future internet

MDPI

Article

Cybersecurity and Safety Co-Engineering of Cyberphysical Systems—A Comprehensive Survey

Georgios Kavallieratos [1,*], Sokratis Katsikas [1,2] and Vasileios Gkioulos [1]

[1] Deparetment of Information Security and Communication Technology, Norwegian University of Science and Technology, 2815 Gjøvik, Norway; georgios.kavallieratos@ntnu.no (G.K.); sokratis.katsikas@ntnu.no (S.K.); vasileios.gkioulos@ntnu.no (V.G.)

[2] Faculty of Pure and Applied Sciences, Open University of Cyprus, Latsia 2220, Cyprus; sokratis.katsikas@ouc.ac.cy

* Correspondence: georgios.kavallieratos@ntnu.no

Received: 28 March 2020; Accepted: 8 April 2020; Published: 11 April 2020

Abstract: Safeguarding both safety and cybersecurity is paramount to the smooth and trustworthy operation of contemporary cyber physical systems, many of which support critical functions and services. As safety and security have been known to be interdependent, they need to be jointly considered in such systems. As a result, various approaches have been proposed to address safety and cybersecurity co-engineering in cyber physical systems. This paper provides a comprehensive survey of safety and cybersecurity co-engineering methods, and discusses relevant open issues and research challenges. Despite the extent of the existing literature, several aspects of the subject still remain to be fully addressed.

Keywords: safety; cybersecurity; co-engineering; cyber physical systems

1. Introduction

The unification of embedded systems with communication technologies gave rise to "Cyber Physical Systems (CPS)". Such systems are deployed in several application domains, such as automotive, smart manufacturing, and healthcare. Due to the "double nature" of such systems—merging of the cyber and the physical worlds—ensuring both safety and cybersecurity are important prerequisites to their reliable operation.

Thus, the study of potential hazards and threats, and the assessment of safety and cybersecurity risks that potential accidents and cyberattacks pose, is important; it is also, usually, complicated. This is because there exist strong dependencies between the two domains, even though cases where they are independent do also exist. Three types of such dependencies have been identified and studied in Reference [1]:

1. **Conditional dependencies:** Safe operations may be conditioned by cybersecurity, for example, malicious modifications of sensor data or control programs may prevent safety systems from protecting an installation in accidental conditions. Conversely, safety may be a condition for cybersecurity, for example, when unmanaged catastrophic conditions weaken the security posture of a system or an organization, and lead to opportunistic malicious acts.
2. **Reinforcement:** Safety and cybersecurity measures can be complementary, for example, event and activity logging may be used both for attack detection and accident anticipation, as well as post-event analysis.
3. **Conflict:** If safety and cybersecurity are considered separately for the same system, it is possible that conflicting requirements or measures may be identified, for example, a safety requirement for an automatic door shutting system, would be to leave the door open, whereas a security requirement would be to leave the door locked in case of failure.

Therefore, there is a need to analyze both the safety and the cybersecurity of CPSs by employing a single approach. Such an approach can be employed to identify system faults/vulnerabilities, hazards/threats, safety/security requirements, and to assess safety/security risks.

Security engineering approaches aim to identify, assess, and manage risks related to the confidentiality, integrity, and availability of the targeted system/component. Various methods for security engineering have been proposed in the literature, that focus on different phases of the system lifecycle. General approaches assess and manage the overall security risk of a system, whilst methods also exist that facilitate the analysis in a particular phase of the lifecycle such as the requirements engineering, the threat analysis, the vulnerability analysis, or the risk analysis phases.

Safety engineering approaches aim to identify, assess, and manage risks related to the safety of the system, of humans, and of the environment. Various safety engineering methods exist, designed for different application domains and for different types of system safety (e.g., functional safety, operational safety etc.). Similarly with the security engineering methods case, different approaches exist for hazard analysis, fault analysis, cause analysis, and safety risk analysis and management.

Accordingly, security and safety co-engineering approaches aim to identify, assess, and manage risks related to both security and safety in systems which are influenced from both the cyber and the physical world/environment. Such approaches are classified according to their goal in three categories [2]:

- **Security-informed safety approaches:** Approaches that extend the scope of safety engineering by adapting cybersecurity-related techniques.
- **Safety-informed security approaches:** Approaches that extend the scope of security engineering by adapting safety-related techniques.
- **Combined safety and security approaches:** Combined approaches for safety and cybersecurity co-engineering.

In recent research, many proposals for security and safety co-engineering methods have appeared, and some survey articles have reviewed these proposed methods in varied degrees of depth and scopes. Piètre-Cambacédès et al. [3] surveyed the differences and similarities between safety and security aspects focusing on their dependencies per application domain. Kriaa et al. [4] conducted a survey of safety and security methods and analyzed methods for industrial control systems. Various safety and security risk assessment methods, categorized according to their application domain, were reviewed by Chockalingam et al. [5]. Abulamddi [6] surveyed existing methods for safety and security requirements engineering in CPSs. A systematic literature review was conducted by Lisova et al. [7] that focused on already developed and evaluated methods. Lyu et al. [8] provided a short survey, in which five integrated safety and security co-engineering methods were analyzed. Finally, Paul and Rioux [2] provided an extended bibliography of research papers on safety and cybersecurity co-engineering since the early 90s without, however, analyzing them.

In this paper we revisit previous surveys on cybersecurity and safety co-engineering approaches; we report on the results of a systematic literature survey of such approaches that have not been reviewed before; we define a multi-attribute taxonomy and we use it to analyze such approaches; and we discuss pertinent open issues and research challenges. The overall contribution of this paper is a comprehensive discussion on the recent advances in cybersecurity and safety co-engineering. A summary of the contributions of the paper follows:

- A comprehensive review of sixty eight methods for cybersecurity and safety co-engineering, of which nine have not been reviewed before.
- The development of a multi-attribute taxonomy of cybersecurity and safety co-engineering methods, encompassing inter alia all attributes used in previous surveys.
- A discussion on open issues, not fully addressed by existing approaches for cybersecurity and safety co-engineering, that give rise to research challenges.

The remainder of this work is structured as follows: Section 2 reviews related work; it is divided into two subsections, one on previous surveys and another on approaches not previously reviewed. In Section 3 we define a multi-attribute taxonomy of cybersecurity and safety co-engineering approaches and we employ it to analyze the reviewed approaches. In Section 4 we discuss the results of the analysis, and we identify issues not fully addressed by existing approaches that give rise to research challenges. Finally, in Section 5 we summarize our conclusions and we outline our future research plans.

2. Related Work

2.1. Previous Reviews

There are two types of reviews; *narrative* and *systematic* reviews [9]. *Narrative* reviews aim to identify studies in the literature that describe a specific problem of interest. In such reviews, systematic guidelines regarding the searching method, the identification of research questions, and the screening process are not considered. Thus, such reviews do not provide a comprehensive understanding of the stated problem.

Systematic reviews are methodical approaches to identify, analyze, and criticize the results concerning predefined research questions. Such reviews aim to provide inclusive results regarding a well predefined problem with specific research questions. Specific processes and guidelines exist for conducting a systematic literature review, including on how to formulate the research questions; research the literature; screen and select the results; and analyze and document the conclusions.

A total of six reviews of joint safety and security analysis methods have been identified in the recent literature. Of those five, References [3–6,8] are narrative and only one [7] is systematic. Even though the total number of methods reviewed therein is 60, surprisingly, the intersection of the set of methods reviewed in Reference [7] and of the set of methods reviewed in all other reviews counts only seven elements.

Piètre-Cambacédès et al. [3] conducted a survey of various safety and security approaches and studied the potential adoption of a safety approach for security analysis and vice versa. Although this work provides insight into safety and security concepts by analyzing the relevant terminology, the methods that are surveyed are not combined approaches but traditional safety and security methods. Specifically, safety standards along with hazard and risk analysis methods on one hand, and vulnerability and threat analysis methodologies on the other have been studied. The surveyed methods have been classified according to type (*safety to security* or *security to safety*); according to the approach taken (*Architectural concepts, Graphical modeling, structured risk assessment, and Testing*); and according to safety characteristics (*fault prevention, fault tolerance, fault removal, and fault forecasting*).

Kriaa et al. [4] provide a survey of approaches combining safety and security risk analysis for industrial infrastructures. Thirty nine methods were analyzed and grouped considering various criteria: the way each method treats safety and security (*unification/integration or harmonization*); the lifecycle phase (*operational/requirements or design*) in which the studied system is; and the type of the risk assessment approach (*quantitative/qualitative*). The methods are classified into *generic* and *model-based*. Methods in the former group describe the lifecycle stages and the sequence of activities in each stage, whereas the latter includes *graphical or non-graphical* methods, that may be supported by software tools. Furthermore, an overview of the safety and security standards for industrial infrastructures is presented. Finally, by analyzing the safety and security dependencies and interdependencies, the authors concluded that safety and security are complementary and should be treated jointly to improve the risk assessment process.

Chockalingam et al. [5] surveyed several integrated safety and security risk assessment methods and identified their key characteristics. The analysis was performed considering five criteria: First the identified approaches were classified according to the number of the *citations* that they had received in the scientific literature. The authors argue that the research community started to recognize the

importance of the combination of safety and security analyses in 2014 and 2015, with the most prominent methods being the Extended Fault Tree (EFT) and the Extended Component Fault Tree (E-CFT). Additionally, the approaches were grouped according to the steps involved in the risk assessment process. Specifically, the authors identified two types of integrated methods: the *sequential* integrated safety and security risk assessment method, and the *non-sequential* method. The third criterion is the stages of the risk management process (*risk identification, risk analysis, risk evaluation* that the method addresses. Further, the identified approaches are classified according to how the integration is achieved: *1) Combination of a conventional safety assessment method and of a variation of it to assess security; 2) Combination of a conventional security assessment method and of a variation of it to assess safety; 3) Combination of a conventional safety and a conventional security method;* and *4) Other - no conventional safety or security assessment method used*. Finally, the survey categorized the approaches considering the *application and the application domain*; four out of seven are methods targeting the transportation domain.

Abulamddi [6] surveyed integrated techniques for requirements engineering in CPSs; eight methods focusing on the requirements engineering phase of the lifecycle were identified and analyzed. The techniques were classified as *safety and security requirements* or *accident analysis*.

Lisova et al. [7] conducted a systematic literature review of joint safety and security analysis methods. The search was performed using the keywords ("safety" AND "security" AND "analysis") in four scientific databases (IEEE, ACM, Web of Science, and Springer link). Thirty three methods that analyze safety and security of CPSs early in the development phase have been identified. Five characteristics of these methods were considered: *application domain; stage in the system lifecycle; association with relevant standards; existence of validation step; and origin of contribution*. Additionally, the identified methods were classified according to the relationship between safety and security in the analysis process (*Unified, Parallel*), and the overall goal of the analysis (*combined safety and security; security informed safety, safety informed security*). Additionally, the yearly distribution of the reviewed papers, based on their security and safety focus was studied.

Finally, Lyu et al. [8] surveyed ten methods for safety and security analysis; these included five integrated approaches. The identified approaches were compared considering characteristics such as: *quantitative/qualitative, model-based/system-based, top-down/bottom-up analysis, and hierarchical/dynamic analysis*. The authors identified the pros and cons of each method and the technical gaps of the interplay of safety and security. Most of the integrated approaches analyzed in this work take a qualitative risk management approach.

2.2. Methods not Included in Previous Reviews

2.2.1. Search Method

Additional methods for safety and cybersecurity co-engineering have been identified in the following research databases: ACM Digital Library, Science Direct, Scopus, and IEEE Xplore. The search process was carried out by searching with the groups of keywords; (**Safety** AND **Security** AND **Cyber-physical systems**) and (**Safety** AND **Cybersecurity** AND **Cyber-physical systems**). The initial search returned 1313 results. The selection of the articles to be considered was performed according to the criteria listed below:

- The article must be explicitly related to a cybersecurity and safety **co-engineering** methodology.
- The article must not be included in previously published reviews.

This process resulted in the methods reviewed in the next section.

2.2.2. Methods

US^2 [10]: This is a unified approach that analyzes safety hazards and security threats for CPSs in automotive vehicles, by leveraging a simple quantitative scheme. It aims to analyze safety and

security concepts simultaneously, and to obtain consistent safety and security requirements and countermeasures. The elicitation of requirements is based on the ISO 26262 Automotive Safety Integrity Level (ASIL) metric and on the Security Level (SEL) metric, proposed in this work. The analysis is initiated by identifying security threats; in the sequel whether these threats may inflict safety hazards is examined. If so, the ASIL is utilized to identify the corresponding safety and security requirements and countermeasures, otherwise the SEL is used.

STPA and Six Step Model [11]: It is an integrated approach to analyze safety and security issues and artefacts for autonomous vehicles. It is based on the SAE J3016, SAE J3061, and ISO 26262 standards. By leveraging the Six Step Model (SSM) [12], the authors integrated the System Theoretic Process Analysis (STPA) [13] and the ISO 26262 standard to enrich the SSM hierarchies and, particularly, the lists of functions, failures, and safety countermeasures. The method comprises six steps, similarly to the SSM. In Steps 1 and 2 the functions, structure, and processes of the CPSs in an autonomous vehicle are identified. Steps 3 and 4 pertain to the safety and security analysis of the targeted system. Namely, the Hazard Analysis and Risk Assessment (HARA) as defined in ISO 26262 [14] and STPA methods are followed, to identify hazards, failures, and requirements. The security analysis is based on TARA as defined by the SAE J3061 standard [15]. Finally, in steps 5 and 6 the safety and security countermeasures are identified, by analyzing the functional safety and security requirements, and added to the model. A software too to support the proposed methodology is under development.

FACT [16,17]: Failure-Attack-CounTermeasure (FACT) is a unified graphical approach for safety and security analysis. This approach facilitates the analysis of CPSs and can be used for verification, validation, monitoring, and periodic safety and security assessment. The proposed approach is based on the ISA84 [18] and ISA99 [19] standards. The integration of the two standards is achieved by merging the corresponding lifecycle phases, resulting in a unified lifecycle of fourteen phases. The FACT graph model is developed in phases 1-9 of the unified lifecycle. The graph is constructed by following four distinct steps: 1) Import failure trees; 2) Include safety countermeasures in the graph; 3) Import attack trees; and 4) Include security countermeasures. Further, by leveraging the FACT graph, the security and safety countermeasures can be mapped to the corresponding attacks and faults. This enables the identification of interrelated countermeasures and the analysis of their interdependencies. The proposed approach has been applied to analyze industrial control systems.

CRAF [20]: The Cyber Risk Assessment Framework (CRAF) aims to facilitate the safety and security analysis of a CPS during the whole system lifecycle. The main focus of the framework is to study how a loss of data security could have safety implications. The framework comprises three steps: 1) Communicating a decision; 2) Raising a conflict; and 3) Conflict resolution. CRAF treats safety and security separately, and utilizes traditional security and safety techniques and concepts (e.g., Threat analysis, Hazard analysis). CRAF aims to bridge the gap between safety and security by comparing and consolidating the security and safety data properties.

UFoI-E [21]: The Uncontrolled Flows of information and Energy (UFoI-E) method enables the analysis and representation of the dependencies of CPSs and facilitates their diagrammatic representation for risk analysis. It provides a generic CPS master diagram to distinguish the cyber and physical environments of the system under study. The method integrates the security and safety concepts from physical, control, and computer systems. The dependencies between information and control flows are studied to examine the causes the could provoke harm to humans, assets, or the environment. The method considers these cyber threats in the information domain that could provoke safety hazards in the energy domain. Security aspects are related to deliberate sources of risk while safety aspects are related to unintentional sources of risk. According to the UFoI-E, both an uncontrolled flow of information (security) and an uncontrolled flow of energy (safety) may result in physical harm.

AVES [22]: The Automated Vehicles Safety and Security Analysis Framework (AVES) aims to facilitate the safety and security analysis of autonomous vehicles by leveraging four relationship matrices and a Safety and Cybersecurity Deployment (SCSD) model. The first matrix describes the

hazards and the threats of the targeted vehicle along with the associated risks and the pertinent safety and security requirements. The second matrix describes the safety and security countermeasures, and the third analyzes the relationships among the countermeasures. The fourth matrix records and tracks the implementation status of the previously identified countermeasures. Finally, the fifth matrix incorporates the other four matrices into a meta-model to better analyze the system by leveraging various data from different matrices. The method is consistent with relevant safety and security standards, covering the vehicle's development lifecycle. AVES is implemented in eleven stages, that cover the concept; product development; production; operations; and service and decommissioning phases of the vehicle lifecycle, and is able to capture various aspects of the vehicle at different automation levels.

CPS master diagram [23]: The CPS master diagram is a hierarchical three-layer representation of the studied system in different process types. The lower level represents the system's physical layer, that consists of the energy flows and the physical interactions that control the flows. The middle level describes the real time information flows to control, and the third (top) level is the cyber layer which consists of information flows for monitoring and supervision. By leveraging the master diagram, experts from the safety or the security field may apply existing or new assessment approaches to analyze different CPS applications. The framework has been used for preliminary safety and security assessments in the maritime [23] and in the Internet of Things (IoT) [24] domains.

IoT medical devices [25]: This work proposes a method to analyze safety and security issues in IoT medical devices. The method is based on the STPA and an analyst is able to identify and assess accidents due to security threats that violate the functional safety. By leveraging this approach the analyst is able to analyze complex systems and perform a quantitative threat analysis by combining the EFT and the Defense Tree (DT) methods. The approach comprises seven steps: In step 1 the accidents, hazards, and safety constraints are identified; in step 2 the control structure of the system is constructed according to the STPA. In steps 3 and 4 the unsafe control actions are identified, as well as the hazards' causal factors, by employing the EFT and DT methods. In step 5 the probability of occurrence of the fundamental events of the EFT that was developed in the previous step is calculated; the estimate is based on both statistical data and the stakeholders' judgement. Finally, in step 6 the selection of the appropriate countermeasures is performed, by considering the impact of the identified accidents and the probability estimates of step 5. The proposed method has been applied to the case of an insulin pump for diabetic patients.

SARA [26]: SARA (Security Automotive Risk Analysis) provides a framework for facilitating threat modeling and the risk assessment processes for driverless vehicles. Although it is a security risk assessment method, it enables the analysis of safety issues inflicted by security threats. This is achieved by examining the impact on safety of the attack goal, and by estimating the safety severity and controllability metrics. SARA consists of four blocks: 1) Feature definition; 2) Threat specification; 3) Risk assessment; 4) Countermeasures. In the third block (risk assessment) security and safety experts identify attacks and the necessary metrics for the risk estimation, such as severity, observation, controllability, and highest attack likelihood. The proposed method was applied to the case of an autonomous car to present the potential impact of a malicious observer and of damaged road infrastructure on the vehicle.

3. Analysis

In order to provide a comprehensive description of the current landscape of methods for the joint analysis of safety and security of CPSs, the following list of attributes is used. Several of these attributes have been used in previous reviews or elsewhere. Each attribute is followed by a short description and a reference to the source(s) where it was originally used.

1. **Type of joint analysis (Type):** This attribute may assume either the value "Integrated (I)" or the value "Unified (U)". In the former case the analysis is done in two separate, yet interrelated processes, whereas in the latter the analysis is performed following a single, unified process. The attribute was originally used in References [4,7].
2. **Model type (Model):** Describes the model that the analysis is based on. Possible values are "Graphical (G)", "Formal (F)" and "Both graphical and formal (Both)". In graphical methods the analysis is carried out by leveraging graphical models, whilst in formal methods the analysis is based on formulas, equations, and modelling languages. This attribute was originally used in References [4,8].
3. **Standards:** The method is informed by and leverages safety/security standards. Possible values are "Yes (Y)" and "No (N)". This attribute was originally used in Reference [7].
4. **Application domain (Domain):** The application domain(s) where the method is applicable or has been applied. Possible values are "CPS", "IoT", "Automotive (A)", "Control Systems (CS)" or combinations thereof. This attribute was originally used in References [5,7].
5. **Approach:** The type of approach followed. Possible values are "Quantitative (QNT)" and "Qualitative (QLT)". This attribute was originally used in References [4,8].
6. **Goal of the analysis (Goal):** Describes the overall goal of the analysis and whether the approach aims to ensure safety, security, or both. Possible values are "Security", "Safety" and "Both". This attribute was originally used in Reference [7].
7. **Lifecycle:** Describes in which phase of the system lifecycle the method is applied. Possible values are "Requirements (RE)", "Risk Analysis (RA)", "Any phase - Generic (GE)". This attribute was originally used in Reference [4].
8. **Stakeholders:** Describes which stakeholders are involved, either by applying it (users) or by giving input (participants); when applying the method. Possible values are "Safety experts (A)", Security experts (B)", "Developers (C)", "Designers (D)", and "Users or system experts (E)". This attribute was originally used in Reference [27].

The above attributes are depicted in Figure 1. Further, the following characteristics provide additional insight into understanding the operational capacity of each method; these have been inspired by the work in Reference [27]. Each of them, with the exception of *Process*, may assume the value "Yes (Y)", "No (N)", or "Partially (P)". *Process* may only assume the values "Yes (Y)" or "No (N)".

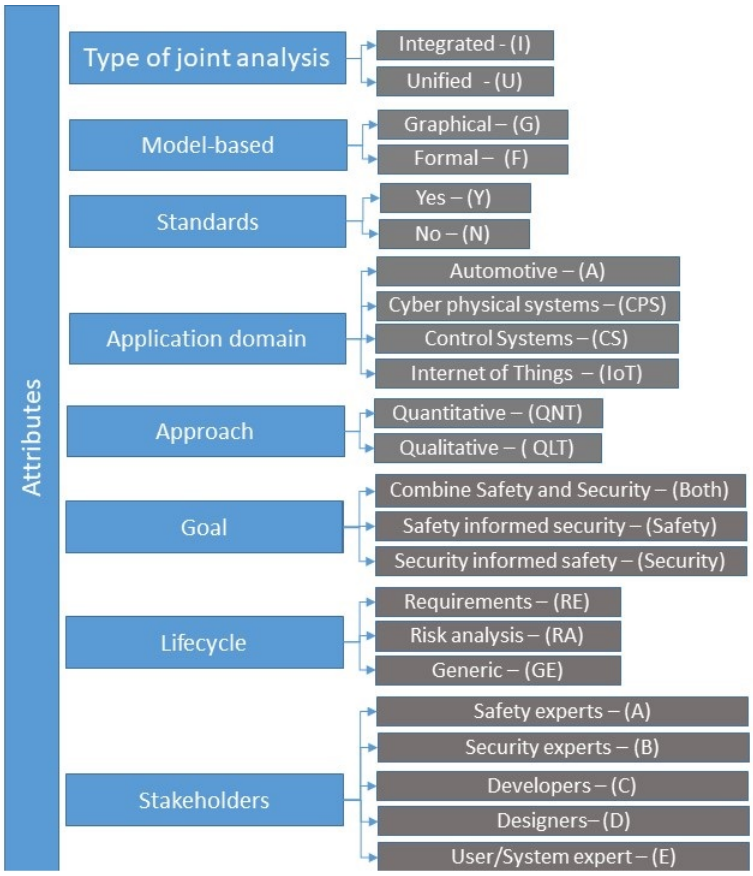

Figure 1. Attributes

1. **Process:** Is the method supported by a systematic and structured process?
2. **Scalability:** Does the method scale well with the size and complexity of the system under assessment?
3. **Creativity:** Does the method include mechanisms to stimulate creativity among the stakeholders? Examples of such mechanisms are guide-words, checklists and questionnaires.
4. **Communication:** Is the method offering features to facilitate communication between different stakeholders during its application? Examples of such features are guidelines, diagrams, schematics, and so forth.
5. **Conflict resolution (Conflict):** Does the method facilitate the identification and study of potential conflicts between safety and security aspects?
6. **Software tool (Tool):** Does a software tool or toolkit that supports the application of the method exist?

Method	Type	Model	Standards	Domain	Approach	Goal	Lifecycle	Stakeholders	Scalability	Creativity	Communication	Process	Conflict	Software
[10]	U	F	No	A	QLT	Both	RE	A/B	Y	Y	P	Y	N	N
[11]	I	G	Yes	A	QLT	Both	RA/RE	A/B/D	Y	Y	Y	Y	P	N
[16,17]	U	G	Yes	CS	QLT	Both	RA/RE	A/B/D	Y	Y	P	Y	Y	N
[20]	I	N/A	No	CPS	QLT	Security	RE/RA	A/C/E	P	P	Y	Y	Y	N
[21]	I	G	Yes	A	QLT	Safety	RA	A/B/C/E	Y	P	Y	Y	P	N
[22]	I	G	No	CPS	QLT	Both	RA/RE	A/B/C/D	P	Y	Y	Y	Y	N
[23]	I	G	No	CPS	QLT	Both	RA	A/B/D/E	Y	Y	Y	Y	N	N
[25]	I	G	No	CPS	QLT	Safety	RA/RE	A/B/D	Y	Y	Y	Y	N	Y
[26]	I	N/A	No	CPS/A	QLT	Both	RA	A/B	N	P	N	Y	N	N
[28]	U	G	No	CPS	QLT	Safety	RE	A/B/C	N	Y	Y	Y	Y	N
[29]	I	N/A	Yes	CS	QLT/QNT	Safety	RA	A/B	P	Y	P	Y	N	N
[30]	U	G	Yes	CPS	QLT	Safety	RA	A/B	P	Y	P	Y	N	N
[31]	U	G	No	CPS	QLT	Both	RA/RE	A/B/D/E	Y	N	Y	Y	P	P
[32]	U	F	Yes	CPS	QLT/QNT	Both	RA	A/B	P	Y	N	Y	N	N
[33]	U	G	Yes	A	QLT	Both	RA	A/B	N	Y	Y	Y	N	N
[34]	U	F	No	CS	QLT/QNT	Both	RA/RE	A/B	P	P	P	Y	Y	Y
[35]	U	Both	Yes	CS	QLT	Safety	GE/RA	A/B	Y	Y	Y	Y	N	N
[36]	U	Both	No	A	QLT/QNT	Safety	RE	A/B/C	P	Y	Y	Y	N	Y
[37]	I	F	No	CS	QLT/QNT	Both	RE	A/B/D	P	P	N	Y	Y	N
[38]	U	F	No	CS	QLT/QNT	Both	RA	A/B/E	Y	P	P	Y	N	Y
[39]	U	F	Yes	A	QNT	Safety	RE	A/B	P	P	Y	Y	N	N
[40]	U	F	Yes	A	QNT	Safety	RA	A/B/D/E	Y	Y	Y	Y	N	N
[41]	U	F	Yes	CPS	QLT/QNT	Safety	RA	A/B	N	Y	N	Y	N	N
[42]	U	G	No	A	QLT	Safety	RA	A/B/D	N	Y	Y	Y	N	N
[43]	I	Both	Yes	A	QLT	Both	GE/RE/RA	A/B/C/D/E	P	Y	Y	Y	N	Y
[44]	I	G	No	IoT	QLT/QNT	Safety	RA	A/B/C/D	Y	Y	Y	Y	Y	N
[45]	U	G	Yes	A	QLT	Both	RE	A/B	N	Y	P	Y	Y	X
[46]	U	G	Yes	A	QLT	Safety	RA/RE	A/B/C/D	Y	Y	P	Y	N	P
[47]	I	G	No	CPS	QLT	Safety	RE	A/B/D	P	Y	N	Y	N	N
[48]	U	N/A	Yes	A	QLT	Safety	GE/RA/RE	A/B/E	Y	Y	N	Y	N	N
[49]	U	G	No	CPS	QLT	Both	RA	A/B/C/D	Y	Y	Y	Y	N	P
[50]	U	F	No	CPS	QLT/QNT	Both	RA/RE	A/B/C	Y	Y	Y	Y	N	Y
[51]	U	Both	No	CPS	QLT/QNT	Both	RA	A/B	Y	N	P	Y	N	Y
[52]	I	N/A	Yes	CPS	QLT	Both	GE/RA/RE	A/B/D	Y	Y	Y	Y	Y	P
[53]	U	N/A	No	CPS	QLT	Both	GE/RA	A/B/D	Y	Y	Y	Y	N	P
[54]	U	N/A	No	IoT	QLT	Safety	GE/RA	A/B	Y	Y	Y	Y	N	P
[55]	I	G	Yes	CPS	QLT	Both	RA	A/B	Y	Y	Y	Y	Y	N
[56]	U	G	Yes	CPS	QLT/QNT	Safety	RA	A/B	Y	Y	Y	Y	N	N
[57]	U	F	No	CS	QLT	Both	RE	A/B	Y	Y	Y	Y	N	P
[58]	U	N/A	No	N/A	QLT/QNT	Both	GE/RA	A/B	Y	N	N	Y	N	N
[59]	U	F	No	N/A	QLT/QNT	Both	GE/RE/RA	A/B	Y	Y	N	Y	N	N
[60]	U	N/A	Yes	CPS	QLT	Both	GE/RE/RA	A/B	Y	Y	P	Y	N	N
[61]	U	N/A	Yes	IoT	QLT	Safety	GE/RA/RE	A/B/C/D	Y	N	N	Y	N	N
[62]	I	N/A	No	CS	QLT	Both	GE/RA	A/B/C	N	P	P	Y	Y	N
[63]	I	N/A	No	CS	QLT	Safety	GE/RE	A/B/C/D	Y	Y	Y	Y	N	N
[64]	I	N/A	No	CS	QLT	Both	GE/RE	A/B	Y	Y	P	Y	Y	N
[65]	I	G	No	CS	QLT	Safety	RE/RA	A/B	Y	Y	N	Y	Y	N
[66]	I	Both	No	CS	QLT/QNT	Safety	RA	A/B	P	Y	N	Y	N	N
[67]	I	Both	No	CPS	QLT/QNT	Safety	RE	A/B	Y	Y	P	Y	N	N
[68]	I	Both	No	CPS	QLT/QNT	Safety	RE/RA	A/B	P	Y	Y	Y	N	Y
[69]	I	Both	No	CS	QLT/QNT	Safety	RA	A/B	P	Y	P	Y	N	N
[70]	U	F	No	N/A	QLT/QNT	Security	RA/RE	A/B/E	P	Y	P	Y	N	Y
[71]	I	Both	No	CS	QLT/QNT	Both	RA	A/B	P	Y	P	Y	N	Y
[72]	I	G	No	CPS	QLT	Security	RE/RA	A/C/D	Y	Y	P	Y	N	N
[73]	I	Both	No	CS	QLT/QNT	Safety	RE	A/B	P	Y	Y	Y	N	Y
[74]	I	F	No	A	QLT/QNT	Security	RE/RA	B/D	Y	Y	N	Y	N	Y
[75]	U	Both	No	CS	QLT/QNT	Safety	RE/RA	B	P	Y	P	Y	N	Y
[76]	I	F	No	CPS	QLT/QNT	Both	RE/RA	A/B/D	Y	P	P	Y	N	Y
[77]	I	Both	No	IoT	QLT	Both	RE	A/B	P	Y	P	Y	Y	Y
[78]	I	F	No	CPS	QLT/QNT	Security	GE/RE/RA	A/B	Y	Y	P	Y	N	N
[79]	I	F	No	CPS	QLT/QNT	Both	GE/RE	A/B	P	Y	P	Y	Y	N
[80]	I	F	No	A	QLT	Security	RE	B	P	Y	P	Y	N	Y
[81]	I	F	No	CPS	QLT	Both	RE	A/B/D	Y	Y	P	Y	N	Y
[82]	I	G	No	CPS	QLT	Safety	RE/RA	A/B/C/D	Y	Y	Y	Y	N	Y
[83]	I	G	No	A	QLT	Safety	RA/RE	A/B	Y	Y	P	Y	N	N
[84]	I	N/A	No	A	QLT	Safety	RA	A/B	P	Y	P	Y	N	N
[85,86]	I	G	No	CS	QLT	Both	RE	A/B/C/D	P	Y	P	Y	Y	Y
[87]	I	N/A	No	CS	QLT	Safety	RA/RE	A	P	Y	P	Y	N	N

Table 1. Attributes and Characteristics

Table 1 depicts both the attributes and the characteristics of all methods reviewed in the surveys of Section 2.1 and of those reviewed in Section 2.2.2.

4. Discussion

The main findings from the analysis of the literature reviewed in the previous section are the following:

- A total of sixty eight methods have been reviewed. These span a time period of approximately 20 years, with most having been proposed after 2013, and with a steady increase in the past 5 years. This is an indication of the timeliness of the subject, which can be attributed to the increased proliferation of cyber physical systems and the integration of Information Technology with Operational Technology.
- The number of integrated methods (37) is slightly larger than that of unified ones (31). According to Reference [62], approaches that attempt to unify safety and security analysis techniques reduce

the developer's understanding of the system being analyzed and prevent a thorough analysis of either property; this leads to an incomplete analysis with subsequent safety and security risks going unobserved. On the other hand, integrated methods extract more rigorous results and facilitate the identification of potential conflicts.

- Model-based methods prevail (52 out of 68). Of these, 18 methods employ formal models, 23 methods employ graphical models, and 11 methods employ both formal and graphical models. Model-based approaches are more practical for modeling a system's components and functionalities for existing and operational systems, by virtue of their qualitative and quantitative capabilities [4]. They are generally able to scale up to complex systems and represent different aspects related to safety and security with different viewpoints and levels of detail. On the other hand, such approaches require the analyst to have a thorough knowledge of the system; engaging all stakeholders in the process my facilitate the fulfillment of this requirement.
- Less than half of the reviewed methods (20) are informed by safety and security standards. Cyberphysical systems often operate in domains and environments highly regulated by safety and security standards. Therefore, they must be engineered to conform to these standards. It follows that safety-security co-engineering methods needs to be informed by standards. This need is more often than not satisfied if the method has been designed for use in a specific application domain. Including a validation phase in the workflow of the method, in which conformance to relevant standards is performed, is a viable alternative that may lead to the development of generic methods informed by standards. A related issue, discussed in the next section, is the need for integrated safety-security standards in several application domains.
- Most (45) of the reviewed methods have been used to analyze general CPS architectures and industrial control systems in various application domains, with the transportation domain prevailing. However, the applicability of the generic methods to different application domains is usually not demonstrated. Developing a method applicable to a broad spectrum of domains and at the same time ensuring compliance with relevant standards appears as a very challenging task.
- The vast majority of the reviewed methods (66) follow -at least partially- a qualitative approach; only two methods are fully quantitative. This is not surprising, because even though quantitative approaches prevail for safety engineering, the opposite is true for security engineering, where quantitative approaches are very rarely used, as they require the existence of a formal model describing the system under study. Attempting to analyze security, particularly security risk, has been shown quantitatively to be either infeasible or inadvisable in most real-world situations. Hence, a reasonable compromise is to opt for a combination of quantitative and qualitative approaches for safety-security co-engineering.
- The number of methods whose goal is to ensure both safety and security (32) is slightly larger than the number of those aiming to ensure safety (30), whilst only six methods have as their primary goal to ensure security. The appropriateness of each of these approaches depends largely on the system's safety/security criticality. When the system under study is safety critical, a method whose goal is to ensure that security will not adversely influence safety is appropriate; the opposite is true when the system is security critical. But if the intention is to also have a secure system beyond the safety relevant security issues, and a safe system beyond the security relevant issues, then neither of these approaches is appropriate. In systems where both safety and security are equally important, an approach aiming to ensure both safety and security would be more appropriate.
- The number of reviewed methods that are applied to both the requirements elicitation and risk analysis phases of the system lifecycle (26) is almost equal to that of methods applied to the risk analysis phase (25), and only slightly exceeds that of methods applied to the requirements elicitation phase (17); only fifteen methods are frameworks, hence applicable to any phase of the lifecycle. This nearly uniform distribution reflects the emphasis given into co-engineering safety

and security as early as possible in the development lifecycle, while allowing for revisiting the results of the analysis when the system under study has been developed or is even operational.

- The application of most of the reviewed methods involves safety and security experts; only few methods require the engagement of developers, designers and systems users. It is important to note that stakeholders, particularly designers and users, may engage with the analysis in two distinct but complementary ways: they provide input to the analysis in the form of domain expert knowledge, and they are the targets of the process of communicating the results; both are equally important. Acknowledging the fact that complex issues such as those of safety and security cannot be effectively analysed by the corresponding experts, it follows that successful methods will seek to involve engaged stakeholders.
- Scalability issues have been discussed in the vast majority (61) of the papers proposing methods, in 24 of which these issues have only briefly been considered. Thirty seven methods are scalable, whereas 7 do not scale well. It should be noted that scalability refers to both the ability of the method to handle complex systems and to the level of abstraction at which the system under study is represented. The two are correlated, as high level abstraction allows for more complex systems to be analyzed. The challenge, therefore, is to develop methods that can strike an appropriate balance between those two aspects of scalability, so that the analysis results in an appropriate and practically useful level of detail.
- The majority (55) of the reviewed methods provide mechanisms to stimulate creativity among the analysts and other relevant stakeholders. As many methods rely, at least to some extent, on scenario development, creativity is an important characteristic. This is even more so when the application of the method calls for a multi-disciplinary, multi-stakeholder team.
- Less than half (28) of the reviewed methods include techniques to communicate their results to the relevant stakeholders. Another 28 methods only briefly address the issue, whilst 10 methods do not address it at all. As already implied above, this characteristic is intertwined with the involvement of stakeholders attribute.
- All methods are process-based; the structure and the steps of the process do vary, however. As pointed out in the sequel, developing a methodology to encompass different process structures is still a challenge.
- The majority (49) of the reviewed methods do not address the conflict resolution issue. Sixteen methods do address it, and a further 3 address it only partially. The implications of this central issue is elaborated upon in the sequel.
- The majority (41) of the reviewed methods are not supported by any software tool or toolkit. Only 20 methods are fully supported, and another 7 are partially supported by such tools. This has been a rather surprising finding, as the purpose of a safety-security co-engineering method is to be applied in real-world application scenarios. The complexity of such methods requires software support for their usage.

To give a bird's eye view of these findings, and also to facilitate cross-referencing, the above are summarized in Figures 2 and 3. Figure 2 depicts the taxonomy of Figure 1, with the number following each attribute indicates the number of methods having the corresponding attribute. Figure 3 provides the same information on characteristics.

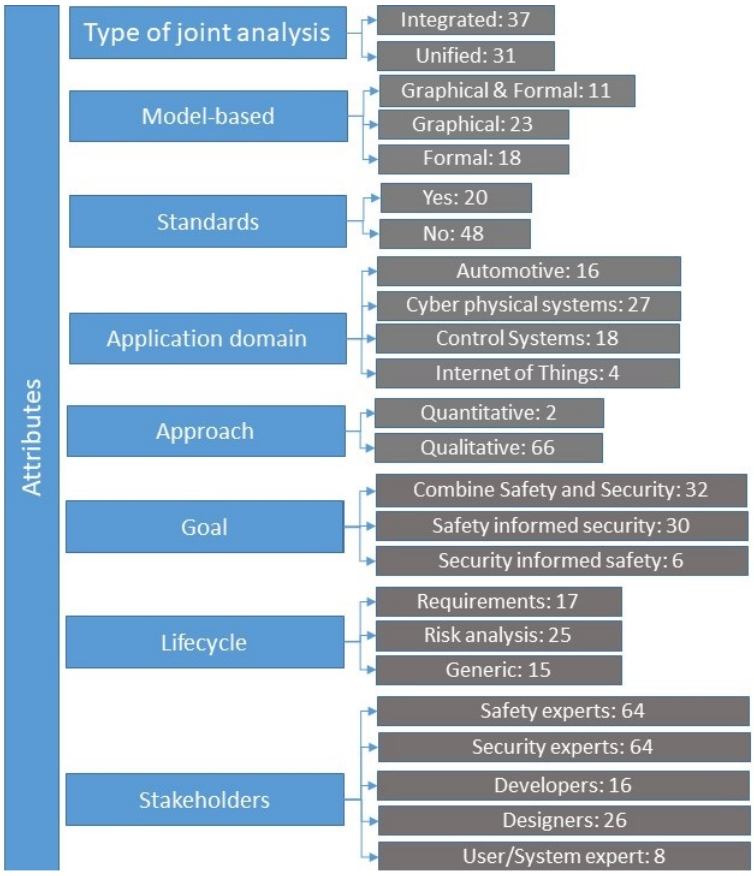

Figure 2. Attributes: Results

Figure 3. Characteristics: Results

Additionally, a number of issues that have been under-researched have been identified. These are as follows:

- *Resolving conflicting safety/security results:* The problem of conflicting results when studying safety and security jointly has been known for some time. There are two approaches to address this problem: either allow conflicting results to be derived and then resolve these conflicts, or avoid the occurrence of such conflicts by design. Unified safety and security co-engineering methods tend to generate less conflicts than integrated methods do. However, integrated methods tend to allow more comprehensive analyses of both domains. Therefore, integrated methods that would by design prevent the occurrence of conflicting results would address this issue effectively. This could perhaps be achieved if goal oriented integrated methods were developed. Further, the analysis is best performed in the early stages (requirements elicitation phase), as this makes the problem of conflict resolution much easier to solve, and leads to the development of safe-and-secure CPSs by design.
- *Standard methodology:* Despite the sizable extent of the literature on safety and security co-engineering methods, a generic, application-domain-independent *methodology*, instances of which would be existing methods and those to be developed in the future, is yet to be developed. An example of such a methodology in the security domain is the risk analysis methodology defined in the ISO 27005 standard.

- *Validation:* Not many of the reviewed papers include information on the validation/evaluation of the method they propose. More research is needed to evaluate the correctness, completeness, effectiveness, efficiency, scalability and so forth, of proposed methods, in a manner that will facilitate comparative assessments.
- *Safety and security standards:* Some standards addressing safety and security for industrial control systems exist. Examples of such standards are ISA99/IEC 6443, IEC 62645, IEC TR63609, ISO 26262 to name a few; cross-references with other standards (e.g., IEC 61508) also exist. However, the applicability of such standards to effectively address both safety and security, particularly in an industry 4.0 context, is still to be firmly established. Hence, a need for revisiting existing standards with an eye towards facilitating their use in industry, by means of reducing ambiguity, arises. Additionally, the adoption of standards specific for industry sectors, along the lines of the practice followed in the nuclear plant domain will guide the development of safe-and-secure by design industrial control systems.
- *Application domains:* As noted before, the transportation domain prevails among application domains addressed by the reviewed methods. Notwithstanding the fact that several methods have been claimed to have been designed to be applicable to any domain, their applicability has not been demonstrated. As several emerging application domains are both safety and security critical (e.g., autonomous vessels, drones), the development of methods addressing specifically systems in such domains remains an issue.
- *Dynamic character of CPS:* CPSs are dynamic by nature. Methods able to model and cope with this characteristic of CPSs are yet to be developed. Existing work on dynamic security and dynamic safety risk assessment can be leveraged to this end.
- *Model type:* Most of the safety analysis approaches are based on formal models. Security techniques on the other hand tend to focus on qualitative analysis. Therefore, an approach able to handle the complexity of CPS by leveraging both graphical models and systematic perspectives would allow the consolidation of advantages of both worlds.
- *Holistic approach:* The human factor in relation with CPSs is often overlooked. In fact, CPSs, particularly safety/security critical ones need to be considered and studied as socio-technical systems. This calls for a holistic approach towards safety and security co-engineering, that would encompass the whole ecosystem into which the CPS under study is expected to operate, and would involve all the relevant stakeholders in the process. To this end, future methods should enjoy previously mentioned attributes such as *scalability*, *communication*, and *model type*, in order to facilitate the analysis of CPSs when both technical and human aspects are considered. Particularly, such methods should be able to handle the complexity (*scalability*) derived from the human-machine interaction; communicate the results by providing reports and leveraging software tools (*communication*); and provide graphical models of the system under study (*model type*) to facilitate the analysis and the validation of the results.

5. Conclusions

We have revisited previous surveys on cybersecurity and safety co-engineering approaches and performed a systematic literature survey of such approaches. We defined a multi-attribute taxonomy for such approaches and we used this to analyze them. We thus provided a comprehensive discussion on the recent advances in cybersecurity and safety co-engineering. The joint study of safety and security has been a goal of researchers in both fields for more than thirty years. Despite the longevity of the problem and the substantial volume of research results on safety and security co-engineering that has been generated in the past few years, several important issues remain open. Through our review, we identified and discussed such issues and the research challenges that they imply. In the future, among the many possible research challenges in the field, we plan to focus on developing a holistic, integrated, graphical model based, safety and security requirements elicitation co-engineering approach, applicable to the autonomous vessel domain.

Author Contributions: Conceptualization, G.K. and S.K.; methodology, G.K.; investigation, G.K.; writing–original draft preparation, G.K.; writing–review and editing, S.K. and G.K.; supervision, S.K. and V.G.; project administration, S.K. and V.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Piètre-Cambacédès, L.; Bouissou, M. Modeling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes). In Proceedings of the 2010 IEEE International Conference on Systems, Man and Cybernetics, Istanbul, Turkey, 10–13 October 2010; pp. 2852–2861.
2. Paul, S.; Rioux, L. *Over 20 Years of Research into Cybersecurity and Safety Engineering: a Short Bibliography*; WIT Press: Ashurst Lodge, UK, 2015, pp. 335–349. doi: 10.2495/SAFE150291.
3. Piètre-Cambacédès, L.; Bouissou, M. Cross-fertilization between safety and security engineering. *Reliab. Eng. Syst. Safe.* **2013**, *110*, 110–126.
4. Kriaa, S.; Pietre-Cambacedes, L.; Bouissou, M.; Halgand, Y. A survey of approaches combining safety and security for industrial control systems. *Reliab. Eng. Syst. Safe.* **2015**, *139*, 156–178.
5. Chockalingam, S.; Hadžiosmanović, D.; Pieters, W.; Teixeira, A.; van Gelder, P. Integrated safety and security risk assessment methods: a survey of key characteristics and applications. In Proceedings of the International Conference on Critical Information Infrastructures Security, Paris, France, 10–12 October 2016, pp. 50–62.
6. Abulamddi, M.F. A Survey on techniques requirements for integrating safety and security engineering for cyber-physical systems. *J. Comput. Commun.* **2017**, *5*, 94–100.
7. Lisova, E.; Sljivo, I.; Causevic, A. Safety and Security Co-Analyses: A Systematic Literature Review. *IEEE Syst. J.* **2018**, *13*, 2189–2200. doi: 10.1109/JSYST.2018.2881017.
8. Lyu, X.; Ding, Y.; Yang, S.H. Safety and security risk assessment in cyber-physical systems. *IET Cyber-Physical Syst. Theory Appl.* **2019**, *4*, 221–232. doi: 10.1049/iet-cps.2018.5068.
9. Hart, C. *Doing a literature review: Releasing the research imagination*; SAGE Publications Ltd: Southend Oaks, CA, USA, 2018.
10. Cui, J.; Sabaliauskaite, G. US 2 : An Unified Safety and Security Analysis Method for Autonomous Vehicles. In Proceedings of the Future of Information and Communication Conference, Singapore, Singapore, 5–6 April 2018, pp. 600–611.
11. 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. Secur.* **2018**, *11*, 160–169.
12. Sabaliauskaite, G.; Adepu, S.; Mathur, A. A six-step model for safety and security analysis of cyber-physical systems. International Conference on Critical Information Infrastructures Security, Paris, France, 10–12 October 2016, pp. 189–200.
13. Leveson, N.G.; Thomas, J.P. *STPA handbook*; **2018**, Available online:https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf.
14. International Organization for Standardization (ISO). *Road vehicles — Functional safety*; Technical report ISO 26262-1:2018. ISO: Geneva, Switzerland, 2018.
15. SAE, J. 3061: Cybersecurity guidebook for cyber-physical vehicle systems, 2016. Available online: https://www.sae.org/standards/content/j3061/ (accessed on 18 October 2019)
16. Sabaliauskaite, G.; Mathur, A.P. Aligning cyber-physical system safety and security, 2015, Available online:http://www.2014.csdm-asia.net/IMG/pdf/Aligning_Cyber-Physical_System_Safety_and_Security-2.pdf (accessed on 20 November 2019)
17. Cui, J.; Sabaliauskaite, G. On the alignment of safety and security for autonomous vehicles. In Proceedings of the CYBER 2017 : The Second International Conference on Cyber-Technologies and Cyber-Systems, IARIA CYBER, Barcelona, Spain, 12–16 November 2017.
18. International Society of Automation - ISA. Technical report, ANSI/ISA 84.00.01-2004, Application of Safety Instrumented Systems for the Process Industries. ISA: Isa, Japan, 2004.
19. International Society of Automation - ISA. Technical report, ANSI/ISA-99-00-01-2007. Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models. ISA: Isa, Japan, 2007.

20. Asplund, F.; McDermid, J.; Oates, R.; Roberts, J. Rapid Integration of CPS Security and Safety. *IEEE Embed. Syst. Lett.* **2018**, *11*, 111–114. doi:10.1109/LES.2018.2879631.
21. Guzman, N.H.C.; Kufoalor, D.K.M.; Kozin, I.; Lundteigen, M.A. 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, Hannover, Germany, 22–26 September 2019, pp. 4099–4106.
22. Sabaliauskaite, G.; Liew, L.S.; Zhou, F. AVES–Automated Vehicle Safety and Security Analysis Framework. In Proceedings of the CSCS '19: ACM Computer Science in Cars Symposium ,Kaiserslautern, Germany, 8 October 2019, pp. 1–8. doi: 10.1145/3359999.3360494.
23. Guzman, N.H.C.; Wied, M.; Kozine, I.; Lundteigen, M.A. Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis. *Syst. Eng.* **2019**, *23*, 189–210.
24. Carreras Guzman, N.H.; Mezovari, A.G. Design of IoT-based Cyber–Physical Systems: A Driverless Bulldozer Prototype. *Information* **2019**, *10*, 343.
25. Hayakawa, T.; Sasaki, R.; Hayashi, H.; Takahashi, Y.; Kaneko, T.; Okubo, T. Proposal and Application of Security/Safety Evaluation Method for Medical Device System that Includes IoT. In Proceedings of the 2018 VII International Conference on Network, Communication and Computing, Taipei, Taiwan, 14–16 December 2018, pp. 157–164.
26. Monteuuis, J.P.; Boudguiga, A.; Zhang, J.; Labiod, H.; Servel, A.; Urien, P. Sara: Security automotive risk analysis method. In Proceedings of the 4th ACM Workshop on Cyber-Physical System Incheon Republic of Korea 2018, pp. 3–14.
27. Raspotnig, C.; Opdahl, A. Comparing risk identification techniques for safety and security requirements. *J. Syst. Softw.* **2013**, *86*, 1124–1151.
28. Raspotnig, C.; Karpati, P.; Katta, V. A combined process for elicitation and analysis of safety and security requirements. *Enterprise, Business-process and Information Systems Modeling*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 347–361.
29. Reichenbach, F.; Endresen, J.; Chowdhury, M.M.; Rossebø, J. A pragmatic approach on combined safety and security risk analysis. In Proceedings the 2012 IEEE 23rd International Symposium on Software Reliability Engineering Workshops, Dallas, TX, USA, 27–30 November 2012; pp. 239–244. doi: 10.1109/ISSREW.2012.98.
30. Silva, N.; Lopes, R. Practical Experiences with real-world systems: Security in the World of Reliable and Safe Systems. 2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W), Budapest, Hungary, 24–27 June 2013, pp. 1–5.
31. Young, W.; Leveson, N. Systems thinking for safety and security. Proceedings of the 29th Annual Computer Security Applications Conference, New Orleans Louisiana USA, December 2013, pp. 1–8.
32. Chen, Y.R.; Chen, S.J.; Hsiung, P.A.; Chou, I.H. Unified security and safety risk assessment-a case study on nuclear power plant. In Proceedings of the 2014 International Conference on Trustworthy Systems and Their Applications, Taichung, Taiwan, 9–10 June 2014, pp. 22–28.
33. Ito, M. Finding threats with hazards in the concept phase of product development. European Conference on Software Process Improvement, Luxembourg, Luxembourg, 25–27 June 2014, pp. 277–284.
34. Kriaa, S.; Bouissou, M.; Colin, F.; Halgand, Y.; Pietre-Cambacedes, L. Safety and security interactions modeling using the BDMP formalism: case study of a pipeline. In Proceedings of the International Conference on Computer Safety, Reliability, and Security, SAFECOMP 2014, Florence, Italy, September 2014, pp. 326–341.
35. Schmittner, C.; Gruber, T.; Puschner, P.; Schoitsch, E. Security application of failure mode and effect analysis (FMEA). In Proceedings of the International Conference on Computer Safety, Reliability, and Security, Florence, Italy, September 2014, pp. 310–325.
36. Apvrille, L.; Roudier, Y. Designing safe and secure embedded and cyber-physical systems with SysML-Sec. In Proceedings of the International Conference on Model-Driven Engineering and Software Development, Angers, France, 9–11 February 2015, pp. 293–308.
37. Gu, T.; Lu, M.; Li, L. Extracting interdependent requirements and resolving conflicted requirements of safety and security for industrial control systems. 2015 First International Conference on Reliability Systems Engineering (ICRSE), Beijing China, October 2015, pp. 1–8.
38. Kriaa, S.; Bouissou, M.; Laarouchi, Y. A model based approach for SCADA safety and security joint modelling: S-Cube. In Proceedings of the 10th IET System Safety and Cyber-Security Conference 2015, Bristol, UK, 21–22 October 2015.

39. Macher, G.; Höller, A.; Sporer, H.; Armengaud, E.; Kreiner, C. A combined safety-hazards and security-threat analysis method for automotive systems. In Proceedings of the International Conference on Computer Safety, Reliability, and Security, Delft, The Netherlands, 22–25 September 2014, pp. 237–250.
40. Popov, P.T. Stochastic Modeling of Safety and Security of the e-Motor, an ASIL-D Device. In *Computer Safety, Reliability, and Security*; Koornneef, F.; van Gulijk, C., Eds.; Springer International Publishing: Cham, Switzerland, 2015; pp. 385–399.
41. Steiner, M.; Liggesmeyer, P. Qualitative and quantitative analysis of CFTs taking security causes into account. In Proceedings of the International Conference on Computer Safety, Reliability, and Security, Delft, The Netherlands, 22–25 September 2014, pp. 109–120.
42. Wei, J.; Matsubara, Y.; Takada, H. HAZOP-Based Security Analysis for Embedded Systems: Case Study of Open Source Immobilizer Protocol Stack. In *Recent Advances in Systems Safety and Security*; Springer International Publishing: Cham, Switzerland, 2016; pp. 79–96.
43. Islam, M.M.; Lautenbach, A.; Sandberg, C.; Olovsson, T. A risk assessment framework for automotive embedded systems. In Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security, Xi'an China, 30 May 2016, pp. 3–14.
44. Nicklas, J.P.; Mamrot, M.; Winzer, P.; Lichte, D.; Marchlewitz, S.; Wolf, K.D. Use case based approach for an integrated consideration of safety and security aspects for smart home applications. In Proceedings of the 2016 11th System of Systems Engineering Conference (SoSE). Kongsberg, Norway, 12–16 June 2016.
45. Ponsard, C.; Dallons, G.; Massonet, P. Goal-oriented co-engineering of security and safety requirements in cyber-physical systems. In Proceedings of the International Conference on Computer Safety, Reliability, and Security, Trondheim, Norway, 20–23 Septembe 2016, pp. 334–345.
46. Schmittner, C.; Ma, Z.; Puschner, P. Limitation and improvement of STPA-Sec for safety and security co-analysis. In Proceedings of the International Conference on Computer Safety, Reliability, and Security, Trondheim, Norway, 20–23 Septembe 2016, pp. 195–209.
47. Troubitsyna, E. An integrated approach to deriving safety and security requirements from safety cases. In Proceedings of the 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, GA, USA, 10–14 June 2016; pp. 614–615.
48. Dürrwang, J.; Beckers, K.; Kriesten, R. A lightweight threat analysis approach intertwining safety and security for the automotive domain. In Proceedings of the International Conference on Computer Safety, Reliability, and Security, Trento, Italy, 12–15 September 2017; pp. 305–319.
49. Friedberg, I.; McLaughlin, K.; Smith, P.; Laverty, D.; Sezer, S. STPA-SafeSec: Safety and security analysis for cyber-physical systems. *J. Inf. Secur. Appl.* **2017**, *34*, 183–196.
50. Howard, G.; Butler, M.; Colley, J.; Sassone, V. Formal analysis of safety and security requirements of critical systems supported by an extended STPA methodology. 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris, France, 26–28 April 2017, pp. 174–180.
51. Kumar, R.; Stoelinga, M. Quantitative security and safety analysis with attack-fault trees. 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), Singapore, Singapore, 12–14 January 2017; pp. 25–32.
52. Pereira, D.; Hirata, C.; Pagliares, R.; Nadjm-Tehrani, S. Towards combined safety and security constraints analysis. In Proceedings of the International Conference on Computer Safety, Reliability, and Security, Trento, Italy, 12–15 September 2017, pp. 70–80.
53. Plósz, S.; Schmittner, C.; Varga, P. Combining safety and security analysis for industrial collaborative automation systems. In Proceedings of the International Conference on Computer Safety, Reliability, and Security, Trento, Italy, 12–15 September 2017; pp. 187–198.
54. Procter, S.; Vasserman, E.Y.; Hatcliff, J. SAFE and secure: Deeply integrating security in a new hazard analysis. In Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, 29 August –1 September 2017, p. 66. doi: 10.1145/3098954.3105823.
55. Sabaliauskaite, G.; Adepu, S. Integrating six-step model with information flow diagrams for comprehensive analysis of cyber-physical system safety and security. 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), Singapore, Singapore, 12–14 January 2017, pp. 41–48.
56. Temple, W.G.; Wu, Y.; Chen, B.; Kalbarczyk, Z. Systems-theoretic likelihood and severity analysis for safety and security co-engineering. In Proceedings of the International Conference on Reliability, Safety and Security of Railway Systems, Italy, 12–15 September 2017; pp. 51–67.

57. Vistbakka, I.; Troubitsyna, E.; Kuismin, T.; Latvala, T. Co-engineering safety and security in industrial control systems: a formal outlook. In Proceedings of the International Workshop on Software Engineering for Resilient Systems, Geneva, Switzerland, 4–5 September 2017, pp. 96–114.
58. Stoneburner, G. Toward a unified security-safety model. *Computer* **2006**, *39*, 96–97.
59. Aven, T. A unified framework for risk and vulnerability analysis covering both safety and security. *Reliab. Eng. Syst. Safe.* **2007**, *92*, 745–754.
60. Derock, A.; Hebrard, P.; Vallée, F. Convergence of the latest standards addressing safety and security for information technology, 2010. Available online: https://hal.archives-ouvertes.fr/hal-02267717/ (accessed on 15 October 2019)
61. Woskowski, C. A pragmatic approach towards safe and secure medical device integration. In Proceedings of the International Conference on Computer Safety, Reliability, and Security, Florence, Italy, September 2014, pp. 342–353.
62. Eames, D.P.; Moffett, J. The integration of safety and security requirements. In Proceedings of the International Conference on Computer Safety, Reliability, and Security, Toulouse, France, 27–29 September 1999, pp. 468–480.
63. Kornecki, A.J.; Zalewski, J. Safety and security in industrial control. In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, Oak Ridge, TN, USA 21–23 April 2010, p. 77. doi: 10.1145/1852666.1852754.
64. Novak, T.; Gerstinger, A. Safety-and security-critical services in building automation and control systems. *IEEE Trans. Ind. Electron.* **2009**, *57*, 3614–3621.
65. Subramanian, N.; Zalewski, J. Assessment of safety and security of system architectures for cyberphysical systems. In Proceedings the 2013 IEEE International Systems Conference (SysCon), Orlando, FL, USA, 15–18 April 2013, pp. 634–641. doi: 10.1109/SysCon.2013.6549949.
66. Fovino, I.N.; Masera, M.; De Cian, A. Integrating cyber attacks within fault trees. *Reliab. Eng. Syst. Safe.* **2009**, *94*, 1394–1402.
67. Bezzateev, S.; Voloshina, N.; Sankin, P. Joint safety and security analysis for complex systems. In Proceedings the 2013 13th Conference of Open Innovations Association (FRUCT), Petrozavodsk, Russia, 22–26 April 2013, pp. 3–13.
68. Kornecki, A.; Liu, M. Fault tree analysis for safety/security verification in aviation software. *Electronics* **2013**, *2*, 41–56.
69. Steiner, M.; Liggesmeyer, P. Combination of safety and security analysis-finding security problems that threaten the safety of a system, 2013. Available online: https://hal.archives-ouvertes.fr/hal-00848604 (accessed on 4 November 2019)
70. Piètre-Cambacédès, L.; Deflesselle, Y.; Bouissou, M. Security modeling with BDMP: from theory to implementation. 2011 Conference on Network and Information Systems Security, La Rochelle, France, 18–21 May 2011; doi: 10.1109/SAR-SSI.2011.5931382.
71. 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. 2013 Federated Conference on Computer Science and Information Systems, Krakow, Poland, 8–11 September 2013, pp. 1393–1399.
72. Sindre, G. A Look at Misuse Cases for Safety Concerns. *Situational Method Engineering: Fundamentals and Experiences*; Ralyté, J.; Brinkkemper, S.; Henderson-Sellers, B., Eds.; Springer US: Boston, MA, USA, 2007; pp. 252–266.
73. Jürjens, J. *Developing safety-and security-critical systems with UML*. DARP workshop: Loughborough, UK, 2003.
74. Apvrille, L.; Roudier, Y. Towards the model-driven engineering of secure yet safe embedded systems.*arXiv* **2014** *arXiv preprint arXiv:1404.1985*. Available online: https://arxiv.org/abs/1404.1985 (accessed on 8 November 2019)
75. Roth, M.; Liggesmeyer, P. Modeling and analysis of safety-critical cyber physical systems using state/event fault trees. Available online: https://hal.archives-ouvertes.fr/SAFECOMP2013-DECS/hal-00848640 (accessed on 18 October 2019)

76. Brunel, J.; Chemouil, D.; Rioux, L.; Bakkali, M.; Vallée, F. A viewpoint-based approach for formal safety & security assessment of system architectures. Available online: https://hal.archives-ouvertes.fr/hal-01070960 (accessed on 22 October 2019)
77. Zafar, S.; Dromey, R.G. Integrating safety and security requirements into design of an embedded system. 12th Asia-Pacific Software Engineering Conference (APSEC'05), Taipei, Taiwan, 15–17 December 2005; pp. 8–pp.
78. Pieters, W.; Lukszo, Z.; Hadziosmanovic, D.; van den Berg, J. Reconciling Malicious and Accidental Risk in Cyber Security. *J. Internet Serv. Inf. Secur.* **2014**, *4*, 4–26.
79. Sun, M.; Mohan, S.; Sha, L.; Gunter, C. 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), Newark, NJ,USA, 22–24, July 2009. doi:10.1049/iet-cps.2018.5068.
80. Simpson, A.; Woodcock, J.; Davies, J. Safety through security. In Proceedings Ninth International Workshop on Software Specification and Design, Available online: https://www.computer.org/csdl/proceedings-article/iwssd/1998/00667912/12OmNx4gUlw (accessed on 22 October 2019)
81. Delange, J.; Pautet, L.; Feiler, P. Validating safety and security requirements for partitioned architectures. In Proceedings of the International Conference on Reliable Software Technologies, Brest, France,8–12 June 2009, pp. 30–43.
82. Young, W.; Leveson, N.G. An integrated approach to safety and security based on systems theory. *Commun. ACM* **2014**, *57*, 31–35.
83. Schmittner, C.; Ma, Z.; Schoitsch, E.; Gruber, T. A case study of fmvea and chassis as safety and security co-analysis method for automotive cyber-physical systems. In Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, Singapore, Singapore, 14 April 2015, pp. 69–80.
84. Schmittner, C.; Ma, Z.; Smith, P. FMVEA for safety and security analysis of intelligent and cooperative vehicles. In Proceeddings of the International Conference on Computer Safety, Reliability, and Security, Florence, Italy, September 2014, pp. 282–288.
85. Chung, L.; Nixon, B.A.; Yu, E.; Mylopoulos, J. *Non-functional Requirements in Software Engineering*; Springer US: Cham, Switzerland; 2012.
86. Subramanian, N.; Zalewski, J. Quantitative assessment of safety and security of system architectures for cyberphysical systems using the NFR approach. *IEEE Syst. J.* **2014**, *10*, 397–409.
87. Winther, R.; Johnsen, O.A.; Gran, B.A. Security assessments of safety critical systems using HAZOPs. International Conference on Computer Safety, Reliability, and Security, Budapest, Hungary, 26–28 September 2001, pp. 14–24.