Security Engineering in Cyber-Physical Systems: A Systematic Review of Methodological Approaches

Elias Seid, Oliver Popov and Fredrik Blix
Department of Computer and Systems Sciences, Stockholm University, Sweden

Keywords: Cyber-Physical Systems Security, Cybersecurity Frameworks, Security Model, Quantitative Research, Qualitative Research, Cyber-Physical System, Security Engineering, Threat Modeling, Cyber Risk.

Abstract: Ensuring strong security in Cyber-Physical Systems (CPS) is increasingly essential as these systems become integral to contemporary industrial and societal infrastructures. The increasing prevalence of security risks requires the advancement of conventional security engineering approaches to tackle the distinct problems presented by CPS. This study offers a thorough assessment of the research methodologies, approaches, and strategies used in security engineering for cyber-physical systems over the last fifteen years. The review analyses the design and execution of security solutions, including empirical and conceptual investigations, along with the integration and enhancement of existing methodologies. This study seeks to offer a systematic overview of contemporary developments and pinpoint methodological concerns essential for future research in adaptive and security engineering -driven for CPS through an analysis of diverse literature. This study enhances the current discussion by providing a thorough analysis of the research environment, demonstrating the requirement for new and contextually relevant security engineering methodologies.

1 INTRODUCTION

Over the past decade, various sectors within society have experienced a rapid process of digitalization. One significant trend involves the migration of crucial information resources and organisational procedures from physical to digital platforms. The implementation of novel sociotechnical solutions has brought about numerous advantages by significantly enhancing operational efficiency in both corporate and governmental organisations, thereby altering the landscape of information and process management. However, it has also presented novel challenges. The growing dependence on systems and networks has resulted in heightened susceptibility of critical service providers, such as government agencies and healthcare organisations, to incidents that impact their operations (Urbach and Röglinger et al., 2019).

Cybersecurity incidents that impact the cyberinfrastructure, encompassing the network and system resources of significant service providers, have the potential to significantly disrupt crucial digital operations. Consequently, this disruption indirectly hampers the organization's capacity to effectively deliver services to its stakeholders. In addition to the general public, various other organisations are also involved. This prompts inquiries into the extent to which cyberattacks can inflict damage on organisational systems and networks, as well as indirectly impacting organisational functions and society as whole [1]

1.1 Cyber-Physical Systems

The field of Industrial Automation and Control Systems (IACS) has received greater focus in research than when considered within the broader framework of information and communication technology (ICT). Originally, a firewall was employed to counteract any potential threat directed towards the central component of the system (Urbach and Röglinger et al., 2018). The internet of things has significantly disrupted the infrastructure of the Industrial automation and control system, leading to substantial changes in various areas such as electrical management systems and manufacturing. The concept of IACS has been researched in the field of cyber-physical systems. They were given the name "cyber-physical systems" when they were incorporated into industries such as manufacturing and energy management systems, where they solely perform operational tasks. Following the advent of the internet of things in 1999, it has become commonplace to use this technology in a wide range of business and industrial environments.

[1] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Seid, E., Popov, O. and Blix, F.
Security Engineering in Cyber-Physical Systems: A Systematic Review of Methodological Approaches.
DOI: 10.5220/0013478100003928
In *Proceedings of the 20th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2025)*, pages 822-834
ISBN: 978-989-758-742-9; ISSN: 2184-4895
Copyright © 2025 by Paper published under CC license (CC BY-NC-ND 4.0)

Several definitions of cyber-physical systems (CPS) have been explored in the literature (Boyes et al., 2018), (Griffor et al., 2017), (Henzinger et al., 2008), (Baheti et al., 2011), and (Poovendran, R. et al., 2010). Nevertheless, (Urbach and Röglinger et al., 2018) has concisely synthesised and integrated all the ideas discussed in the literature related to CPS, establishing a shared foundation. Cyber-Physical System (CPS), is a system that consists of a collection of interconnected physical and digital components, which can be either centralised or decentralised. This definition comprises three key elements: sensing, computation, and networking, which are crucial for addressing real-world challenges through the utilisation of physical processes. The Industrial Internet of Things (IIoT) expands upon the principles and definitions employed in CPS. It refers to intelligent interconnected assets or objects that form a component of a larger system or a network of systems, constituting the intelligent manufacturing enterprise (Shafi, Q et al., 2012).

The Internet of Things (IoT) is a specific form of CPS. The complexity of IoT becomes particularly apparent when implemented in an industrial setting, where a multitude of technological advancements, such as processing, communication, manufacturing, and sensing devices, are used, often incorporating elements of Artificial Intelligence. The various opportunities presented by the Industrial Internet of Things (IIoT) are also exploited by malefactors or cyber criminals, thereby making security a prominent deterrent to the widespread adoption of Industry 4.0. The convergence of Information and communication technology (ICT) with Operational Technology (OT) has intensified the difficulties, particularly due to the contrasting nature of changes in ICT and OT. ICT is characterised by its dynamic and aggressive nature, while OT is slower and often more expensive to innovate (Awotunde, J et al., 2023).

The Objective of the Study. The study aims to achieve two primary objectives. First, it seeks to conduct a comprehensive literature review spanning approximately fifteen years, focusing on key issues and aspects related to Security Engineering for CPS. This review will critically evaluate existing research methodologies within the field. Additionally, the study aims to identify gaps in the literature and propose enhancements to specific algorithms and procedures that, while proven effective in traditional security contexts, have yet to be explored in the CPS domain. The overarching goal of this review is to systematically identify and analyze the research approaches, methodologies, and strategies employed in selected publications addressing security engineering for CPS.

Moreover, this study conducted a systematic literature review by analysing existing approaches, methods, and frameworks based on selected papers. The review was performed using automated search techniques on relevant academic databases. The findings of this review will be discussed in the following section. This literature review examined scholarly papers that primarily focused on formalisations, meta-studies, and various topics such as Security, cybersecurity, and Industrial Internet of Things (IIoT). Model-driven security has been widely used in the domains of software adaption, security, legal compliance, and business intelligence. The unit of analysis for this study is the methods and research strategies employed in the selected papers.

To select papers for this study, we relied on reputable sources, including Google Scholar, Web of Science, and Scopus. Among these, Scopus was particularly emphasized due to its extensive coverage of major publishers in the Software Engineering domain, such as ACM, Springer, and IEEE. Scopus provides a notable advantage in terms of inclusiveness, surpassing the coverage of Web of Science, although it is more focused in scope. Google Scholar, on the other hand, encompasses a broader range of materials, including non-peer-reviewed works like technical papers, which can provide additional insights into the domain of CPS.

The primary objective of this review process is to identify the research approaches, methodologies, and strategies employed in the selected publications that address security engineering within CPS. A total of 86 articles were reviewed from the total of 240 papers obtained from the search results. The reviewed articles analysed Security engineering for Cyber-Physical Systems, with a particular emphasis on innovative proposals, formalisation, meta-studies, implementation, integration/transformation, evaluation, and case studies. This preliminary stage involves using various search terms to evaluate relevant research articles from selected databases, including Google Scholar, Scopus, and Web of Sciences. It is necessary to assess the appropriateness of these terms in addressing the research inquiries. Table 1 displays the combination of terms employed to extract relevant documents.

The subsequent sections of the paper are organised in the following manner. Section 2 outlines the research methodology, whereas Section 3 presents the obtained results and findings. Section 4 discusses the societal considerations and lessons learned in employing qualitative research methodology, while Section 5 concludes the paper.

Table 1: Categories of relevant topics.

Category of topics
Adaptive systems and adaptability
Evolvable systems
Security Attack Pattern
Cyber-physical systems
Industrial internet of things
Security attack events
Security Engineering
Security requirements engineering
Threat Modeling
Model-driven security
Adaptive security solution
Security, privacy and Risk analysis
Adaptive-driven software development

2 RESEARCH METHODOLOGY

To conduct this work, a comprehensive literature review was undertaken. The research adopts several established methodologies (DeLoach, S.A. et al., 2017, Petersen, K et al., 2015), including research inquiries, search strategies, selection and validation processes, classification approaches, formal frameworks and models, meta-analyses, and an examination of various threats, attacks, and incidents. Moreover, the study adheres to these methodologies to ensure rigor and reliability. In the subsequent subsection, the research questions guiding the selection and analysis of the articles will be discussed, with a focus on their methodological significance.

2.1 Research Question

This section outlines recent advancements in security engineering for cyber-physical systems through the formulation of key research question. The research question (RQ) detailed below have guided the comprehensive review process.

RQ: What are the key research objectives and methodological approaches used in security engineering for Cyber-Physical Systems

2.2 The Review Process

The review process includes employing a reputable database to conduct a thorough search for relevant articles that align with the selected topic. These databases have extensive usage and are highly recognized, with numerous publications on cyber security being included in their indexes. The articles were selected using search strings that include operators such as "and" and "or", as well as keywords like "cyber security", "CPS", and "security engineering". In addition, the search process also involves manually browsing through highly cited papers and applying forward search through the use of Google Scholar. Tables 5 and 6 demonstrate types of papers, Journals, and conferences. In order to gather the articles, various potential sources have been investigated, including Google Scholar and Web of Science. While Google Scholar and Web of Science are widely used sources, the primary choice has been Scopus. Search strings were employed to restrict and evaluate articles that have been published in peer-reviewed Journals and conferences.

Table 2: Attempt one: searching for relevant papers.

Scopus	Google Scholar	Web of Science
total hits: 1400	Total hits: 440	Total hits: 216

Using the following combination of search terms has provided the following results (Cyber security AND CPS) OR (security engineering AND CPS) Cyber security AND security engineering OR (cyber-physical Systems)

Table 3: Attempt two: searching for relevant papers.

Scopus	Google Scholar	Web of Science
total hits: 840	Total hits: 360	Total hits: 116

Following the search process, a total of 240 peer-reviewed articles were initially identified. To ensure both feasibility and relevance, the selection was refined based on the specific requirements of the study. Citation rank was employed as a criterion for this process, resulting in the exclusion of 240 articles with fewer than four citations. Additionally, 83 articles were deemed outside the scope of the study. Ultimately, 86 articles that aligned with the established criteria and addressed the research questions were selected for inclusion. Tables 2 and 3 present the frequency of attempts made to identify relevant articles.

The articles in this study have been categorised into two primary classifications: conceptual and empirical research. Moreover, the review process for this study has specifically examined articles published from 2008 to 2023, covering a span of 15 years. By using the publication year as a criterion, the search process has effectively excluded articles that do not meet the specified criteria. However, this approach has also had a detrimental effect on articles that could have been included, provided their topic aligns with

the study's objective. Another criterion employed in the search process involves excluding papers that do not offer comprehensive research output, such as position papers, short papers, poster papers, technical reports, and book chapters.

The papers have been excluded due to their incomplete analysis and the difficulty in drawing conclusive results. Moreover, the inclusion or exclusion of papers has been determined based on the bibliographic information. The bibliographic information for the papers included in this study has been automatically extracted from Scopus. This information includes the paper title, authors' affiliation, country, conference venue, year of publication, and the number of citations. The extraction process involves employing Scopus, Google Scholar, and Web of Science.

Exclusion and Inclusion Criteria. This study aims to comprehensively review relevant literature on security engineering driven cyber physical systems from multiple perspectives, considering both the research contributions and methodologies, as well as the focus of the studies, irrespective of their specific research approaches. Workshop publications and regional conferences were excluded from the analysis due to inconsistencies in quality and impact, as well as their limited citation consideration. Furthermore, short papers were omitted because they typically lack the depth found in full research articles, particularly in terms of methodology, data collection, and findings. Finally, feasibility studies with low citation counts were also excluded from the review.

This evaluation has only included publications that use security engineering methodologies, as long as they are applicable to cyber security within the realm of cyber-physical systems, in order to fulfill the inclusion criteria. The primary emphasis of the paper relates to the current developments in security engineering for cyber-physical systems. Only papers that focus solely on security engineering and present independent research techniques and designs within the cyber security field have been selected as more relevant to the goal of this review process. The grounded analysis technique (Kai Petersen, et al., 2015, Adolph, S et al., 2011) was employed during the review process to aid in the classification and selection of papers for this study. This technique facilitated the identification of papers in the security engineering domain that we were already familiar with, and we further analyzed them using the reference links to find related papers. Tables 6 and 7 display the various types of papers, along with their research design respectively. Moreover, the tables provide information on the type of journal and conference venues associated with each paper.

Table 4: Key words used for searching.

Most Frequent Keywords
Cyber security, Security, Attack Surface Analysis
Cyber-Physical Systems Security, Cyber-Physical Energy Systems
privacy and Threat Modeling
Security attack, Security Engineering
Model driven engineering, Security Requirements Engineering
Security events, Cybersecurity Frameworks
Attack monitoring, Advanced Persistent Threats (APT)
vulnerability, Security Evaluation
Threat, Case Study Analysis
Security incident, Industrial Control Systems (ICS) Security
Adaptive, Smart Grid Security, Internet of Things (IoT) Security
Cyber risk, Risk Classification
Adaptive framework, STRIDE, Systematic Mapping

2.3 Initial Analysis of the Selected Papers

RQ: What are the research objectives and the methodologies employed in the development of security engineering approaches for CPS? The incorporation of publication year as a selection criterion has considerably improved the rigor and efficiency of the paper selection process. A minimum citation requirement of four was implemented, which automatically biases the results in favor of older articles that have had more time to gather citations. As a result, articles with fewer than four citations were omitted from the analysis. An in-depth analysis of the chosen literature uncovers new trends in the development of innovative methodologies and experimental implementation strategies. There has been a gradual rise in the number of studies employing integration and extension approaches. This analysis indicates that research using and integrating previous methodologies has received heightened academic interest and relevance. The review includes research using previous methodologies, specifically those conducted by A. Humayed et al., 2017, Banerjee et al. (2012), Raspotnig et al. (2012), Moore et al. (2011), Kephart et al. (2013), Mirko et al. (2008), Tounsi et al. (2017), Awotunde et al. (2023), Massimo et al. (2022), and Ainslie et al. (2023).

This study demonstrates that the selected papers

Table 5: Types of papers used for the study.

Types of papers	Description
Proposal	Publications that propose something new, e.g., a language, extension, integration, algorithm
Formalization	If the publication contains axioms,, some formal logical language, relating to the proposal, it has a formalization
Meta-Study	Publication which provided a significant overview of existing work or a study of existing research
Implementation	Publication that mention the development of a tool or implementation
Integration	Category was assigned if the publication contribution described two different, distinct, named things
Extension	Publication which focuses on some concepts which are not named language or method
Evaluation case study	The publication includes a case study which evaluates the contribution

have analysed and made significant progress in the domain of security engineering. Among these papers, six were deemed irrelevant as they exhibited a similarity in subject matter but did not correspond with the aim of this study. These papers were deficient in terms of clearly defined research methods throughout their study. Publications that lack the specified research strategy have been excluded due to their apparent irrelevance. Moreover, this study has revealed a substantial increase in research focus on security engineering in the last decade. This is noticeable from the considerable amount of references related to cyber security, security and privacy, and adaptive security, as shown in Table 5. The study also encompassed articles published in conferences and journals that were relevant to the chosen articles for this review process.

3 ANALYSIS AND RESULT

Data Collection and Analysis. Table 7 presents a systematic overview of the research designs employed in the publications analyzed in this study. The identified methodologies include "New Proposals," "Formalization," "Meta-Study," "Implementation," "Integration," "Extension," and "Evaluation Case Study." The analysis further reveals an increasing scholarly focus on research investigating disparities (adaptations) and employing case study methodologies. Additionally, there is a discernible upward trend in research output within the domain of security engineering for cyber-physical systems, underscoring the growing academic interest in this field. The majority of the reviewed studies introduce theoretical propositions, which are subsequently validated through empirical research utilizing real-world applications. By implementing methodologically rigorous case studies, these studies offer robust empirical evidence in support of their proposed frameworks and methodologies, thereby contributing to the advancement of knowledge in this domain. In response to their research questions, the articles that have been documented in table 7 are those that have presented novel proposals and research methods to address the problem that they have specified. In addition, there are articles that demonstrate the use of more than two different research designs. "A goal-driven approach for adaptive system" by (Kephart, J. et al., 2013) and security analysis for socio-technical systems by (Antoineailliau et al., 2019) are two examples of articles that fall into this category.

Several studies incorporate multiple research design objectives. Notable examples include "A Goal-Based Modelling Approach to Develop Requirements of an Adaptive System with Environmental Uncertainty" by Kephart et al. (2013) and "Holistic Security Requirements Analysis for Socio-Technical Systems" by Antoineailliau et al. (2019). Additionally, two studies proposed a research framework and subsequently validated it through comprehensive case studies, demonstrating the applicability and robustness of their approach. In both cases, the proposed framework was developed, empirically tested, and systematically evaluated within real-world contexts. Table 7 provides a visual representation of the various research designs employed to effectively address multiple research questions.

Research Method Used in the Selected Articles. This section provides an evaluation of the research methodologies employed in the selected publications. Through a systematic screening process, a total of 86 papers were identified for inclusion in this study. Among these, seven studies utilized a case study approach, three employed a survey-based methodology, and three adopted a mixed-methods approach. The specific details are presented in Table 9. Furthermore, this study identified six publications that employed quantitative data analysis methods, including

Table 6: Types of Journal and Conference.

Types of Journal and conference	Articles
International Conference on the Internet of Things (IoT)	(C. Klötzer, 2015)
Practise of Enterprise Modeling Conference	(A. Banerjee, 2012, Kephart, J. 2013)
Journal of Intelligence Information Systems	(Silva S, 2011)
Requirement Engineering Journal	(Moore, 2011)
International Conference on Software Specification and Design	(Mburu, 2016)
ACM Transaction on Autonomous use and Adaptive Systems(TAAS)	(Zhu, B, 2011, Li, T., 2014)
Requirement Engineering Conference	(Lin, J, 2017, ; Van L, 2011; Baumgarten, 2012)
International Journal of Software Engineering and Knowledge Engineering(IJSEKE)	(Kephart, J. 2013)
System Modeling journal (SoSym)	(Cheminod, M, 2013, Antoine, 2019)
International Journal on Systems of Systems Engineering	(Turpe, S, 2017)
International Conference on Software Engineering	(Yan, Y, 2012)
International Symposium on Engineering Secure Software and Systems, ESSoS	(Hafiz, M., 2009)
IEEE Transaction on Software Engineering	(Yampolskiy, M, 2013, Van L, 2011)
International Conference on Model Driven Engineering Language and Systems	(Kephart, J. 2013)

Table 7: Research design used in the selected papers.

Research Design	Articles
Proposal	(Van Lamsweerde, 2011; Turpe, S, 2017; Raspotnig, C.,, 2012; Moore, 2011; Türpe, S., 2018 Baumgarten, M., 2012; Gharib, M., 2022)
Formalization	(Zhu, B, 2011, Lin, J, 2017, Li, T, 2014; Mburu, L, 2016)
Meta-Study	(Yan, Y, 2012, Baumgarten, M, 2012)
Implementation	(Pasqualetti, F, 2013; Zonouz, S., 2014; Kephart, J, 2013; Teixeira, A.,2015; Zhu, Q. 2011; Mo, Y., Kim, 2012; Bresciani, 2014; Cheminod, M, 2013, Yampolskiy, M, 2013)
Integration	(Sandberg, H. 2015; Srivastava, A., 2016; Wang, Y, 2013; Mirko, 2008; Moore,, 2011; Kephart, J., 2013; A. Banerjee, 2012)
Extension	(Moore, 2011; Raspotnig, C., 2012)
Evaluation case study	(Yan, Y, 2012, Antoine, 2019)

(Humayed, A.,, et al., 2017; Khalid, F., et al., 2022; Kim, D et al., 2022; Li, S., etal., 2016; Zografopoulos, I., et al., 2017; Kephart et al. (2013), Antoine et al. (2019), Moore et al. (2011), Silva et al. (2011), Mirko et al. (2008), and Van L. et al. (2012).

The corresponding results are summarized in Table 8. Conversely, several studies, including those by (Shevchenko, N, etal., ; 2018, Xiong, W.,et al., 2019; Tatam, J. etal., 2021; Valenza, F. etal., 2020; Kriaa, etal., 2015; Mekdad, Y. etal., 2021; Neubert, S. etal., 2020; Paudel, S.etl., 2017; Raspotnig et al. (2012), Baumgarten et al. (2012), Turpe et al. (2017), and Gharib et al. (2022), applied qualitative data analysis techniques, as detailed in Table 8. Additionally, three studies, including those by Li et al. (2018) and Mburu et al. (2016), integrated multiple methodological approaches. Notably, among the selected publications, only one study, conducted by Turpe et al. (2017), adopted a conceptual framework as its primary research methodology.

This study revealed that a significant proportion of the reviewed papers relied on pre-existing methodologies, with many studies employing an approach that incorporates and extends established techniques. Specifically, among the analyzed publications, seven introduced novel research proposals, including those by (Kim, D., etal, 2022; Valenza, F. etal., 2020; Khalid, F. etal., 2022; Tatam, J., etal., 2021; Shevchenko, N. etal., 2018; Neubert, S. etal., 2020; Kephart et al. (2013), Antoine et al. (2019), Moore et al. (2011), Van L. et al. (2012), Raspotnig et al. (2012), Baumgarten et al. (2012), Turpe et al. (2017), and Gharib et al. (2022). Additionally, four studies focused on various forms of methodological integration, namely Kriaa, S etal., 2015; Mekdad, Y., etal., 2021; Xiong, W. etal., 2019; Humayed, A et al., 2017; Li, S. etal., 2016; Banerjee et al.

Table 8: Summary of the data analysis method used in the selected articles.

Data Analysis Method	Articles
Quantitative	(Humayed, A.,, 2017, Khalid, F., 2022, Kim, D., 2022, Li, S., 2016, Zografopoulos, I., 2017, Kephart, J., 2013; Antoine, 2019; Zhu, B, 2011; Lin, J, 2017; Moore, 2011; Mirko, 2008; A. Van, 2019)
Qualitative	(Shevchenko, N, 2018, Xiong, W., 2019, Tatam, J.,, 2021, Valenza, F.,, 2020, Kriaa, 2015, Mekdad, Y.2021, Neubert, S.,, 2020, Paudel, S., 2017, Raspotnig, C.,, 2012; Baumgarten, M., 2012; Turpe, S, 2017; Gharib, M., 2022; Cheminod, M, 2013, Yampolskiy, M, 2013)

(2012), Moore et al. (2011), Kephart et al. (2013), and Silva Souza et al. (2011). Two papers, Moore et al. (2011) and Raspotnig et al. (2012), adopted an extension-based approach, building upon previous research and methodologies. Moreover, studies by Li et al. (2014) and Antoine et al. (2019) demonstrated a degree of formalization, particularly in terms of the classification and categorization of research contributions. Furthermore, four publications—Kephart et al. (2013), Bresciani et al. (2014), and Silva et al. (2011)—employed experimentation as a primary research method.

Based on the study's findings, it can be inferred that over fifty percent of the publications suggest innovative techniques or approaches, while the rest of the papers mainly depend on established methodologies. Researchers in the subject of cyber security, particularly in security engineering, often use empirical research methods such as surveys, case studies, mixed methods, and experiments. However, security engineering solutions rely less on conceptual analysis as a research design process. Furthermore, this study has definitively shown that case studies have been used as a research approach in over fifty percent of the papers. Furthermore, it indicates an inclination for prolonged usage, specifically in studies that include qualitative data analysis.

This study makes a significant contribution by looking at and assessing the research strategy employed and the extent to which qualitative and quantitative data analysis methods have been applied in the field of security engineering. In furthermore, the study reveals that the quantitative research data analysis method has been widely used in the selected papers that underwent review. This can be observed in articles authored by (Humayed, A.,, 2017, Khalid, F., 2022, Kim, D., 2022, Li, S., 2016, Zografopoulos, I., 2017, Van Lamsweerde et al 2011; Gharib, M et al., 2022; Moore et al., 2011; Antoine et al., 2019; Kephart, J., 2013; Bresciani, P et al., 2014 and Silva S et al., 2011), as indicated in Table 8. Furthermore, these papers employed the research strategies of case study and survey. On the contrary, studies conducted by ((Shevchenko, N, 2018, Xiong, W., 2019, Tatam, J.,, 2021, Valenza, F.,, 2020, Kriaa, 2015, Mekdad, Y.2021, Neubert, S.,, 2020, Paudel, S., 2017, Turpe, S. et al., 2017; Raspotnig, C., et al., 2012;Baumgarten, M et al., 2012; Gharib, M et al., 2022; Mirko et al., 2008; Moore et al., 2011; Kephart, J., 2013; A. Banerjee et al., 2012) have employed qualitative data analysis, and used case study research strategy. Moreover, the papers by (Turpe, S et al., 2017; Raspotnig, C., et al., 2012; Baumgarten, M et al., 2012 ; Turpe, S et al., 2017) used interviews and questionnaires as methods for collecting data. On the other hand, the papers by (Paudel, S. et al. 2017, Van Zografopoulos, I, 2017, Lamsweerde et al 2011; Gharib, M et al., 2022; Moore et al., 2011; Antoine et al., 2019; Kephart, J., 2013; Bresciani, P., et al., 2014; and Silva S et al., 2011) employed experiments as their data collection methods.

The reviewed studies were categorized into two primary classifications: empirical and conceptual research. Within the empirical category, both quantitative and qualitative data collection methods were utilized, with surveys and case study methodologies being the most frequently employed approaches. Importantly, a considerable proportion of studies in the domain of security engineering for cyber-physical systems (CPS) predominantly adopted quantitative research methodologies. However, several studies revealed limitations in conducting rigorous empirical evaluations, despite assertions of having undertaken such assessments. For instance, Li et al. (2014) reported the use of empirical evaluation; however, a more in-depth analysis exposed shortcomings in both validity and practical applicability. This highlights the challenges encountered by many studies in aligning methodological rigor with their stated research objectives. A total of 85 publications incorporated empirical evaluations, emphasizing the critical role of long-term empirical investigations and industrial case studies in assessing various research methodologies. This is particularly relevant to the field of Security Engineering for Cyber-Physical Systems, which constitutes the primary focus of this study. The reliance on these comprehensive assessments reflects the field's ongoing shift towards more rigorous and application-oriented research approaches.

Validity of Research Method. This study attempted

to evaluate the reliability of research methodologies (Denscombe, M. et al., 2010; Morrow, S.L., et al., 2005, Petersen, K. 2015,Kitchenham, B 2007) designed to ensure that the study accurately measures or tests its intended objectives, hence enhancing the credibility of the research. The study considered the criteria of internal and external validity to identify the limitations of each review article in the use of diverse research methodologies.

Table 9: Research Method.

Research Method	**Articles**
Case study	(Zhu, B, 2011, Lin, J, 2017, Kriaa, S., 2015, Mekdad, Y., 2021, Neubert, S.2020, Paudel, S., 2017, Zografopoulos, 2017, Moore, 2011; Kephart, J., 2013; Moore, 2011; Antoine, 2019; Van L, 2011; Turpe, S, 2017)
Survey	(Harkat, H.,, 2024, A. Humayed, 2017, Raspotnig, C., 2012; Baumgarten, M., 2012; Gharib, M.,, 2022 ; Türpe, S. 2018)
Mixed	(Kriaa, S., , 2015, Mekdad, Y, 2021, Cheminod, M, 2013, Yampolskiy, M, 2013, Li, T., 2014; Mburu, L.W., 2016)
Conceptual Framework	(Shevchenko, N, 2018, Xiong, W, 2021 Yan, Y, 2012, Valenza, F. 2020, Turpe, S, 2017)

Internal Validity. We assess the cause-and-effect connection between the components under study in the case studies (Methods Map - SAGE Research Methods). This study has found a constraint in empirical research that systematically analyzes the implementation of extensive case studies. The review as shown in Table 9, substantiates this finding. Proficient application and implementation of the suggested frameworks and experiments in extensive case studies involving a substantial number of participants necessitate a significant level of competence in the particular discipline. The research methodology employed in many works, including articles (Shafi, Q. et al., 2012; Moore, et al., 2011; Kephart, J. et al., 2013 ; A. Banerjee et al., 2012), entailed the implementation of empirical investigations using a quantitative approach, specifically employing a case study strategy and experiment.

Nevertheless, it is crucial to acknowledge that these papers have limitations due to the fact that the evaluation and experimentation were exclusively conducted by the authors within controlled settings, such as research groups. To enhance the quality and dependability of their approach, the authors suggest conducting assessments and experiments with external users in their future research endeavours, with the objective of guaranteeing trustworthiness (Brink, H.. et al., 1993)

Transferability and External Validity. This study analysed the constraints of the articles in relation to their method of research, enabling an assessment of their external validity. Transferability is a standard that guarantees reliability by highlighting external validity. The study analyses the degree to which its findings can be reproduced in various contexts (Mirko Morandini et al., 2008). Articles (Antoine et al., 2019; Moore et al., 2011; A. Banerjee et al., 2012; A. Van Lamsweerde et al., 2011; Baumgarten, M., et al., 2012) employed illustrative scenarios and created a prototype tool to evaluate their proposal, although limited to the control ground.

In the context of construct validity, an essential criterion concerns the extent to which a test accurately measures the concept it is intended to assess. It is generally recommended that customer-centric approaches—particularly those directly impacting end users—undergo testing and evaluation by domain experts, excluding the authors of the proposed approach, to ensure unbiased validation. This form of validation is particularly crucial in critical systems, such as adaptive security solutions for Air Traffic Management Systems, financial sector security, and other domains with comparable requirements. However, the review of existing literature reveals that a majority of the analyzed studies lack this essential validation. Instead, many were evaluated solely by experts from external domains, aiming to establish external validity rather than ensuring comprehensive construct validity (Brink et al., 1993; Morrow et al., 2005)

Dependability and Reliabiltiy. Dependability, the fourth criterion, pertains to the issue of reliability. It involves demonstrating that if a study were to be replicated under identical conditions, using the same methods and participants, it would yield consistent results (Denscombe et al., 2010; Morrow et al., 2005). Moreover, reliability is a relative concept that reflects the extent to which data analysis is influenced by the specific researchers conducting the study. The findings of this review indicate that articles in which the validation process is conducted exclusively by the authors of the proposed approach exhibit a lack of reliability. A notable example is the study by Baumgarten et al. (2012), which employed a qualitative research methodology. However, as the evaluation and validation were performed solely by the authors, the study's reliability is diminished, making its applicability to real-world scenarios more challenging.

To mitigate this limitation, it is essential that the proposed solution undergo evaluation not only by its

authors but also by independent researchers. Self-evaluation by the original researchers poses a threat to the validity of the study, as it limits the generalizability of the findings and raises concerns regarding potential biases. To ensure the validity of the evaluation, external participants should be involved in assessing its effectiveness, thereby enhancing the credibility and applicability of the research.

Challenges Associated with the Review Process. This section focuses on the issues faced during the review process, with a particular focus on those connected to the analysis and results. From the original pool of 240 publications, only the top 86 were selected based on their direct alignment with the study's purpose. Any papers that had less than four citations were not taken into account. Furthermore, works that had fewer than two citations, according to Scopus, were considered to have an invalid conclusion. The reason for this is that shorter publications frequently lack a thorough research strategy, which is a crucial element of a research technique. However, the review method unintentionally omitted a substantial number of intriguing articles that expressly focus on the subject area of security engineering for cyber-physical systems by eliminating papers with less than four citations. In addition, this study only evaluates articles that satisfy the requirements of having at least four citations and undergoing peer review. As a result, it did not incorporate recent papers and contributions on this subject, which may have possibly been used as sources for qualitative and quantitative techniques.

Another issue that demonstrated bias is the use of inclusion and exclusion criteria for the selection of papers. The determination of the inclusion and exclusion criteria in this study was purely based on the author's subjective judgment, making them very prone to error. Our personal interest has informed our selection of articles that specifically address security engineering for cyber-physical systems. However, we excluded other relevant studies either based on our personal preference or because they did not correspond with a certain study plan. Assessing the robustness of studies is often challenging due to the presence of numerous assumptions, such as the lack of adequate justification for the selection of data collection and analysis methods in the chosen articles. However, several papers include a section where they explicitly acknowledge the limitations of their study. Some even provide a discussion of these limitations in the conclusion and future work section. This information is valuable for assessing the extent to which research methodologies were employed and proved helpful during the review process.

Authors employing a case study as a research method have expressed concerns. This concern relates to the extent to which their findings can be applied to a broader population. For example, papers such as (Kephart, J et al., 2013; Antoine et al., 2019 ; Moore, Andrew et al., 2011 ; Shafi, Q. et al., 2012; A. Van Lamsweerde et al., 2011) suffer from a lack of generalizability in their findings. In order to enhance the reliability of qualitative research, it is essential for papers using a case study as a research strategy to explicitly demonstrate the methods employed for data collection and analysis. Additionally, these papers should include an evaluation of transferability, confirmability, credibility, and dependability in relation to their findings. It is observed that many papers in the field of security engineering for cyber-physical systems fail to provide such information.

Moreover, this study has ascertained that the qualitative technique to data analysis is constrained in its ability to explore questions related to the causes and methodologies underlying specific events. The articles reviewed in this study have mostly concentrated on finding different variables associated with security engineering. While qualitative research studies are commonly used scenarios, they were unable to demonstrate how applicable they were. Conducting an online survey using a self-selecting sampling approach severely limits the capacity to apply the findings to a larger population. Several research studies have used triangulation as a method to gather data from several sources of verification, including extensive data sets such as publications (Kephart, J. et al., 2013; Bresciani, P., et al., 2014; Moore, et al., 2011; Li, T. et al., 2014). Other research employed a hybrid methodology for data collecting, notably adopting the approach used by (Van Lamsweerde et al., 2011).

Societal Considerations and Lessons Learned Within the Realm of Cyber Physical-Systems. It is essential for researchers to cultivate the necessary expertise to identify and apply appropriate research methodologies that effectively establish the relationship between the applicability and reusability of their proposed approaches. As highlighted in the reviewed literature, some findings could not be independently verified, underscoring the importance of methodological rigor. To enhance the reliability and impact of their contributions, researchers should strive to produce valid and replicable findings that can be utilized by scholars both within and beyond their immediate field of study. People, operational procedures, cutting-edge technology, and physical structures are all components of CPS, which are complex systems that include all of these elements. When it comes to the development of security solutions for CPS, it is of the utmost importance to take into consideration the

social aspect or social domain as one of the key components to be considered in the early stages of system development.

The research we have undertaken provides a full analysis of security engineering, considering it in terms of three layers of CPS: The business layer is responsible for conceptualizing the social component, the application layer is responsible for the software, and the infrastructure layer is responsible for deploying the system. The business layer serves as the main entry point for any potential security breaches that may occur inside these three layers. The security breach might be attributed to the business layer. Regarding cybersecurity, studies that concentrate on the business aspects generally adopt a qualitative methodology, whereas research that centers on the application and infrastructure layer typically employs a quantitative methodology. Both methodologies were considered in all of the selected papers during the review process. This assessment procedure has suggested a modest rise in the use of the quantitative approach as a research method in the sector of cybersecurity.

4 CONCLUSION

This study provides a comprehensive systematic review of security engineering methodologies applied to Cyber-Physical Systems (CPS), analyzing 86 selected papers published over the past 15 years. Our findings reveal a strong emphasis on empirical research methodologies, particularly case studies, surveys, and mixed-method approaches, demonstrating the field's shift toward application-driven and evidence-based security engineering. The analysis highlights a predominant reliance on quantitative methodologies, reinforcing the growing importance of integrating established techniques to address CPS security challenges effectively.

Despite these advancements, our study identifies critical gaps in the literature, including limited generalizability of findings, insufficient external validation, and inconsistencies in empirical rigor. Many security engineering frameworks lack extensive real-world evaluation, making their practical applicability uncertain. Addressing these challenges requires stronger interdisciplinary collaborations, robust validation processes, and the development of scalable, adaptable security models that align with the dynamic nature of CPS environments. This study contributes to the field by offering a structured assessment of existing security engineering methodologies, identifying key trends, and outlining essential research directions for the future. The findings underscore the necessity of advancing context-aware, adaptive security solutions that integrate cyber and physical domains while incorporating both technical and socio-technical considerations. Future research should focus on developing innovative security paradigms that balance theoretical robustness with practical applicability, ensuring that CPS remain resilient in the face of evolving cyber threats.

By bridging the gap between theoretical models and practical implementations, this study provides a foundation for enhancing the security engineering landscape within CPS. We advocate for a more systematic approach to evaluating and refining security frameworks, fostering a research environment that prioritizes empirical validation, cross-domain applicability, and sustainable security practices.

REFERENCES

A. Humayed, J. Lin, F. Li and B. Luo, "Cyber-Physical Systems Security—A Survey," in IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1802-1831, Dec. 2017

Harkat, H., Camarinha-Matos, L. M., Goes, J., & Ahmed, H. F. T. (2024). Cyber-physical systems security: A systematic review. Computers and Industrial Engineering, 188, 109891.

Petersen, K., Feldt, R., Mujtaba, S., & Mattsson, M. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. Information and Software Technology, 64, 1-18.

Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering (EBSE Technical Report No. EBSE-2007-01). Keele University and Durham University. Retrieved from

Urbach, N.; Röeglinger, M. Introduction to Digitalization Cases: How Organizations Rethink Their Business for the Digital Age; Springer: Berlin/Heidelberg, Germany, 2019

Cardenas, A. A., Amin, S., & Sastry, S. (2008). Research challenges for the security of control systems. Proceedings of the 3rd Conference on Hot Topics in Security, 6.

Krotofil, M., & Gollmann, D. (2013). Industrial control systems security: What is happening? Proceedings of the 11th IEEE International Conference on Industrial Informatics, 670-675.

Kwon, C., Liu, W., & Hwang, I. (2013). Security analysis for cyber-physical systems against stealthy deception attacks. Proceedings of the American Control Conference, 3344-3349.

Mo, Y., Kim, T. H., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2012). Cyber-physical security of a smart grid infrastructure. Proceedings of the IEEE, 100(1), 195-209.

Pasqualetti, F., Dorfler, F., & Bullo, F. (2013). Attack detection and identification in cyber-physical systems.

IEEE Transactions on Automatic Control, 58(11), 2715-2729.

Sandberg, H., Teixeira, A., & Johansson, K. H. (2015). Cyber-physical security in networked control systems: An introduction to the issue. IEEE Control Systems Magazine, 35(1), 20-23.

Srivastava, A., & Amin, S. (2016). Cyber-security and privacy in cyber-physical systems: Threats and defenses. IEEE Transactions on Sustainable Computing, 1(2), 110-112.

Teixeira, A., Shames, I., Sandberg, H., & Johansson, K. H. (2015). A secure control framework for resource-limited adversaries. Automatica, 51, 135-148.

Wang, Y., & Lu, X. (2013). Cyber security in the Smart Grid: Survey and challenges. Computer Networks, 57(5), 1344-1371.

Zhang, Y., Xiang, Y., Wang, L., Wright, M., & Liu, S. (2012). Enhancing cyber-physical systems with wireless sensor and actuator networks. Ad Hoc Networks, 10(3), 233-244.

Zhu, B., Joseph, A., & Sastry, S. (2011). A taxonomy of cyber attacks on SCADA systems. Proceedings of the International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, 380-388.

Zhu, Q., & Başar, T. (2011). Robust and resilient control design for cyber-physical systems with an application to power systems. Proceedings of the 50th IEEE Conference on Decision and Control and European Control Conference, 4066-4071.

Zonouz, S., Rrushi, J., & Rogers, K. (2014). Detecting industrial control malware using automated PLC code analytics. Proceedings of the 19th European Symposium on Research in Computer Security, 439-456.

Khalid, F., Latif, K., & Latif, S. (2022). A systematic mapping study on security requirements engineering approaches for cyber-physical systems. Journal of Systems and Software, 183, 111091.

Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. (2017). STRIDE-based threat modeling for cyber-physical systems. Proceedings of the IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 1-6

Kim, D., Kim, J., & Kim, H. (2022). Security risk assessment framework for cyber-physical systems using STRIDE and DREAD. Sensors, 22(3), 1045

Kriaa, S., Bouissou, M., & Pièrre-Cambacédès, L. (2015). Modeling the Stuxnet attack with BDMP: Towards more formal risk assessments. Proceedings of the 7th International Conference on Risks and Security of Internet and Systems (CRiSIS), 1-8.

Li, S., Tryfonas, T., & Li, H. (2016). The Internet of Things: A security point of view. Internet Research, 26(2), 337-359

Mekdad, Y., Chehab, A., & Tawil, R. (2021). A threat model method for ICS malware: The TRISIS case. Computers & Security, 105, 102224.

Neubert, S., & Vielhauer, C. (2020). Kill chain attack modeling for hidden channel attack scenarios in industrial control systems. Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES), 1-6.

Paudel, S., Clements, S., & McLaughlin, K. (2017). Attack models for advanced persistent threats in smart grid wide area monitoring. Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR), 1-8.

Shevchenko, N., Chick, T., O'Riordan, P., Scanlon, T., & Woody, C. (2018). Threat modeling: A summary of available methods. Carnegie Mellon University Software Engineering Institute.

Tatam, J., Jones, K., & Janicke, H. (2021). A review of threat modelling approaches for APT-style attacks. Journal of Cyber Security Technology, 5(2), 85-106.

Valenza, F., Armando, A., & Compagna, L. (2020). A hybrid threat model for smart systems. Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES), 1-10

Xiong, W., & Lagerström, R. (2019). Threat modeling—A systematic literature review. Computers & Security, 84, 53-69.

Zografopoulos, I., Koutsandria, G., & Maniatakos, M. (2017). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Transactions on Emerging Topics in Computing, 5(3), 391-407

Awotunde, J. B., Oguns, Y. J., Amuda, K. A., Nigar, N., Adeleke, T. A., Olagunju, K. M., & Ajagbe, S. A. (2023). Cyber-physical systems security: analysis, opportunities, challenges, and future prospects. Blockchain for Cybersecurity in Cyber-Physical Systems, 21-46.

Boyes H, Hallaq B, Cunningham J, Watson T. The industrial internet of things (IIoT): An analysis framework. Computers in industry. 2018 Oct 1;101:1-2.

Griffor, E. R., Greer, C., Wollman, D. A., & Burns, M. J. (2017). Framework for cyber-physical systems: Volume 2, working group reports.

Henzinger, Tom, Edward A. Lee, Alberto Sangiovanni-Vincentelli, Shankar Sastry, Alex Aiken, Dave Auslander, Ruzena Bajcsy et al. "Center for Hybrid and Embedded Software Systems." (2008).

Baheti, R., & Gill, H. (2011). Cyber-physical systems. The impact of control technology, 12(1), 161-166.

Poovendran, R. (2010). Cyber-physical systems: Close encounters between two parallel worlds [point of view]. Proceedings of the IEEE, 98(8):1363-1366

Shafi, Q. (2012). Cyber physical systems security: A brief survey. In 2012 12th International Conference on Computational Science and Its Applications, pages 146-150. IEEE

Massimo G., Cassavia, N., Pisani, F. S., & Manco, G. (2022). Boosting cyber-threat intelligence via collaborative intrusion detection. Future Generation Computer Systems, 135, 30-43.

Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. Computers & Security, 132, 103352.

Tounsi, W., & Rais, H. (2018). A survey on technical threat

intelligence in the age of sophisticated cyber attacks. Computers & security, 72, 212-233.

Conway, John. "The Industrial Internet of Things: an evolution to a smart manufacturing enterprise." Schneider Electric (2016).

C. Klötzer and A. Pflaum, "Cyber-physical systems as the technical foundation for problem solutions in manufacturing, logistics and supply chain management," 2015 5th International Conference on the Internet of Things (IOT), Seoul, Korea (South), 2015

A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee and S. K. S. Gupta, "Ensuring Safety, Security, and Sustainability of Mission-Critical Cyber-Physical Systems," in Proceedings of the IEEE, vol. 100, no. 1, pp. 283-299, Jan. 2012

Li, T., Horkoff, J. (2014). Dealing with Security Requirements for Socio-Technical Systems: A Holistic Approach. In: Jarke, M., et al. Advanced Information Systems Engineering. CAiSE 2014. Lecture Notes in Computer Science, vol 8484. Springer, Cham.

Ali, R., Dalpiaz, F. & Giorgini, P. A goal-based framework for contextual requirements modeling and analysis. Requirements Eng 15, 439-458 (2010).

Li, T., Horkoff, J., Mylopoulos, J. (2014). Integrating Security Patterns with Security Requirements Analysis Using Contextual Goal Models. In: Frank, U., Loucopoulos, P., Pastor, Ó., Petrounias, I. (eds) The Practice of Enterprise Modeling. PoEM 2014. Lecture Notes in Business Information Processing, vol 197. Springer, Berlin, Heidelberg

Antoineailliau and Axel Van Lamsweerde. 2019. Runtime Monitoring and Resolution of Probabilistic Obstacles to System Goals. ACM Trans. Auton. Adapt. Syst. 14, 1, Article 3 (March 2019), 40 pages.

Li, T., Horkoff, J. & Mylopoulos, J. Holistic security requirements analysis for socio-technical systems. Softw Syst Model 17, 1253-1285 (2018)

Türpe, S., 2017, September. The trouble with security requirements. In 2017 IEEE 25th International Requirements Engineering Conference (RE) (pp. 122-133). IEEE.

Yoder, J. and Barcalow, J., 1997, September. Architectural patterns for enabling application security. In Proceedings of the 4th Conference on Patterns Language of Programming (PLoP'97) (Vol. 2, p. 30).

Fernández, Eduardo B., Mihai Fonoage, Michael VanHilst and Mirela Marta. "The Secure Three-Tier Architecture Pattern." 2008 International Conference on Complex, Intelligent and Software Intensive Systems (2008): 555-560.

Fernandez, Eduardo B. "Two Patterns for Web Services Security." In International Conference on Internet Computing, pp. 801-807. 2004.

Asnar, Yudis, Fabio Massacci, Ayda Saidane, Carlo Riccucci, Massimo Felici, Alessandra Tedeschi, Paul ElKhoury, Keqin Li, Magali Séguran, and Nicola Zannone. "Organizational Patterns for Security and Dependability: from design to application." International Journal of Secure Software Engineering (IJSSE) 2, no. 3 (2011): 1-22.

Fernandez-Buglioni, Eduardo. Security patterns in practice: designing secure architectures using software patterns. John Wiley & Sons, 2013.

Hafiz, M., Adamczyk, P. and Johnson, R.E., 2007. Organizing security patterns. IEEE software, 24(4), pp.52-60.

Scandariato, Riccardo, Koen Yskout, Thomas Heyman, and Wouter Joosen. "Architecting software with security patterns." CW Reports (2008).

Wang, E.K., Ye, Y., Xu, X., Yiu, S.M., Hui, L.C.K. and Chow, K.P., 2010, December. Security issues and challenges for cyber physical system. In 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing (pp. 733-738). IEEE.

Zhu, B., Joseph, A., & Sastry, S. (2011). A Taxonomy of Cyber Attacks on SCADA Systems. 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing

CheminodM., Durante, M., Durante, L., & Valenzano, A. (2013). Review of security issues in industrial networks. IEEE Transactions on Industrial Informatics

Lin J., Yu, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5),

Yan Y., Qian, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on cyber security for smart grid communications. IEEE Communications Surveys & Tutorials, 14(4), 998-1010

Yan Y., Qian, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on cyber security for smart grid communications. IEEE Communications Surveys & Tutorials, 14(4), 998-1010.

Yampolskiy, M., Horvath, P., Koutsoukos, X. D., Xue, Y., & Sztipanovits, J. (2013). Taxonomy for description of cross-domain attacks on CPS. Proceedings of the 2nd ACM International Conference on High Confidence Networked Systems, 135-142.

Bresciani, P., Perini, A., Giorgini, P., Giunchiglia, F. and Mylopoulos, J., 2004. Tropos: An agent-oriented software development methodology. Autonomous Agents and Multi-Agent Systems, 8, pp.203-236.

Li, T., Horkoff, J., Paja, E., Beckers, K. and Mylopoulos, J., 2015. Analyzing attack strategies through anti-goal refinement. In The Practice of Enterprise Modeling: 8th IFIP WG 8.1. Working Conference, PoEM 2015, Valencia, Spain, November 10-12, 2015, Proceedings 8 (pp. 75-90). Springer International Publishing.

Raspotnig, C., Karpati, P., Katta, V. (2012). A Combined Process for Elicitation and Analysis of Safety and Security Requirements. In: Bider, I., et al. Enterprise, Business-Process and Information Systems Modeling. BPMDS EMMSAD 2012 2012. Lecture Notes in Business Information Processing, vol 113. Springer, Berlin, Heidelberg

Dalpiaz, F., Borgida, A., Horkoff, J. and Mylopoulos, J., 2013, May. Runtime goal models: Keynote. In IEEE 7th international conference on research challenges in information science (RCIS) (pp. 1-11). IEEE.

Müller, H., Litoiu, M. and Mylopoulos, J., 2016, October. Engineering cybersecurity in cyber physical systems. In Proceedings of the 26th Annual International Conference on Computer Science and Software Engineering (pp. 316-320).

Axel Van Lamsweerde. 2009. Requirements Engineering: From System Goals to UML Models to Software Specifications (1st. ed.). Wiley Publishing.

V. E. S. Souza, "A requirements-based approach for the design of adaptive systems," 2012 34th International Conference on Software Engineering (ICSE), Zurich, Switzerland, 2012

A. Van Lamsweerde, "Goal-oriented requirements engineering: a guided tour," Proceedings Fifth IEEE International Symposium on Requirements Engineering, Toronto, ON, Canada, 2001, pp. 249-262, doi: 10.1109/ISRE.2001.948567.

Haley, C.B., Laney, R.C., Moffett, J.D. et al. Using trust assumptions with security requirements. Requirements Eng 11, 138-151 (2006)

Mburu, L.W. and Helbich, M., 2016. Environmental risk factors influencing bicycle theft: A spatial analysis in London, UK. PLoS one, 11(9), p.e0163354.

Feather, S. Fickas, A. van Lamsweerde and C. Ponsard, "Reconciling system requirements and runtime behavior," Proceedings Ninth International Workshop on Software Specification and Design, Ise-Shima, Japan, 1998

Moore, Andrew, Robert Ellison, and Richard Linger. "Attack Modeling for Information Security and Survivability." (Technical Note CMU/SEI-2001-TN-001). Carnegie Mellon University, Software Engineering Institute's Digital Library, Software Engineering Institute, 1 Mar. 2001.

C. Haley, Jonas. MoffettR. Laney, and B. Nuseibeh, "Security Requirements Engineering: A Framework for Representation and Analysis," in IEEE Transactions on Software Engineering, vol. 34, no. 1, pp. 133-153, Jan.-Feb. 2008, doi: 10.1109/TSE.2007.70754.

Qureshi, N.A., Jureta, I.J. and Perini, A., 2011. Requirements engineering for self-adaptive systems: Core ontology and problem statement. In Advanced Information Systems Engineering: 23rd International Conference, CAiSE 2011, London, UK, June 20-24, 2011. Proceedings 23 (pp. 33-47). Springer Berlin Heidelberg.

Kephart, J. and David M. Chess. "The Vision of Autonomic Computing." Computer 36 (2003): 41-50.

Betty H.C, B.H., Sawyer, P., Bencomo, N. and Whittle, J., 2009, October. A goal-based modeling approach to develop requirements of an adaptive system with environmental uncertainty. In International Conference on Model Driven Engineering Languages and Systems (pp. 468-483). Berlin, Heidelberg: Springer Berlin Heidelberg.

Silva Souza, V.E., Lapouchnian, A., Robinson, W.N. and Mylopoulos, J., 2011, May. Awareness requirements for adaptive systems. In Proceedings of the 6th international symposium on Software engineering for adaptive and self-managing systems (pp. 60-69).

Mirko Morandini, Loris Penserini, and Anna Perini. 2008. Towards goal-oriented development of self-adaptive systems. In Proceedings of the 2008 international workshop on Software engineering for adaptive and self-managing systems (SEAMS '08). Association for Computing Machinery, New York, NY, USA, 9-16.

Mouratidis, H., Weiss, M. and Giorgini, P., 2006. Modeling secure systems using an agent-oriented approach and security patterns. International Journal of Software Engineering and Knowledge Engineering, 16(03), pp.471-498.

Yijun Yu, Haruhiko Kaiya, Hironori Washizaki, Yingfei Xiong, Zhenjiang Hu, and Nobukazu Yoshioka. 2008. Enforcing a security pattern in stakeholder goal models. In Proceedings of the 4th ACM workshop on Quality of protection (QoP '08). Association for Computing Machinery, New York, NY, USA,

Phillips, C. and Swiler, L.P., 1998, January. A graph-based system for network-vulnerability analysis. In Proceedings of the 1998 workshop on New security paradigms (pp. 71-79).

Martins, Eliane, Anderson Morais, and Ana Cavalli. "Generating attack scenarios for the validation of security protocol implementations." In The 2nd Brazilian Workshop on Systematic and Automated Software Testing (SBES 2008-SAST). 2008.

Adam Shostack. 2014. Threat Modeling: Designing for Security (1st. ed.). Wiley Publishing.

DeLoach, S.A. and Miller, M., 2017. A goal model for adaptive complex systems. J. Adv. Comput. Res, 2, pp.83-92.

Kai Petersen, Sairam Vakkalanka, Ludwik Kuzniarz, Guidelines for conducting systematic mapping studies in software engineering: An update, Information and Software Technology, Volume 64, 2015, Pages 1-18,

Adolph, S., Hall, W. and Kruchten, P. 2011. Using grounded theory to study the experience of software development. Empirical Software Engineering, 16, 4, 487-513.

Denscombe, M. (2010) The good research guide: For small-scale social research projects (4ed) Berkshire: Open University Press

Brink, H.. (1993). Validity and reliability in qualitative research. Curationis. 16. 35-8. 10.4102/curationis.v16i2.1396.

Morrow, S.L., 2005. Quality and trustworthiness in qualitative research in counseling psychol-ogy. Journal of Counseling Psychology 52, 250-260.

Baumgarten, M., 2012. Paradigm wars-validity and reliability in qualitative research. GRIN Ver-lag.

Turpe, S.: The trouble with security requirements. In: Requirements Engineering Conference (RE), 2017 IEEE 25th International. pp. 122-133. IEEE (2017)

Gharib, M., Ceccarelli, A., Lollini, P. and Bondavalli, A., 2022. A cyber-physical-social approach for engineering Functional Safety Requirements for automotive systems. Journal of Systems and Software, 189, p.111-310.

Liliana Pasquale, Dalal Alrajeh, Claudia Peersman, Thein Tun, Bashar Nuseibeh, and Awais Rashid. 2018. Towards forensic-ready software systems. In Proceedings of the 40th International Conference on Software Engineering: