Turkish Journal of Electrical Engineering and Computer Sciences

Volume 30 | Number 4 Article 1

1-1-2022

Software security management in critical infrastructures: a systematic literature review

GÜLSÜM ECE EKŞİ

BEDİR TEKİNERDOĞAN

CAGATAY CATAL

Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Review Article

Turk J Elec Eng & Comp Sci
(2022) 30: 1142 – 1161

doi:10.55730/1300-0632.3841

Software security management in critical infrastructures: a systematic literature review

Gulsum Ece EKSI[1], Bedir TEKINERDOGAN[1,*], Cagatay CATAL[2]
[1]Information Technology Group, Wageningen University & Research, Wageningen, Netherlands
[2]Department of Computer Science and Engineering, Qatar University, Doha, Qatar

Received: 09.11.2021 • **Accepted/Published Online:** 12.03.2022 • **Final Version:** 31.05.2022

Abstract: Critical infrastructure (CI) is an integrated set of systems and assets that are essential to ensure the functioning of a nation, including its economy, the public's health and/or safety. Hence, protecting critical infrastructures (CI) is vital because of the potential severe consequences that may emerge at the national level. Many CIs are now controlled by software, and likewise, software is often the major source of many security problems in critical infrastructures. Software security management in CIs has been addressed in the literature and several useful approaches have been provided. Yet, these approaches are fragmented over multiple different studies, often do not explicitly relate to CIs, and a synthesized overview of the state-of-the-art on software security in CIs is lacking. To this end, this article presents the results of a systematic literature review (SLR) that identifies and synthesizes how software security has been addressed in CIs. This study identifies and synthesizes the current approaches applied for security management in critical systems in terms of identified security threats, adopted solutions, CI domains, and evaluation approaches. Hereby 32 primary studies were retrieved from electronic databases to respond to the research questions defined in this study. Based on the outcome of the SLR the reported approaches are discussed, and a roadmap is described for security management in CIs. The results of the SLR identify the current open challenges and pave the way for further research. In addition, practitioners can benefit from the best practices in the security management of CIs.

Key words: Software security management, critical infrastructures, systematic literature review

1. Introduction

Critical infrastructure (CI) is an integrated set of systems and assets that are essential to ensure the functioning of a nation, including its economy, the public's health and/or safety. Proper protection of CIs is vital to avoid the serious consequences that may emerge at the national level. Examples of CIs include the transport network, the finance network, the power grid, and information and communication systems. Each of these CIs has their own vulnerabilities and needs to be protected in different ways. Since these critical infrastructures are managed as a combination of different physical and virtual structures and these structures are interconnected, a failure in any of these systems may cause the collapse of the interconnected systems. Moreover, many critical infrastructures are now controlled by software which as such makes software a key critical asset.

Adversarial attacks to software systems in CIs, together with the potential vulnerabilities of CIS can create serious risks for the continuous well functioning of CIs. It can be deduced that most of the challenges in software systems are related to detecting these attacks/vulnerabilities/failures in the software systems before

*Correspondence: bedir.tekinerdogan@wur.nl

the system crashes. Since failures can cause different types of consequences such as financial and public safety consequences, it is critical to develop effective mechanisms to ensure the continuation of these systems.

Software security management in CIs has been broadly addressed in the literature [3–5]. Yet, these approaches are fragmented over multiple different studies, the direct relation to CIs is less explicit, and a systematic overview of the state-of-the-art on software security in critical infrastructures is lacking. To this end, this article presents the results of a systematic literature review (SLR) that identifies and synthesizes how software security has been addressed in CIs.

The SLR guidelines of Kitchenham [6] developed for the software engineering domain have been used in this study. This study identifies and synthesizes the current approaches applied for security management in critical systems in terms of identified security threats, adopted solutions, challenges, CI domains, and evaluation approaches. Hereby 32 primary studies were retrieved from electronic databases to respond to the research questions defined in this study. Based on the outcome of the SLR the reported approaches are discussed, and a roadmap is described for security management in CIs. The results of the SLR identify the current open challenges and pave the way for further research. In addition, practitioners can benefit from the best practices in the security management of CIs.

The outline of this paper is as follows: Section 2 includes the related work of software security management in CIs. Section 3 describes the research methodology of this SLR. The results of the selected primary studies in terms of their methodological quality and systems investigated in Section 4. Section 5 includes the discussion of primary studies in the light of conducted SLR and potential threats to validity during the SLR phase. Finally, Section 6 concludes the paper and includes future work.

2. Related work

With the disruptive impact of digitalization in many domains, software has now also become an important part of critical infrastructures. In parallel, with the increased size and complexity of software systems, vulnerabilities related to software security have increased as well. As such, the key security related issues in critical infrastructures are often based on software security concerns. Software security management is not new and has been explored in several studies [13], [14], and [15]. On the other hand security of critical infrastructures has been addressed in a few systematic reviews but no study has explicitly addressed software security management in critical infrastructures.

[17] states that there is a need for identifying critical infrastructure interdependencies in cases of natural hazards and extracting patterns among them, and they carry out a methodical approach for it. This research differs from previous researches which only focuses on specific case studies of natural disasters or identifying theoretical frameworks for the critical infrastructure interdependency and gives researchers more systematic information about critical infrastructures. In this study, although hazards to critical infrastructures are mostly discussed in the direction of natural disasters and physical situations, they also discussed in their research that cyber/logical structures of critical infrastructures may be under threat and be damaged. However, their work mainly focuses on the civil and civic infrastructures of the CI systems. It can be stated that software security has a lack of concern in this study.

In [18], the aim of the authors is to state emergency management, protection and resilience policies of critical infrastructures; recommendations that can be applied to improve heterogenetic critical infrastructure and critical information infrastructure dependency and cascading models. To achieve this goal, they have carried out meticulous research which includes disruption incidents of CIs collected from public news resources for 15

years and gather a database. This database includes the information to understand the underlying threat causes of CI disruptions and failures, analyze the consequences of these disruptions, cascading effects, and good and bad practices. Although the information of this research includes valuable things, it is difficult to obtain data about the software and software security concerns.

Study [19] takes potential threats to build CI resilience at the national level into consideration. According to their results, these potential threats can be listed as follows: (1) natural disasters, (2) ageing and decay, (3) cyber threats, (4) terrorist activities, (5) contamination and (6) cascading failure/threat. It is obvious that only one threat in their work is software related which is cyber threats. Although they cover many threats to critical infrastructures, unfortunately, it is not a very guiding paper for researchers in terms of software security management.

Study [20] provides the information of existing critical infrastructure protection approaches including tools, techniques and methodologies to mention Internet of Things (IoT)-centric security risks. This study carries out a systematic literature review with considering critical infrastructure types, applicable modelling techniques, risk management sub-stages covered, and (inter)dependency and resilience modelling considerations. Although security issues of IoT systems in CIs are discussed and comprehensive research is carried out, security threats, vulnerabilities and risks in software systems in which critical infrastructures are directly involved are not taken into account in this study.

Study [21] handles the issues of reliability, availability, maintainability, and safety/security analysis in CIs altogether and introduces an SLR to the researchers. Although this study is related to software, due to its wide range, it moves away from the issue of security management in the software of critical infrastructures that we focus on. In addition, the authors determine the review/case study papers as primary studies, and the papers do not include critical infrastructures as primary studies.

To the best of our knowledge, our SLR is the first and only study so far, focusing not only on the papers involving critical infrastructures but also the software security management issues of CI systems. Table 1 also shows the related works' research direction in terms of software security concerns. Although previous SLR studies have provided research in the CI domain, they cannot provide the desired information about security concerns in a software system, which is our main area of interest. With this SLR study, researchers and practitioners who are interested in software systems in CIs can find out what the software security problems in CI systems are, in which software development life cycle they are handled, by which methodology they are solved, in which CI domain and how the solutions are evaluated.

Table 1. Related works according to software security concern.

Related work ID	Software related	Security related	Main focus for software security
[17]	No	Yes	No
[18]	No	Yes	No
[19]	Yes	Yes	No
[20]	Yes	Yes	No
[21]	Yes	Yes	No

3. Research methodology

The objective of this systematic review is to identify and analyze these approaches related to software security management methodologies for critical infrastructures. This SLR is carried out with the multiphase study

selection process using journals, conferences, workshops, and symposium papers related to software security management in CIs. We retrieved 1087 papers from electronic databases using search criteria. After we applied study selection criteria (SSC1-SSC4), we reached 110 papers and later, we used the rest of the selection criteria (SSC5-SSC7) and had 32 papers in total. With the help of snowballing technique, [22], 32 papers were selected. We investigate these studies from several dimensions that are related to our research questions and also, we identify potential research topics for further research. This SLR helps researchers and practitioners to gain an insight into how software security management in critical infrastructures are conducted.

3.1. Systematic reviews

A systematic literature review has been defined as follows in the literature: "identifying, evaluating and interpreting all available research relevant to a particular research question, or topic area, or phenomenon of interest [6]". Primary studies are called the research studies we chose before the SLR is conducted, and the SLR studies are the secondary studies that are performed based on those primary studies systematically. Initially, a research methodology must be identified to start the systematic review process. With respect to our research methodology, the SLR is conducted to collect and synthesize the existing studies related to our research area and inform other researchers/practitioners about open research problems, challenges, and potential solutions. In our work, we evaluate the primary studies and present several aspects that need to be improved and also, discuss open research problems. This SLR study is carried out based on several research questions and relevant primary studies are identified. In the light of [6] and [23], we set up our methodology and carry out the SLR.

3.2. Review protocol

The first step of our systematic literature review is defining a review protocol. Figure 1 states our road map of this SLR. Our research questions are defined in subsection 3.3 based on our motivation in this SLR. According to these research questions, our search strategy is stated in subsection 3.4. After that, to decide which studies will be used as a primary study, we identify study selection criteria in subsection 3.4.3. We evaluate these primary studies according to a quality assessment included in subsection 3.4.4. The data extraction process included in subsection 3.4.5 shows the process of collecting information from our primary studies. Finally, in subsection 3.4.6, we show our extracted data and related results in the data synthesis part.

3.3. Research questions

Identification of the research questions is a critical part of systematic reviews. The quality of research is affected by the quality of research questions. In this systematic review process, we focus on software security management in critical infrastructures. Following research questions are determined to get relevant studies:

- RQ.1: What are the identified software security threats in CIs?
- RQ.2: What are the proposed solutions for coping with the software security threats in CIs?
- RQ.3: Which CI domains have been identified related to software security?
- RQ.4: What are the adopted evaluation approaches of CIs with respect to software security?

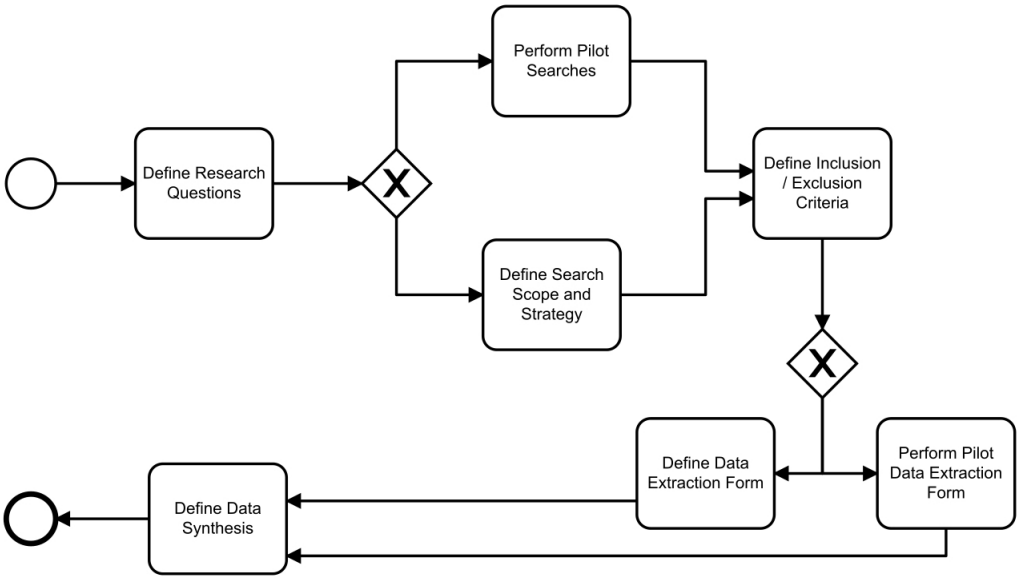

Figure 1. BPMN (business process modeling notation) diagram of reviewing protocol of SLR.

3.4. Search strategy

In this section, we present the scope, search strategy, and search strings that are prepared for electronic databases.

3.4.1. Scope

We carried out our search on the following electronic databases: ACM Digital Library, IEEE Xplore, Science Direct, and Wiley Online Library. In all databases, we search the sources published within the last 10 years. Our scope is related to "computer science", "software engineering", and "critical infrastructures". Our search focuses on journal, conference, workshop, and symposium papers.

3.4.2. Search methodology

Search strategy definition/monitoring is essential to have high-quality systematic literature reviews. For our search strategy, we carried out the following steps based on the work [6]:

1. Searching related SLRs and survey papers to our research area.
2. Creating search strings using "AND" and "OR" operators to get sophisticated search terms for electronic databases.
3. Checking conference, journal, workshop, and symposium papers.
4. Monitoring the collected results and eliminating the unrelated papers manually.

In the second phase, some difficulties may arise in terms of the working mechanism of the electronic databases. They may return too many unrelated papers. Some related studies cannot be retrieved because of the electronic databases' internal working mechanism. Therefore, we also did an additional manual lot of work to specify the relevant studies and updated our search strings during the research process to overcome these potential problems. A search string used in IEEE Xplore is shown as follows:

("Document Title":security management) AND ("Full Text Only":data intensive systems) AND ("Full Text Only":critical infrastructures) AND ("All Metadata":software) Filters Applied: 2010 - 2021.

Our search results conducted on electronic databases and applied study selection criteria are shown in Table 2. A total of 1087 numbers of sources are retrieved from databases automatically. Most of them are unrelated to our objective and we reviewed these sources manually according to our study selection criteria. Firstly, we eliminate the papers whose full texts are not available and not related to software engineering, security management and CIs. Secondly, we eliminate the papers that have duplicates, do not satisfy the content and are an experience/proposal/critical review, and survey papers. At the end of this process, we conduct snowballing technique [22] to gain more relevant studies in the literature.

Table 2. Search results according to search strings and study selection criteria.

Source	New number of included studies after applying search query	Number of included studies after SSC1-SSC4	Number of included studies after SSC5-SSC7
ACM Digital Library	692	18	5
IEEE Xplore	289	42	8
Science Direct	58	24	8
Wiley Online Library	48	26	3
Snowballing	-	-	8
Total	1087	110	32

3.4.3. Study selection criteria

After applying search strings on electronic databases, many studies are obtained. Most of them can be unrelated to our objectives, motivation, and the main aim in this SLR. We defined the following study selection criteria for our study:

- SSC 1: Paper where the full text is not available.
- SSC 2: Paper does not relate to software engineering.
- SSC 3: Paper does not relate to software security management.
- SSC 4: Paper does not relate to critical infrastructures.
- SSC 5: Paper does not satisfy the scope of this research.
- SSC 6: Duplicate publications found in different search sources.
- SSC 7: Papers that are experience, proposal, critical review, and survey papers.

We apply manual elimination after gathering all the sources from databases according to two exclusion criteria: the former includes SS1-SS4, the latter includes SS5-SS7. At the end of this phase, 32 papers are selected as primary studies shown in Table 3.

Table 3. Primary studies (sources reviewed in the SLR).

[PS_1]	Zhu Q, Basar T. A Dynamic Game-Theoretic Approach to Resilient Control System Design for Cascading Failures. In: International conference on High Confidence Networked Systems (HiCoNS); Beijing, China; 2012. pp. 41–46.
[PS_2]	Fuchs A, Weber D. Analysis of the SYM2 Smart Meter Remote Software Download using formal methods reasoning. Proceedings of the International Workshop on Security and Dependability for Resource Constrained Embedded Systems (S&D4RCES); 2011. 3: pp. 1–12.
[PS_3]	Hunter D, Parry J, Radke K, Fidge C. Authenticated Encryption for Time-Sensitive Critical Infrastructure. In: Proceedings of the Australasian Computer Science Week Multiconference (ACSW); Geelong, Australia; 2017. 19: pp. 1–10.
[PS_4]	Dantas H, Erkin Z, Doerr C. eFuzz: A Fuzzer for DLMS/COSEM Electricity Meters. Proceedings of the 2nd Workshop on Smart Energy Grid Security (SEGS); 2014. pp. 31-38.
[PS_5]	Hewett R, Kijsanayothin P. Securing system controllers in critical infrastructures. Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW); 2013. 29: pp.1-4.
[PS_6]	Koch T, Möller DPF, Deutschmann A. A Python-Based Simulation Software for Monitoring the Operability State of Critical Infrastructures Under Emergency Conditions. In: IEEE International Conference on Electro/Information Technology (EIT); Rochester, USA; 2018. pp. 290-295.
[PS_7]	Almalawi A, Fahad A, Tari Z, ALamri A, AlGhamdi R, Zomaya AY. An Efficient Data-Driven Clustering Technique to Detect Attacks in SCADA Systems. IEEE Transactions on Information Forensics and Security; 2016. 11(5): pp. 893-906.
[PS_8]	Mylrea M, Gourisetti SNG. Blockchain for Supply Chain Cybersecurity, Optimization and Compliance. In: Resilience Week (RWS); Denver, USA; 2018. pp. 70–76.
[PS_9]	Tseng KY, Chen D, Kalbarczyk Z, Iyer RK. Characterization of the error resiliency of power grid substation devices. In: IEEE/IFIP International Conference on Dependable Systems and Networks (DSN); Boston, USA; 2012. pp.1-8.
[PS_10]	Yasakethu SLP, Jiang J, Graziano A. Intelligent risk detection and analysis tools for critical infrastructure protection. In: Eurocon; Zagreb, Croatia; 2013. pp. 52-59.
[PS_11]	Mazloomzadeh A, Mohammed O, Zonouz S. TSB: Trusted sensing base for the power grid. In: IEEE International Conference on Smart Grid Communications (SmartGridComm); Vancouver, Canada; 2013. pp. 803-808.
[PS_12]	Lee S, Chen L, Duan S, Chinthavali S, Shankar M, Prakash BA. URBAN-NET: A network-based infrastructure monitoring and analysis system for emergency management and public safety. In: IEEE International Conference on Big Data (Big Data); Washington, USA; 2016. pp. 2600-2609.
[PS_13]	Caire R, Sanchez J, Hadjsaid N. Vulnerability analysis of coupled heterogeneous critical infrastructures: A Co-simulation approach with a testbed validation. In: IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe); Lyngby, Denmark; 2013. pp. 1-5.
[PS_14]	Cantelli-Forti A, Capria A, Saverino AL, Berizzi F, Adami D, Callegari C. Critical infrastructure protection system design based on SCOUT multitech seCurity system for intercOnnected space control groUnd staTions. International Journal of Critical Infrastructure Protection; 2020. 32.

Table 3. (Continued).

[PS_15]	Gourisetti SNG, Mylrea M, Patangia H. Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. Future Generation Computer Systems; 2020. 105: pp. 410-431.
[PS_16]	Gonen S, Sayan H, Yılmaz EN, Ustunsoy F, Karacayılmaz G. False Data Injection Attacks and the Insider Threat in Smart Systems. Computers & Security; 2020. 97.
[PS_17]	Windelberg M. Objectives for managing cyber supply chain risk. International Journal of Critical Infrastructure Protection; 2016. 12: pp. 4-11.
[PS_18]	Kampovaa K, Loveceka T, Rehakb D. Quantitative approach to physical protection systems assessment of critical infrastructure elements: Use case in the Slovak Republic. International Journal of Critical Infrastructure Protection; 202. 30.
[PS_19]	Chekole EG, Ochoa M, Chattopadhyay S. SCOPE: Secure Compiling of PLCs in Cyber-Physical Systems. International Journal of Critical Infrastructure Protection; 2021. 33.
[PS_20]	Maziku H, Shetty S, Nicol DM. Security risk assessment for SDN-enabled smart grids. Computer Communications; 2019. 133: pp.1-11.
[PS_21]	Piedrahita AFM, Gaur V, Giraldo J, Cardenas AA, Rueda SJ. Virtual incident response functions in control systems. Computer Networks; 2018. 135: pp. 147-159.
[PS_22]	Baker T, Asim M, MacDermott A, Iqbal F, Kamoun F, Shah B, Alfandi O, Hammoudeh M. A secure fog-based platform for SCADA-based IoT critical infrastructure. Software: Practice and Experience; 2019. 33(5): pp. 503-518.
[PS_23]	Horowitz BM, Pierce KM. The integration of diversely redundant designs, dynamic system models, and state estimation technology to the cyber security of physical systems. Systems Engineering; 2013. 16(4): pp. 401-412.
[PS_24]	Leszczyna R, Wrobel MR. Threat intelligence platform for the energy sector. Software: Practice and Experience; 2019. 49(8): pp. 1225-1254.
[PS_25]	Faza A, Sedigh S, McMillin B. Integrated Cyber-Physical Fault Injection for Reliability Analysis of the Smart Grid. In: Schoitsch E. (eds) Computer Safety, Reliability, and Security (SAFECOMP), Lecture Notes in Computer Science; Springer, Berlin, Heidelberg; 2010. 6351: pp. 277-290.
[PS_26]	Zhu Q, Rieger C, Basar T. A hierarchical security architecture for cyber-physical systems. International Symposium on Resilient Control Systems (ISRCS); Boise, ID, USA; 2011. pp.15-20.
[PS_27]	Robertson P, Gordon C, Loo S. Implementing Security for Critical Infrastructure Wide-Area Networks. In: Power and Energy Automation Conference; Spokane, WA, USA; 2013. pp.1-10.
[PS_28]	Farzan F, Jafari MA, Wei D, Lu Y. Cyber-related risk assessment and critical asset identification in power grids. In: Innovative Smart Grid Technologies (ISGT); Washington, DC, USA; 2014. pp. 1-5.
[PS_29	Almalawi A, Yu X, Tari Z, Fahad A, Khalil I. An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems. Computers & Security; 2014. 46: pp. 94-110.
[PS_30]	Alcaraz C, Lopez J. Diagnosis mechanism for accurate monitoring in critical infrastructure protection. Computer Standards & Interfaces; 2014. 36: pp. 501–512.
[PS_31]	Lee S, Chinthavali S, Duan S, Shankar M. Utilizing Semantic Big Data for realizing a National-scale Infrastructure Vulnerability Analysis System. International Workshop on Semantic Big Data (SBD); 2016. 3: pp. 1-6.
[PS_32]	Lin CT, Wu SL, Lee ML. Cyber Attack and Defense on Industry Control Systems. In: IEEE Conference on Dependable and Secure Computing; Taipei, Taiwan; 2017. pp. 524-526.

3.4.4. Study quality assessment

We define quality assessment criteria to analyze each primary study in terms of quality and quantity aspects [6]. With this quality assessment methodology, we could facilitate the analysis and interpretation of the primary works for future research. With this quality assessment checklist, the bias within the primary studies is decreased. Quality checklist questions are shown in Table 4. We present a scoring technique to rank the studies according to a quality score. If the answer to the related question is "No", the score is: 0, if the answer is "partially correct", the score is: 1, and if the answer is "Yes", the score is: 2. The gathered results of the quality assessment checklist criteria are shown in Table 5. Subsection 4.2 provides more information about the applied procedure and threshold levels.

Table 4. Quality assessment checklist.

No	Question
Q1	Are the main theme and motivation of the study clearly stated?
Q2	Do the researchers clearly define the scope and context of the study?
Q3	Do the researchers clearly define methods/approaches/technologies given in the study?
Q4	Do the researchers clearly explain the proposed solutions and validate them by an empirical study?
Q5	Is the study reporting clear and coherent?
Q6	Do the researchers answer all the study questions?
Q7	Do the researchers present negative findings in the study?
Q8	Do the researchers explain the consequences of any problems with the validity/reliability of their measures?
Q9	Do the conclusions satisfy the purpose of the study?
Q10	Does the study have implications in practice and results in a research area for software security management in critical infrastructures?

3.4.5. Data extraction

We read the 32 selected primary studies during this data extraction step. Analyzing them is conducted by answering the research questions defined at the beginning of this SLR. The extracted data which includes the main theme, the motivation for the study, and the assessment approach according to our research questions is shown in Table 6. Additionally, the data extraction form is presented in Table 7. It includes the general information of the primary study such as ID, title, authors, publication year, and repository.

3.4.6. Data synthesis

Extracted data is used in this data synthesis step. Synthesis of both quantitative and qualitative analysis of the primary studies are important in this phase. The primary studies include both qualitative and quantitative aspects supported by experiments. Even though most papers include both qualitative and quantitative aspects, we interpret the qualitative aspects of the papers and reach quantitative results to compare them with each other effectively.

4. Results

4.1. Overview of the reviewed studies

In this section, we represent the primary studies in terms of the year, publication channel, and other deterministic characteristics. The distribution of the selected primary studies in terms of publication year can be seen in Figure 2. It can be concluded that disasters such as [7] and [8] might affect the scientific research on critical infrastructures and after such critical events, researchers would turn their research directions to consider these

Table 5. Study quality assessment.

	Quality of reporting				Rigor		Credibility		Relevance						
Study	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Quality of reporting	Rigor	Credibility	Relevance	Total
1	2	1	2	0	2	1	0	1	1	1	5	3	1	2	11
2	2	2	2	0	2	1	2	1	1	1	6	3	3	2	14
3	2	2	2	2	2	1	1	2	2	1	8	3	3	3	17
4	2	2	2	2	2	1	2	2	2	2	8	3	4	4	19
5	2	2	2	1	2	1	0	1	2	0	7	3	1	2	13
6	2	2	2	1	2	1	2	2	2	1	7	3	4	3	17
7	2	2	2	2	2	1	0	1	1	1	8	3	1	2	14
8	2	2	2	1	2	1	2	2	2	2	7	3	4	4	18
9	2	2	2	1	2	1	1	1	1	1	7	3	2	2	14
10	2	2	2	2	2	1	0	1	2	1	8	3	1	3	15
11	2	2	2	2	2	1	0	2	2	0	8	3	2	2	15
12	2	2	2	1	2	1	1	1	2	1	7	3	2	3	15
13	2	2	2	1	2	1	1	1	2	1	7	3	2	3	15
14	2	1	2	1	2	1	1	2	2	1	6	3	3	3	15
15	2	2	2	1	2	1	1	2	2	1	7	3	3	3	16
16	2	2	2	1	2	1	1	1	2	1	7	3	2	3	15
17	2	2	2	1	2	1	1	1	2	1	7	3	2	3	15
18	2	2	2	2	2	1	0	1	2	1	8	3	1	3	15
19	2	2	2	1	1	1	0	1	2	1	7	2	1	3	13
20	2	2	2	2	2	1	2	1	2	2	8	3	2	4	17
21	2	2	2	2	2	1	2	2	2	2	8	3	4	4	19
22	2	2	2	2	2	1	0	2	2	1	8	3	2	3	16
23	2	2	2	1	2	1	1	1	2	2	7	3	2	4	16
24	2	2	2	2	2	1	1	1	2	2	8	3	2	4	17
25	2	2	2	1	2	1	2	1	2	2	7	3	3	4	17
26	2	2	2	0	2	1	1	1	2	1	6	3	2	3	14
27	2	2	2	0	1	1	2	2	2	1	6	2	4	3	15
28	2	2	2	0	1	1	1	1	1	1	6	2	2	2	12
29	2	2	2	2	1	1	2	2	2	1	8	2	4	3	17
30	2	2	2	1	1	1	1	2	2	2	7	2	3	4	16
31	2	2	2	0	2	1	0	1	2	1	6	3	1	3	13
32	2	2	2	2	1	1	1	1	2	1	8	2	2	3	15

Table 6. Data extraction.

Research questions	Data extracted
RQ.1	Targeted domain, main theme of study, motivation for study
RQ.2	Security management methodology / technology / technique / type; constraints, limitations and challenges of proposed solution, findings
RQ.3	Contribution type, solution area
RQ.4	Assessment approach, evidence type

issues, conduct new studies, and propose solutions to overcome them. We also see that this research field is still active and new research is carried out each year.

As shown in Table 2, the primary studies have been found in different databases including IEEE, Science Direct, ACM and Wiley. A total of 8 of the primary studies that were found with the snowballing technique were also indexed by IEEE and ACM.

Table 7. Data extraction form.

Extraction element	Contents
General information	
ID	Unique ID of the study
Title	Title of the study
Year	Publication year of the study
Authors	Authors of the study
Repository	ACM / IEEE / Science Direct / Wiley Online Library
Publication type	Conference / Journal / Workshop / Symposium
Publication channel	
Study description	
Main theme of the study	
Motivation of the study	
Keywords	
Security threat concern	Attacks / Failures / Vulnerabilities
CI research area	Energy/Telecommunication/Transportation, etc.
Contribution type	Analysis/Design/Implementation/Verification
Assessment approach	Experiment/Case Study/Example Scenario
Findings	
Constraints / Limitations	
Evaluation	
Personal note	
Quality assessment	Quality scores

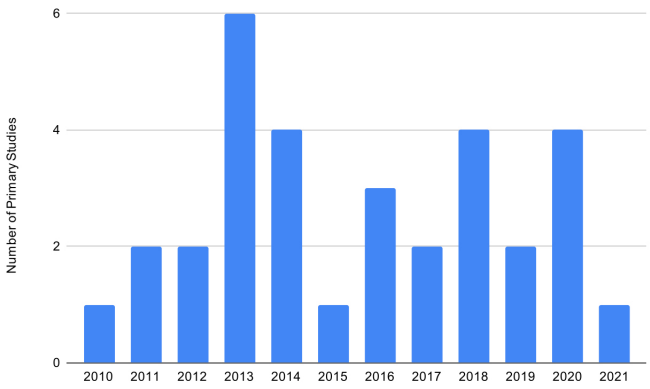

Figure 2. Publication years of the primary studies.

4.2. Methodological quality

We carried out a quality assessment criteria specified in subsection 3.4.4 to state the quality of the primary papers. The quality of reporting, rigor, credibility, and relevance of the studies are evaluated based on these criteria. The first four questions mentioned in Table 4 correspond to the quality of reporting, the questions 5th and 6th correspond to the rigor of the studies, the questions 7th and 8th correspond to the credibility of the studies, and the last two questions correspond to the relevance of them. At the end of this methodology, we can calculate the total quality of the primary studies by adding up their scores. The actual results of the quality assessment can be seen in Table 5.

The quality of reporting of the primary studies is shown in Figure 3. According to this figure, we can say that 78.1% of papers (i.e. 25 of them) are good in terms of quality of reporting. We assume that the threshold level for this dimension is 7. Rigor quality of the primary studies is presented in Figure 4. According to this figure, we can state that 81.2% of the papers (i.e. 26 of them) have a good rigor quality. We assume that the threshold level is 3 for rigor quality dimension.

We also evaluate the primary papers in terms of their evidence types. The credibility of the primary studies based on this evaluation is shown in Figure 5. According to our findings, 18.75% (i.e. 6 of them) of the papers have full credibility, 18.75% (i.e. 6 of them) of the papers have good evidence quality, 40.6% (i.e. 13 of them) of the papers have normal evidence quality, however, 21.8% (7 of them) of the papers have low credibility.

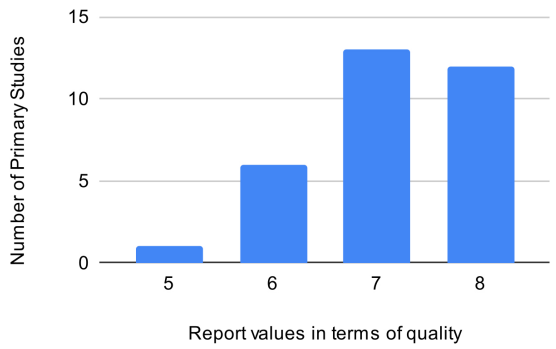

Figure 3. Quality of reporting of the primary studies.

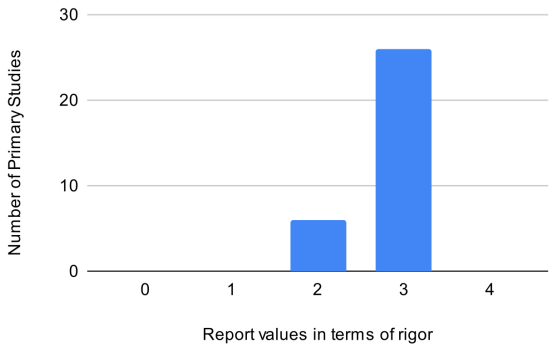

Figure 4. Rigor quality of the primary studies.

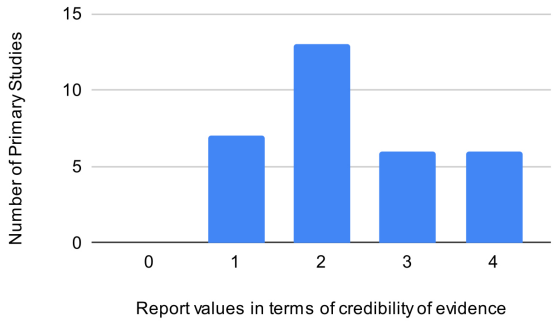

Figure 5. Credibility quality of the primary studies.

We examine the primary studies in terms of relevance quality depending on our research area, which is shown in Figure 6. 21.8% (7 of them) of the studies have poor relevance, 53.1% (17 of them) have a normal relevance quality, 25% (8 of them) of them have a good relevance ratio according to our results. We sum the values of each category of the primary studies to gather the total quality of them. According to Figure 7, we divide the quality value into three parts: if the total value is between 16 and 20, it means very good quality, if it is between 12 and 15, it means good, if it is lower than 12, it means the study has poor quality. It is stated that 40.6% of papers (13 of them) are very good, 56.2% of papers (18 of them) are good and 3.1% of papers (1 of them) have poor quality.

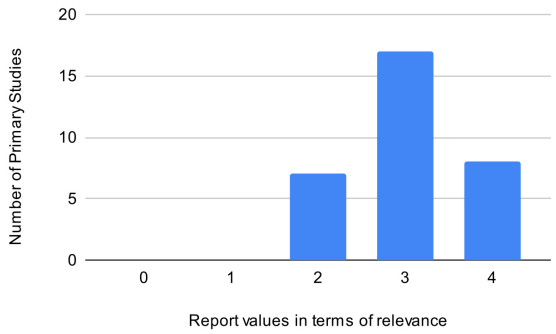

Figure 6. Relevance quality of the primary studies.

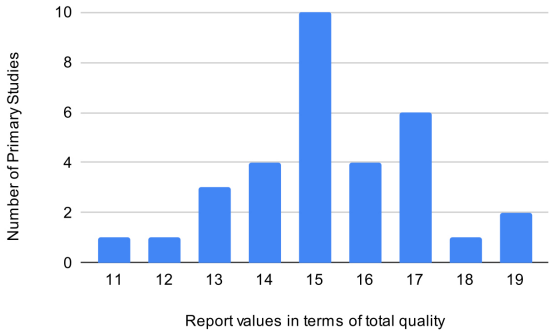

Figure 7. Total quality of the primary studies.

4.3. Systems investigated

After the thorough and systematic data extraction we can now provide answers to our defined research questions.

- RQ.1: What are the identified software security threats in CIs?

According to our findings, which is shown in Figure 8, 50% (i.e. 16 of them) of the primary studies consider attacks to the software systems in CIs. Software vulnerabilities are focused in 34.4% (11 of them) of the primary studies. In 21.8% (i.e. 7 of them) of the primary studies, security issues in software systems of CIs were handled in a more general framework and focused on how these software problems affect critical infrastructures and what precautions can be taken. Two of the studies consider both software vulnerabilities and attacks to these systems in CIs.

At this point, it is necessary to explain what these security threats are specifically. Attacks to software systems in CIs include cyber-attacks, network attacks and memory-safety attacks. The primary studies focus on the detection and prevention of these attacks, automatically notifying the relevant systems/people as soon as they are detected or strengthening the system against these attacks. Although in some papers these attacks are handled and conducted a general intrusion detection mechanisms, the majority of the papers focus on the specific type of software attacks in the CI systems. For instance, the studies [24], [25], [26], [27] and [28] address cyber attacks, [29], [30], [31] identified network attacks; [11] focused on memory-safety, [10] focuses on false data injection (FDI) attacks which are cyber attacks.

Software vulnerabilities are the weaknesses in software that malicious attacks can make use of accessing a network's sensitive data and conduct unauthorized actions. Vulnerabilities in software systems in CIs are handled in terms of cyber [16], [28] and network security [32], [33], [34] in CI systems. Also, software failures can be regarded as one of the main causes of software vulnerabilities. Software failure can be described as the inability of the system to continue working due to a bug/error in the software. The severity of this failure level is important. For instance, an operating system crash is the most serious type of failure in a software system since it could stop the entire computer system [35]. It is crucial as a failure in software used in critical infrastructure systems can cause the system to crash. Several studies have focused on how these errors can be detected and prevented in advance [3], [36], [37] and [38]. The prevention of these vulnerabilities and building software systems without them are the main concepts in the related primary studies.

- RQ.2: What are the proposed solutions for coping with software security threats in CIs?

Various solutions have been proposed to cope with software security threats in CIs. These can be categorized over the software development life cycle stages as it is shown in 9. As we can see from the figure, the majority of the solutions appear to be at the implementation stage. During the analysis and design stages of the software life cycle, the solution methodologies with respect to the vulnerabilities in critical infrastructures are discussed in a few primary studies. In the following we describe the specific solutions that have been proposed.

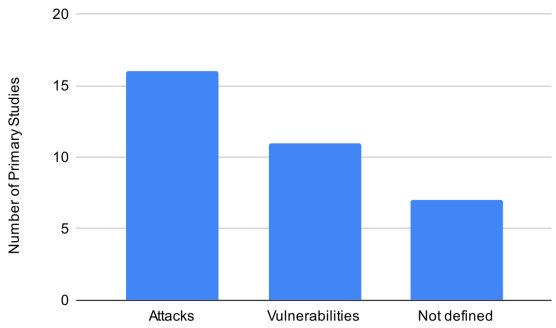

Figure 8. Identified security threats in CIs in the primary studies.

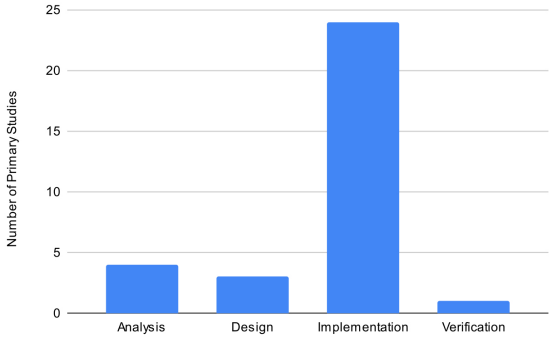

Figure 9. Primary studies according to software development life cycle solution.

In the work of [27], a cyber security design approach is presented in order to address cyber attacks. These attacks could affect the management of software-controlled automated systems. The presented design approach is based on fault-tolerant and automatic control system techniques which are the basis for the cyber security of physical systems and subsystems. The technique for providing cyber security relies on using information consistency checking for system dynamics models and redundant state estimation techniques. According to their findings, the proposed consistency-checking solutions can associate perimeter (perimeter security technologies—such as firewalls, encryption, and advanced user authentication) and network security capabilities to provide more improved protection for critical system functions.

The study [39] adopts a hierarchical viewpoint design approach for security issues for cyber-physical systems. The authors address the security concerns at each level and emphasize a holistic crosslayer philosophy for developing these software-related security solutions. Their 6-layer security architecture model takes the concerns from network and communication levels into consideration.

The authors in the work of [34] combine the Semantic Big Data (SBD) tools, Big Data, and Geo-graphical Information Systems (GIS) tools in order to handle vulnerability analysis in CIs and present an Infrastructure Vulnerability Analysis System (IVAS) for realizing a national-scale network-based vulnerability analysis system.

In [26], the authors present a requirement analysis for both anticyber-attacks tools and detection of foreign physical objects. According to them, critical infrastructure security needs to be addressed both in cyber and physical domains that are multilayer problems. They analyze the key aspects, needs, and objectives of the 3 main systems that are used in SCOUT (SeCurity system for intercOnnected space control groUnd staTions) system. These 3 systems are the cyber (CYBERSENS), physical (SENSNET) thread detection and identification; and recovery (RECOVER) system.

In the work of [40], defining tradeoffs, acquisition objectives and their concomitant requirements, risk tolerance or risk appetite, namely risk management are so crucial in supply chains for cyber-based products and services. The best way to provide secure, reliable, and safe operations of these systems is to manage the risk

factors in them. These systems need numerous suppliers of software components, hardware, firmware, and global services. The authors in this study consider the objectives of different stakeholders. These objectives/needs must be clearly understood and prioritized in order to provide a secure and reliable system where risk can be managed.

Study [38] shows that the failures in Smart Grid operations can be arisen due to the malfunctions that occurring in both physical and cyber components of critical infrastructure. The work identifies the causes and effects relationship of these software-related failures in the CI systems. They use fault injection for identifying failure scenarios for the Smart Grid systems.

Providing secure networks for data communications and preventing unauthorized access to safety-critical systems are the concerns of authors in the work [30]. For critical infrastructure applications, the authors present best practices for securing wide-area network (WAN) communication. While doing this, they define objectives and necessities of the related systems in order to mitigate the risks of cyber-attacks.

The main focus of almost all studies is detecting an attack/vulnerability/failure in a software system included in CIs in the early stages. Monitoring and evaluating these possible faults are crucial for the system to continue its life without any errors and stay viable. It is important to do this automatically without a person standing by the system all the time, both for speed and to directly detect and resolve the root cause of the error in the system. In all primary studies, although the main focus is software security management, which solution methodology is used in which stage of the software development life cycle is very crucial in determining the direction of the research. With this SLR, it can be determined in which phase of the software systems which solutions are produced and which research directions are more carried out and which are less pursued.

Since the studies involving the implementation stage are in the majority, the work done of the studies are more related to building a tool or a framework. Although the studies about design contain a solution architecture or a viewpoint, even the studies related to requirement analysis phases contain work done that include a solution methodology based on the implementation of a software, a tool or a framework. This situation clearly shows us the lack of applications in the fields of analysis, design, and verification. More precisely, the deficiency in these areas is a lack of approaches, perspectives, algorithms and technics rather than the lack of solving problems in these areas with an implementation methodology.

- RQ.3: Which CI domains have been identified related to software security?

According to our results in Figure 10, most of the primary studies conduct their research on all types of critical infrastructures such as power grids, water, and telecommunication. The power grid industry, namely the energy sector, is one of the most studied areas in primary studies. Although water, nation's control stations and other areas of CIs have been studied relatively less the reliability and security of the equipment used in critical infrastructures are the basis. In other words, it can be deduced that the researches are focused more on power supply subject since electricity is the basis and main provider of every resource the nations have.

- RQ.4: What are the adopted evaluation approaches of CIs with respect to software security?

Although in 21.8% of the primary studies, the adopted evaluation methodology for the approaches was not clearly stated, in 78.2% of the primary studies, they were supported by national projects, experiments, and case studies. In almost all primary studies, the software solutions have been tried in a real CI domain or a testbed for a CI infrastructure has been arranged.

We present the evidence type of the selected primary studies in Figure 11. According to our observations, most of the studies 40.6% (13 of them) conduct an experiment in their work. Case studies 28.1% (9 of them) and possible real-life scenarios 9.3% (3 of them) are also used in order to show the reliability and quality of the applied work. The work done is conducted with national projects and related public enterprises in the primary studies which are [37], [33], [26], [41], [29], [12], [27] and [42]. It can be deduced that the evidence type of most of the studies is reliable.

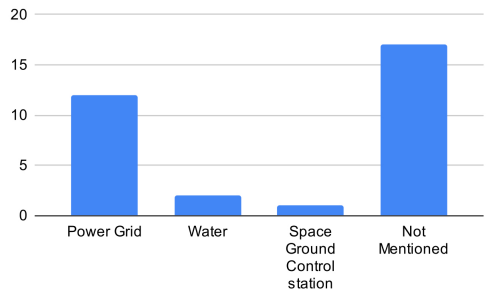

Figure 10. Critical infrastructure research area of the primary studies.

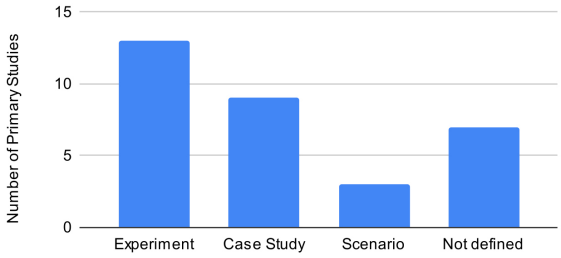

Figure 11. Evidence type of the primary studies.

5. Discussion

5.1. General discussion

Various CIs domains have been identified which have become even more important with the increased dependency on software. From the systematic review we can observe that software security management has thus become an important concern for CIs. Solutions for software security management in CIs cover the whole software life cycle, but the majority of the proposed solution approaches have been still in the implementation stage and solutions for analysis, design and verification are not widespread yet. Obviously, software security management needs to be considered in a holistic manner which requires adequate solutions across the software and systems engineering life cycle.

In Table 8, multiple requirements of the primary studies, which are stated separately in the results section, are shown by bringing them together. According to the data in Table 8, most of the studies, which focus on the design and analysis phases in primary studies have not done an experiment or a case study while evaluating their approach. Likewise, the authors who carried out their studies in the design and analysis stages developed their studies by considering the applicability to all CI types. Since it is more feasible to evaluate the work done in the stage of implementation and try it on a certain CI domain, the studies involving the implementation stage are in the majority. It would not be appropriate to mention solution methodologies and CI domains for the verification phase, as it is only carried out on one primary study. However, we could deduce that the design and analysis phases of the research area need more evidence-based studies and applied CI domains.

5.2. Threats to validity

Similar to other systematic reviews, a number of validity threats can also be identified for this review. We can gather these threats in 3 main groups as internal, external and construct threats to validity.

Internal validity: The evidence type of the primary studies is satisfactory that 40.6% (i.e. 13 papers) of the primary studies validated their work with an experimental setup and 28.1% (i.e. 9 papers) of the studies included real-world case studies. If we consider the internal threats to validity, the percentage of

Table 8. Primary studies according to multiple requirements.

Study ID	Security threat	Solution area	CI domain	Evidence type
1	Vulnerability	Implementation	Power grid	Not defined
2	Vulnerability, attack	Implementation	Power grid	Not defined
3	Attack	Implementation	All CIs	Experiment
4	Vulnerability	Implementation	Power grid	Experiment
5	Attack	Verification	All CIs	Case study
6	Attack	Implementation	Power of CIs	Scenario
7	Attack	Implementation	All CIs	Experiment
8	Not defined	Implementation	Power grid	Case study
9	Vulnerability	Implementation	Power grid	Case study
10	Attack	Implementation	All CIs	Experiment
11	Not defined	Implementation	Power grid	Experiment
12	Vulnerability	Implementation	All CIs	Case study
13	Vulnerability	Implementation	Power grid	Case study
14	Attack	Analysis	Space control ground station	Experiment
15	Vulnerability	Implementation	All CIs	Case study
16	Attack	Implementation	All CIs	Case study
17	Not defined	Analysis	All CIs	Not defined
18	Not defined	Implementation	Water	Case study
19	Attack	Implementation	All CIs	Experiment
20	Attack	Implementation	Power grid	Experiment
21	Attack	Implementation	All CIs	Experiment
22	Not defined	Implementation	All CIs	Experiment
23	Attack	Design	All CIs	Scenario
24	Not defined	Implementation	Power grid	Experiment
25	Vulnerability	Analysis	Power grid	Case study
26	Not defined	Design	All CIs	Not defined
27	Attack	Analysis	All CIs	Not defined
28	Vulnerability, Attack	Implementation	Power grid	Not defined
29	Attack	Implementation	All CIs	Experiment
30	Vulnerability	Implementation	All CIs	Scenario
31	Vulnerability	Design	All CIs	Not defined
32	Attack	Implementation	Water	Experiment

primary studies that evaluate their work with an experiment is quite high and it is deduced that when it comes to the reliability of critical infrastructures, most researchers have taken responsibility and performed their work with experimental analysis. Since all systems such as telecommunication, transportation, mains water management, gas distribution, which are of great importance for nations, come from an electricity provider, critical infrastructure systems used in electricity supply systems have been mentioned more in the studies. On the other hand, the vast majority of the primary studies have discussed the security problems of software used in CI systems in general, not directly aimed at a critical infrastructure system, and offered solutions. Assuming that an unproven work in a particular field will work across all systems is one of the main internal threats to validity.

External validity: While we were doing this systematic literature review, as we could not handle newly published studies or studies that will be published after this study, the potentials of the relevant studies in the area of software security management in CIs could not be discussed.

Construct validity: While we are carrying out this SLR, searching on electronic databases constitutes the construct threat in this work. Because of the fact that electronic databases search methodologies are weak in terms of finding related papers, the most relevant papers can be overlooked or some unrelated papers can be retrieved from the databases. We use the study selection criteria stated in subsection 3.4.3 to overcome unrelated papers coming from the electronic databases. We eliminate a large number of papers this way. By this selection process, we reached 32 primary studies. We evaluated these primary papers considering potential research topics, inadequacies, drawbacks, and affirmative contributions. We differentiate them according to their motivation, methodology, and assessment approach. Secondly, with respect to construct validity we might have missed some papers which are related to our research question. To mitigate this risk we have carefully defined the queries and also used snowballing techniques for capturing any relevant study.

6. Conclusion

In this article we have provided the results of an SLR on software security management in critical systems. The defined research questions focused on the CI domains, the identified software security threats, and the solution directions. In addition we have also analyzed the adopted evaluation approaches for CI together with the evidence types. A number of interesting conclusions can be derived from this study. By definition CIs are critical systems, but with the increased dependency on software, the maintenance and operation of CIs have been even more important. Hence, software security management has become a critical concern in CIs. This is a big challenge given the increased size and complexity of software that has dramatically increased in the last decades.

CIs has been related to different domains but primarily discussed in the context of power supply chains. Various software security threats can be identified in CIs which are related to the vulnerability of CIs, the cyber attacks or failures within the CIs. About half of the primary studies in the review indicate that the vast majority of software used in critical infrastructure systems is subject to various attacks. Although software security management requires a holistic perspective with solutions across the life cycle, it appears that currently focus has been given on the implementation solutions, while solutions for the other life cycle stages are less addressed. Hence, more research is needed for providing the solution abstractions and tools in the analysis, design and verification stages.

To complement the current literature, in our future work we will focus on the architecture design of dependable software-intensive CIs. For this we will consider the modeling, design and analysis of CIs with respect to software security concerns.

References

[1] Adepu S, Kang E, Mathur AP. Challenges in Secure Engineering of Critical Infrastructure Systems. In: IEEE/ACM International Conference on Automated Software Engineering Workshop (ASEW); San Diego, USA 2019; 61–64.

[2] Gad M, Abualhaol I. Securing Smart Cities Systems and Services: A Risk-Based Analytics-Driven Approach. Transportation and Power Grid in Smart Cities: Communication Networks and Services. USA: John Wiley & Sons, 2018.

[3] Zhu Q, Basar T. A Dynamic Game-Theoretic Approach to Resilient Control System Design for Cascading Failures. In: International Conference on High Confidence Networked Systems (HiCoNS); Beijing China 2012; 41–46.

[4] Hunter D, Parry J, Radke K, Fidge C. Authenticated Encryption for Time-Sensitive Critical Infrastructure. In: Proceedings of the Australasian Computer Science Week Multiconference (ACSW); Geelong, Australia 2017; 19: pp. 1–10.

[5] Mylrea M, Gourisetti SNG. Blockchain for Supply Chain Cybersecurity, Optimization and Compliance. In: Resilience Week (RWS); Denver, USA 2018. pp. 70–76.

[6] Kitchenham B, Charters S. Guidelines for performing systematic literature reviews in software engineering, EBSE Technical Report; 2007.

[7] Lee RM, Assante MJ, Conway T. Analysis of the Cyber Attack on the Ukrainian Power Grid. In: Electricity Information Sharing and Analysis Center, Tech. Rep.; 2016.

[8] Albright D, Brannan P, Walrond C. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment. In: Institute of Science and International Security; 2010.

[9] T. F. U.S.-Canada, Power System Outage, Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations, 2004.

[10] Gonen S, Sayan H, Yılmaz EN, Ustunsoy F, Karacayılmaz G. False Data Injection Attacks and the Insider Threat in Smart Systems. Computers & Security; 2020. 97.

[11] Chekole EG, Ochoa M, Chattopadhyay S. SCOPE: Secure Compiling of PLCs in Cyber-Physical Systems. International Journal of Critical Infrastructure Protection; 2021. 33.

[12] Baker T, Asim M, MacDermott A, Iqbal F, Kamoun F et al. A secure fog-based platform for SCADA-based IoT critical infrastructure. Software: Practice and Experience; 2019; 33 (5): pp. 503-518.

[13] Rindell K, Holvitie J. Security Risk Assessment and Management as Technical Debt. In: International Conference on Cyber Security and Protection of Digital Services (Cyber Security); Oxford, UK; 2019. pp. 1-8.

[14] Nunes FJB, Belchior AD, Albuquerque AB. Security Engineering Approach to Support Software Security. In: World Congress on Services; Miami, USA; 2010. pp. 48-55.

[15] Tung YH, Lo SC, Shih JF, Lin HF. An integrated security testing framework for Secure Software Development Life Cycle. Asia-Pacific Network Operations and Management Symposium (APNOMS); Kanazawa, Japan; 2016. pp. 1-4.

[16] Gourisetti SNG, Mylrea M, Patangia H. Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. Future Generation Computer Systems; 2020. 105: pp. 410-431.

[17] Kang K, Khallaf R, Hastak M. Systematic Literature Review on Critical Infrastructure Interdependencies impacted by Natural Disasters. In: Conference: International Conference on Maintenance and Rehabilitation of Constructed Infrastructure Facilities (MAIREINFRA); South Korea; 2017. pp. 1–6.

[18] Luiijf E, Klaver M. Analysis and lessons identified on critical infrastructures and dependencies from an empirical data set. International Journal of Critical Infrastructure Protection; 2021. 35.

[19] Kyei RO, Tam V, Ma M, Mashiri F. Critical review of the threats affecting the building of critical infrastructure resilience. International Journal of Disaster Risk Reduction 2021; 60: 1-11.

[20] Ani UPD, Watson JDM, Nurse JRC, Cook A. A Review of Critical Infrastructure Protection Approaches: Improving Security through Responsiveness to the Dynamic Modelling Landscape. In: PETRAS/IET Conference Living in the Internet of Things: Cybersecurity of the IoT; London, England; 2019.

[21] Pirbhulala S, Gkioulosa V, Katsikasa S. A Systematic Literature Review on RAMS analysis for critical infrastructures protection. International Journal of Critical Infrastructure Protection; 2021. 33.

[22] Wohlin C. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In: International Conference on Evaluation and Assessment in Software Engineering (EASE); New York, United States; 2014. 38: pp. 1-10.

[23] Kitchenham B, Budgen D, Brereton OP, Turner M, Bailey J et al. Systematic literature reviews in software engineering - a systematic literature review. Information and Software Technology 2009; 51 (1): pp. 7-15.

[24] Koch T, Möller DPF, Deutschmann A. A Python-Based Simulation Software for Monitoring the Operability State of Critical Infrastructures Under Emergency Conditions. In: IEEE International Conference on Electro/Information Technology (EIT); Rochester, USA; 2018. pp. 290-295.

[25] Yasakethu SLP, Jiang J, Graziano A. Intelligent risk detection and analysis tools for critical infrastructure protection. In: Eurocon; Zagreb, Croatia; 2013. pp. 52-59.

[26] Cantelli-Forti A, Capria A, Saverino AL, Berizzi F, Adami D et al. Critical infrastructure protection system design based on SCOUT multitech seCurity system for intercOnnected space control groUnd staTions. International Journal of Critical Infrastructure Protection; 2020. 32.

[27] Horowitz BM, Pierce KM. The integration of diversely redundant designs, dynamic system models, and state estimation technology to the cyber security of physical systems. Systems Engineering 2013; 16 (4): pp. 401-412.

[28] Farzan F, Jafari MA, Wei D, Lu Y. Cyber-related risk assessment and critical asset identification in power grids. In: Innovative Smart Grid Technologies (ISGT); Washington, DC, USA; 2014. pp. 1-5.

[29] Maziku H, Shetty S, Nicol DM. Security risk assessment for SDN-enabled smart grids. Computer Communications 2019; 133: pp.1-11.

[30] Robertson P, Gordon C, Loo S. Implementing Security for Critical Infrastructure Wide-Area Networks. In: Power and Energy Automation Conference; Spokane, WA, USA; 2013. pp.1-10.

[31] Lin CT, Wu SL, Lee ML. Cyber Attack and Defense on Industry Control Systems. In: IEEE Conference on Dependable and Secure Computing; Taipei, Taiwan; 2017. pp. 524-526.

[32] Lee S, Chen L, Duan S, Chinthavali S, Shankar M et al. URBAN-NET: A network-based infrastructure monitoring and analysis system for emergency management and public safety. In: IEEE International Conference on Big Data (Big Data); Washington, USA; 2016. pp. 2600-2609.

[33] Caire R, Sanchez J, Hadjsaid N. Vulnerability analysis of coupled heterogeneous critical infrastructures: A Co-simulation approach with a testbed validation. In: IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe); Lyngby, Denmark; 2013. pp. 1-5.

[34] Lee S, Chinthavali S, Duan S, Shankar M. Utilizing Semantic Big Data for realizing a National-scale Infrastructure Vulnerability Analysis System. International Workshop on Semantic Big Data (SBD); 2016. 3: pp. 1-6.

[35] Schmidt RF. Software Engineering Architecture-driven Software Development. USA: Morgan Kaufmann, 2013.

[36] Dantas H, Erkin Z, Doerr C. eFuzz: A Fuzzer for DLMS/COSEM Electricity Meters. Proceedings of the 2nd Workshop on Smart Energy Grid Security (SEGS) 2014; 31-38.

[37] Tseng KY, Chen D, Kalbarczyk Z, Iyer RK. Characterization of the error resiliency of power grid substation devices. In: IEEE/IFIP International Conference on Dependable Systems and Networks (DSN); Boston, USA; 2012. pp.1-8.

[38] Faza A, Sedigh S, McMillin B. Integrated Cyber-Physical Fault Injection for Reliability Analysis of the Smart Grid. In: Schoitsch E. (eds) Computer Safety, Reliability, and Security (SAFECOMP), Lecture Notes in Computer Science; Springer, Berlin, Heidelberg; 2010. 6351: pp. 277-290.

[39] Zhu Q, Rieger C, Basar T. A hierarchical security architecture for cyber-physical systems. International Symposium on Resilient Control Systems (ISRCS); Boise, ID, USA; 2011. pp.15-20.

[40] Windelberg M. Objectives for managing cyber supply chain risk. International Journal of Critical Infrastructure Protection; 2016. 12: pp. 4-11.

[41] Kampovaa K, Loveceka T, Rehakb D. Quantitative approach to physical protection systems assessment of critical infrastructure elements: Use case in the Slovak Republic. International Journal of Critical Infrastructure Protection; 2020. 30.

[42] Leszczyna R, Wrobel MR. Threat intelligence platform for the energy sector. Software: Practice and Experience; 2019. 49 (8): pp. 1225-1254.