Received: 3 April 2020 | Revised: 2 September 2020 | Accepted: 5 January 2021

DOI: 10.1002/smr.2346

SPECIAL ISSUE - REVIEW ARTICLE

Journal of Software: Evolution and Process WILEY

Security risks in cyber physical systems—A systematic mapping study

Maryam Zahid[1] | Irum Inayat[2] | Maya Daneva[3] | Zahid Mehmood[4]

[1]Product Realisation Division, IDT, Malardalen University, Västerås, Sweden

[2]Department of Software Engineering, Software Engineering and Automation Lab, National University of Computer and Emerging Sciences, Islamabad, Pakistan

[3]School of Computer Science, Services and Cyber Security Group, University of Twente, Enschede, Netherlands

[4]Independent Researcher, Islamabad, Pakistan

Correspondence
Irum Inayat, School of Computing, Department of Software Engineering, National University of Computer and Emerging Sciences, Islamabad, Pakistan.
Email: irum.inayat@nu.edu.pk

Abstract

The increased need for constant connectivity and complete automation of existing systems fuels the popularity of Cyber Physical Systems (CPS) worldwide. Increasingly more, these systems are subjected to cyber attacks. In recent years, many major cyber-attack incidents on CPS have been recorded and, in turn, have been raising concerns in their users' minds. Unlike in traditional IT systems, the complex architecture of CPS consisting of embedded systems integrated with the Internet of Things (IoT) requires rather extensive planning, implementation, and monitoring of security requirements. One crucial step to planning, implementing, and monitoring of these requirements in CPS is the integration of the risk management process in the CPS development life cycle. Existing studies do not clearly portray the extent of damage that the unattended security issues in CPS can cause or have caused, in the incidents recorded. An overview of the possible risk management techniques that could be integrated into the development and maintenance of CPS contributing to improving its security level in its actual environment is missing. In this paper, we are set out to highlight the security requirements and issues specific to CPS that are discussed in scientific literature and to identify the state-of-the-art risk management processes adopted to identify, monitor, and control those security issues in CPS. For that, we conducted a systematic mapping study on the data collected from 312 papers published between 2000 and 2020, focused on the security requirements, challenges, and the risk management processes of CPS. Our work aims to form an overview of the security requirements and risks in CPS today and of those published contributions that have been made until now, towards improving the reliability of CPS. The results of this mapping study reveal (i) integrity authentication and confidentiality as the most targeted security attributes in CPS, (ii) model-based techniques as the most used risk identification and assessment and management techniques in CPS, (iii) cyber-security as the most common security risk in CPS, (iv) the notion of "mitigation measures" based on the type of system and the underline internationally recognized standard being the most used risk mitigation technique in CPS, (v) smart grids being the most targeted systems by cyber-attacks and thus being the most explored domain in CPS literature, and (vi) one of the major limitations, according to the selected literature, concerns the use of the fault trees for fault representation, where there is a possibility of runtime system faults not being accounted for. Finally, the

mapping study draws implications for practitioners and researchers based on the findings.

INDEX TERMS

Cyber Physical System (CPS), dependability attributes, Internet of Things (IoT), risk identification, risk assessment, risk mitigation, risk management, security, Supervisory Control and Data Acquisition (SCADA) system, systematic mapping study.

1 | INTRODUCTION

The Internet of Things (IoT) is defined as an interconnected network of physical devices embedded with sensors, actuators, software, and network connectivity, enabling the objects to remotely control each other while exchanging data with each other.[1] The increase in the interconnectedness through time and space is fueled through the increased use of collaborative devices (e.g., laptops, tablets, smartphones, smart-watches, and personal computers). Large corporations and government agencies embrace this trend for interconnectedness and are moving towards the development and adoption of IoT considering it a means of changing the future.

The motivation behind IoT is the automation of work leading to a smart community. IoT forms a unit, linking all the devices together to generate a new emergent behavior where every single node contributes to achieving the desired functionality.[2] Smart Cars are just one example where each vehicle communicates with another while being on road to maintain traffic and to utilize energy resources efficiently.

Cyber Physical Systems (CPS) are embedded systems integrated with physical processors and computing.[3] The operations of such physical and software systems are constantly monitored, coordinated, controlled, and integrated by a core based on computing and communications, in other words, IoT.[4] Successful applications of such systems include communications systems, home appliances, automotive electronics, games, drones, weapons, and aircraft control systems, to name a few. On the other hand, most of the applications of CPS can be found in safety-critical systems such as medical devices, autonomous vehicles, and other devices involving an environment where safety is of paramount importance.[5] While having a great impact on our society, CPS is said to revolutionize our industry as they have been driving the biggest shift in business and technology since World War II.[4]

The requirements of constant interconnectedness among physical objects and the user in IoT/CPS are complex in nature due to limited computation, limited bandwidth, power consumption, and storage problems among others. Since safety and security of a system overlap and affect each other,[6] it is mandatory to analyze all possible layers of a system especially of a cyber-physical system to identify and control those risks[7] having the potential to compromise not only the security but also the safety of the system, its environment, and its users.[8] This, in turn, will also enhance the user's trust in IoT/CPS.[9–11] The complex nature of CPS makes it difficult to integrate the traditional security protocols and mechanisms in it. Implementing complex security requirements does not only demand their elicitation and modeling but also requires a risk analysis and mitigation to determine the importance of these requirements within the system. Ensuring the system's adequate handling of safety, security, and privacy threats is the only way to gain public trust in CPS. Despite the awareness of the importance of security requirements and risks in the analysis of CPS, little effort has been spent on consolidating our knowledge on the subject. An overview of the possible risk management techniques that could be integrated into the development and maintenance of CPS contributing to improving its security level is still lacking.[5] Yet understanding of the landscape of the proposed approaches to risk handling in security requirements engineering is beneficial for both practitioners and researchers in the field. Practitioners would be informed on those approaches for which empirical evidence exists that they work in context, while researchers would be informed on those security requirements and risk related aspects that have seen much investigation and those that are under-researched.

Most of the literature reviews conducted over the last two decades cover only pro-active risk management techniques[12] that are mainly proposed for traditional IT systems and are modified to be integrated in the development of CPS. To provide such an overview, we carried out a systematic mapping study of literature by using the guidelines of "Systematic Mapping Studies in Software Engineering".[13,14] Our study not only covers the security requirements of CPS and their associated risks but also includes the techniques and frameworks proposed to identify, assess, mitigate, and manage these risks along with the evaluation mechanism used to assess its performance.

In what follows, we first present related work and then describe our research process including our research goals, search strategy, the process of selecting studies, and our results to the designed research questions, followed by the discussion on our findings, the possible threats to the validity and measures taken to eliminate or minimize the effect of those threats to our research, possible future work, and finally the conclusion of our study.

2 | RELATED WORK

The differences between the traditional IT security systems and CPS are based on the identification, assignment, and calculation of assets, threats, and vulnerabilities.[15] In regards to these topics, scholars form two streams of the related work which is relevant for this paper:

(i) studies on security requirements for CPS and (ii) studies on security risk assessment methods for CPS. As part of preparing this paper, we specifically selected for inclusion as related work, those publications that are surveys of the literature on identification, assignment, and calculation of assets, threats, and vulnerabilities. These sources (21 in total, obtained using the search process mentioned in Section 3) shown in Table 1, are where we compare previously published work with our work reported in the present paper. In what follows, we summarize the findings of these sources.

2.1 | Security requirements in CPS

Security requirements are reported to be specific to every sector in the economy implementing CPS with different priorities and vulnerability levels (e.g., Mashkoor et al.[8]). These requirements can be classified as sensing requirements, storage requirements, communication requirements, actuation control requirements, and feedback security requirements.[32] According to Shafi,[32] prevention, detection, and mitigation are the building blocks of a security mechanism for CPS and prevention, detection, and recovery; resilience and deterrence are some of the countermeasures to counteract the risks identified against each of the security requirements in CPS.[33]

Three key security requirements identified for IoT are confidentiality, trust, and access control.[13,14] In another study, availability, confidentiality, and integrity are considered to be the three main security objectives in CPS like the smart grid.[31] However, the most reported security requirement in literature is the reliability of the CPS.[39] Although, these requirements have their associated open issues that raise serious concerns on the integration of IoT and the communication technologies in a secure middleware. For systems involving different technologies and varying communication standards, there is a need to develop a unified vision regarding the assurance of security and privacy requirements, for example, in systems with heterogeneous environments.[20] These requirements are considered an important part of IoT, implementation of which has led to the development of user's trust in a software system.[23] Table 1 below presents literature sources on security requirements of CPS and the risk processes adopted in the context of these systems to reduce the impact of possible hazards. Therein, we also highlight differences of our work from the published literature studies; please see the last column of Table 1.

2.2 | Security risks in CPS

Source, target, motive, attack vector, and potential consequences are the five common factors identified against every threat to CPS security, categorized as physical threats, political threats, criminal threats, and privacy threats.[19] For every CPS system such as ICS, smart grids, remote medical devices, and smart cars, the factors against each of the categorized threats vary; this variation is a result of isolation assumptions, cyber vulnerabilities, cyber physical vulnerabilities, increase in connectivity, and heterogeneity.[34] Cyber attacks on CPS can also be classified into a targeted security objective.[31] Some of the major cyber attacks on CPS reported are compromised-key attacks, man-in-the-middle attacks, eavesdropping, denial of service (DoS), and spoofing.[38] Threats, such as the DoS, and unauthorized access/integrity breach are the roots of the risks to the government and industry.[40] These risks include brand damage, share price reduction, loss of revenue, and in the worst-case scenario a loss of life. Flaws in the architecture of Supervisory Control and Data Acquisition (SCADA) systems give away the opportunity to hackers in exploiting the system's services. To mitigate these risks various standards and a set of best practices have been established over the years.[26]

2.3 | Managing risks in CPS

Considering the wide range of threats imposed at various levels of CPS, implementation of security requirements itself alone is not enough to ensure security in critical systems and develop user's trust in the system. Management of risks related to these security requirements is also necessary to achieve the objective of gaining a user's trust in the system. Risk management involves the process of identifying risks, analyzing the impact of the identified risks, mitigating the risks to reduce their impact on the system, and monitoring the system for any risks left un-attended.[41] The need for managing security risks of CPS like ICS is well emphasized in the literature (e.g., Cheminod et al.[25]).

2.3.1 | Risk identification

Regarding the second stream of our related work, that is, the management of security risks in CPS, risk identification is the first phase of the risk management process identifying any possible risks from both the requirements and the architecture of the software system. Multiple intrusion detection techniques were reported in literature categorized into four types, that is, anomaly-based, specification-based, signature-based, and reputation-based instruction detection techniques. According to the study, behavior- and traffic-based collection in various wireless systems is

TABLE 1 Contribution of published literature surveys on CPS security and risk processes

Ref	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	15	34	35	36	37	38	Our work
Security requirements																									
Authentication	Y	Y	Y		Y		Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y	Y
Authorization		Y	Y	Y	Y		Y	Y				Y					Y			Y		Y			Y
Confidentiality	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y
Non-Repudiation					Y	Y	Y	Y				Y					Y								Y
Linkability		Y																							Y
Anonymity					Y			Y		Y					Y										Y
Integrity	Y		Y		Y		Y	Y		Y	Y	Y	Y		Y	Y	Y	Y		Y		Y		Y	Y
Liability			Y												Y										Y
Availability	Y		Y	Y	Y		Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y		Y	Y
Reliability	Y			Y				Y		Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y
Trust	Y		Y		Y			Y	Y	Y			Y	Y	Y	Y	Y			Y			Y	Y	Y
Self-Healing					Y					Y					Y				Y						Y
Fault-Tolerance														Y	Y				Y						Y
Resilience		Y	Y							Y					Y	Y		Y		Y	Y			Y	Y
Data-Freshness				Y	Y										Y										Y
Risk processes																									
Risk Identification	Y		Y	Y			Y		Y			Y	Y		Y	Y		Y	Y		Y	Y			Y
Risk Assessment	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y
Risk Mitigation	Y		Y	Y		Y					Y					Y		Y						Y	Y
Risk Management	Y	Y	Y		Y							Y		Y											Y

important for detecting attacks in such systems.[22] Based on such nature of the CPS, the existing attack detection methods can be classified in four schemes namely signal-based, packet-based, pro-active,[42] and hybrid schemes.

2.3.2 | Risk assessment

It is necessary to take fully into consideration the CPS characteristics to find a suitable and specific risk assessment method.[30] For that, it is important to explore the interdependencies between system components to identify all the possible risks. These interdependencies can be categorized as common/geographical, cascading/functional, and escalating/impact failures and can be identified and assessed using hazard identification methods, causal analysis methods, consequence analysis methods, topological analysis methods, and dynamic analysis methods but still unreliable.[35]

The studies conducted on risk assessment approaches divided them into two main categories, namely, qualitative approaches and the quantitative approaches depending upon the conditions applied under.[27] The qualitative approaches are deemed best suitable to contexts in which there is time-related urgency, small budget, non-availability of relative data, or situations in which the agents conducting the process of risk assessment do not have the skill set required to conduct a quantitative analysis of the identified risks,[27] such as risk assessment matrix[43] and impact matrix.[44] In contrast to the qualitative approaches, the quantitative analysis techniques such as fault trees,[37,45] bow-tie trees,[46] and event trees,[35] allow comparative analysis of risks involved and protection measures[47] providing a more precise evaluation of the risks of an application.[48] However, according to the results of a review study, that is, Cherdantseva et al.,[16] risk assessment techniques for the security requirements in CPS are difficult to be categorized. The review[16] thus classifies the techniques based on the level of detail covered by the technique, the type of risk values assigned to a particular requirement, and the type of method adopted, that is, a formal method or a model-based technique.

One of the most commonly used risk assessment technique, that is, attack trees are considered to be self-documenting but are difficult when enumerating all the actions of an attacker and his/her concurrent actions. Fault trees, on the other hand, are good at explicitly visualizing the relationship between the events and the causes leading to the system failure but become complex when expressing all possible sequences of a large system, plus fault trees fail to visualize the interdependencies between them.[37] Game-theoretic approaches are also commonly used approaches to identify and analyze the risks related to the security requirements of a system, although these approaches help to identify and analyze the severity of the risk but are known to be unreliable due to the factor of biasness resulting from analyzer's lack of domain knowledge and motivation. Even with such drawbacks, the approach is known to be a versatile tool in analyzing complex systems.[24]

Some authors (e.g., Nazir et al.[38]) argue that simulations and models representing the attack designs could possibly help in the better assessment of risks related to the security of CPS, providing theoretical guidelines detecting attacks and resilience controls. However, a study[36] conducted on such methods highlighted the limitations of using existing risk assessment techniques and mitigation strategies as there exists a distinct difference between IT security and CPS security, and these risk assessment methods are not specifically designed for CPS security. From the perspective of CPS, the lack of security testing technology, lack of risk assessment systems, and the lack of behavior audit along with the use of malicious code to gain unauthorized access are the main causes of CPS (e.g., the ICS,[28] unmanned drones,[49] medical monitoring systems,[50] autonomous automotive systems,[51] and distributed robotics[52]) being vulnerable to cyber attacks which in turn are a major strategic issue for the national economy and the livelihood of the people.[28]

2.3.3 | Risk mitigation and management

Risk mitigation techniques can be classified based on the layer applied on, that is, application layer mitigation, network layer mitigation, and physical layer mitigation.[31] Nature of CPS leads to varying priority of security attribute in CPS and thus requires specific mitigation measures.[6] The mitigation measures proposed over the years range from physically placing security personnel guarding the system,[53] to controlling access to the system or data and[54] finally to integrating encryption schemes[55] ensuring confidentiality, authenticity, and integrity[56] of the data being transmitted between different components of the system. Most of the mitigation measures proposed over the years are driven either from exiting literature or internationally recognized standards introduced against the development of safety and security-critical infrastructures.[57]

A survey conducted on risk assessment and management methodologies specific to ICS revealed that the security metrics specific to these systems are the main obstacle in implementing the surveyed risk assessment and management methodologies. The study revealed the failures that occur in each of the risk management activities without implementing the countermeasures. Although the study provides a comprehensive survey of risk processes in ICS, it still lacks research of the domain in smart systems, for example, smart grid systems, smart homes, autonomous vehicles, and weapons.[17] Similarly, a study was conducted on performance assessment of three state-of-the-art risk management approaches, namely, MEDUSA, MITIGATE, and CYSM approaches for a CPS, that is, maritime supply chain and port services. The results revealed the limitations of the aforementioned approaches.[58]

Summarizing Table 1, we conclude that existing related reviews lack information on the risk management process for some of the security requirements such as liability, data-freshness, fault-tolerance, self-healing, linkability, and authorization. Also, risk management and mitigation are

altogether ignored since the majority of the reviews are focused on risk assessment and identification. This lack of consolidation of the published findings on CPS Security and Risk Processes motivated us to conduct the present systematic mapping study. Our aim for this study is not only to highlight the security requirements essential for the development of a CPS system but also to report on the related possible security risks, proactive, and reactive risk management processes adopted for managing those risks and the evaluation methods adopted to validate the performance of those techniques, approaches, and framework techniques along with some demographics related to the origin of the study and the popularity of CPS around the world.

3 | GOALS AND OBJECTIVES

The goals of this mapping study and their related research questions have been carefully identified using the Goal-Question-Matric Paradigm.[59] Table 2 presents both the goals and the research questions to be answered. Therein, G1–G5 are the goals and the research questions (RQs) associated with these goals and are labeled accordingly, for example, G1.RQ1 means the first RQ associated with goal G1.

3.1 | Search string

The search string used for this research consists of three parts marked as C1–C3:

- C1 is a string made up of keywords related to the cyber physical system such as "cyber physical system (CPS)," "smart systems," and "industrial control systems."
- C2 is a string made up of keywords related to risk processes such as "risk identification," "risk assessment," "risk mitigation," and "risk management."
- C3 is a string made up of keywords related to the security requirements such as "security requirements" and "security."

Below, we present our search criteria in the form of a Boolean expression:

$$C1\ AND\ C2\ AND\ C3\ (\text{search criteria in the form of a Boolean expression}). \quad (1)$$

More in detail, we show below the formulated combinations of the search strings used in electronic databases to conduct the required research:

- ("Cyber Physical System") AND ("Risk Identification") AND ("Security Requirements")
- ("Cyber Physical System") AND ("Risk Assessment") AND ("Security Requirements")
- ("Cyber Physical System") AND ("Risk Mitigation") AND ("Security Requirements")
- ("Cyber Physical System") AND ("Risk Management") AND ("Security Requirements")
- ("Smart System") AND ("Risk Identification") AND ("Security Requirements")
- ("Smart System") AND ("Risk Assessment") AND ("Security Requirements")
- ("Smart System") AND ("Risk Mitigation") AND ("Security Requirements")
- ("Smart System") AND ("Risk Management") AND ("Security Requirements")
- ("Industrial Control System") AND ("Risk Identification") AND ("Security Requirements")
- ("Industrial Control System") AND ("Risk Assessment") AND ("Security Requirements")
- ("Industrial Control System") AND ("Risk Mitigation") AND ("Security Requirements")
- ("Industrial Control System") AND ("Risk Management") AND ("Security Requirements")

The search string was manually deployed on the electronic databases that are presented in Table 3, based on the search options provided by each of these databases.

3.2 | Search strategy

Our search strategy involved defining the repositories of literature in terms of the electronic databases searched, the items extracted, and the target language of the literature, as shown in Table 3.

TABLE 2 Research goals and research questions

G1	To classify the nature of published scientific articles in the area of risk identification, assessment, mitigation, and management of the security requirements in IoT/CPS, whether new techniques are being developed, whether they are supported by tools.	
Research Questions	G1.RQ1. What types of articles are published in this area? G1.RQ2. What approaches/methods/models/techniques are proposed for risk identification of the security requirements in IoT/CPS? G1.RQ3. What approaches/methods/models/techniques are proposed for risk assessment of the security requirements in IoT/CPS? G1.RQ4. What approaches/methods/models/techniques are proposed for risk mitigation of the security requirements in IoT/CPS? G1.RQ5. What of the proposed approaches/methods/models/techniques are used to conduct risk management of the security requirements in IoT/CPS?	Our focus in this area is on the following risk processes: 1. Risk Identification 2. Risk Assessment 3. Risk Mitigation 4. Risk Management
G2	To understand the various aspects of security requirements in IoT/CPS (e.g. types of security requirements, differences between the security requirements of IoT/CPS and in IT Networking) that are being investigated by researchers	
	G2.RQ1. What are the reported security requirements of IoT/CPS in the studied articles?	
G3	To understand the various aspects of risk assessment of security requirements in IoT/CPS (e.g., risks identified, mitigated and managed against each of the security requirements in IoT/CPS) that are being investigated by researchers	
	G3.RQ1. What risks have been identified associated with the highlighted security requirements in IoT/CPS?	Highlights the type of risks identified e.g., violation in user authentication
	G3.RQ2. What is the risk impact investigated with the associated security requirement in IoT/CPS	Identifies the part of the system showing the impact of attack occurred
G4	To study the nature of empirical evaluation, if any, that is being conducted, the tools being used for evaluation and the application domain, and the contextual settings where the evaluation happened application domain(s)	
	G4.RQ1. What mechanisms of evaluation have been adopted to test the proposed approach?	Identifies whether the evaluation was conducted manually or automatically
	G4.RQ2. What metrics have been used for evaluating the proposed approaches?	Identifies the methods, approaches, and tools used to test the performance of the proposed risk identification, assessment, mitigation, and management techniques
	G4.RQ3. Which application domain(s) have been used for evaluating the developed approaches?	Identifies the case study(s) and dataset (if any) used for evaluation purpose
G5	To identify the most active researchers in this area and their affiliations, and to identify the most influential articles	
	G5.RQ1. What is the annual article count? G5.RQ2. What is the article count by venue type? G5.RQ3. What is the citation count by venue type? G5.RQ4. What are the most influential articles in terms of citation count? G5.RQ5. What are the venues with the highest article count? G5.RQ6. What are the venues with the highest citation count? G5.RQ7. Who are the authors with the highest number of articles? G5.RQ8. What are the author affiliations, i.e., do they belong to academia or industry? G5.RQ9. Which countries have produced most of the articles?	Identifies the "intensity" of published output in terms of volume of papers published per year and venue type; most used venues; most frequently published authors and publication citation output with highest counts.
G6	To determine the recent trends in this area and to identify future research directions	
	G6.RQ1. What limitations have been reported? G6.RQ2. What lessons learned have been reported? G6.RQ3. What are the trends in the area? G6.RQ4. What future research directions are being suggested?	Identifies the strengths, weaknesses, and challenges faced during the implementation of existing methods used for risk identification, assessment, mitigation, and management of security requirements in IoT/CPS.

TABLE 3 Search sources

Source of research papers	Electronic databases	Initial paper count
	Springer	522
	ACM digital library	51
	IEEE Xplore	491
	Science direct	204
Search items	Journals, conference papers, book chapters, and workshop papers	
Search applied on	Full text—to avoid missing any possible publication in the area	
Language	English	
Publication period	2000–2020 March	
Initial paper count	1,268	
2nd iteration paper count	1,285	
3rd iteration paper count	440	
Final paper count	312 (see Appendix B)	

TABLE 4 Inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
I1. Papers are written in English language.	E1. Papers that discuss risk identification, assessment, mitigation, and management of security requirements of CPS, as background only or as a side topic.
	E2. Papers that only present a vision or a viewpoint, or report keynotes, or discussions, opinions, editorials comments, prefaces, tutorials and anecdote papers, and presentations in the form of slides without any associated research articles.
I2. Contents of the paper are focused on risk identification, risk mitigation, and risk management of the security requirements in CPS.	E3. Papers that are not peer-reviewed and appeared as technical reports, white papers, and editorial papers.
	E4. Papers related to security or security of CPS but not related to the risk identification, assessment, mitigation, and management of security requirements of CPS, for example, papers presenting security breaches in CPS.[60]

Other than restricting our study to the above defined electronic databases, we scrutinized the full text of each article based on the following inclusion and exclusion criteria (see Table 4) before including it into our mapping study:

3.3 | Study search and selection

Our initial search (first iteration) resulted in a total of 1,268 papers. This first iteration was the extraction of potentially relevant papers using the above-mentioned search strings one at a time. During the second iteration, the overall paper count came to a total of 1,285 via the reference search (snowballing[61]). In a third iteration, we read the abstract and the introduction sections of the papers that we identified. During this iteration, nearly 66% of the 1,285 papers failed to meet our inclusion criteria defined above; hence, we excluded them. This left us with 440 papers whose text we read completely. However, after the whole text was read, some of the papers failed to meet the above-stated criteria and were excluded. This made the final count of 312 papers to be included in our mapping study.

4 | FINDINGS OF OUR REVIEW

This section provides answers to our research questions.

4.1 | (G1.RQ1) what types of articles are published in this area?

As Figure 1 indicates, we found that 52% of the articles covered in this review were published in conferences followed by journal publications (44%) and workshop papers (4%). Most of these articles focus on risk assessment of the security attributes in IoT/CPS followed by identification, mitigation, and management. We observed that nearly half of all selected papers are dedicated to risk assessment, and only 9% are on risk management. Venues of all the articles included in our study can be seen in tables: Tables A1–A3 in Appendix A.

4.2 | (G1.RQ2) what approaches/methods/models/techniques have been proposed to conduct risk identification of the security requirements in IoT/CPS

The review shows that 105 papers out of the 312 in our set focus on risk identification in CPS. Figure 2 shows the detailed results including names of the proposed framework, technique, or approach against its frequency in those 105 papers used to identify the security risks within the CPS. The risk identification mechanisms proposed over the years can be classified based upon the nature of the process executed, that is, the use of UML models[62] and Markov Chain Monte Carlo algorithm.[63] According to Figure 2, the most commonly used techniques are Model-based techniques used in 32 articles, followed by intrusion detection in 19 papers and matrix-based techniques in nine articles. The techniques are traceable to various theoretical foundations such as the use of models[64] (such as trees,[35] dependency graphs,[65] and flow charts[35]), game theory,[66] and on standards.[67] Furthermore, fuzzy logic-based approaches[20] have also been proposed over the years to identify the security risks more accurately within IoT/CPS.

Some of the papers proposed frameworks such as the Generic Security Engineering Framework for the overall security engineering process (SEP),[68] structured object-oriented security requirements analysis,[69,70] that consisted of certain steps to be executed for risk identification.

4.3 | (G1.RQ3) what approaches/methods/models/techniques have been proposed to conduct a risk assessment of the security requirements in IoT/CPS?

In our final pool of 312 papers, we found 233 papers that discussed the techniques proposed for risk assessment as shown in Figure 3. Among the proposed techniques, model-based risk assessment was the most frequent in our selected literature (92 times). For example, fault trees, hierarchical holographic models (HHM),[71] fuzzy modeling,[72] attack trees,[73] and formal models[74] were used.

Furthermore, matrix-based risk assessment techniques[75] were indicated in 31 papers and standard-based techniques such as risk assessment technique based on ISO/IEC 27005:2011 standard[30] occurred in 20 papers. Finally, frameworks proposing hybrid assessment techniques were presented in 17publications. These frameworks are as follows:

1. Unified framework based on probability measure (literature, statistics, brainstorming activities, and specific tools such as failure model, effects, and criticality analysis [FMECA], hazard and operability study [HAZOP], and quantitative analysis),[76] the generic security engineering framework for overall security engineering process (SEP),[68] and knowledge-in-the-loop approach.[77]

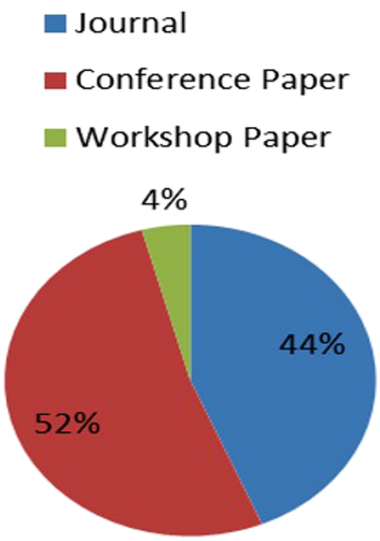

FIGURE 1 Types of articles published in the area

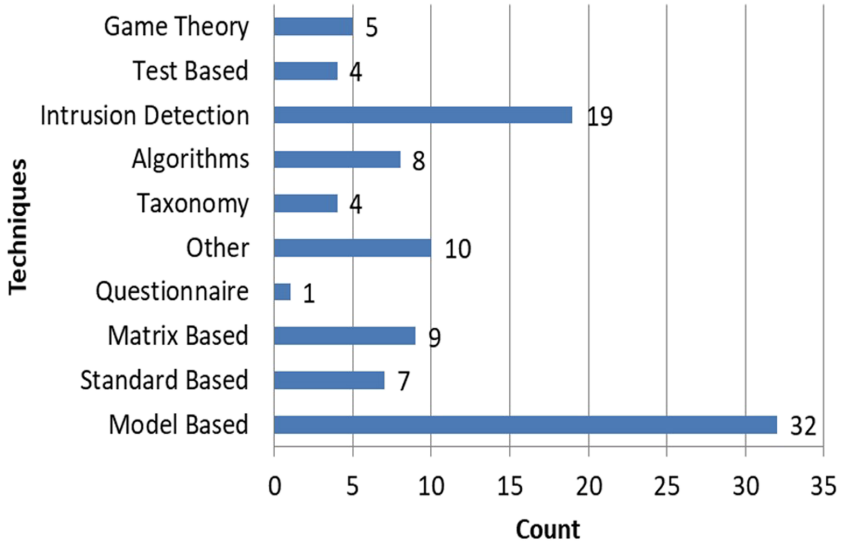

FIGURE 2 Risk identification techniques

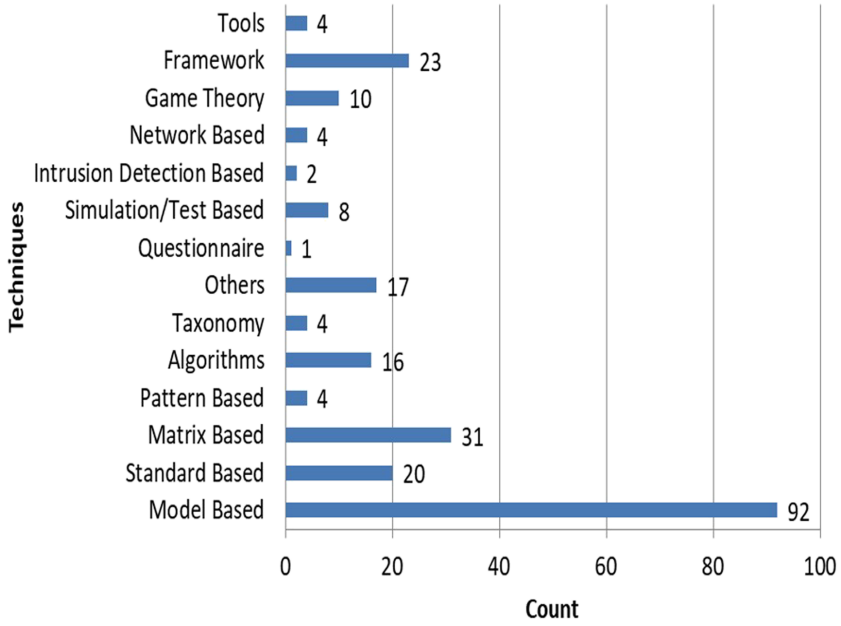

FIGURE 3 Risk assessment techniques

2. Frameworks based on model-based techniques to assess the impact a particular risk can have on the system such as Markov-based approach,[15] dynamic cyber-security risk assessment approach based on Bayesian network,[78] and methods such as three-layer cyber-physical risk assessment methodology based on Deterministic Stochastic Petri Net (DSPN).[79]
3. Frameworks following the guidelines provide by existing standards[51,80,81] introduced for the development of safety and security-critical systems such as the railway fire alarm system or implantable smart medical devices and avionics, for example, Security Information Correlation Methods integrated with Cyber Threat Intelligence Analysis Engine (CAESAIR),[82] and System Theoretic Process Analysis (STPA)-SafeSec method.

Other than these techniques, probability-based,[83] game theoretic-based,[84,85] and standard-based techniques have been proposed over the years to accurately identify the severity of the identified risks. Game-theoretic techniques include components for risk identification and mitigation activities.[86] The tools developed for risk assessment of security requirements in CPS such as the Physical and Cyber Risk Analysis Tool (PACRAT),[87] were based on standards. Some well-developed approaches have also been used for assessing the severity of the security risks in

CPS such as the Security Quality Requirements Engineering (SQUARE), Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE),[15] and Expression of Needs and Identification of Security Objectives (EBIOS).[88]

In terms of security and safety risk assessment of CPS, we observe that many of the standard-based techniques used the International Organization for Standardization (ISO) standard as a basis for calculating risk values. However, we also observe that some techniques employed a standard, that is, European Norms (EN) and International Electrotechnical Commission (IEC) that was specifically developed for the peculiarities of application domains, that is, railway (EN50128–IEC 61508),[5] avionics (DO-178B/C),[89] and medical equipment development (ISO 14971).[90]

4.4 | What approaches/methods/models/techniques have been proposed to conduct risk mitigation of the security requirements in IoT/CPS?

Our findings revealed that almost 21% of our selected papers were based on risk mitigation. Figure 4 shows the techniques extracted from the papers. The most frequently proposed approach is based on what is called a "mitigation measures": this is a set of guidelines specific to mitigating a particular risk, for example, use of secure communication channel,[91] integrity checks on data transactions,[91] limited access control,[31] filtering and monitoring countermeasures,[92] reconfiguration, use of coordinated and uncoordinated protocols,[31] and physical and environmental security.[25] We also note that these mitigation measures are derived from existing standards, observations of real-world incidents, and the literature.

Furthermore, the second most frequently discussed approach in our set of selected papers is grounded in the use of models (10), for example, cyber-physical cost modeling using game-theoretic approach,[93] SmartOrBAC model,[94] adaptive decision-making models, and the evaluation and validation models.[95] Finally, the frameworks proposed for risk mitigation are a combination of model-based risk mitigation techniques with a set of controls or guidelines provided by the standards specific to mitigating particular security risks, for instance, the use of cryptosystem to ensure secure data transactions between the various nodes of the system,[96] the installation of firewalls,[97] and use of intrusion detection and prevention systems.[98]

4.5 | (G1.RQ5) what approaches/methods/models/techniques have been proposed to conduct risk management of the security requirements in IoT/CPS?

We found 41 papers that focused on risk management techniques as shown in Figure 5. As can be seen therein, most of the work done in the risk management domain rests on model-based techniques (31%) and standard-based techniques (4%). Examples of model-based techniques are those

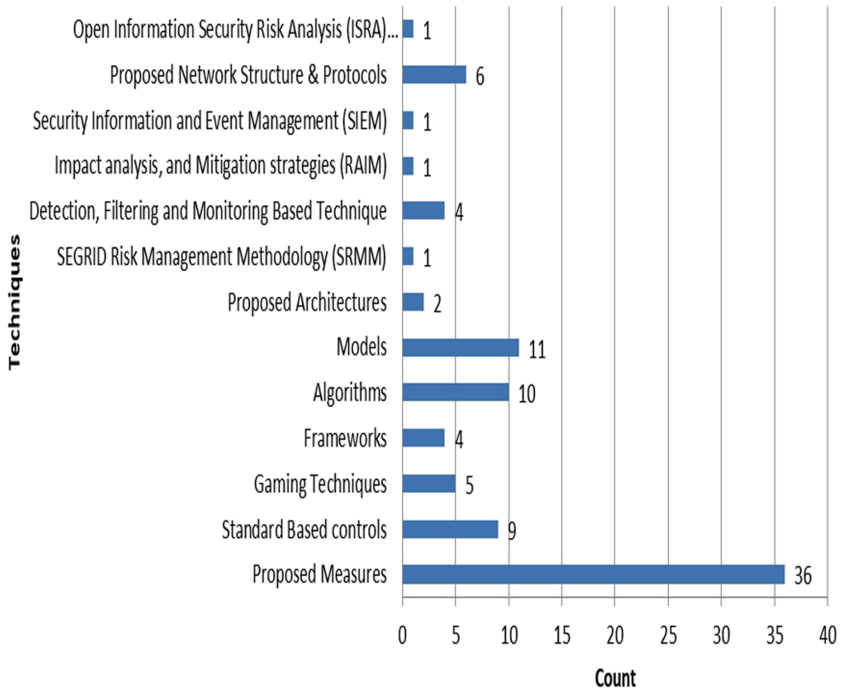

FIGURE 4 Risk mitigation techniques

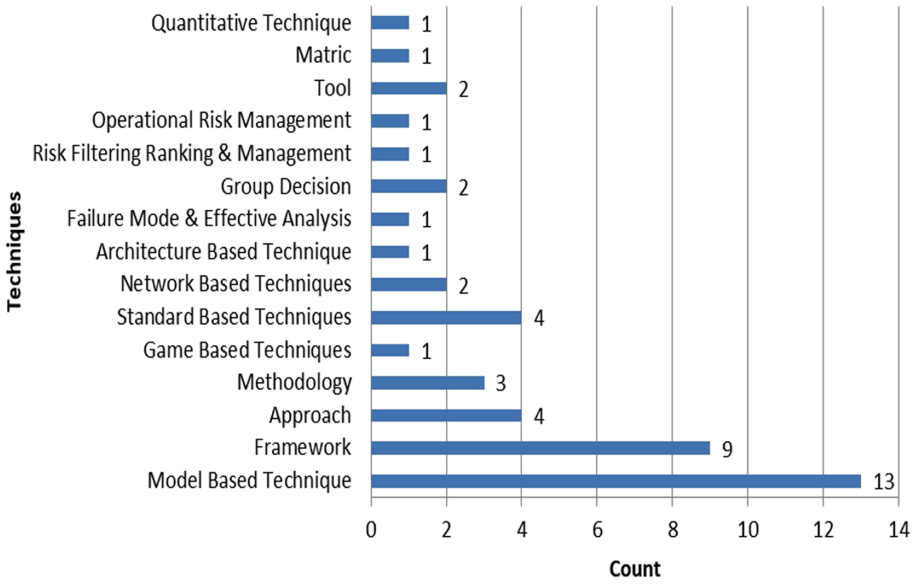

FIGURE 5 Risk management techniques

using HHM, graphs, and trees. Examples of standard-based techniques rest on, for example, Capability Maturity Model Integration (CMMI) and Control Objectives for Information and Related Technologies (COBIT 5). Furthermore, trust management is also considered as a risk management technique as trust is one of the security attributes in IoT/CPS.[23] We found that around 22% of the papers representing the risk management framework proposals consisted of a combination of various techniques in particular to each phase of the risk management process, that is, risk identification, assessment, mitigation, and monitoring, for example, framework based on SEP[99] and Criticality-Aware Access Control (CAAC) theoretical framework.[100]

4.6 | (G2.RQ1) what are the reported security requirements of IoT/CPS in the studied articles?

Our reviewed literature sources covered eight security requirements (see Figure 6, on the left) also known as security attributes that are of utmost importance in implementing a secure CPS. These security requirements attribute consist of the following:

- Authentication (the ability of verifying the identity of a user or a process[68,101,102]).
- Authorization (the ability of verifying privileges of a particular user or a process[81]).
- Confidentiality (a property of data usually resulting from legislative measures preventing it from unauthorized disclosure[68,102]).
- Non-repudiation (repudiation protects against false denial of having participated in a communication or transaction[81]).
- Data freshness (refers to the property of a system keeping the data up-to-date[30]).
- Anonymity (refers to the property of a user having the permission to disclose its own identity within the network[33]).
- Integrity (ensures that the data is not maliciously or accidentally altered during storage or transition[16]).

Along with these, the researchers and practitioners have also emphasized on integrating the following dependability attributes (see Figure 6) in CPS:

- Linkability (is concerned with the extent to which a given data set allows one to establish the identity between the two pseudonyms[103]).
- Liability (refers to having an accountable responsibility defined within the system in-case of any loss, misuse, theft or during any unusual event[30]).
- Availability (refers to the availability of the system during the defined time[16]).
- Reliability (is concerned with the reliability of the operations to be performed by the system or a sub-system[16]).
- Self-healing (if one device fails to operate then the rest of the system should provide maximum level of security in CPS[30]).
- Resilience (refers to the property of the system showing resilience to any attacks in case of a component failure[30]).
- Trust (ensures the privacy of personal information[16]).

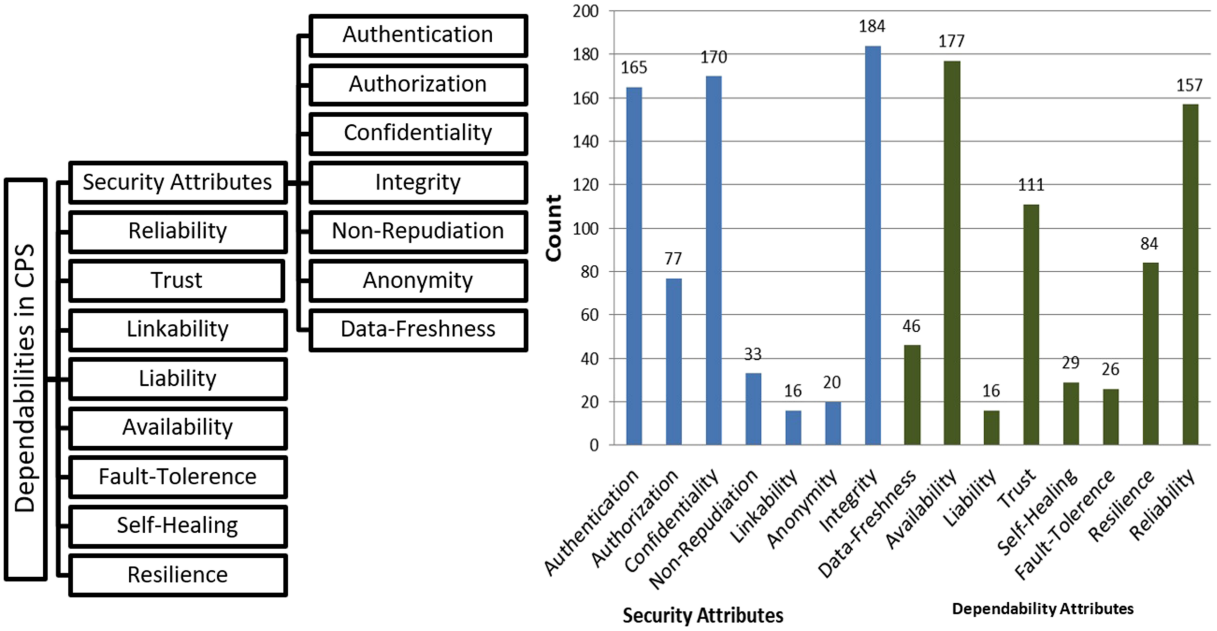

FIGURE 6 Security requirements and dependabilities in CPS

Since trust, system reliability, and resilience against security threats in CPS are mainly based on data confidentiality, integrity, authenticity, and system's authorized access,[104] some papers have considered them along with availability, fault-tolerance, and self-healing to be a crucial factor being integrated in CPS.[5] In our selected set of papers, the most frequently covered security requirements are integrity (in 184 papers), confidentiality (170 papers), and authentication (165), while the most studied dependability attributes consisted of availability (177 papers), reliability (157 papers), and trust (108 papers). However, linkability (16 papers), anonymity (20 papers), fault tolerance (26 papers), and liability (16 papers) were the least frequently discussed (see Figure 6, on the right).

4.7 | (G3.RQ1) what risks have been identified associated with the highlighted security requirements in IoT/CPS?

As the term of CPS covers all types of mission-critical, safety-critical, and security-critical systems, the risks identified do not cover only the software part but are also relate to the physical impact of the system. Figure 7 presents the 22 risks identified in the final set with respect to the security requirement attributes of CPS(s). The most frequently reported risk is cyber security (195 times), followed by privacy and confidentiality violation (56 times), abnormal behavior (47 times), and cascading failure (46 times). However, socioeconomic affairs and backup failure are the least discussed risks in the list.

4.8 | (G3.RQ2) what is the risk impact investigated with the associated security requirement in IoT/CPS?

The statistical results obtained on the reported risks in CPS from our studies show that the most reported impact of the identified risks consisted of (1) communication disruptions [57,105], (2) system or sub-system being compromised,[106,107] and (3) leading to system's abnormal behavior[108] and thus failure as a result of a malicious attack.[109–111] Another frequently reported impact is related to the physical aspect of the CPS and that is the equipment failure leading to financial losses, for example, Lopez et al.[73]

4.9 | (G4.RQ1) what mechanisms of evaluation were adopted to test the proposed approach?

Out of the 312 papers studied, 178 (57.1%) papers validated their proposed approach. Figure 8 and Table A4 present the 11 validation techniques adopted by the authors of these 178 papers to empirically evaluate the proposed risk identification, assessment, mitigation, and management techniques. The figure indicates simulations, case studies, implementations, and statistical calculations among other validation techniques, which are the most employed mechanism by researchers to evaluate their proposed methods. The case studies included either real world industrial cases (as, e.g., in

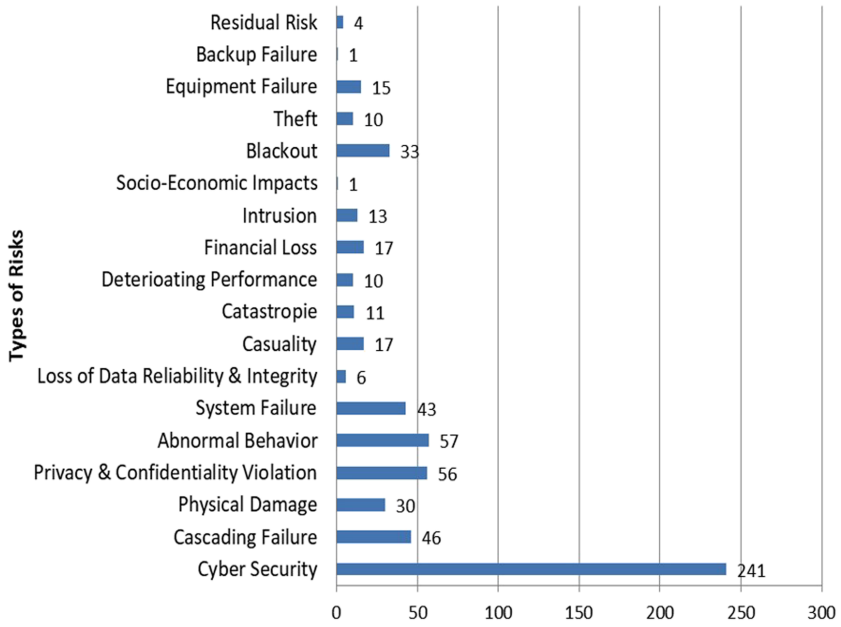

FIGURE 7 Risks in CPS

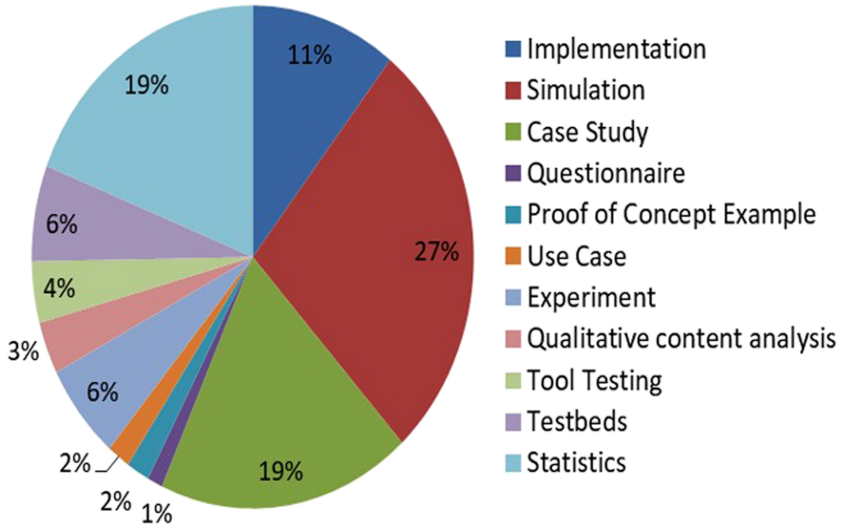

FIGURE 8 Validation techniques

Tsigkanos et al.[64]) or were proof-of-concept case studies (e.g., Aissani & Guetarni[105]). Simulations and experiments were based either on designed testbeds (e.g., Patel et al.[112]), opensource cases (e.g. Grechanik et al.[113]), or real-world industrial cases (e.g.,Wang et al.[114]). Some papers investigated the performance of their proposed techniques using the frequency of a load shedding or by using statistical tests such as the Wilcoxon signed-rank test.[115] Other researchers employed special-purpose tools to evaluate their proposed techniques: Cyber Security Argument Graph Evaluation (CyberSAGE) tool,[87] Smart Grid Information Security (SGIS) Toolbox,[116] and network application tool (NetAPT).[117] Some authors used manual risk assessment[118,119] and compared their results generated through computer-aided tools. For manual risk assessment, the techniques used are risk matrix, where for each identified risk value of H (High), M (Medium), and L (Low) is assigned by the professionals during meetings or group sessions.[120]

4.10 | (G4.RQ2) what metrics have been used for evaluating the proposed approach?

This subsection reports on the specific metrics that the 178 papers included in this mapping study had used in their empirical evaluations. Figure 9 and Table A5 present the validation metrics used to assess the performance of the proposed techniques. As we could see, some papers

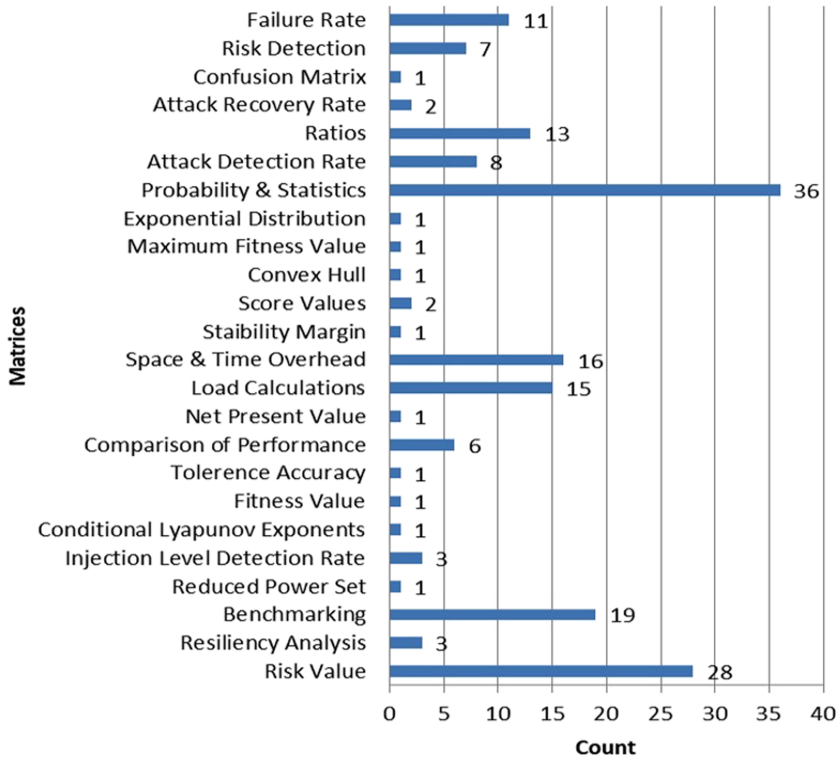

FIGURE 9 Validation matrices used during evaluation

reported the results in the form of ratios such as Potential Target Ratio,[121] message validation ratio percentage,[122] load loss ratio also known as load loss factor (LFR), and benefit-cost ratio (BCR).[84] The load calculations used for evaluating the performance of their proposed techniques consisted of readings on load shedding,[123] rate of cascading failure, LFR, load drop percentage, load curtailment (CL),[124] load forecasting,[125] and active power generation.[109] Markov steady-state probability,[126] probability of success, incidents, attack, loss,[127] line tripping, and failure[79] were also used to assess the performance of the proposed techniques in some of the papers studied. In general, statistical analysis conducted based on these ratios, risk value calculation, and benchmarking were among the most used matrices for validating a risk identification, assessment, mitigation, or management technique.

4.11 | (G4.RQ3) what application domains(s) have been used for evaluating the developed approach?

Figure 10 presents the application domains used for evaluating the proposed work in the papers included in the final set. Therein, there are 25 different domains used in 178 papers. It indicates that smart grid stations, IEEE 14/39/118-bus systems,[128] network applications,[58] and avionics-based application[107] were the most used application domains during the evaluation of the proposed techniques. In the case of smart grid stations, the main focus was to test the effect of the proposed technique in risk identification, assessment, mitigation of the known risks on communication, and load distribution systems (e.g.,Habash et al.[70]). The utility applications used as subject applications consisted of electricity billing software (e.g., Kaster & Sen[67]). The SCADA systems used consisted of smart grid stations, avionics, and other safety-critical systems (e.g., Banerje et al.[100]).

We also aggregated these domains into the three major categories shown in Orojloo and Azgomi[129]:

1. Mission-Critical Software Systems,[130] for example, Avionics and drones, more specifically.
2. Safety-Critical Software Systems,[25,71] for example, implantable smart blood sugar control systems, pacemakers, patient monitor control systems, chemical control systems, and railway control systems.
3. Security Critical Software Systems,[25] for example, email accounts, financial applications, office environment, and utility applications.

Using this categorization, we found that 34% of the 312 papers went to the mission-critical system category, 35% of the papers to the safety-critical system category, and 31% of the papers to the security-critical software system category.

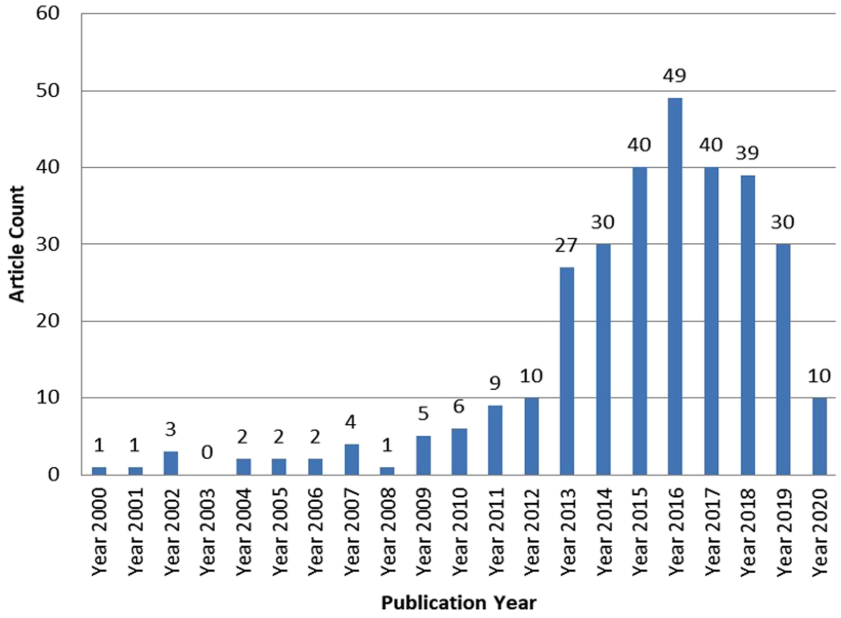

FIGURE 10 Annual article count

4.12 | (G5.RQ1) what is the annual article count?

Figure 10 reports the annual article count from 2000 to March 2020. We observe significant growth of published papers in the years 2013–2016. More than half of the papers selected in our review are published in this period. A slight decrease in the number of article publication can be seen in the years 2017–2019 but remains nearly constant.

4.13 | (G5.RQ2) what is the article count by venue type?

The information regarding the article count concerning the venue type is presented in Tables A1–A3. We note that there is no one specific venue dedicated to CPS and their security requirements. In fact, the 312 papers have been published in more than 215 different venues. Among those, IEEE Access, Transactions on Smart Grid Journal, Transactions on Power Delivery Journal, Power and Energy Society General Meeting (PES), and International Conference on Availability, Reliability, and Security (ARES), venues with an article count of 7, 6, 6, and 4, respectively, are the most targeted by the authors in this research area.

4.14 | (G5.RQ3) what is the citation count by venue type?

The venues along with their citation counts are shown in Tables A1–A3. Therein, we observe that 10.5% of the total number of venue types targeted had a citation count greater than 100. On the other hand, 8.3% of the total number of venue types targeted has a citation count of 0 due to the recent publication in these venues.

4.15 | (G5.RQ4) what are the most influential articles in terms of citation count?

Table 5 lists the details of the most influential journal articles, conference papers, and workshop paper in terms of their citation count. Due to space issues, we present only the two topmost cited papers form each category.

From the data extracted, most influential journal articles were published in 2010 and 2015. The most influential conference papers are dated from 2013 and 2017, while the most influential workshop papers are from 2004 and 2009, whereas the articles published in the last 5 years are found to have a citation count between 100 and 350 for journal articles, 1 and 80 for conference papers, and between 1 and 10 for workshop papers.

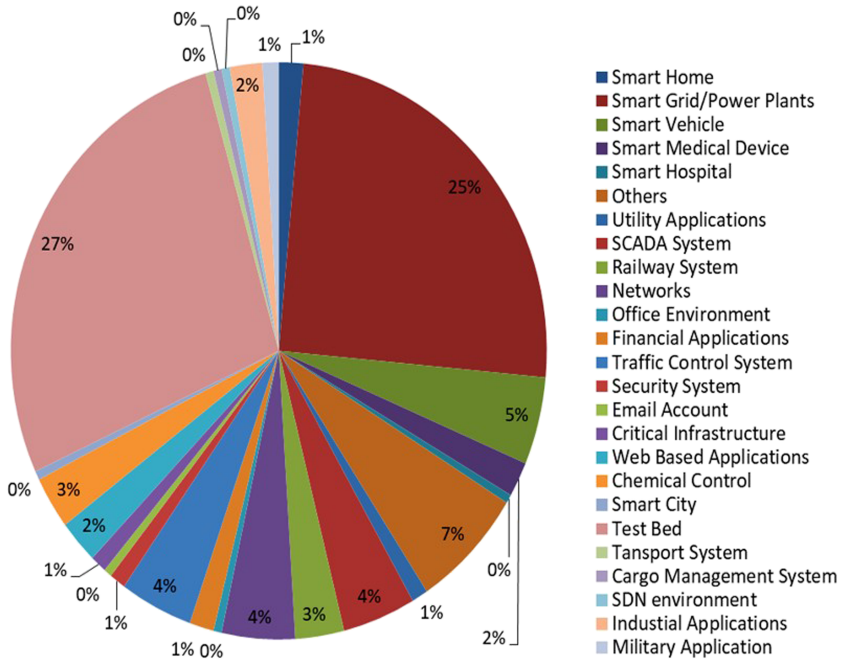

FIGURE 11 Application domains used for the evaluation

TABLE 5 List of influential articles w.r.t. citation count

Ref	Article type	Venue	Citation count	Publication year
[131]	Journal	Computer Law & Security Review	1,339	2010
[20]	Journal	Computer Networks	1,327	2015
[49]	Conference Paper	International Conference on Cyber Conflict	165	2013
[132]	Conference Paper	IEEE European Symposium on Security and Privacy	118	2017
[33]	Workshop Paper	Future Directions in Cyber-Physical Systems Security	450	2009
[133]	Workshop Paper	International Infrastructure Survivability Workshop	257	2004

4.16 | (G5.RQ5) what are the venues with the highest article count?

The highest numbers of journal articles were published in "Computer & Security" (9 papers), "IEEE Access" (7 papers), "IEEE Transactions on Smart Grids" and "Future Generation Computer Systems" (6 papers each), and "Journal of Reliability Engineering and System Safety" (5 papers). Regarding conference publications, "IEEE Power and Energy Society General Meeting (PES)" (5 papers), the "International Conference on Availability, Reliability, and Security (ARES)" and "IEEE International Conference on Technologies for Homeland Security" contributed 4 papers each, while the" IEEE International Smart Cities Conference", "IEEE International Conference on System of Systems Engineering", "International Conference on Intelligent Information Hiding and Multimedia Signal Processing", and "IEEE International Conference on Systems, Man, and Cybernetics", published 3 papers each. The pattern can be observed in the answer to the research question G5.RQ2 (Section 4.13).

4.17 | (G5.RQ6) what are the venues with the highest citation count?

The information on the citation for each venue targeted can be found in detail in G5.RQ3 and in Appendix A. There exists a varying number of citations against each of the selected papers in our review. Some of the most cited venues in terms of journals are "Computer Networks" (2214), "Computer Law & Security Review" (1,339), "Proceedings of the IEEE" (1,191), "Computers & Security" (1,050), "Journal of Network and Computer Applications" (777), "ACM Computing Surveys" (668), and "IEEE Transactions on Power Delivery" (616). Some of the most influential conferences based on their overall citation count consisted of "International Conference on Cloud Computing" (264), "International Conference on Cyber Conflict" (189), "International IEEE Enterprise Distributed Object Computing Conference" (144), and "IEEE European Symposium on Security and Privacy" (118).

4.18 | (G5.RQ7) who are the authors with the highest number of articles?

The results show that out of all 1,260 authors that published the 312 papers, only 2 authors (i.e., Nian Liu[109,124,128,134] and Manimaran Govindarasu[79,93,135,136]) published 4 articles, 7 authors (i.e., Tansu Alpcan,[24,85,137] Aditya Ashok,[79,93,136] Quanyan Zhu,[24,66,138] Yingmeng Xiang,[109,124,128] Mohammad Shahidehpour,[126,139,140] John Hird,[91,141,142] and Lingfeng Wang[109,124,128]) published 3 articles, and 70 authors published 2 articles. However, the rest of the authors are there with single entries. This suggests a broad variety of research organizations and researchers are interested in securing CPS and yet there exists no specific well-established schools of thought on the topic.

4.19 | (G5.RQ8) what are the authors' affiliations, that is, do they belong to academia or industry?

The affiliation of each individual author of an article included in this study was confirmed based on the information provided with the published article. The results revealed that most of the articles were authored by authors affiliated to academic institutions (72.04%), 22.1% of the authors were from industry, and less than 1% (in fact 0.64%) of the authors showed dual affiliation. We note that 4.8% of authors did not reveal their affiliation with any type of organization. These percentages suggest that most of the research on security requirements for CPSs happens in universities. The studies articulating collaborative research (5%) conducted by both the academia and the industry showed dual affiliation, where some authors belonged to academia and their co-authors to industry.

4.20 | (G5.RQ9) which countries have produced most of the articles?

A detailed description of the country-specific article distribution is shown in Figure 12. The country having the highest publication rate in the domain was found to be the United States (33.3%). The countries from which the least research were established were in Azerbaijan, Turkey, Denmark, Malaysia, Luxembourg, Cyprus, Morocco, Colombia, Slovenia, Czech Republic, and Oman (0.32% each). Next, much research comes from the European (52.2%) and the Asian countries (30.88%). The geographic zone with minimum articles is Africa (0.02%). The articles count among European countries shows that United Kingdom published 33, Italy published 23, Germany published 17, Norway published 11, and Sweden published 11 articles in the area of security of CPS. Last, the articles' count from Asia countries tells us that countries such as China (45), India (11), Pakistan (6), South Korea (6), and Iran (6) took the lead in producing most of the articles published in the area of risk identification, assessment, mitigation, and management for CPS.

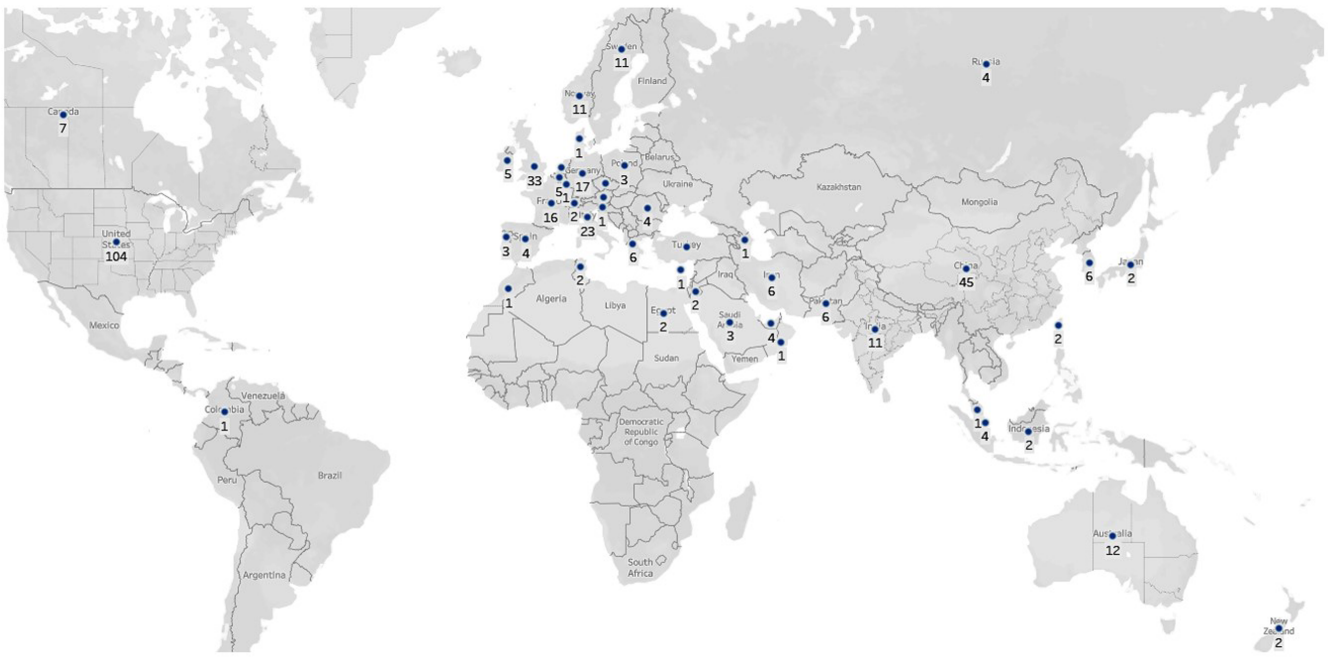

FIGURE 12 Country wise annual article count

4.21 | (G6.RQ1) what limitations have been reported in the set of selected papers?

We categorized the limitations reported in the studied literature as follows:

1. Most of the studies used fault trees for fault representation in the system under discussion. However, fault trees cannot be used to identify both the static and dynamic sub-trees representing various faults within the system.[37] The use of fault trees might give rise to overlook runtime faults in the system.
2. The papers in our set of 312 shows that most of the work done in terms of the techniques proposed for risk identification, assessment, mitigation, and management is specific to smart grids. The focus of the aforementioned techniques was on safety, security, and risk management standards specific to smart grids as in previous works.[62,104,105] In one way, this is not a limitation for professionals working on smart grids; however, it opens up avenues for researchers to explore other domains also. We think so because the proposed techniques might not be generalizable for other domains; thus, necessary tweaking in addition to groundwork is needed.
3. It is observed that nearly half of the proposed work lacked empirical validation[47,69,106,143] and was based on a large number of assumptions making it less generalizable to real world scenarios. For instance, in Dondossola et al.,[144] the proposed weight-based risk assessment framework was validated through an experiment done under a controlled environment where only certain attacks were implemented onto the system. This might raise some unseen concerns and questions on applying the proposed work to the real world scenarios
4. Probability-based techniques such as the PRA can be applied at its best when the potential security incidents are already in the history databases.[16] Otherwise, such techniques can lead to incomplete and inefficient risk identification in CPS. This dependency on the history database is a limitation towards new risks and security threats.
5. The proposed techniques focus on known risks, that is, risks reported in the literature. It is noticed that identification of new domain-specific risks is not that pursued in the literature that often leads to inefficient risk assessment, mitigation, and management of security in critical systems.

The limitations stated above open up avenues for the researchers and practitioners to fill in the gaps and improve the risk management process of CPS.

4.22 | (G6.RQ2) what lessons learned have been reported?

The following are the reported lessons learned in our 312 studied literature sources. For clarity, we would like to note that some of these lessons were discussed explicitly as a lesson learned after evaluation or experimentation, while others were derived from the preliminaries conducted within the published studies and the authors of the respective papers used them as a basis to propose their work in various risk management processes.

1. There exists a need to focus on developing techniques for risk identification and mitigation.[145]
2. Cyber attacks usually occur through password reset and firewall model dealing with intrusion clearance.[79]
3. Unlike IT systems, CPS(s) have more attack and fault points that make the systems vulnerable to malicious attacks.[30] This calls for a rigorous security risk management process for CPS. The merger of cloud technology for big data storage and efficient service provision over the internet has made software systems security-critical requiring more rigorous risk management processes.[29] Another reason to introduce a more rigorous risk management technique for CPS is having to deal with realtime requirements such as real time availability.[33]
4. One way to reduce the probability of system failure is to use a combination of various risk identification, assessment, mitigation, and management techniques during the different phases of the software development life cycle.[146] This helps to overcome the shortcomings of a certain method. For instance, the use of fault trees alone might not be that useful for dynamic risk identification. Furthermore, the physical behavior of the system should also be considered for a holistic risk assessment of a CPS system.[140] In case of failures, the protection of business assets and cost minimization are the main goals of a risk management process.[58] In terms of specific domains, that is, smart grids, it is learned that the development of a secure smart grid requires the implementation of risk management processes in both the communication networks and in the power infrastructures.[31]

4.23 | (G6.RQ3) what are the trends in the area?

Figure 13 and Table A6 maps the security and dependability attributes against the four risk processes (risk identification, assessment, mitigation, and management). The figure shows that each of the risk management phases had a varying focus on the security requirements; that is, most of

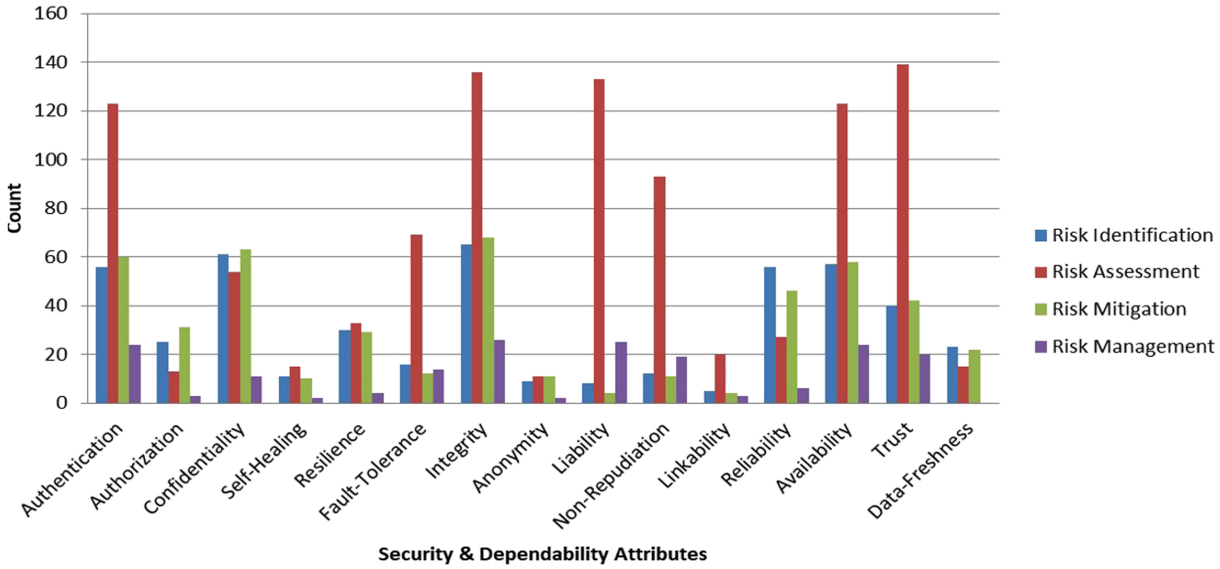

FIGURE 13 Security and dependability attributes covered during various phases of risk management in CPS

the risk identification techniques proposed were for authentication, integrity, availability, and reliability, whereas, in risks assessment, most of the proposed techniques were focused on assessing the severity of risks related to authentication, integrity, non-repudiation, liability, availability, and trust. The techniques proposed for risk mitigation were focused on reducing the risks for authentication, confidentiality, integrity, availability, reliability, and trust, while the techniques proposed for risk management focused on authentication, integrity, liability, non-repudiation, and availability. The conclusion that can be drawn from Figure 13 is that the most research attention was paid to authentication, integrity, availability, and trust which can also be seen in the answer to research question G2.RQ1.

4.24 | (G6.RQ4) what future research directions are being suggested?

The findings of this mapping indicate the following research directions suggested for future research:

1. Security risk identification, assessment, mitigation, or a holistic security risk management technique should be developed. Some of the security concerns that lack attention are self-healing, anonymity, linkability, and data-freshness (also shown in Figure 13).
2. No replication study has been conducted on the techniques proposed and validated in regarding all the phases of risk management. Therefore, replication studies could and should be conducted on the most investigated security requirements types (e.g., integrity) so that the proposed techniques are validated in all the phases of risk management.
3. CPSs other than smart grids should be studied with respect to rising security vulnerabilities to provide domain-specific threats and security solutions. For this, studies conducted on smart grid systems may be replicated on other systems to find the differences.

5 | DISCUSSION

Our mapping study highlighted a very important aspect of the publications growth in recent years. Although a slight decrease is seen in the number of publications in the area during the years 2016–2019, the number of publications so far remains relatively stable of around 30+ papers annually. Our review shows that the annual article count in this domain increased exponentially over the years and thus hints towards the rapid growth in the research efforts in the area. As far as the influence of an article is concerned, some articles have relatively lower citation count either due to being published recently or due to the selected venue for publishing the article being recently introduced.

In our set of selected papers, we found that the majority were published in conferences and these conferences were related to Electrical Engineering. This could possibly suggests a linkage between the electrical engineering filed and the files of cybersecurity systems. Although none of the publications included in our mapping study was explicitly dedicated to this linkage between the two areas, we think that the linkage is logical for the following reasons: (1) industry survey analysts (i.e., CrowsStrike) indicate that 73% of engineering firms reported a security attack related to firms' supply chains, in 2018,[147] and (2) practitioners' voices have been raised that securing electronic devices from malicious attacks is in fact

becoming the responsibility of electrical engineers as they are designing all those pieces of electrical equipment utilized in industrial, business, and household applications.[148] Another important finding in our review is the distribution of the author's affiliations. We found that the USA, UK, Italy, and China were those countries publishing the highest number of articles in this domain, with the USA at the top of the list with 104 articles. This finding means that our knowledge of the risk in CPS is skewed, as the empirical evidence produced by the authors relates to contexts, organizational settings, and cultures specific to these regions. It might well be that empirical research on security risks in CPS might bring different results if the contexts of study are those in India or North Europe. We, therefore, call for more research in the area to achieve generalizable results across contexts. We also notice that several articles in our set were in fact authored by researchers of several countries working together. The majority of these papers are written in partnerships between authors of the US and China. Furthermore, an increase in the number of publications targeting the risks in CPS is observed in developing countries of Asia (i.e., India, Pakistan, and Iran), Eastern Europe (Romania, Poland, and Ukraine), and Africa (i.e., Tunisia). Based on our findings, it can be inferred that many countries in Eastern Europe (Romania, Poland, and Ukraine) and Asia (e.g., India and Iran) are still adopting industrial IoT and maturing their understanding of CPS. However, it is alarming to see not fewer publications some of the well developed countries such as Russia, Australia, Canada, and countries of South America (i.e., Brazil). For Russia and South American countries, we assume that local conferences are publishing scientific output in local languages and thus we could not extract those papers. But for Canada, the language is again not an issue. Since the area is emerging, so most of the authors published in conferences. This shows the promising side of research that novel ideas are proposed by the majority of authors in conferences. On the other hand, it also summons for more empirical evaluation of proposed ideas in multiple domains. It surprised us that journal papers had a higher citation count as compared with international conferences and workshops.

Next, our study revealed that it is hard to pinpoint to a research school or schools generating visibly sizeable publication output on security requirements for CPSs. We found a huge amount of researchers being authors of only one paper; out of 1,260 authors, only 70 authors had more than a single article published in the area. We think that our observation might be traceable to the fact that the authors of papers are active in the technical sub-areas of computer science, and not in the field of Requirement Engineering (RE). In turn, their research focus might go much beyond the immediate subject of security requirements and center on any of the other important aspects of CPS development and operation. As a matter of fact, we found only one paper[149] published at RE events (SREIS and RE). We think that the finding that many researchers outside the area of RE are writing articles on security requirements methods is a positive development, as it indicates that other communities explicitly acknowledge the role of requirements and their implementation in the development of secure CPSs.

In general, most of the techniques proposed or studied in the literature are proactive risk management techniques rather than reactive risk management techniques. In some cases, the techniques, approaches and frameworks proposed for risk management used both proactive and reactive risk management technique to better monitoring and controlling the risks in CPS. Most of the risk identification, assessment, mitigation, and management techniques proposed focused on the risks associated with the security requirements for smart grid stations. This shows that smart grids remained the most discussed application domain and it also calls for attention that other application domains lack research. The reason for this heightened interest in smart grids might be the availability of datasets and previous work on the topic. The case studies selected for evaluation purposes were dependent on the domain focused on the IEEE busses used for evaluation purposes consisted of IEEE 14-, 9-, 68-, 39-, 118-, and 3-bus systems.

Regarding the security attributes identified during this mapping study, we observe a similarity between security requirements deemed important for both the CPS and the better-researched (or "traditional") IT (e.g., in healthcare information systems,[121] in cloud computing applications,[122] or in process-aware information systems[123]). However, we observe a difference is in the application priority of those attributes. For instance, traditional IT systems initially require ensuring confidentiality, integrity, and then the availability of the system, whereas the priorities of these attributes in CPS do vary (e.g., data freshness and availability are the primary concern). However, CPS(s) require implementation of availability, integrity, and then finally confidentiality.[78] Most of the literature covered in our study assigned the highest priority to the implementation of authentication, confidentiality, non-reliability, integrity, availability, and trust-related requirements in the development of a secure and reliable CPS. However, in the years 2017–2020, a gradual increase can be seen in the papers focusing on system resilience, data freshness, and non-repudiation. This opens up avenues for the researchers to explore the rest of the security requirements for variable domains. Below, we discuss some of these avenues.

First, most CPSs include sensitive data and applications that process these data (e.g., pacemakers). Therefore, the techniques proposed risk identification, assessment, mitigation, and management for traditional IT applications (e.g., mobile application) might not be directly applicable to CPS(s) (e.g., pacemakers or drones). Therefore, the assumption that one solution would fit all areas is unrealistic. We need to consider specific risk identification techniques to see which new risks are there for a particular CPS. Similarly, we require a dedicated risk assessment, mitigation, and management solutions for particular CPS applications. It is worth mentioning here that the most investigated type of CPSs in literature so far is smart grid systems, and unfortunately, the risk processes developed for that type of system are not largely generalizable.

Second, this mapping study's results show that risk assessment is the most researched topic for CPS so far. However, the risk assessment process alone is not enough to shield CPSs from security vulnerabilities. It is also observed that most of the risk assessment techniques covered in this review study involve the factor of biasness because the calculated risk value against the identified risk factor is assigned by an individual. It could be calculated based on expert opinion collected from domain experts or by consulting risk taxonomy and literature. This opens up a debate

for practitioners and researchers on the authenticity of the existing assessment methods and on how to design the new methods to overcome this loophole.

Third, we compared the most researched types of security requirements of CPS and those of other systems. For example, in the area of cloud computing,[122] it is reported that access control, integrity, and auditability are the most-studies quality attributes. Our results agree with this review's findings regarding the popularity of integrity as a research topic among scholars. However, in contrast to these authors,[122] we found that reliability and availability were among the top 3 most investigated security requirements among CPS researchers. We think that this observation could be traceable to the priorities that these types of security requirements take as already indicated earlier in our discussion. To know this for sure, more empirical research on security requirements prioritization is needed in real-world contexts.

Our mapping study suggests that model-based techniques have been the most used techniques for the defined risk processes in CPSs. We think this is not surprising given the fact that the CPSs are a domain for which numerous formal methods and models have been developed and employed in the past decades. CPSs are mission-critical systems and benefit from the application of models and model-proving technologies.

Furthermore, we note that the severity value of risk is dependent on the quality of the implementation of the security requirements. Plus, we acknowledge the fact that most of these risks are dependent on the nature of the system. Lack of attention to any of the system's security requirements leaves an open access point for the attacks; for example, cyber security risks are open doors for hackers to exploit vulnerabilities of the system. A recorded example of the impact of these risks is that unauthorized access and control of the power grid station's functionality led to a cascading failure which eventually led to a blackout in most of the areas covered by the power plant.[34] Any malicious code or a false data injection into the system may lead to the execution of incorrect operation or abnormal behavior of the system. In the worst case scenario, the lack of assessment and mitigation of such a risk can lead to catastrophe or casualties.

Regarding the level of evaluation of the proposed methods and techniques, we observed that around 41% of papers did not even discuss validity issues. The rest lack well-defined evaluation mechanisms for the proposed work. This indicates incompleteness in our knowledge of the applicability of the published proposals to practical contexts. We found that among those papers that evaluated their proposed approaches, most used simulation for evaluation purposes. The reason for this, we think, is the nature of CPS that involves hardware and software both and that simulation replicates the real scenario while being in a controlled environment. We also found that testbeds used on the other hand allowed rigorous testing of the proposed technique and were used where no particular case in an application domain was available.

6 | THREATS TO VALIDITY

The validity assessment conducted throughout this mapping study can be divided into the following categories based on the various phases of mapping study[14]; see Table 6. Essentially, it indicates the strategies that we employed in order to counter the validity threats specific for each phase.

7 | RECOMMENDATIONS FOR A RESEARCH AGENDA

This mapping study consolidated the current state of knowledge on security risks for CPS as per scientific publications in the period of 2000–2020. Our findings allow us to derive some themes that we think are worthwhile to consider for inclusion in an agenda for future research. These are as follows.

1. *Theory-building*. We reviewed 312 papers, and we found an increase in the research community's scientific output in the resent years. This lets us think that the field might well be now ready to move towards more systematic theory building.[150] As research methodologists argue,[151,152] theory-building would pave the way to improve the consistency in the use of the security and dependability attributes when proposing approaches to managing security risk in CPSs and when comparing new proposals to already published approaches.
2. *Empirical research towards improving generalizability*. Our findings indicated that less than 60% of our included papers provided an evaluation and validation process of newly proposed approaches (Section 4.9). This suggests that we know relatively little about the contexts to which the proposed security risk methods are suitable. More research is therefore needed to understand those contexts to which certain methods are idea or at least more useful than others. As already mentioned in the Section 5, we think that not all proposed methods would work equally well in all contexts and that based on context certain method might be more usable than others. Section 4.9 also indicates that case study research has been employed by security risk researchers. While this means the application of a proposed method is more realistic, it also means that replications are needed to understand the contextual settings that help or hurt a method's use. Only then, we could have generalizable knowledge on which method to use in which context.
3. *Exploring theories from other fields for use in security risk approaches in CPSs*. Our findings in Figures 2, 3 and 5 indicate cases in which risk mitigation approaches for CPS were developed while leveraging theories and theoretical concepts from other fields (e.g., game theory and

TABLE 6 Validity threats countered

Type of validity	Phases of study	Sub-categories	Strategies
Construction, Internal	Planning Phase	Setting of systematic mapping	A protocol was established and followed while conducting this study. The protocol consisted of defining the venues, digital libraries, search strings, time-span, standard language, search application criteria, search items, inclusion and exclusion criteria, eliminating the possible threats to repeatability and replicability of the study.
Construction, Internal		Search items	All results and decisions are checked and rechecked for inconsistencies. Additional terms i.e. synonyms to the original key words were used to identify related studies from the digital libraries targeted.
Construction, Internal		Standard languages and terminologies	External evaluation is used to eliminate the threat related to the lack of standard languages and terminologies in this study
Construction, Internal		Search method	A combination of both automatic and manual search methods is used to identify possible set of related studies. Parsing through the full text of the articles left us with only the most relevant set of related studies to be used in this mapping study
Construction		Venues and databases	Queries were executed on multiple databases providing access to the targeted search items to collect the required set of studies to be included in this mapping study
Construction		Exclusion and inclusion criteria	A search strategy was established defining the search items to be used in this study. Upon collecting the initial set of related studies, full-text of each article was parsed to obtain only the most relevant articles
Construction		Research questions	Discussion meeting was conducted with the team members and experts of this research domain
Interval		Article count	Multiple electronic databases were accessed to obtain the relevant articles in the domain studied. Snowballing was conducted to avoid missing any relevant articles
Construction, External		Restricted time span	A protocol was formed and followed to identify and extract data from the relevant papers
Internal, Conclusion	Conducting Phase	Study selection	The inclusion and exclusion criteria used for study selection allow us to extract only the most relevant papers eliminating any redundancy or inclusion of incomplete data or data that has not been reviewed
Construction, Internal, Conclusion		Identification of related studies	A protocol was formed and followed to identify and extract data from the relevant papers
Interval, Conclusion		Duplication of related studies	Any duplicated study identified was reported only once in this mapping study
Interval, Conclusion		Classification of related studies	Opinions from experts in this domain were incorporated to classify the studied articles with respect to the risk management process discussed
Interval		Inclusion of publications	A standard review protocol and multi-step selection process was applied to extract articles relevant to this mapping study
External		Accessibility of papers/databases	The authors were contacted to obtain the paper required for this study
Internal, Conclusion		Data extraction	A protocol formed during the planning phase has been used to extract the data from the studies selected for inclusion in this mapping study
Interval		Data synthesis	External evaluations have been used to avoid unsatisfactory data synthesis
External	Reporting Phase	Generalizability of related study	Guidelines[59] were used to conduct this mapping studies to avoid the threats related to the repeatability and replication of this mapping study

operation research). Applying theories from other disciplines in the field of RE has been a well-recognized research trend (see, e.g., the D4RE workshop as part of the annual RE conference, http://d4re.iese.fraunhofer.de/). We therefore think that security risk researchers should expand upon the existing method proposals conceived as a result of collaborations across disciplines. More exploration into using theories from other disciplines would enrich the spectrum of proposed security risk methods and creating a body of knowledge of the synergies between other fields and security requirements engineering for CPSs.

4. *Research on data-freshness, self-healing, resilience, likability, and anonymity*. Our finding on the security and dependability attributes covered in the process of managing risk in CPS (Figure 13) indicate that some attributes are well researched while others are under-researched—in particular data-freshness, self-healing, resilience, likability, and anonymity. These attributes form classes of non-functional requirements for which more research is needed in the context of CPS.

5. *Comparative research of newly proposed methods and model-based methods*. Our mapping study found that model-based methods are the most investigated approaches in the context of CPS. This suggests that if a newly proposed method is designed, it might be a good idea to compare the new proposal's performance with the performance of a model-driven technique that is well-known in the community of security risk researchers. Such benchmarking studies could possibly help understand the strong and weak points of new proposals in regard to methods that have already been proven to work well in realistic contexts. We think the empirical work on this forms an important line of research for the future as it would add up new knowledge to the existing body of empirical knowledge on model-based security risk methods.

8 | CONCLUSION

This systematic mapping study provides a structured understanding of the state of the art techniques, methods, and frameworks proposed in the area of risk identification, assessment, mitigation, and management of the security requirements in IoT/CPSs. During this mapping study, we identified, classified, and analyzed literature published until March 2020. The most important findings of this review are summarized below (following the goals G1–G6 as shown in Table 1):

1. In the selected 312 papers, we found that the sub-area of risk assessment was the one for which the most techniques were proposed (G1). This sub-area is followed by risk identification and risk mitigation. The least number of techniques were proposed for risk management. We also found that model-based techniques dominated the list of solutions for risk assessment (Figure 3), risk identification (Figure 2), and risk mitigation (Figure 4). The prominent role of models might be a sign to suggest that if security requirements engineering is to make an impact on CPS, it should be grounded on the model-based paradigm.
2. In the selected 312 papers, a total of 8 security requirements and 7 dependability related requirements were treated (G2). However, the most frequently researched security requirements are integrity, authentication, confidentiality, and the most frequently researched dependability attributes are availability, reliability, and trust. We conclude that more research is needed regarding anonymity, non-repudiation, and data freshness, in terms of security requirements and linkability, liability, and fault tolerance, in terms of dependability attributes liked to these security attributes.
3. Regarding the risks addressed in our 312 studies, we found the most common risk was cyber security (G3). This is unsurprising given the mission-critical nature of CPS.
4. In terms of empirical evaluation, we found that simulation techniques (Figure 8) are the most preferred evaluation method. These techniques most often employ probabilistic reasoning as their foundation (Figure 9). Regarding application domains (G4), the most studied domain is smart grids. The second most studied type of CPSs is in the domain of chemical control. We found in total 25 application areas; however, many of those have been addressed in a few papers only. Due to recent efforts in industrial automation, a gradual increase in the number of publications is found to have presented their studies in robotics.
5. Regarding the demographics of our 312 included studies (G5), we found that it is hard to pinpoint few well-known venues publishing most of the scientific output. Instead, we found a huge number of authors, research schools, and publication destinations that served as the outlet of the studies. In terms of citations, however, the Journal of Computer Networks seems to be the venue with the highest cited venue.
6. Regarding the limitations of the proposed techniques and the collective lessons learned from the community of authors of the studied 312 papers (G6), our most important conclusions are these two: first, our current knowledge of risk and security requirements mostly comes from the application domain of smart grids, which poses generalizability questions regarding the applicability of this knowledge in other area. It might well be the case that the proposed techniques for smart grid systems might need some modifications or extensions to make them work for other types of CPSs; second, our systematic mapping study supports the understanding that risk is security requirements for CPSs should best be approached by applying not one technique, but multiple techniques, so that the risks are reasoned about by taking various perspectives and also making different assumptions. Only then, it would be possible to develop a complete understanding of the requirements and the involved risks while developing a particular CPS.

Our work has some implications for research and practice. From research perspective, our mapping study indicates that scholars in risk and security requirements of CPS brought interesting theoretical results, but the research output seems far from responding to specific practical challenges of the application domains in which specific CPS are part of. The lack of empirical evaluation efforts concerning nearly 43% of the proposals signals that our knowledge of the suitability of the respective proposals to context is skewed. To achieve more realism in the proposed frameworks and approaches, more case study research in real-world organizations and industrial contexts would be instrumental. Furthermore, scholars should expand their research to cover those under-researched aspects indicated in the previous paragraphs.

From practical standpoint, our review allows practitioners in CPS delivery projects to clearly see those types of risk identification, assessment, mitigation, and management techniques that could possibly be considered as candidates for adoption, dependent on the type of CPS to be developed. For instance, the safety-critical systems such as the avionics system, autonomous vehicles, or pace makers according to the standards can

use either fault trees or event trees for risk assessment due to their proven accuracy for such systems. However, other types of systems can use any of those techniques based on the resources available; for example, small-scale projects can use model-based techniques since they are easier to use, are quicker, and in some cases are also accurate. Second, regarding the mitigation measures, although in most cases the practitioners do implement encryption schemes, they should also consider incorporating coding standards making their developed software systems more secure. As far as the large organizations and other critical infrastructure are concerned, the best way to ensure confidentiality and authenticity of their data while maintaining client's trust in them is to implement a set of controls outside the software system's environment as well, that is, limited access to confidential data, implementation of protocol for data-transmission among employees, and other physical security measures.

9 | OUR FUTURE WORK

According to our study, one of the main reasons for a possible cyber-attack risk in CPS is the presence of software bugs or loop holes in the software system allowing unauthorized access to the system for exploitation. This can be a result of either the mismanagement at software architectural level in CPS or the existence of bad code smells in the implemented code of CPS. The mismanagement of software architectural components of CPS is mainly due to integration of third party software component's code to the original CPS code or due to software project forking, without having to record these changes at the architectural level of the original CPS. These kinds of changes to the implemented CPS can also result in bad code smells deteriorating its performance and even making the system vulnerable. Based on this, our next goal will be to explore the impact software forking, presence of code smells, and software architecture erosion can have on the reliability, security, and safety of CPS.

ORCID

Irum Inayat https://orcid.org/0000-0001-5576-6212
Maya Daneva https://orcid.org/0000-0001-7359-8013

REFERENCES

1. Weinmann O, "Internet of things," *Bosch ConnectedWorl d Blog*, 2018. [Online]. Available: https://blog.bosch-si.com/internetofthings.
2. Li S, Da Xu L, Zhao S. The internet of things: a survey. *Inf Syst Front*. 2015;17(2):243-259.
3. Lee EA, "Cyber physical systems: design challenges," in 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), 2008, pp. 363-369.
4. Carruthers K. Internet of things and beyond: cyber-physical systems. *IEEE Newsl*. 2016;(May 2016):2016-2018.
5. Zahid M, Inayat I, Daneva M, Mehmood Z. A security risk mitigation framework for cyber physical systems. *J Softw Evol Process*vol. Special Is, no. February, pp. 2020;1-15.
6. Biro M, Mashkoor A, Sametinger J, Seker R. Software safety and security risk mitigation in cyber-physical systems. *IEEE Softw*. 2017;35(1):24-29.
7. Mashkoor A, Biró M, Messnarz R, Colomo-Palacios R. Selected functional safety and cybersecurity concerns in system, software, and service process improvement and innovation. *J. Softw. Evol. Process*. 2018;30(5):3-5.
8. Mashkoor A, Sametinger J, Biro M, Egyed A. Security- and safety-critical cyber-physical systems. *J Softw Evol Process*. 2020;32(2):1-2.
9. Fovino IN and Masera M, "Emergent disservices in interdependent systems and system-of-systems," in Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics, 2007, vol. 1, pp. 590-595.
10. Best J, Wake up baby: man HACKS into 10-month-old's baby monitor to watch sleeping infant, *Mirror Online*, Apr 2014.
11. Daine K, Hawton K, Singaravelu V, Stewart A, Simkin S, Montgomery P. The Power of the Web: A Systematic Review of Studies of the Influence of the Internet on Self-Harm and Suicide in Young People. *PLoS One*. 2013;8(10):e77555. https://doi.org/10.1371/journal.pone.0077555
12. Badri A, Boudreau-Trudel B, Souissi AS. Occupational health and safety in the industry 4.0 era: a cause for major concern? *Saf Sci*. 2018;109(May):403-411.
13. Petersen K, Feldt R, Mujtaba S, and Mattsson M, "Systematic mapping studies in software engineering," 12Th Int. Conf Eval Assess Softw Eng, vol. 17, p. 10, 2008.
14. Petersen K, Vakkalanka S, Kuzniarz L. Guidelines for conducting systematic mapping studies in software engineering: an update. *Inf Softw Technol*. 2015;64:1-18.
15. Ralston PAS, Graham JH, Hieb JL. Cyber security risk assessment for SCADA and DCS networks. *ISA Trans*. 2007;46(4):583-594.
16. Cherdantseva Y et al. A review of cyber security risk assessment methods for SCADA systems. *Comput Secur*. 2015;56:1-27.
17. Knowles W, Prince D, Hutchison D, Disso JFP, Jones K. A survey of cyber security management in industrial control systems. *Int J Crit Infrastruct Prot*. 2015;9:52-80.
18. Hong JB, Nhlabatsi A, Kim DS, Hussein A, Fetais N, Khan KM. Systematic identification of threats in the cloud: a survey. *Comput Networks*. 2019;150:46-69.
19. Humayun M, Niazi M, Jhanjhi N, Alshayeb M, Mahmood S. Cyber security threats and vulnerabilities: a systematic mapping study. *Arab J Sci Eng*. 2020;45:3171-3189.
20. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. *Comput Networks*. 2015;76:146-164.
21. Walker-Roberts S, Hammoudeh M, Aldabbas O, Aydin M, Dehghantanha A. Threats on the horizon: understanding security threats in the era of cyber-physical systems. *J Supercomput*. 2020;76(4):2643-2664.
22. Mitchell R, Chen I-R. A survey of intrusion detection in wireless network applications. *Comput Commun*. 2014;42:1-23.

23. Yan Z, Zhang P, Vasilakos AV. A survey on trust management for Internet of Things. *J Netw Comput Appl*. 2014;42:120-134.
24. Manshaei MH, Zhu Q, Alpcan T, Bacşar T, Hubaux J-P. Game theory meets network security and privacy. *ACM Comput Surv*. 2013;45(3):1-39.
25. Cheminod M, Durante L, Valenzano A. Review of security issues in industrial networks. *IEEE Trans Ind Informatics*. 2013;9(1):277-293.
26. Nicholson A, Webber S, Dyer S, Patel T, Janicke H. SCADA security in the light of cyber-warfare. *Comput Secur*. 2012;31(4):418-436.
27. Ray PD, Harnoor R, and Hentea M, "Smart power grid security: a unified risk management approach," in 44th Annual 2010 IEEE International Carnahan Conference on Security Technology, 2010, pp. 276-285.
28. Fan X, Fan K, Wang Y, and Zhou R, "Overview of cyber-security of industrial control system," in 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications, SSIC 2015 - Proceedings, 2015.
29. Damenu TK and Balakrishna C, "Cloud security risk management: a critical review," in Next Generation Mobile Applications, Services and Technologies, 2015 9th International Conference on, 2015, pp. 370-375.
30. Peng Y, Lu T, Liu J, Gao Y, Guo X, and Xie F, "Cyber-physical system risk assessment," in 9th International Conference Proceedings on Intelligent Information Hiding and Multimedia Signal, 2013, pp. 442-447.
31. Wang W, Lu Z. Cyber security in the Smart Grid: survey and challenges. *Comput. Networks*. 2013;57(5):1344-1371.
32. Shafi Q, "Cyber physical systems security: a brief survey," in 2012 12th International Conference on Computational Science and Its Applications, 2012, pp. 146-150.
33. Cárenas AA, Amin S, Sinopoli B, Giani A, Perrig A, Sastry S. Challenges for securing cyber physical systems. In: *Workshop on future directions in cyber-physical systems security*; 2009.
34. Humayed A, Lin J, Li F, Luo B. Cyber-physical systems security—a survey. *IEEE Internet Things J*. 2017;4(6):1802-1831.
35. Anne Tøndel I, Foros J, Skaufel Kilskar S, Hokstad P, Gilje Jaatun M. Interdependencies and Reliability in the Combined ICT and Power System: an overview of current research. *Appl Comput Informatics*. 2018;14(1):17-27.
36. Wu G, Sun J, Chen J. A survey on the security of cyber-physical systems. *Control Theory Technol*. 2016;14(1):2-10.
37. Nagaraju V, Fiondella L, and Wandji T, "A survey of fault and attack tree modeling and analysis for cyber risk management," in 2017 IEEE International Symposium on Technologies for Homeland Security (HST), 2017, pp. 1-6.
38. Nazir S, Patel S, Patel D. Assessing and augmenting SCADA cyber security—a survey of techniques. *Comput Secur*. 2017;70(September 2017):436-454.
39. Hashemi-Dezaki H, Agah SMM, Askarian-Abyaneh H, Haeri-Khiavi H. Sensitivity analysis of smart grids reliability due to indirect cyber-power interdependencies under various DG technologies, DG penetrations, and operation times. *Energ Conver Manage*. 2016;108:377-391.
40. Lin K and Holbert KE, "PRA for vulnerability assessment of power system infrastructure security," *Proc. 37th Annu. North Am. Power Symp*. 2005, vol. 2005, pp. 43-51.
41. I. S. T. Institute, "What is software risk and software risk management?," *International Software Test Institute*, 2018. [Online]. Available: https://www.test-institute.org/What_Is_Software_Risk_And_Software_Risk_Management.php
42. Gawand HL, Bhattacharjee AK, Roy K. Securing a cyber physical system in nuclear power plants using least square approximation and computational geometric approach. *Nucl Eng Technol*. 2016;49(3):484-494.
43. Green B, Krotofil M, and Hutchison D, "Achieving ICS resilience and security through granular data flow management," 2016.
44. Jillepalli AA, Sheldon FT, De Leon DC, Haney M, and Abercrombie RK, "Security management of cyber physical control systems using NIST SP 800-82r2," in *International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2017, pp. 1864-1870.
45. Zahid M, Inayat I, and Allah Bukhsh F, "Towards mitigating security risks in cyber physical system," in *Euromicro Conference on Software Engineering and Applications*, 2018, pp. 6-7.
46. Omerovic A, Vefsnmo H, Erdogan G, and Gjerde O, "A feasibility study of a method for identification and modelling of cybersecurity risks in the context of smart power grids," in 4th International Conference on Complexity, Future Information Systems and Risk (COMPLEXIS 2019), 2019, no. Complexis, pp 39-51.
47. Saripalli P and Walters B, "QUIRC: a quantitative impact and risk assessment framework for cloud security," in 2010 IEEE 3rd International Conference on Cloud Computing, 2010, pp. 280-288.
48. Dondossola G, Terruggia R. Cyber security of smart grid communications: risk analysis and experimental testing. *Cyber Physical Systems Approach to Smart Electric Power Grid*. 2015;33-40.
49. Hartmann K and Steup C, "The vulnerability of UAVs to cyber attacks—an approach to the risk assessment," in *Cyber Conflict (CyCon), 2013 5th International Conference on*, 2013, pp. 1-23.
50. Boddy A, Hurst W, Mackay M, and El Rhalibi A, "A study into detecting anomalous behaviours within healthcare infrastructures," in *Proceedings - 2016 9th International Conference on Developments in eSystems Engineering*, DeSE *2016*, 2017, pp. 111-117.
51. Kong H-K, Kim T-S, and Hong M-K, "A security risk assessment framework for smart car," 2016 10th Int. Conf. Innov. Mob. Internet Serv. Ubiquitous Comput., pp. 102-108, 2016.
52. Faughnan MS et al., "Risk analysis of Unmanned Aerial Vehicle hijacking and methods of its detection," in Systems and Information Engineering Design Symposium (SIEDS), 2013 IEEE, 2013, pp. 145-150.
53. Ramasamy RP, Praveen Kumar M, Sarath Kumar S, Raman RR. Avoidance of fire accident on running train using ZigBee wireless sensor network. *Int J Inf Comput Technol*. 2013;3(6):583-592.
54. Sun CC, Hahn A, Liu CC. Cyber security of a power grid: state-of-the-art. *Electr Power Energy Syst*. 2018;99(November 2017):45-56.
55. Hunter D, Parry J, Radke K, and Fidge C, "Authenticated encryption for time-sensitive critical infrastructure," in ACM Proceedings of the Australasian Computer Science Week Multiconference, 2017, p. 19.
56. Wadhwa N, Hussain SZ, Rizvi SAM. A combined method for confidentiality, integrity, availability and authentication (CMCIAA). *World Congress on Engineering*. 2013;II:6-9.
57. Gu A, Yin Z, Cui C, Li Y. Integrated functional safety and security diagnosis mechanism of CPS based on blockchain. *IEEE Access*. 2020;8:15241-15255.
58. Polemi N and Papastergiou S, "Current efforts in ports and supply chains risk assessment," in 2015 10th International Conference for Internet Technology and Secured Transactions, ICITST, 2015, 2015, pp. 349-354.
59. van Solingen R, Basili V, Caldiera G, Rombach HD. Goal Question Metric (GQM) approach. *Encycl Softw Eng*. 2002;2:1-10.

60. Walker-Roberts S, Hammoudeh M, Aldabbas O, Aydin M, Dehghantanha A. Threats on the horizon: understanding security threats in the era of cyber-physical systems. *J Supercomput*. 2019;76:2643-2664.
61. Zhou X, Jin Y, Zhang H, Li S, and Huang X, "A map of threats to validity of systematic literature reviews in software engineering," Proc - Asia-Pacific Softw Eng Conf APSEC, pp. 153-160, 2017.
62. Oveisi S, Ali M, Nadjafi M, Moeini A. Computer & robotics: a new approach to promote safety in the software life cycle. *J Comput Robot*. 2019;12(1): 77-91.
63. You B, Zhang Y, and Cheng L-C, "Review on cybersecurity risk assessment and evaluation and their approaches on maritime transportation," 30th Annu. Conf. Int. Chinese Transp. Prof. Assoc., no. October, p. 18, 2017.
64. Tsigkanos C, Pasquale L, Ghezzi C, Nuseibeh B. Ariadne: topology aware adaptive security for cyber-physical systems. *Proc - Int Conf Softw Eng*. 2015;2:729-732.
65. Wu W, Kang R, and Li Z, "Risk assessment method for cybersecurity of cyber-physical systems based on inter-dependency of vulnerabilities," in IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), 2015, pp. 1618-1622.
66. Xu Z and Zhu Q, "A cyber-physical game framework for secure and resilient multi-agent autonomous systems," in *Proceedings of the IEEE Conference on Decision and Control*, 2011, vol. 2016-Febru, no. Cdc, pp. 5156-5161.
67. Kaster P and Sen PK, "Cyber security and rural electric power systems," in 2015 IEEE Rural Electric Power Conference, 2015, pp. 49-54.
68. Jaiswal S and Gupta D, "Security requirements for internet of things (IOT)," in Proceedings of the 6th International Conference on Communication Systems and Networks, 2014, pp. 419-427.
69. Fletcher KK and Liu X, "Security requirements analysis, specification, prioritization and policy development in cyber-physical systems," in 2011 5th International Conference on Secure Software Integration and Reliability Improvement – Companion, SSIRI-C 2011, 2011, pp. 106-113.
70. Habash RWY, Groza V, Krewski D, and Paoli G, "A risk assessment framework for the smart grid," in Proceedings- IEEE Electrical Power & Energy Conference (EPEC), 2013.
71. Chittester CG, Haimes YY. Risks of terrorism to information technology and to critical interdependent infrastructures. *J Homel Secur Emerg Manag*. 2004;1(4):1-20.
72. Havens TC, Anderson DT, Stone K, Becker J, Pinar AJ. Recent advances in computational intelligence in defense and security. *Stud Comput Intell*. 2016;621:13-44.
73. Lopez AB, Vatanparvar K, Deb Nath AP, Yang S, Bhunia S, Al Faruque MA. A security perspective on battery systems of the internet of things. *J Hardw Syst Secur*. 2017;1(2):188-199.
74. Rahman MA, Jakaria AHM, and Al-Shaer E, "Formal analysis for dependable supervisory control and data acquisition in smart grids," in 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2016, pp. 263-274.
75. Haimes Y, Kaplan S, Lambert JH. Risk filtering, ranking, and management framewerk using hierarchical holographie modeling. *Risk Anal an Int J*. 2002; 22(2):383-397.
76. Aven T. A unified framework for risk and vulnerability analysis covering both safety and security. *Reliab Eng Syst Saf*. 2007;92(6):745-754.
77. Chen D, Meinke K, Ostberg K, Asplund F, and Baumann C, "A knowledge-in-the-loop approach to integrated safety & security for cooperative system-of-systems," in 2015 *IEEE 7th International Conference on Intelligent Computing and Information Systems*, ICICIS *2015*, 2016, pp. 13-20.
78. Zhang Q, Zhou C, Xiong N, Qin Y, Li X, Huang S. Multi-model based incident prediction and risk assessment in dynamic cybersecurity protection for industrial control systems. *IEEE Trans Syst Man, Cybern Syst*. 2015;1-16.
79. Wang P, Ashok A, and Govindarasu M, "Cyber-physical risk assessment for smart grid system protection scheme," in *IEEE Power and Energy Society General Meeting*, 2015, pp. 1-4.
80. Stjohn-Green M, Piggin R, Mcdermid JA, and Oates R, "Combined security and safety risk assessment—what needs to be done for ics and the IoT," 10th Int. Conf. Syst. Saf. Cyber Secur. Conf., 2015.
81. Chan ACF, Zhou J. On smart grid cybersecurity standardization: issues of designing with NISTIR 7628. *IEEE Commun Mag*. 2013;51(1):58-65.
82. Settanni G, Shovgenya Y, Skopik F, Graf R, Wurzenberger M, and Fiedler R, "Acquiring cyber threat intelligence through security information correlation," in Proceedings - 3rd International Conference on Cybernetics (CYBCONF), 2017, pp. 1-7.
83. Zhao T, Wang D, Lu D, Zeng Y, and Liu Y, "A risk assessment method for cascading failure caused by Electric Cyber-Physical System (ECPS)," in Proceedings-5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies, 2015, pp. 5-9.
84. He X, Sui Z, and De Meer H, "Game-theoretic risk assessment in communication networks," in 16th IEEE International Conference on Environment and Electrical Engineering (EEEIC), 2016, pp. 0-5.
85. Law YW, Alpcan T, and Palaniswami M, "Security games for voltage control in smart grid," in 2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton), 2012, pp. 212-219.
86. Wei L, Moghadasi AH, Sundararajan A, and Sarwat AI, "Defending mechanisms for protecting power systems against intelligent attacks," 2015 10th Syst. Syst Eng Conf SoSE 2015, pp. 12-17, 2015.
87. Jauhar S, Chen B, Temple WG, Dong X, Kalbarczyk Z, Sanders WH, Nicol DM. "Model-based cybersecurity assessment with NESCOR smart grid failure scenarios," in Proceedings - 2015 IEEE 21st Pacific Rim International Symposium on Dependable Computing, PRDC 2015, 2016, pp. 319-324.
88. McDonald J, Oualha N, Puccetti A, Hecker A, and Planchon F, "Application of EBIOS for the risk assessment of ICT use in electrical distribution substations," in 2013 IEEE Grenoble Conference PowerTech, POWERTECH 2013, 2013.
89. Rierson L. *Developing Safety-Critical Software: A Practical Guide for Aviation Software and DO-178C Compliance*. 1sted. CRC Press; 2013.
90. Speer J and Rish T, Management for medical devices: the definitive guide management for medical devices: the definitive guide. 2016.
91. Di Marco D, Hird J, Manzo A, and Ivaldi M, "Security testing with controller-pilot data link communications," in Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016, 2016, pp. 526-531.
92. Markantonakis K and Mayes K, "SCADA system cyber security," in *Secure Smart Embedded Devices, Platforms and Applications*, Springer, New York, NY, 2013, pp. 451-471.
93. Ashok A and Govindarasu M, "Cyber-physical risk modeling and mitigation for the smart grid using a game-theoretic approach," in 2015 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference, ISGT 2015, 2015, vol. 2015-Janua.
94. Bouij-Pasquier I, Ouahman AA, El Kalam AA, and De Montfort MO, "SmartOrBAC security and privacy in the Internet of Things," Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. AICCSA, vol. 2016-July, 2016.

95. Abie H and Balasingham I, "Risk-based adaptive security for smart IoT in eHealth," in *Proceedings of the 7th International Conference on Body Area Networks*, 2012, no. SeTTIT, pp. 269-275.
96. Waidner M and Kasper M, "Security in Industrie 4. 0—challenges and solutions for the fourth industrial revolution," pp. 1303-1308, 2016.
97. Sindre G, Opdahl AL. Eliciting security requirements with misuse cases. *Requir Eng*. 2005;10(1):34-44.
98. Axelrod CW, "Reducing software assurance risks for security-critical and safety-critical systems," 2014 IEEE Long Isl. Syst Appl Technol Conf LISAT 2014, 2014.
99. Chiprianov V, Gallon L, Salameh K, Munier M, and El Hachem J, "Towards security software engineering the smart grid as a system of systems," in 10th System of Systems Engineering Conference (Se, 2015, pp. 77-82.
100. Banerjee A, Venkatasubramanian KK, Mukherjee T, Gupta SKS. Ensuring safety, security, and sustainability of mission-critical cyber-physical systems. *Proc IEEE*. 2012;100(1):283-299.
101. Ericsson GN. Cyber security and power system communication-essential parts of a smart grid infrastructure. *IEEE Trans. Power Deliv*. 2010;25(3):1501-1507.
102. Oh S-R and Kim Y-G, "Security requirements analysis for the IoT," in 2017 International Conference on Platform Technology and Service (PlatCon), 2017, pp. 1-6.
103. Axelrod CW, "Managing the risks of cyber-physical systems," in 2013 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2013, pp. 1-6.
104. Ali S, Al Balushi T, Nadir Z, Hussain OK. Embedded systems security for cyber-physical systems. *Stud Comput Intell*. 2018;768:115-140.
105. Aissani N, Guetarni IHM. *From Centralized Modelling to Distributed Design in Risk Assessment and Industrial Safety- Survey and Proposition*. Serv. Oriented Holonic Multi-agent Manuf; 2015.
106. Ericsson GN. Information security for electric power utilities (EPUs)—CIGRÉ developments on frameworks, risk assessment, and technology. *IEEE Trans Power Deliv*. 2009;24(3):1174-1181.
107. Zahid M, Inayat I, Mashkoor A, and Mehmood Z, "Security risk mitigation of cyber physical systems: a case study of a flight simulator maryam," in International Conference on Database and Expert Systems Applications, 2019, pp. 129-138.
108. Garcia HE, Aumeier SE, Al-Rashdan AY, Rolston BL. Secure embedded intelligence in nuclear systems: Framework and methods. *Ann Nucl Energy*. 2020;140:107261.
109. Xiang Y, Wang L, Liu N, Xiao R, and Xie K, "A resilient power system operation strategy considering presumned attacks," in International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), 2016, pp. 3-8.
110. Carelli A, Vallero A, Di Carlo S. Performance monitor counters: Interplay between safety and security in complex cyber-physical systems. *IEEE Trans Device Mater Reliab*. 2019;19(1):73-82.
111. Jillepalli AA et al., "METICS: a holistic cyber physical system model for IEEE 14-bus power system security," in 13th International Conference on Malicious and Unwanted Software: "Know Your Enemy" (MALWARE), 2018, pp. 95-102.
112. Patel SC, Graham JH, Ralston PAS. Quantitatively assessing the vulnerability of critical information systems: a new method for evaluating security enhancements. *Int J Inf Manage*. 2008;28(6):483-491.
113. Grechanik M, McKinley KS, and Perry DE, "Recovering and using use-case-diagram-to-source-code traceability links," Proc. 6th Jt. Meet. Eur. Softw. Eng. Conf. ACM SIGSOFT Symp. Found. Softw. Eng. - ESEC-FSE'07, p. 95, 2007.
114. Wang Y, Xu Z, Zhang J, Xu L, Wang H, and Gu G, "SRID: state relation based intrusion detection for false data injection attacks in SCADA," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 8713 LNCS, no. PART 2, pp. 401-418, 2014.
115. Beckers K et al. A structured hazard analysis and risk assessment method for automotive systems—a descriptive study. *Reliab Eng Syst Saf*. 2016;158:185-195.
116. Langer L, Smith P, and Hutle M, "Smart grid cybersecurity risk assessment experiences with the SGIS toolbox," in International Symposium on Smart Electric Distribution Systems and Technologies (EDST), 2015, pp. 475-482.
117. Zonouz S, Haghani P. Cyber-physical security metric inference in smart grid critical infrastructures based on system administrators' responsive behavior. *Comput Secur*. 2013;39(PART B):190-200.
118. Friedberg I, McLaughlin K, Smith P, Laverty D, Sezer S. STPA-SafeSec: safety and security analysis for cyber-physical systems. *J Inf Secur Appl*. 2016;1-16.
119. Waedt K, Ciriello A, Parekh M, and Bajramovic E, "Automatic assets identification for Smart Cities: Prerequisites for cybersecurity risk assessments," in *IEEE 2nd International Smart Cities Conference: Improving the Citizens Quality of Life, ISC2* 2016 - *Proceedings*, 2016.
120. Motii A et al., "Guiding the selection of security patterns based on security requirements and pattern classification," in ACM The 20th European Conference on Pattern Languages of Programs, EuroPLoP 2015, 2015, vol. 0, no. 0, p. 10.
121. Fan Y, Li J, Zhang D, Pi J, Song J, Zhao G. Supporting sustainable maintenance of substations under cyber-threats: an evaluation method of cybersecurity risk for power CPS. *Sustainability*. 2019;11:1-30.
122. Jurgen D, Schmittner C, Krisper M, and Macher G, "Towards integrated quantitative security and safety risk assessment," in International Conference on Computer Safety, Reliability, and Security, 2019, vol. 1, pp. 102-116.
123. Min B and Varadharajan V, "Design and analysis of security attacks against critical smart grid infrastructures," in *Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems, ICECCS*, 2014, pp. 59-68.
124. Xiang Y, Wang L, Liu N. Coordinated attacks on electric power systems in a cyber-physical environment. *Electr Pow Syst Res*. 2017;149:156-168.
125. Ashok A, Govindarasu M, Wang J. Cyber–physical attack-resilient wide-area monitoring, protection, and control for the power grid. *Proc IEEE*. 2017;105(7):1389-1407.
126. Liu X, Shahidehpour M, Cao Y, Wu L, Wei W, Liu X. Microgrid risk analysis considering the impact of cyber attacks on solar PV and ESS control systems. *IEEE Trans Smart Grid*. 2017;8(3):1330-1339.
127. Ji X, Yu H, Fan G, and Fu W, "Attack-defense trees based cyber security analysis for CPSs," in 2016 *IEEE/ACIS 17th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, SNPD 2016, 2016, pp. 693-698.
128. Xiang Y, Wang L, Liu N. A robustness-oriented power grid operation strategy considering attacks. *IEEE Trans Smart Grid*. 2017;3053(c):1-1.
129. Orojloo H, Azgomi MA. A method for evaluating the consequence propagation of security attacks in cyber–physical systems. *Futur Gener Comput Syst*. 2017;67:57-71.

130. Rasmussen TB, Yang G, and Nielsen AH, "A review of cyber-physical energy system security assessment," in Proceeding-12th IEEE Power and Energy Society PowerTech Conference, 2017.
131. Weber RH. Internet of things—new security and privacy challenges. *Comput Law Secur Rev*. 2010;26(1):23-30.
132. Trippel T, Weisse O, Xu W, Honeyman P, and Fu K, "WALNUT: waging doubt on the integrity of MEMS accelerometers," in IEEE Security and Privacy Symposium, 2017, no. April.
133. Byres EJ, Franz M, and Miller D, "The use of attack trees in assessing vulnerabilities in SCADA systems," 2004.
134. Liu N, Zhang J, Wu X. Asset Analysis of risk assessment for IEC 61850-based power control systems—Part I: methodology. *IEEE Trans Power Deliv*. 2011;26(2):869-875.
135. Patapanchala PS, Huo C, Bobba RB, and Cotilla-Sanchez E, "Exploring security metrics for electric grid infrastructures leveraging attack graphs," in 2016 *IEEE Conference on Technologies for Sustainability*, SusTech *2016*, 2017, pp. 89-95.
136. Ashok A, Hahn A, Govindarasu M. Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment. *J Adv Res*. 2014;5(4):481-489.
137. Law YW, Alpcan T, Palaniswami M, Dey S. Security games and risk minimization for automatic generation control in smart grid. *IEEE Trans Power Syst*. 2012;7638:281-295.
138. Chen J, Zhu Q. Security as a service for cloud-enabled internet of controlled things under advanced persistent threats: a contract design approach. *IEEE Trans Inf Forensics Secur*. 2017;6013(c):1-1.
139. Li Z, Jin D, Hannon C, Shahidehpour M, Wang J. Assessing and mitigating cybersecurity tisks of traffic light systems in smart cities. *IET Cyber-Physical Syst Theory Appl*. 2016;1(1):60-69.
140. Liu X, Shahidehpour M, Li Z, Liu X, Cao Y, Li Z. Power system risk assessment in cyber attacks considering the role of protection systems. *IEEE Trans. Smart Grid*. 2017;8(2):572-580.
141. Hird J, Hawley M, and Machin C, "Air traffic management security research in SESAR," in *Proceedings - 11th International Conference on Availability, Reliability and Security (ARES)*, 2016, pp. 486-492.
142. Hird J, Koelle R, and Kolev D, "Towards mathematical modelling in security risk management in system engineering," in Integrated Communications, Navigation and Surveillance Conference (ICNS), 2013, 2013, no. IEEE, pp 1-13.
143. Anwar A, Mahmood A. Cyber security of smart grid infrastructure. *State Art Intrusion Prev Detect*. 2014;January(January):139-154.
144. Dondossola G, Garrone F, and Szanto J, "Cyber risk assessment of power control systems—a metrics weighed by attack experiments," in *IEEE Power and Energy Society General Meeting*, 2011, pp. 1-9.
145. DeSmit Z, Elhabashy AE, Wells LJ, Camelio JA. Cyber-physical vulnerability assessment in manufacturing systems. *Procedia Manuf*. 2016;5:1060-1074.
146. Cong SUN, Jianfeng MA, Qingsong YAO. On the architecture and development life cycle of secure cyber-physical systems. *J Commun Inf Networks*. 2016;1(4):1-21.
147. CrowdStrike, "Securing the supply chain," 2018.
148. Ikimi O., "Cyber attacks that target electrical devices and equipment: what engineers should know," *All About Circuits*, 2020. [Online]. Available: https://www.allaboutcircuits.com/news/cyber-attacks-that-target-electrical-devices-and-equipment-what-engineers-should-know/
149. Lee S, Gandhi R, and Ahn G, "Security requirements driven risk assessment for critical infrastructure information systems," in *Proceedings - 13th IEEE International Requirements Engineering Conference, Symposium on Requirements Engineering for Information Security (SREIS-05)*, 2005, no. Sreis 05, pp. 2–9.
150. Wieringa RJ. *Design Science Methodology: For Information Systems and Software Engineering*. Berlin, Heidelberg: Springer; 2014.
151. Hall JG, Rapanotti L. A design theory for software engineering. *Inf Softw Technol*. 2017;87:46-61.
152. Stol KJ, Fitzgerald B. Theory-oriented software engineering. *Sci Comput Program*. 2015;101:79-98.

How to cite this article: Zahid M, Inayat I, Daneva M, Mehmood Z. Security risks in cyber physical systems—A systematic mapping study. *J Softw Evol Proc*. 2021;33:e2346. https://doi.org/10.1002/smr.2346

APPENDIX A: TABULAR RESULTS

This section of the document represents the tabular results obtained from the systematic mapping conducted.

TABLE A1 Journals included

Journal title	Article count	Citation count	Journal title	Article count	Citation count
1. IEEE Transactions on Smart Grid	6	359	2. In Renewable Energy Integration	1	2
3. IEEE Transactions on Power Delivery	4	616	4. Computer	1	14
5. International Journal of Critical Infrastructure Protection	2	95	6. Cyber Physical Systems Approach to Smart Electric Power Grid	2	15
7. IEEE Transactions on Dependable and Secure Computing	2	108	8. Secure Cloud Computing	1	3
9. IEEE Systems Journal	2	79	10. Electric Power System Research	1	57
11. IEEE Transactions on Systems, Man and Cybernetics	2	74	12. IET Cyber-Physical Systems: Theory & Applications	3	32
13. IEEE Internet of Things Journal	2	396	14. IEEE Access	7	23
15. Journal of Hardware and Systems Security	1	10	16. IEEE Cloud Computing	1	116
17. Journal of Network and Computer Applications	1	777	18. Service Oriented in Holonic and Multi-agent Manufacturing	1	2
19. ISA Transactions	1	286	20. Recent Advances in Computational Intelligence in Defense and Security	1	2
21. Journal of Advanced Research	1	86	22. ACM Computing Surveys (CSUR)	1	668
23. International Journal of Production Economics	1	34	24. IEEE Network	1	91
25. IEEE Communications Magazine	1	36	26. Applied Computing and Informatics	1	26
27. Journal of Communication and Information Networks	1	4	28. Computer Law & Security Review	1	1,339
29. IEEE Transactions on Industrial Informatics	2	311	30. Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare	1	18
31. Risk Analysis An International Journal	1	254	32. Secure Smart Embedded Devices, Platforms and Applications	1	9
33. Journal of Systems & Software	1	182	34. Energy Conversion and Management	1	9
35. Journal of Homeland Security and Emergency Management	1	56	36. Procedia Manufacturing	1	38
37. IEEE Transactions on Information Forensics and Security	1	48	38. IFAC Proceedings Volumes	1	17
39. Journal of Automatica Sinica	1	15	40. ACM Transactions on Cyber-Physical Systems	2	5
41. Journal of China Universities of Posts and Telecommunications	1	29	42. Neural Computing and Applications	1	11
43. Journal of Information Security and Applications	1	94	44. IEEE Transactions on Device and Material Reliability	1	5
45. Environment Systems and Decisions	1	81	46. International Journal of Electrical Power and Energy Systems	1	117
47. European Journal of Control	1	267	48. CIRP Annals - Manufacturing Technology	2	48
49. IEEE Power Engineering Society Winter Meeting	1	9	50. Journal of Software Evolution and Processes	2	0
51. IEEE Transactions on Power Systems	1	72	52. Arabian Journal for Science and Engineering	0	10
53. CSI Transactions on ICT	1	13	54. Automatic Control and Computer Science	1	27
55. Proceedings of the IEEE	4	1,191	56. International Journal of Distributed Sensor Networks	1	15
57. Computers & Security	9	1,050	58. Journal of Information Processing Systems	2	12

TABLE A1 (Continued)

Journal title	Article count	Citation count	Journal title	Article count	Citation count
59. Renewable and Sustainable Energy Reviews	2	222	60. Technologies	1	18
61. Journal of Supercomputing	1	5	62. Journal of Applied Sciences	2	33
63. IEEE Embedded Systems Letters	2	41	64. Sensors	1	16
65. Annual Reviews in Control	1	32	66. IEEE Transactions on Industrial Electronics	1	36
67. Reliability Engineering and System Safety	5	597	68. Cyber Security for Cyber Physical Systems	1	1
69. Computer Networks	4	2,214	70. Sustainability	1	3
71. Annals of Nuclear Energy	1	0	72. Journal of Sensor and Actuator Networks	1	5
73. Microprocessors and Microsystems	1	0	74. Safety Science	1	91
75. Computer Standards & Interfaces	2	253	76. Business and Information Systems Engineering	1	0
77. Future Generation Computer Systems	6	371	78. Robotics and Computer Integrated Manufacturing	1	34
79. Computer Communications	1	163	80. Computers in Industry	2	124
81. Control Theory and Technology	1	46			

TABLE A2 Conferences included

Conference title	Article count	Citation count	Conference title	Article count	Citation count
1. International Conference on Availability, Reliability and Security	4	21	2. IEEE International conference on Power System Technology	1	5
3. IEEE International Smart Cities Conference	3	28	4. International Conference on Software, Knowledge, Information Management and Applications	1	4
5. IEEE PES Conference on Innovative Smart Grid Technologies	5	70	6. IEEE International Conference on Industrial Engineering and Engineering Management	1	11
7. IEEE International Conference on System of Systems Engineering	3	29	8. International Conference on Reliability Engineering	1	17
9. International Conference on Intelligent Information Hiding and Multimedia Signal Processing	3	109	10. International Conference on Body Area Networks	1	116
11. IEEE International Conference on Internet of Things	2	33	12. International Conference on Platform Technology and Service	1	44
13. International Conference on Cyber Conflict	2	189	14. IEEE International Conference on Secure Software Integration and Reliability Improvement Companion	1	25
15. IEEE International Conference on Technologies for Homeland Security	4	113	16. International Conference on Communication and Networks	1	13
17. IEEE International Conference on Electric Utility Deregulation, Restructuring and Power Technologies	1	5	18. IEEE International Carnahan Conference on Security Technology	1	58
19. International Conference on Architecture of Computing Systems	1	11	20. IEEE/ACS International Conference of Computer Systems and Applications	1	18
21. IEEE International Conference on Systems, Man, and Cybernetics	3	78	22. International Energy and Sustainability Conference	1	0
23. International Conference on Information Fusion	1	7	24. ACM SIGITE Conference on Information Technology Education	1	6

(Continues)

TABLE A2 (Continued)

Conference title	Article count	Citation count	Conference title	Article count	Citation count
25. IEEE International Conference on Intelligent Computing and Information System	1	5	26. International Conference on Electricity Distribution	1	7
27. International Conference on Probabilistic Methods Applied to Power Systems	1	0	28. Integrated Communications, Navigation, and Surveillance Conference	1	3
29. IEEE PES PowerTech Conference	1	10	30. IEEE International Conference on Cloud Computing	1	264
31. IEEE Electrical Power and Energy Conference	1	29	32. International conference on Wireless Communications & Mobile Computing	1	10
33. IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids	1	2	34. Allerton Conference on Communication, Control, and Computing	1	19
35.International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing	1	5	36. International Conference on Network-Based Information Systems	1	4
37. International Conference on Control Systems and Computer Science	1	4	38. IEEE International Symposium on Industrial Electronics	2	11
39. International Conference on the Developments on eSystems Engineering	1	10	40. Smart City Symposium Pargue	1	4
41. IEEE International Conference on Cybernetics	1	8	42.International Symposium on High Assurance Systems Engineering	1	0
43. International Conference on Information, Intelligence, Systems and Applications	1	4	44. International Symposium on Real-Time and Embedded Systems and Technologies	1	6
45. International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery	1	1	46. IEEE Symposium on Computational Intelligence in Cyber Security	1	4
47. International Conference on Modeling and Simulation	1	8	48. IEEE Systems and Information Engineering Design	1	33
49. Asset Management Conference	1	4	50. Symposium on Requirements Engineering for Information Security	1	18
51. IEEE International Conference on Cyber Physical and Social Computing	2	33	52. European Conference on Research in Computer Security	1	57
53. IEEE International Conference on Green Computing and Communications	2	33	54. International Symposium on Resilient Control Systems	1	67
55. International Conference on Information Systems Security and Privacy	1	4	56. IEEE European Symposium on Security and Privacy	1	118
57. IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing	1	19	58. IEEE Pacific Rim International Symposium on Dependable Computing	2	27
59. IEEE International Conference on Computational Systems and Information Technology for Sustainable Solution	1	4	60. IEEE Symposium on Product Compliance Engineering	1	4
61. International Conference for Internet Technology and Secured Transactions	1	7	62. IEEE International Symposium on Computational Intelligence and Informatics	1	29
63. International Conference on Computational Science and its Applications	1	60	64. International Symposium on Smart Electric Distribution Systems and Technologies	1	11
65. IEEE Rural Electric Power Conference	2	7	66. Annual North American Power Symposium	1	25
67. International Conference on Research Challenges in Information Science	1	2	68. IEEE Power and Energy Society General Meeting Conference	5	79
69. International Conference on Electronical Engineering and Informatics	1	7	70. Embedded, Cyber-Physical, and IoT Systems	1	0
71. National Power Systems Conference	1	30	72. Performance Management of Integrated Systems and its Applications in Software Engineering	1	0

TABLE A2 (Continued)

Conference title	Article count	Citation count	Conference title	Article count	Citation count
73. IEEE Region 10 Conference	1	7	74. International Conference on Computer Safety, Reliability, and Security	1	1
75. IEEE/AFCEA Military Communications Conference	1	6	76. IEEE Taxes Power and Energy Conference	1	9
77. IEEE Information Technology, Electronics and Mobile Communication Conference	1	3	78. International Conference on Artificial Intelligence	1	2
79. International Conference on Engineering of Complex Computer Systems	1	14	80. International Conference on Frontiers of Information Technology	1	0
81. Federated Conference on Computer Science and Information Systems	1	8	82. IEEE International Conference on Software Quality, Reliability, and Security	1	0
83. IEEE Conference on Technologies for Sustainability	1	5	84. IEEE Conference on Decision and Control	2	29
85. IEEE PES Innovative Smart Grid Technologies Conference Europe	1	1	86. ACM International Conference on Security of Information and Networks	1	3
87. IEEE/IFIP International Conference on Dependable Systems and Networks	1	8	88. International Conference on Malicious and Unwanted Software	1	1
89. IEEE International Conference on Environment and Electrical Engineering	1	1	90. IEEE International Conference on Data Science in Cyberspace	1	4
91. IEEE International Conference on Connected Vehicles and Expo	1	0	92. ACM Asia Conference on Computer and Communications Security	1	20
93. International Conference on Engineering of Complex Computer Systems	2	21	94. IEEE National Aerospace Electronics Conference	1	0
95. IEEE International Conference on Advances in Computing, Communications and Informatics	1	11	96. IEEE International Conference on Industrial Informatics	1	1
97. International Conference on Information Technology Systems and Innovation	1	4	98. IEEE International Systems Conference	2	25
99. IEEE International Information Technology and Artificial Intelligence Conference	1	10	100. International Conference on Smart Grid and Clean Energy Technologies	1	3
101.IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support	1	3	102. Forum on Specification and Design Languages Conference	1	0
103. IEEE Long Island Systems, Applications and Technology Conference	1	40	104. International Conference on Hybrid Information Technology	1	1
105. International Conference on Innovative Computing Technology	1	15	106. IEEE Industry Applications Society Annual Meeting	1	9
107. Conference on Systems Engineering Research	1	31	108. IEEE Grenoble Conference PowerTech	1	8
109. International Conference on Radar, Antenna, Microwave, Electronics and Telecommunications	1	12	110. Applied Cyber-Physical Systems	1	3
111. International IEEE Enterprise Distributed Object Computing Conference	1	144	112. International Conference on Next Generation Mobile Applications, Services and Technologies,	1	17
113. International Conference on Risks and Security of Internet and Systems	1	64	114. System Safety and Cyber-Security Conference	1	15
115. Conference on Information Sciences and Systems	1	13	116. Technical Innovation for Smart Systems	1	0
117. International Conference Eco-friendly Computing and Communication Systems	1	11	118. IEEE International Conference on Dependable, Autonomic and Secure Computing	1	1
119. International Conference on Security of Smart Cities, Industrial Control System and Communications	1	25	120. IEEE International Conference on Pervasive Intelligence and Computing	1	1

(Continues)

TABLE A2 (Continued)

Conference title	Article count	Citation count	Conference title	Article count	Citation count
121. International Conference on Critical Infrastructures	1	11	122. IEEE International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress	1	1
123. Resilience Week (RWS) IEEE	1	4	124. IEEE International Conference on Smart Data	1	32
125. International Conference on Frontier of Computer Science and Technology	1	18	126. International Conference on Database and Expert Systems Applications	1	0

TABLE A3 Workshops included

Workshop title	Article count	Citation count	Workshop title	Article count	Citation count
1. Future directions in cyber-physical systems security	1	450	2. International Infrastructure Survivability Workshop	1	257
3. ACM Workshop on Cyber-Physical Systems Security and Privacy	1	13	4. Workshop on Critical Infrastructures: Contingency Management, Intelligent, Agent-based, Cloud Computing and Cyber Security	1	0
5. CIRED Workshop	1	7	6. IEEE/ACM International Workshop on Software Engineering for Smart Cyber-Physical Systems	1	5
7. Joint Workshop on Cyber- Physical Security and Resilience in Smart Grids	1	5	8. ACM/ASIA CCS Workshop on Cyber-Physical System Security	1	10
9. Workshop on Computing, Networking and Communications	1	21	10. Euromicro Conference on Software Engineering and Applications	1	0
11. IEEE Annual International Computers, Software and Applications Conference Workshop	1	18	12. IEEE Security & Privacy Workshops	1	9
13. IEEE International Conference on Communications Workshops	1	2			

TABLE A4 Validation techniques reported

Validation technique	Use count
Implementation	19
Simulation	49
Case study	33
Questionnaire	2
Proof of concept example	3
Use case	3
Experiment	11
Qualitative content analysis	6
Tool testing	7
Testbeds	11
Statistics	34

TABLE A5 Validation metrics reported

Validation matrices	Count	Validation matrices	Count
Risk value	28	Stability margin	1
Resiliency analysis	3	Score values	2
Benchmarking	19	Convex Hull	1
Reduced power set	1	Maximum fitness value	1
Injection level detection rate	3	Exponential distribution	1
Conditional Lyapunov exponents	1	Probability & statistics	36
Fitness value	1	Attack detection rate	8
Tolerence accuracy	1	Ratios	13
Comparison of performance	6	Attack recovery rate	2
Net present value	1	Confusion matrix	1
Load calculations	15	Risk detection	7
Space & time overhead	16	Failure rate	11

TABLE A6 Total number of articles w.r.t. security requirements and risk processes focused

Security requirement	Risk identification	Risk assessment	Risk mitigation	Risk management
Authentication	56	123	60	24
Authorization	25	13	31	3
Confidentiality	61	54	63	11
Self-healing	11	15	10	2
Resilience	30	33	29	4
Fault-tolerance	16	69	12	14
Integrity	65	136	68	26
Anonymity	9	11	11	2
Liability	8	133	4	25
Non-repudiation	12	93	11	19
Linkability	5	20	4	3
Reliability	56	27	46	6
Availability	57	123	58	24
Trust	40	139	42	20
Data freshness	23	15	22	0

APPENDIX B: A LIST OF REVIEWED STUDIES

This section of the document represents the references of the literature studied.

1. S. Lee, R. Gandhi, and G. Ahn, "Security requirements driven risk assessment for critical infrastructure information systems," ... *Inf. Secur.* (..., 05, pp. 2–9, 2005.
2. C. Alberts and A. Dorofee, "Introduction to the OCTAVE Approach," ..., *PA*, *Carnegie Mellon* ..., no. August, pp. 1–37, 2003.
3. V. Chiprianov, L. Gallon, K. Salameh, M. Munier, and J. El Hachem, "Towards Security Software Engineering the Smart Grid as a System of Systems," in *10th System of Systems Engineering Conference (Se*, 2015, pp. 77–82.
4. M. Athinaiou, "Cyber Security Risk Management for Health- based Critical Infrastructures," in *11th International Conference on Research Challenges in Information Science (RCIS)*, 2017.
5. X. He, Z. Sui, and H. De Meer, "Game-theoretic Risk Assessment in Communication Networks," in *16th IEEE International Conference on Environment and Electrical Engineering (EEEIC)*, 2016, pp. 0–5.
6. R. Santini and S. Panzieri, "A Graph-Based Evidence Theory for Assessing Risk," *18th Int. Conf. Inf. Fusion*, pp. 1467–1,474, 2015.

7. S. Yoneda, S. Tanimoto, and T. Konosu, "Risk Assessment in Cyber-physical System in Office Environment," in *1th Internation Conference on Network-Based Information Systems*, 2015.
8. E. A. Lee, "Cyber Physical Systems: Design Challenges," *11th IEEE Int. Symp. Object Component-Oriented Real-Time Distrib. Comput.*, pp. 363–369, 2008.
9. C. Tranchita, N. Hadjsaid, and A. Torres, "Overview of the power systems security with regard to cyberattacks," *2009 4th Int. Conf. Crit. Infrastructures,*, pp. 1–8, 2009.
10. M. H. Henry, R. M. Layer, K. Z. Snow, and D. R. Zaret, "Evaluating the risk of cyber attacks on scada systems via petri net analysis with application to hazardous liquid loading operations," *2009 IEEE Conf. Technol. Homel. Secur. HST 2009*, pp. 607–614, 2009.
11. P. Saripalli and B. Walters, "QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security," *2010 IEEE 3rd Int. Conf. Cloud Comput.*, pp. 280–288, 2010.
12. K. K. Fletcher and X. Liu, "Security requirements analysis, specification, prioritization and policy development in cyber-physical systems," *5th Int. Conf. Secur. Softw. Integr. Reliab. Improv. - Companion, SSIRI-C 2011*, pp. 106–113, 2011.
13. Z. Zhigang, L. Hao, N. Shuangxia, and M. Jiansong, "Information security requirements and challenges in smart grid," *2011 6th IEEE Jt. Int. Inf. Technol. Artif. Intell. Conf.*, vol. 1, pp. 90–92, 2011.
14. S. L. Clements, H. Kirkham, M. Elizondo, and S. Lu, "Protecting the smart grid: A risk based approach," *2011 IEEE Power Energy Soc. Gen. Meet.*, pp. 1–7, 2011.
15. Q. Shafi, "Cyber Physical Systems Security: A Brief Survey," *2012 12th Int. Conf. Comput. Sci. Its Appl.*, pp. 146–150, 2012.
16. Y. W. Law, T. Alpcan, and M. Palaniswami, "Security games for voltage control in smart grid," *2012 50th Annu. Allert. Conf. Commun. Control. Comput.*, pp. 212–219, 2012.
17. R. Kozik and M. Chora??, "Current cyber security threats and challenges in critical infrastructures protection," *2013 2nd Int. Conf. Informatics Appl. ICIA 2013*, pp. 93–97, 2013.
18. C. Brasca, E. Ciapessoni, D. Cirio, A. Pitto, M. Sforna, and A. Morini, "Extended risk analysis of power and ICT systems," *2013 4th IEEE/PES Innov. Smart Grid Technol. Eur. ISGT Eur. 2013*, pp. 1–5, 2013.
19. J. McDonald, N. Oualha, A. Puccetti, A. Hecker, and F. Planchon, "Application of EBIOS for the risk assessment of ICT use in electrical distribution sub-stations," *2013 IEEE Grenoble Conf. PowerTech, POWERTECH 2013*, 2013.
20. K. Mansfield, T. Eveleigh, T. H. Holzer, and S. Sarkani, "Unmanned aerial vehicle smart device ground control station cyber security threat model," *2013 IEEE Int. Conf. Technol. Homel. Secur. HST 2013*, pp. 722–728, 2013.
21. C. W. Axelrod, "Managing the risks of cyber-physical systems," *2013 IEEE Long Isl. Syst. Appl. Technol. Conf.*, pp. 1–6, 2013.
22. M. a. Mustafa and G. Kalogridis, "Smart electric vehicle charging: Security analysis," *2013 IEEE PES Innov. Smart Grid Technol. Conf.*, pp. 1–6, 2013.
23. D. MacDonald et al., "Cyber/physical security vulnerability assessment integration," *2013 IEEE PES Innov. Smart Grid Technol. Conf. ISGT 2013*, 2013.
24. S. Sierla, M. Hurkala, K. Charitoudi, C.-W. Yang, and V. Vyatkin, "Security risk analysis for smart grid automation," *2014 IEEE 23rd Int. Symp. Ind. Electron.*, no. 257459, pp. 1737–1744, 2014.
25. T. Shawly, J. Liu, N. Burow, S. Bagchi, R. Berthier, and R. B. Bobba, "A risk assessment tool for advanced metering infrastructures," *2014 IEEE Int. Conf. Smart Grid Commun.*, pp. 989–994, 2014.
26. F. Farzan, M. A. Jafari, D. Wei, and Y. Lu, "Cyber-related risk assessment and critical asset identification in power grids," *2014 IEEE PES Innov. Smart Grid Technol. Conf. ISGT 2014*, pp. 1–5, 2014.
27. H. Onishi, "Guidelines against diversified vehicle cyber risks," *2014 Int. Conf. Connect. Veh. Expo, ICCVE 2014 - Proc.*, no. 1, pp. 625–626, 2015.
28. C. W. Axelrod, "Software Security Assurance of Electrical Grid Systems Relating Mechatronics to Software Security Engineering," *2014 Int. Energy Sustain. Conf.*, 2014.
29. D. Kolev and E. Morozov, "Mathematical Modelling in Air Traffic Management Security," *2014 Ninth Int. Conf. Availability, Reliab. Secur.*, pp. 523–529, 2014.
30. N. Polemi and S. Papastergiou, "Current efforts in ports and supply chains risk assessment," *2015 10th Int. Conf. Internet Technol. Secur. Trans. ICITST 2015*, pp. 349–354, 2016.
31. L. Wei, A. H. Moghadasi, A. Sundararajan, and A. I. Sarwat, "Defending mechanisms for protecting power systems against intelligent attacks," *2015 10th Syst. Syst. Eng. Conf. SoSE 2015*, pp. 12–17, 2015.
32. D. Chen, K. Meinke, K. Ostberg, F. Asplund, and C. Baumann, "A knowledge-in-the-loop approach to integrated safety & security for cooperative system-of-systems," in *2015 IEEE 7th International Conference on Intelligent Computing and Information Systems, ICICIS 2015*, 2016, pp. 13–20.
33. A. Ashok and M. Govindarasu, "Cyber-physical risk modeling and mitigation for the smart grid using a game-theoretic approach," *2015 IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. ISGT 2015*, vol. 2015–Janua, 2015.

34. P. Kaster and P. K. Sen, "Cyber security and rural electric power systems," *2015 IEEE Rural Electr. Power Conf.*, pp. 49–54, 2015.
35. S. Jagannathan and A. Sorini, "A cybersecurity risk analysis methodology for medical devices," *2015 IEEE Symp. Prod. Compliance Eng.*, no. June 2013, pp. 1–6, 2015.
36. X. Fan, K. Fan, Y. Wang, and R. Zhou, "Overview of cyber-security of industrial control system," *2015 Int. Conf. Cyber Secur. Smart Cities, Ind. Control Syst. Commun. SSIC 2015 - Proc.*, 2015.
37. H.-K. Kong, T.-S. Kim, and M.-K. Hong, "A Security Risk Assessment Framework for Smart Car," *2016 10th Int. Conf. Innov. Mob. Internet Serv. Ubiquitous Comput.*, pp. 102–108, 2016.
38. M. Mori, A. Ceccarelli, T. Zoppi, and A. Bondavalli, "On the impact of emergent properties on SoS security," *2016 11th Syst. Syst. Eng. Conf.*, 2016.
39. M. A. Rahman, A. H. M. Jakaria, and E. Al-Shaer, "Formal Analysis for Dependable Supervisory Control and Data Acquisition in Smart Grids," *2016 46th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Networks*, pp. 263–274, 2016.
40. Xiaoxue Liu, Jiexin Zhang, and Peidong Zhu, "Dependence analysis based cyber-physical security assessment for critical infrastructure networks," *2016 IEEE 7th Annu. Inf. Technol. Electron. Mob. Commun. Conf.*, pp. 1–7, 2016.
41. P. S. Patapanchala, C. Huo, R. B. Bobba, and E. Cotilla-Sanchez, "Exploring security metrics for electric grid infrastructures leveraging attack graphs," *2016 IEEE Conf. Technol. Sustain. SusTech 2016*, pp. 89–95, 2017.
42. A. Y. Nur and M. E. Tozal, "Defending Cyber-Physical Systems against DoS Attacks," *2016 IEEE Int. Conf. Smart Comput. SMARTCOMP 2016*, pp. 8–10, 2016.
43. S. Imbrogno, C. Foglietta, C. Palazzo, and S. Panzieri, "Managing decisions for smart grid using interdependency modeling," *2016 IEEE Int. Multi-Disciplinary Conf. Cogn. Methods Situat. Aware. Decis. Support. CogSIMA 2016*, pp. 198–204, 2016.
44. S. J. De and D. Le Metayer, "Privacy Harm Analysis: A Case Study on Smart Grids," *2016 IEEE Secur. Priv. Work.*, pp. 58–65, 2016.
45. X. Ji, H. Yu, G. Fan, and W. Fu, "Attack-defense trees based cyber security analysis for CPSs," *2016 IEEE/ACIS 17th Int. Conf. Softw. Eng. Artif. Intell. Netw. Parallel/Distributed Comput. SNPD 2016*, pp. 693–698, 2016.
46. A. K. Koundinya, Sharvani G.S., and K. U. Rao, "Calibrated security measures for centralized IoT applications of smart grids," *2016 Int. Conf. Comput. Syst. Inf. Technol. Sustain. Solut.*, pp. 153–157, 2016.
47. W. G. Temple, B. A. N. Tran, B. Chen, Z. Kalbarczyk, and W. H. Sanders, "On Train Automatic Stop Control Using Balises: Attacks and a Software-Only Countermeasure," *2017 IEEE 22nd Pacific Rim Int. Symp. Dependable Comput.*, pp. 274–283, 2017.
48. V. Nagaraju, L. Fiondella, and T. Wandji, "A survey of fault and attack tree modeling and analysis for cyber risk management," *2017 IEEE Int. Symp. Technol. Homel. Secur.*, pp. 1–6, 2017.
49. W. M. Bateman, A. Amaya, and J. Fenstermaker, "Securing the Grid and Your Critical Utility Functions," *2017 IEEE Rural Electr. Power Conf.*, pp. 29–37, 2017.
50. H. Maziku and S. Shetty, "Software Defined Networking enabled resilience for IEC 61850-based substation communication systems," *2017 Int. Conf. Comput. Netw. Commun. ICNC 2017*, pp. 690–694, 2017.
51. S.-R. Oh and Y.-G. Kim, "Security Requirements Analysis for the IoT," *2017 Int. Conf. Platf. Technol. Serv.*, pp. 1–6, 2017.
52. J. Mcdonald et al., "the Sinari Project: Security Analysis and Risk Assessment Applied To the Electrical Distribution Network," *22nd Int. Conf. Electr. Distrib.*, no. 995, pp. 10–13, 2013.
53. L. K. Nozick, M. A. Turnquist, D. A. Jones, J. R. Davis, and C. R. Lawton, "Assessing the performance of interdependent infrastructures and optimizing investments," *37th Annu. Hawaii Int. Conf. Syst. Sci. 2004. Proc.*, vol. 0, no. C, p. 7 pp., 2004.
54. P. Datta Ray, R. Harnoor, and M. Hentea, "Smart power grid security: A unified risk management approach," *44th Annu. 2010 IEEE Int. Carnahan Conf. Secur. Technol.*, pp. 276–285, 2010.
55. L. Ledwaba, "A Threat-Vulnerability Based Risk Analysis Model for Cyber Physical System Security," in *50th International Conference on System Sciences*, 2017, pp. 6021–6,030.
56. S. Kriaa, M. Bouissou, and L. Piètre-Cambacédès, "Modeling the Stuxnet attack with BDMP: Towards more formal risk assessments," *7th Int. Conf. Risks Secur. Internet Syst. Cris. 2012*, 2012.
57. R. S. H. Piggin, "Governance, risk and compliance: impediments and opportunities for managing operational technology risk in industrial cyber security and safety," *9th IET Int. Conf. Syst. Saf. Cyber Secur.*, p. 4.2.2-4.2.2, 2014.
58. Y. Peng, T. Lu, J. Liu, Y. Gao, X. Guo, and F. Xie, "Cyber-Physical System Risk Assessment," in *9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2013.
59. M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux, *Game theory meets network security and privacy*, vol. 45, no. 3. 2013.
60. A. Motil et al., "Guiding The Selection Of Security Patterns Based On Security Requirements And Pattern Classification," *ACM 20th Eur. Conf. Pattern Lang. Programs, Eur. 2015*, vol. 0, no. 0, p. 10, 2015.
61. H. Sandberg and K. H. Johansson, "Networked Control Systems under Cyber Attacks with Applications to Power Networks," in *American Control Conference*, 2010, pp. 3690–3,696.

62. I. Anne Tøndel, J. Foros, S. Skaufel Kilskar, P. Hokstad, and M. Gilje Jaatun, "Interdependencies and Reliability in the Combined ICT and Power System: An overview of current research," *Appl. Comput. Informatics*, 2017.
63. J. Haehner et al., "A Concept for Securing Cyber-Physical Systems with Organic Computing Techniques," in *Architecture of Computing Systems (ARCS), Proceedings of 2013 26th International Conference on*, 2013, vol. 9, pp. 1–13.
64. T. Kiesling, M. Krempel, J. Niederl, and J. Ziegler, "A Model-Based Approach for Aviation Cyber Security Risk Assessment.," *Ares*, pp. 517–525, 2016.
65. M. Hawley, P. Howard, R. Koelle, and P. Saxton, "Collaborative Security Management: Developing Ideas in Security Management for Air Traffic Control," *Availability, Reliab. Secur. (ARES), 2013 Eighth Int. Conf.*, pp. 802–806, 2013.
66. I. Mihai-Gabriel and P. Victor-Valeriu, "Achieving DDoS resiliency in a software defined network by intelligent risk assessment based on neural networks and danger theory," in *CINTI 2014-15th IEEE International Symposium on Computational Intelligence and Informatics, Proceedings*, 2014, pp. 319–324.
67. H. H. Safa, D. M. Souran, M. Ghasempour, and A. Khazaee, "Cyber security of smart grid and SCADA systems, threats and risks," *CIRED Work. 2016*, no. 245, p. 92 (4.)-92 (4.), 2016.
68. R. Wolthuis, F. Fransen, and J. E.Y. Rossebø, "An Enhanced Risk- for Smart Grids," *Computer (Long. Beach. Calif).*, vol. 50, no. 4, pp. 62–71, 2017.
69. R. Mitchell and I.-R. Chen, "A survey of intrusion detection in wireless network applications," *Comput. Commun.*, vol. 42, pp. 1–23, 2014.
70. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Networks*, vol. 76, pp. 146–164, 2015.
71. W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Comput. Networks*, vol. 57, no. 5, pp. 1344–1,371, 2013.
72. D. Mellado, E. Fernández-Medina, and M. Piattini, "A common criteria based security requirements engineering process for the development of secure information systems," *Comput. Stand. Interfaces*, vol. 29, no. 2, pp. 244–253, 2007.
73. S. Nazir, S. Patel, and D. Patel, "Title: Assessing and Augmenting SCADA Cyber Security-A Survey of Techniques," *Comput. Secur.*, 2017.
74. Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: analysis, challenges and solutions," *Comput. Secur.*, vol. 68, pp. 81–97, 2017.
75. Y. Cherdantseva et al., "A review of cyber security risk assessment methods for SCADA systems," *Comput. Secur.*, vol. 56, pp. 1–27, 2015.
76. G. S. Bopche and B. M. Mehtre, "Graph similarity metrics for assessing temporal changes in attack surface of dynamic networks," *Comput. Secur.*, vol. 64, pp. 16–43, 2017.
77. Y. Ben Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the Internet of Things: A context-aware and multi-service approach," *Comput. Secur.*, vol. 39, no. PART B, pp. 351–365, 2013.
78. S. Zonouz and P. Haghani, "Cyber-physical security metric inference in smart grid critical infrastructures based on system administrators' responsive behavior," *Comput. Secur.*, vol. 39, no. PART B, pp. 190–200, 2013.
79. A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "SCADA security in the light of cyber-warfare," *Comput. Secur.*, vol. 31, no. 4, pp. 418–436, 2012.
80. Y. J. Chen, J. S. Shih, and S. T. Cheng, "A cyber-physical integrated security framework with fuzzy logic assessment for cultural heritages," *Conf. Proc. - IEEE Int. Conf. Syst. Man Cybern.*, pp. 1843–1847, 2011.
81. I. N. Fovino and M. Masera, "Emergent disservices in interdependent systems and system-of-systems," *Conf. Proc. - IEEE Int. Conf. Syst. Man Cybern.*, vol. 1, pp. 590–595, 2007.
82. C. W. Ten, C. C. Liu, and M. Govindarasu, "Anomaly extraction and correlations for power infrastructure cyber systems," *Conf. Proc. - IEEE Int. Conf. Syst. Man Cybern.*, pp. 7–12, 2008.
83. G. Wu, J. Sun, and J. Chen, "A survey on the security of cyber-physical systems," *Control Theory Technol.*, vol. 14, no. 1, pp. 2–10, 2016.
84. B. Green, M. Krotofil, and D. Hutchison, "Achieving ICS Resilience and Security through Granular Data Flow Management," *CPS-SPC - Cyber-Physical Syst. Secur. Priv.*, pp. 93–101, 2016.
85. H. Orojloo and M. A. Azgomi, "Evaluating the complexity and impacts of attacks on cyber-physical systems," *CSI Symp. Real-Time Embed. Syst. Technol. RTEST 2015*, 2015.
86. K. Chatterjee, D. Gupta, and A. De, "'A framework for development of secure software,'" *CSI Trans. ICT*, vol. 1, no. 2, pp. 143–157, 2013.
87. H. Onishi, "Paradigm change of vehicle cyber security," *Cyber Confl. (CYCON), 2012 4th Int. Conf.*, pp. 1–11, 2012.
88. K. Hartmann and C. Steup, "The vulnerability of UAVs to cyber attacks - An approach to the risk assessment," *Cyber Confl. (CyCon), 2013 5th Int. Conf.*, pp. 1–23, 2013.
89. H. Bayanifar and H. Kuhnle, "Enhancing Dependability and Security of Cyber-Physical Production Systems," in *Doctoral Conference on Computing, Electrical and Industrial Systems*, 2017, vol. 499, pp. 167–174.
90. Y. Xiang, L. Wang, and N. Liu, "Coordinated attacks on electric power systems in a cyber-physical environment," *Electr. Power Syst. Res.*, vol. 149, pp. 156–168, 2017.

91. H. Hashemi-Dezaki, S. M. M. Agah, H. Askarian-Abyaneh, and H. Haeri-Khiavi, "Sensitivity analysis of smart grids reliability due to indirect cyber-power interdependencies under various DG technologies, DG penetrations, and operation times," *Energy Convers. Manag.*, vol. 108, pp. 377–391, 2016.
92. D. DiMase, Z. A. Collier, K. Heffner, and I. Linkov, "Systems engineering framework for cyber physical security and resilience," *Environ. Syst. Decis.*, vol. 35, no. 2, pp. 291–300, 2015.
93. A. Sangiovanni-Vincentelli, W. Damm, and R. Passerone, "Taming Dr. Frankenstein: Contract-Based Design for Cyber-Physical Systems*," *Eur. J. Control*, vol. 18, no. 3, pp. 217–238, 2012.
94. L. Rajbhandari and E. A. Snekkenes, *Mapping Between Classical Risk Management and Game Theoratical Approaches*. 2011.
95. T. Kirkham, D. Armstrong, K. Djemame, and M. Jiang, "Risk driven Smart Home resource management using cloud services," *Futur. Gener. Comput. Syst.*, vol. 38, pp. 13–22, 2014.
96. A. Jacobsson, M. Boldt, and B. Carlsson, "A risk analysis of a smart home automation system," *Futur. Gener. Comput. Syst.*, vol. 56, pp. 719–733, 2016.
97. H. Orojloo and M. A. Azgomi, "A method for evaluating the consequence propagation of security attacks in cyber–physical systems," *Futur. Gener. Comput. Syst.*, vol. 67, pp. 57–71, 2017.
98. M. Teimourikia and M. Fugini, "Ontology development for run-time safety management methodology in Smart Work Environments using ambient knowledge," *Futur. Gener. Comput. Syst.*, vol. 68, pp. 428–441, 2017.
99. T. Liu et al., "Abnormal traffic-indexed state estimation: A cyber-physical fusion approach for Smart Grid attack detection," *Futur. Gener. Comput. Syst.*, vol. 49, pp. 94–103, 2015.
100. Y. W. Law, T. Alpcan, M. Palaniswami, and S. Dey, "Security Games and Risk Minimization for Automatic Generation Control in Smart Grid.," *GameSec*, vol. 7,638, pp. 281–295, 2012.
101. R. Delamare, F. Munoz, B. Baudry, and Y. Le Traon, *Testing Software and Systems*, vol. 6,435. 2010.
102. I. Symeonidis, M. A. Mustafa, and B. Preneel, "Keyless car sharing system: A security and privacy analysis," *IEEE 2nd Int. Smart Cities Conf. Improv. Citizens Qual. Life, ISC2 2016 - Proc.*, 2016.
103. A. Vasenev and L. Montoya, "Analysing non-malicious threats to urban smart grids by interrelating threats and threat taxonomies," *IEEE 2nd Int. Smart Cities Conf. Improv. Citizens Qual. Life, ISC2 2016 - Proc.*, pp. 0–3, 2016.
104. K. Waedt, A. Ciriello, M. Parekh, and E. Bajramovic, "Automatic assets identification for Smart Cities: Prerequisites for cybersecurity risk assessments," *IEEE 2nd Int. Smart Cities Conf. Improv. Citizens Qual. Life, ISC2 2016 - Proc.*, 2016.
105. A. Gabriel, "Design and Evaluation of Safety Instrumented Systems: A Simplified and Enhanced Approach," *IEEE Access*, vol. 5, pp. 3813–3,823, 2017.
106. N. H. Ab Rahman, W. B. Glisson, Y. Yang, and K.-K. R. Choo, "Forensic-by-Design Framework for Cyber- Physical Cloud Systems," *IEEE Cloud Comput.*, vol. 3, no. 1, pp. 50–59, 2016.
107. A. C. F. Chan and J. Zhou, "On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 58–65, 2013.
108. L. Wei, A. I. Sarwat, and W. Saad, "Risk assessment of coordinated cyber-physical attacks against power grids: A stochastic game approach," *IEEE Ind. Appl. Soc. 52nd Annu. Meet. IAS 2016*, pp. 1–7, 2016.
109. W. Wu, R. Kang, and Z. Li, "Risk Assessment Method for Cybersecurity of Cyber-Physical Systems Based on Inter-Dependency of Vulnerabilities," in *IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, 2015, pp. 1618–1,622.
110. P. K. Das, S. Narayanan, and N. K. Sharma, "Context-Sensitive Policy Based Security in Internet of Things," *IEEE Int. Conf. Smart Comput.*, pp. 1–6, 2016.
111. A. Pereira, N. Rodrigues, J. Barbosa, and P. Leitao, "Trust and risk management towards resilient large-scale cyber-physical systems," *IEEE Int. Symp. Ind. Electron.*, 2013.
112. N. Choucri and G. Agarwal, "Analytics for Smart Grid Cybersecurity," in *IEEE International Symposium on Technologies for Homeland Security (HST)*, 2017, pp. 1–3.
113. M. Moness and A. M. Moustafa, "A Survey of Cyber-Physical Advances and Challenges of Wind Energy Conversion Systems: Prospects for Internet of Energy," *IEEE Internet Things J.*, vol. 3, no. 2, pp. 134–145, 2016.
114. A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security – A Survey," *IEEE Internet Things J.*, vol. 4,662, no. c, 2017.
115. Y. Yang, K. McLaughlin, S. Sezer, Y. B. Yuan, and W. Huang, "Stateful intrusion detection for IEC 60870-5-104 SCADA security," *IEEE Power Energy Soc. Gen. Meet.*, vol. 2014–Octob, no. October, pp. 5–9, 2014.
116. C. C. Fung, M. A. Roumani, and K. P. Wong, "A Proposed Study on Economic Impacts due to Cyber Attacks in Smart Grid: A Risk Based Assessment," *IEEE Power Energy Soc. Gen. Meet.*, pp. 1–5, 2013.
117. J. E. Y. Rossebo, F. Fransen, and E. Luiijf, "Including threat actor capability and motivation in risk assessment for Smart GRIDs," *IEEE Proc. 2016 Jt. Work. Cyber-Physical Secur. Resil. Smart Grids, CPSR-SG 2016 - This Work. is Part CPS Week 2016*, 2016.

118. T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu, "WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers," *IEEE Secur. Priv. Symp.*, no. April, 2017.
119. A. Ben Aissa, R. K. Abercrombie, F. T. Sheldon, and A. Mili, "Quantifying the Impact of Unavailability in Cyber- Physical Environments," in *IEEE Symposium on Computational Intelligence in Cyber Security (CICS)*, 2014, pp. 1–14.
120. G. Kalogridis, M. Sooriyabandara, Z. Fan, and M. A. Mustafa, "Toward unified security and privacy protection for smart meter networks," *IEEE Syst. J.*, vol. 8, no. 2, pp. 641–654, 2014.
121. Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 4, pp. 1396–1,407, 2014.
122. A. Nourian and S. Madnick, "A systems theoretic approach to the security threats in Cyber Physical Systems applied to Stuxnet," *IEEE Trans. Dependable Secur. Comput.*, vol. PP, no. 99, pp. 1–20, 2015.
123. C. Tsigkanos, L. Pasquale, C. Ghezzi, and B. Nuseibeh, "On the Interplay Between Cyber and Physical Spaces for Adaptive Security," *IEEE Trans. Dependable Secur. Comput.*, vol. PP, no. 99, p. 1, 2016.
124. M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in industrial networks," *IEEE Trans. Ind. Informatics*, vol. 9, no. 1, pp. 277–293, 2013.
125. S. C. Muller, U. Hager, and C. Rehtanz, "A multiagent system for adaptive power flow control in electrical transmission systems," *IEEE Trans. Ind. Informatics*, vol. 10, no. 4, pp. 2290–2,299, 2014.
126. Y. Xu et al., "An Intelligent Dynamic Security Assessment Framework for Power Systems with Wind," *IEEE Trans. Ind. informatics*, no. c, 2011.
127. J. Chen and Q. Zhu, "Security as a Service for Cloud-Enabled Internet of Controlled Things under Advanced Persistent Threats: A Contract Design Approach," *IEEE Trans. Inf. Forensics Secur.*, vol. 6,013, no. c, pp. 1–1, 2017.
128. G. N. Ericsson, "Information Security for Electric Power Utilities (EPUs)—CIGRÉ Developments on Frameworks, Risk Assessment, and Technology," *IEEE Trans. Power Deliv.*, vol. 24, no. 3, pp. 1174–1,181, 2009.
129. Nian Liu, Jianhua Zhang, and Xu Wu, "Asset Analysis of Risk Assessment for IEC 61850-Based Power Control Systems—Part I: Methodology," *IEEE Trans. Power Deliv.*, vol. 26, no. 2, pp. 869–875, 2011.
130. G. N. Ericsson, "Cyber security and power system communicationessential parts of a smart grid infrastructure," *IEEE Trans. Power Deliv.*, vol. 25, no. 3, pp. 1501–1,507, 2010.
131. G. N. Ericsson, "Toward a Framework for Managing Information Security for an Electric Power Utility—CIGRÉ Experiences," *IEEE Trans. Power Deliv.*, vol. 22, no. 3, pp. 1461–1,469, 2007.
132. C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "CPI NDEX: Cyber-Physical Vulnerability Assessment for Power-Grid Infrastructures," *IEEE Trans. Smart Grid*, pp. 1–10, 2014.
133. X. Liu, M. Shahidehpour, Y. Cao, L. Wu, W. Wei, and X. Liu, "Microgrid Risk Analysis Considering the Impact of Cyber Attacks on Solar PV and ESS Control Systems," *IEEE Trans. Smart Grid*, vol. 8, no. 3, pp. 1330–1,339, 2017.
134. T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, "Petri net modeling of cyber-physical attacks on smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 741–749, 2011.
135. Y. Xiang, L. Wang, and N. Liu, "A Robustness-Oriented Power Grid Operation Strategy Considering Attacks," *IEEE Trans. Smart Grid*, vol. 3,053, no. c, pp. 1–1, 2017.
136. E. Ciapessoni, D. Cirio, G. Kjølle, S. Massucco, A. Pitto, and M. Sforna, "Probabilistic Risk-Based Security Assessment of Power Systems Considering Incumbent Threats and Uncertainties," *IEEE Trans. Smart Grid*, vol. 7, no. 6, pp. 2890–2,903, 2016.
137. X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Li, "Power System Risk Assessment in Cyber Attacks Considering the Role of Protection Systems," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 572–580, 2017.
138. T. A. Longstaff and Y. Y. Haimes, "A holistic roadmap for survivable infrastructure systems," *IEEE Trans. Syst. Man, Cybern. Part ASystems Humans.*, vol. 32, no. 2, pp. 261–268, 2002.
139. R. Paper, "Multi-Model Based Incident Prediction and Risk Assessment in Dynamic Cybersecurity Protection for Industrial Control Systems," *IEEE Trans. Syst. Man, Cybern. Syst.*, pp. 1–16, 2015.
140. C. W. Lin, Q. Zhu, C. Phung, and A. Sangiovanni-Vincentelli, "Security-aware mapping for CAN-based real-time distributed automotive systems," *IEEE/ACM Int. Conf. Comput. Des. Dig. Tech. Pap. ICCAD*, vol. 7, no. 1, pp. 115–121, 2013.
141. H. Boyes, P. Norris, and T. Watson, "Application of asset management in managing cyber security of complex systems," *IET Conf. Publ.*, vol. 2014, no. CP642, pp. 1–6, 2014.
142. Z. Li, D. Jin, C. Hannon, M. Shahidehpour, and J. Wang, "Assessing and Mitigating Cybersecurity Tisks of Traffic Light Systems in Smart Cities," *IET Cyber-Physical Syst. Theory Appl.*, vol. 1, no. 1, pp. 60–69, 2016.
143. A. Stefanov and C. C. Liu, *Cyber-physical system security and impact analysis*, vol. 19, no. 3. IFAC, 2014.
144. L. Rajbhandari and E. A. Snekkenes, *Using Game Theory to Analyze Risk to Privacy: An Initial Insight*, vol. 390 AICT. 2012.

145. A. Karantjias, N. Polemi, and S. Papastergiou, "Advanced security management system for critical infrastructures," *IISA 2014, 5th Int. Conf. Information, Intell. Syst. Appl.*, no. Cii, pp. 291–297, 2014.
146. K. Saleem, Z. Tan, and W. Buchanan, "Security for Cyber-Physical Systems in Healthcare," *Heal. 4.0 How Virtualization Big Data are Revolutionizing Healthc.*, pp. 233–251, 2017.
147. A. B. Setiawan, A. Syamsudin, and A. S. Sastrosubroto, "Information Security Governance on National Cyber Physical Systems," *Inf. Technol. Syst. Innov. (ICITSI), 2016 Int. Conf.*, 2016.
148. T. Gopal, M. Subbaraju, R. V Joshi, and S. Dey, "MAR(S)2: Methodology to articulate the requirements for security In SCADA," *Innov. Comput. Technol. (INTECH), 2014 Fourth Int. Conf.*, pp. 103–108, 2014.
149. J. Hird, R. Koelle, and D. Kolev, "Towards Mathematical Modelling in Security Risk," *Integr. Commun. Navig. Surveill. Conf. (ICNS), 2013*, no. IEEE, pp. 1–13, 2013.
150. K. Östberg, M. Törngren, F. Asplund, and M. Bengtsson, "Intelligent Transport Systems - The Role of a Safety Loop for Holistic Safety Management," in *International Conference on Computer Safety, Reliability, and Security*, pp. 3–10.
151. H. Wei, Z. Ling, G. Yajuan, and C. Hao, "Research on Information Security Testing Technology for Smart Substations," in *International Conference on Power System Technology (POWERCON 2014)*, 2014, no. Powercon, pp. 20–22.
152. Y. Xiang, L. Wang, N. Liu, R. Xiao, and K. Xie, "A Resilient Power System Operation Strategy Considering Presumned Attacks," in *International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*, 2016, pp. 3–8.
153. R. Rogers, E. Apeh, and C. J. Richardson, "Information Assurance (IA) Perspective," in *International Conference on Software, Knowledge, Information Management & Applications (SKIMA)*, 2016, pp. 110–115.
154. E. J. Byres, M. Franz, and D. Miller, "The use of attack trees in assessing vulnerabilities in SCADA systems," *Int. Infrastruct. Surviv. Work.*, pp. 1--9, 2004.
155. S. Huang, C. Zhou, S. Yang, and Y. Qin, "Cyber-physical System Security for Networked," *Int. J. Autom. Comput.*, vol. 12, no. December, pp. 567–578, 2015.
156. M. Krotofil, A. Cárdenas, J. Larsen, and D. Gollmann, "Vulnerabilities of cyber-physical systems to stale data-Determining the optimal time to launch attacks," *Int. J. Crit. Infrastruct. Prot.*, vol. 7, no. 4, pp. 213–232, 2014.
157. W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones, "A survey of cyber security management in industrial control systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 9, pp. 52–80, 2015.
158. D. Bogataj, M. Bogataj, and D. Hudoklin, "Mitigating risks of perishable products in the cyber-physical systems based on the extended MRP model," *Int. J. Prod. Econ.*, vol. 193, no. June, pp. 51–62, 2017.
159. P. A. S. Ralston, J. H. Graham, and J. L. Hieb, "Cyber security risk assessment for SCADA and DCS networks," *ISA Trans.*, vol. 46, no. 4, pp. 583–594, 2007.
160. G. a Francia, D. Thornton, and J. Dawson, "Security Best Practices and Risk Assessment of SCADA and Industrial Control Systems," *Jacksonv. State Univ. USA*, p. 36265, 2012.
161. A. Ashok, A. Hahn, and M. Govindarasu, "Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment," *J. Adv. Res.*, vol. 5, no. 4, pp. 481–489, 2014.
162. L. Zhang, Q. Wang, and B. Tian, "Security threats and measures for the cyber-physical systems," *J. China Univ. Posts Telecommun.*, vol. 20, no. SUPPL. 1, pp. 25–29, 2013.
163. S. U. N. Cong, M. A. Jianfeng, and Y. A. O. Qingsong, "On the architecture and development life cycle of secure cyber-physical systems," *J. Commun. Inf. Networks*, vol. 1, no. 4, pp. 1–21, 2016.
164. A. B. Lopez, K. Vatanparvar, A. P. Deb Nath, S. Yang, S. Bhunia, and M. A. Al Faruque, "A Security Perspective on Battery Systems of the Internet of Things," *J. Hardw. Syst. Secur.*, 2017.
165. C. G. Chittester, and Y. Y, C. G. Chittester, and Y. Y. Haimes, "Risks of Terrorism to Information Technology and to Critical Interdependent Infrastructures," *J. Homel. Secur. Emerg. Manag.*, vol. 1, no. 4, pp. 1–20, 2004.
166. I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, and S. Sezer, "STPA-SafeSec: Safety and security analysis for cyber-physical systems," *J. Inf. Secur. Appl.*, pp. 1–16, 2016.
167. Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, 2014.
168. Y. Wang, Z. Xu, J. Zhang, L. Xu, H. Wang, and G. Gu, "SRID: State relation based intrusion detection for false data injection attacks in SCADA," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8,713 LNCS, no. PART 2, pp. 401–418, 2014.
169. B. Y. J. Best, "Wake up baby': Man HACKS into 10-month-old's baby monitor to watch sleeping infant," *Mirror Online*, pp. 1–5, 2017.
170. T. K. Damenu and C. Balakrishna, "Cloud Security Risk Management: A Critical Review," *Next Gener. Mob. Appl. Serv. Technol. 2015 9th Int. Conf.*, pp. 370–375, 2015.

171. P. Maille, P. Reichl, and B. Tuffin, "Of Threats and Costs: A Game Theoretic Approach to Security Risk Management," *Perform. Model. Risk Manag. Commun. Syst.*, vol. 46, pp. 33–54, 2011.
172. J. Yan, M. Govindarasu, C.-C. Liu, and U. Vaidya, "A PMU-based risk assessment framework for power control systems," *Power Energy Soc. Gen. Meet. (PES), 2013 IEEE*, pp. 1–5, 2013.
173. G. Dondossola and R. Terruggia, *Cyber Physical Systems Approach to Smart Electric Power Grid*, vol. 79. 2015.
174. H. L. Gawand, A. K. Bhattacharjee, and K. Roy, "Online Monitoring of a Cyber Physical System Against Control Aware Cyber Attacks," *Procedia Comput. Sci.*, vol. 70, pp. 238–244, 2015.
175. E. B. Rice and A. AlMajali, "Mitigating the risk of cyber attack on smart grid systems," *Procedia Comput. Sci.*, vol. 28, no. Cser, pp. 575–582, 2014.
176. Z. DeSmit, A. E. Elhabashy, L. J. Wells, and J. A. Camelio, "Cyber-physical Vulnerability Assessment in Manufacturing Systems," *Procedia Manuf.*, vol. 5, pp. 1060–1,074, 2016.
177. W. Z. Khan, H. M. Zangoti, M. Y. Aalsalem, M. Zahid, and Q. Arshad, "Mobile RFID in Internet of Things: Security attacks, privacy risks, and countermeasures," *Proceeding - 2016 Int. Conf. Radar, Antenna, Microwave, Electron. Telecommun. ICRAMET 2016*, pp. 36–41, 2017.
178. T. B. Rasmussen, G. Yang, and A. H. Nielsen, "A Review of Cyber-Physical Energy System Security Assessment," in *Proceeding-12th IEEE Power and Energy Society PowerTech Conference*, 2017.
179. J. Hird, M. Hawley, and C. Machin, "Air Traffic Management Security Research in SESAR.," in *Proceedings - 11th International Conference on Availability, Reliability and Security (ARES)*, 2016, pp. 486–492.
180. D. Kostopoulos, G. Leventakis, V. Tsoulkas, and N. Nikitakos, "An intelligent fault monitoring and risk management tool for complex critical infrastructures: The SERSCIS approach in air-traffic surface control," *Proc. - 2012 14th Int. Conf. Model. Simulation, UKSim 2012*, pp. 205–210, 2012.
181. F. Xie, T. Lu, X. Guo, J. Liu, Y. Peng, and Y. Gao, "Security analysis on cyber-physical system using attack tree," *Proc. - 2013 9th Int. Conf. Intell. Inf. Hiding Multimed. Signal Process. IIH-MSP 2013*, pp. 429–432, 2013.
182. A. Kovacs, I. Karakatsanis, and D. Svetinovic, "Argumentation-based security requirements analysis: Bitmessage case study," *Proc. - 2014 IEEE Int. Conf. Internet Things, iThings 2014, 2014 IEEE Int. Conf. Green Comput. Commun. GreenCom 2014 2014 IEEE Int. Conf. Cyber-Physical-Social Comput. CPS 20*, no. iThings, pp. 408–414, 2014.
183. L. Vegh and L. Miclea, "A simple scheme for security and access control in cyber-physical systems," *Proc. - 2015 20th Int. Conf. Control Syst. Comput. Sci. CSCS 2015*, pp. 294–299, 2015.
184. S. Jauhar et al., "Model-Based Cybersecurity Assessment with NESCOR Smart Grid Failure Scenarios," *Proc. - 2015 IEEE 21st Pacific Rim Int. Symp. Dependable Comput. PRDC 2015*, pp. 319–324, 2016.
185. D. Di Marco, J. Hird, A. Manzo, and M. Ivaldi, "Security Testing with controller-pilot data link communications," *Proc. - 2016 11th Int. Conf. Availability, Reliab. Secur. ARES 2016*, pp. 526–531, 2016.
186. A. Boddy, W. Hurst, M. Mackay, and A. El Rhalibi, "A Study into Detecting Anomalous Behaviours within HealthCare Infrastructures," *Proc. - 2016 9th Int. Conf. Dev. eSystems Eng. DeSE 2016*, pp. 111–117, 2017.
187. J. C. Talwana and H. J. Hua, "Smart World of Internet of Things (IoT) and Its Security Concerns," *Proc. - 2016 IEEE Int. Conf. Internet Things; IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016*, pp. 240–245, 2017.
188. S. Green, I. Cicek, and C. K. Koc, "Continuous-Time Computational Aspects of Cyber-Physical Security," *Proc. - 2016 Work. Fault Diagnosis Toler. Cryptogr. FDTC 2016*, pp. 59–62, 2016.
189. G. Settanni, Y. Shovgenya, F. Skopik, R. Graf, M. Wurzenberger, and R. Fiedler, "Acquiring Cyber Threat Intelligence through Security Information Correlation," in *Proceedings - 3rd International Conference on Cybernetics (CYBCONF)*, 2017, pp. 1–7.
190. B. Genge, A. Beres, and P. Haller, "A survey on cloud-based software platforms to implement secure smart grids," *Proc. - 49th Int. Conf. Univ. Power Eng.*, 2014.
191. J. Yao, P. Venkitasubramaniam, S. Kishore, L. V. Snyder, and R. S. Blum, "Network Topology Risk Assessment of Stealthy Cyber Attacks on Advanced Metering Infrastructure Networks," *Proc. - 51st Annu. Conf. Inf. Sci. Syst.*, 2017.
192. W. Jiang, W. Guo, and N. Sang, "Periodic real-time message scheduling for confidentiality-aware cyber-physical system in wireless networks," *Proc. - 5th Int. Conf. Front. Comput. Sci. Technol. FCST 2010*, pp. 355–360, 2010.
193. J. Aagedal, F. Den Braber, T. Dimitrakos, B. A. Gran, D. Raptis, and K. Stolen, "Model-based risk assessment to improve enterprise security," *Proc. - 6th Int. Enterp. Distrib. Object Comput. Conf.*, vol. 2002–Janua, no. January, pp. 51–62, 2002.
194. P. Dong, Y. Han, X. Guo, and F. Xie, "A Security and Safety Framework for Cyber Physical System," *Proc. - 7th Int. Conf. Control Autom. CA 2014*, pp. 49–51, 2014.
195. K. Zhao and L. Ge, "A survey on the internet of things security," *Proc. - 9th Int. Conf. Comput. Intell. Secur. CIS 2013*, pp. 663–667, 2013.

196. [196]C. Xia et al., "An Efficient Tool for Industrial Control System Security Analysis.," in *Proceedings - Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), 2016 IEEE 14*, 2016, pp. 424–427.
197. M. Uslar, C. Rosinger, and S. Schlegel, "Security by design for the smart grid: Combining the SGAM and NISTIR 7628," *Proc. - IEEE 38th Annu. Int. Comput. Softw. Appl. Conf. Work. COMPSACW 2014*, pp. 110–115, 2014.
198. W. Gavins and J. Hemenway, "Cybersecurity: A joint terminal engineering office perspective," *Proc. - IEEE Mil. Commun. Conf. MILCOM*, pp. 918–923, 2010.
199. I. A. Tøndel, M. B. Line, and G. Johansen, "Assessing Information Security Risks of AMI - What Makes it so Difficult?.," in *Proceedings - International Conference on Information Systems Security and Privacy (ICISSP)*, 2015, no. 217528, pp. 56–63.
200. Y. Wang, Z. Yan, and J. Wang, "The cross space transmission of cyber risks in electric cyber-physical systems," *Proc. - Int. Conf. Nat. Comput.*, vol. 2016–Janua, pp. 1275–1,279, 2016.
201. C. Tsigkanos, L. Pasquale, C. Ghezzi, and B. Nuseibeh, "Ariadne: Topology Aware Adaptive Security for Cyber-Physical Systems," *Proc. - Int. Conf. Softw. Eng.*, vol. 2, pp. 729–732, 2015.
202. A. Giani, S. Sastry, K. H. Johansson, and H. Sandberg, "The VIKING project: An initiative on resilient control of power networks," *Proc. - ISRCS 2009-2nd Int. Symp. Resilient Control Syst.*, pp. 31–35, 2009.
203. R. W. Y. Habash, V. Groza, D. Krewski, and G. Paoli, "A Risk Assessment Framework for the Smart Grid," in *Proceedings- IEEE Electrical Power & Energy Conference (EPEC)*, 2013.
204. J. Guan, J. H. Graham, and J. L. Hieb, "A digraph model for risk identification and mangement in SCADA systems," *Proc. 2011 IEEE Int. Conf. Intell. Secur. Informatics, ISI 2011*, pp. 150–155, 2011.
205. P. R. Dunaka and B. McMillin, "Cyber-physical security of a chemical plant," *Proc. IEEE Int. Symp. High Assur. Syst. Eng.*, no. 60, pp. 33–40, 2017.
206. I. Bouij-Pasquier, A. Ait Ouahman, A. Abou El Kalam, and M. Ouabiba De Montfort, "SmartOrBAC security and privacy in the Internet of Things," *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. AICCSA*, vol. 2016–July, 2016.
207. T. D. Atmaja and F. Fitriana, "Cyber security strategy for future distributed energy delivery system," *Proc. 2011 Int. Conf. Electr. Eng. Informatics*, no. July, pp. 1–6, 2011.
208. N. Enose, "Implementing an integrated security management framework to ensure a secure smart grid," *Proc. 2014 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2014*, pp. 778–784, 2014.
209. A. Bialas, "Experimentation tool for critical infrastructures risk management," *Proc. 2015 Fed. Conf. Comput. Sci. Inf. Syst.*, vol. 5, pp. 1099–1,106, 2015.
210. K. Lin and K. E. Holbert, "PRA for vulnerability assessment of power system infrastructure security," *Proc. 37th Annu. North Am. Power Symp. 2005*, vol. 2005, pp. 43–51, 2005.
211. S. Jaiswal and D. Gupta, "Security Requirements for Internet of Things (IOT)," *Proc. 6th Int. Conf. Commun. Syst. Networks*, pp. 419–427, 2014.
212. H. Abie and I. Balasingham, "Risk-Based Adaptive Security for Smart IoT in eHealth," *Proc. 7th Int. Conf. Body Area Networks*, no. SeTTIT, pp. 269–275, 2012.
213. C. Pak, "The near real time statistical asset priority driven (nrtsapd) risk assessment methodology," *Proc. 9th ACM SIGITE Conf. Inf. Technol. Educ.*, no. 443, pp. 105–112, 2008.
214. Y. Soupionis, R. Piccinelli, and T. Benoist, "Cyber Security Impact on Power Grid Including Nuclear Plant," *Proc. Fed. Conf. Comput. Sci. Inf. Syst.*, vol. 8, pp. 767–773, 2016.
215. S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, 2012.
216. A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, "Ensuring safety, security, and sustainability of mission-critical cyber-physical systems," *Proc. IEEE*, vol. 100, no. 1, pp. 283–299, 2012.
217. F. Li, Z., Shahidehpour, M., and Aminifar, "Cybersecurity in Distributed Power Systems," *Proc. IEEE*, vol. PP, no. 99, pp. 1–22, 2017.
218. Z. Xu and Q. Zhu, "A cyber-physical game framework for secure and resilient multi-agent autonomous systems," *Proc. IEEE Conf. Decis. Control*, vol. 2016–Febru, no. Cdc, pp. 5156–5,161, 2011.
219. B. Min and V. Varadharajan, "Design and analysis of security attacks against critical smart grid infrastructures," *Proc. IEEE Int. Conf. Eng. Complex Comput. Syst. ICECCS*, pp. 59–68, 2014.
220. A. Motii, B. Hamid, A. Lanusse, and J. M. Bruel, "Guiding the Selection of Security Patterns for Real-Time Systems," *Proc. IEEE Int. Conf. Eng. Complex Comput. Syst. ICECCS*, pp. 155–164, 2017.
221. J. Dagle, "Vulnerability assessment activities," *Proc. IEEE Power Eng. Soc. Transm. Distrib. Conf.*, vol. 1, no. WINTER MEETING, pp. 108–113, 2001.

222. T. Zhao, D. Wang, D. Lu, Y. Zeng, and Y. Liu, "A Risk Assessment Method for Cascading Failure Caused by Electric Cyber-Physical System (ECPS)," in Proceedings-5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies, 2015, pp. 5–9.
223. E. Zio, "Challenges in the vulnerability and risk analysis of critical infrastructures," Reliab. Eng. Syst. Saf., vol. 152, pp. 137–150, 2016.
224. K. Beckers et al., "Author' s Accepted Manuscript A Structured Hazard Analysis and Risk Assessment Study Reference: To appear in: Reliability Engineering and System Safety Method for Automotive Systems - A Descriptive Study," Reliab. Eng. Syst. Saf., 2016.
225. T. Aven, "A unified framework for risk and vulnerability analysis covering both safety and security," Reliab. Eng. Syst. Saf., vol. 92, no. 6, pp. 745–754, 2007.
226. R. Arghandeh, A. Von Meier, L. Mehrmanesh, and L. Mili, "On the definition of cyber-physical resilience in power systems," Renew. Sustain. Energy Rev., vol. 58, pp. 1060–1,069, 2016.
227. H. Guo, C. Zheng, H. H.-C. Iu, and T. Fernando, "A critical review of cascading failure analysis and modeling of power system," Renew. Sustain. Energy Rev., vol. 80, no. May, pp. 9–22, 2017.
228. L. E. Jones, J. Dumas, and D. Maggio, "Renewable Energy Integration," Renew. Energy Integr., pp. 117–124, 2014.
229. H. Abdo, M. Kaouk, J. Flaus, and F. Masse, "A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie - combining new version of attack tree with bowtie analysis," Comput. Secur., 2017.
230. Y. Hu, A. Yang, H. Li, Y. Sun, and L. Sun, "A survey of intrusion detection on industrial control systems," Int. J. Distrib. Sens. Networks, vol. 14, no. 8, 2018.
231. N. Y. Kim, S. Rathore, J. H. Ryu, J. H. Park, and J. H. Park, "A Survey on Cyber Physical System Security for IoT: Issues, Challenges, Threats, Solutions," J. Inf. Process. Syst., vol. 14, no. 6, pp. 1361–1,384, 2018.
232. E. Lisova, A. Cauˇ, H. Thane, and H. Hansson, "A Systematic Way to Incorporate Security in Safety Analysis," 2018 48th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Networks Work., pp. 166–171, 2018.
233. S. ur Rehman and V. Gruhn, "An Effective Security Requirements Engineering Framework for Cyber-Physical Systems," Technologies, vol. 3, pp. 1–20, 2018.
234. H. I. Kure, S. Islam, and M. A. Razzaque, "An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System," Appl. Sci., vol. 8, pp. 1–29, 2018.
235. K. M. A. Yousef, A. Almajail, S. Abu Ghalyon, W. Dweik, and B. J. Mohd, "Analyzing Cyber-Physical Threats on Robotic Platform," Sensors, vol. 5, pp. 1–22, 2018.
236. K. Huang, C. Zhou, Y. Tian, S. Yang, and Y. Qin, "Assessing the Physical Impact of Cyber-Attacks on Industrial Cyber-Physical Systems," IEEE Trans. Ind. Electron., vol. 0046, no. c, 2018.
237. K. Tam and K. Jones, "Cyber-Risk Assessment for Autonomous Ships," in International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 2018, pp. 1–8.
238. S. Park et al., "Design and Implementation of a Smart IoT Based Building and Town Disaster Management System in Smart City Infrastructure," Appl. Sci., vol. 11, 2018.
239. M. Zahid, I. Inayat, A. Mashkoor, and Z. Mehmood, "Security Risk Mitigation of Cyber Physical Systems: A Case Study of a Flight Simulator Maryam," in International Conference on Database and Expert Systems Applications, 2019, pp. 129–138.
240. M. Zahid, I. Inayat, M. Daneva, and Z. Mehmood, "A security risk mitigation framework for cyber physical systems," J. Softw. Evol. Process., vol. Special Is, no. June, pp. 1–15, 2019.
241. S. Ali, T. Al Balushi, Z. Nadir, and O. K. Hussain, "Embedded systems security for cyber-physical systems," Stud. Comput. Intell., vol. 768, pp. 115–140, 2018.
242. A. Ceccarelli and T. Zoppi, "Threat Analysis in Systems-of-Systems: An Emergence-Oriented Approach," ACM Trans. Cyber-Physical Syst., vol. 3, no. 2, pp. 1–24, 2018.
243. Y. Fan, J. Li, D. Zhang, J. Pi, J. Song, and G. Zhao, "Supporting Sustainable Maintenance of Substations under Cyber-Threats: An Evaluation Method of Cybersecurity Risk for Power CPS," Sustainability, vol. 11, pp. 1–30, 2019.
244. M. Z. A. Bhuiyan, G. J. Anders, J. Philhower, and S. Du, "Review of static risk-based security assessment in power system," IET Cyber-Physical Syst. Theory Appl., vol. 4, no. 3, pp. 233–239, 2019.
245. F. G. Birleanu et al., "Resilience Enhancement of Cyber-Physical Systems: A Review," in Power System Resilience, 2019, pp. 269–287.
246. J. Xu, L. Wei, W. Wu, A. Wang, Y. Zhang, and F. Zhou, "Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber–physical system," Futur. Gener. Comput. Syst., 2018.
247. M. MacKintosh, G. Epiphaniou, H. Al-Khateeb, K. Burnham, P. Pillai, and M. Hammoudeh, "Preliminaries of orthogonal layered defence using functional and assurance controls in industrial control systems," J. Sens. Actuator Networks, vol. 8, no. 1, 2019.
248. A. Badri, B. Boudreau-Trudel, and A. S. Souissi, "Occupational health and safety in the industry 4.0 era: A cause for major concern?," Saf. Sci., vol. 109, no. May, pp. 403–411, 2018.

249. D. Miehle, B. Häckel, S. Pfosser, and J. Übelhör, "Modeling IT Availability Risks in Smart Factories: A Stochastic Petri Nets Approach," *Bus. Inf. Syst. Eng.*, 2019.
250. N. Nikolakis, V. Maratos, and S. Makris, "A cyber physical system (CPS) approach for safe human-robot collaboration in a shared workplace," *Robot. Comput. Integr. Manuf.*, vol. 56, no. October 2018, pp. 233–243, 2019.
251. N. Nikolakis, V. Maratos, and S. Makris, "A cyber physical system (CPS) approach for safe human-robot collaboration in a shared workplace," *Robot. Comput. Integr. Manuf.*, vol. 56, no. October 2018, pp. 233–243, 2019.
252. L. Deka, S. M. Khan, M. Chowdhury, and N. Ayres, *Transportation Cyber-Physical System and its importance for future mobility*. Elsevier Inc., 2018.
253. R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," *Comput. Ind.*, vol. 100, no. April, pp. 212–223, 2018.
254. R. Raval, A. Maskus, B. Saltmiras, M. Dunn, P. J. Hawrylak, and J. Hale, "Competitive Learning Environment for Cyber-Physical System Security Experimentation," in *1st International Conference on Data Intelligence and Security Competitive*, 2018, pp. 211–218.
255. Y. Hou, J. Such, and A. Rashid, "Understanding Security Requirements for Industrial Control System Supply Chains," *Proc. - 2019 IEEE/ACM 5th Int. Work. Softw. Eng. Smart Cyber-Physical Syst. SEsCPS 2019*, pp. 50–53, 2019.
256. G. Stergiopoulos, D. Gritzalis, and V. Kouktzoglou, "Using formal distributions for threat likelihood estimation in cloud-enabled IT risk assessment," *Comput. Networks*, vol. 134, pp. 23–45, 2018.
257. M. Zhang, S. Ali, T. Yue, R. Norgren, and O. Okariz, "Uncertainty-Wise Cyber-Physical System test modeling," *Softw. Syst. Model.*, vol. 18, no. 2, pp. 1379–1,418, 2019.
258. Z. Kan and X. Wang, "The design of remote monitoring and warning system for dangerous chemicals based on CPS," *J. Inf. Process. Syst.*, vol. 15, no. 3, pp. 632–644, 2019.
259. A. Khalid, P. Kirisci, Z. H. Khan, Z. Ghrairi, K. D. Thoben, and J. Pannek, "Security framework for industrial collaborative robotic cyber-physical systems," *Comput. Ind.*, vol. 97, pp. 132–145, 2018.
260. R. K. Kaur, L. K. Singh, and B. Pandey, "Security Analysis of Smart Grids: Successes and Challenges," *IEEE Consum. Electron. Mag.*, vol. 8, no. 2, pp. 10–15, 2019.
261. X. Lyu, Y. Ding, and S. H. Yang, "Safety and security risk assessment in cyberphysical systems," *IET Cyber-Physical Syst. Theory Appl.*, vol. 4, no. 3, pp. 221–232, 2019.
262. B. T. Carter, G. Bakirtzis, C. R. Elks, and C. H. Fleming, "A systems approach for eliciting mission-centric security requirements," in *12th Annual IEEE International Systems Conference, SysCon*, 2018, pp. 1–8.
263. S. H. Bouk, S. H. Ahmed, R. Hussain, and Y. Eun, "Named Data Networking's Intrinsic Cyber-Resilience for Vehicular CPS," *IEEE Access*, vol. 6, no. c, pp. 60570–60,585, 2018.
264. A. Gawanmeh and A. Alomari, "Taxonomy analysis of security aspects in cyber physical systems applications," in *IEEE International Conference on Communications Workshops, ICC Workshops 2018 - Proceedings*, 2018, pp. 1–6.
265. R. Fernandes, P. Benjamin, B. Li, A. Stephenson, M. Patel, and J. Hwang, "Use of Topological Vulnerability Analysis for Cyberphysical Systems," *Proc. IEEE Natl. Aerosp. Electron. Conf. NAECON*, vol. 2018-July, pp. 78–81, 2018.
266. S. A. P. Kumar and B. Xu, "Vulnerability Assessment for Security in Aviation Cyber-Physical Systems," *Proc. - 4th IEEE Int. Conf. Cyber Secur. Cloud Comput. CSCloud 2017 3rd IEEE Int. Conf. Scalable Smart Cloud, SSC 2017*, no. 1, pp. 145–150, 2017.
267. M. Rocchetto and N. O. Tippenhauer, "Towards formal security analysis of industrial control systems," *ACM Asia Conf. Comput. Commun. Secur.*, pp. 114–126, 2017.
268. A. Riel, C. Kreiner, G. Macher, and R. Messnarz, "Integrated design for tackling safety and security challenges of smart products and digital manufacturing," *CIRP Ann. - Manuf. Technol.*, vol. 66, no. 1, pp. 177–180, 2017.
269. T. Wang, Q. Su, and T. Chen, "Formal Analysis of Security Properties of Cyber-Physical System Based on Timed Automata," *Proc. - 2017 IEEE 2nd Int. Conf. Data Sci. Cyberspace, DSC 2017*, pp. 534–540, 2017.
270. D. P. Zegzhda and E. Y. Pavlenko, "Cyber-physical system homeostatic security management," *Autom. Control Comput. Sci.*, vol. 51, no. 8, pp. 805–816, 2017.
271. A. A. Jillepalli et al., "METICS: A Holistic Cyber Physical System Model for IEEE 14-bus Power System Security," in *13th International Conference on Malicious and Unwanted Software: "Know Your Enemy" (MALWARE)*, 2018, pp. 95–102.
272. R. Fu, X. Huang, Y. Xue, Y. Wu, Y. Tang, and D. Yue, "Security Assessment for Cyber Physical Distribution Power System under Intrusion Attacks," *IEEE Access*, vol. 7, no. c, pp. 75615–75,628, 2018.
273. I. Kotenko, S. Ageev, and I. Saenko, "Implementation of intelligent agents for network traffic and security risk analysis in cyber-physical systems," in *ACM 11th International Conference on Security of Information and Networks*, 2018, pp. 10–13.
274. Y. Wadhawan and C. Neuman, "RL-BAGS: A tool for smart grid risk assessment," in *International Conference on Smart Grid and Clean Energy Technologies*, 2018, pp. 7–14.

275. H. Huang and K. Davis, "Power System Equipment Cyber-Physical Risk Assessment Based on Architecture and Critical Clearing Time," in *IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, SmartGridComm 2018*, 2018, pp. 1–6
276. X. Zhang and D. Zhang, "Quantitative Risk Assessment of Cyber Ohysical Power System Using Bayesian Based on Petri Net," in *5th IEEE International Conference on Cloud Computing and Intelligence Systems*, 2018, pp. 988–992.
277. Z. Qu, Y. Zhang, N. Qu, L. Wang, Y. Li, and Y. Dong, "Method for Quantitative Estimation of the Risk Propagation Threshold in Electric Power CPS Based on Seepage Probability," *IEEE Access*, vol. 6, pp. 68813–68,823, 2018.
278. A. Riel, C. Kreiner, R. Messnarz, and A. Much, "An architectural approach to the integration of safety and security requirements in smart products and systems design," *CIRP Ann. - Manuf. Technol.*, vol. 67, no. 1, pp. 173–176, 2018.
279. C. C. Sun, A. Hahn, and C. C. Liu, "Cyber security of a power grid: State-of-the-art," *Electr. Power Energy Syst.*, vol. 99, no. November 2017, pp. 45–56, 2018.
280. G. Bakirtzis, B. T. Carter, C. R. Elks, and C. H. Fleming, "A model-based approach to security analysis for cyber-physical systems," in *12th Annual IEEE International Systems Conference, SysCon*, 2018, pp. 1–8.
281. J. P. Monteuuis, A. Boudguiga, J. Zhang, H. Labiod, A. Servel, and P. Urien, "SARA: Security automotive risk analysis method," 2018.
282. E. Zio, "The future of risk assessment," *Reliab. Eng. Syst. Saf.*, vol. 177, no. March, pp. 176–190, 2018.
283. S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A systems and control perspective of CPS security," *Annu. Rev. Control*, vol. 47, pp. 394–411, 2019.
284. D. Jurgen, C. Schmittner, M. Krisper, and G. Macher, "Towards Integrated Quantitative Security and Safety Risk Assessment," in *International Conference on Computer Safety, Reliability, and Security*, 2019, vol. 1, pp. 102–116.
285. I. A. Oyewumi et al., "ISAAC: The Idaho CPS smart grid cybersecurity testbed," in *IEEE Texas Power and Energy Conference*, 2019, pp. 1–6.
286. Á. J. Varela-Vaca, L. Parody, R. M. Gasca, and M. T. Gómez-López, "Automatic Verification and Diagnosis of Security Risk Assessments in Business Process Models," *IEEE Access*, vol. 7, pp. 26448–26,465, 2019.
287. J. Dsouza, L. Elezabeth, V. P. Mishra, and R. Jain, "Security in Cyber-Physical Systems," in *Amity International Conference on Artificial Intelligence (AICAI)*, 2019, pp. 840–844.
288. Y. L. Huang, W. L. Sun, and Y. H. Tang, "3aRAM: A 3-Layer AHP-Based Risk Assessment Model and its Implementation for an Industrial IoT Cloud," in *19th IEEE International Conference on Software Quality, Reliability and Security*, 2019, pp. 450–457.
289. S. Walker-Roberts, M. Hammoudeh, O. Aldabbas, M. Aydin, and A. Dehghantanha, "Threats on the horizon: understanding security threats in the era of cyber-physical systems," *J. Supercomput.*, no. 0123456789, 2019.
290. L. Babun, H. Aksu, and A. S. Uluagac, "A system-level behavioral detection framework for compromised CPS devices: Smart-grid case," *ACM Trans. Cyber-Physical Syst.*, vol. 4, no. 2, 2019.
291. C. Sharma, R. Sinha, and P. Leitao, "IASelect: Finding best-fit agent practices in industrial CPS using graph databases," *IEEE Int. Conf. Ind. Informatics*, vol. 2019-July, pp. 1558–1,563, 2019.
292. A. Carelli, A. Vallero, and S. Di Carlo, "Performance monitor counters: Interplay between safety and security in complex cyber-physical systems," *IEEE Trans. Device Mater. Reliab.*, vol. 19, no. 1, pp. 73–82, 2019.
293. H. Pearce, S. Pinisetty, P. S. Roop, M. M. Y. Kuo, and A. Ukil, "Smart I/O modules for mitigating cyber-physical attacks on industrial control systems," *IEEE Trans. Ind. Informatics*, no. c, pp. 1–11, 2019.
294. L. Gressl, C. Steger, and U. Neffe, "Security driven design space exploration for embedded systems," in *Forum on Specification and Design Languages*, 2019, no. i, pp. 1–8.
295. B. K. Chejerla and S. K. Madria, "Information fusion architecture for secure cyber physical systems," *Comput. Secur.*, vol. 85, pp. 122–137, 2019.
296. C. Orellana, M. M. Villegas, and H. Astudillo, "Mitigating security threats through the use of security tactics to design secure cyber-physical systems (CPS)," in *13th European Conference on Software Architecture*, 2019, pp. 109–115.
297. R. Gifty, R. Bharathi, and P. Krishnakumar, "Privacy and security of big data in cyber physical systems using Weibull distribution-based intrusion detection," *Neural Comput. Appl.*, vol. 31, pp. 23–34, 2019.
298. Ai Gu, Z. Yin, *C. cui*, and Y. Li, "Integrated Functional Safety and Security Diagnosis Mechanism of CPS Based on Blockchain," *IEEE Access*, vol. 8, pp. 15241–15,255, 2020.
299. B. Potteiger, Z. Zhang, and X. Koutsoukos, "Integrated moving target defense and control reconfiguration for securing Cyber-Physical systems," *Microprocess. Microsyst.*, vol. 73, p. 102954, 2020.
300. H. Martin et al., "Combined automotive safety and security pattern engineering approach," *Reliab. Eng. Syst. Saf.*, vol. 198, 2020.
301. H. E. Garcia, S. E. Aumeier, A. Y. Al-Rashdan, and B. L. Rolston, "Secure embedded intelligence in nuclear systems: Framework and methods," *Ann. Nucl. Energy*, vol. 140, p. 107261, 2020.
302. A. S. Poonia, C. Banerjee, A. Banerjee, and S. K. Sharma, "Interpreting the Objective Outcome of the Proposed Misuse Case Oriented Quality Requirements (MCOQR) Framework Metrics for Security Quantification," in *Performance and its Applications of Integrated Systems Management in Software Engineering*, 2020, pp. 101–106.

303. G. Kavallieratos, S. Katsikas, and V. Gkioulos, "SafeSec Tropos: Joint security and safety requirements elicitation," *Comput. Stand. Interfaces*, vol. 70, p. 103429, 2020.
304. J. Hu, S. Guo, X. Kuang, F. Meng, D. Hu, and Z. Shi, "I-HMM-Based Multidimensional Network Security Risk Assessment," *IEEE Access*, vol. 8, pp. 1431–1,442, 2020.
305. M. T. Khan, D. Serpanos, and H. Shrobe, "Run-Time Security Assurance of Cyber Physical System Applications," *Embed. Cyber-Physical, IoT Syst.*, pp. 79–88, 2020.
306. N. Chaudhry, M. M. Yousaf, and M. T. Khan, "Security assessment of data management systems for cyber physical system applications," *J. Softw. Evol. Process*, vol. 32, no. 2, pp. 1–19, 2020.
307. M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," *Arab. J. Sci. Eng.*, no. 0123456789, 2020.
308. S. Nateghi, Y. Shtessel, J. P. Barbot, and C. Edwards, "Cyber Attack Reconstruction of Nonlinear Systems via Higher-Order Sliding-Mode Observer and Sparse Recovery Algorithm," in *IEEE Conference on Decision and Control*, 2018, vol. 2018-Decem, no. Cdc, pp. 5963–5,968.
309. S. U. Rehman, C. Allgaier, and V. Gruhn, "Security requirements engineering: A framework for cyber-physical systems," in *International Conference on Frontiers of Information Technology*, 2018, pp. 315–320.
310. F. Asplund, J. McDermid, R. Oates, and J. Roberts, "Rapid Integration of CPS Security and Safety," *IEEE Embed. Syst. Lett.*, vol. 11, no. 4, pp. 111–114, 2019.
311. M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Networks*, vol. 169, p. 107094, 2020.
312. M. Zahid, I. Inayat, and F. Allah Bukhsh, "Towards Mitigating Security Risks in Cyber Physical System", "Euromicro Conference on Software Engineering and Applications", 2018.