IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 13 June 2023, accepted 13 July 2023, date of publication 20 July 2023, date of current version 11 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3297446

RESEARCH ARTICLE

Safety and Cybersecurity Assessment Techniques for Critical Industries: A Mapping Study

IEVGEN BABESHKO[1,2] AND FELICITA DI GIANDOMENICO[2]

[1]Computer Systems, Networks and Cybersecurity Department, National Aerospace University "Kharkiv Aviation Institute," 61070 Kharkiv, Ukraine
[2]Istituto di Scienza e Tecnologie dell'Informazione Alessandro Faedo-CNR, 56127 Pisa, Italy

Corresponding author: Ievgen Babeshko (ievgen.babeshko@isti.cnr.it)

ABSTRACT The paper presents a mapping study of safety and cybersecurity assessment techniques used in critical industries such as nuclear power plants, the oil and gas sector, autonomous vehicles, railways, etc., with particular emphasis on instrumentation and control systems (I&C). Modern I&Cs are complex electronic systems comprising thousands of components, therefore their reliability and safety when employed in critical application domains are challenging. With the development and integration of Industry 4.0 technologies such systems become more open for communication and flexible usage due to gradual interconnection with public networks and the Internet, but new cybersecurity and safety challenges are introduced. This paper states research questions and provides analysis results of recent relevant sources. Initially, 320 records (acquired between 2018 and 2022 inclusive) were identified. Later on, 187 studies were processed to check eligibility criteria. Overall, this mapping study includes 49 papers, after examining the pre-defined criteria and guidelines. The results of the analysis performed allow to systemize techniques being utilized in practice right now, as well as to identify trends of further techniques development. In fact, although the techniques used are not novel and most of them have been used for decades, our study shows that there are still some new trends in this field. In particular, the unified safety and cybersecurity assessment technique is a promising research direction, worth further investigation.

INDEX TERMS Safety, cybersecurity, assessment techniques, instrumentation and control systems.

I. INTRODUCTION

Safety and cybersecurity issues have always been among the top priorities in critical industries, but today they are becoming even more urgent. Assessment of modern critical instrumentation and control systems is a complicated process, principally due to the size (system consists of many components) and volatility (system perpetually evolves throughout lifecycle) problem. Cybersecurity contributes to safety and sometimes conflicts with it, but it is not always considered at all lifecycle stages together with safety. The results of the assessment are considerably dependent on metrics/techniques/assumptions chosen. Therefore, arranging an assessment process based on solid methodologies/techniques is of high importance, because there is a risk of safety underestimation or overestimation, with potential severe impact on the service delivered. With the focus on critical sectors, this paper considers the following domains: nuclear power plants, the oil and gas sector, autonomous vehicles, and railways.

The purpose of the work is to survey recent literature in order to develop a mapping study useful to understand:

- which 'classical' (described in standards or other normative documents) assessment techniques are used in recent primary studies;
- advancements of such "classical" techniques, to respond to needs posed by modern critical systems;
- application of specific techniques to assess different metrics/properties they were originally developed for (i.e. modification of reliability assessment techniques for cybersecurity assessment);
- combinations of techniques used;
- needs for additional research in the generalization of assessment techniques so as to provide a unified assessment approach.

The associate editor coordinating the review of this manuscript and approving it for publication was Diana Gratiela Berbecaru.

The paper is organized as follows. In Section II we analyze existing systematic literature reviews, surveys, and mapping studies on adjacent topics. A description of the approach used, as well as research questions, are provided in Section III. In section IV we present our analysis of the collected data and our results in response to the research questions. In Section V we list key findings. Section VI presents the threats to the validity. Finally, we make conclusions and outline future research directions in Section VII.

II. COMPARISON WITH RELATED WORKS

This study fills a gap in research on cybersecurity and safety assessment techniques: although several reviews exist, to the best of the authors' knowledge no previous work provides a comprehensive and up-to-date systematic mapping study that covers different critical domains. To facilitate comparison, related works are summarized in Table 1. For each work, the following information is presented:

- Reference;
- Year of publication;
- Application domain;
- The number of references included in the paper.

TABLE 1. Comparison with other systematic literature reviews, surveys, and mapping studies.

Ref.	Year	Domain	Number of references
[19]	2019	Nuclear	32
[24]	2021	Nuclear	52
[30]	2021	Critical Infrastructures	107
[41]	2020	Autonomous Vehicles	23

The review made in [19] discusses U.S. Nuclear Regulatory Commission (NRC)'s proposed vulnerability assessment methodology, as well as additions and changes that must be made to increase its efficacy. It mainly includes references to normative documents for the nuclear field, not research studies.

In [24], the focus is put on the identification of scientific papers discussing cybersecurity frameworks, standards, guidelines, best practices, and any additional cybersecurity protection measures for the nuclear domain. Safety issues are not covered, as well as cybersecurity and safety co-engineering were not addressed in this report.

Report [30] focuses on studies that combine Bayesian Networks and Graph Theory for safety and cybersecurity integrated assessment. Other techniques and their combinations are not covered.

In [41], blockchain-based methods are discussed for cybersecurity assurance in the autonomous vehicles domain.

III. REVIEW APPROACH

A. GENERAL INFORMATION

This study was performed according to guidelines on systematic literature reviews and surveys [59] and guidelines for conducting systematic mapping studies [60]. First of all, a set of research questions that our study aims to answer was formulated. These research questions address safety and cybersecurity techniques used, as well as their combinations and modifications, and are listed in Section III-B. From the research questions, we defined the research query and then the search strategy, as presented in Section III-C. We applied this search strategy to the following popular electronic databases:

- IEEE Explore (https://ieeexplore.ieee.org/);
- ScienceDirect (https://www.sciencedirect.com/);
- SpringerLink (https://link.springer.com/);
- Wiley (https://onlinelibrary.wiley.com/);
- MDPI (https://www.mdpi.com/).

After that, the selection process described in Section III-D was applied so as to identify the set of relevant primary studies that we analysed to answer the research questions. We present the results of our analysis in Section IV and Section V.

B. RESEARCH QUESTIONS

Implementation of deep and throughout safety assessment was a strong requirement for critical industries for a long time, but the essential rise of cyberattacks and malware targeted for this particular sector during the last 5 years has intensified the discussions around the convergence of safety and cybersecurity.

Traditional safety assessment approaches either did not focus on cybersecurity, leaving its issues to particular separate disciplines, or at most referred to generic cybersecurity approaches and guidelines which were not feasible to follow or implement.

To overcome the abovementioned challenges, traditional approaches were modified in different ways, so as to consider cybersecurity-related threats and make assessment more comprehensive. Such modifications could be the following:

- assessment techniques determine the impact of cybersecurity threats and vulnerabilities on system safety as an adjunct to 'traditional' hazards; an example of such an approach is Hazard Analysis and Risk Assessment (HARA) combined with Threat Analysis and Risk Assessment (TARA);
- adaptation of traditional dependability and safety assessment techniques to the cybersecurity domain; an example of such an approach is Intrusion Modes, Effects, and Criticality Analysis (IMECA), where the traditional Failure Modes, Effects, and Criticality Analysis (FMECA) approach is utilized for intrusion analysis;
- include combinations of several safety and cybersecurity assessment techniques.

Despite the variety of approaches safety and cybersecurity assessment for critical industries is still a challenge requiring further investigation.

The following research questions were formulated to attain such investigation:

- (RQ1) Which safety indicators (metrics) are considered during safety assessment?
- (RQ2) Which cybersecurity indicators (metrics) are considered during cybersecurity assessment?
- (RQ3) Which techniques (classical, modified, combinations) are used for safety assessment?
- (RQ4) Which techniques (classical, modified, combinations) are used for cybersecurity assessment?
- (RQ5) Which limitations are applied to techniques currently used?

C. SEARCH STRATEGY

The search string used for the selection of studies is presented in Table 2. Only studies published from 2018 through 2022 inclusive were considered.

TABLE 2. Search string.

({safety} < OR > {cybersecurity} < OR > {security}) < AND > ({assessment} < OR > {evaluation} < OR > {analysis}) < AND > ({nuclear} < OR > {oil} < OR > {vehicle} < OR > {transport} < OR > {railway} < OR > {automotive})

D. SELECTION PROCESS

The following inclusion and exclusion criteria (Table 3) were applied to the studies identified using the search string (figure 1).

TABLE 3. Inclusion and exclusion criteria.

Inclusion Criteria
• Papers published in journals or conference proceedings. • Studies presenting a modified technique or combination of several techniques and description of usage • Studies providing use cases to support the performed assessment or introducing a tool • Studies that are peer-reviewed
Exclusion Criteria
• Studies that are PhD thesis, published in workshop proceedings and book chapters. • Studies from fields different from safety and cybersecurity assessment in critical industries domains (nuclear, aerospace, maritime, oil and gas, railway, automotive) • Studies that do not provide clear evidence of the benefits obtained through a proposed modified technique (criteria of clearness: measurable results compared to unmodified technique(s)) • Multiple studies authored by the same researchers on the same/similar topic (in this case the more relevant source was chosen, i.e. journal paper had priority over conference proceeding, most recent one had priority over older ones) • Studies that are not written in English

To ensure quality assessment the following questions were addressed:

- Are claims clearly defined?
- Is it possible to reuse the presented assessment technique, its modification or a combination of techniques (is description detailed enough)?

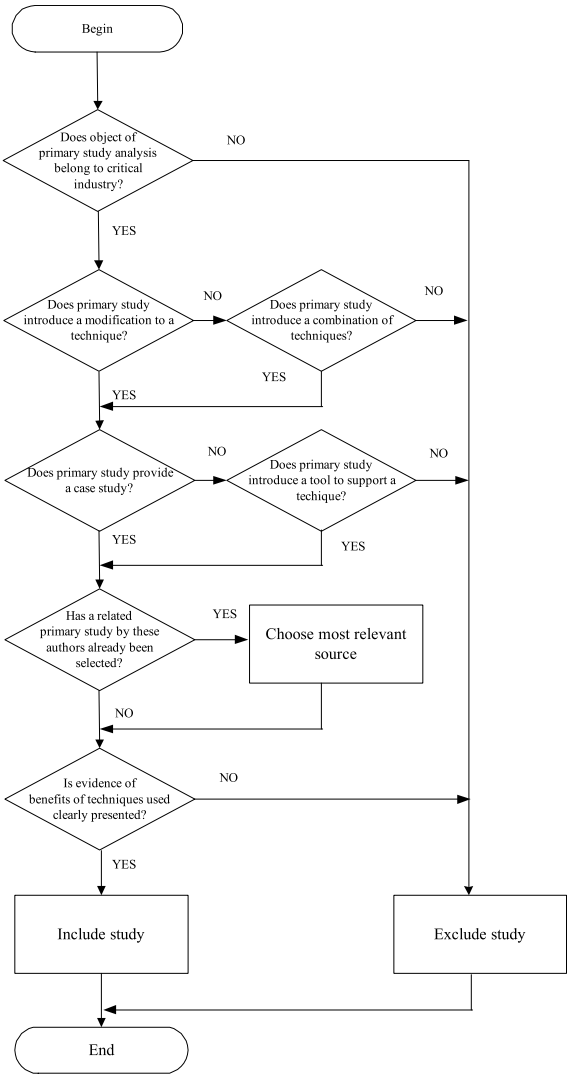

FIGURE 1. Flowchart of the selection process for each primary study.

Initially, 320 records (acquired between 2018 and 2022 inclusive) were identified according to the search string. After examining titles, abstracts and keywords, the number of records was reduced to 187 by excluding not relevant studies.

After the application of the selection process shown on Fig. 1, 49 papers were selected from a total number of 187.

IV. DATA ANALYSIS

A. DISTRIBUTION BY YEAR AND TYPE

The distribution of primary studies by years in the window 2018-2022 is shown in Fig. 2.

Most of the studies are journal papers as shown in Table 4 and Fig. 3, but conference proceedings were also analysed.

B. OVERVIEW OF THE ADOPTED TECHNIQUES AND ASSESSMENT METRICS

The performed research has shown that techniques listed in Table 5 below are typically used during the safety and/or cybersecurity assessment process.

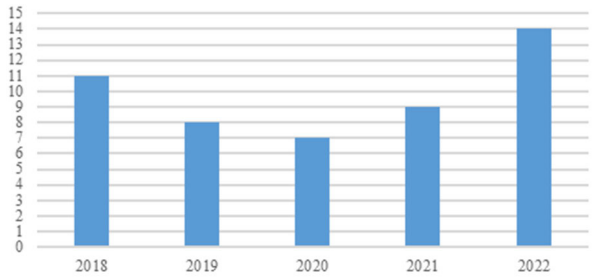

FIGURE 2. Distribution of primary studies by year.

TABLE 4. Year and type of primary studies.

Year	Type	List of References
2018	Conference	[26], [27], [50]
	Journal	[18], [21], [29], [32], [39], [40], [45], [51]
2019	Conference	[38]
	Journal	[1], [23], [33], [34], [35], [37], [47]
2020	Conference	-
	Journal	[12], [20], [22], [36], [46], [49], [52]
2021	Conference	[2], [4], [6], [7], [42], [48]
	Journal	[11], [28], [31]
2022	Conference	[3], [14]
	Journal	[5], [8], [9], [10], [13], [15], [16], [17], [25], [44], [43], [53]

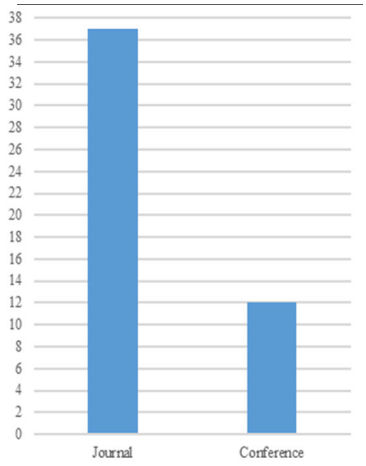

FIGURE 3. Distribution of primary studies by type.

We classified techniques listed in Table 5 by their focus (safety or cybersecurity) and analysis process (spreadsheet-based, scenario-based, tree-based, and model-based) and prepared a taxonomy shown in Fig. 4.

By spreadsheet-based process (Fig. 5) we mean an approach that gathers data into a single spreadsheet and the main deliverables (metrics, assessment results) are based

TABLE 5. Techniques used for safety and cybersecurity analysis.

Technique Id	Abbreviation	Technique Title
T1	FMEDA	Failure Modes, Effects, and Diagnostics Analysis
T2	FTA	Fault Tree Analysis
T3	BDMP	Boolean-driven Markov process
T4	HARA	Hazard Analysis and Risk Assessment
T5	RBD	Reliability Block Diagram
T6	RBI	Risk-based inspection
T7	ATA	Attack tree analysis
T8	PSA	Probabilistic safety assessment
T9	SM	Semi-Markov
T10	BN	Bayesian Networks
T11	MC	Monte-Carlo Simulation
T12	BA	Bowtie Analysis
T13	ETA	Event Tree Analysis
T14	FMEA / FMECA	Failure Modes and Effects Analysis / Failure Modes, Effects, and Criticality Analysis
T15	STAMP	Systems-Theoretic Accident Model and Process
T16	DVAG	Dynamic Vulnerability Assessment Graph
T17	MBAEM	Model-based Assurance Evidence Management.
T18	TARA	Threat Analysis and Risk Assessment
T19	IMECA	Intrusion Modes, Effects, and Criticality Analysis
T20	CRA	Cybersecurity Risk Assessment

on processing the spreadsheet data. A typical example of a spreadsheet-based process is a failure mode, effect, and diagnostic analysis (FMEDA), a systematic analysis technique to obtain subsystem/product level failure rates, failure modes, and diagnostic capability. The main purpose of FMEDA is to evaluate hardware architecture metrics and safety goal violations due to random hardware failures and provide sufficient information to improve safety gaps if the required hardware safety level is not fulfilled [54].

Another example of spreadsheet-based process is a risk-based inspection (RBI) which is well-established and used in the Oil& Gas and Chemical industries. This approach, along with risk-based maintenance, is described by API RP 581 [55], originally developed for application in the refining industry. The standard represents a correlation between maintenance activities and main events in the industries. RBI is also adapted and applied in many other sectors and inspection activities, allowing for the identification of failure mechanisms and rates based on equipment status.

Instead, tree-based techniques (Fig. 6) process graphical representation in the form of a tree. The classical example of a tree-based technique is a fault tree analysis (FTA) used for the reliability assessment of a system. FTA is a deductive

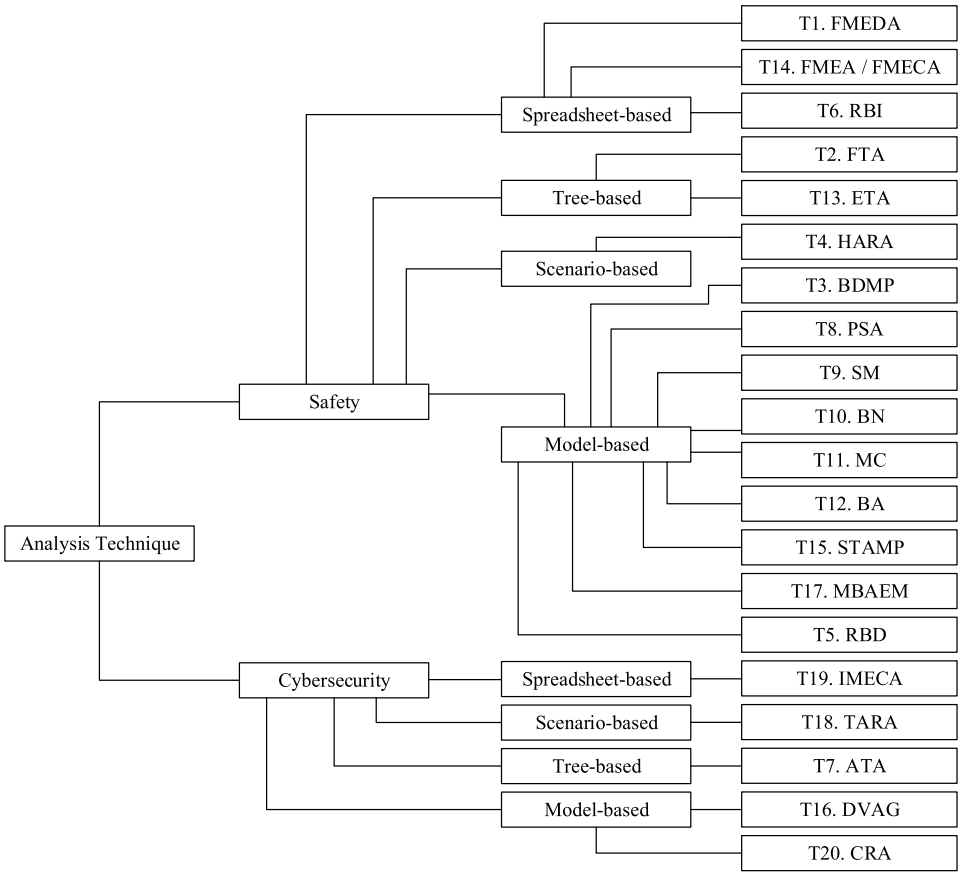

FIGURE 4. Taxonomy of analysis techniques.

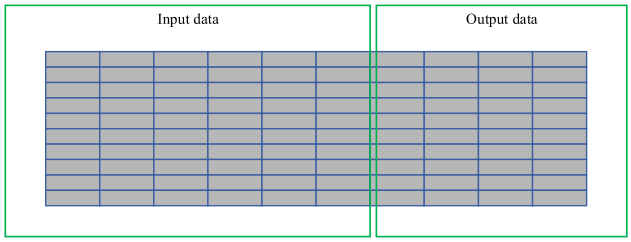

FIGURE 5. Spreadsheet-based technique.

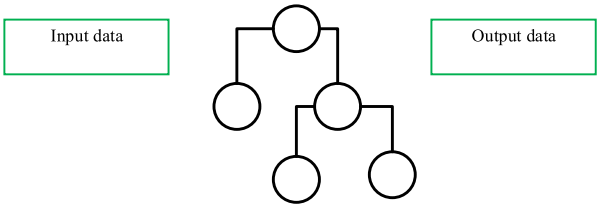

FIGURE 6. Tree-based technique.

process by means of which an undesirable event, called the top event, is postulated, and after that, the possible ways for this event to occur are systematically deduced. The deduction process is performed so that the fault tree embodies all

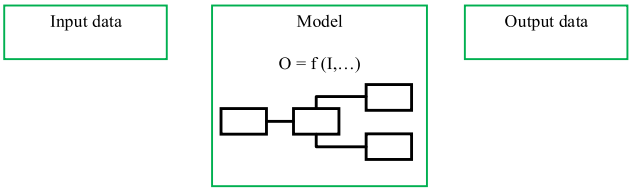

FIGURE 7. Model-based technique.

component failures (i.e., failure modes) that contribute to the occurrence of the top event. The fault tree itself is a graphical representation of the various combinations of failures that led to the occurrence of the top event [56]. In [45] it is proposed to apply FTA for cybersecurity assessment by using a model that integrates fault tree analysis, decision theory, and fuzzy theory to ascertain the current causes of cyberattack prevention failures and determine the vulnerability of a given cybersecurity system. Moreover, for cybersecurity assessment, another tree-based technique called attack tree analysis (ATA) is actively utilized [57].

By model-based techniques (Fig. 7) we mean approaches that perform an assessment using different models – graphs, equations etc.

For example, reliability block diagrams (RBD) represent sequences of system components and their connections. Each

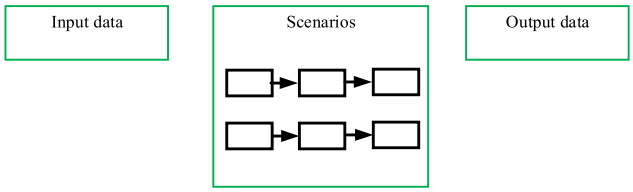

FIGURE 8. Scenario-based technique.

sequence consists of an input point and output point, several blocks representing system components, and the multiple paths from the input point to the output point that represent successful system operations, where an interruption of these paths may lead to the failure of the whole system. Therefore, an RBD model represents the static topology of I&C reliability, where the topology can be a serial, parallel or a combination of serial and parallel sections. Contrary to FTA, RBD models are success-oriented sequences that describe the function of a system by probabilistic means. Component blocks in an RBD are arranged to illustrate the proper combinations of working components that keep the entire system operational and, therefore, safe. Failure of a component can be represented by removing the component as well as its connections with other components from the sequence. When the number and position of failed components in the RBD model are such that there is no connection between the input and output point, the whole system fails.

Another example is a Bayesian network (BN) that represents a hypothesis of rationalizing from uncertain evidence to uncertain conclusions since it can perform the factorization of the collective distribution of variables, based on the conditional dependencies. BN helps to address uncertainty and incompleteness problems; thus, it is extensively applied in several domains. BNs are generally utilized for examining the hazards and vulnerabilities of networks, which are acyclic graphs that provide a quantitative and qualitative assessment of risks.

Model-based assurance evidence management (MBAEM) is another model-based technique that considers different activities for assurance evidence management, namely the determination of the evidence to provide, the possibility of reusing evidence, the collection of evidence information, tracing, evaluation, and change impact analysis of assurance evidence, and the use of the evidence for, e.g., compliance management and argumentation.

Finally, Probabilistic Safety Assessment (PSA) is the most common method to assess the risk of a nuclear power plant. It employs a graphical approach based on event and fault tree methods.

As for scenario-based processes (Fig. 8), they are typically based on profiling of scenarios collection obtained from different sources (accident, research, expert data, etc.) by focusing on safety and/or cybersecurity-relevant scenarios.

A typical example of a scenario-based process is HARA, where malfunctions and/or the functional insufficiencies are analyzed in terms of identification of both safety-relevant scenarios (known-safe and known-unsafe), as well as a set of unknown-unsafe scenarios, with further focus on required countermeasures.

The list of metrics is given in Table 6 and includes both safety and cybersecurity related metrics.

TABLE 6. Assessment metrics.

Metric Id	Metric Name
M1	SFF – Safe Failure Fraction
M2	SIL – Safety Integrity Level
M3	SPFM – Single-Point Fault Metric
M4	LFM – Latent (Multi-Point) Fault Metric
M5	PMHF – Probabilistic Metric for Hardware Failures
M6	PFH – Probability of Failure on Demand per Hour
M7	SL – Security Level
M8	ASIL – Automotive Safety Integrity Level
M9	Risk
M10	CDF – core damage frequency
M11	InTo-CSI – Intrusion Tolerance-based Cyber Security Index
M12	MTTC – Mean Time To Compromise
M13	CVSS – common vulnerability scoring system

SFF is a metric used to measure the likelihood of getting a dangerous failure that is not detected by diagnostics.

SIL is used to claim that all safety instrumented functions are operating satisfactorily under all stated conditions within a stated period of time.

SPFM is a hardware architectural metric used to show the sufficiency of safety mechanisms to prevent risk from single-point faults.

LFM is a hardware architectural metric used to show the sufficiency of safety mechanisms to prevent risk from latent faults.

PMHF is a probability of a safety goal violation caused by a random hardware failure.

PFH is the probability of dangerous failure that would prevent the system to be able to perform its safety function when required.

SL is a metric to measure how well a system component is protected from a certain level of threat and potential vulnerabilities.

ASIL is a risk classification metric.

CDF is a metric used to measure frequency and consequences considering initiating event frequency with system failure probabilities and fatalities (or environmental effects).

InTo-CSI is an index defined through relative comparison of two security states of the same system: a system without any cyber security controls, and a system with scrutiny controls.

The value of MTTC is the estimated figure of the time required for the valid attack assuming uniformly expended efforts.

CVSS is used to evaluate the severity of vulnerabilities, representing the virtual consequences on the vulnerable component in terms of confidentiality, integrity, and availability.

A considerable number of studies use Risk to represent the outputs of assessment technique utilization. In most cases, this metric represents the likelihood of the hazardous event and the severity of its consequences. Typical examples of what is used as a risk in the analysed studies are provided below. In [1], [4], [7], and [9] traditional risk priority number (RPN) is used, which is determined by three indicators: effect severity, occurrence probability, and detection difficulty. In [3] it is extended to cover risk interaction. In [5] risk assessment objectivity and accuracy are enhanced by the utilization of fuzzy confidence interval number (FCIN), generalized trapezoidal fuzzy numbers (GTrFN) evaluation model and the evaluation parameter sensitivity analysis. In [6] risk is calculated using the severity of the hazard, the exposure of that particular situation and the controllability of the system to mitigate hazardous situations. In [8] fairness risk is also considered separately from safety risk. In [10] special attention is given to considering assurance risks. In [12] risk is computed using potential risk impact due to vulnerabilities/attacks and the likelihood of the risk. In [13] risk includes attack cost, attack difficulty, and detected possibility.

C. USING PRIMARY STUDIES TO ANSWER RESEARCH QUESTIONS

To answer research questions (RQ1) and (RQ2), we have arranged the selected primary studies in the form of a table with the following columns (see Table 7):

- Reference;
- Techniques used (see Table 5);
- Metrics (see Table 6).

Based on the analysed studies, the resulting most popular techniques are listed in Table 8 below.

Therefore, the answer to RQ1 includes the following metrics: PFH, SFF, SIL, and ASIL are the most popular safety metrics. Also, in many studies, generic risk metric is used.

As for cybersecurity (RQ2), SL, MTTC, InTo-CSI, and CVSS scores are used as quantitative metrics. Just like with safety, the major part of studies considers generic risk metric more appropriate and comprehensive.

To answer research questions (RQ3) and (RQ4), we have arranged the list of selected primary studies in the form of a table with the following columns (see Table 10):

- Reference;
- Focus on safety;
- Focus on cybersecurity;
- Usage of several assessment techniques;
- Usage of modified assessment techniques;

TABLE 7. Techniques and metrics of primary studies.

Ref.	Techniques	Metrics
[1]	T14, T2	M9
[2]	T1, T2	M3, M4, M5
[3]	T14	M9
[4]	T14	M9
[5]	T14	M9
[6]	T4	M9
[7]	T14	M9
[8]	T14	M9
[9]	T14	M9
[10]	T17	M9
[11]	T18, T4	M8
[12]	T18	M9
[13]	T20	M9
[14]	T19	M9
[15]	T10	M13
[16]	T7	M9
[17]	T1,T14	M9
[18]	T11	M9
[20]	T8, T2, T13	M9, M10
[21]	T13	M11, M12
[22]	T9, T2, T13	M9
[23]	T2, T8, T13	M9
[25]	T16	M9
[26]	T8	M7, M9
[27]	T2	M9
[28]	T6	M9, M6
[29]	T10	M9
[31]	T15	M9
[32]	T10	M9
[33]	T10	M9
[34]	T16	M9
[35]	T10	M9
[36]	T10	M9
[37]	T2, T4, T14	M5, M6
[38]	T9, T10	M9
[39]	T12, T7	M9
[40]	T14	M9
[42]	T4, T18	M9
[43]	T2, T14	M9
[44]	T1	M1, M2, M3, M4, M5, M8
[45]	T2	M9
[46]	T2, T14	M8
[47]	T2	M9
[48]	T2	M9
[49]	T1	M9

TABLE 7. *(Continued.)* **Techniques and metrics of primary studies.**

[50]	T2, T9	M9
[51]	T2	M9
[52]	T5	M9
[53]	T10	M9

TABLE 8. **The most used techniques for safety and cybersecurity assessment.**

Technique Id	Number of references	References
T2	10	[1], [2], [20], [22], [23], [46], [47], [48], [50], [51]
T14	9	[1], [3], [4], [5], [7], [8], [9], [17], [37], [46]
T10	7	[29], [32], [33], [35], [36], [38], [53]
T1	4	[2], [17], [44], [49]
T13	4	[20], [21], [22], [23]
T9	3	[22], [38], [50]
T8	3	[20], [23], [26]

TABLE 9. **Types of case studies.**

Case study type Id	Case study type
C0	No case study provided.
C1	The provided case study is only theoretical (formulas are provided, but no calculations are performed).
C2	The provided case study is demonstrated using a simulated environment and artificial input values.
C3	The provided case study is demonstrated using a simulated environment, but real input values are used.
C4	The provided case study demonstrates application on a real system with real values used.

- Generalization (i.e. utilization of techniques initially designed for safety assessment to assess cybersecurity with minor modifications of the technique itself) of assessment techniques;
- Availability of case study and its type according to Table 9 below.

The list of possible types of case studies was prepared after a preliminary analysis of primary studies. Types and corresponding identifiers are provided in Table 9.

For safety assessment (RQ3), modifications of well-known reliability assessment techniques like FMEA/FMECA, FTA, and Bayesian networks are mostly used.

As for cybersecurity (RQ4), either specific modifications are utilized (like IMECA), or in most cases cybersecurity assessment is integrated into the overall safety assessment process. In most cases, the assessment process is risk-based, including risk identification, risk analysis, risk evaluation, and documentation.

The main limitations identified (RQ5) include dimension issues (the approach is not applicable due to a huge number of components to be analyzed) and too strict assumptions (like independent failures or attacks). To overcome such limitations, modifications to methodologies used are being introduced, for example, focusing only on elements that are part of the safety function for complex safety systems, etc.

V. KEY FINDINGS

The discussion on key findings focuses primarily on the most interesting results regarding the adopted assessment techniques, namely their combined usage, proposed modifications, and attempts toward generalization. A few other general findings are also highlighted.

A. USE OF SEVERAL ASSESSMENT TECHNIQUES

As shown in Table 7, altogether 28 studies were focusing on several assessment techniques utilization. The main motivation to use several techniques derives from the fact that the results of one technique usually either don't cover all the non-functional aspects of interest (i.e. the technique is focused on safety and doesn't consider cybersecurity issues) or need to be verified through a different technique (i.e. different techniques are used in parallel and then the obtained results are being compared and processed).

Though cybersecurity analysis is implemented in the overall I&C design procedure, it is generally not combined with the safety analysis development. In several analysed studies, the introduced approaches comprehended the significance of integrated safety and cybersecurity analysis and intended to incorporate both into a joint methodological process. For instance, two applicable techniques, which describe the integration of cybersecurity into safety analysis (cybersecurity-informed safety, or security-informed safety), recommend a merging of fault tree analysis (FTA) with attack tree analysis (ATA) or Boolean-driven Markov processes (BDMP). Other introduced approaches either combine safety and cybersecurity methods, e.g., ATA and bowtie analysis, or integrate both fields (i.e. implement strategies devoted to ''unintentional'' (safety) events as well as to ''intentional'' (cybersecurity) chains).

In [42], the scenario-based approach utilizing HARA and TARA techniques is pursued. In particular, correlation of damage scenario and hazard scenario is performed, so as to show the connection of safety with cybersecurity.

The authors of [37] present a framework for performing safety analyses, risk assessment, and safety requirements management using semi-formal and formal techniques like FMEA, FMECA, and FTA. The framework implements a compositional V-cycle methodology, covering all phases of the system development lifecycle. Future integration of other assessment techniques into the framework is planned by the authors.

TABLE 10. The focus of the primary studies.

Ref.	Safety	Cybersecurity	Several assessment techniques	Modification of assessment techniques	Assessment technique generalization	Availability of case study
[1]	√		√	√		C1
[2], [46]	√		√			C0
[3], [8], [9], [33], [48], [49]	√			√		C1
[4],[22]	√			√		C3
[5], [7]	√			√		C2
[6], [38]	√		√			C2
[10]	√		√	√	√	C2
[11], [17]	√	√	√		√	C1
[12], [51]		√	√	√		C1
[13], [14], [26]		√	√	√		C2
[15], [18], [21], [25]		√		√		C2
[16], [36], [53]		√	√			C1
[20]		√	√			C2
[23], [40], [45]		√		√		C1
[27]	√	√		√		C2
[28], [29], [32]	√		√			C1
[31]	√	√	√		√	C2
[34]	√	√	√	√	√	C1
[35]	√	√	√			C1
[37], [47]	√		√	√		C1
[39]	√	√		√	√	C1
[42]	√	√	√			C2
[43]	√	√	√	√	√	C2
[44], [50]	√		√	√		C2
[52]	√	√	√	√		C1

B. MODIFICATION OF ASSESSMENT TECHNIQUES

In 33 studies, listed in Table 10, modifications of assessment techniques are considered. Among the reasons of modification, the following are mentioned: dimension problem of the technique, reduction of resources required to perform the analysis, and application of well-known approaches to different domains.

In [5] FMEA is modified by the introduction of the risk evaluation methodology for controlling multi-uncertainties in the assessment process. It is shown that the proposed methodology can significantly improve the risk assessment results and the risk discrimination of failure modes, but at the current stage controlling only a single uncertainty is implemented.

Authors of [4] propose a novel approach to calculate risk priority numbers based on factors like severity, occurrence, and detection during the application of FMEA, and outline that classical FMEA only considers risk factors regarding safety, ignoring other factors (i.e. cybersecurity or economic impacts).

In [27] initial events for FTA include not only safety-related issues like failures in components or subsystems but also cybersecurity ones like attacks.

It cannot be too highly stressed that several reviewed studies provide evidence that methods originally intended for reliability assessment could be successfully utilized for safety and/or cybersecurity assessment with minor modifications. For example, the probabilistic risk assessment method which is the most general method to get the risk information could be applied to cybersecurity, safety block diagrams, and cybersecurity block diagrams, etc.

Finally, on the aspect of safety and cybersecurity protection mechanisms, it is suggested that they could be based on recent technologies successfully used in other sectors, such as blockchain technology [41], [52].

C. ASSESSMENT TECHNIQUES GENERALIZATION

Generalization of assessment techniques is addressed only in 7 studies but looks as a promising direction for research. The main idea is to develop generic approaches that could be parametrized, so as to be 'tuned' to a required domain or set of metrics. The relatively limited number of studies could be explained by the complexity of such task and the amount of resources needed to provide representative case studies.

In [43], a hybrid ontology is presented that could be utilized for safety and cybersecurity assessment. The authors claim that a true combined approach also needs to include dependability engineering to harmonize the basic concepts between all three disciplines: safety, cybersecurity and dependability. It is also highlighted that focusing on cybersecurity risks requires more effort compared to safety risk analyses due to risk nature: safety risks are based on systematic faults or quite well-known random faults and allow implementation of a systematic assessment approach, while cybersecurity risks are mainly caused by malicious acts which originate a huge number of possible threat scenarios.

The authors of [31] propose an ontological metamodel that considers safety, cybersecurity, and resiliency. Co-engineering of safety and cybersecurity is based on a system losses approach, i.e. system losses caused either by safety or cybersecurity violations are prioritized so as to provide a structured approach for their mitigation. It is claimed that such an approach allows achieving an overall increase in scalability, usability, and unification of already existing models.

In [17] a generic XMECA (FMECA + IMECA = XMECA) technique is presented, intended to cover different domains – safety and cybersecurity – using a unified approach. Verification of XMECA results is performed using EUMECA (E – error, U – uncertainty) with a focus on decisions and judgments made by experts during the XMECA process.

D. METRICS AND CASE STUDIES

Techniques used in a majority of the analysed studies are tailored to risk assessment (risk-based approach), covering only failures, only vulnerabilities, or covering both of them.

Some cybersecurity risk assessment methods with application on real I&C systems are based on national standards. An example is the Chinese national standard GB/T 36466-2018: Information security technology-Implementation guide [58]. According to this document, four risk elements including asset, threat, vulnerability, and protection capability would be first identified and assessed adopting a combination of qualitative methods of expert evaluation and quantitative methods of numerical calculation. Possibility of, and loss from, security incidents then would be calculated through the above four elements and, finally, the risk value is obtained.

Aiming at providing an internationally valid reference methodology, a common international method for combined safety and security modeling, design and assessment is an open and active research topic.

The major part of the case studies presented in the reviewed publications are theoretical ones or taken from realistic contexts but adopting artificial inputs (case studies classified as C1 and C2 in Table 9). Although application to real systems would be highly desirable, this is not expected to be possible in the foreseeable time due to the limitations stated. Indeed, the assumptions adopted to make the technique manageable (e.g., with reference to scalability) are sources of inaccuracy in the obtained results when analyzing realistic systems that do not fully adhere to such assumptions. Devising assessment techniques suitable to deal with real system contexts is an active, challenging research direction.

E. GENERAL FINDINGS

The performed review shows that the focus of recent publications is more on cybersecurity and less on safety as a whole. This could be explained by the modernization of control systems in critical industries, especially towards more flexibility, but a drawback is that new potential cybersecurity issues are introduced.

With the integration of information systems and physical systems, the cybersecurity of information systems and functional safety of physical systems interact with each other, resulting in a type of new comprehensive problem and introducing serious risks. New approaches addressing this issue are needed.

Existing technologies of the I&C system, including programmable logic controllers (PLCs) and FPGA-based platforms, are vulnerable as they are attractive targets for the cyberattack threats. Appropriate risk assessment that includes not only failure analysis and reliability issues but possible intrusions can strongly contribute to enhancing cybersecurity and safety, by providing support to the development of preventive measures in avoiding/mitigating potential cyberattacks.

VI. THREATS TO THE VALIDITY OF THIS STUDY

In this section, we discuss major threats to the validity of this mapping study.

The possibility exists that some relevant studies have not been chosen due to the expertise of the authors. We mitigated this threat, as much as possible, by examining the titles, abstract, and keywords at the first stage and going deeper into

the checks at the second stage, following the steps shown in Figure 1. Moreover, several meetings have been carried out during the selection process, to discuss possible doubts.

Another potential threat relates to the defined search string, since a different set of primary studies may be derived with even slight variation of the search string. This threat characterizes all systematic surveys. To mitigate it, we discussed in depth the goal of the planned study, for which clear and relevant research questions were then identified and used to build the search question.

Regarding the quality of reviewed studies, we did not adopt any specific quality criteria, as usually recommended when performing systematic literature reviews and mapping studies. However, we excluded studies that had not undergone a peer-review process, thus assuring the scientific quality of the selected papers.

Potential issues on generalization of the obtained results constitute another threat that is common to all the mapping studies. While it is not feasible to generalize the drawn conclusions to the whole universe of primary studies on a specific topic, to mitigate this threat we considered only primary studies published during the last 5 years, thus focusing mainly on current trends in the field.

VII. CONCLUSION

This mapping study analysed 49 papers dealing with cybersecurity and safety assessment. Major concluding points include:

- It is observed that out of the 49 included studies, 16 focus on cybersecurity only, 23 focus on safety only, and the remaining 10 are based on a joint approach to safety and cybersecurity. This distribution trend testifies that needs in the different application domains are rather wide in terms of metrics of primary interest.
- It should be particularly emphasized that the majority of techniques used in studies were either based on simulation analysis or theoretical concepts.
- A great majority of the studies (33 out of 49) propose modifications/extensions of classical assessment techniques, either to address joint safety and cybersecurity analysis, or to accommodate new needs of the application context. This trend shows that classical assessment techniques, well consolidated by long-lasting practice, are still very popular and constitute a basis for enhancements to satisfy more sophisticated analysis needs.

The results of the performed survey indicate the lack of a systematic process of unified safety and cybersecurity assessment.

Among future research directions for safety and cybersecurity integration:

- There is a clear need in putting efforts into developing a generic technique (method or standard) supported by tool to combine cybersecurity and safety, which can be helpful for different applications in critical industries, since the significance of integrating both measures was demonstrated in this mapping study, and a generic approach may offer benefits such as feasibility and flexibility.
- It is observed that there are various approaches for evaluating the indicators of interest, including the usage of different assessment techniques and comparison of their outputs for validation purposes. A more extended investigation is necessary to estimate the accuracy and efficiency of assessment mechanisms, in order to find the optimal option to employ in a specific context, guided by criteria of accuracy and cost.

REFERENCES

[1] X. Zhang, Y. Li, Y. Ran, and G. Zhang, "A hybrid multilevel FTA-FMEA method for a flexible manufacturing cell based on meta-action and TOPSIS," *IEEE Access*, vol. 7, pp. 110306–110315, 2019, doi: 10.1109/ACCESS.2019.2934189.

[2] C. Kymal and O. G. Gruska, "Integrating FMEAs, FMEDAs, and fault trees for functional safety," in *Proc. Annu. Rel. Maintainability Symp. (RAMS)*, May 2021, pp. 1–6, doi: 10.1109/RAMS48097.2021.9605786.

[3] P. Liu, Y. Xu, and Y. Li, "An improved failure mode and effect analysis model for automatic transmission risk assessment considering the risk interaction," *IEEE Trans. Rel.*, early access, Oct. 27, 2022, doi: 10.1109/TR.2022.3215110.

[4] S. K. Akula and H. Salehfar, "Risk-based classical failure mode and effect analysis (FMEA) of microgrid cyber-physical energy systems," in *Proc. North Amer. Power Symp. (NAPS)*, College Station, TX, USA, Nov. 2021, pp. 1–6, doi: 10.1109/NAPS52732.2021.9654717.

[5] Y. Liu, B. Chen, Q. Dong, W. Liu, W. Nie, and C. Yang, "Failure mode risk assessment methodology for controlling multi-uncertainties in the evaluation process," *Eng. Appl. Artif. Intell.*, vol. 116, Nov. 2022, Art. no. 105470, doi: 10.1016/j.engappai.2022.105470.

[6] A. R. Patel and P. Liggesmeyer, "Machine learning based dynamic risk assessment for autonomous vehicles," in *Proc. Int. Symp. Comput. Sci. Intell. Controls (ISCSIC)*, Rome, Italy, Nov. 2021, pp. 73–77, doi: 10.1109/ISCSIC54682.2021.00024.

[7] L. Pokoradi, S. Kocak, and E. Toth-Laufer, "Fuzzy hierarchical failure mode and effect analysis," in *Proc. IEEE 19th Int. Symp. Intell. Syst. Informat. (SISY)*, Sep. 2021, pp. 71–76, doi: 10.1109/SISY52375.2021.9582523.

[8] J. Li and M. Chignell, "FMEA-AI: AI fairness impact assessment using failure mode and effects analysis," *AI Ethics*, vol. 2, no. 4, pp. 837–850, Nov. 2022, doi: 10.1007/s43681-022-00145-9.

[9] S. E. Fatollah, R. Dabbagh, and A. S. Jalavat, "An extended approach using failure modes and effects analysis (FMEA) and weighting method for assessment of risk factors in the petrochemical industry," *Environ., Develop. Sustainability*, pp. 1–26, Oct. 2022, doi: 10.1007/s10668-022-02609-8.

[10] J. L. de la Vara, A. S. García, J. Valero, and C. Ayora, "Model-based assurance evidence management for safety–critical systems," *Softw. Syst. Model.*, vol. 21, no. 6, pp. 2329–2365, Dec. 2022, doi: 10.1007/s10270-021-00957-z.

[11] C. Schwarzl, N. Marko, H. Martin, V. E. Jiménez, J. C. Triginer, B. Winkler, and R. Bramberger, "Safety and security co-engineering for highly automated vehicles," *Elektrotechnik Informationstechnik*, vol. 138, no. 7, pp. 469–479, Nov. 2021, doi: 10.1007/s00502-021-00934-w.

[12] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan, "IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process," *EURASIP J. Inf. Secur.*, vol. 2020, no. 1, pp. 1–18, Dec. 2020, doi: 10.1186/s13635-020-00111-0.

[13] H. Guo, L. Ding, and W. Xu, "Cybersecurity risk assessment of industrial control systems based on order—A divergence measures under an interval-valued intuitionistic fuzzy environment," *IEEE Access*, vol. 10, pp. 43751–43765, 2022, doi: 10.1109/ACCESS.2022.3169133.

[14] A. Abakumov and V. Kharchenko, "Combining IMECA analysis and penetration testing to assess the cybersecurity of industrial robotic systems," in *Proc. 12th Int. Conf. Dependable Syst., Services Technol. (DESSERT)*, Athens, Greece, Dec. 2022, pp. 1–7, doi: 10.1109/DESSERT58054.2022.10018823.

[15] Y. Wang, B. Yu, H. Yu, L. Xiao, H. Ji, and Y. Zhao, "Automotive cybersecurity vulnerability assessment using the common vulnerability scoring system and Bayesian network model," *IEEE Syst. J.*, vol. 17, no. 2, pp. 2880–2891, Jun. 2023, doi: 10.1109/JSYST.2022.3230097.

[16] S.-G. Tân, I.-H. Liu, and J.-S. Li, "Threat analysis of cyber security exercise for reservoir testbed based on attack tree," in *Proc. 10th Int. Symp. Comput. Netw. Workshops (CANDARW)*, Himeji, Japan, Nov. 2022, pp. 375–379, doi: 10.1109/CANDARW57323.2022.00023.

[17] I. Babeshko, O. Illiashenko, V. Kharchenko, and K. Leontiev, "Towards trustworthy safety assessment by providing expert and tool-based XMECA techniques," *Mathematics*, vol. 10, no. 13, p. 2297, Jun. 2022, doi: 10.3390/math10132297.

[18] W. Wang, A. Cammi, F. D. Maio, S. Lorenzi, and E. Zio, "A Monte Carlo-based exploration framework for identifying components vulnerable to cyber threats in nuclear power plants," *Rel. Eng. Syst. Saf.*, vol. 175, pp. 24–37, Jul. 2018.

[19] J. Peterson, M. Haney, and R. A. Borrelli, "An overview of methodologies for cybersecurity vulnerability assessments conducted in nuclear power plants," *Nucl. Eng. Des.*, vol. 346, pp. 75–84, May 2019.

[20] J. W. Park and S. J. Lee, "A quantitative assessment framework for cyber-attack scenarios on nuclear power plants using relative difficulty and consequence," *Ann. Nucl. Energy*, vol. 142, Jul. 2020, Art. no. 107432.

[21] C. Lee, H. B. Yim, and P. H. Seong, "Development of a quantitative method for evaluating the efficacy of cyber security controls in NPPs based on intrusion tolerant concept," *Ann. Nucl. Energy*, vol. 112, pp. 646–654, Feb. 2018.

[22] Y. Zhao, L. Huang, C. Smidts, and Q. Zhu, "Finite-horizon semi-Markov game for time-sensitive attack response and probabilistic risk assessment in nuclear power plants," *Rel. Eng. Syst. Saf.*, vol. 201, Sep. 2020, Art. no. 106878.

[23] J. W. Park and S. J. Lee, "Probabilistic safety assessment-based importance analysis of cyber-attacks on nuclear power plants," *Nucl. Eng. Technol.*, vol. 51, no. 1, pp. 138–145, Feb. 2019.

[24] N. Chowdhury, "CS measures for nuclear power plant protection: A systematic literature review," *Signals*, vol. 2, no. 4, pp. 803–819, Nov. 2021, doi: 10.3390/signals2040046.

[25] A. Boudermine, R. Khatoun, and J.-H. Choyer, "Attack graph-based solution for vulnerabilities impact assessment in dynamic environment," in *Proc. 5th Conf. Cloud Internet Things (CIoT)*, Marrakesh, Morocco, Mar. 2022, pp. 24–31, doi: 10.1109/CIoT53061.2022.9766588.

[26] D. Liu, Y. Chen, J. Shi, and D. Chen, "Study on cyber security risk assessment of digital instrumentation & control system of nuclear power plant," in *Proc. Int. Conf. Power Syst. Technol. (POWERCON)*, Guangzhou, China, Nov. 2018, pp. 4742–4750.

[27] R. B. Ferreira, D. M. Baum, E. C. P. Neto, M. R. Martins, J. R. Almeida, P. S. Cugnasca, and J. B. Camargo, "A risk analysis of unmanned aircraft systems (UAS) integration into non-segregate airspace," in *Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS)*, Dallas, TX, USA, Jun. 2018, pp. 42–51, doi: 10.1109/ICUAS.2018.8453455.

[28] B. H. Davatgar, N. Paltrinieri, and R. Bubbico, "Safety barrier management: Risk-based approach for the oil and gas sector," *J. Mar. Sci. Eng.*, vol. 9, no. 7, p. 722, Jun. 2021, doi: 10.3390/jmse9070722.

[29] M. Bucelli, N. Paltrinieri, and G. Landucci, "Integrated risk assessment for oil and gas installations in sensitive areas," *Ocean Eng.*, vol. 150, pp. 377–390, Feb. 2018.

[30] S. Pirbhulal, V. Gkioulos, and S. Katsikas, "Towards integration of security and safety measures for critical infrastructures based on Bayesian networks and graph theory: A systematic literature review," *Signals*, vol. 2, no. 4, pp. 771–802, 2021, doi: 10.3390/signals2040045.

[31] G. Bakirtzis, T. Sherburne, S. Adams, B. M. Horowitz, P. A. Beling, and C. H. Fleming, "An ontological metamodel for cyber-physical system safety, security, and resilience coengineering," *Softw. Syst. Model.*, vol. 21, no. 1, pp. 113–137, Feb. 2022, doi: 10.1007/s10270-021-00892-z.

[32] Y. Zhou, C. Li, C. Zhou, and H. Luo, "Using Bayesian network for safety risk analysis of diaphragm wall deflection based on field data," *Rel. Eng. Syst. Saf.*, vol. 180, pp. 152–167, Dec. 2018.

[33] H. Xu, Y. Zhang, H. Li, M. Skitmore, J. Yang, and F. Yu, "Safety risks in rail stations: An interactive approach," *J. Rail Transp. Planning Manage.*, vol. 11, Oct. 2019, Art. no. 100148.

[34] C. Chen, G. Reniers, and N. Khakzad, "Integrating safety and security resources to protect chemical industrial parks from man-made domino effects: A dynamic graph approach," *Rel. Eng. Syst. Saf.*, vol. 191, Nov. 2019, Art. no. 106470.

[35] N. U. I. Hossain, R. Jaradat, S. Hosseini, M. Marufuzzaman, and R. K. Buchanan, "A framework for modeling and assessing system resilience using a Bayesian network: A case study of an interdependent electrical infrastructure system," *Int. J. Crit. Infrastruct. Protection*, vol. 25, pp. 62–83, Jun. 2019.

[36] R. Arief, N. Khakzad, and W. Pieters, "Mitigating cyberattack related domino effects in process plants via ICS segmentation," *J. Inf. Secur. Appl.*, vol. 51, Apr. 2020, Art. no. 102450.

[37] M. Adedjouma and N. Yakymets, "A framework for model-based dependability analysis of cyber-physical systems," in *Proc. IEEE 19th Int. Symp. High Assurance Syst. Eng. (HASE)*, Hangzhou, China, Jan. 2019, pp. 82–89, doi: 10.1109/HASE.2019.00022.

[38] M. Galagedarage Don and F. Khan, "Process fault prognosis using hidden Markov model–Bayesian networks hybrid model," *Ind. Eng. Chem. Res.*, vol. 58, no. 27, pp. 12041–12053, Jul. 2019.

[39] H. Abdo, M. Kaouk, J.-M. 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.*, vol. 72, pp. 175–195, Jan. 2018.

[40] A. Asllani, A. Lari, and N. Lari, "Strengthening information technology security through the failure modes and effects analysis approach," *Int. J. Quality Innov.*, vol. 4, no. 1, pp. 1–14, Dec. 2018, doi: 10.1186/s40887-018-0025-1.

[41] R. Gupta, S. Tanwar, N. Kumar, and S. Tyagi, "Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review," *Comput. Electr. Eng.*, vol. 86, Sep. 2020, Art. no. 106717.

[42] M. Khatun, M. Glaß, and R. Jung, "An approach of scenario-based threat analysis and risk assessment over-the-air updates for an autonomous vehicle," in *Proc. 7th Int. Conf. Autom., Robot. Appl. (ICARA)*, Prague, Czech Republic, Feb. 2021, pp. 122–127, doi: 10.1109/ICARA51699.2021.9376542.

[43] J. Alanen, J. Linnosmaa, T. Malm, N. Papakonstantinou, T. Ahonen, E. Heikkilä, and R. Tiusanen, "Hybrid ontology for safety, security, and dependability risk assessments and security threat analysis (STA) method for industrial control systems," *Rel. Eng. Syst. Saf.*, vol. 220, Apr. 2022, Art. no. 108270, doi: 10.1016/j.ress.2021.108270.

[44] K.-L. Lu and Y.-Y. Chen, "Safety-oriented system hardware architecture exploration in compliance with ISO 26262," *Appl. Sci.*, vol. 12, no. 11, p. 5456, May 2022, doi: 10.3390/app12115456.

[45] A. P. H. D. Gusmão, M. M. Silva, T. Poleto, L. C. E. Silva, and A. P. C. S. Costa, "Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory," *Int. J. Inf. Manage.*, vol. 43, pp. 248–260, Dec. 2018.

[46] G. Xie, Y. Li, Y. Han, Y. Xie, G. Zeng, and R. Li, "Recent advances and future trends for automotive functional safety design methodologies," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 5629–5642, Sep. 2020.

[47] M. Ghadhab, S. Junges, J.-P. Katoen, M. Kuntz, and M. Volk, "Safety analysis for vehicle guidance systems with dynamic fault trees," *Rel. Eng. Syst. Saf.*, vol. 186, pp. 37–50, Jun. 2019.

[48] S. Atsushi, "A framework for performing quantitative fault tree analyses for subsystems with periodic repairs," in *Proc. Annu. Rel. Maintainability Symp. (RAMS)*, Orlando, FL, USA, May 2021, pp. 1–6.

[49] J. Famfulik, M. Richtar, R. Rehak, J. Smiraus, P. Dresler, M. Fusek, and J. Mikova, "Application of hardware reliability calculation procedures according to ISO 26262 standard," *Qual. Rel. Eng. Int.*, vol. 36, no. 6, pp. 1822–1836, Oct. 2020.

[50] T. Wang, X. Chen, Z. Cai, J. Mi, and X. Lian, "A mixed model to evaluate random hardware failures of whole-redundancy system in ISO 26262 based on fault tree analysis and Markov chain," *Proc. Inst. Mech. Eng. D, J. Automobile Eng.*, vol. 233, no. 4, pp. 890–904, Mar. 2019.

[51] C.-S. Cho, W.-H. Chung, and S.-Y. Kuo, "Using tree-based approaches to analyze dependability and security on I&C systems in safety-critical systems," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1118–1128, Jun. 2018, doi: 10.1109/JSYST.2016.2635681.

[52] A. 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. 15241–15255, 2020, doi: 10.1109/ACCESS.2020.2967453.

[53] Y. Tian, J. Li, and X. Huang, "A cybersecurity risk assessment method and its application for instrumentation and control systems in nuclear power plants," *IFAC-PapersOnLine*, vol. 55, no. 9, pp. 238–243, 2022, doi: 10.1016/j.ifacol.2022.07.042.

[54] *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)*, Standard IEC 61508, 2010.

[55] *Risk-Based Inspection Methodology*, Standard API RP 581, 3rd ed., Oct. 2020.
[56] *Fault Tree Analysis (FTA)*, IEC 61025, 2006.
[57] C. E. Budde, C. Kolb, and M. Stoelinga, "Attack trees vs. fault trees: Two sides of the same coin from different currencies," in *Quantitative Evaluation of Systems* (Lecture Notes in Computer Science), vol. 12846. Cham, Switzerland: Springer, 2021, doi: 10.1007/978-3-030-85172-9_24.
[58] *Information Security Technology—Implementation Guide to Risk Assessment of Industrial Control Systems*, Standard GB/T 36466-2018, 2018.
[59] A. Carrera-Rivera, W. Ochoa, F. Larrinaga, and G. Lasa, "How-to conduct a systematic literature review: A quick guide for computer science research," *MethodsX*, vol. 9, Jan. 2022, Art. no. 101895, doi: 10.1016/j.mex.2022.101895.
[60] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Inf. Softw. Technol.*, vol. 64, pp. 1–18, Aug. 2015, doi: 10.1016/j.infsof.2015.03.007.

IEVGEN BABESHKO is currently a Graduate Fellow with the Software Engineering & Dependable Computing Laboratory, Institute of Information Science and Technologies "Alessandro Faedo," and an Associate Professor with the Computer Systems, Networks and Cybersecurity Department, National Aerospace University "Kharkiv Aviation Institute." He is also the Head of the Functional Safety Division, Ukrainian Technical Committee TC185 "Industrial Automation." He covered a contributor roles in several European projects, including TEMPUS/ERASMUS+ (MASTAC, SAFEGUARD, SEREIN, CABRIOLET, CERES, and ALIOT) and Horizon 2020 (ECHO). He is involved as a regular member of Program Committee of IEEE DESSERT Conference. He is the coauthor of more than 50 scientific papers and reports, including ten monographs. His professional and research interests include reliability, safety, cybersecurity assessment, assurance and certification of industrial control systems, the dependability and resilience of IIoT systems, and academia-industry cooperation.

FELICITA DI GIANDOMENICO is currently the Research Director of ISTI-CNR, Pisa, Italy, where she is also leading the Software Engineering and Dependable Computing Research Laboratory. Her research interests include the design of dependable computing systems, software implemented fault/intrusion tolerance, and the modeling and evaluation of dependability attributes, with a focus on critical infrastructures. She covered the role of a principal investigator of CNR and/or the Work-Package Leader in several European projects (including Caution++, CRUTIAL, SAFEDMI, CHESS, and SmartC2Net) and national projects (more recently, TENACE). She has been the Chair of the IEEE Technical Committee on Dependable Computing and Fault Tolerance, from January 2017 to December 2018, and the Chair of the IEEE/IFIP DSN Steering Committee, from January 2017 to December 2018. She is routinely involved in program committee of the most relevant conferences in the dependability area. She was the Program Co-Chair of SRDS 2008, DSN 2009, SAFECOMP 2014, and SERENE 2019. She is a member of the IFIP WG10.4 on Dependable Computing and Fault Tolerance and a member of the Steering Committee of the Conferences IEEE/IFIP DSN and EDCC.

Open Access funding provided by 'Consiglio Nazionale delle Ricerche-CARI-CARE-ITALY' within the CRUI CARE Agreement