and simulations, to ensure the reliability and generalizability of these models. This gap in validation not only limits the practical application of the models but also hinders the advancement of the field as a whole.

As we move forward, it is imperative for researchers and practitioners to focus on enhancing the interoperability, consistency, timeliness, and comprehensiveness of enterprise architecture models in cybersecurity. Future research should aim to address the identified gaps, explore new methodologies, and test the effectiveness of these models in diverse and evolving cybersecurity landscapes. By doing so, we can ensure that enterprise architecture models remains a robust and dynamic tool in the fight against cyber threats in critical infrastructure sectors.

Acknowledgment

The 2nd author was supported in part by the PICS collaboration platform at the University of Skövde, <https://www.his.se/en/pics>. This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

- Akailvi, S., Gautam, U., Bhandari, P., Rashid, H., Huff, P.D., Springer, J.P., 2022. Helot-hunting evil life in operational technology. *IEEE Transactions on Smart Grid* doi:10.1109/TSG.2022.3222261.
- Aldea, A., Hacks, S., 2022. Analyzing enterprise architecture models by means of the meta attack language, in: *International Conference on Advanced Information Systems Engineering*, Springer. pp. 423–439. doi:https://doi.org/10.1007/978-3-031-07472-1_25.
- Aldea, A., Vaicekauskaitė, E., Daneva, M., Piest, J.P.S., 2021. Enterprise architecture resilience by design: A method and case study demonstration, in: *2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW)*, IEEE. pp. 147–156. doi:10.1109/EDOCW52865.2021.00044.
- Alexander, R.D., Panguluri, S., 2017. Cybersecurity terminology and frameworks. *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level*, 19–47doi:https://doi.org/10.1007/978-3-319-32824-9_2.
- Andrews, C., Monk, C., Johnston, R., 2014. Integrated architecture framework and security risk management for complex systems doi:10.1049/cp.2014.0965.
- Band, I., Engelsman, W., Feltus, C., Paredes, S.G., Diligens, D., 2015. Modeling enterprise risk management and security with the archimate®. Language, The Open Group.
- Barrett, M.P., 2018. Framework for improving critical infrastructure cybersecurity version 1.1.
- Bernus, P., Noran, O., Molina, A., 2014. Enterprise architecture: Twenty years of the geram framework. *IFAC Proceedings Volumes* 47, 3300–3308. doi:10.3182/20140824-6-ZA-1003.01401. 19th IFAC World Congress.
- Brooks, M., Hause, M., 2023. Model-based cyber security at the enterprise and systems level, in: *INCOSE International Symposium*, Wiley Online Library. pp. 649–665. doi:<https://doi.org/10.1002/iis2.13044>.
- Burgess, J.P., 2010. *Handbook of New Security Studies*. Routledge.
- Burkett, J.S., 2012. Business security architecture: weaving information security into your organization's enterprise architecture through SABSA®. *Inf Secur J Global Perspect* 21, 47–54. doi:<https://doi.org/10.1080/19393555.2011.629341>.
- Cadete, G., da Silva, M.M., 2018. Using an enterprise architecture model for assessing the resilience of critical infrastructure, in: *Safety and Reliability-Safe Societies in a Changing World*. CRC Press, pp. 1459–1466.
- Casola, V., De Benedictis, A., Mazzocca, C., Montanari, R., 2022. Designing secure and resilient cyber-physical systems: a model-based moving target defense approach. *IEEE Transactions on Emerging Topics in Computing* doi:10.1109/TETC.2022.3197464.
- Chapman, T.A., Reithel, B.J., 2021. Perceptions of cybersecurity readiness among workgroup it managers. *Journal of Computer Information Systems* 61, 438–449. doi:<https://doi.org/10.1080/08874417.2019.1703224>.
- Chmielecki, T., Cholda, P., Pacyna, P., Potrawka, P., Rapacz, N., Stankiewicz, R., Wydrych, P., 2014. Enterprise-oriented cybersecurity management, in: *2014 Federated Conference on Computer Science and Information Systems*, IEEE. pp. 863–870. doi:10.15439/2014F38.
- CISA, 2013. National infrastructure protection plan 2013. <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/national-infrastructure-protection-plan-and-resources>. Accessed: 2024-May-06.
- Colombo, A.W., Karnouskos, S., Kaynak, O., Shi, Y., Yin, S., 2017. Industrial cyberphysical systems: A backbone of the fourth industrial revolution. *IEEE Industrial Electronics Magazine* 11, 6–16. doi:10.1109/MIE.2017.2648857.
- Community, C.C., 2021. Center for internet security. URL: <https://www.cisecurity.org/controls/cis-controls-list>.
- Craigen, D., Diakun-Thibault, N., Purse, R., 2014. Defining cybersecurity. *Technology Innovation Management Review* 4. doi:<http://doi.org/10.22215/timreview/835>.
- de Kinderen, S., Kaczmarek-Heß, M., Hacks, S., 2023. A reference model and a dedicated method in support of cyber-security by design: A reality check, in: Hacks, S., Jung, J. (Eds.), *Proceedings of the 13th International Workshop on Enterprise Modeling and Information Systems Architectures (EMISA 2023)*, CEUR-WS.org. pp. 1–8. 13th International Workshop on Enterprise Modeling and Information Systems Architectures, EMISA 2023 ; Conference date: 11-05-2023 Through 12-05-2023.
- De Rosa, F., Maunero, N., Prinetto, P., Talentino, F., Trussoni, M., 2022. Threma: Ontology-based automated threat modeling for ict infrastructures. *IEEE Access* 10, 116514–116526. doi:10.1109/ACCESS.2022.3219063.
- Dedousis, P., Stergiopoulos, G., Arampatzis, G., Gritzalis, D., 2021a. A security-aware framework for designing industrial engineering processes. *IEEE Access* 9, 163065–163085. doi:10.1109/ACCESS.2021.3134759.
- Dedousis, P., Stergiopoulos, G., Arampatzis, G., Gritzalis, D., 2021b. Towards integrating security in industrial engineering design practices., in: *SECRYPT*, pp. 161–172. doi:10.5220/0010544001610172.
- Diefenbach, T., Lucke, C., Lechner, U., 2019. Towards an integration of information security management, risk management and enterprise architecture management – a literature review, in: *2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, Sydney, Australia, December 11-13, 2019, IEEE. pp. 326–333. doi:10.1109/CloudCom.2019.00057.
- Echeverría, A., Cevallos, C., Ortiz-Garcés, I., Andrade, R.O., 2021. Cybersecurity model based on hardening for secure internet of things implementation. *Applied Sciences* 11, 3260. doi:<https://doi.org/10.3390/app11073260>.

- Ekstedt, M., Johnson, P., Lagerström, R., Gorton, D., Nydrén, J., Shahzad, K., 2015. Securi cad by foreseeti: A cad tool for enterprise cyber security management, in: 2015 IEEE 19th International Enterprise Distributed Object Computing Workshop, pp. 152–155. doi:10.1109/EDOCW.2015.40.
- Ekstedt, M., Sommestad, T., 2009. Enterprise architecture models for cyber security analysis, in: 2009 IEEE/PES Power Systems Conference and Exposition, IEEE, pp. 1–6. doi:10.1109/PSCE.2009.4840267.
- Ellerhold, C., Schnagl, J., Schreck, T., 2023. Enterprise cyber threat modeling and simulation of loss events for cyber risk quantification, in: Proceedings of the 2023 on Cloud Computing Security Workshop, Association for Computing Machinery, New York, NY, USA, p. 17–29. URL: <https://doi.org/10.1145/3605763.3625244>, doi:10.1145/3605763.3625244.
- Ellerm, A., Morales-Trujillo, M.E., 2020. Modelling security aspects with archimate: a systematic mapping study, in: 2020 46th Euromicro Conference on Software Engineering and Advanced Applications (SEAA), IEEE, pp. 577–584. doi:10.1109/SEAA51224.2020.00094.
- Falliere, N., Murchu, L.O., Chien, E., 2011. W32. stuxnet dossier. White Paper, Symantec Corp., Security Response 5, 29.
- Feltus, C., Khadraoui, D., 2016. Designing security policies for complex scada systems management and protection. International Journal of Information Technology and Management 15, 313–332. doi:https://doi.org/10.1504/IJITM.2016.079602.
- Feltus, C., Ouedraogo, M., Khadraoui, D., 2014. Towards cyber-security protection of critical infrastructures by generating security policy for scada systems, in: 2014 1st International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), IEEE, pp. 1–8. doi:10.1109/ICT-DM.2014.6917782.
- Fink, A., 2019. Conducting research literature reviews: From the internet to paper. Sage publications.
- Gaspar, J., Cruz, T., Lam, C.T., Simões, P., 2023. Smart substation communications and cybersecurity: A comprehensive survey. IEEE Communications Surveys & Tutorials doi:10.1109/COMST.2023.3305468.
- Grandry, E., Feltus, C., Dubois, E., 2013. Conceptual integration of enterprise architecture management and security risk management, in: Bagheri, E., Gasevic, D., Hallé, S., Hatala, M., Nezhad, H.R.M., Reichert, M. (Eds.), 17th IEEE International Enterprise Distributed Object Computing Conference Workshops, EDOC Workshops, Vancouver, BC, Canada, Sept 9–13, 2013, IEEE Computer Society, pp. 114–123. doi:10.1109/EDOCW.2013.19.
- Hacks, S., Hacks, A., Katsikeas, S., Klaer, B., Lagerström, R., 2019. Creating meta attack language instances using archimate: applied to electric power and energy system cases, in: 2019 IEEE 23rd International Enterprise Distributed Object Computing Conference (EDOC), IEEE, pp. 88–97. doi:10.1109/EDOC.2019.00020.
- Hacks, S., Kaczmarek-Heß, M., de Kinderen, S., Töpel, D., 2022. A multi-level cyber-security reference model in support of vulnerability analysis, in: International Conference on Enterprise Design, Operations, and Computing, Springer, pp. 19–35. doi:https://doi.org/10.1007/978-3-031-17604-3_2.
- Hacks, S., Katsikeas, S., 2021. Towards an ecosystem of domain specific languages for threat modeling, in: International Conference on Advanced Information Systems Engineering, Springer, pp. 3–18. doi:https://doi.org/10.1007/978-3-030-79382-1_1.
- Hacks, S., Lagerström, R., Ritter, D., 2021. Towards automated attack simulations of bpmn-based processes, in: 2021 IEEE 25th International Enterprise Distributed Object Computing Conference (EDOC), IEEE, pp. 182–191. doi:10.1109/EDOC52215.2021.00029.
- Hamdi, Z., Norman, A.A., Molok, N.N.A., Hassandoust, F., 2019. A comparative review of isms implementation based on iso 27000 series in organizations of different business sectors, in: Journal of Physics: Conference Series, IOP Publishing, p. 012103. doi:10.1088/1742-6596/1339/1/012103.
- Hannou, F.Z., Rihany, M., Lammari, N., Hamdi, F., Mimouni, N., Atigui, F., Cherfi, S.S.S., Tourron, P., 2022. Semantic-based approach for cyber-physical cascading effects within healthcare infrastructures. IEEE Access 10, 53398–53417. doi:10.1109/ACCESS.2022.3171252.
- Hause, M., 2020. Integrating security into enterprise architecture with uaf and ple. Insight 23, 44–50. doi:https://doi.org/10.1002/inst.12310.
- Hoffmann, R., Pereira, D., Nishimura, H., 2023. Security viewpoint and resilient performance in the urban air mobility operation. IEEE Open Journal of Systems Engineering doi:10.1109/OJSE.2023.3327524.
- Holm, H., Shahzad, K., Buschle, M., Ekstedt, M., 2014. PQ2} cysemol: Predictive, probabilistic cyber security modeling language. IEEE Transactions on Dependable and Secure Computing 12, 626–639. doi:10.1109/TDSC.2014.2382574.
- Holt, J., Perry, S., 2008. SysML for systems engineering, volume 7. IET.
- Husák, M., Sadlek, L., Špaček, S., Laštovička, M., Javorník, M., Komárková, J., 2022. Crusoe: A toolset for cyber situational awareness and decision support in incident handling. Computers & Security 115, 102609. doi:https://doi.org/10.1016/j.cose.2022.102609.
- IFIP-IFAC Task Force on Architectures for Enterprise Integration, 1999. Geram: The generalised enterprise reference architecture and methodology: Version 1.6. 3 (final), in: Handbook on enterprise architecture. Springer, pp. 21–63. doi:https://doi.org/10.1007/978-3-540-24744-9_2.
- ISO 42010, 2022. Software, systems and enterprise - Architecture description. Standard. International Organization for Standardization. Geneva, Switzerland.
- Janulevičius, J., Marozas, L., Čenys, A., Goranin, N., Ramanauskaitė, S., 2017. Enterprise architecture modeling based on cloud computing security ontology as a reference model, in: 2017 Open Conference of Electrical, Electronic and Information Sciences (eStream), pp. 1–6. doi:10.1109/eStream.2017.7950320.
- Jeusfeld, M.A., 2009. Metamodeling and method engineering with ConceptBase, in: Metamodeling for Method Engineering. MIT Press, pp. 89–168.
- Jiang, Y., Jeusfeld, M., Atif, Y., Ding, J., Brax, C., Nero, E., 2018. A language and repository for cyber security of smart grids, in: 2018 IEEE 22nd International Enterprise Distributed Object Computing Conference (EDOC), IEEE, pp. 164–170. doi:10.1109/EDOC.2018.00029.
- Jiang, Y., Jeusfeld, M.A., Ding, J., Sandahl, E., 2023. Model-based cybersecurity analysis: Extending enterprise modeling to critical infrastructure cybersecurity. Business & Information Systems Engineering , 1–34doi:https://doi.org/10.1007/s12599-023-00811-0.
- Jillepalli, A.A., Sheldon, F.T., de Leon, D.C., Haney, M., Abercrombie, R.K., 2017. Security management of cyber physical control systems using nist sp 800-82r2, in: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE, pp. 1864–1870. doi:10.1109/IWCMC.2017.7986568.
- Johnson, P., Ullberg, J., Buschle, M., Franke, U., Shahzad, K., 2014. An architecture modeling framework for probabilistic prediction. Information Systems and e-Business Management 12, 595–622. doi:https://doi.org/10.1007/s10257-014-0241-8.
- Josey, A., 2016. TOGAF® version 9.1-A pocket guide. Van Haren.
- Juma, A.H., Arman, A.A., Hidayat, F., 2023. Cybersecurity assessment framework: A systematic review, in: 2023 10th International Conference on ICT for Smart Society (ICISS), IEEE, pp. 1–6. doi:10.1109/ICISS59129.2023.10291832.
- de Kinderen, S., Kaczmarek-Heß, M., Hacks, S., 2022. Towards cybersecurity by design: A multi-level reference model for requirements-driven smart grid cybersecurity, in: 30th European Conference on Information Systems (ECIS 2022): New Horizons in Digitally United Societies, AIS Electronic Library, p. 1479. doi:https://aisel.aisnet.org/ecis2022_rp/89/.
- Kinderen, S.d., Kaczmarek-Heß, M., Hacks, S., 2023. A reference model and a dedicated method in support of cyber-security by design: Reality check, in: 13th International Workshop on Enterprise Modeling and Information Systems Architectures (EMISA 2023), May 11–12, 2023, Stockholm, Sweden, CEUR.
- Komárková, J., Husák, M., Laštovička, M., Tovarňák, D., 2018. Crusoe: Data model for cyber situational awareness, in: Proceedings of the 13th International Conference on Availability, Reliability and Security, pp. 1–10. doi:https://doi.org/10.1145/3230833.3232798.

- Korman, M., Lagerström, R., Vålja, M., Ekstedt, M., Blom, R., 2016. Technology management through architecture reference models: a smart metering case, in: 2016 Portland International Conference on Management of Engineering and Technology (PICMET), IEEE. pp. 2338–2350. doi:10.1109/PICMET.2016.7806518.
- Korman, M., Sommestad, T., Hallberg, J., Bengtsson, J., Ekstedt, M., 2014. Overview of enterprise information needs in information security risk assessment, in: 2014 IEEE 18th International Enterprise Distributed Object Computing Conference, IEEE. pp. 42–51. doi:10.1109/EDOC.2014.16.
- Kotusev, S., Kurnia, S., 2021. The theoretical basis of enterprise architecture: A critical review and taxonomy of relevant theories. *Journal of Information Technology* 36, 275–315. doi:https://doi.org/10.1177/026839622097787.
- Kotusev, S., Singh, M., Storey, I., 2015. Investigating the usage of enterprise architecture artifacts doi:http://aisel.aisnet.org/ecis2015_rip/15.
- Krassnig, C., 2011. European programme on critical infrastructure protection (epcip), in: 1st international workshop on regional critical infrastructures protection programmes, pp. 1–16.
- Kriaa, S., Bouissou, M., Laarouchi, Y., 2015. A model based approach for scada safety and security joint modelling: S-cube doi:10.1049/cp.2015.0293.
- Lacerda, T.C., von Wangenheim, C.G., 2018. Systematic literature review of usability capability/maturity models. *Computer Standards & Interfaces* 55, 95–105. doi:https://doi.org/10.1016/j.csi.2017.06.001.
- Lankhorst, M.M., Proper, H.A., Jonkers, H., 2010. The anatomy of the archimate language. *Int. J. Inf. Syst. Model. Des.* 1, 1–32. URL: https://doi.org/10.4018/jismd.2010092301, doi:10.4018/JISMD.2010092301.
- Lapalme, J., Gerber, A., Van der Merwe, A., Zachman, J., De Vries, M., Hinkelmann, K., 2016. Exploring the future of enterprise architecture: A zachman perspective. *Computers in Industry* 79, 103–113. doi:https://doi.org/10.1016/j.compind.2015.06.010.
- Leune, K., Kim, S., 2021. Supporting cyber threat analysis with service-oriented enterprise modeling, in: di Vimercati, S.D.C., Samarati, P. (Eds.), *Proceedings of the 18th International Conference on Security and Cryptography (SECRYPT)*, July 6–8, Scitepress. pp. 385–394. doi:10.5220/0010502503850394.
- Levy, Y., Ellis, T.J., 2006. A systems approach to conduct an effective literature review in support of information systems research. *Informing Science* 9.
- Lewis, T.G., 2019. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. John Wiley & Sons.
- Lindström, M., Olsson, S., 2009. The european programme for critical infrastructure protection, in: *Crisis management in the European Union*. Springer, pp. 37–59. doi:https://doi.org/10.1007/978-3-642-00697-5_3.
- Loft, P., He, Y., Janicke, H., Wagner, I., 2021. Dying of a hundred good symptoms: why good security can still fail-a literature review and analysis. *Enterprise Information Systems* 15, 448–473. doi:https://doi.org/10.1080/17517575.2019.1605000.
- Loft, P., He, Y., Yevseyeva, I., Wagner, I., 2022. Caesar8: An agile enterprise architecture approach to managing information security risks. *Computers & Security* 122, 102877. doi:https://doi.org/10.1016/j.cose.2022.102877.
- Longueira-Romero, Á., Iglesias, R., Flores, J.L., Garitano, I., 2022. A novel model for vulnerability analysis through enhanced directed graphs and quantitative metrics. *Sensors* 22, 2126. doi:https://doi.org/10.3390/s22062126.
- Makrakis, G.M., Koliass, C., Kambourakis, G., Rieger, C., Benjamin, J., 2021. Industrial and critical infrastructure security: Technical analysis of real-life security incidents. *Ieee Access* 9, 165295–165325. doi:10.1109/ACCESS.2021.3133348.
- Manzur, L., Ulloa, J.M., Sánchez, M., Villalobos, J., 2015. xarchimate: Enterprise architecture simulation, experimentation and analysis. *Simulation* 91, 276–301. doi:https://doi.org/10.1177/0037549715575188.
- Masi, M., Sellitto, G.P., Aranha, H., Pavleska, T., 2023. Securing critical infrastructures with a cybersecurity digital twin. *Software and Systems Modeling* 22, 689–707. URL: https://doi.org/10.1007/s10270-022-01075-0, doi:10.1007/s10270-022-01075-0.
- McClintock, M., Falkner, K., Szabo, C., Yarom, Y., 2020. Enterprise security architecture: Mythology or methodology?, in: *ICEIS* (2), pp. 679–689. doi:10.5220/0009404406790689.
- Mohurle, S., Patil, M., 2017. A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science* 8.
- Moreno, J., Rosado, D.G., Sánchez, L.E., Serrano, M.A., Fernández-Medina, E., 2021. Security reference architecture for cyber-physical systems (cps). *JUCS: Journal of Universal Computer Science* 27. doi:10.3897/jucs.68539.
- Mylopoulos, J., 1992. Conceptual modelling and telos. *Conceptual modelling, databases, and CASE: An integrated view of information system development*, 49–68.
- Mylopoulos, J., Borgida, A., Jarke, M., Koubarakis, M., 1990. Telos: Representing knowledge about information systems. *ACM Transactions on Information Systems (TOIS)* 8, 325–362. doi:https://doi.org/10.1145/102675.102676.
- Nahar, K., Gill, A.Q., 2022. Integrated identity and access management metamodel and pattern system for secure enterprise architecture. *Data & Knowledge Engineering* 140, 102038. doi:https://doi.org/10.1016/j.datak.2022.102038.
- Narang, N.K., Sharma, M., Berry, T., 2023. Architectural and systems approach to sustainable digital transformation of distribution utilities, in: *27th International Conference on Electricity Distribution (CIRED 2023)*, pp. 3944–3948. doi:10.1049/icp.2023.0507.
- Neisse, R., Fovino, I.N., Baldini, G., Stavroulaki, V., Vlacheas, P., Gialfreda, R., 2014. A model-based security toolkit for the internet of things, in: *2014 Ninth International Conference on Availability, Reliability and Security, IEEE*. pp. 78–87. doi:10.1109/ARES.2014.17.
- Nightingale, A., 2009. A guide to systematic literature reviews. *Surgery (Oxford)* 27, 381–384. doi:https://doi.org/10.1016/j.mpsur.2009.07.005.
- Njanka, S.Q., Sandula, G., Colomo-Palacios, R., 2021. IT-Business alignment: A systematic literature review. *Procedia Computer Science* 181, 333–340. doi:https://doi.org/10.1016/j.procs.2021.01.154.
- Okoli, C., Schabram, K., 2015. A guide to conducting a systematic literature review of information systems research doi:http://sprouts.aisnet.org/10-26.
- Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E., et al., 2021. The prisma 2020 statement: an updated guideline for reporting systematic reviews. *Bmj* 372. doi:https://doi.org/10.1136/bmj.n71.
- Pavleska, T., Aranha, H., Masi, M., Grandry, E., Sellitto, G.P., 2019. Cybersecurity evaluation of enterprise architectures: The e-sens case, in: Gordijn, J., Guédria, W., Proper, H.A. (Eds.), *The Practice of Enterprise Modeling – 12th IFIP Working Conference, PoEM 2019, Luxembourg, Nov 27–29, 2019, Proceedings*, Springer. pp. 226–241. doi:https://doi.org/10.1007/978-3-030-35151-9.
- Pleinevaux, P., 2016. Towards a metamodel for SABSA conceptual architecture descriptions, in: *2016 11th International Conference on Availability, Reliability and Security (ARES), IEEE*. pp. 187–194. doi:10.1109/ARES.2016.87.
- Samanis, E., Gardiner, J., Rashid, A., 2022. Sok: A taxonomy for contrasting industrial control systems asset discovery tools, in: *Proceedings of the 17th International Conference on Availability, Reliability and Security, Association for Computing Machinery, New York, NY, USA*. URL: https://doi.org/10.1145/3538969.3538979, doi:10.1145/3538969.3538979.
- San Martín, L., Rodríguez, A., Caro, A., Velásquez, I., 2022. Obtaining secure business process models from an enterprise architecture considering security requirements. *Business Process Management Journal* 28, 150–177. doi:https://doi.org/10.1108/BPMJ-01-2021-0025.
- Santangelo, G.V., Colacino, V.G., Marchetti, M., 2021. Analysis, prevention and detection of ransomware attacks on industrial control systems, in: *2021 IEEE 20th International Symposium on Network Computing and Applications (NCA), IEEE*. pp. 1–5. doi:10.1109/NCA53618.2021.

- 9685713.
- Scheer, A., 1993. Architecture of integrated information systems (ARIS), in: Yoshikawa, H., Goossenaerts, J. (Eds.), *Information Infrastructure Systems for Manufacturing*, Proceedings of the JSPE/IFIP TC5/WG5.3 Workshop on the Design of Information Infrastructure Systems for Manufacturing, DIISM '93, Tokyo, Japan, 8-10 November, 1993, North-Holland. pp. 85–99.
- Scheer, A., Nüttgens, M., 2000. ARIS architecture and reference models for business process management, in: van der Aalst, W.M.P., Desel, J., Oberweis, A. (Eds.), *Business Process Management, Models, Techniques, and Empirical Studies*, Springer, Heidelberg. pp. 376–389. doi:https://doi.org/10.1007/3-540-45594-9_24.
- Schmidt, D.C., et al., 2006. Model-driven engineering. *Computer-IEEE Computer Society-* 39, 25. doi:10.1109/MC.2006.58.
- Sedano, W.K., Salman, M., 2021. Auditing Linux operating system with center for internet security (cis) standard, in: 2021 International Conference on Information Technology (ICIT), IEEE. pp. 466–471. doi:10.1109/ICIT52682.2021.9491663.
- SEGRID Consortium, 2017. Security for smart Electricity GRIDs, How to address the security challenges in smart grids. Technical Report. Segrid.eu. URL: https://segrid.eu/wp-content/uploads/2017/10/Whitepaper-Segrid-9-FV.pdf.
- Sellitto, G.P., Masi, M., Pavleska, T., Aranha, H., 2021. A cyber security digital twin for critical infrastructure protection: the intelligent transport system use case, in: IFIP Working Conference on The Practice of Enterprise Modeling, Springer. pp. 230–244. doi:https://doi.org/10.1007/978-3-030-91279-6_16.
- Sherwood, N., 2005. Enterprise security architecture: a business-driven approach. CRC Press.
- Snyder, H., 2019. Literature review as a research methodology: An overview and guidelines. *Journal of business research* 104, 333–339. doi:https://doi.org/10.1016/j.jbusres.2019.07.039.
- Sommestad, T., Ekstedt, M., Holm, H., 2012. The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures. *IEEE Systems Journal* 7, 363–373. doi:10.1109/JSYST.2012.2221853.
- Sowa, J.F., Zachman, J.A., 1992. Extending and formalizing the framework for information systems architecture. *IBM Syst. J.* 31, 590–616. URL: https://doi.org/10.1147/sj.313.0590, doi:10.1147/SJ.313.0590.
- Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., 2022. Guide to operational technology (OT) security. National Institute of Standards and Technology: Gaithersburg, MD, USA doi:https://doi.org/10.6028/NIST.SP.800-82r3.
- Tatar, U., Karabacak, B., Katina, P.F., Ignor, A., 2019. A complex structure representation of the us critical infrastructure protection program based on the zachman framework. *International Journal of System of Systems Engineering* 9, 221–234. doi:https://doi.org/10.1504/IJSSE.2019.102869.
- Töpel, D., Kaczmarek-Heß, M., 2022. Towards flexible creation of multi-level models: bottom-up change support in the modeling and programming environment xmodeler, in: Proceedings of the 25th International Conference on Model Driven Engineering Languages and Systems: Companion Proceedings, pp. 404–413. doi:https://doi.org/10.1145/3550356.3561553.
- Valenza, F., Karafili, E., Steiner, R.V., Lupu, E.C., 2022. A hybrid threat model for smart systems. *IEEE Transactions on Dependable and Secure Computing* 20, 4403–4417. doi:10.1109/TDSC.2022.3213577.
- Välja, M., Heiding, F., Franke, U., Lagerström, R., 2020. Automating threat modeling using an ontology framework. *Cybersecurity* 3, 1–20. doi:https://doi.org/10.1186/s42400-020-00060-8.
- Vernotte, A., Välja, M., Korman, M., Björkman, G., Ekstedt, M., Lagerström, R., 2018. Load balancing of renewable energy: a cyber security analysis. *Energy Informatics* 1, 1–41. doi:https://doi.org/10.1186/s42162-018-0010-x.
- Webster, J., Watson, R.T., 2002. Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly*, xiii–xxiii.
- Wee, B.V., Banister, D., 2016. How to write a literature review paper? *Transport reviews* 36, 278–288. doi:https://doi.org/10.1080/01441647.2015.1065456.
- White, R., 2019. Risk analysis for critical infrastructure protection. *Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies*, 35–54doi:https://doi.org/10.1007/978-3-030-00024-0_3.
- Wood, A., He, Y., Maglaras, L.A., Janicke, H., 2017. A security architectural pattern for risk management of industry control systems within critical national infrastructure. *International Journal of Critical Infrastructures* 13, 113–132. doi:https://doi.org/10.1504/IJCIS.2017.088229.
- Xiong, W., Legrand, E., Åberg, O., Lagerström, R., 2022. Cyber security threat modeling based on the mitre enterprise attack matrix. *Software and Systems Modeling* 21, 157–177. doi:https://doi.org/10.1007/s10270-021-00898-7.
- Yaacoub, J.P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A., Malli, M., 2020. Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and microsystems* 77, 103201. doi:https://doi.org/10.1016/j.micpro.2020.103201.
- Zachman, J.A., 1987. A framework for information systems architecture. *IBM systems journal* 26, 276–292. doi:10.1147/sj.263.0276.
- Zhi, Q., Yamamoto, S., Morisaki, S., 2018. Quantitative evaluation in security assurance, in: 2018 IEEE 4th International Conference on Computer and Communications (ICCC), IEEE. pp. 2477–2483. doi:10.1109/CompComm.2018.8780877.