Received: 5 January 2024 | Revised: 24 April 2024 | Accepted: 23 May 2024

IET Cyber-Physical Systems: Theory & Applications

DOI: 10.1049/cps2.12095

REVIEW

Joint safety and security risk analysis in industrial cyber-physical systems: A survey

Zhicong Sun[1,2] | **Guang Chen**[3,4] | **Yulong Ding**[4,5] | **Shuang-Hua Yang**[4,6]

[1]Department of Civil and Environmental Engineering, Hong Kong Polytechnic University, Hong Kong SAR, China

[2]Institute of Advanced Computing and Digital Engineering, Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences, Shenzhen, China

[3]Department of Mechanical and Energy Engineering, Southern University of Science and Technology, Shenzhen, China

[4]Shenzhen Key Laboratory of S&S for Next Generation of Industrial Internet, Southern University of Science and Technology, Shenzhen, China

[5]Department of Computer Science and Engineering, Southern University of Science and Technology, Shenzhen, China

[6]Department of Computer Science, University of Reading, Reading, UK

Correspondence

Shuang-Hua Yang.
Email: shuang-hua.yang@reading.ac.uk

Funding information

Educational Commission of Guangdong Province, Grant/Award Number: 2019KZDZX1018; Shenzhen Science and Technology Program, Grant/Award Numbers: GJHZ20210705141808024, ZDSYS20210623092007023; National Natural Science Foundation of China, Grant/Award Numbers: 92067109, 61873119, 62211530106

Abstract

Industrial Cyber-Physical Systems (iCPSs) represent a new generation of industrial systems that enable a profound integration of industrial processes and informational spaces, thereby empowering the fourth industrial revolution. iCPSs confront more severe safety and security (S&S) challenges compared to traditional industrial systems. One of the most critical challenges is the joint risk analysis of S&S. Many scholars have devoted their research to this area. However, there is a dearth of literature reviews encapsulating recent advancements, which provides the motivation for this study. The authors review the methodologies in this field, delve into the S&S relationships involved, and propose 12 criteria for evaluating these methods. Furthermore, the current research limitations were analysed and potential directions were suggested for future research.

KEYWORDS

computer network security, cyber-physical systems, risk analysis, safety systems

1 | INTRODUCTION

With the advancement of Information Technology (IT), Communication Technology (CT), and Operational Technology (OT), an increasing number of industrial devices are being interconnected, evolving into industrial Cyber-Physical Systems (iCPSs) [1]. Serving as the foundation of the new industrial revolution [2], iCPSs monitor industrial devices in real-time, abstracting information from industrial processes to the information space. Here, they conduct intelligent evaluation, forward prediction, and decision-making, and ultimately control industrial devices. While offering real-time capability, component interaction, and dynamic system configuration, they also present amplified safety and security (S&S) challenges compared to traditional industrial systems.

One of the principal challenges encountered involves the collaborative analysis of S&S. While safety equips iCPSs to handle hazards, such as component failures and explosions, security shields iCPSs from threats like cyberattacks [3, 4, 4, 5]. Traditionally, S&S serve iCPSs and are analysed separately to ensure reliable system operation. However, the interconnected nature of iCPSs renders the weak integration of S&S unreliable, which has been revealed in incidents resulting from cyberattacks, such as Stuxnet (2010) [6], Duqu (2011) [7], and Wannacry (2017) [8]. These attacks not only infringed on data privacy, but also exploited security vulnerabilities to impair critical safety-related physical devices, making scholars recognise that S&S risk analysis are intertwined, mutually influential, and necessitate simultaneous consideration [1, 9–13].

Substantial research has been undertaken towards the collective analysis of S&S risks for iCPSs. These efforts span a range of subjects, including risk identification [14–18], risk assessment [19–24], risk management [15, 25], lifecycle integration [4], and requirements engineering [12, 26–28].

Numerous studies in the field have examined these literature, which comprises review papers focussing on safety [29, 30], security [31–35], as well as those addressing both domains [13, 36–41]. However, there remains a research gap in reviewing the latest methodological approach to joint S&S risk analysis within the field of iCPSs, which this paper aims to address.

In this context, the purpose of this paper is to make an overall assessment of the up-to-date research status of methods aiming to joint S&S risk analysis for iCPSs. In addition to summarising recent work, this article offers three main contributions. First, the four relationships of S&S, namely independence, conditional dependence, mutual reinforcement, and antagonism, are explored in greater depth, and existing work is classified in detail according to these relationships. Secondly, 12 criteria are summarised and adopted for evaluating existing methods. Lastly, the current state of research is summarised and the potential study directions are identified.

The remainder of this paper unfolds as follows: Section 2 delves extensively into the four relationships between S&S and provides a brief review of existing methods that take these relationships into account. Section 3 meticulously details the extant methodologies for the joint S&S risk analysis, discussing their merits and constraints. Section 4 introduces 12 criteria for evaluating S&S risk analysis methods, presents the corresponding analysis results, and canvasses potential limitations and prospects for future research. Finally, Section 5 summarises this work and highlights promising research directions for future research.

2 | RELATIONSHIPS BETWEEN S&S

In order to propose improved methodologies for joint S&S risk analysis throughout the system lifecycle, it is crucial to explore the relationships between these two domains. Numerous authors have discussed the similarities and differences between S&S, including [17, 42–44]. S&S share a common aim of addressing undesirable events within the system and engage in overlapping tasks, such as identifying, analysing, assessing, and mitigating risks. However, S&S also have distinct areas given the different risk sources they manage. That is, security addresses threats while safety handles hazards. Furthermore, beyond their similarities and differences, S&S have more intricate interdependencies that can influence their synergy, namely, independence, conditional dependence, mutual reinforcement, and antagonism [13] as illustrated in Figure 1. These relationships should be considered during the complete lifecycle, that is, design, development, and maintenance. The subsequent section elucidates each relationship and introduces studies addressing each specific type of relationship.

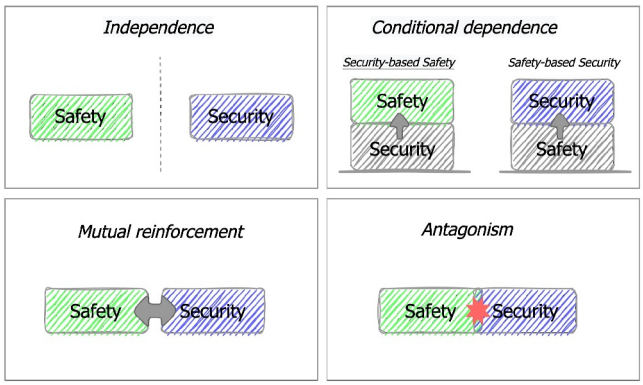

FIGURE 1 Relationships between S&S.

2.1 | Independence

Independence implies that S&S do not consider influence on each other, either at the requirement or strategy level. In this context, safety requirements or measures primarily aim to bolster process safety, without taking security factors into account directly, as exemplified by explosion-proof measures. Conversely, security requirements or measures focus predominantly on enhancing information security. This includes requirements such as denying access to critical industrial data and implementing measures to detect cyber-attacks, all while not directly considering the impact on safety.

Safety risk analysis methodologies primarily fall into two categories based on the perceived underlying causes of failures. The first category, including methods such as Fault Tree Analysis (FTA) [45], Event Tree Analysis (ETA) [46], Bow-Tie Analysis (BTA) [47], Failure Mode and Effects Analysis (FMEA) [48], Hazard and Operability (HAZOP) [49], Probabilistic Risk Assessment (PRA) [50, 51], and Goal Tree-Success Tree and Master Logic Diagram (GTST-MLD) [52–54], presupposes system component failures as the cause of undesirable events. The second category posits that unexpected events stem from not only component failures but also complex component interactions, with methodologies primarily grounded in System Theoretic Accident Model and Processes (STAMP) [55–57]. Typical methods in this category include System Theoretic Process Analysis (STPA) [56] and Causal Analysis based on System Theory (CAST) [56, 58]. Additionally, Model-based Safety Analysis (MBSA) methods [59–61, 61] and Uncontrolled Flows of Information and Energy (UFoI-E) method also belong to this category.

Security risk analysis methods, typically independent of safety, usually originate from the conventional domain of cybersecurity infrastructure analysis, namely, firewalls, identity and authentication management, access management, cryptography, and intrusion detection systems [62]. These techniques are occasionally beneficial for iCPSs. For instance, a custom-built firewall can monitor and evaluate the system status in real-time. On detecting unusual traffic or access, it can dynamically generate filtering rules to decrease workload and maintain system stability and availability. However, traditional

IT security technologies primarily focus on information confidentiality rather than the system availability that iCPSs requires, resulting in insufficiency to safeguard iCPSs against novel cyber-physical attacks [41]. This issue has garnered considerable attention from scholars, prompting them to focus more on the models and characteristics of cyber-physical attacks [63–68], as well as exploring detection [69–75], and defence methods [34, 63, 64, 66, 76–79].

2.2 | Conditional dependence

Conditional dependence implies that the achievement of safety is a prerequisite for security, and the fulfillment of security is vital for ensuring safety. Consequently, risk analysis technologies can be divided into safety-based security risk analysis and security-based safety risk analysis.

In the context of safety-based security risk analysis, the majority of the pertinent research bolsters the system's resistance by integrating security analysis methodologies based on existing safety analysis. For example, System Theoretic Process Analysis for Security (STPA-Sec) [44] expands upon the safety analysis method in STPA, deriving security requirements and constraints from the identification of unsafe or insecure control actions. Cyber-Risk Assessment for Marine Systems (CYRA-MS) [80], used to identify and rank various cyber-attack scenarios within networked ship systems, is premised on Cyber Preliminary Hazard Analysis (CPHA, akin to hazard identification).

The reference work for security-based safety risk analysis is relatively scarce. This can be attributed to the developmental history of iCPSs. Originally, most systems in the iCPSs domain were developed from non-networked devices, such as industrial control systems (ICS), which primarily focused on safety over security. Only after these systems were networked was security considered in the original safety analysis, leading to a majority of work focusing on safety-based security analysis rather than security-based safety analysis. However, as networked devices began to take over industrial systems, scholars started paying attention to security-based safety analysis. Liao et al. [81] proposed a Bayesian-based approach to analyse the vulnerabilities and potential malicious attack paths in the safety data network of railway signalling systems. The proposed method begins by establishing the safety data network of a railway signalling system. Next, it identifies potential vulnerabilities and malicious attack paths, and constructs an extended Bayesian attack graph model with system functional safety accidents as target nodes. Finally, the Bayesian network (BN) model is used to calculate the probability of safety accidents.

2.3 | Mutual reinforcement

The ideal relationship between S&S is one that involves their mutual reinforcement towards achieving common objectives. This stands in contrast to a conditionally dependent relationship where the purpose of risk analysis methods is to achieve either safety or security but not both. In a mutually reinforcing relationship, appropriate S&S requirements and measures have the capacity to meet both S&S goals simultaneously. For instance, implementing fire prevention facilities in a data centre both protects the physical integrity of the centre, and prevents data loss. Similarly, prohibiting the entry of mobile storage devices within the data centre guards against unauthorised data intrusion, and physical failures due to data tampering.

The majority of researches aim to enhance S&S co-analysis through an integrated approach. Conventionally, these approaches fuse existing methods of S&S analysis into one single method or alternatively analyse each aspect of S&S separately before combining the results. Several tree-based methodologies, such as Failure-Attack-Countermeasure Tree (FACT) [4], SCADA S&S Joint modelling (S-cube) [14], Attack Fault Trees (AFTs) [21], along with the research conducted by Gu et al. [25], portray risk scenarios by melding different tree structures or encompassing knowledge pertinent to S&S. The Six-Step Model (SSM) [82] offers a framework to consolidate S&S assessments, examine each aspect sequentially, and incorporate the consequential results into the risk model. The Cyber Layer of Protection Analysis (CLOPA) method [24] presents a modified LOPA equation, which includes the probability of a security attack on iCPSs, and illustrates a limit on the probability of physical failure regarding safety systems framed by security failure probabilities. The Cyber Risk Assessment Framework (CRAF) [23] amalgamates diverse taxonomies from the S&S fields into a single framework supplemented by an associated procedure. Lyu and colleagues [83] studied the influence of cyber threats on the safety of physical processes and proposed an approach for cyber-to-physical risk assessment, supported by the Bayesian Network (BN). Lastly, methods based on System Theoretic Process Analysis (STPA), such as the Improved STPA-Sec [84], STPA-SafeSec [15], SafeSec Tropos [15], and STPA-SafeSec-CDCL [85], aim to integrate the safety analysis method STPA and the security analysis method STPA-Sec into one clear and concise framework.

Several studies jointly enhance S&S using unified approaches, adopting a consistent perspective on S&S and utilising similar analysis. Notably, the Non-functional Requirement (NFR) approach [19], the research conducted by Kornecki et al. [20], and the work of Ponsard et al. [26] harmonise S&S through the implementation of goal-oriented co-engineering. STORM [28] applies a model-based technique to synchronise the requirements engineering of S&S. Furthermore, the Unified Flow of Information and Energy (UFoI-E) methodology [86] along with the research produced by Z. Sun et al. [87] consider the risk sources as stemming from the unchecked flow of energy and information, employing a similar causal model to analyse S&S.

2.4 | Antagonism

Typically, the term "antagonism" suggests a contradiction between S&S requirements or measures when considering them in conjunction. On the one hand, enhancing a system's safety

might inadvertently compromise its security [88]. For instance, a feature in a European luxury car unlocks the doors if the car is involved in an accident and rolls over [88]. While this serves a safety purpose, it undermines the vehicle's security by making it more susceptible to break-ins. Also, bolstering a system's security can sometimes undermine its safety. As an example, the authentication mechanism, used to minimise illicit access and thereby ensure security in the IT domain, can potentially compromise safety when implemented for a safety-critical function of iCPSs, as it prolongs the function access time [89].

A significant number of scholars emphasise the requirement for resolving S&S contradictions [12, 42, 89–91]. However, in the iCPSs domain, only a limited amount of research work has specifically investigated methods for identifying and resolving these contradictions. For instance, M. Sun and colleagues [88] adapted domain models to represent S&S requirements and provided a rudimentary form of the conflicting model to evaluate the conflict between S&S requirements. STPA-SafeSec-CDCL [85] offers an approach to analyse and reconcile requirements contradictions between S&S. Furthermore, Z. Sun et al. [87] delineated a more comprehensive definition of S&S requirement contradictions and suggested an approach and algorithms to pinpoint these contradictions. However, it must be acknowledged that other works, including NFR [19], CRAF [23], and STORM [28], only claim to facilitate handling S&S contradictions but are not truly dedicated to resolving these contradictions.

3 | S&S CO-ANALYSIS METHODS IN iCPSs

This section presents a discussion on the merits and constraints of methodologies for S&S joint risk analysis for iCPSs referenced in Section 2.3 and Section 2.4. Every method described involves at least one of the two S&S relationships of mutual reinforcement and antagonism.

3.1 | M. Sun et al.'s work (2009)

M. Sun et al. [88] proposed a general framework for specifying domain models and detecting contradictions between S&S requirements. They define both S&S worlds as a four-tuple consisting of the model (classes and objects), propositions (and definitions), assumptions, and requirements, and then use a rewriting logic language named Maude to specify the system, environment, and domain requirements. This work provides mechanisms to relate requirements across classes, and the process of detecting conflicts between requirement classes is reduced to finding any world models that satisfy a specific form.

3.2 | Kornecki et al.'s work (2013)

Kornecki et al. [20] provided a quantitative approach based on BN to evaluate and analyse the interdependencies between S&S for software assurance in iCPSs. The method includes the following five steps: The method includes the following four steps: 1) Identify the factors that can affect S&S in the system; 2) Construct a BN model to represent the interdependencies between S&S; 3) Assign initial likelihoods that represent the probability of correct operation to the nodes of the BN model; 4) Conduct experiments to analyse and assess the impact of specific events or evidence on the likelihoods of system S&S; 5) Deduce conditional probabilities from the BN model to quantify the likelihood of system S&S in different scenarios. By utilising BN model, this approach enables a systematic assessment of potential risks, allowing for proactive measures to mitigate those risks. Nevertheless, accurate modelling of factors affecting S&S can be challenging due to the complexity and diversity of cyber-physical systems. Additionally, obtaining reliable likelihood estimates for nodes in a BN model might be difficult, as it requires access to relevant data and expert knowledge.

3.3 | FACT (2015)

Sabaliauskaite et al. [4] proposed the FACT graph, that is constructed using fault trees, safety countermeasures, attack trees, and security countermeasures, for integrating S&S analysis during early development. The FACT graph helps identify duplication, vacancy, and inconsistencies of S&S countermeasures [4]. The authors also tried to merge the lifecycle of ISA84 and ISA99 standards based on FACT graph, extending FACT's availability to the development and operation phases. The S&S alignment method helps analysts consistently implement S&S standards, analyse accidental failures and system vulnerabilities during iCPSs operation, and update countermeasures. However, the FACT graph cannot model the propagation of accidental or malicious failures over time [21].

3.4 | S-cube (2015)

S-cube is a model-based approach that provides a framework for evaluating the risks of industrial information systems and control architectures [14]. S-cube uses a domain-specific language, named S-cube KB, to model the input SCADA architecture. The system is represented by a textual model that describes S&S events and the propagation of instantaneous effects. Then, this model is processed by quantitative processing tools Yams and Figseq for automatically generating attack and failure scenarios. The S-cube approach has several advantages. For example, the formal modelling method of the system in S-cube allows analysts to add changes to the input system architecture when the system changes, rather than revamping the entire model. Moreover, S-cube can automatically generate S&S risk models with the ability to perform both qualitative and quantitative analysis [14].

However, S-cube cannot discover risks that have never been seen before since the S-cube KB is an expertise base that relies on previous risk records and specific architecture knowledge.

3.5 | Ponsard et al.'s work (2016)

Ponsard et al. [26] presented a method that uses goal-oriented requirements engineering to initially specify S&S properties in iCPSs. The method analyses S&S goals, obstacles, and countermeasures, providing a framework for reasoning about the interplay between S&S properties. However, one limitation of this work is that it focuses on the initial specification of S&S properties and does not address how to maintain these properties over time as new threats emerge.

3.6 | NFR (2016)

The NFR [19] method is used to simultaneously evaluate S&S of iCPSs at the architectural level. It has five iterative steps [92]: (1) Decompose safety into its constituent softgoals; (2) Decompose security into its constituent softgoals; (3) Decompose the system architecture into components and connections, and create a hierarchy of operationalising softgoals that represent the architectural constituents; (4) Determine the contributions of architectural constituents to the softgoals and capture justifications for these contributions in the form of claim softgoals; (5)Evaluate the overall S&S by applying the propagation rules and observing the labels propagated to the S&S softgoals.

The NFR approach allows for both qualitative and quantitative evaluation of S&S by transforming the qualitative elements of the Softgoal Interdependency Graph (SIG) into a quantitative scheme [92]. This approach aids in determining if the iCPSs design meets stakeholder S&S needs, as well as enables tracing properties back to iCPSs requirements and analysing S&S trade-offs, thereby facilitating the development of a iCPSs that is both safe and secure.

However, the NFR approach, being goal-oriented and reliant on subjective experience for system architecture and goal decomposition, may struggle to ensure consistent and objective evaluation outcomes.

3.7 | Improved STPA-sec (2016)

Schmittner et al. [84] conducted an attempt to address the limitations of STPA-Sec. They pointed out two main limitations: firstly, guidance for identifying intentional causal scenarios is difficult to apply, and secondly, security-related elements have not been included in the control loop model, limiting the model's ability to capture the view of attackers. To overcome these gaps, Schmittner et al. [84] adopted two measures: establishing a common understanding of S&S terminology, and improving the annotated control loop used for causal analysis in STPA to identify unsafe control actions caused by security attacks [84]. However, according to Schmittner's report [84], they did not completely align S&S standards and activities according to the recommendations of ISO 26262 (i.e. analysts should use top-down and bottom-up technologies for safety analysis)—the improved method is still top-down.

3.8 | STPA-SafeSec (2017)

STPA-SafeSec integrates S&S analysis by merging STPA and STPA-Sec into one concise framework, addressing the limiting factors of traditional STPA methods [15]. The integration is achieved through two extensions. Firstly, STPA-SafeSec views S&S equally and extends the safety-focused causal factor guidance of STPA into the security domain, supporting the analyst and making the assessment results more comparable. Secondly, it defines a generic component layer diagram to represent the real system control architecture and maps the abstract control structure to real system components, helping analysts refine constraints and identify the most critical system components. Based on these extensions, STPA-SafeSec provides an integrated approach for identifying S&S constraints, supporting analysts in identifying dependencies between S&S properties and deriving optimal results.

3.9 | AFTs (2017)

To overcome the limitations of the FACT graph, Kumar et al. [21] developed AFTs and equipped them with Stochastic Model Checking (SMC) and Stochastic Timed Automaton (STA) techniques. AFTs is a formalism that combines fault trees and attack trees. The STA, based on state-transition diagrams, is a powerful and flexible formalism that supports many features, such as different discrete and continuous probability distributions, hard and soft time constraints, and cost variables [21]. Each element of an AFT has a corresponding STA template, which provides unambiguous semantics for analysts. After translating the AFTs to STA, statistical model checking tools such as Uppaal SMC can be used for the system's quantitative or qualitative risk assessment. The qualitative assessment concerns the cause of system failure, while the quantitative assessment focuses on the expected cost, time, and damage of different attackers [21]. Steiner's work applied this approach to a pipeline spill, an emergency exit door, and a pipeline.

3.10 | SSM (2018)

SSM [82] provides a framework to integrate S&S assessment for iCPSs. It extends the GTST-MLD and 3-Step Model [93] by considering threats and vulnerabilities that may compromise the safety of iCPSs. It uses a set of relationship matrices to define the interdependencies between six dimensions (i.e. functions, structure, failures, safety countermeasures, cyberattacks, and security countermeasures) of iCPSs [82]. These

six dimensions and their relationships constitute a knowledge base to support an integrated S&S analysis.

There are six steps to constructing the model [82]: 1) Model the functional hierarchy of the system by goal tree (GT) and define the relationships between functions by matrix F-F; 2) Describe the system structural hierarchy by success tree (ST) and define the relationships between structure and functions by matrix S-F; 3) Analyse the safety hazard and add failures to the model; 4) Analyse the security threat and add threat to the model; 5) Add safety countermeasures to the model; 6) Add security countermeasures to the model.

Due to its excellent expandable nature, SSM has been regarded as a backbone and incorporated with STPA in Sabaliauskaite's work [82] to assess the S&S of autonomous vehicles. Additionally, SSM has been integrated with information flow diagrams (IFD) to overcome its lack of identifying failures and attacks and selecting S&S countermeasures [94]. However, this model does not include physical resource flow, which represents the energy flow of the physical world.

3.11 | CRAF (2018)

Fredrik et al. [23] proposed the CRAF to provide quick feedback early in the lifecycle of iCPSs development. The CRAF is based on openly available and widely used taxonomies from the S&S domains, and a unique mapping of where loss of data security may impact aspects of data with safety implications. The main contribution of this work is the development of a framework that brings together different elements from the S&S domains into a single framework with an associated process. However, CRAF has several limitations. For example, CRAF determines the relationship between S&S by considering the implications of a loss of data security on safety, which may not be the most suitable way to map safety to security.

3.12 | Lyu et al.'s work (2019)

Lyu et al. [83] defined cyber-to-physical (C2P) risk as the impact of cyber threat on physical process safety, and proposed an integrated C2P risk assessment method for iCPSs based on BN. The main steps of the method include constructing a BN model, determining the conditional probability distributions, assessing the probabilities of asset loss, and quantifying the C2P risk values. The contribution of this method lies in its ability to capture the hierarchical structure of iCPSs and quantify the impact of cyber threats on physical process safety. It provides a systematic approach for identifying and assessing C2P risks, which can be used as a basis for decision-making in the design and development of iCPSs. However, the limitations of this method include its reliance on a static BN model, the focus on asset loss in terms of cost, and the lack of consideration for dynamic evaluations and a wider range of impacts.

3.13 | SafeSec tropos (2020)

Kavallieratos et al. [12] proposed a method named SafeSec Tropos for joint S&S requirements elicitation. This approach combines the graphical concepts of Secure Tropos, a method for security analysis, with the systemic perspective of STPA, providing a single model to analyse S&S and representing their requirements using similar documentation structures. Notably, this work was the first to propose eliciting requirements based on safety objectives (i.e. confidentiality, integrity, availability, authenticity, possession and control, utility, and non-repudiation) and security objectives (controllability, observability, operability, resilience, survivability, graceful degradation, quality of service, availability, redundancy, fault tolerance, and integrity). This is a generic and elegant idea, that is, eliciting requirements through several atomic objectives that can meet safety or security goals. However, this method does not explain in detail how to elicit requirements through objectives but only corresponds these objectives to S&S requirements.

3.14 | UFoI-E (2020)

The UFoI-E method is a systematic methodology that facilitates the process of risk identification in iCPSs, considering cascading risks across the layers of the system and its environments. The UFoI-E concept groups safety hazards and security threats into the generic category of risk sources and conceives a risk caused by uncontrolled or undesired energy and information.

This method consists of three aspects. The first is the CPS master diagram, a multi-layered systems model used to present the architecture of CPS [86, 95]. The CPS master diagram refines the CPS aspects conceived by Humayed et al. [96] in the security context and combines it with the notion of a control structure as proposed by STAMP in the safety context. The second is the UFoI-E causality concept, a novel causation model used to conceptualise cascading risks across the information and energy domains of a system [16, 17]. The third is Cyber-Physical Harm Analysis for S&S (CyPHASS), a harm scenario builder that serves as a practical toolkit for systematically performing risk identification [18]. CyPHASS considers the CPS master diagram as the system model and uses the UFoI-E causality concept as the theoretical model of causation.

Unlike STPA-based methods, which are more generic and can be applied to many engineering systems, the UFoI-E method is explicitly tailored for CPS. Additionally, a comparative study [97] argued that both UFoI-E and STPA-based methods achieved similar completeness in S&S co-analysis under a similar degree of effort required to perform the analyses.

3.15 | Gu et al.'s work (2020)

Gu et al. [25] proposed a functional safety and information security protection mechanism based on blockchain

technology for iCPSs. This work introduces the design of the basic level and integration level blockchain structure of iCPSs distributed architecture and related functional safety and information security measures. The authors propose an effective communication judgement mechanism based on a functional safety error threshold, which is stored and judged by a smart contract. The paper also describes the Safety Integrity Level (SIL) judgement method of iCPSs physical equipment and functional safety loop, and combines SIL with fault diagnosis and risk protection. The proposed mechanism is shown to be rational in terms of information security, functional security, real-time performance, and maintainability. However, the paper does not discuss the potential limitations or challenges of implementing the proposed mechanism in practice.

3.16 | STORM (2020)

Japs [28] presented the STORM approach, a holistic S&S model-based requirements engineering (MBRE) method for the development of iCPSs. STORM enhances stakeholder understanding, integrates S&S considerations, and provides tools and standards to support the requirements engineering process. It may partly address the important and timely topic of integrating S&S considerations in MBRE for cyber-physical systems. Additionally, the proposed eight criteria for a holistic MBRE approach add value to the field by providing a framework for evaluating and improving existing approaches. However, the main limitation is the lack of thorough evaluation and validation, making it challenging to assess the real-world applicability and effectiveness of the proposed methods. Further research is needed to validate and refine the approach for practical implementation.

3.17 | CLOPA (2022)

Tantawy et al. [24] proposed the CLOPA, a modified version of LOPA that considers the probability of a security attack on a iCPSs. CLOPA has three main contributions. Firstly, the CLOPA method provides modified equations, known as CLOPA equations, to present the upper bound on the probability of physical failure for the safety system in terms of security failure probabilities [24]. The CLOPA equations mathematically describe the coupling between S&S system design and can be used to identify the CLOPA design region to support the trade-off between S&S during the design process. Secondly, this method provides a way to integrate S&S lifecycles based on a rigorous mathematical formulation, that is, CLOPA equations, rather than similarities and differences between activities and intuition. Thirdly, this CLOPA method focuses on the system design phase and shows how the design phase is developed using the outcome of combined safety-security risk assessment [24]. The S&S requirements are coupled in the context of HAZOP and LOPA risk assessment methods, which help analysts develop corresponding countermeasures to satisfy the CLOPA equations.

However, CLOPA is primarily a framework for safety instrumented system design. It focuses on the impact of security threats on system safety but does not consider security consequences such as information loss or leakage.

3.18 | STPA-SafeSec-CDCL (2023)

The STPA-SafeSec-CDCL [85] approach combines the STPA-SafeSec approach for S&S analysis and the Conflict-Driven Clause Learning (CDCL) approach for conflict identification, analysis, and resolution. Additionally, this method provides a practical case study using the Tennessee Eastman Plant process model, which adds credibility to the proposed methodology. However, the evaluation of the proposed methodology is limited to the case study. It would be beneficial to have a broader evaluation that includes comparisons with other existing methods or baselines.

3.19 | Z. Sun et al.'s work (2023)

M. Sun et al., in collaboration with Huawei [87], provided a comprehensive definition of contradictions in S&S requirements and proposed a systematical approach for contradictions identification. The first major innovation of this work lies in the reduction of inconsistencies and ambiguities in S&S requirements through the use of a consistent iCPSs conceptual model, a unified process for eliciting S&S requirements, and a unified template for expressing S&S requirements. This approach creates a more favourable premise for automated contradictions identification. The second major innovation is the proposal of sufficient conditions for contradictions identification and a machine-executable contradictions identification algorithm. In addition, this work proposes numerous potential points that warrant further investigation. For example, the causes-phenomena-effects analysis (CPEA) method fully considers the factors of S&S and their interactions during the requirement elicitation. Furthermore, eliciting S&S requirements through objectives may be a new direction that conforms to the first principles. However, although this work proposed a series of theoretical methods, there are still many potential problems that need to be solved. For example, how to better combine expert knowledge by introducing human-computer interaction theory is a potential research direction.

4 | DISCUSSION

To furnish an intuitive and comprehensive perspective for future research on S&S joint risk analysis in iCPSs, this section supplies 12 criteria to evaluate these methods and examines the results. Section 4.1 introduces these criteria, while Section 4.2 presents each criterion's analysis result. Lastly, Section 4.3 discusses limitations of reviewed methods and proposes potential research directions.

4.1 | Criteria for assessing approaches

The significance of assessing the risk analysis methods has received sufficient attention not only in the research literature [13, 36, 37], but also in S&S standards such as the IEC 61508 to the IEC 62443. In this study, we have developed a comprehensive set of 12 criteria for evaluating risk analysis methods. The selected criteria include those emphasised in relevant reviews, as well as those frequently mentioned in risk analysis research but not yet formally adopted as evaluation criteria.

Among the 12 criteria, Criterion 1 (C1) is used to classify the relationship that the method addresses, either contradictions or enhancement or both. The remaining criteria can be categorised into three categories. The first category pertains to the philosophical underpinnings of the methods, exploring views on risk sources (C2) and whether an integrated or unified approach is adopted (C3). The second category investigates the dependencies of the methods, such as whether they depend on subjective experience or objective knowledge (C4), their reliance on system theory (C5), whether they are graph-based (C6) or model-based (C7). The third category measures the analytical capabilities of the methods, including their ability to perform risk causal analysis (C8), dynamic assessment (C9), measures support (C10), and both quantitative and qualitative analysis (C11), as well as their support for the system lifecycle (C12). This comprehensive set of criteria provides a robust framework for evaluating the effectiveness of safety and security joint analysis methods in iCPSs.

Criterion 1 (C1): *Relationship between S&S addressed in the method*. Several scholars [13, 90] have highlighted the significance of exploring the interdependencies between S&S. This emphasis prompted us to classify the existing joint S&S analysis methods into two categories: those aimed at enhancing the integration of S&S and those intended to address the antagonism between them. This classification serves the purpose of summarising the main areas of focus in previous research and facilitating researchers in locating the specific reference material they seek.

Criterion 2 (C2): *View on the sources of risks*, encompasses perspectives that risk stems from system component failure, system interactions, or a combination of both. This criterion is significant in our study as it determines the scope and comprehensiveness of risk analysis, a fact recognised by scholars. The "component failure causes risk" perspective applies mainly to specific system-level components and suits systems with simple interactions. Conversely, the "interaction causes risk" viewpoint is more relevant to modern complex systems. Meanwhile, the third perspective takes into account both factors, rendering it more comprehensive.

Criterion 3 (C3): *Integrated or unified*, is a criterion used to categorise a S&S risk analysis method based on the combination of S&S. Integrated approaches incorporate existing S&S analysis methods into a singular approach, employing varied steps during S&S analysis. Conversely, unified approaches maintain a consistent process during S&S analysis and do not strictly differentiate between S&S. While there is no definitive preference for one method over the other in joint S&S risk analysis, this indicator is deemed significant by scholars [12, 42]. It signifies the convergence of two distinct philosophical notions on S&S, as well as individuals' orientations towards S&S.

Criterion 4 (C4): *Based on subjective experience or knowledge base*. Lyu et al. [36] considered subjective analysis as an attribute in their review, inspiring us to include this criterion. Methods based on subjective experience perform risk analysis mainly according to experts' experience, and their diversity may result in inconsistent analysis results. In contrast, methods based on a knowledge base, which rely primarily on data and patterns, can overcome this limitation. Additionally, a knowledge base can be continuously expanded with information and provide a foundation for performing deep learning and machine learning, aiding automatic risk assessment and prediction.

Criterion 5 (C5): *System-theory-based or not*. Systems theory encompasses the principles, models, and laws essential for comprehending the intricate interrelationships and interdependencies among the various components (technical, human, organisational, and management) of a complex system [98]. Patriarca et al. [56] introduced systems theory into risk assessment field, proposing a novel accident model called STAMP and expanding its ability to analyse safety (i.e. STPA) and security (i.e. STPA-Sec). Within the STAMP framework, a system is composed of control structures at different hierarchical levels that emerge through the interaction of system components within an environment. In this context, S&S are considered control problems at each level. This perspective has gained significant recognition in the field of iCPSs risk analysis, leading to the emergence of a series of related studies [12, 15, 57, 84, 85].

Criterion 6 (C6): *Graphics-based or not*, is a criterion deemed significant in Kriaa's research [13] for categorising model-based risk analysis methods. In this study, it is applicable to all types of risk analysis methods and evaluates whether a method offers a graphical library to illustrate concepts during risk analysis. Compared to text-based descriptions, a graphical library provides clear definitions and usage protocols for system elements and risk concepts, thereby facilitating analysts' comprehension and application.

Criterion 7 (C7): *Model-based or generic*, is a prevalent criterion employed to evaluate a method's dependency on the system model [13, 36]. Generic methods typically analyse S&S at the system component level, not taking the specific system model into account. Conversely, model-based methods tend to establish a mathematical or conceptual model for the system's functional mechanism or architectural design. While the former proves pragmatic and more accessible to learn, the latter facilitates modelling the system's components and functions, providing a comprehensive depiction of various

S&S aspects at diverse detail levels and is often considered worthy of further research.

Criterion 8 (C8): *Ability of risk causal analysis*, pertains to the proficiency in identifying or characterising risk sources and examining their causes and consequences. As per the sequence of risk sources, three corresponding factors emerge namely causes, phenomena, and consequences [87, 99]. These factors aid S&S experts in the spectrum of various S&S enhancement solutions, which ranges from precaution, detection, and response [100]. The more detailed the causal information that can be derived from a method regarding risk sources, the stronger the risk causal analysis capability of that method becomes.

Criterion 9 (C9): *Ability of dynamic risk assessment*, mainly referring to the risk assessment ability during iCPSs operation, is widely recognised as important by scholars, such as in refs. [13, 36, 37, 39], but rarely explained and discussed formally as a criterion. In this work, dynamic risk assessment capability is classified into three tiers: proficiency in performing risk assessment on iCPSs solely during the design phase, capability to execute real-time risk assessment on iCPSs during the operational phase, and the ability to conduct real-time risk assessment on systems under operation as well as dynamic development.

Criterion 10 (C10): *Measures support*, refers to whether a method includes measures to manage risks. As articulated in Criterion 6, the S&S precautions, along with detection and response measures, are indispensable in guaranteeing the smooth functioning of systems. High-performing S&S risk analysis methods, therefore, must have the capacity to provide such measures founded on their risk analysis outcomes.

Criterion 11 (C11): *Qualitative or quantitative risk analysis*, is a commonly employed criterion in relevant literature reviews [13, 36, 37]. Quantitative analysis indicates a numeric outcome from the risk analysis method, whereas qualitative analysis typically results in text expressions. Additionally, the quantitative method offers a more robust risk assessment capability compared to the qualitative one, equipping analysts with comprehensive information for decision-making.

Criterion 12 (C12): *Lifecycle support*. Many scholars have delineated the various stages encompassed within iCPSs lifecycle [1, 36, 37]. These stages encompass system design, development, and maintenance, a comprehensive perspective that we have synthesised from relevant academic viewpoints. In the design stage, iCPSs is described by requirements and concepts and has not yet become a real-world object. Then the development phase transfers the requirements and concepts into real systems. It's crucial to acknowledge that potential risks may still manifest, even if the system is deemed risk-free in the conceptual stage, due to development measures implemented for actualising the system requirements. Finally, the maintenance phase, when the system is in operation, spans the subsequent lifecycle of the system. Ascertainment of the particular stage of the S&S collaboration for which a method is applicable helps us judiciously determine its adoption in the current stage. Consequently, we consider this as a key criterion.

4.2 | Analysis

Upon the application of these aforementioned criteria, we conducted an evaluation of the surveyed methods. A summary of the evaluation results is displayed in Table 1.

4.2.1 | C1-based analysis

The enhancement of the interaction between S&S is a persistent focus among scholars, whereas the antagonism between the two is studied sporadically. Methods to reinforce S&S can be broadly categorised into two types. The first category aims to enhance S&S by integrating existing methods, including the works of Kornecki et al., FACT, Improved STPA-Sec, Ponsard et al., STPA-SafeSec, AFTs, Lyu et al., CRAF, SafeSec Tropos, Gu et al., and CLOPA. The second category, indicative of a move towards innovation, emphasises the similarities between S&S and adapts similar or identical processes for S&S analysis. This category encompasses the NFR, S-cube, SSM, UFoI-E, STORM, and Z. Sun et al.'s work. Scholars have also explored various methods to address the issue of S&S antagonism, including its representation, identification, and resolution. Antagonism is represented through the model-based method in SSM, the formal-method approach in the work of M. Sun et al., and comprehensively defined in the work of Z. Sun et al. Initial ideas for identifying S&S contradiction can be found in the works of M. Sun et al. and STPA-SafeSec-CDCL, while Z. Sun et al.'s work systematically solves this issue. Other methods, although not specifically focused on representation, identification, or resolution, can still contribute to addressing these aspects. For instance, the NFR approach posits that a soft goal interdependency graph can facilitate trade-offs between contradictory S&S aspects; similarly, Ponsard et al.'s study is credited with being able to identify and resolve conflicts between S&S. Case studies of AFTs provide quantitative evidence for determining S&S contradictions, while CRAF case studies offer a simplified example of conflict resolution. SafeSec Tropos provides a unified document of S&S requirements which aids in contradiction identification. Moreover, Ponsard et al. advocated goal-driven requirements engineering as beneficial for identifying potential conflicts.

4.2.2 | C2 and C5-based analysis

The choice to employ system theory in the S&S analysis is intimately tied to one's view on risk sources. Thus, it becomes pertinent to concurrently discuss the evaluation results of C2 and C5. Most risk analysis methods based on system theory, including Improved STPA-sec, STPA-SafeSec, SafeSec Tropos, UFoI-E, STPA-SafeSec-CDCL, and Z. Sun et al.'s work, reference the STAMP. These methods attribute risk sources to malfunctioning interactions between various components, as well as poor engineering design or failure. Such an understanding aligns more closely with the conditions of modern complex systems than the traditional

TABLE 1 Summary of reviewed S&S joint risk analysis methods for iCPSs.

Year	Approaches	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12
2009	M. Sun et al. [88]	A	-	-	S	×	×	G	R	L	×	L	S
2013	NFR [19, 92]	M&A	F	U	S	×	✓	G	A&R	L	✓	L&N	S&L
2013	Kornecki et al. [20]	M	-	U	S&K	×	✓	G	A&R&C	L	×	L&N	S&L&M
2015	FACT [4]	M	F	I	S	×	✓	G	A	L	×	L&N	S
2015	S-cube [14]	M	F&C	I	K	×	✓	M	A&R	M&H	×	L&N	S&L&M
2015	Improved STPA-Sec [84]	M	F&C	I	S	✓	✓	M	A&C	L	✓	L	S&L
2016	Ponsard et al. [26]	M	F&C	U	S	×	✓	M	A&R&C	L	✓	L	S
2017	STPA-SafeSec [15]	M	F&C	I	S	✓	✓	M	A&C	L	✓	L	S&L
2017	AFTs [21]	M	F	I	S	×	✓	G	A	L&M	×	L&N	S&L&M
2017	SSM [82]	M	-	I	S&K	×	✓	M	×	L	×	L	M
2018	CRAF [23]	M&A	-	I	S	×	×	-	-	L	✓	L	S
2019	Lyu et al. [83]	M	F&C	I	S&K	×	✓	M	A&R&C	L	×	L&N	M
2020	SafeSec Tropos [12]	M	F&C	I	S	✓	✓	M	A&C	L	✓	L	S
2020	UFoI-E [15–18, 86, 95]	M	F&C	U	S	✓	✓	M	A&R&C	L	✓	L	S&L
2020	Gu et al. [25]	M	F	I	S	×	✓	M	A&R&C	M	✓	L&N	M
2020	STORM [28]	M&A	-	U	S	×	✓	M	A&R&C	L	✓	L	S
2022	CLOPA [24]	M	F	I	S	×	×	M	×	L	×	L&N	S
2023	STPA-SafeSec-CDCL [85]	M&A	F&C	I	S	✓	✓	M	A&R&C	L	✓	L	S
2023	Z. Sun et al. [87]	M&A	F&C	U	S	✓	✓	M	A&R&C	L	✓	L	S

Note: [1]C1. Relationship between S&S addressed in the method: M (mutual reinforcement), A (antagonism). [2]C2. View on the sources of risks: F (regard the sources of risks caused by component failures or vulnerability), C (regard the sources of risks caused by system cascade). [3]C3. Integrated or unified: I (integrated), U (unified). [4]C4. Based on subjective experience or knowledge base: S (subjective experience), K (knowledge base). [5]C5. System-theory-based or not: ✓(system-theory-based), × (not system-theory-based). [6]C6. Graph-based or not: ✓ (graph-based), × (non-graphical). [7]C7. Model-based or generic: M (model-based), G (generic). [8]C8. Ability of risk causal analysis: A (can identify causes of risk sources), R (can identify S&S risk sources), C (can identify consequences of risk sources). [9]C9. Ability of dynamic risk assessment: L (risk assessment during design phase), M (real-time risk assessment during operational phase), H (real-time risk assessment under operational and dynamic development phases). [10]C10. Measures support: ✓(providing measures), × (not providing measures). [11]C11. Qualitative or quantitative risk analysis: L (qualitative), N (quantitative). [12]C12. Lifecycle support: S (design phase), L (development phase), M (maintenance phase). [13]Symbol "-" means that insufficient information is provided by the method to evaluate.

perspective, which links undesirable events to component failures. Among these methods, the UFoI-E method is noteworthy for its introduction of a novel causality concept termed uncontrolled information and energy flows. Instead of circumscribing risk within control action, the UFoI-E causality concept posits that uncontrolled energy (e.g. unwanted release of potential energy or toxic materials) and information (e.g. software flaws or cyber-physical attacks) can lead to human fatalities, asset damages, and environmental impacts. Besides these methods, some approaches lacking system theory support adopt a similar standpoint on risk sources as the STAMP-based approaches. For instance, the S-cube method models the propagation of instantaneous effects like compromised components and cascading failures by adapting interaction rules.

4.2.3 | C3-based analysis

Rather than unifying, a majority of methods concurrently boost S&S through integration. Integrated methods generally enhance S&S by incorporating security capabilities into prevalent safety risk analysis strategies. In contrast, unified methods devise novel frameworks, thereby fostering fresh insights for S&S co-analysis. Within these unified methods, approaches like NRF and the works of Kornecki et al. and Ponsard et al. utilise goal-oriented co-engineering to harmonise S&S. These methods adopt strategies such as goal decomposition to consistently address S&S. While these methods are relatively simplified, they have proven to be effective. STORM, akin in approach, employs a model-based technique to unify the requirements engineering of S&S, outlining similar procedural steps for their analysis. Notably, both UFoI-E and the works of Z. Sun et al. delve deeper, unravelling the intrinsic nature of S&S. They unify S&S through common elements and propose that S&S pervade the entire hazard and threat process, attributing this to uncontrolled energy and information flow. They endorse the application of causal models for S&S, advocating preventive measures for the roots of risk sources, detection for risk sources, and response strategies for impacts. While focussing on S&S similarities, these works maintain distinctive S&S characteristics during unification. As an

illustration, the work of Z. Sun et al. defines objectives for S&S respectively to align with their fundamental differences.

4.2.4 | C4-based analysis

Many methods rely primarily on subjective expertise, with only a handful such as Kornecki et al., S-cube, SSM, and Lyu et al. employing a knowledge base for risk analysis. As an example, S-cube utilises a domain-specific language knowledge base to portray the input SCADA architecture and subsequently generate risk scenarios. However, these scenarios are inherently confined to the knowledge base of S-cube, which restricts the detection of unspecified attacks. SSM, on the other hand, uses system functions and structure as a knowledge base for additional analysis. Lyu et al. proposed a pragmatic, data-driven strategy utilising BN to evaluate current S&S risks and predict unknown threats and hazards using historical data. Nevertheless, BN-based methodologies share a common issue with other methods mentioned earlier: while the risk analysis process remains objective, the initial BN model, which necessitates expert input, is inherently subjective. Furthermore, models that offer superior risk assessment capabilities require extensive, high-quality historical data, which might pose a challenge to obtain practically.

4.2.5 | C6-based analysis

The graphics-based methods for risk analysis can be divided into several categories: tree-based, bowtie-based, net-based, and others. The tree-based methods, such as the works of Kornecki et al., NFR, FACT, S-cube, Ponsard et al., AFTs, and Gu et al., usually represent one of the causes or consequences of a risk scenario in a tree structure, holding the advantages of easy-understanding and applicable. The bowtie-based method, that is, UFoI-E, extend the presentation ability to describe the causes and consequences of a risk source simultaneously. The net-based methods, that is, the works of Kornecki et al. and Lyu et al., flexibly represent complex interactions especially those between S&S factors in risk scenarios. Other graphic-based methods include STPA-based methods, SSM, STORM, and the work of Z. Sun et al. STPA-based methods employ a specific diagram to depict the control layer of each control loop, as well as its corresponding component layer. SSM utilises the goal tree, success tree, and master logic diagram to represent the relationships between system functions and structure. STORM employs SysML to model the system, incorporating a notation for security threats and hazards. Z. Sun et al. proposed an object-energy-interaction diagram to model the components and interactions in the conceptual iCPSs model during the design phase. Comparing the suitability of these graphical representations for risk analysis is difficult; however, expressing more information is undeniably more helpful in risk assessment. Hence, among these methods, further investigation is warranted for the net structure of BN and the extended bowties of UFoI-E.

4.2.6 | C7-based analysis

Findings from C10 indicate an unavoidable rise in dependence on system model, and underscore the difficulty in augmenting S&S and reconciling the conflict between them without extensive system knowledge. Furthermore, these methodologies model iCPSs from various perspectives. For instance, research by STPA-SafeSec, Improved STPA-Sec, SafeSec Tropos, and STPA-SafeSec-CDCL has emphasised modelling iCPSs from a control hierarchy point of view, while the studies by S-cube, Lyu et al., and CLOPA have specialised in system architectural models. Taking a differentiated approach, the works of Ponsard et al., SSM, and Gu et al. have majorly modelled systems from a functionality perspective. Research by STORM, UFoI-E, and Z. Sun et al. have prominently focused on systems with conceptual models underpinned by a broad understanding.

4.2.7 | C8-based analysis

Approaches capable of identifying or representing risk sources, along with their causes and consequences, are deemed significant by scholars. However, among the reviewed methods, only Z. Sun et al.'s work and the UFoI-E method deeply incorporate the analysis of causes and consequences into the S&S analysis process. The UFoI-E method offers a comprehensive risk identification technique for detecting S&S harm scenarios, together with their causes and consequences. Z. Sun et al. presented a systematic approach for eliciting S&S requirements by conducting a causes-phenomena-effects analysis. Crucially, both these efforts consider prevention, detection, and response measures to address the origins of risk, the risk sources themselves, and the subsequent consequences.

4.2.8 | C9-based analysis

Only the S-cube, AFTs, and the research by Gu et al. possess the capability to dynamically assess risks during the operational phase, with only the S-cube method potentially fulfilling the requirements of evaluating risks as the system is dynamically configured. The S-cube method constructs varying hypotheses based on a consistent system architecture. Therefore, when the system undergoes assumption changes, the exclusive requirement is to integrate these changes into the system model rather than overhauling the entire model. However, architectural changes, which are sometimes seen in the iCPSs domain, can cause the failure of the S-cube model. Gu et al.'s approach leverages smart contracts to store functional safety error thresholds and judge them in addition to proposing a clock-initiated refund transaction, ensuring the efficacious execution of the functional safety error threshold mechanism. Alternatively, AFTs amalgamate the benefits of attack trees and dynamic fault trees, enabling the capture of dynamic propagation of accidental and malicious failures overtime.

4.2.9 | C10-based analysis

Most methods reviewed, including the works of NFR, Improved STPA-Sec, Ponsard et al., STPA-SafeSec, SafeSec Tropos, STORM and Z. Sun et al., consider providing S&S requirements, which is to some extent a measures support, while the works of Gu et al. and UFoI-E provide specific measures to protect iCPSs. Additionally, most of the methods considering the antagonism between S&S do not put forward measures to solve or alleviate antagonism, only the CRAF and STPA-SafeSec-CDCL propose some measures to deal with contradictions.

4.2.10 | C11-based analysis

Numerous scholars have acknowledged the significance of transitioning risk assessment from a qualitative approach to a quantitative one and have made concerted efforts towards this end. Currently, methods capable of quantitative analysis include NFR, approaches based on tree structures, such as FACT, AFTs, S-cube, along with the work from Gu et al. Moreover, BN-based approaches such as those propounded by Kornecki and Lyu et al., as well as CLOPA are also integral in this context.

4.2.11 | C12-based analysis

The preponderance of existing strategies predominantly concentrate on bolstering the system design phase, guiding designers in S&S analysis to ascertain suitable S&S requirements and measures. A limited number of methods, notably those forged by SSM, Lyu et al., and Gu et al., allocate their focus to the system's operational stage, facilitating S&S analysis that propels future system ameliorations. Scarce approaches, namely those propagated by Korneck et al., the S-cube, and AFTs, advocate general methods that incorporate S&S analysis, thereby offering support over the system's complete lifecycle. In essence, while a focus on a specific stage holds merit, we also argue that methods applicable across a broader range of stages demonstrate superior lifecycle support capabilities.

4.3 | Limitations and research directions

Based on the comprehensive analysis provided above, we have further identified and summarised the primary limitations of the joint S&S risk analysis approach for iCPSs. In light of these limitations, we propose several research directions that have the potential to effectively address these gaps. These main limitations and directions are outlined below:

1. Numerous studies have explored the enhancement of S&S collaboration, yet few have delved into the contradictions aspects between S&S. There exist several scientific questions that warrant investigation within this field. For instance, existing research pays limited attention to the S&S contradictions that arise during system runtime. There is a lack of methods for identifying and resolving such contradictions. Furthermore, despite M. Sun et al. providing a systematic approach for identifying S&S requirement contradictions, challenges remain regarding the high time and resource costs associated with this approach. Addressing these challenges and further enhancing the automation of dealing with contradictions merit consideration.
2. Most methods for risk analysis in iCPSs depend on subjective experience, with only a few, such as S-cube, SSM, and BN-based, being based on a knowledge model. The BN-based method, as a representative of knowledge-based approaches, shows great promise in combining with data-driven and artificial intelligence technologies. However, these methods require experts to build the initial model, which means that re-modelling is necessary when the system architecture changes. This limitation renders existing knowledge-based methods unusable in scenarios involving dynamic system configuration and lacking the capability for dynamic risk analysis. It is reasonable to expect overcoming this limitation, perhaps by drawing lessons from the successful performance of S-cube and AFTs in dynamic analysis.
3. Few method can really meet the needs of S&S analysis during the dynamic configuration of iCPSs. The S-cube method is worthy of further study since it can automatically export risk scenarios when the system architecture remains unchanged while the system assumptions change.
4. The heterogeneity of iCPSs data resources puts obstacle in advancing the S&S collaborative analysis. The heterogeneous data is invariably present regardless of whether we employ an integrated or unified way to joint S&S analysis. This data may originate from artefacts produced by various S&S risk analysis methods or from data generated by heterogeneous system components. Therefore, it is an important and promising research direction to pay attention to cross-method and cross-layer heterogeneous data fusion analysis.
5. Few studies have recognised the potential of utilising a causal model to unify S&S risk analysis. The work of M. Sun et al. and the UFoI-E method have made efforts to identify S&S risk sources, analyse causes and consequences, and propose corresponding S&S precaution, detection, and response measures. These studies hold significant value and warrant further investigation. The methods based on system theory use the innovative accident causation models to treat the risk sources, which has been proved to be effective in S&S joint risk analysis. To advance the unification of S&S risk analysis, it is recommended to expand the scope by considering additional accident causation models [101]. It would be advantageous to conduct comparative experiments to assess the efficacy of diverse causal models in performing joint S&S risk analysis.
6. Graphical representations provide valuable information for analysing the S&S risks of a system. However, there has

been no study comparing the impact of existing graphical representation methods on S&S risk analysis. This comparison is worthy of further research. Furthermore, investigating the contribution of human-computer interaction (HCI) technology to S&S risk analysis is highly recommended. This is because most existing methods heavily rely on expert knowledge and practitioner experience, and there is a need to provide approaches that effectively and efficiently integrate human expertise with risk analysis.

Beyond these primary limitations and directions, there are also topics that warrant further investigation. For instance, existing studies lack sufficient quantitative analysis, with an overemphasis on the system design phase and inadequate attention to the operational phase. Also, a minority of recent studies fails to recognise system interactions as one potential source of risks.

5 | END REMARKING

The interconnected nature of iCPSs significantly undermines the reliability of loosely coupled S&S risk analysis. Recognising this, scholars have conducted a series of studies. Our work surveys the recent advancements in joint S&S risk analysis methods for iCPSs, delving into the S&S relationships involved. We provide 12 criteria for evaluating these methods, discussing the evaluation results, and analysing the existing limitations and potential research directions. However, we do not purport to have reviewed all S&S joint risk analysis methods. Our analysis concentrates on crucial methods that are most applicable to the iCPSs domain. Additionally, our investigation is strictly confined to the scope of the methods reviewed. We view our work as laying a foundational brick to attract refined jade. We hope that this paper will invigorate more scholars to participate in discussing the S&S joint risk analysis methods for iCPSs. Finally, we re-emphasise the potential research directions, which include the following five points.

1. Further work is necessary to address S&S contradictions, particularly those occurring in the operational phase. We need to develop systematic methods for the analysis and resolution of these contradictions, while also enhancing the automation capabilities of the methodologies.
2. Knowledge-based and data-driven methods warrant further investigation, as they can be integrated with advanced artificial intelligence technologies and possess the potential for dynamic risk analysis. Additionally, improving the rationality of initial model building in these methods is worth profound consideration.
3. Causal models, which involve philosophical considerations of the sources, procedures and responses of S&S risks are worthy of further exploration. Specifically, an investigation into the impact of various existing causal models on risk analysis is required.
4. Given that S&S risk analysis inevitably encompasses numerous expert experiences, we also strongly recommend intensifying the support of visualisation and human-computer interaction technologies in this domain.
5. The fusion of heterogeneous data warrants further investigation. The inherent heterogeneity of iCPSs and the integration of different methods to analyse S&S result in the heterogeneity of data resources. We recommend investigating cross-method and cross-layer data fusion theory.

AUTHOR CONTRIBUTIONS

Zhicong Sun: Conceptualization; data curation; investigation; methodology; validation; visualisation; writing—original draft; writing—review and editing. **Guang Chen**: Conceptualization; data curation; resources; validation; visualisation; writing—review and editing. **Yulong Ding**: Funding acquisition; project administration; resources; supervision; validation. **Shuang-Hua Yang**: Conceptualization; funding acquisition; project administration; resources; supervision; writing—review and editing.

ACKNOWLEDGEMENTS

This research is supported by the National Natural Science Foundation of China (Grant Nos. 92067109, 61873119, and 62211530106), the Shenzhen Science and Technology Program (Grant Nos. ZDSYS20210623092007023 and GJHZ20210705141808024), and the Educational Commission of Guangdong Province (Grant No. 2019KZDZX1018).

CONFLICT OF INTEREST STATEMENT

None.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

REFERENCES

1. Wolf, M., Serpanos, D.: Safety and security in cyber-physical systems and internet-of-things systems. Proc. IEEE 106(1), 9–20 (2018). https://doi.org/10.1109/jproc.2017.2781198
2. Colombo, A., et al.: Industrial cyberphysical systems: a backbone of the fourth industrial revolution. IEEE Ind Electron Mag 11(1), 6–16 (2017). https://doi.org/10.1109/mie.2017.2648857
3. Rausand, M., Haugen, S.: Risk Assessment: Theory, Methods, and Applications, vol. 115. John Wiley and Sons (2013). https://doi.org/10.1002/9781119377351
4. Sabaliauskaite, G., Mathur, A.P.: Aligning cyber-physical system safety and security. In: Complex Systems Design and Management Asia, pp. 41–53 (2015)
5. Dzung, D., et al.: Security for industrial communication systems. Proc. IEEE 93(6), 1152–1177 (2005). https://doi.org/10.1109/jproc.2005.849714
6. Langner, R.: Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security and Privacy 9(3), 49–51 (2011). https://doi.org/10.1109/msp.2011.67
7. Bencsáth, B., et al.: Duqu: analysis, detection, and lessons learned. In: ACM European Workshop on System Security (EuroSec). Citeseer (2012)
8. Ganesan, A., et al.: A brief study of Wannacry threat: Ransomware attack 2017 8(5), 2016–2018 (2019)
9. Piètre-Cambacédès, L., Bouissou, M.: Modeling safety and security interdependencies with bdmp (boolean logic driven markov processes). In: 2010 IEEE International Conference on Systems, Man and Cybernetics, pp. 2852–2861. IEEE (2010)

10. Lisova, E., Šljivo, I., Čaušević, A.: Safety and security co-analyses: a systematic literature review. IEEE Syst. J. 13(3), 2189–2200 (2018). https://doi.org/10.1109/jsyst.2018.2881017
11. Chockalingam, S., et al.: Integrated safety and security risk assessment methods: a survey of key characteristics and applications. In: Critical Information Infrastructures Security: 11th International Conference, CRITIS 2016, Paris, France, October 10–12, 2016, Revised Selected Papers 11, pp. 50–62. Springer (2017)
12. Kavallieratos, G., Katsikas, S., Gkioulos, V.: Safesec tropos: joint security and safety requirements elicitation. Comput. Stand. Interfac. 70, 103429 (2020). https://doi.org/10.1016/j.csi.2020.103429
13. Kriaa, S., et al.: A survey of approaches combining safety and security for industrial control systems. Reliab. Eng. Syst. Saf. 139, 156–178 (2015). https://doi.org/10.1016/j.ress.2015.02.008
14. Kriaa, S., Bouissou, M., Laarouchi, Y.: A model based approach for SCADA safety and security joint modelling: S-cube. In: IET Conference Proceedings (2015)
15. Friedberg, I., et al.: STPA-SafeSec: safety and security analysis for cyber-physical systems. J. Inf. Secur. Appl. 34, 183–196 (2017). https://doi.org/10.1016/j.jisa.2016.05.008
16. Guzman, N.C., et al.: Combined safety and security risk analysis using the ufoi-e method: a case study of an autonomous surface vessel. In: Proceedings of the 29th European Safety and Reliability Conference, pp. 22–26. Lower Saxony, Germany (2019)
17. Carreras Guzman, N.H., Kozine, I.: Uncontrolled flows of information and energy in cyber-physical systems. In: European Safety and Reliability Association Newsletter, pp. 2–3 (2018)
18. Guzman, N.H.C., Kozine, I., Lundteigen, M.A.: An integrated safety and security analysis for cyber-physical harm scenarios. Saf. Sci. 144, 105458 (2021). https://doi.org/10.1016/j.ssci.2021.105458
19. Subramanian, N., Zalewski, J.: Assessment of safety and security of system architectures for cyberphysical systems. In: 2013 IEEE International Systems Conference (SysCon), pp. 634–641. IEEE (2013)
20. Kornecki, A.J., Subramanian, N., Zalewski, J.: Studying interrelationships of safety and security for software assurance in cyber-physical systems: approach based on bayesian belief networks. In: 2013 Federated Conference on Computer Science and Information Systems, pp. 1393–1399. IEEE (2013)
21. Kumar, R., Stoelinga, M.: Quantitative security and safety analysis with attack-fault trees. In: 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), pp. 25–32. IEEE (2017)
22. Sabaliauskaite, G., Liew, L.S., Cui, J.: Integrating autonomous vehicle safety and security analysis using stpa method and the six-step model. Int. J. Adv. Security 11(1), 160–169 (2018)
23. Asplund, F., et al.: Rapid integration of cps security and safety. IEEE Embed. Syst. Lett. 11(4), 111–114 (2018). https://doi.org/10.1109/les.2018.2879631
24. Tantawy, A., Abdelwahed, S., Erradi, A.: Cyber lopa: an integrated approach for the design of dependable and secure cyber-physical systems. IEEE Trans. Reliab. 71(2), 1075–1091 (2022). https://doi.org/10.1109/tr.2022.3163652
25. Gu, A., et al.: Integrated functional safety and security diagnosis mechanism of cps based on blockchain. IEEE Access 8, 15241–15255 (2020). https://doi.org/10.1109/access.2020.2967453
26. Ponsard, C., Dallons, G., Massonet, P.: Goal-oriented co-engineering of security and safety requirements in cyber-physical systems. Lect. Notes Comput. Sci. 9923, 334–345 (2016). https://doi.org/10.1007/978-3-319-45480-1_27
27. Brunner, M., et al.: Towards an integrated model for safety and security requirements of cyber-physical systems. In: 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp. 334–340. IEEE (2017)
28. Japs, S.: Security and safety by model-based requirements engineering. In: 2020 IEEE 28th International Requirements Engineering Conference (RE), pp. 422–427. IEEE (2020)
29. Jiang, Y., Yin, S., Kaynak, O.: Data-driven monitoring and safety control of industrial cyber-physical systems: Basics and beyond. IEEE Access 6, 47374–47384 (2018). https://doi.org/10.1109/access.2018.2866403
30. Mubeen, S., Lisova, E., Vulgarakis Feljan, A.: Timing predictability and security in safety-critical industrial cyber-physical systems: a position paper. Appl. Sci. 10(9), 3125 (2020). https://doi.org/10.3390/app10093125
31. Kayan, H., et al.: Cybersecurity of industrial cyber-physical systems: a review. ACM Comput. Surv. 54(11s), 1–35 (2022). https://doi.org/10.1145/3510410
32. Ding, D., et al.: A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing 275, 1674–1683 (2018). https://doi.org/10.1016/j.neucom.2017.10.009
33. Franco, J., et al.: A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems. IEEE Commun. Surv. Tutor. 23(4), 2351–2383 (2021). https://doi.org/10.1109/comst.2021.3106669
34. Zhang, D., et al.: A survey on attack detection, estimation and control of industrial cyber–physical systems. ISA Trans. 116, 1–16 (2021). https://doi.org/10.1016/j.isatra.2021.01.036
35. Agrawal, N., Kumar, R.: Security perspective analysis of industrial cyber physical systems (i-cps): a decade-wide survey. ISA Trans. 130, 10–24 (2022). https://doi.org/10.1016/j.isatra.2022.03.018
36. Lyu, X., Ding, Y., Yang, S.H.: Safety and security risk assessment in cyber-physical systems. IET Cyber-Phys. Syst.: Theory Appl. 4(3), 221–232 (2019). https://doi.org/10.1049/iet-cps.2018.5068
37. Oueidat, T., Flaus, J.-M., Massé, F.: A review of combined safety and security risk analysis approaches: application and classification. In: 2020 International Conference on Control, Automation and Diagnosis (ICCAD), pp. 1–7. IEEE (2020)
38. Khalid, H., et al.: Security and safety of industrial cyber-physical system: systematic literature review. PalArch's J. Archaeol. Egypt/ Egyptol. 17(9), 1592–1620 (2020)
39. George, P.G., Renjith, V.: Evolution of safety and security risk assessment methodologies towards the use of bayesian networks in process industries. Process Saf. Environ. Protect. 149, 758–775 (2021). https://doi.org/10.1016/j.psep.2021.03.031
40. Canonico, R., Sperlì, G.: Industrial cyber-physical systems protection: a methodological review. Comput. Secur. 135, 103531 (2023). https://doi.org/10.1016/j.cose.2023.103531
41. Jiang, Y., et al.: Monitoring and defense of industrial cyber-physical systems under typical attacks: from a systems and control perspective. IEEE Transactions on Industrial Cyber-Physical Systems 1, 192–207 (2023). https://doi.org/10.1109/ticps.2023.3317237
42. Eames, D.P., Moffett, J.: The integration of safety and security requirements. In: International Conference on Computer Safety, Reliability, and Security, pp. 468–480. Springer (1999)
43. Pièrre-Cambacédès, L.: Des relations entre sûreté et sécurité. Ph.D. dissertation. Télécom ParisTech (2010)
44. Young, W., Leveson, N.G.: An integrated approach to safety and security based on systems theory. In: Commun, pp. 31–35. ACM (2014)
45. Ruijters, E., Stoelinga, M.: Fault tree analysis: a survey of the state-of-the-art in modeling, analysis and tools. Computer Science Review 15, 29–62 (2015). https://doi.org/10.1016/j.cosrev.2015.03.001
46. Andrews, J.D., Dunnett, S.J.: Event-tree analysis using binary decision diagrams. IEEE Trans. Reliab. 49(2), 230–238 (2000). https://doi.org/10.1109/24.877343
47. Ferdous, R., et al.: Handling and updating uncertain information in bow-tie analysis. J. Loss Prev. Process. Ind. 25(1), 8–19 (2012). https://doi.org/10.1016/j.jlp.2011.06.018
48. Schmittner, C., et al.: Security application of failure mode and effect analysis (fmea). In: International Conference on Computer Safety, Reliability, and Security, pp. 310–325. Springer (2014)
49. Suhardi, B., et al.: Analysis of the potential hazard identification and risk assessment (HIRA) and hazard operability study (HAZOP): case study. Int. J. Eng. Technol. 7(3), 1–7 (2018). https://doi.org/10.14419/ijet.v7i3.24.17290
50. Stamatelatos, M.: Probabilistic risk assessment: what is it and why is it worth performing it. NASA Office of Safety and Mission Assurance 4(05) (2000)

51. Wreathall, J., Nemeth, C.: Assessing risk: the role of probabilistic risk assessment (PRA) in patient safety improvement. Qual. Saf. Health Care 13(3), 206–212 (2004). https://doi.org/10.1136/qshc.2003.006056
52. Guo, C., et al.: Extended GTST-MLD for Aerospace system safety analysis. Risk Anal. 32(6), 1060–1071 (2012). https://doi.org/10.1111/j.1539-6924.2011.01718.x
53. Modarres, M., Cheon, S.W.: Function-centered modeling of engineering systems using the goal tree-success tree technique and functional primitives. Reliab. Eng. Syst. Saf. 64(2), 181–200 (1999). https://doi.org/10.1016/s0951-8320(98)00062-3
54. Di Maio, F., Mascherona, R., Zio, E.: Risk analysis of cyber-physical systems by GTST-MLD. IEEE Syst. J. 14(1), 1333–1340 (2020). https://doi.org/10.1109/jsyst.2019.2928046
55. Khan, S., Madnick, S., Moulton, A.: Cyber-safety analysis of an industrial control system for chillers using stpa-sec. SSRN Electron. J. (2019). https://doi.org/10.2139/ssrn.3370540
56. Patriarca, R., et al.: The past and present of System-Theoretic Accident Model and Processes (STAMP) and its associated techniques: a scoping review. Saf. Sci. 146(October 2021), 105566 (2022). https://doi.org/10.1016/j.ssci.2021.105566
57. Song, Y.: Applying System-Theoretic Accident Model and Processes (Stamp) to Hazard Analysis. Ph.D. dissertation (2012)
58. Li, F., et al.: A cast-based causal analysis of the catastrophic underground pipeline gas explosion in taiwan. Eng. Fail. Anal. 108, 104343 (2020). https://doi.org/10.1016/j.engfailanal.2019.104343
59. Yakymets, N., et al.: Model-based engineering, safety analysis and risk assessment for personal care robots. In: 2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), pp. 6136–6141. IEEE (2018)
60. Joshi, A., et al.: A proposal for model-based safety analysis. In: 2005 AIAA/IEEE 24th Digital Avionics Systems Conference, pp. 13. IEEE (2005)
61. Lisagor, O., Kelly, T., Niu, R.: Model-based safety assessment: review of the discipline and its challenges. In: The Proceedings of 2011 9th International Conference on Reliability, Maintainability and Safety, pp. 625–632. IEEE (2011)
62. Mo, Y., et al.: Cyber-physical security of a smart grid infrastructure. Proc. IEEE 100(1), 195–209 (2012). https://doi.org/10.1109/jproc.2011.2161428
63. Cao, L., et al.: A survey of network attacks on cyber-physical systems. IEEE Access 8, 44219–44227 (2020). https://doi.org/10.1109/access.2020.2977423
64. Duo, W., Zhou, M., Abusorrah, A.: A survey of cyber attacks on cyber physical systems: recent advances and challenges. IEEE CAA J. Autom. Sinica 9(5), 784–800 (2022). https://doi.org/10.1109/jas.2022.105548
65. Khojasteh, M.J., et al.: Learning-based attacks in cyber-physical systems. IEEE Trans. Control Netw. Syst. 8(1), 437–449 (2020). https://doi.org/10.1109/tcns.2020.3028035
66. Li, J., et al.: Adversarial attacks and defenses on cyber–physical systems: a survey. IEEE Internet Things J. 7(6), 5103–5115 (2020). https://doi.org/10.1109/jiot.2020.2975654
67. Arnaboldi, L., et al.: Modelling load-changing attacks in cyber-physical systems. Electron. Notes Theor. Comput. Sci. 353, 39–60 (2020). https://doi.org/10.1016/j.entcs.2020.09.018
68. Kim, S., Park, K.-J.: A survey on machine-learning based security design for cyber-physical systems. Appl. Sci. 11(12), 5458 (2021). https://doi.org/10.3390/app11125458
69. Deng, W., et al.: Detecting intelligent load redistribution attack based on power load pattern learning in cyber-physical power systems. IEEE Trans. Ind. Electron. 71(6), 6285–6293 (2024). https://doi.org/10.1109/tie.2023.3294646
70. Huang, K., et al.: False data injection attacks detection in smart grid: a structural sparse matrix separation method. IEEE Trans. Netw. Sci. Eng. 8(3), 2545–2558 (2021). https://doi.org/10.1109/tnse.2021.3098738
71. Tan, S., et al.: Brief survey on attack detection methods for cyber-physical systems. IEEE Syst. J. 14(4), 5329–5339 (2020). https://doi.org/10.1109/jsyst.2020.2991258
72. Zhang, J., et al.: Deep learning based attack detection for cyber-physical system cybersecurity: a survey. IEEE CAA J. Autom. Sinica 9(3), 377–391 (2021). https://doi.org/10.1109/jas.2021.1004261
73. Lucia, W., Gheitasi, K., Ghaderi, M.: Setpoint attack detection in cyber-physical systems. IEEE Trans. Automat. Control 66(5), 2332–2338 (2020). https://doi.org/10.1109/tac.2020.3004326
74. Ding, D., et al.: Recursive filtering of distributed cyber-physical systems with attack detection. IEEE Trans. Syst. Man Cybern.: Syst. 51(10), 6466–6476 (2020). https://doi.org/10.1109/tsmc.2019.2960541
75. Hussain, B., et al.: Deep learning-based ddos-attack detection for cyber–physical system over 5g network. IEEE Trans. Ind. Inf. 17(2), 860–870 (2020). https://doi.org/10.1109/tii.2020.2974520
76. Wu, S., et al.: An integrated data-driven scheme for the defense of typical cyber–physical attacks. Reliab. Eng. Syst. Saf. 220, 108257 (2022). https://doi.org/10.1016/j.ress.2021.108257
77. Griffioen, P., Weerakkody, S., Sinopoli, B.: A moving target defense for securing cyber-physical systems. IEEE Trans. Automat. Control 66(5), 2016–2031 (2020). https://doi.org/10.1109/tac.2020.3005686
78. Su, Q., et al.: Cyber-attacks against cyber-physical power systems security: state estimation, attacks reconstruction and defense strategy. Appl. Math. Comput. 413, 126639 (2022). https://doi.org/10.1016/j.amc.2021.126639
79. Liu, H., Wang, S., Li, Y.: Event-triggered control and proactive defense for cyber–physical systems. IEEE Trans. Syst. Man Cybern.: Syst. 52(10), 6305–6313 (2022). https://doi.org/10.1109/tsmc.2022.3144337
80. Bolbot, V., et al.: A novel cyber-risk assessment method for ship systems. Saf. Sci. 131, 104908 (2020). https://doi.org/10.1016/j.ssci.2020.104908
81. Liao, Y., et al.: Risk analysis for railway signaling safety data network based on extend bayesian attack graph. J. Phys. Conf. 1549(5), 052070 (2020). https://doi.org/10.1088/1742-6596/1549/5/052070
82. Sabaliauskaite, G., Adepu, S., Mathur, A.: A six-step model for safety and security analysis of cyber-physical systems. In: International Conference on Critical Information Infrastructures Security, pp. 189–200. Springer (2016)
83. Lyu, X., Ding, Y., Yang, S.-H.: Bayesian network based c2p risk assessment for cyber-physical systems. IEEE Access 8, 88506–88517 (2020). https://doi.org/10.1109/access.2020.2993614
84. Schmittner, C., Ma, Z., Puschner, P.: Limitation and improvement of stpa-sec for safety and security co-analysis. In: International Conference on Computer Safety, Reliability, and Security, pp. 195–209. Springer (2016)
85. Agbo, C., Mehrpouyan, H.: Conflict analysis and resolution of safety and security boundary conditions for industrial control systems. In: 2022 6th International Conference on System Reliability and Safety (ICSRS), pp. 145–156. IEEE (2022)
86. Guzman, N.H.C., et al.: Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis. Syst. Eng. 23(2), 189–210 (2020). https://doi.org/10.1002/sys.21509
87. Sun, Z., et al.: Contradictions identification of safety and security requirements for industrial cyber-physical systems. IEEE Internet Things J., 1 (2023)
88. Sun, M., et al.: Addressing safety and security contradictions in cyber-physical systems. In: Proceedings of the 1st Workshop on Future Directions in Cyber-Physical Systems Security (CPSSW'09). Citeseer (2009)
89. Novak, T., Gerstinger, A.: Safety-and security-critical services in building automation and control systems. IEEE Trans. Ind. Electron. 57(11), 3614–3621 (2009). https://doi.org/10.1109/tie.2009.2028364
90. Piètre-Cambacédès, L., Bouissou, M.: Modeling safety and security interdependencies with bdmp (boolean logic driven markov processes). In: 2010 IEEE International Conference on Systems, Man and Cybernetics, pp. 2852–2861. IEEE (2010)
91. Gu, T., Lu, M., Li, L.: Extracting interdependent requirements and resolving conflicted requirements of safety and security for industrial control systems. In: 2015 First International Conference on Reliability Systems Engineering (ICRSE), pp. 1–8. IEEE (2015)

92. Subramanian, N., Zalewski, J.: Quantitative assessment of safety and security of system architectures for cyberphysical systems using the NFR approach. IEEE Syst. J. 10(2), 397–409 (2016). https://doi.org/10.1109/jsyst.2013.2294628
93. Brissaud, F., et al.: Reliability study of an intelligent transmitter. In: 15th ISSAT International Conference on Reliability and Quality in Design, pp. 224–233. International Society of Science and Applied Technologies (2009)
94. Sabaliauskaite, G., Adepu, S.: Integrating six-step model with information flow diagrams for comprehensive analysis of cyber-physical system safety and security. In: 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), pp. 41–48. IEEE (2017)
95. Guzman, N.H.C., Mezovari, A.G.: Design of iot-based cyber–physical systems: a driverless bulldozer prototype. Information 10(11), 343 (2019). https://doi.org/10.3390/info10110343
96. Humayed, A., et al.: Cyber-physical systems security—a survey. IEEE Internet Things J. 4(6), 1802–1831 (2017). https://doi.org/10.1109/jiot.2017.2703172
97. Guzman, N.H.C., et al.: A comparative study of stpa-extension and the ufoi-e method for safety and security co-analysis. Reliab. Eng. Syst. Saf. 211, 107633 (2021). https://doi.org/10.1016/j.ress.2021.107633
98. Yousefi, A., Hernandez, M.R.: Using a system theory based method (stamp) for hazard analysis in process industry. J. Loss Prev. Process. Ind. 61, 305–324 (2019). https://doi.org/10.1016/j.jlp.2019.06.014
99. Bolbot, V., et al.: A novel risk assessment process: application to an autonomous inland waterways ship. Proc. Inst. Mech. Eng. O J. Risk Reliab. 237(2), 436–458 (2023). https://doi.org/10.1177/1748006x211051829
100. Zhou, C., et al.: A unified architectural approach for cyberattack-resilient industrial control systems. Proc. IEEE 109(4), 517–541 (2020). https://doi.org/10.1109/jproc.2020.3034595
101. Fu, G., et al.: The development history of accident causation models in the past 100 years: 24Model, a more modern accident causation model. Process Saf. Environ. Protect. 134, 47–82 (2020). https://doi.org/10.1016/j.psep.2019.11.027

How to cite this article: Sun, Z., et al.: Joint safety and security risk analysis in industrial cyber-physical systems: A survey. IET Cyber-Phys. Syst., Theory Appl. 9(4), 334–349 (2024). https://doi.org/10.1049/cps2.12095