Safety and Security Co-Analyses: A Systematic Literature Review

Elena Lisova, Irfan Šljivo, and Aida Čaušević

Abstract—**Latest technological trends lead towards systems connected to public networks even in critical domains. Bringing together safety and security work is becoming imperative, as a connected safety-critical system is not safe if it is not secure. The main objective of this study is to investigate the current status of safety and security co-analysis in system engineering by conducting a Systematic Literature Review. The steps of the review are the following: the research questions identification; agreement upon a search string; applying the search string to chosen databases; a selection criterion formulation for the relevant publications filtering; selected papers categorization and analysis. We focused on the early system development stages and identified 33 relevant publications categorized as: combined safety and security approaches that consider the mutual influence of safety and security; safety informed security approaches that consider influence of safety on security; security informed safety approaches that consider influence of security on safety. The results showed that a number of identified approaches are driven by needs in fast developing application areas, e.g., automotive, while works focusing on combined analysis are mostly application area independent. Overall, the study shows that safety and security co-analysis is still a developing domain.**

Index Terms—**Functional safety, security, co-analysis, requirements engineering, hazards, vulnerabilities, threats.**

I. Introduction

WITH ubiquitous presence of technology and our increased reliance on it, the risk of harm we face due to such technology increases as well. The harm we are exposed to is not just direct physical harm due to for example car accidents, but it includes e.g., financial, environmental, emotional harm, which can also lead to physical harm. Traditionally, different causes that may lead to harm have been treated seperately in safety-critical system engineering. For example, unreasonable risk of harm due to malfunctioning behaviour of technological systems is addressed under the umbrella of functional safety, where functional safety is described as *"a freedom from unacceptable risk"* [1]. With increased connectivity of these systems, the risk of undesirable consequences has increased due to the possibility of an adversary intentionally causing the undesirable consequences. The risk of such intentionally caused harm through the technological systems has been generally addressed by security solutions, which were traditionally analysed and proposed separately from safety solutions [2]. Security is often defined as a system property that allows the system *"to perform its mission or critical functions despite risks posed by threats"* [3].

Safety engineering and security engineering as a way of addressing safety/security challenges have developed separately. While the malfunctioning behaviour addressed by safety engineering was the primary concern in such systems, the increased risk of intentionally caused harm required additional focus on security engineering. Nowadays, there is a need to integrate safety and security engineering in such a way that the unreasonable risk of harm due to either malfunctioning or malicious intent is adequately addressed. This is particularly important for highly connected modern safety-critical systems that cannot be considered safe unless they are secure at the same time. The way in which this integration is performed significantly influences the efforts needed to design a safe and secure system. For example, safety and security solutions do not always support each other, e.g., encrypting a message needed for security reasons increases the time needed to deliver the message, which may increase the delivery time over the required safety threshold. If safety and security are being treated separately and their integration takes place at later development stages, it implies greater effort to harmonise different solutions. As with requirements engineering, the later the inconsistencies are detected, the more work needs to be performed due to repetition. The earlier the integration of safety and security can be achieved, the fewer iterations are needed to harmonise them. We have identified the early system development stages where safety and security analyses are performed as the most critical stage for their harmonisation. Significant amount of academic effort is being invested into researching harmonisation at early system development stages [4]–[6]. At the same time, state of the practice is lagging behind due to the strict certification and standardization requirements that take longer time to adapt to new developments.

In this paper we investigate the existing research that addresses the analysis of both safety and security aspects. For this purpose we present a structured map of the available research literature, focusing on the holistic safety and security analysis by conducting a systematic literature review (SLR) method as described in Section II. The goal of the study is to get better comprehension of the available safety and security analysis approaches. In particular, we explore what kind of integration the available approaches promote. This information can tell us if the research is converging towards a particular kind of integration, and what are the causes for such convergence. The insights from this study might be useful for both academia and industry, as the first might get a better view of the directions and possible gaps in state-of-the-art, while the latter can use the study as a source to find suitable co-analysis methods relevant for their domains. We present the results and

E. Lisova, I. Šljivo, and A. Čaušević are with Mälardalen University, Västerås, Sweden.
E-mail: {elena.lisova, irfan.sljivo, aida.causevic}@mdh.se

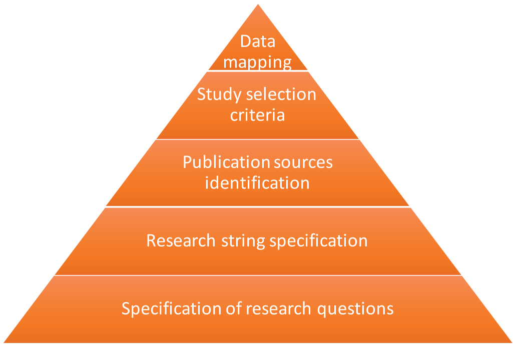
Data mapping
Study selection criteria
Publication sources identification
Research string specification
Specification of research questions

Fig. 1: Steps of the SLR process

their analysis in Section III. The classification of the relevant papers is done with respect to type of the approach, where we have identified three categories: security informed safety, safety informed security and combined safety and security approaches. Additionally, we have investigated if the analysis is performed on the hazard/threat identification level or during requirements engineering. Furthermore, we have investigated whether the analyses of both safety and security are unified or they are parallel and need additional harmonisation. Finally, we have identified different characteristics of each publication regarding the relation with industry, application domain, relevant standards and the type of validation used. We discuss validity of presented results in Section IV, followed by Section V where we present the related work. The final conclusions are described in Section VI.

II. Research Method

The work in this paper is based on a SLR, an empirical study with the purpose to evaluate and interpret all available research relevant to a particular question, topic of interest or phenomenon. We have adopted an approach and guidelines to conduct a SLR proposed by Kitchenham [7]. The aim of a SLR is to present an impartial evaluation of a research topic using reliable and rigorous methodology. In the review process, we have adopted a process that defined all steps needed to be taken for a review to account as a SLR. The process includes description of the research questions, search string specification, publication sources identification as well as preliminary study selection criterion and data mapping. The process is depicted in Fig. 1 and the details of individual steps are provided in the following sections.

A. Research Questions

SLRs are driven by a specific purpose translated into a set of research questions that is the initial step of the study. We formulate the following research questions focusing on the research area of *“Functional safety and security co-analysis at the early system development stages”*:

RQ-1: What are the analysis methods adopted to address interplay of safety and security at the early system development stages?

RQ-2: How do the identified analysis methods address the interplay of safety and security?

The main reason for limiting the scope of the work to the early system development stages is the importance of the harmonisation of safety and security at those stages for the overall cost and effort needed to design a safe and secure system. Considering the whole development lifecycle could introduce a larger amount of publications that we would not be able to asses in the right way, possibly losing the focus from the main goal. Hence, in this review, we focus on analyses that take part during the hazards and threats identification and risk assessment, and requirements elicitation/analysis. Since both safety and security engineering promote to design safety and security in the system from the beginning, the selected stages become critical as there we identify the problems and choose ways to address them. The earlier we discover inconsistencies between the chosen solutions, the fewer repetitions are needed. The efforts needed to achieve an adequate design depends on whether the safety and security analyses are performed separately and then the results are evaluated jointly, or if a unified analysis is performed. Hence, we also investigate the nature of those analyses in more depth.

B. Scope of the Search

In the next step of the study we have specified the search string that is used to find relevant publications in selected databases. The search string is based on the keywords that are in line with the purpose of the paper, as discussed in Section I. We specify the following Boolean string to search the relevant databases:

(*“safety”* **AND** *“security”* **AND** *“analysis”*)

The following on-line databases have been part of the investigation: IEEE Xplore digital library [1], ACM digital library [2], Web of Science [3], SpringerLink [4]. We have performed our search to find suitable publications from year 2012 until the end of 2017. We have restricted the search to journal, conference and workshop papers as well as peer-reviewed book chapters, while excluding non-peer reviewed abstracts and publications from the search. We have used the Mendeley application to record the search results.

C. The Selection Criterion

Our initial search, i.e., Stage 1 in Table I, resulted in 13711 papers in total. For a paper to be included in the next phase, the following criterion must be met, *Criterion 1: the publication must propose or discuss safety and security analysis approaches in system engineering*. Thus, at Stage 1 at least one person has read all the titles and excluded papers that have not been related to the inclusion criterion. After this step we have had 351 papers for Stage 2 as given in Table I, where we have read both the titles and abstracts. This step has been performed by all reviewers, i.e., the review authors, with a possibility to grade every paper with one out of three choices: X - paper is not relevant, ⋄ - paper is borderline, ✓- paper

[1] http://ieeexplore.ieee.org/Xplore/home.jsp

[2] https://dl.acm.org/

[3] http://webofknowledge.com/

[4] https://link.springer.com/

TABLE I: Study selection stages performed by the authors

Stage	Activity	Papers
1	Applied the search query to all the sources and gathered the results	13711
2	Applied inclusion/exclusion criterion to the papers titles and abstracts	351
3	Applied inclusion/exclusion criterion to the full texts	69
4	Finalised the set of included papers	33

TABLE II: Stage 2 paper distribution

Paper group			Number of papers
Reviewer 1	**Reviewer 2**	**Reviewer 3**	
X	X	X	154
✓	✓	✓	41
X	◇	X	19
X	X	◇	21
◇	X	X	19
✓	◇	◇	13
◇	◇	◇	10
✓	◇	X	9
◇	◇	X	8
✓	✓	◇	8
✓	◇	✓	7
X	◇	◇	5
◇	✓	✓	6
✓	X	X	4
◇	◇	✓	4
✓	✓	X	3
◇	X	◇	5
◇	✓	◇	3
X	✓	◇	3
X	X	✓	2
X	✓	✓	3
◇	✓	X	2
X	◇	✓	1
✓	X	✓	1
X	✓	X	0
✓	X	◇	0
◇	X	✓	0

TABLE III: Stage 3 paper distribution

Paper group			Number of papers	Relevant papers
✓	✓	✓	41	22
✓	✓	◇	8	2
✓	◇	✓	7	3
◇	✓	✓	6	3
✓	✓	X	3	0
✓	X	✓	1	1
X	✓	✓	3	2

is relevant. As a result, the groups presented in Table II have been derived. Stage 3 in Table III implies reading of complete papers and includes papers for which at least two reviewers have marked it as relevant (✓). At stage 3, we have evaluated the papers to see whether they include a complete description about an analysis method (i.e., position or work in progress papers have been discarded) that incorporates both safety and security, as well as evaluation on a case study. This approach has provided us with 69 papers to be included at Stage 3 (see Table III). While reading the full papers, we have had cases when not all reviewers agreed upon whether the paper should be included or not. Such cases have been discussed to make a consensus, and some of these papers have been included in the final list. Within Stage 4 we have identified 33 papers as relevant for addressing our RQ-1 (Section II-A).

D. Characterization of the Selected Papers

Our selection process resulted in 33 papers on safety and security analysis. Table IV shows the number of papers returned by each source, as well as the number of papers that we have selected after applying the inclusion/exclusion criterion. The table also includes the differences between sources in terms of included studies (precision) and coverage level (recall). The precision of the selected sources, i.e., how many papers are identified as relevant at the Stage 4 out of the the initial search result at Stage 1 within a particular search source, varied from 0.1% to 2.4% and recall, i.e., how many papers within a particular search source are identified as relevant out of relevant papers collected from all sources, from 7% to 39%. IEEE Explore and SpringerLink have been the sources with the most selected studies (13) and (14), and with an average precision of 0.6% and 0.2% respectively. SpringerLink also has had the highest number of items returned by the query (8479). When it comes to the coverage level, SpringerLink has had the highest coverage (42%), the next is IEEE Explore (39%), then ACM digital library (12%) and Web of Science (WoS) (7%). IEEE Explore, ACM digital library and SpringerLink have been chosen as prime sources for the search, while WoS has been considered as a secondary source since it covers publications from multiple publishers. Since papers from WoS have been overlapping with the papers identified from the prime sources, only 15 papers from WoS, not already in other databases, have been included in Stage 2 (see Table IV). We have analysed what kind of papers have been published in this area (Table Vb) and how many studies have been published per year (Table Va). Searches in all sources are covering the range 2012 - 2017.

E. Data Mapping

In this phase the 33 selected papers have been categorised into five groups. The classification has been based on titles, abstracts, and full-text reading. A brief description of each group is provided below, while detailed discussion can be found in Section III.

Five groups have been derived based on the following two criteria: (*i*) what is the overall reason for considering both safety and security: to achieve a safe system, to achieve a secure system, or to achieve both safe and secure system; (*ii*) how is the process of performing both safety and security analyses done: jointly — both safety and security analysis are part of the same activity, parallel — safety and security analyses are performed separately and an additional activity is needed to integrate the results. Based on the first criterion we identify the following three groups: **combined approaches** — safety and security are both the overall target of the analysis, **security informed safety approaches** – safety is considered as an overall goal, **safety informed security approaches** — methods where performing both safety and security analyses is done for the sake of achieving a secure system. We identify two more groups based on the second criterion: **unified approaches** — safety and security are analysed jointly, **parallel approaches** — additional harmonization of separate safety and

TABLE IV: Number of retrieved papers per source

Source	Stage 1	Stage 2	Stage 3	Stage 4	Precision (%)	Recall (%)
IEEE Explore	2264	167	40	13	0.6	39
ACM digital library	166	116	7	4	2.4	12
SpringerLink	8479	53	18	14	0.2	42
Web of Science	2802	15	4	2	0.1	7

TABLE V: Paper distributions

Publication year	Quantity	Percentage (%)
2012	2	6
2013	2	6
2014	6	18
2015	5	15
2016	7	22
2017	11	33
Total	33	100

(a) Paper distribution per year

Paper type	Quantity	Percentage (%)
Conference paper	23	70
Workshop paper	3	9
Symposium paper	5	15
Journal	1	3
Book chapter	1	3
Total	33	100

(b) Paper type distribution

security analyses outcomes is required to address the possible dependencies between safety and security.

Beside this classification we also take into account information regarding application area, existence of validation within the approach, source of publication (i.e., research or industrial community), as well as whether the approach is associated in any way with existing standards (see Table VI). More detailed classification of retrieved results have been done with respect to which part of the lifecycle the approach is applicable to. We have considered Hazard Analysis and Risk Assessment (HARA) [8], approaches that provide hazard identification, as well as hazard analysis including identification and assessment of environmental conditions along with exposure or duration. Additionally, Threat Assessment and Remediation Analysis (TARA) that has been defined in SAE J3061 [9] has been considered. It is an engineering methodology to identify, prioritize, and respond to cyber threats by introducing countermeasures that reduce sensitivity to cyber attack. Finally, we have also considered analysis at the Requirement Engineering (RE) stage, which is the process of requirements elicitation, analysis and conflict resolving (see Table VI).

III. Results and Analysis

In this section we first briefly describe papers that are identified as relevant to RQ-1, and further present analysis results of our findings, relevant for answering RQ-2.

A. Papers Identified as Relevant

This subsection presents a brief overview of the 33 papers ordered in the chronological and alphabetical order that we have identified as relevant.

1) **Raspotning et al. (2012)** [10] present Combined Harm Assessment of Safety and Security for Information Systems (CHASSIS) that is a high level approach combining safety and security methods in order to provide a joint assessments approach, suitable for early phases of system development. The approach is based on modelling misuse cases and misuse sequence diagrams within a UML behaviour diagram, which might imply some additional modelling expenses for the early development phase, and provides as an outcome security and safety requirements specification.

2) **Reichenbach et al. (2012)** [11] propose an approach on combined safety and security risk analysis by extending Threat Vulnerability and Risk Assessment (TVRA) technique with Safety Integrity Levels (SILs) from the generic functional safety standard IEC 61508 [1]. The risk associated with a function in this extended TVRA is calculated based on both security factors as well as SILs of the considered function. The approach aims at identifying which security vulnerabilities are safety-relevant. The technique does not depend on safety analysis, but provides means to identify the influence of security vulnerabilities on safety.

3) **Silva and Lopes (2013)** [12] present activities that have been performed in order to certify a safety-critical system in the railway domain and describe how security can be taken care of without endangering reliability or safety. In this work they use Failure Modes, Vulnerabilities and Effect Analysis (FMVEA) and fault tree analysis where for every safety failure event they derive possible security failure events.

4) **Young and Leveson (2013)** [6] propose a STPA-Sec method, which is based on already existing top-down safety hazard analysis method System-Theoretic Process Analysis (STPA). The method requires a multidisciplinary team consisting of security, operations, and domain experts to identify and constrain the system from entering vulnerable states that lead to losses and is useful at the concept phase. In the approach hazards are presented as control problems. Each control action is reviewed under a set of a different conditions and guidewords to identify loss scenarios. The approach allows to focus on vulnerable states in order to avoid threats to exploit them and create disruptions, and eventual losses.

5) **Chen et al. (2014)** [13] build upon extending the NIST 800-30 [14] methodology to consider safety aspects contributing to risk assessment by establishing a functional relationship between vulnerabilities, threats and hazards. Hazards occurrence levels are assigned depending on a value of a hazard-threat conditional probability. The assets impact is assigned based on a critical digit asset characterization. These values

along with control risk reflecting safety and security design assessment define safety-security risk of an incident.

6) **Ito (2014)** [15] proposes an analysis for threats and hazards identification as an extension of the hazard identification approach CARDION. The approach is iterative and includes four phases: system sketching; top goal identification and its decomposition; applying HAZOP guidewords to each goal; threat and hazards identification. System sketching can be performed with UML, SysML or CATALYSIS [16].

7) **Kriaa et al. (2014)** [17] present a case study on an industrial control system in which the previously developed BDMP formalism is used to model safety and security interdependencies. The approach allows reasoning about antagonism between safety and security, as well as conditional dependency and mutual reinforcement between the two. The case study illustrates the ability of BDMP not only to evaluate risks, but also to optimise the choice of countermeasures against attacks. The analysis is performed as a single joint activity to address both safety and security, but it may depend on other safety/security activities for input.

8) **Schmittner et al. (2014)** [18] propose the FMVEA, method based on already existing approach from the safety domain FMEA, described in IEC 60812 [19]. The method incorporates both failure mode and failure effect model for safety and security cause-effect analysis. It is a high level approach suitable for design and verification phase in a system development and for an analysis of only single causes of an effect. In the approach threats are quantified using threat agents that represent attackers, threat modes are extracted using STRIDE model [20] that result in threat effects and attack probabilities. Since the analysis depends on the accuracy of a system model, one of the benefits of the approach is a possibility to reuse previously acquired results and redo the analysis in case a new threat or vulnerability is identified [4].

9) **Apvrille and Roudier (2015)** [21] propose to use SysML-Sec to investigate possible impact of introducing security solutions on safety-related functions for embedded and Cyber-Physical Systems (CPSs). SysML-Sec adapts a goal-oriented approach for capturing requirements and a model-oriented approach for specifying architecture and threats. Within the analysis resources to be protected and their connection to safety and security requirements are identified. The analysis methodology is based on Y-chart approach [22] and follows V-cycle. The analysis is supported by an open-source software TTool for model specification and verification, and by AVATAR for analysing requirements and attacks. SysML-Sec assesses compatibility of security requirements with regards to system safety at partitioning and design stages.

10) **Cimatti et al. (2015)** [23] present an overview of the D-MILS approach for verification of safety and security requirements. Both types of requirements are allocated to the system components and formalised via component contracts. The verification of the requirements in the given system can be performed by checking contract refinement between the contracts of components comprising the system. The result of the refinement analysis can be previewed as fault trees showing the dependencies of the system and components failures.

11) **Gu et al. (2015)** [24] present an approach for treating safety and security requirements together with a focus on resolving their conflicts. The analysis is based on identification of safety and security goals, their corresponding requirements and a connection between them, i.e, checking whether they undermine or improve each other. A conflict resolutionis done based on weighting of resolutions values for conflicted requirements.

12) **Kriaa et al. (2015)** [25] present an approach for joint risk assessment that can be applied for both design and operational phases of the system development. The S-cube (SCADA Safety and Security modelling) approach takes as input the system architecture and provides attacks and failures scenarios that may lead to given hazards. The analysis relies on a knowledge base of safety and security risks and uses Figaro language to model different system components, each of which is associated with related failure modes and attacks.

13) **Macher et al. (2015)** [26] describe Security-Aware Hazard and Risk Analysis (SAHARA). The method combines two well known approaches HARA [27] coming from automotive domain and STRIDE [20] that focuses on threat modelling to review system design in a methodical way. The result of the method is quantified security impact on the safety-critical system development. Initially, the safety analysis is done with respect to ISO 26262 and using HARA analysis, while the security analysis is done based on STRIDE method independently. The results form security analysis are further used in ASIL quantification concept providing the resulting security level.

14) **Popov (2015)** [28] presents an approach for stochastic modelling of safety-critical systems considering both random failures and malicious attacks. In particular, the approach considers only those attacks that may lead to elimination of the safe state of the device. By considering probabilistic modelling of both failures and attacks it is possible to quantify the risk from cyber attacks.

15) **Steiner and Liggesmeyer (2015)** [29] propose a Security Enhanced Component Fault Trees (SECFTs) analysis. In order to assign probabilities to security related causes, i.e., to conduct a quantitative analysis, basic events are grouped into minimal cut sets (MCSs), and probabilities are assigned to sets instead of events. The probabilities values are picked from the discreet set aligned with classification from IEC 61025 [30]. The qualitative analysis within the approach is based on identification of all MCSs and their handling depending on included events nature, i.e., security, safety or mixed.

16) **Wei et al. (2015)** [31] describe an approach based on HAZOP in which they strive towards including security related information into the hazard analysis, and apply it to an open source immobiliser protocol stack.The authors focus on the design phase in the system development and extend the guidewords by reusing the attack taxonomy of the Computer Emergency Response Team (CERT). The approach provides a detailed information on a set of primary and secondary guidewords and their combinations.

17) **Islam et al. (2016)** [32] propose a framework for threat analysis and risk assessment inspired by ISO 26262 [27].

Due to the tight coupling with the automotive safety standard and inspired by the industry, the paper aims at providing a framework readily applicable in the automotive domain. The framework addresses security risks and aligns the proposed security analysis with the ISO 26262 development process. The work aims to ease co-certification of safety and security for a given system. By proposing a security analysis aligned to the existing safety analysis, the approach addresses identification of all properties relevant for safety or security.

18) **Nicklas et al. (2016)** [33] propose a system engineering-based approach that consist of a SySML-based model accompanied with a procedure in order to establish safe and secure design of cyber physical systems. Initially a system definition is provided via the Generic Systems Engineering analysis and a safety case is described using SySML notation. The combination of these two enables identification of possible attacks scenarios. A qualitative assessment of probabilities of occurrence and goal achievement of the attack scenarios is used to derive security structures containing the limitation of communication and encryption. In the final step possible safety-security goal conflicts related to the analysed safety use case are harmonized into a sequence diagram to achieve an adequate safety and security level.

19) **Ponsard et al. (2016)** [34] present a methodology that utilises existing techniques such as Goal-oriented requirements Engineering (GORE), to co-engineer safety and security. The approach takes results from safety and security analysis to build a goal tree connecting requirements with the related hazards/vulnerabilities where each object can be marked as safety or security relevant. The analysis of safety and security requirements is performed jointly, although the input to this technique from hazard/threat identification activities may come from different sources.

20) **Schmittner et al. (2016)** [35] focus on improving existing approach STPA-Sec [6] and concept phase in the lifecycle. They have identified the guidance for the identification of intentional casual scenarios not being clear enough and proposed some modifications, as well as a need to include security relevant elements into control loop model.

21) **Shapiro (2016)** [36] proposes a modification of STPA-SEC [6] to support a technical risk analysis for privacy engineering, namely STPA-Priv. The approach is based on the already existing one while introducing the systematic analysis of system controls and their ability to constrain behaviours that might compromise privacy.

22) **Troubitsyna (2016)** [37] proposes an approach for integrated derivation and analysis of safety and security constraints built on top of the systems thinking paradigm presented by STAMP, and the assurance case structuring via Goal Structuring Notation (GSN). The proposed approach consists of a GSN pattern inspired by STAMP. The work proposes a joint treatment of safety and security requirements by using the described GSN pattern for their structuring.

23) **Dürrwang et al. (2017)** [38] describe a Security Guideword Method (SGM) approach used to identify information assets and protection goals relevant for safety where artefacts from the ISO 26262 hazard analysis are reused. SGM is based on security guidewords, useful when identifying possible attack scenarios, similar to HAZOP from safety domain. The approach provides unified safety and security constructs that minimise safety and security integration effort in automotive domain, and enable non-security engineers to identify information assets and protection goals.

24) **Friedberg et al. (2017)** [39] present a combined analysis method for safety and security called STPA-SafeSec based on STPA [40] and STPA-Sec [6], and used to choose the most effective mitigation strategies to ensure system safety and security. The benefits of the approach is unified safety and security consideration while choosing suitable mitigation strategies, a possibility to prioritize the most critical system components for an in-depth security analysis (e.g. penetration testing). The analysis identifies potential system losses, caused by a specific security or safety vulnerability, and better mitigation strategies.

25) **Howard et al. (2017)** [41] propose a method to identify and formally analyse safety and security requirements. This approach is based on the STPA [40] methodology and combined with modelling, traceability and formal verification through use of the Event-B formal method. The aim is to generate critical requirements to be able to prevent undesirable system states. Using Event-B language and the Rodin toolset they demonstrate and verify that these critical requirements fully mitigate against the undesirable system states.

26) **Kumar and Stoelinga (2017)** [42] propose an approach handling attack-fault trees (AFT) with dynamic gates allowing to consider more complex multiple step scenarios. The authors present possible transformation of dynamic gates into stochastic times automata that allows to use UPPAAL model checker for statical model checking. The approach includes quantitative analysis of AFTs and consideration of several safety-security scenarios, e.g., *as-is scenario* and *what-if scenario*, leading to identification of the most risky scenarios and selection of the most effective countermeasure.

27) **Pereira et al. (2017)** [40] present an analysis built on a combination of STPA and guidelines from NIST SP800-30. The rationale behind the analysis is merging of a system based approach addressing safety and a component-based approach focused on threats and vulnerabilities. The authors demonstrate how to align safety and security workflows and where they need to overlap.

28) **Plósz et al. (2017)** [43] propose a method combining parts of existing methodologies, STRIDE [20] and FMEA [19]. These safety and security analyses are divided in two parts with an integration stage after the first parallel activities that provides a combined safety and security threat catalogue. Integration results are further fed into the second part of both methods for impact assessment on the security side and likelihood assessment on the safety side. The approach advantages are saving effort by taking care of commonalities of separate assessments at once, utilizing the combined catalogue to raise awareness on issues that has high impact or likelihood on both areas, and supporting multi-dimensional decisions made by tackling security and safety together.

29) **Procter et al. (2017)** [44] extend the Systematic Analysis

of Faults and Errors (SAFE) to provide better integration of security reasoning within safety. In this paper the authors advocate that the Dolev-Yao model provides better integration of security into safety, the model is extended with guidewords to accommodate both safety and security.

30) **Ruijters et al. (2017)** [45] present an uniform meta-model allowing to merge attack tree analysis (ATA) and fault tree analysis (FTA) in AFT. The developed tool provides a bidirectional transformation between joined AFT model and independent models The AFT model can be transferred to UPPAAL for quantitative analysis purposes, e.g., reliability.

31) **Sabaliauskaite and Adepu (2017)** [46] extend the six-step model for design of safe and secure CPSs with support for identification of possible failures and cyber attacks. In the first two steps of the approach, the functions/requirements are defined together with the system architecture. In the next two steps, failures and corresponding safety measures are added to the model. In the final two steps, attacks and the corresponding security countermeasures are added to the model. The paper extends this model by introducing Information Flow Diagrams (IFDs) that are used to support the safety and security steps. The approach captures different information flows related to different safety and security aspects in IFDs, and aims at analysing their interdependency.

32) **Temple et al. (2017)** [47] propose an approach combining STPA-Sec [6] and FMVEA [48], and integrating them into a unified analytical process called Systems-Theoretic Likelihood and Severity Analysis (STLSA). STLSA focuses on system functional control actions, includes humans-in-the-loop and incorporates semi-quantitative risk assessment aligned with EN 50126.

33) **Vistbakka et al. (2017)** [49] describe a unified approach that enables safety and security co-engineering. The main goal of the approach is to demonstrate the benefit of formal methods when analysing impact of security to safety and other way around by using Event-B [50]. The initial model is based on the abstract specification, further refined to include system nominal and failure behaviours. The authors consider the effect of security vulnerabilities on system safety.

B. Results

The main information extracted from the papers has been summarized in Table VI. It presents the summary of the following characteristics of the identified papers: *(i)* whether the approach is associated with any of the relevant safety/security standards; *(ii)* a type of an approach validation presented in the paper; *(iii)* whether the approach is proposed by industry or academia; *(iv)* which is the application area of the approach demonstrated in the paper; and *(v)* which early system development stages does the work cover, HARA/TARA and/or RE. The mapping of the relevant papers as described in Section II-E, is presented in Table VII.

In Table VI, we consider the following types of validation based on the paper text: case study, example, empirical study or conceptual validation. The latter implies only a sketch of the approach without a concrete example. Moreover, we distinguish between academia and industry driven publications based on the origin of the authors as well as the explicit correlation of the used case study or example with a particular company. We have also examined the connection of the proposed approaches with existing safety or security standards. One can notice that the association with a standard is almost in all cases directly related to the targeted application area of the approaches. A large number of papers is aiming at addressing safety/security concerns in the automotive domain, thus using ISO 26262 standard, an international standard for functional safety of electrical and/or electronic systems in automotive domain, followed by generic approaches applicable to any domain, and industrial control systems domain. Furthermore, we have identified which early system development stages do the papers cover with their proposed contributions, identifying whether they cover only one of the two stages, or both.

In Table VII, we have grouped each paper in two categories: one considering the focus of the work; and the other identifying the way interdependencies are managed. In the first category (columns in Table VII), we have mapped papers into three groups (*i*) safety informed security; (*ii*) security informed safety; and (*iii*) combined safety and security approaches. In the second category (rows in Table VII), we investigated whether the work proposes a unified way of analysing interdependencies between safety and security or a parallel approach where additional harmonisation of interdependencies is required. As shown in Table VII, we have not identified works that focus on exploring only the influence of safety on security, i.e., safety informed security approaches. All publications focus on either exploring the influence of security on safety or exploring the interdependencies between safety and security. This two step categorization resulted in 4 groups of papers. In the reminder of the section we discuss the typical limitations of papers from each group.

Combined safety and security approaches that perform safety and security analyses in parallel are located in the upper left cell of Table VII. Generally, approaches in this group require an integration activity to harmonise the results of the separate safety and security analyses. While such approaches to analysing the interplay of safety and security may be the easiest to implement in practice, they may also incur too many iterations needed for harmonising the conflicting safety and security requirements. For example, Gu et al. (2015) [24] require safety and security mechanisms already in place, while Islam et al. (2016) [32] do not include formulation of technical security requirements for the system nor assumptions regarding hardware and software level based on the security level. The most important activity for approaches in this group is the integration activity for harmonising safety and security analyses results. In this respect, we have identified the need for further improvement of the proposed integration activities in these types of approaches.

Security informed safety approaches that take safety and security analyses results performed in parallel and analyse the influence of security on safety are presented in the right upper cell of Table VII. What we can say for all parallel approaches, just as for the previous group, the post safety and security analyses integration activity is the most important aspect. While in the previous group that activity included analysis of dependencies of both safety on security and vice versa, in

TABLE VI: Relevant papers characterization

	Paper	Associated with a standard	Validation	Contribution origin	Application area	Lifecycle stages coverage	
						HARA and TARA	RE
1	Raspotnig et al. (2012) [10]	No	Example	Academic	Air traffic		✓
2	Reichenbach et al. (2012) [11]	IEC 61508, ETSI TS 102 165-1	Example	Industrial	Control Systems	✓	
3	Silva et al. (2013) [12]	EN 5012x, IEEE 1474	Case Study	Industrial	Railway	✓	
4	Young and Leveson (2013) [6]	No	Conceptual	Academic	Generic	✓	✓
5	Chen et al. (2014) [13]	NIST 800-30	Case Study	Academic	Nuclear	✓	
6	Ito (2014) [15]	ISO 26262, ISO/IEC 27000	Conceptual	Industrial	Automotive	✓	
7	Kriaa et al. (2014) [17]	No	Case Study	Industrial	Control Systems	✓	✓
8	Schmittner et al. (2014) [18]	IEC 61508, ISO/IEC 27000	Example	Academic	Automotive	✓	
9	Apvrille and Roudier (2015) [21]	No	Example	Academic	Automotive		✓
10	Cimatti et al. (2015) [23]	No	Example	Academic	Generic		✓
11	Gu et al. (2015) [24]	No	Example	Academic	Control Systems	✓	✓
12	Kriaa et al. (2015) [25]	No	Case Study	Academic	Control Systems	✓	
13	Macher et al. (2015) [26]	ISO 26262	Example	Academic	Automotive	✓	
14	Popov (2015) [28]	ISO 26262	Case Study	Academic	Automotive	✓	
15	Steiner and Liggesmeyer (2015) [29]	IEC 61025, IEC 60300-3-1	Conceptual	Academic	Generic	✓	
16	Wei et al. (2015) [31]	No	Case Study	Academic	Automotive	✓	
17	Islam et al. (2016) [32]	ISO 26262, SAE J3061	Example	Industrial	Automotive	✓	
18	Nicklas et al. (2016) [33]	No	Case Study	Academic	Smart home	✓	
19	Ponsard et al. (2016) [34]	IEC61508, SAE J3061	Case Study	Academic	Automotive		✓
20	Schmittner et al. (2016) [35]	ISO 26262, SAE J3061	Case Study	Academic	Automotive	✓	✓
21	Shapiro (2016) [36]	No	Example	Academic	Generic	✓	✓
22	Troubitsyna(2016) [37]	No	Conceptual	Academic	Generic		✓
23	Dürrwang et al. (2017) [38]	ISO 26262	Empirical Study	Academic	Automotive	✓	✓
24	Friedberg et al. (2017) [39]	No	Case Study	Academic	Generic	✓	
25	Howard et al. (2017) [41]	No	Conceptual	Academic	Generic	✓	✓
26	Kumar and Stoelinga (2017) [42]	No	Case Study	Academic	Generic	✓	
27	Pereira et al. (2017) [40]	NIST 800-30	Example	Academic	Generic	✓	✓
28	Plósz et al. (2017) [43]	No	Case Study	Academic	Generic	✓	
29	Procter et al. (2017) [44]	No	Example	Academic	Medical	✓	
30	Ruijters et al. (2017) [45]	No	Case Study	Academic	Generic	✓	
31	Sabaliauskaite and Adepu(2017) [46]	ISA-99	Example	Academic	Generic	✓	
32	Temple et al. (2017) [47]	EN 50126-1	Case Study	Academic	Railway	✓	
33	Vistbakka et al. (2017) [49]	No	Case Study	Academic	Control Systems		✓

this group only influence of security on safety is considered. This is appropriate for those systems where security is relevant only if it influences safety. But if the intention is to also have a secure system beyond the safety relevant security issues, then these approaches are not appropriate for such systems as they do not cover analysing the influence of safety on security. For example, one of the possible limitations of the work presented by Nicklas et al. (2016) [33], is the lack of information regarding the approach suitability in larger systems where both safety and security may be equally important.

Combined safety and security approaches that propose joint analysis of safety and security and their interdependencies are located in the bottom left cell of Table VII. In general, this is the group of approaches that support building both safe and secure systems. To reduce the amount of possible iterations that may be incurred by the conflicting safety and security requirements in parallel approaches, this group of approaches proposes new ways of joint safety and security analyses that treat their interdependencies during the analysis. While reducing the number of iterations for harmonising safety and security is an important goal, the limitation of these methods is that they are generally more complex and would require more time to perform than perhaps two separate activities for analysis of safety and security. Furthermore, these approaches may be more challenging to implement in practice since they require more change to the state of practice for safety and security processes used in companies. A general concern with approaches from this group is the extent to which they support safety and security, i.e., whether they succeed in identifying hazards and vulnerabilities at least as good as the independent methods. For example, Young and Leveson (2013) [6] focus on losses that are results from violations of integrity and availability, while confidentiality is not tackled. Also, the ability of the approach to assist analysts in examining security constraints degradation over time is not addressed. Kriaa et al. (2014) [17] present an approach where it might be difficult to evaluate the parameters associated to the security part of the model. To tackle this they address robustness of the decisions that can be taken, trying to determine decisions that remain valid for a wide range of values of the most uncertain parameters. The approach presented by Cimatti et al. (2015) [23] that relies on MILS architecture and contract-based method can be seen as a promising approach given that it provides support for modelling the system architecture, contract-based analysis of the architecture, automatic configuration of the platform, and assurance case generation from patterns. However, the approach is very specific and lack of knowledge in this domain might provide incomplete results and there is no support for finer-grained information flow properties handling. Frieberg et al. (2017) [39] consider methods such as traditional failure modes and effects analysis (FMEA), more focused on component failure, while STPA-Sec is regarded as systems-based hazard analysis. This might question the scalability of the approach as for systems with complex interactions or emergent behaviour, becomes questionable whether lower level failures and threats are sufficient for system-level analysis [47].

Approaches proposing a unified way of analysing safety and security with safety as an overall goal, i.e., unified security informed safety approaches, are grouped in the bottom right cell of the Table VII. As this group of approaches is focused on safety as an overall goal, many of them are application specific due to alignment with a specific standard, however considered approaches are quite mature as limitations are already going into consideration of failures connections and complex attacks. Since the overall focus of this group of approaches is safety, the potential limitation is the application of these approaches in systems where also non-safety related security issues are important. In such case there would be duplication of work as a part of the security analysis would be performed in the unified security-informed safety activity, and the full security analysis would still have to be performed separately. While this could reduce the amount of possible iterations for harmonising safety and security, it would still mean duplication of work compared to the combined unified approaches. Furthermore, some of the approaches are domain specific and may require further work to be applied in other areas. For example, since the approach presented by Raspotnig et al. (2012) [10], specifies requirements based on ISO 26262 [27] and Hazard and Operability Study (HAZOP) tables combined with Boolean logic Driven Markov Processes (BDMP) [51] technique, thus a high level of details and good expert knowledge are required. As it depends on the expert knowledge the reusability in repeated analysis is not applicable since the level of experiences might be different in different teams, potentially affecting results [4]. The approach presented by Silva et al. (2013) [12] is also aligned with a standard from the railway domain, and in general depends on the expert knowledge. Given this the authors have not been completely convinced that the approach would be suitable for other domains without tailoring it to the specific needs. Procter et al. (2017) [44] also aim to extend the SAFE analysis proposed by them to other domains using guidewords. The analysis proposed by Schmittner et al. (2014) [18] is based on FMEA that considers only single causes of an effect, which excludes multi-stage attacks consideration. The method presented by Popov (2015) [28] may require a more complex failure model to address failure dependencies and trade-offs between safety and security. The approach proposed by Wei et al. (2015) [31] has a limitation in terms of failures connections. As the future work, the authors plan to address more complex dependencies between failures and guidewords used for the analysis, e.g., to consider multi-stages attacks. Dürrwang et al. (2017) [38] aim to add item attributes in their approach and consider guidewords, to cover more complex failure scenarios.

TABLE VII: Paper distribution based on their focus

	Combined safety and security approaches	**Security informed safety approaches**
Parallel	[24], [32], [40], [45], [46]	[11], [33]
Unified	[6], [13], [15], [17], [23], [25], [34], [36], [39], [41], [42], [43], [35], [49]	[10], [12], [18], [21], [26], [28], [29], [31], [37], [38], [44], [47]

In general, we have noticed that the identified approaches do not focus on the fact that security is dynamic in its nature [52]. This dynamic nature implies frequent system updates as a response to a new attack being developed or a new vulnerability being exploited. Such an update requires change impact analysis to the safety of the system, potentially leading to increase in time and cost. The challenge of efficient incorporation of a system update may limit the applicability of the proposed approaches. Addressing this challenge may be needed for bringing safety and security co-analysis into safety and security-critical systems engineering state-of-the-practice.

C. *Results Analysis*

We analyse the information from Tables VI and VII to identify the trends in addressing the dependencies between safety and security.

In Fig. 2, we present the correlation between the categories from Table VII and the early system development stages the papers focus on. We group the approaches with respect to the early system development stages on those addressing only RE or HARA/TARA, and those addressing both. We can notice that in general for all groups we have more unified than parallel approaches. This is in particular visible, when considering RE where all approaches focus on unified analysis of both safety and security while exploring the influence of safety on security and vice versa. Furthermore, when it comes to the distribution between security informed safety and combined safety and security analyses, we can notice from Fig. 2 that approaches addressing only RE or HARA/TARA have approximately equal focus on both. Conversely, the approaches addressing both activities focus on combined safety and security analysis.

In Fig. 3, we examine trends of addressing the combined analysis on one side, and security informed safety analyses on the other side, over the years. Over the years the focus is steadily increasing on the combined safety and security analyses side, while the research on security informed safety has been in focus for some time already, with increased focus in 2015. The trend of increased focus on combined safety and security analyses is continuing in 2017 as well.

In Fig. 4 we consider the three most active domains (automotive, generic, and control systems) and explore their

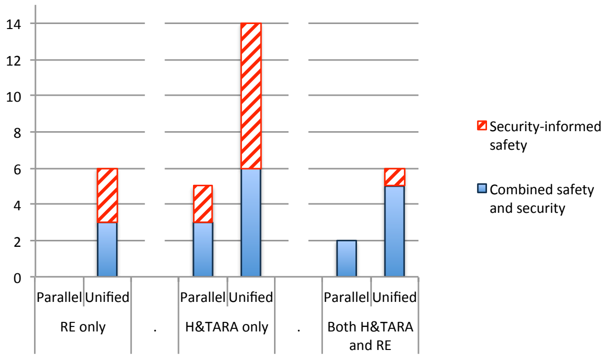

Fig. 2: The paper distribution based on the stage they address and their safety/security focus

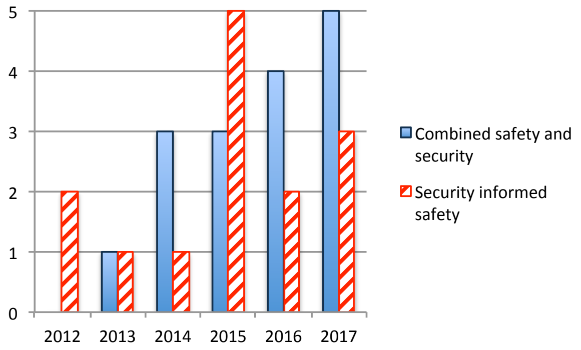

Fig. 3: The yearly paper distribution based on their safety/security focus

focus on the interplay of safety and security. We can notice that most works on combined safety and security analyses address the problem in a generic manner, while the security informed safety analyses are mostly associated with the automotive domain. In fact, both generic and approaches from the industrial control systems domain put more focus on combined safety and security approaches, while the automotive domain is the only one that focuses on the security informed safety. Furthermore, we can notice that unified analyses dominate both automotive and generic domains in security informed safety. Although, unified analyses also dominate combined safety and security approaches, there is quite some works that rely on harmonisation of parallel safety and security analyses in this category.

IV. Validity of Results

As with all empirical studies, there are many threats to validity that may impair the generalisability of the results. In this section we address the most prominent threats to validity [7] namely publication bias as well as bias in data selection, extraction and classification.

A. Publication Bias

A threat that the examined research literature does not represent all the available knowledge on the topic is always present, i.e., due to exclusion of on-line databases that might have relevant publications, in our case Science Direct. Publication bias is one of the reasons that contribute to that threat since positive results are more likely to be published than negative ones. Meaning, solutions that do not work might not get published. In our search we have focused on three independent publishers and a WoS as a common source. We have focused only on peer-reviewed publications in English, leaving out grey literature such as PhD theses, reports and papers that have not been peer reviewed. Furthermore, we have seen fewer results from the industry on this topic, which may be due to the fact that an industrial funder chooses not to publish certain results. This may be due to commercial opportunities, but also not to reveal ways in which security vulnerabilities are handled, which may in itself be a security vulnerability if it becomes known that a certain analysis misses certain types of security vulnerabilities. Based on our contacts with industrial practitioners, we believe the risk of this threat is minimal. Nevertheless, we plan to investigate this threat in the future by validating its results with the practitioners.

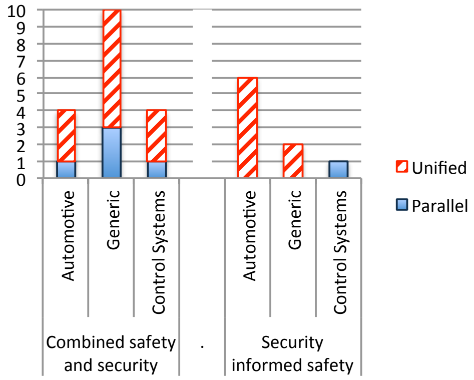

Fig. 4: The paper distribution based on the domain and their safety/security focus

B. Bias in Data Selection

One of the steps that have been taken in order to identify relevant studies for this review has been discussion on research questions, the inclusion/exclusion criterion, as well as search strategy. We have been able to agree upon research questions and derive from research questions a suitable search string. We have made sure that all involved researches had the same definitions of terms related to this study. Also, our selection process has been divided in several stages in order to further reduce the risk of excluding relevant studies. Furthermore, all authors have been involved in the study selection process based on the inclusion/exclusion criterion. The collected publications have been reviewed first based on their titles and abstracts and in cases when no decision could be made based on the abstracts and titles, a full-text reading was performed to decide about the relevance of the paper for our study.

The decision results from Stage 2 (see Table II), where the review has been conducted by all three reviewers, i.e., authors of this paper, have been analysed by means of Cohen's kappa coefficient extended for a case with more than two reviewers and multiple grading scale [53]. The kappa coefficient for Stage 2 is 0.48, which falls into *Moderate Strength Agreement* group [54]. A possible cause for the level of agreement being only moderate is the fact that reviewers are coming from three different domains, namely safety, security, and formal methods. To minimise the risk of excluding relevant studies, we have discussed and taken to the next stage all papers that have been marked as relevant by at least two reviewers.

C. Bias in Data Extraction and Misclassification

To reduce the risk of wrong data extraction and classification, all authors have agreed upon the set of information to be extracted from the selected papers. In many cases we had to interpret information ourselves. For example, whether an approach focuses more on safety or security or both equally, but even simpler information such as validation type could not be simply extracted, e.g., the type of validation used in a paper could not be simply taken as stated in the paper since different papers consider the same type of validation differently. Case study in one paper is an application example in another, so we chose to interpret ourselves the type of validation so we could have comparable values. To ensure the agreement over the extracted data and classification, first, each author extracted data from a subset of papers. Then authors verified each others data by reviewing the papers themselves. All differences were discussed amongst all the authors.

V. Related Work

Safety and security interplay can be considered from many perspectives, e.g., one of the aspects is their joint consideration from a process point of view. Sabaliauskaite et al. [55] consider domain lifecycle alignment on an example of ISA84 (IEC 61511) and ISA99 (IEC 62443) standards. An overview of lifecycles provided by standards from both domains is presented by Schmittner et al. [56], where authors have identified the main phases of safety and security processes and proposed a combined version. However, in this work we focus only on analyses related to early system development stages. Chockalingam et al. [57] present a survey on integrated safety and security risk assessments methods and their application domains. An overview of approaches based on attack and fault trees has been presented by V. Nagaraju et al. [58]. In our review, we consider system analyses without a limitation to a particular approach form, moreover identified methods have been analysed depending on more general categories, e.g., association to existing standards, approach validation, etc. In 2013 Piètre-Cambacédès et al. [59] provided a survey on differences and similarities with respect to security and safety approaches, along with their interdependencies and possible adaptation of approaches from one domain into the another. The authors have presented a comprehensive analysis of both domains including operational principles, assessment methods, architectural concepts and approaches suitable for adaptation in the other domain. S. Kriaa et al. [5] present a survey on combined safety and security approaches with focus on industrial control applications. The main criteria for the analysis has been lifecycle phases for an approach application, whether integration or unification of an approach is a base for a joint consideration of two domains, and whether it is qualitative or quantitative method. In contrast to both above mentioned works, our study is focused on already developed and evaluated approaches, and how safety and security overlap is addressed within them.

VI. Conclusions

We have witnessed an increased need of safety and security co-analysis in the recent years. In this paper we have presented a systematic literature review exploring ways and trends in addressing safety and security co-analysis in system engineering. Since safety and security can negatively influence each other, analysing their interplay in an efficient manner means reducing the effort that needs to be invested in achieving a safe and secure system. The results of our review indicate that the most works focus on unified safety and security analysis that aims at exploring the influence of both security on safety and vice versa. This is the absolute case for approaches considering both threats/hazards analyses and requirements engineering. Concerning the influence of security on safety within the safety analysis, also referred to as security informed safety, the automotive domain is the main driver in that direction. Considering that combined safety and security analysis can be used for both achieving safe and secure systems, we have noticed increase in published research of such analyses for the reviewed period. The results also indicate that there is no work addressing safety within existing security analyses, i.e., safety informed security analyses. Furthermore, we have identified that many works lack extensive evaluation of the proposed approaches and methodologies. We have also noticed that the identified approaches lack evaluation of their support for efficient system update handling that characterises the security-critical systems. The lack of focus on such an important issue regarding the dynamic nature of security and its influence on safety may impair the applicability of the approaches in safety and security–critical systems. It is evident that more efforts are needed in proposing new and evaluating existing proposals for co-analysis of safety and security in all application areas.

Acknowledgement

This work is performed within the following projects: RAASS project (the Vinnova PiiA program); SafeCOP project (ECSEL JU, grant agreement n692529 and National funding); the FiC project (SSF) and the SAFSEC-CPS project (KKS).

References

[1] CENELEC, *IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. Parts 1-7.* International Electrotechnical Comission, 2010.

[2] W. Young and N. G. Leveson, "An integrated approach to safety and security based on systems theory," *Commun. ACM*, vol. 57, no. 2, 2014.

[3] R. Kissel, *Glossary of key information security terms.* U.S. Dept. of Commerce, National Institute of Standards and Technology, 2006.

[4] C. Schmittner, Z. Ma, E. Schoitsch, and T. Gruber, "A Case Study of FMVEA and CHASSIS As Safety and Security Co-Analysis Method for Automotive Cyber-physical Systems," in *1st ACM Workshop on Cyber-Physical System Security*, 2015.

[5] S. Kriaa, L. Piètre-Cambacédès, M. Bouissou, and Y. Halgand, "A survey of approaches combining safety and security for industrial control systems," *Reliability Engineering and System Safety*, 2015.

[6] W. Young and N. Leveson, "Systems thinking for safety and security," in *Proceedings of the 29th Annual Computer Security Applications Conference*, ser. ACSAC. ACM, 2013.

[7] B. Kitchenham and S. Charters, “Guidelines for performing systematic literature reviews in software engineering version 2.3,” EBSE Technical Report, Keele University and University of Durham, 2007.

[8] N. G. Leveson, *Safeware: System Safety and Computers*. ACM, 1995.

[9] SAE J3061, “Cybersecurity Guidebook for Cyber-Physical Vehicle Systems.” SAE International, 2016.

[10] C. Raspotnig, P. Karpati, and V. Katta, *A Combined Process for Elicitation and Analysis of Safety and Security Requirements*. Springer, 2012.

[11] F. Reichenbach, J. Endresen, M. M. R. Chowdhury, and J. Rossebø, “A pragmatic approach on combined safety and security risk analysis,” in *23rd IEEE International Symposium on Software Reliability Engineering*, 2012.

[12] N. Silva and R. Lopes, “Practical experiences with real-world systems: Security in the world of reliable and safe systems,” in *43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W)*, 2013.

[13] Y.-R. Chen, S.-J. Chen, P.-A. Hsiung, and I.-H. Chou, “Unified security and safety risk assessment - A case study on nuclear power plant,” in *TSA*. IEEE, 2014.

[14] NIST, “NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments,” 2012.

[15] M. Ito, *Finding Threats with Hazards in the Concept Phase of Product Development*, 2014.

[16] D. F. D’Souza and A. C. Wills, *Objects, Components, and Frameworks with UML: The Catalysis Approach*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1999.

[17] S. Kriaa, M. Bouissou, F. Colin, Y. Halgand, and L. Pietre-Cambacedes, *Safety and Security Interactions Modeling Using the BDMP Formalism: Case Study of a Pipeline*. Springer, 2014.

[18] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch, *Security Application of Failure Mode and Effect Analysis (FMEA)*. Springer, 2014.

[19] International Electrotechnical Commission, “IEC 60812: Analysis techniques for system reliability - procedure for failure mode and effects analysis (FMEA),” 2006.

[20] Microsoft Corporation, “The STRIDE threat model,” 2005.

[21] L. Apvrille and Y. Roudier, *Designing Safe and Secure Embedded and Cyber-Physical Systems with SysML-Sec*. Springer, 2015.

[22] F. Balarin, Y. Watanabe, H. Hsieh, L. Lavagno, C. Passerone, and A. Sangiovanni-Vincentelli, “Metropolis: an integrated electronic system design environment,” *Computer journal*, 2003.

[23] A. Cimatti, R. DeLong, D. Marcantonio, and S. Tonetta, *Combining MILS with Contract-Based Design for Safety and Security Requirements*. Springer, 2015.

[24] T. Gu, M. Lu, and L. Li, “Extracting interdependent requirements and resolving conflicted requirements of safety and security for industrial control systems,” in *1st International Conference on Reliability Systems Engineering*, 2015.

[25] S. Kriaa, M. Bouissou, and Y. Laarouchi, “A model based approach for scada safety and security joint modelling: S-cube,” in *10th IET System Safety and Cyber-Security Conference*, 2015.

[26] G. Macher, A. Höller, H. Sporer, E. Armengaud, and C. Kreiner, *A Combined Safety-Hazards and Security-Threat Analysis Method for Automotive Systems*. Springer, 2015.

[27] International Organization for Standardization (ISO), *ISO 26262: Road vehicles — Functional safety*. ISO, 2011.

[28] P. T. Popov, *Stochastic Modeling of Safety and Security of the e-Motor, an ASIL-D Device*. Springer, 2015.

[29] M. Steiner and P. Liggesmeyer, *Qualitative and Quantitative Analysis of CFTs Taking Security Causes into Account*. Springer, 2015.

[30] International Electrotechnical Commission, “IEC 61025: Fault Tree Analysis (FTA), year = 2006.”

[31] J. Wei, Y. Matsubara, and H. Takada, “HAZOP-based security analysis for embedded systems: Case study of open source immobilizer protocol stack,” in *7th International Conference on Electronics, Computers and Artificial Intelligence*, 2015.

[32] M. M. Islam, A. Lautenbach, C. Sandberg, and T. Olovsson, “A risk assessment framework for automotive embedded systems,” in *2nd ACM International Workshop on Cyber-Physical System Security*, 2016.

[33] J. P. Nicklas, M. Mamrot, P. Winzer, D. Lichte, S. Marchlewitz, and K. D. Wolf, “Use case based approach for an integrated consideration of safety and security aspects for smart home applications,” in *11th System of Systems Engineering Conference*, 2016.

[34] C. Ponsard, G. Dallons, and P. Massonet, *Goal-Oriented Co-Engineering of Security and Safety Requirements in Cyber-Physical Systems*. Springer, 2016.

[35] C. Schmittner, Z. Ma, and P. Puschner, *Limitation and Improvement of STPA-Sec for Safety and Security Co-analysis*. Springer, 2016.

[36] S. S. Shapiro, “Privacy risk analysis based on system control structures: Adapting system-theoretic process analysis for privacy engineering,” in *IEEE Security and Privacy Workshops*, 2016.

[37] E. Troubitsyna, “An integrated approach to deriving safety and security requirements from safety cases,” in *40th Annual Computer Software and Applications Conference*. IEEE, 2016.

[38] J. Dürrwang, K. Beckers, and R. Kriesten, “A lightweight threat analysis approach intertwining safety and security for the automotive domain,” in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2017.

[39] I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, and S. Sezer, “STPA-SafeSec: Safety and security analysis for cyber-physical systems,” *Journal of Information Security and Applications*, 2017.

[40] D. Pereira, C. Hirata, R. Pagliares, and S. Nadjm-Tehrani, “Towards combined safety and security constraints analysis,” in *Int. Conference on Computer Safety, Reliability, and Security*. Springer, 2017.

[41] G. Howard, M. Butler, J. Colley, and V. Sassone, “Formal Analysis of Safety and Security Requirements of Critical Systems Supported by an Extended STPA Methodology,” in *2017 IEEE European Symposium on Security and Privacy Workshops*, 2017.

[42] R. Kumar and M. Stoelinga, “Quantitative security and safety analysis with attack-fault trees,” in *18th IEEE International Symposium on High Assurance Systems Engineering*, 2017.

[43] S. Plósz, C. Schmittner, and P. Varga, “Combining safety and security analysis for industrial collaborative automation systems,” in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2017.

[44] S. Procter, E. Y. Vasserman, and J. Hatcliff, “SAFE and Secure: Deeply Integrating Security in a New Hazard Analysis,” in *12th ACM International Conference on Availability, Reliability and Security*, 2017.

[45] E. Ruijters, S. Schivo, M. Stoelinga, and A. Rensink, “Uniform analysis of fault trees through model transformations,” in *2017 Annual Reliability and Maintainability Symposium*, 2017.

[46] G. Sabaliauskaite and S. Adepu, “Integrating six-step model with information flow diagrams for comprehensive analysis of cyber-physical system safety and security,” in *18th IEEE International Symposium on High Assurance Systems Engineering*, 2017.

[47] W. G. Temple, Y. Wu, B. Chen, and Z. Kalbarczyk, “Systems-theoretic likelihood and severity analysis for safety and security co-engineering,” in *Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification*. Springer, 2017.

[48] C. Schmittner, Z. Ma, and P. Smith, *FMVEA for Safety and Security Analysis of Intelligent and Cooperative Vehicles*. Springer, 2014.

[49] I. Vistbakka, E. Troubitsyna, T. Kuismin, and T. Latvala, “Co-engineering safety and security in industrial control systems: A formal outlook,” in *Software Engineering for Resilient Systems*. Springer, 2017.

[50] J.-R. Abrial, *Modeling in Event-B: System and Software Engineering*, 1st ed. Cambridge University Press, 2010.

[51] L. Piètre-Cambacédès and M. Bouissou, “Modeling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes),” in *IEEE International Conference on Systems, Man and Cybernetics*, 2010.

[52] P. Johnson, D. Gorton, R. Lagerström, and M. Ekstedt, “Time between vulnerability disclosures: A measure of software product vulnerability,” *Computers & Security*, 2016.

[53] J. Fleiss, “Measuring nominal scale agreement among many raters,” *Psychological Bulletin*, 1971.

[54] J. R. Landis and G. G. Koch, “The measurement of observer agreement for categorical data,” *Biometrics*, 1977.

[55] G. Sabaliauskaite and A. P. Mathur, *Aligning Cyber-Physical System Safety and Security*. Springer, 2015.

[56] C. Schmittner, Z. Ma, and E. Schoitsch, “Combined safety and security development lifecylce,” in *13th IEEE International Conference on Industrial Informatics*, 2015.

[57] S. Chockalingam, D. Hadziosmanovic, W. Pieters, A. Texeira, and P. van Gelder, *Integrated Safety and Security Risk Assessment Methods: A Survey of Key Characteristics and Applications*. Springer, 2016.

[58] V. Nagaraju, L. Fiondella, and T. Wandji, “A survey of fault and attack tree modeling and analysis for cyber risk management,” in *IEEE International Symposium on Technologies for Homeland Security*, 2017.

[59] L. Piètre-Cambacédès and M. Bouissou, “Cross-fertilization between safety and security engineering,” *Reliability Engineering and System Safety*, 2013.