Roadblocks on the Highway to Secure Cars: An Exploratory Survey on the Current Safety and Security Practice of the Automotive Industry

Michael Huber[1(✉)], Michael Brunner[1], Clemens Sauerwein[1], Carmen Carlan[2], and Ruth Breu[1]

[1] Department of Computer Science, University of Innsbruck, Innsbruck, Austria
{michael.huber,michael.brunner,clemens.sauerwein,ruth.breu}@uibk.ac.at
[2] fortiss GmbH, Munich, Germany
carlan@fortiss.org

Abstract. With various advances in technology, cars evolved to highly interconnected and complex Cyber-Physical Systems. Due to this development, the security of involved components and systems needs to be addressed in a rigorous way. The resulting necessity of combining safety and security aspects during the development processes has proven to be non-trivial due to the high interference between these aspects and their respective treatment. This paper discusses the results of an exploratory survey on how organizations from the automotive industry in the Euroregion tackle the challenge of integrating safety and security aspects during system development. The observed state of practice shows that there are significant deficits in the integration of both domains. The results of the exploratory survey enabled us to identify the most common challenges of realizing an integrated approach in a practical setting and discuss implications for future research.

Keywords: Automotive · Cyber-Physical Systems · Safety · Security Integration · Industrial survey

1 Introduction

The upcoming generation of Cyber-Physical Systems (CPSs) will be characterized by fragmentation, heterogeneity, short release cycles, cross-organizational nature and safety criticality [6]. Due to technological advances, safety-critical CPSs like modern vehicles become security-sensitive, with high interference between safety and security requirements that need to be addressed [1,17,22]. These – and many more – new conditions pose a specific challenge for the development and ongoing operation of CPSs: The integrated treatment of safety and security aspects [10]. Within this paper, the definition of safety and security is in accordance with [7], that is, safety is concerned with protecting valuable assets

B. Gallina et al. (Eds.): SAFECOMP 2018, LNCS 11093, pp. 157–171, 2018.
https://doi.org/10.1007/978-3-319-99130-6_11

by preventing, detecting and properly reacting to accidental harm. Security, in contrast, is concerned with protecting these assets by preventing, detecting and properly reacting to malicious harm [7]. The automotive domain is particularly affected, since innovation-related challenges are transforming the traditional automotive industry [11]. Unlike the nuclear or avionics industry, where certification of products or systems usually follows a process-oriented approach (i.e., a system is considered safe when developed in accordance to processes mandated by industry standards), manufacturers in the automotive industry need to show that they achieved certain safety objectives using safety assurance cases as required by the ISO 26262 [12] standard. Assurance cases are an established method within certification processes of embedded systems. They trace safety goals down to safety solutions and provide arguments supported by evidence for the satisfaction of relevant types of system properties within a certain context and under certain assumptions [3,14]. When assurance cases offer argumentation and evidence for the correct implementation of a system's safety requirements, they are called safety cases.

In recent years, a considerable amount of research has been done on safety and security assurance in the automotive domain [10,19,27]. To the best of our knowledge, the perspective of industry regarding this matter has hardly been investigated. In order to address this gap, we explored how industry deals with potentially interrelated safety and security aspects during development of CPSs and components.

We conducted an exploratory survey in the automotive domain with organizations which have their headquarter in the Euroregion. By means of in-depth interviews with system development experts, we were able to observe the current state of practice and prevalent challenges. In addition, we evaluated our previously proposed conceptual model [4] for safety and security aspects of CPSs.

The remainder of this paper is structured as follows: Sect. 2 describes the applied research methodology. Section 3 presents the results of the survey and discusses threats to validity. Section 4 presents key findings from the survey, their implications for future research and motivates the use of a holistic model. Section 5 presents related work. Finally, Sect. 6 concludes the paper and provides an outlook on future work.

2 Research Methodology

The main goal of our research is to better understand how the challenge of treating safety and security assurance in an integrated manner during the development and operation of CPSs is confronted by the automotive domain. Our research objective is to analyze the current real-world difficulties of realizing an integrated approach in order to elicit challenges that occur in practical settings. In the pursuit of achieving this objective, we investigate the current state of practice by answering the following research questions:

RQ1: What is the state of practice to unify or synchronize methods and processes of the safety and security domain?

RQ2: How is the safety and security domain differentiated regarding definitions, requirements, processes and utilized tools?
RQ3: How are interdependencies between the safety and security domain identified and treated?

The remainder of this section is dedicated to the design of the conducted exploratory survey, the applied procedure for data collection and a thorough description of survey participants and their selection procedure.

2.1 Survey Design

A survey is a comprehensive research method for collecting information to describe, compare, or explain knowledge and behavior [15]. In order to observe the relevant aspects regarding the safety and security assurance of CPSs in a practical setting, we followed the paradigm of exploratory research. We collected data using expert interviews. This allowed for a flexible research design and quick adaptation to changes in the observed phenomenon [30].

The survey design followed a three-step process with (1) an initial survey design proposal, (2) a subsequent refinement of central questions and finally, (3) a pilot interview to validate the survey design in a practical setting. In order to structure and define the initial survey design, we utilized a conceptual model which was previously developed to document security and safety requirements in an integrated manner to support certification processes during design and run-time phases of CPSs [4]. This model unifies relevant documentation artifacts from four main domains: *Requirements Engineering*, *System Modeling*, *Risk Assessment*, and *Evidence Documentation*. Requirements are modeled in a hierarchical fashion distinguishing between functional and non-functional requirements (primarily concerning safety and security aspects). System Modeling is represented as the interrelated composition of hardware and software components. Risk Assessment is primarily derived from vulnerabilities and corresponding threats. Evidence Documentation is modeled based on various kinds of assurance artifacts.

Guided by the structure of this model, we derived questions for the survey that aligned with our research questions. The initial proposal, as well as the final survey, comprised a single key question and three sets of additional structural questions to guide the interview process. All questions were formulated in German and later translated into English for interviewees not speaking German. The key question was closely related to our research objective and formulated to approach the subject as broadly as possible in order to prevent the introduction of an initial bias to the interview. Subsequently we defined the following key question:

> "What are the three main challenges for an integrated consideration of security and safety aspects in the development and operation of cyber-physical systems in the automotive domain?"

All structural questions were intended to pinpoint and further refine our understanding of the participants' response to the key question and helped us answer our research questions (i.e., RQ1, RQ2 and RQ3). The aforementioned conceptual model was used as a basis for the structural questions and as a visual representation of potentially relevant structures, processes, and interfaces in order to encourage discussions during the interviews. Figure 1 illustrates the final survey design and all relevant documentation artifacts that were prepared.

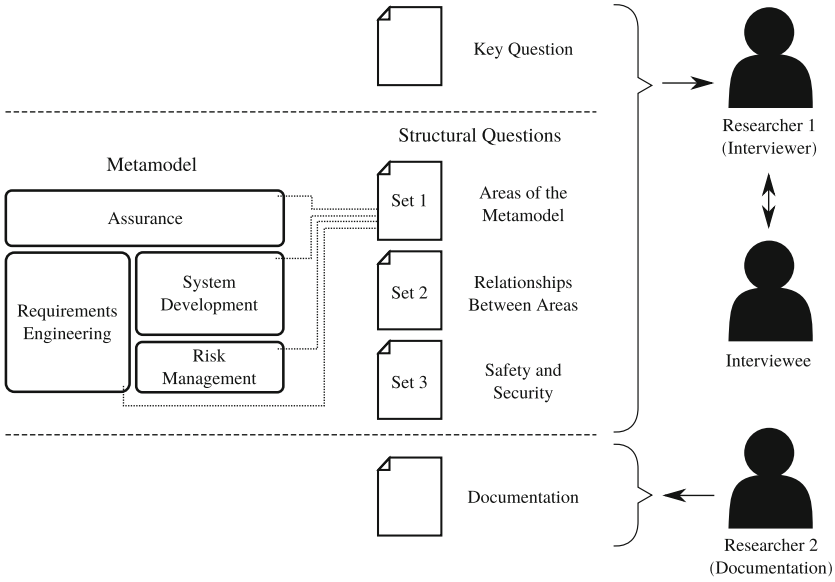

Fig. 1. Structure of the survey

The first set of structural questions covered the *four areas of the conceptual model independently*, addressing activities involving requirements engineering, system development, risk management, and evidence documentation. These questions were aimed at identifying involved stakeholders, utilized tools, relevant data sources and the most prominent challenges occurring in the respective area. For each of the four areas, the same set of questions was used. For example, we asked *"What tools are used for requirements engineering?"* and *"What stakeholders are involved in the assessment of risks?"*.

The second set of structural questions was concerned with the *relationships between the different areas of the conceptual model* considering exchanged information, nature of communication, utilized tools, methods, processes and the most prominent challenges. For example, we asked *"How is information between stakeholders performing risk analysis and stakeholders responsible for requirements engineering exchanged?"* and *"Do you use any software solutions to facilitate this communication?"*.

The third set of structural questions were aimed at understanding the respective organization's *differentiation between safety and security requirements* concerning definition, methods, processes, tools, their identification, assessment and implementation including interactions with stakeholders. For example, we asked *"How do you differentiate between safety and security requirements?"* and *"Do you use different methods/processes/tools for the identification of safety and security requirements?"*.

An initial pilot interview was used to test and validate our survey design with an expert from the automotive industry. The expert was contacted within the context of the research project SALSA[1] and its industrial network. Criteria for the selection of the expert are described in Sect. 2.4. In a follow-up meeting the pilot expert gave feedback regarding the content and structure of the interview and its delivery. The pilot expert confirmed the alignment of the survey with our research objective. Subsequent changes to the survey design involved time management only.

2.2 Data Collection

All interviews were conducted face-to-face, allowing for a more complex interaction between the interviewers and the participants. Each of the interviews was conducted by two researchers – one taking notes and one interviewing the participants as depicted in Fig. 1. After an initial presentation of the general procedure, purpose, and specific goal of the survey, the participants were asked if they consented to the recording of the interview in audio format. With participants who did not give consent, the process of documenting the interview was conducted in a handwritten format only. This was followed by collecting quantitative data about the participants, their roles and organizations. Finally, the key question was discussed with the help of the aforementioned structural questions and the conceptual model. All questions and illustrations of the model were available in printed format, logically grouped and presented as needed during the interviews. If the interviewee was able to directly respond to the key question, the interviewer chose to discuss and analyze challenges with the appropriate sets of structural questions and the conceptual model in order to gain a detailed understanding. If the interviewee was unable to directly state any challenges, the interviewer presented the conceptual model and followed the first set of structural questions in order to detect problematic areas through deviating data sources, responsibilities, tools or processes. The time required for individual interviews averaged 60 min with only minor deviations. The study was conducted within a time frame of 8 months, starting in February 2017 and ending in September 2017.

2.3 Analysis Procedure

Directly after conducting the interview, the two researchers discussed and documented the obtained data during a debriefing followed by writing a summary

[1] https://salsa.q-e.at/ (Accessed: 02/12/2018).

for each interview. Audio recordings were transcribed and all produced documentation was further analyzed. We followed the guidelines set out by Mayring et al. [21] to produce qualitative summaries from the collected data in order to extract the facets relevant to our research questions [5]. We grouped the results inductively by reducing, paraphrasing, and generalizing relevant text passages.

2.4 Participants

In the context of the research project SALSA and its industrial network, the participants were contacted by e-mail and provided with a brief summary of the survey goals and procedure. Criteria for the selection of participants were (1) employment in a leading role in development and operation of CPSs in the automotive domain or a closely related safety-critical domain, (2) at least 4 years of professional experience and (3) employment at a company with at least 150 employees. Upon agreement to an appointment, the interviews were conducted on site. All participants offered to take part in the interview voluntarily. An overview of all participants is presented in Table 1. The majority of participants held a degree in Computer Science or another engineering discipline. The encountered roles of the participants within the organizations were predominantly titled *Safety Team Leader* or *Safety Manager* with an average of 17 years of experience in their field. All participants represented companies based in, or having their headquarters in the Euroregion. While the majority of these companies were active in the automotive domain, one was active in avionics. Three of these companies were considered small companies with 150 to 1000 employees and the remainder large companies with more than 1000 employees.

Table 1. Participants of the survey

ID	Operational role	Education	Experience	Type of organization	# Employees
A	Safety team leader	University	25 years	Supplier	150–1000
B	Expert SW	University	10 years	OEM	>1000
C	Safety manager	University	4 years	Supplier	150–1000
D	System engineer	Technical apprentice-ship	24 years	Consulting	>1000
E	Director safety management	University	25 years	Supplier	>1000
F	Safety team leader	University	11 years	Supplier	>1000
G	Team leader	University	21 years	Supplier	150–1000
H	Chief expert safety, security, reliability, availability	University	22 years	OEM and supplier	>1000

3 Results

In this section we present the results of our survey by addressing the research questions depicted in Sect. 2. Subsequently, we highlight identified challenges and discuss threats to validity.

3.1 State of Practice Regarding the Unification of the Safety and Security Domain

We encountered three distinct cases concerning the integration of the safety and security domains. Interviewees G and H followed an (1) integrated approach where both domains were considered from the beginning of the system life cycle. All remaining interviewees A-F either (2) treated security as an afterthought, where existing concepts, functionalities, and components were analyzed for their security relevance or (3) did not consider the security domain.

Participants G and H stated that their companies treat security and safety requirements in an integrated way. The company interviewee G works for employs dedicated security teams. The company follows a system development process which involves these security teams from initial phases. Furthermore, there exists a set of internal security guidelines and specifications, however, their source, content, and application, as well as the security teams' interactions with the safety processes or other entities during development or operation were kept confidential by the interviewee. There are dedicated security teams in the company participant H works for also. Processes like HAZOP [16] in the safety domain and threat analysis in the security domain were said to be executed in parallel with defined points of synchronization to treat interdependencies between both domains. Participant H mentioned the organization's approach to be in an early stage, thus, when and how to synchronize both domains was not clearly stated. The approach addresses economical interests by keeping adaptations or changes to established processes of the safety domain to a minimum with processes of the security domain being decoupled, at least during the elicitation of requirements.

When treating security as an afterthought only, a truly bidirectional consideration of the influences of the safety and security domains of the System Under Development (SUD), including treatment, is only possible with considerable and often economically unviable effort, as stated by participant A and D. In case of occurring conflicts between both domains, late treatments might entail costly changes to prevalent system designs. As stated by participant D, this is due to the potential of the safety and security considerations to influence the architecture of a system. Participant A compared this situation to requirements which are supplied by the customer in a late phase of the system life cycle and require changes to the prevalent system design. This circumstance was stated to not be economically desirable. However, participant A and H pointed out that in some cases knowledge of the system which is only available in later phases of the system life cycle or only within the context of the system of a subordinate organization of the supply chain is required. The statement emphasizes the necessity

to synchronize the safety and security life cycles within the overall system life cycle and to proper orchestrate, distribute and communicate safety and security objectives which span multiple organizations of a supply chain.

Classical software engineering problems were observed as a challenge complicating the integration of security aspects. Mastering the current complexity of existing work flows was a frequently mentioned problem. The amount of artifacts accumulating during development processes (for example processes compliant with the V-model XT [8]) were stated to be difficult to manage. Artifacts explicitly named by the participants were: *Process documents* required by ISO 26262 [12] which are necessary for subsequent processes and the establishment of evidence traces through assurance procedures. *Requirements*, imposed on development processes and the SUD which originate from standards, internal documents, and customers. The volume and complex structure of these artifacts were stated to result in difficulties in *traceability*, a recognized problem in software engineering [13].

The problem to establish links and traces throughout the aforementioned artifacts is further exacerbated by the *heterogeneous and diverse tool landscape*, as stated by all participants. Besides popular software solutions, like IBM Rational DOORS and PTC-Integrity for e.g. requirements engineering purposes, Enterprise Architect and Visio for e.g. system development and Microsoft Word and Microsoft Excel for e.g. risk management and assurance purposes, all participants use a variety of proprietary tools developed by the companies. Their purpose is to accommodate for missing functionalities, provide adaptations in highly customized processes and to support intercommunication between different tools. The result is a *complex tool chain*, sometimes unique to even a particular project within an organization. This has consequences for the integration of safety and security as well due to rigid and time intensive *change management*. Participant G stated a case of obsolescence management where the removal of a tool from the tool chain made subsequent changes or any kind of maintenance impossible.

Another frequently mentioned challenge were *economical aspects*. It is well known that the costs of software engineering projects may rapidly escalate [2]. As stated by all participants, the amount and quality of treating security properties will always be limited by available resources within a project's budget and prioritized by the severity of consequences.

3.2 Differences Between the Safety and Security Domain

All interviewees exhibited a uniform understanding of the distinction between the two types of system qualities, citing generally accepted definitions for the safety and security domains [7], respectively. However, concerning the requirements engineering domain, we observed no distinction between safety and security requirements in conducted processes or utilized software solutions for participants A-F, who treat security as an afterthought. As an example, interviewee A described the combined administration of safety and security requirements in the software solution *PTC Integrity* where security requirements are assigned

the Automotive Safety Integrity Level (ASIL) of Quality Management (QM). This is normally used to declare the risk associated with a safety requirement as not being unreasonable and therefore would not require any dedicated safety treatment as declared in the ISO 26262 standard [12]. The definition of safety requirements was stated to be conducted in accordance with the ISO 26262 standard, whereas the origin of security requirements was limited to requirements imposed by customers. As for the combined approach depicted by interviewee H, there was no distinction between requirements from both domains after their definition, except for testing procedures. The definition of security requirements was conducted within a threat analysis which was decoupled from the definition of safety requirements.

Regarding risk assessment, no safety and security co-analysis was mentioned to be applied by participants A–H. Furthermore, all interviewees acknowledged the fact that while they are able to rely on years of experience, standards, and guidelines in the safety domain, they are unable to do so in the security domain. This holds especially true for risk assessment, as stated by many participants. Interviewees A, C, and F stated that they are not obliged to comply with any security standard and thus security problems are only dealt with if the customer demands it and if it is within the limit of the project budget.

The difference between both domains on a process level was stressed by participants A, E, and G. One example given by interviewee A was that while tasks concerning the safety assurance of a vehicle are completed by the Start Of Production (SOP), the scope of the security domain extends into the operational phase where new security incidents have to be dealt with until decommission. Furthermore, due to the nature of security, the time frame in which a security measure remains effective is unpredictable. This contradicts the scope and resource allocation of the classical safety domain. Interviewees A, E, and G gave this circumstance as a reason for why prevalent safety processes are unfit to deal with security properties of a system.

Interviewees A, C, and E mentioned that there are no dedicated employees for the security domain, even when security issues are taken into account and addressed. These responsibilities are integrated into roles like safety managers, system engineers, or system architects.

3.3 Elicitation and Treatment of Interdependencies Between the Safety and Security Domain

We encountered two organizations, G and H, that follow an integrated approach. Both representatives of these organizations described the classification of occurring interdependencies between the safety and security domain as published in [18], namely: *conditional*, *reinforcement*, *antagonism*, and *independence*. Due to confidentiality concerns, we are unable to provide details about the integrated approach followed by participant G. As for participant H, the elicitation and treatment of interdependencies between safety and security requirements is conducted within defined points in the system life cycle, where both domains were

synchronized. The interviewee stated the approach to be in an early stage. Challenges were said to be (1) the meaningful definition of points in the system life cycle where it makes sense to jointly consider artifacts of both domains and (2) develop efficient, holistic and systematic approaches for the elicitation and resolution of these interdependencies within the points of synchronization. Participant H stated that their approach utilizes the concept of risk as a common ground between the safety and security domains in order to harmonize processes for the mitigation of risk. In order to improve the maturity of their approach, processes and methods within these synchronization points were stated to be the main focus of current internal research.

Participant E treats conflicting safety and security requirements by conducting risk assessments in order to determine and prioritize requirements which have more severe consequences. No further method for the elicitation or treatment of interdependencies between the safety and security domain were encountered in the course of the survey.

3.4 Identified Challenges

Concerning our research objective, we identified the following challenges for an integrated consideration of security and safety aspects in the development and operation of CPSs in the automotive domain: (1) Coping with the complexity of prevalent development processes and overcoming traceability issues to enable appropriate change management and thus timely responses to security incidents. (2) Dealing with economic limitations regarding the increased complexity due to interdependencies between domains, the extended time frame in which security has to be treated and the possibly, timely restricted, viability of measures taken. (3) Dealing with the current lack of experience, standards, and guidelines concerning the combination of the safety and the security domain.

3.5 Threats to Validity

Our survey might be limited by certain threats to validity that we are aware of and, to the best of our knowledge, counteracted. The following argumentation is based on the guidelines set out by Runeson et al. [26].

Concerning construct validity, a major objective of the survey was to understand the participants' respective understanding and practice of the subject under investigation. We argue that the nature of our survey inherently counters threats to construct validity. Furthermore, in order to overcome limitations regarding language barriers, we offered interviews in English and German language. The interviews were always moderated by a researcher proficient in the interview language, all handouts, interview guidelines, and questions have been carefully translated and double-checked by native speakers.

Threats to internal validity were avoided by peer debriefing. Concerning external validity, our survey is highly focused and can not be generalized to other domains without considering potential differences.

In order to counter threats to reliability, we avoided influences of moderators through a predefined protocol including a preset pool of questions and dedicated interview guidelines. Moreover, all interviews were conducted by two researchers with fixed roles which were asking the participant questions and documenting the course of the interview, respectively. We further avoided influencing the participants before interviews by only providing broadly formulated contextual informations beforehand.

In order to counteract a biased selection of study participants, we selected interviewees based on criteria as described in Sect. 2.4. Finally, limitations from biased opinion of interviewees were avoided by comparing the transcripts and results of different interviews.

4 Discussion

In this section we derive four key findings from the previously presented answers to the research questions alongside their implications for future research. The section concludes by motivating the use of a holistic model.

We observed that (KF1) *the majority of organizations not actively take interdependencies between safety and security requirements into account.* The majority of participants stated that they do not follow an integrated approach and treat security only if explicitly requested. The current state of practice was claimed to be due to the novelty of the security domain within the automotive industry, lack of standards, guidance and experience, and economic limitations. Further research is necessary in order to be able to synchronize the safety and security life cycle, facilitating efficient and holistic elicitation and treatment of interdependencies.

In addition, (KF2) *prevalent problems concerning complexity, traceability, change management and availability of recourses complicate the integration of security.* The most common consequences inherent to the complexity faced in prevalent development processes are difficulties in traceability and the resulting inefficient change management. The average time to re-certify a system as a consequence of applied changes, due to a security incident, was stated to be too long for the volatile security domain. Future research needs to investigate how to reduce and/or manage the complexity of prevalent development processes in order to facilitate traceability and change management which is applicable for the security domain. Economic limitations further hamper the integration of security, especially maintaining traceability for effective change management is expensive [13]. Developed approaches need to be economically viable, despite the extended time frame in which security has to be treated, the elicitation and resolution of conflicts between requirements and the possibly time-restricted viability of measures taken to mitigate risks.

Participants stated that (KF3) *objectives of the security domain, as well as the safety domain span across multiple organizations.* Further research needs to investigate how to orchestrate, distribute and communicate responsibilities concerning these objectives within an inter-organizational context in order to

facilitate synchronization of the safety and security life cycle regarding processes and process artifacts within the system life cycle of a single organization.

We observed a (KF4) *uniform understanding and general awareness concerning the differences between the safety and security domain.* All interviewees cited generally accepted definitions for the safety and security domain, according to [24]. Participants following an integrated approach described the classification of occurring interdependencies between the safety and security domain as published in [18].

The challenges identified in Sect. 3.4 and the key findings presented above emphasize the necessity for a holistic model which unifies documentation artifacts, e.g. process documents of the system life cycle, in order to reduce complexity and facilitate efficient change management. Our conceptual model [4], which was validated during the course of the survey, was perceived as correct and suitable by interview partners. The model unifies relevant documentation artifacts from requirements engineering, system modeling, risk assessment and evidence documentation. It further establishes dependencies between documentation artifacts of different areas (e.g., between individual requirements, the system components they are defined for, the associated risks and available evidence showing the correct implementation of said requirements). The model constitutes a base for future research by enabling cross-domain documentation of safety and security requirements, and unifying design- and runtime aspects while supporting (re-)certification in accordance with prevalent security and safety standards.

5 Related Work

In recent years, the integrated handling of safety and security has gained more and more interest in the research community. While the research community is concerned with the importance of integrating safety and security and proposes various approaches [18], there are no insights into how this problem is currently treated in industrial practice. To the best of our knowledge, no survey has been performed regarding the integrated consideration of safety and security for CPSs in the automotive industry.

Kriaa et al. [18] provide an overview of a number of industry reports on approaches integrating safety and security treatment. While their work shows that various industries are interested in an integrated treatment of the safety and security domains, our survey focuses on the automotive industry and identifies real world challenges which prohibit a trivial integration of these approaches into prevalent development processes. Glas et al. [10] investigate the integration of the safety and security domain by discussing conflicts between safety and security mechanisms, whereas we explore the perspective of the industry in order to elicit challenges emerging from the current state of practice as perceived by representatives of organizations from the automotive industry. An industrial survey conducted in the area of safety engineering by Jose Luis de la Vara et al. [29] gives an overview on practices for safety evidence change impact analysis. Notander et al. [23] report on a survey regarding challenges in

the development of safety-critical systems. Martins et al. [20] conducted expert interviews and studied literature concerning requirements engineering for safety-critical systems. Ray et al. [25] discuss the current state of practice in automotive security architecture, investigating trade-offs between security countermeasures, real-time requirements, and in-field configurability needs. Sojka et al. [28] conducted a case study on testing and validating safety- and security-related properties of control software in the AUTOSAR [9] architecture. They show that the combination of procedures from the safety and security domain can bring economic benefits.

6 Conclusion

We conducted a survey of experts in the automotive domain in order to gain an understanding of real-world challenges occurring when combining safety and security for CPSs during development and operation. We observed significant deficiencies in the integration of both domains. Identified challenges are: (1) Coping with the complexity of prevalent development processes and its consequences, (2) dealing with economic limitations and (3) the current lack of experience, standards and guidelines concerning the combination of the safety and the security domains. We conclude that the utilization of a conceptual model unifying relevant documentation artifacts from requirements engineering, system modeling, risk assessment and evidence documentation can address these issues. Future research will be conducted in alignment with derived criteria in order to investigate how change management can be facilitated by introducing state-machine based automation capabilities to this model. Means to enable state propagation, the definition of accommodating work flows and a prototypical implementation is planned for the near future. A quality and cost model will be developed to assess the economic viability of our approach addressing aforementioned concerns of interviewees.

Acknowledgments. This work was partially supported by the Austrian Federal Ministry of Science, Research and Economics (BMWFW), FFG Project 855383 SALSA (ICT of the Future).

References

1. Almeida, J.R., Camargo, J.B., Cugnasca, P.S.: Safety and security in critical applications and in information systems-a comparative study. IEEE Latin Am. Trans. **11**(4), 1127–1133 (2013)
2. Baheti, R., Gill, H.: Cyber-physical systems. Impact Control Technol. **12**, 161–166 (2011)
3. Bloomfield, R., Bishop, P.: Safety and assurance cases: past, present and possible future-an adelard perspective. In: Dale, C., Anderson, T. (eds.) Making Systems Safer, pp. 51–67. Springer, Heidelberg (2010). https://doi.org/10.1007/978-1-84996-086-1_4

4. Brunner, M., Huber, M., Sauerwein, C., Breu, R.: Towards an integrated model for safety and security requirements of cyber-physical systems. In: 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp. 334–340. IEEE (2017)
5. Campbell, J.L., Quincy, C., Osserman, J., Pedersen, O.K.: Coding in-depth semistructured interviews problems of unitization and intercoder reliability and agreement. Sociol. Methods Res. **42**(3), 294–320 (2013)
6. Derler, P., Lee, E.A., Vincentelli, A.S.: Modeling cyber-physical systems. Proc. IEEE **100**(1), 13–28 (2012)
7. Firesmith, D.G.: Common concepts underlying safety security and survivability engineering. Carnegie-mellon University, Pittsburgh, PA, Software Engineering Institute, Technical report (2003)
8. Friedrich, J., Kuhrmann, M., Sihling, M., Hammerschall, U.: Das V-Modell XT. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-540-76404-5_1
9. Fürst, S., et al.: AUTOSAR-a worldwide standard is on the road. In: 14th International VDI Congress Electronic Systems for Vehicles, Baden-Baden, vol. 62, p. 5 (2009)
10. Glas, B., et al.: Automotive safety and security integration challenges. In: Automotive-Safety & Security 2014 (2015)
11. He, W., Yan, G., Da Xu, L.: Developing vehicular data cloud services in the IoT environment. IEEE Trans. Ind. Inform. **10**(2), 1587–1595 (2014)
12. ISO/TC 22: ISO/DIS 26262–1 - Road vehicles functional safety Part 1–10. Technical report, Technical Committee 22, Geneva, Switzerland, July 2009
13. Kannenberg, A., Saiedian, H.: Why software requirements traceability remains a challenge. CrossTalk J. Defense Softw. Eng. **22**(5), 14–19 (2009)
14. Kelly, T.P.: Arguing safety: a systematic approach to managing safety cases. Ph.D. thesis, University of York (1999)
15. Kitchenham, B.A., Pfleeger, S.L.: Guide to advanced empirical software engineering. Springer, London **46**, 48–49 (2008)
16. Kletz, T.A.: HAZOP and HAZAN: Identifying and Assessing Process Industry Hazards. IChemE, Boca Raton (1999)
17. Kornecki, A.J., Subramanian, N., Zalewski, J.: Studying interrelationships of safety and security for software assurance in cyber-physical systems: approach based on Bayesian belief networks. In: 2013 Federated Conference on Computer Science and Information Systems (FedCSIS), pp. 1393–1399. IEEE (2013)
18. Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., Halgand, Y.: A survey of approaches combining safety and security for industrial control systems. Reliab. Eng. Syst. Saf. **139**, 156–178 (2015)
19. Macher, G., Höller, A., Sporer, H., Armengaud, E., Kreiner, C.: A combined safety-hazards and security-threat analysis method for automotive systems. In: Koornneef, F., van Gulijk, C. (eds.) SAFECOMP 2015. LNCS, vol. 9338, pp. 237–250. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-24249-1_21
20. Martins, L.E., Gorschek, T.: Requirements engineering for safety-critical systems: overview and challenges. IEEE Softw. **34**, 49–57 (2017)
21. Mayring, P., Gläser-Zikuda, M.: Die Praxis der Qualitativen Inhaltsanalyse. Beltz Weinheim (2008)
22. Nostro, N., Bondavalli, A., Silva, N.: Adding security concerns to safety critical certification. In: 2014 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), pp. 521–526. IEEE (2014)

23. Pedersen Notander, J., Höst, M., Runeson, P.: Challenges in flexible safety-critical software development – an industrial qualitative survey. In: Heidrich, J., Oivo, M., Jedlitschka, A., Baldassarre, M.T. (eds.) PROFES 2013. LNCS, vol. 7983, pp. 283–297. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39259-7_23
24. Piètre-Cambacédès, L., Bouissou, M.: Cross-fertilization between safety and security engineering. Reliab. Eng. Syst. Saf. **110**, 110–126 (2013)
25. Ray, S., Chen, W., Bhadra, J., Al Faruque, M.A.: Extensibility in automotive security: current practice and challenges. In: 2017 54th ACM/EDAC/IEEE Design Automation Conference (DAC), pp. 1–6. IEEE (2017)
26. Runeson, P., Host, M., Rainer, A., Regnell, B.: Case Study Research in Software Engineering: Guidelines and Examples. Wiley, Hoboken (2012)
27. Schoitsch, E., Schmittner, C., Ma, Z., Gruber, T.: The need for safety and cybersecurity co-engineering and standardization for highly automated automotive vehicles. In: Schulze, T., Müller, B., Meyer, G. (eds.) Advanced Microsystems for Automotive Applications 2015. LNM, pp. 251–261. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-20855-8_20
28. Sojka, M., Krec, M., Hanzálek, Z.: Case study on combined validation of safety & security requirements. In: 2014 9th IEEE International Symposium on Industrial Embedded Systems (SIES), pp. 244–251. IEEE (2014)
29. de la Vara, J.L., Borg, M., Wnuk, K., Moonen, L.: An industrial survey of safety evidence change impact analysis practice. IEEE Trans. Softw. Eng. **42**(12), 1095–1117 (2016)
30. Wohlin, C., Runeson, P., Höst, M., Ohlsson, M.C., Regnell, B., Wesslén, A.: Experimentation in Software Engineering. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29044-2